Type	Versions	Last Updated
Application	10.4.2	27 July 2025
Help Guide	10.4.2:1	27 July 2025

Introduction

MemberCheck is an AML/CTF compliance service designed to enable you to check individuals and businesses against global sanctions, financial regulatory, law enforcement and politically exposed person lists, in an efficient and cost-effective manner, obtaining immediate and up-to-date feedback on the potential exposure of individuals and corporates to money laundering, terrorism financing activities and reputational risk exposure.

MemberCheck is a secure and comprehensive web-based solution, which is pre-configured with multiple data sources from providers such as Acuris Risk Intelligence, LexisNexis WorldCompliance and MemberCheck's own proprietary data for receiving PEP and sanctioned watchlists.

The service assists reporting entities in meeting their obligations under the AML/CTF Act 2006 (Australia), the AML/CFT Act 2009 (New Zealand) and other AML/CTF legislation worldwide.

Multi-region Service

MemberCheck operates in multiple regions worldwide, giving clients data sovereignty in their chosen location.

Service Region	Link	Release Version
Australia (Global Service)	https://app.membercheck.com	10.4.2
Indonesia (Global Service)	https://app.id.membercheck.com	10.4.2
Germany (Global Service)	https://app.eu.membercheck.com	10.4.2
Oman (Regional Service)	https://app.z.membercheck.com	10.4.2

Supported Browsers

MemberCheck is best viewed using the latest versions of major browsers such as

- Mozilla Firefox
- Google Chrome
- Microsoft Edge and
- Apple Safari.

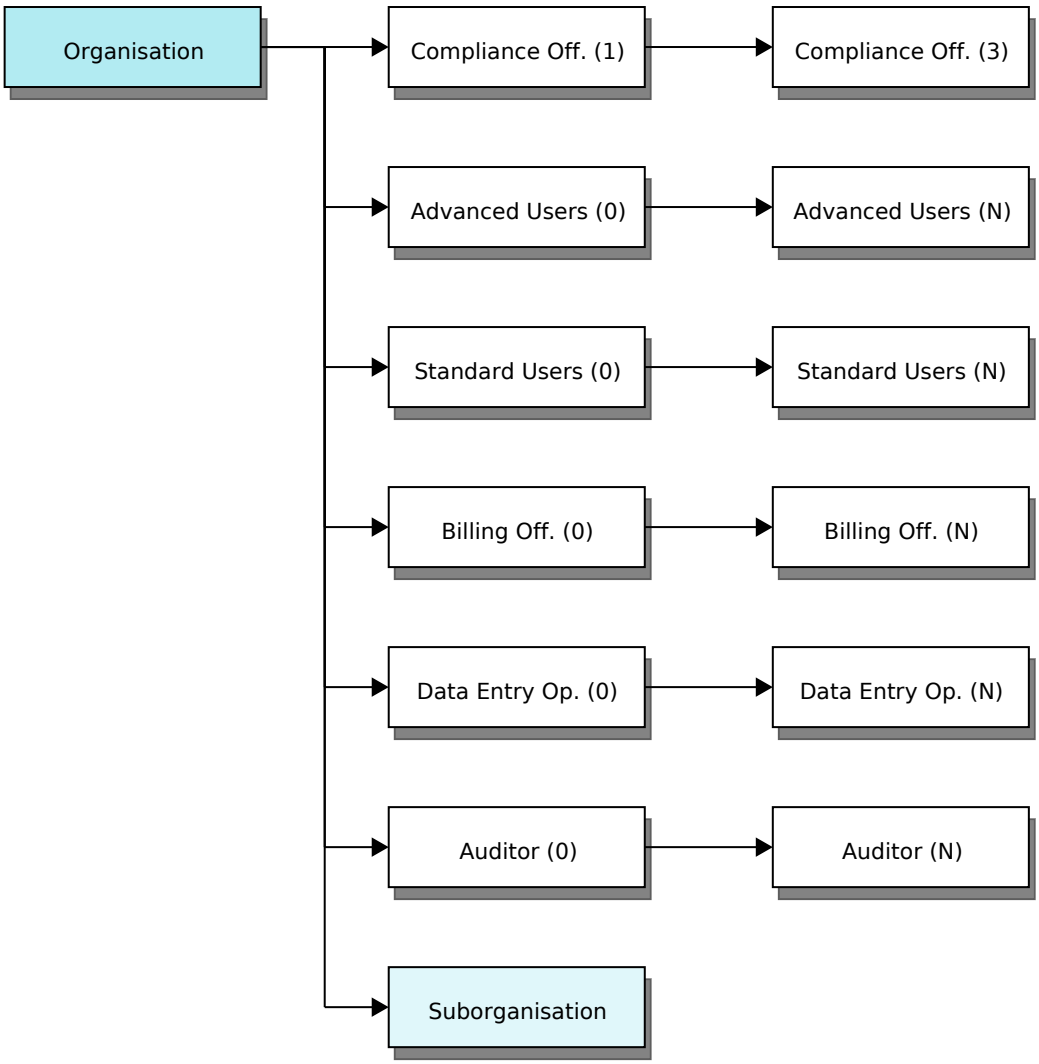
User Roles and Permissions

User Roles

Access to the system is regulated by assigning users to one of the role-based user types. Users may be assigned to multiple suborganisations, however, they will retain the same user role type across these suborganisations.

Each organisation or suborganisation can have up to **3 Compliance Officers** assigned and unlimited number of users for the other roles.

Role	Number of users (per organisation or suborganisation)
Compliance Officer	Up to 3
Advanced User	Unlimited
Standard User	Unlimited
Billing Officer	Unlimited
Data Entry Operator	Unlimited
Auditor	Unlimited



The roles are summarised as follows from the highest level of access to lowest.

Role	Overview

Compliance Officer

Up to three per organisation or suborganisation

- Set up and manage organisations and organisation hierarchies.
- Set up and manage MemberCheck users.
- Scan member against the watchlists, in single scans or in batch file scans.
- Scan corporate entities against the watchlists, in single scans or in batch file scans.
- Review results of ALL scans conducted by any user, for all organisations for which he/she is the Compliance Officer.
- Implement due diligence decisions on scan matches and allocate assessed risk to true matches.
- Generate activity reports, which summarise the organisation's scanning activity.
- Generate due diligence reports, which show scan match results, due diligence decisions and assessed risk allocated.
- View and edit own and all user details, for all organisations he/she is assigned.
- Receives email notification of the results of each scan performed for any of the organisations in the hierarchy for which he/she is the Compliance Officer, unless an alternative Organisation email have been set up for the organisation to receive scan notifications.

Advanced User

Multiple per organisation or suborganisation

- Scan members against the watchlists, in single scans or in batch file scans.
- Scan corporate entities against the watchlists, in single scans or in batch file scans.
- Review results of ALL scans conducted by any user, for all organisations to which he/she is assigned.
- Implement due diligence decisions on scan matches and allocate assessed risk to true matches.
- Generate activity reports, which summarise the organisation's scanning activity.
- Generate due diligence reports, which show scan match results, due diligence decisions and assessed risk allocated.
- View and edit own user details.

Standard User

Multiple per organisation or suborganisation

- Scan members against the watchlists, in single scans or in batch file scans.
- Scan corporate entities against the watchlists, in single scans or in batch file scans.
- Review results of scans conducted by self, for all organisations to which he/she is assigned.
- Implement due diligence decisions on scan matches and allocate assessed risk to true matches.
- Generate activity reports, which summarise the organisation's scanning activity.
- Generate due diligence reports, which show scan match results, due diligence decisions and assessed risk allocated.
- View and edit own user details.

Billing Officer

Multiple per organisation or suborganisation

- Review results of scans conducted, for all organisations to which he/she is assigned.
- Generate activity reports, which summarise the organisation's scanning activity.
- Generate due diligence reports, which show scan match results and due diligence decisions.
- View and edit own user details.

Data Entry Operator

Multiple per organisation or suborganisation

- Scan members against the watchlists, in single scans or in batch file scans.
- Scan corporate entities against the watchlists, in single scans or in batch file scans.
- View and edit own user details.

Auditor

Multiple per organisation or suborganisation

- Read-only access to all features available to the Compliance Officer

Feature Permission Matrix

The table below provides an overview of access by user role:

Feature	Compliance Officer	Advanced User	Standard User	Billing Officer	Data Entry Operator	Auditor
Run single scans for individuals	✓	✓	✓	✗	✓	✗
Run batch scans for individuals	✓	✓	✓	✗	✓	✗
Run corporate single scans	✓	✓	✓	✗	✓	✗
Run corporate batch scans	✓	✓	✓	✗	✓	✗
View own scan results	✓	✓	✓	✗	✗	✗

View scan results run by others	✓	✓	✗	✓	✗	✓
Perform due diligence	✓	✓	✓ Own scans	✗	✗	✗
View due diligence decisions	✓	✓	✓ Own scans	✗	✗	✓
View supporting documents	✓	✓	✓	✓	✗	✓
Add supporting documents	✓	✓	✓	✗	✓	✗
Manage supporting documents	✓	✓	✓	✗	✗	✗
Delete supporting documents	✓	✓	✓	✗	✗	✗
View reports	✓	✓	✓	✓	✗	✓
View Dashboard	✓	✓	✓	✓	✗	✓
View Users in organisation	✓	✗	✗	✗	✗	✓
Manage Users (add, edit, deactivate)	✓	✗	✗	✗	✗	✗
View Organisation settings	✓	✓	✗	✗	✗	✓

Manage Organisation (add, edit, deactivate)	✓	✗	✗	✗	✗	✗
Manage Data (delete scans history)	✓	✗	✗	✗	✗	✗

User Permissions

Permissions for an individual user can be further refined and restricted by **Access Rights**.

Access Rights	Description
Single Scan	Permission to perform single scans for individuals.
Scan Results	Permission to view scan results.
Batch Scan	Permission to perform batch scans for individuals.
Batch Scan Results	Permission to view batch scan results
Corporates	Access to Corporate scan functionality. This is used in addition to the above permissions to enable the user to run corporate scans, view corporate scan results, run corporate batch scans and view corporate batch scan results.
Due Diligence Decisions	Permission to perform due diligence decisions. The user may be able to view the final match decision but is not able to view history of due diligence decisions and comments.
Due Diligence Report	Permission to view the Due Diligence Reports for individuals and corporates.
Activity Report	Permission to view the Activity Reports for individuals and corporates.
View Supporting Document	Permission to view Source of Funds and Source of Wealth documentation for individuals and corporates.
Add Supporting Document	Permission to add Source of Funds and Source of Wealth documentation for individuals and corporates.

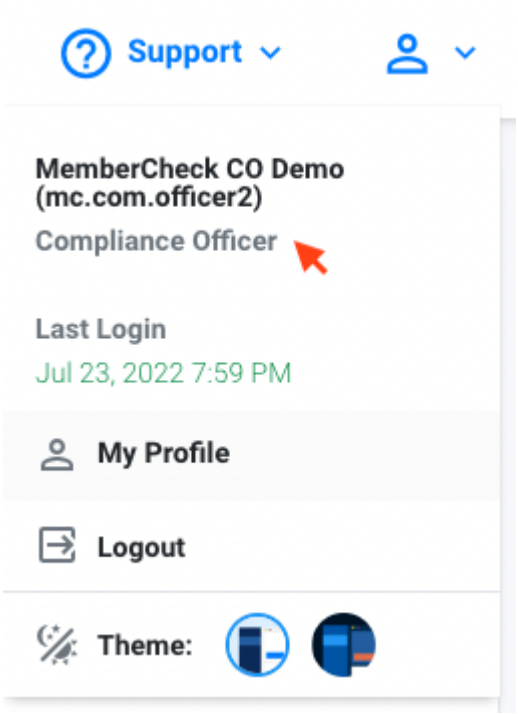
Manage Supporting Document	Permission to download Source of Funds and Source of Wealth documentation for individuals and corporates.
Delete Supporting Document	Permission to delete Source of Funds and Source of Wealth documentation for individuals and corporates.
Organisation Management	Permission to manage organisation settings. This applies to Compliance Officers of a suborganisation.
Data Management	Permission to remove scan data. This applies to Compliance Officers of a suborganisation.
Monitoring	Permission to access the ongoing monitoring features including adding scans to the monitoring list.
Dashboard	Permission to view the organisation dashboard.
ID Verification Service	Permission to screen for Identity Verification (IDV) in Individual Single Scan. This does not restrict the ability to view IDV results if `Scan Results` permission is enabled. This is visible if the organisation has been activated for the IDV service and the user role permits screening.
Know Your Business Service	Permission to screen for Know Your Business (KYB) in Corporate Single Scan. This does not restrict the ability to view KYB results if `Scan Results` permission is enabled. This is visible if the organisation has been activated for the KYB service and the user role permits screening.

Example of user roles and the relevant access rights available for each role.

Your browser does not support the video tag.

Which user role are you assigned to?

If you are unsure which user role you have been assigned to, you can check this through the profile drop down menu in the top right corner, or in **My Profile**.



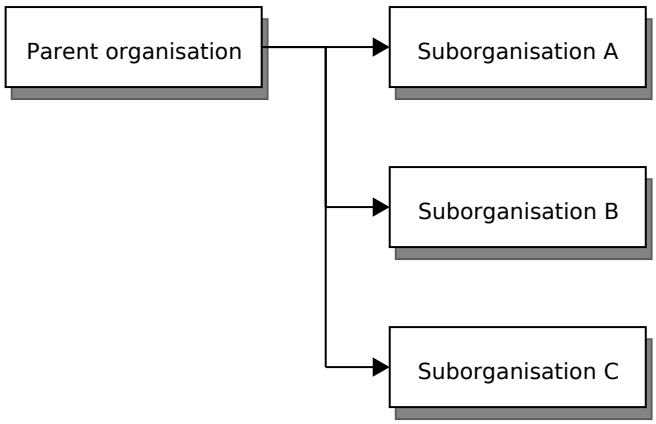
Set Up Suborganisations

Permissions

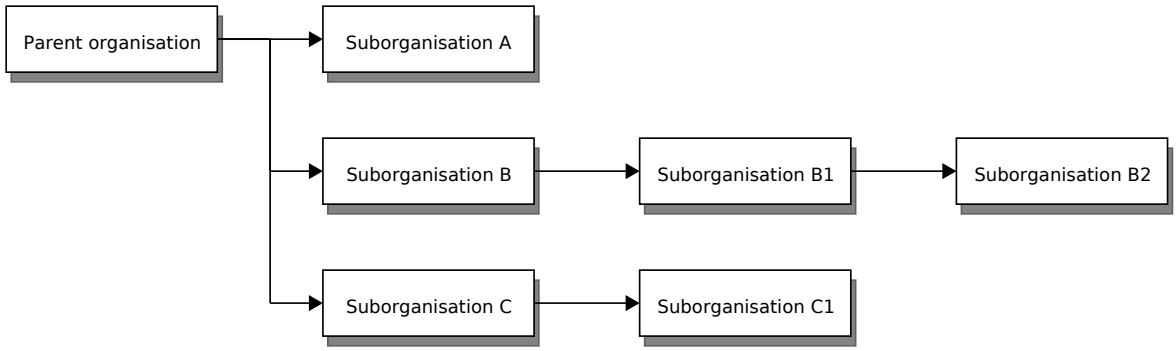
Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	✗	✗	✗	✗	✗

The **Compliance Officer** of the parent organisation can set up multiple suborganisations for different departments or for specific scan criteria and sanction lists based on your organisation's anti-money laundering and risk compliance obligations. The suborganisation structure can be flat and wide, or deep and nested, depending on your preference.

Example of an organisation hierarchy within the system with a flat suborganisation setup:



Example of an organisation hierarchy with nested suborganisation setup:



Each suborganisation can have its own **Compliance Officer** (CO) responsible for managing the suborganisation's profile, scan settings, and associated users. These Compliance Officers have access to and can manage the details of any suborganisation within their purview. The table below illustrates an example of access to suborganisations should different Compliance Officers be designated for the organisation hierarchy mentioned above.

Compliance Officer	Access to organisation
CO of **Parent Org**	All (**Parent Org**, **A**, **B**, **C**, **B1**, **C1**, **B2**)
CO of **Suborganisation A**	**Suborganisation A**
CO of **Suborganisation B**	**Suborganisation B** and all its suborganisations (**B1**, **B2**)
CO of **Suborganisation C**	**Suborganisation C** and its suborganisation (**C1**)
CO of **Suborganisation B1**	**Suborganisation B1**
CO of **Suborganisation C1**	**Suborganisation C1**
CO of **Suborganisation B2**	**Suborganisation B2**

To create a suborganisation and associate a user to the new suborganisation, you must **first** create the suborganisation. Once created, you can create the user account, or select an existing user, and assign the user to the new suborganisation.

Important Information:

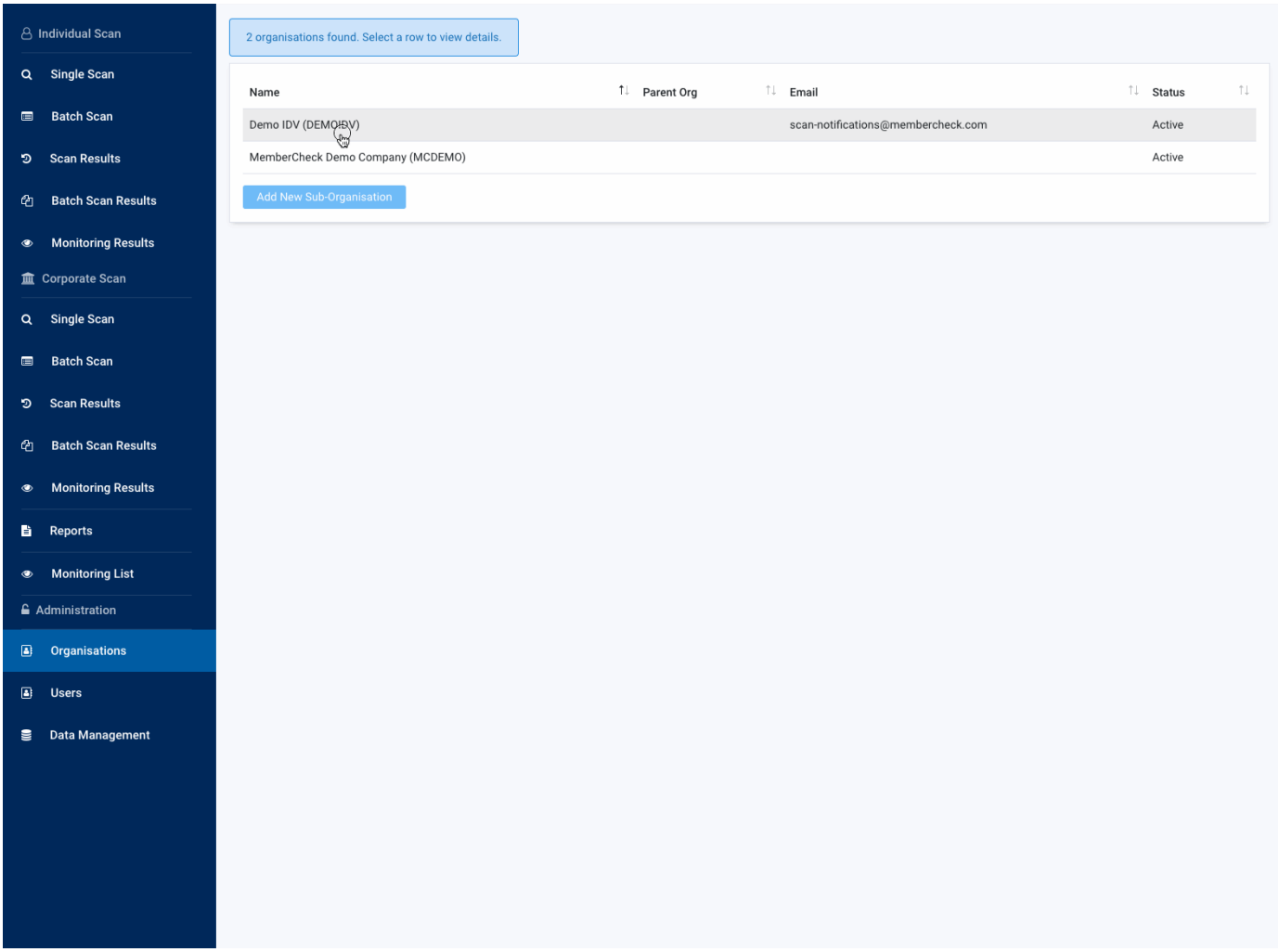
- Each organisation or suborganisation can only be allocated up to **3 Compliance Officers**.
- You can assign different **Compliance Officers** to different suborganisations.
- **Compliance Officers** can view and manage details of any suborganisation within their purview.
- A suborganisation cannot be transferred or moved once created.
- A suborganisation can be deleted, but only if there are no scan history or user accounts associated with the suborganisation.
- A user account must be assigned to an existing organisation.

You can manage organisation and users within the **Administration** section of the site.

Create a Suborganisation

Within **Administration > Organisations**, select the parent organisation from the list to create the new suborganisation. This can be the root parent organisation or another suborganisation to create a nested suborganisation structure.

In the example, we create a new suborganisation, assign existing users, and adjust the scope of the watchlists.



To create a ***new user account*** to assign to the suborganisation, refer out **Getting Started > Set Up Users**.

Set Up Users

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
	✕	✕	✕	✕	✕

Each organisation and suborganisation can have unlimited number of users for all roles (except Compliance Officers), and up to **3 Compliance Officers**.

Role	Maximum number of users (per organisation or suborganisation)
Compliance Officer	3
Advanced User	Unlimited
Standard User	Unlimited
Billing Officer	Unlimited
Data Entry Operator	Unlimited
Auditor	Unlimited

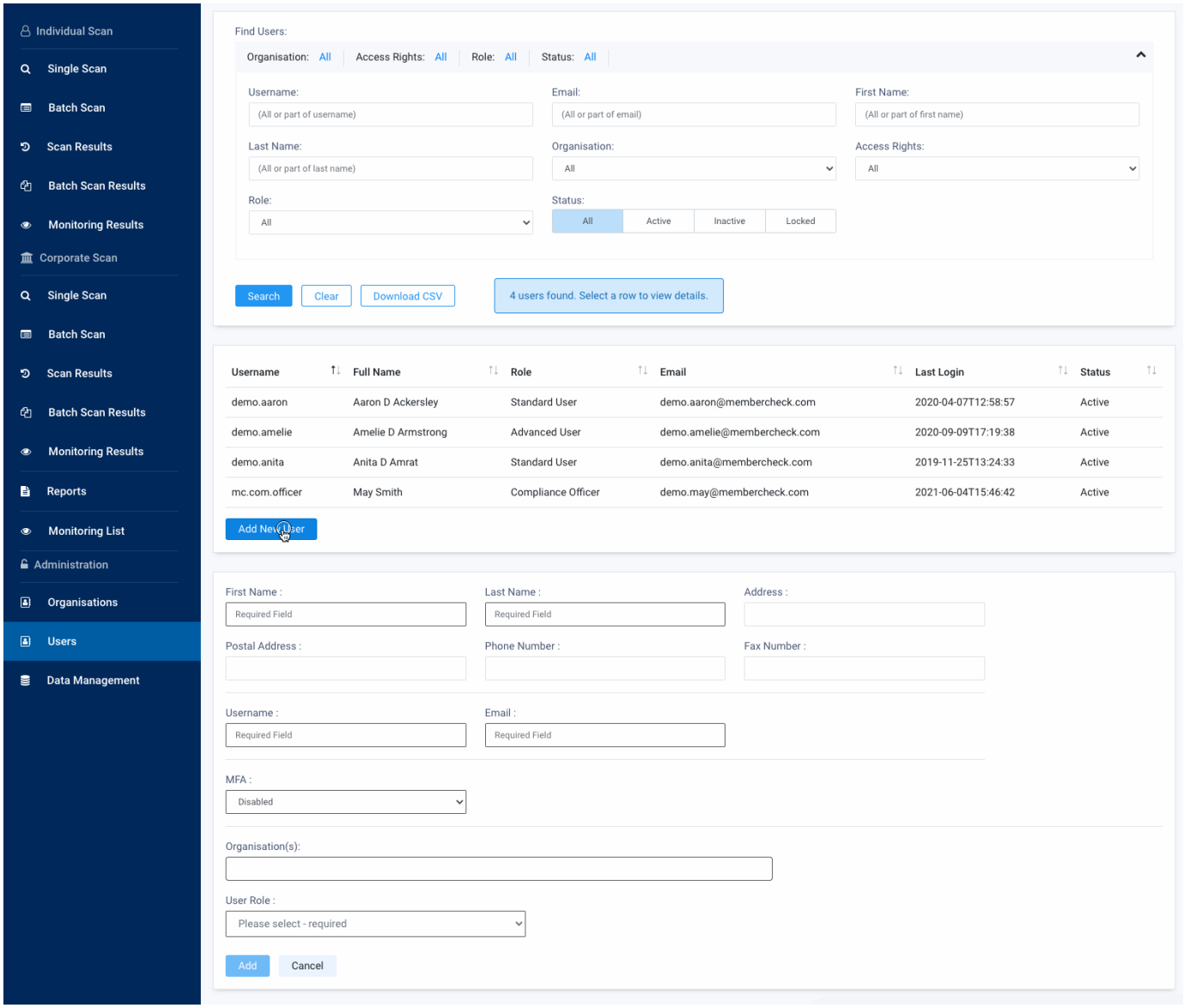
The user roles and their access permissions are described in **Overview > User Roles**.

Create New User and assign to Suborganisation

Each user account is associated with a single user role and requires a unique username and unique email address. If a user requires access as multiple roles in the system, separate user accounts must be created with different usernames and email addresses.

If a new user account is required, create the suborganisation first before creating the new user account.

In the example, we create the new user account and then assign the user to the relevant organisation or suborganisation.



You can select multiple organisations or suborganisations to assign to the user as appropriate.

Setup and Customise Scan Settings

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

Settings and Policies

A number of settings and policies can be applied to streamline and standardise the scanning and matching process, in accordance with the appropriate AML/CTF or AML/CFT legislation. They can be applied at organisation level to have preset settings, or set as `User Defined` to provide flexibility for the authorised user to adjust prior to scanning.

Customisation of the scan settings and policies may significantly reduce the number of false positive matches, enabling a more targetted and refined screening process.

The following scan settings and policies listed below affect matching and is recommended to be reviewed.

- **Watchlist** category selection to define scope of screening
- **Name Match type** for exact or close matches on names
- **Close name match rate** threshold for relevant of results
- **Whitelist policy** to take into consideration due diligence decisions
- **Country of residence policy** to match using location information available in the watchlist profiles
- **Default country of residence** to nominate a default country where the screened individual's country of residence in the address cannot be identified
- **Politically Exposed Person (PEP) jurisdiction policy** to enable exclusion of PEPs and RCAs (Relatives and Close Associates) within specific countries e.g. domestic PEPs.
- **Ignore Date of Birth Policy** to enforce matching of Date of Birth or Year of Birth

For details of the settings and policies, please refer to **Scan Settings in Guides > Administration > Manage Organisation**.

Procedure for Ongoing Monitoring

MemberCheck offers continuous screening and automated alerts for any changes in your customers' risk profiles, providing enhanced protection against financial crimes and reputational risk exposure.

An overview of the ongoing monitoring process from registration, usage, monitoring and renewal.

Sign Up

Register for a 12-month subscription to access the MemberCheck monitoring services

Upon signing up for the service, you will gain access to a pre-defined number of scans which you can use to screen names against our AML watchlists.

Use of Scans

Utilise your allocated scans to screen individuals and entities.

Add names to your monitoring lists, during screening or post-screening, which will be monitored on a daily basis to ensure compliance with AML regulations

Pre-Renewal Notification

Be aware of upcoming subscription renewal.

You will receive notifications alerting you that your subscription renewal is approaching, usually 3 months and another at 1 month before the renewal date.

Review Monitoring List

Check your current monitoring list for accuracy.

Prior to renewal, review the monitoring list to ensure there are no duplicates and that it only includes active customers. Remove any individuals or entities that are no longer relevant to your operations.

Renewal and Rescreening

Automated renewal and rescreening of names on monitoring list.

On the renewal date, all names that are active on the monitoring list will be automatically rescreened. This scan counts towards your scan usage for the new subscription term.

Continuous Monitoring

Continue the monitoring process.

The monitoring and rescreening process will repeat each subscription term, ensuring ongoing compliance and vigilance.

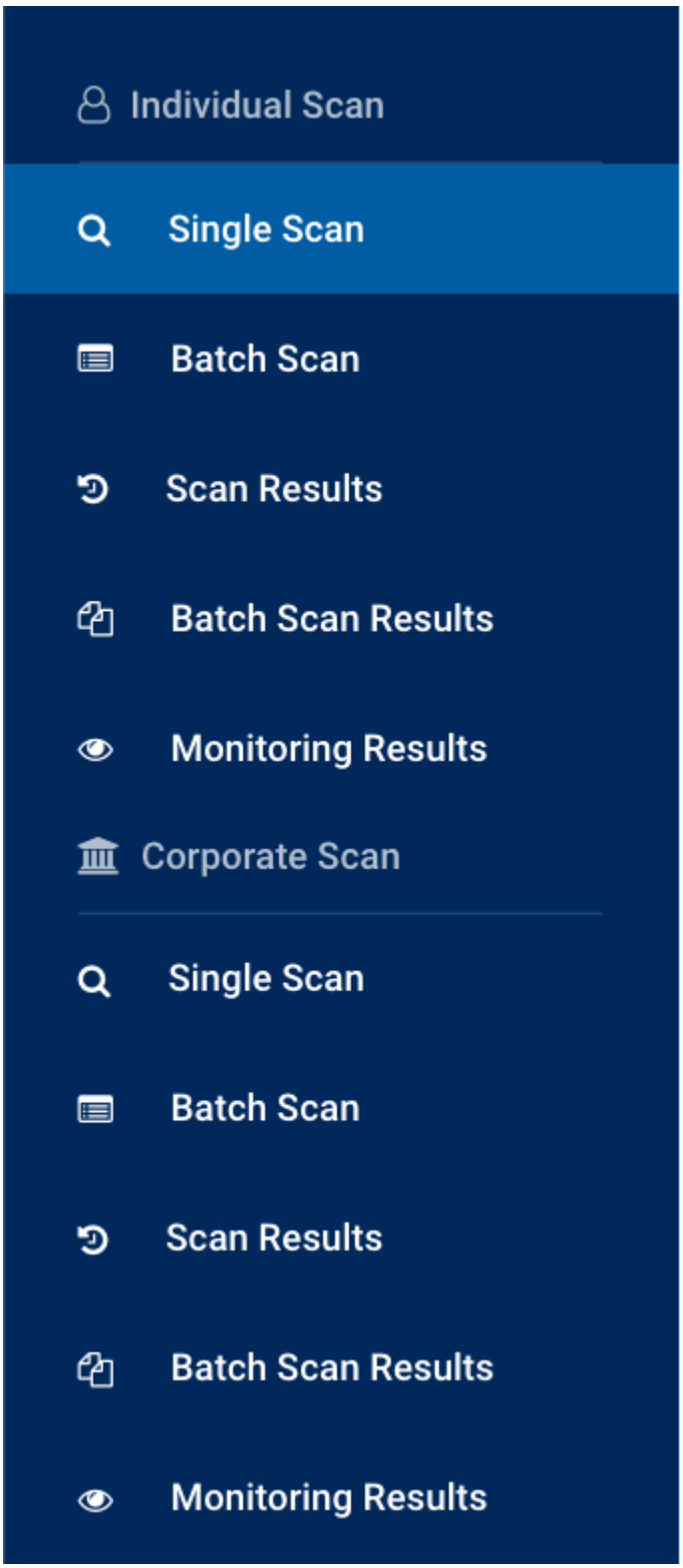
> **Important Notes**
>
> **Subscription Flexibility**:
>
> The number of scans and the frequency of monitoring can be adjusted based on your needs and regulatory requirements. Please contact your account manager for more information.
>
> **Support**:
>
> MemberCheck support is available to assist with any questions or adjustments required during your subscription period.

Single Scans of Individuals

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

You can screen for PEP & Sanction, Law Enforcement, Regulatory Enforcement and Adverse Media checks for an individual person as well as ID Verification screening via **Individual Scan > Single Scan**.



Before Running a Scan

To perform a scan of a person, you will need to check or select the following before entering details:

1. Organisation

2. Scan service type
3. Scan settings

Organisation

If you are part of a multi-level organisation structure, select the organisation which you would like to run the check for from the drop-down list for **Organisation**.

If you are part of a single level organisation, you do not need to do anything for this step.

Scan Service Type

If your organisation and user account has been enabled with additional scan services, you have the option to select these services such as ID Verification.

By default, `PEP and Sanctions` is selected.

Scan Settings

There are multiple settings provided to manage the scope and coverage of PEP, sanction and adverse media screening as per your organisation's risk level compliance requirements.

Compliance Officers can predetermine and preset these settings or set them to be user defined to enable the settings to be changed during scanning. These settings are defined in the **Organisation Settings**.

Scan Setting Details and Description

Option	Description

Name Match Type

Used to determine how closely a watchlist profile must match a person's name before being consider

The options are `Exact`, `Exact (Including Middle Name)` or `Close`.

Exact

Scan results show matches where the First and Last Name match exactly (spaces and hyphens are ig are also taken into account but Middle Name matching does not eliminate watchlist entities with no r results include matches, where:

- The First and Middle and Last Name match exactly.
- The First and Last Name match exactly and the watchlist record Middle Name contains the Midd
- The First and Last Name match exactly and the watchlist record has no Middle Name.
- The First and Last Name match exactly and the Middle Name does not match.

Exact (Including Middle Name)

- The First and Middle and Last Name match exactly.
- The First and Last Name match exactly and the watchlist record Middle Name contains the Midd
- The First and Last Name match exactly and the watchlist record has no Middle Name.

Close

- The First Name and Last Name or Latin-based Full Name match based on phonetic matching alg sounding names) and fuzzy searches. Middle Names and Original Script Names (non-Latin based Cyrillic, Chinese, Korean etc.) are ignored.

Match Rate

If `Close` Name Match Type is selected, this can be used to control the results by setting a match rate

A higher threshold will return results with minor variations whereas a lower threshold will return large sound of the name.

Example: The name `John` at various thresholds:

- **100%**>: `John` .
- **80%**: `John` , `Johnnie` , `Johnny` .
- **50%**: `John` , `Johnnie` , `Johnny` , `Jon` , `Joan` , `Jonah` , `Jean` , `Jan` , `Joanne` , `Joanna` , `Janie` , `Gena` ,
- **1%**: `John` , `Johnnie` , `Johnny` , `Jon` , `Joan` , `Jonah` , `Jean` , `Jan` , `Joanne` , `Joanna` , `Janie` , `Gena` , `(` `Jayne` , `Juan` etc.

Example: The first name and last name `Richard JOHN` at various thresholds (asterisk indicates existe middle name or last name and may not contain `Richard` or `John`):

- **100%**: `Richard JOHN` , `Richard * JOHN` , `John RICHARD` , `John * RICHARD` , `Richard John *` .
- **80%**: `Richard JOHN` , `Richard * JOHN` , `John RICHARDS` , `John * RICHARDS` , `John RICHARDSON` , `J` `John REICHARDT` .
- **50%**: `Richard JOHN` , `Richard * JOHN` , `Richard John *` , `John Richard *` , `John * RICHARD` , `Jo` `John * RICHARDS` , `John RICHARDSON` , `John * RICHARDSON` , `John REICHARDT` , `Jon RICHARDS` , `J` `Johnny RICHARDSON` , `* John RICHARDS` , `John ROCHARD` , `Joan RICHARDS` etc.
- **1%**: `Richard JOHN` , `Richard * JOHN` , `Richard John *` , `* Richard JOHN` , `John Richard *` , `Joh` `RICHARDS` , `John * RICHARDS` , `John RICHARDSON` , `John * RICHARDSON` , `John REICHARDT` , `Jon RI` `RICHARDSON` `Johnny RICHARDS` , `Johnny RICHARDSON` , `* John RICHARDS` , `John ROCHARD` , `Joan R` `RICHARD` , `Joanne RICHARD` , `Joanne RICHARDS` , `Joanne RICHARDSON` , `Richard JANE` , `Jayne RICH` `Jean-Pierre RICHARD` , `Jean-paul RICHARD` , `June RICHARD` , `June RICHARDS` , `June RICHARDSON` `Richard GENAO` , `Richard GIANNI` . `Juan RICHARTE` etc.

Whitelist Policy	If Due Diligence has previously been carried out, profiles marked as `No Match` are whitelisted, and ca excluded from being returned and displayed. This can help eliminate match results previously determ match. This option requires a `Client ID` to be associated with the person during scanning for identification The options are: • `Apply` : Whitelisted profiles marked as `No Match` for the person being scanned are excluded and • `Ignore` : Display all results regardless of previous due diligence decisions.
(Country of) Residence Policy	Used for matching the Country in the Address of the person with the locations associated with the ma requires the Country to be specified in the Address field when scanning for the person. The options are: • `Apply to All` : Apply the matching of country to all profiles for all categories. • `Apply to PEP` : Apply the matching of country only to profiles with the category `PEP` (Politically l • `Apply to POI` : Apply the matching of country only to profiles with the category `POI` (Profile of I • `Apply to RCA` : Apply the matching of country only to profiles with the category `RCA` (Relatives c • `Apply to SIP (incl.TER)` : Apply the matching of country only to profiles with the category `SIP` Person), which includes `Terrorism` . • `Ignore` : Display all results regardless of whether the country matches with the profiles. If you want to apply the defined PEP Jurisdiction Inclusion or Exclusion list, do not check `Apply`

Default Country of Residence	Used for nominating a Country of Residence for an individual's address where a country cannot be ide which are not blank but do not contain an identifiable country, if a **Default Country of Residence** has b be automatically assigned to the individual as the Country of Residence. This setting is defined by the Compliance Officer in the **Organisation Settings**.
Apply to blank Addresses	Used in conjunction with **Residence Policy** and **Default Country of Residence**, this is used for elimina where the individual's Country of Residence is not found in any of the Locations in the matching entity This option applies the preset Default Country of Residence to blank addresses during PEP and Sanc
PEP Jurisdiction	This setting filters PEP and RCA profiles based on defined jurisdictions for inclusion or exclusion, and filtering domestic PEPs. To use this setting, ensure `Apply to PEP` in the **Residence Policy** is unchecked. The settings available are based on the organisation settings defined by the Compliance Officer and c or Include: • `Exclude` : Exclude from matching, PEPs and RCAs with locations within the defined PEP Jurisdic • `Include` : Include in matching, PEPs and RCAs with locations within the defined PEP Jurisdiction • `Ignore` : Ignore any exclusion or inclusion of PEP jurisdictions. If no jurisdictions are defined, this will behave the same way as `Ignore` .

Exclude Deceased Persons	Used for eliminating match results where the person is recorded as deceased. The options are: • `Yes` : Exclude deceased persons from matching results. • `No` : Include deceased persons in matching results.
Web Search	Perform additional search for adverse media on third party search engines e.g. Google search. This o independent search for adverse media to the existing adverse media sources within PEP and Sanctio The options are: • `Yes` : Run the scan on available search engines for adverse media. • `No` : Do not run additional independent adverse media search.
Advanced Media Search	Perform advanced media search for recent news articles. This option provides additional AML/CTF re to the existing adverse media sources within PEP and Sanctions profiles. Results may include article date of publication, author and article readership. The options are: • `Yes` : Run the scan for recent news media. • `No` : Do not run scans for recent news media.

FATF Jurisdiction Risk	Perform additional search to include technical compliance and effectiveness ratings, based on FATF countries linked to matched profiles. The options are: • `Yes` : Include FATF Jurisdiction Risk rating information. • `No` : Do not include FATF Jurisdiction Risk rating information.
Watchlists	Scope of watchlist categories applied for the new scan. The available options are based on the Orgar The **Compliance Officer** can edit the list in **Organisation Settings** as well lock the editing of the list.

Running a Single Scan

PEP, Sanction and Adverse Media screening

To start screening an individual for PEP, sanctions and adverse media, the following are necessary information:

- **First Name and Last Name** or **Full Name** or **Original Script Name**
- **Client ID** (check conditions below)
- **Date of Birth** (check conditions below)
- **Country of Residence** (recommended)

Client ID

Formerly "Member Number". A unique reference identifier for the individual is required if you want to add the person for ongoing monitoring or perform due diligence.

You may use a Customer Reference or Client Account ID or any unique identifer for the person.

In cases where individuals do not have and never will have a Client ID, such as staff for example, arbitrary Client IDs can be used and prefixed by a letter, or letters, to distinguish them from your regular client base.

In cases where individuals may be allocated a unique identifier in the future, such as new clients for example, an arbitrary number should not be allocated. The prospect or client number that will be allocated to the individual when they become a 'new client' should be used as the Client ID for scanning and monitoring purposes. In this way due diligence decisions will be allocated to the real client number and subsequently the whitelist will also be appropriately applied to that Client ID.

Date of Birth

The Date of Birth will be required during scanning if your **Compliance Officer** has enabled this feature in the **Organisation Settings > Ignore Blank DOB**.

The more information you are able to provide for the person will enable more targetted matches and improve the results returned.

Providing Scan Information

You can provide information of the individual in the following fields:

Field	Required	Field Limit	Description

First Name	Conditional	255 char	First name or Given name of the individual. This field is *Mandatory*, unless you are entering an **Original Script Name** or **Full Name**. Where only the initial of the first name is available, you can enter the letter followed by an asterisk. Example: • **K*** will return matching profiles containing first names such as `Kay`, `Karim`, `Ken`, `Kennard`, `Kennedy`, `Kenneth`, `Kevin` etc • **Ken*** will return matching profiles containing first names such as `Ken`, `Kennard`, `Kennedy`, `Kenneth` etc
Middle Name	Optional	255 char	If the individual has multiple middle names, enter all middle names separated by spaces.
Last Name	Conditional	255 char	Last Name or Surname or Family Name of the individual. This field is mandatory, unless you are entering an **Original Script Name** or **Full Name**. If the individual has a single mononymous name, enter the name in this field and enter a dash (`-`) in the First Name field.

Original Script Name/Full Name	Conditional	255 char	Non-Latin names such as Cyrillic, Hebrew, Chinese, Korean, Japanese, Arabic, Indian names etc in **original script** should be entered in this field due to different matching algorithms in the system. You can also enter Latin-based **full name** in this field if you are not able to separate the individual's name into First, Middle and Last, or if you are uncertain of the order of the First and Last Name. Unless you are entering the **First and Last Name**, this field is mandatory. This field can be hidden if the **Original Script Search/Full Name** setting is disabled by the **Compliance Officer** in the **Organisation Settings**.
Gender	Optional	-	Select from the drop-down list. Options are: • `Male (M)` • `Female (F)` • `Unspecified (X)` Matches will include entities with no gender recorded or other values such as `Unknown`, `Not specified` or `Transgender`, etc.

Date of Birth	Conditional	10 digits with "/" or 4 digits	Use the format `DD/MM/YYYY` or `YYYY`. Matching will be performed on date of birth or year of birth. If your Compliance Officer has enabled date of birth or year of birth tolerance, you will see additional options to specify the permitted year variations. This value applies to both before and after the birthdate. Enabling this tolerance disregards the specific day and month, returning matches within the specified year range. This field is mandatory if the **Compliance Officer** has enabled the feature to ignore blank DOBs in the Organisation Settings.
Client ID	Conditional	100 char	Unique identifier for the individual such as Customer Reference Number or Account ID. This unique ID is associated with due diligence decisions and ongoing monitoring updates. Retaining the same Client ID for an individual will assist with tracking changes. This field is mandatory if the **Compliance Officer** has enabled the update monitoring list feature or if you have elected to perform due diligence and monitoring. If you do not have a Client ID to uniquely identify and track the individual, you are welcome to use the auto-generate function to suggest an identifier ().
Country of Residence	Optional	-	Country of residence of the Individual. You can select up to 5 countries. Results will include profiles matching all specified locations as well as no known locations to minimise potential match exclusions.

Nationality	Conditional	-	Nationality or citizenship of the Individual. You can use this to search for dual citizenship and supports up to 5 nationalities. Results will include profiles matching any of the specified nationalities as well as no known nationality to minimise potential match exclusions. This field is mandatory if the **Compliance Officer** has enabled the setting to ignore blank nationality in the Organisation Settings. The results will only include profiles matching any of the specified nationalities and blank nationalities will be excluded.
ID Number	Optional	100 char	Use this field to refine and target your search for identification numbers like Passport Number, National ID, VAT/Tax Number, and Professional Registration Number. Watchlist profiles that match this identifier as well as profiles that do not have any identifiers will be returned as a result to minimise the risk of overlooking potential matches.
Email Address	Optional	128 char	Optionally, enter an email address for the individual to run a check for compromised information in known data breaches. This search is provided as supplementary information about the individual and is not required as part of the AML KYC regulatory compliance checks.
Update Monitoring List	Optional	-	To add the member to ongoing monitoring, select this check box to add the member to the Monitoring List. Only members with a Client ID will be able to be monitored by the system. Where the Compliance Officer has set the monitoring settings to be automatically added during scans, you will be displayed an appropriate message. Any scans with a Client ID will automatically be added for ongoing monitoring. Note: This option is only visible if your organisation and user account is enabled for monitoring.

ID Verification (IDV)

Customer identity verification consists of 2 key processes: **ID Check** (document verification) and **FaceMatch** (biometric facial matching).

- ID Check - Verification of documentation information against multiple independent data sources including official government and commercial sources. This option supports 20+ countries that provide verification against official data sources.
- FaceMatch - Customer self-verification using biometric facial matching against government-issued documentation. This option recognises documents in 240+ countries and territories.

You can verify the identity of an individual using either or both options as part of the ID Verification service. If you do not see both options, the Compliance Officer of your organisation may have enabled only one of the options.

To screen an individual for ID Verification (name, address, date of birth), you will need the following to get started:

- **First Name and Last Name** or **Original Script Name** (check conditions below)
- **Date of Birth**
- **Mobile Number** or **Email Address** for biometric facial matching

> **When is Original Script Name required**
>
> The requirement for **First Name, Middle Name and Last Name**, or **Original Script Name** depends on the Country selected for verification.
>
> All countries require First and Last Name, except China. If China is selected as the Country of verification, then the Original Script Name should be entered.

Methods for ID Verification and face matching

You can run the ID Verification on behalf of the individual or have the verification completed by the individual themselves. For biometric facial matching, this must be completed by the individual themselves.

Options:

- Run the verification yourself
- SMS the verification to the individual

- Email the verification to the individual

If you opt to run the verification yourself, you will be presented with the option to email the biometric facial matching to the individual within this process.

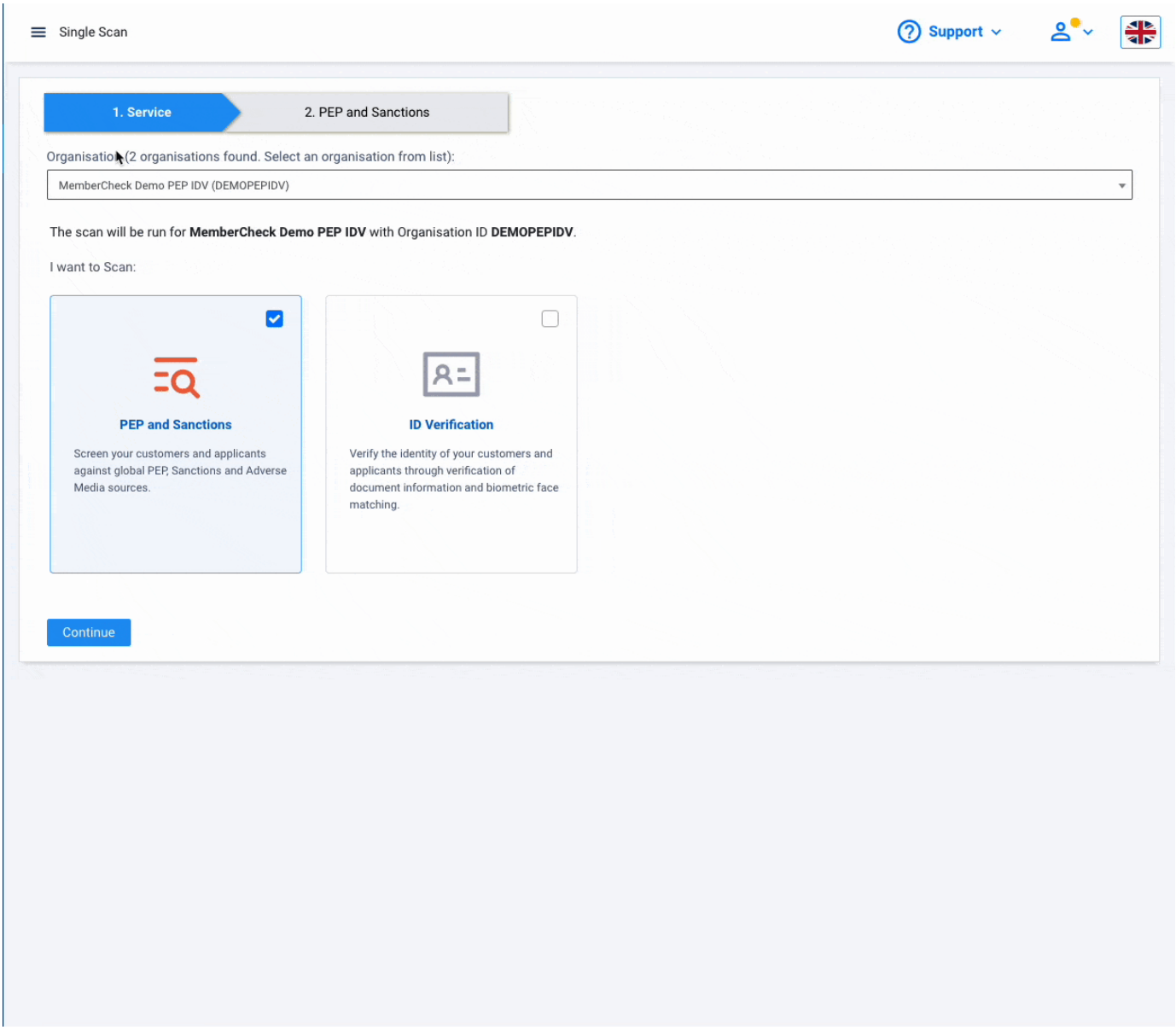
Providing Scan Information

You can fill in information of the individual in the following fields to initiate the ID Check and FaceMatch processes. Depending on the IDV option selected, you will be required to provide some information. For biometric face matching, the individual will need to complete the verification themselves on their own device or computer with a camera:

Field	Required	Field Limit	Description
Country of Verification	Required	-	Country for source of verification of the individual's details.
Mobile Number	Conditional	14 digits	If you have selected to SMS the verification, select the country prefix and enter the individual's mobile number to receive the SMS with a URL to complete the verification process.
Email Address	Conditional	128 characters	If you have selected to Email the verification, enter the individual's email address to receive the email with a URL to complete the verification process.
First Name	Required	255 char	First name or Given name of the individual. If there are multiple names for the given name, enter the first name into this field and the additional names into **Middle Name**.
Middle Name	Optional	255 char	If the individual has multiple middle names, enter all middle names separated by spaces.
Last Name	Required	255 char	Last Name or Surname or Family Name of the individual.
Original Script Name	Conditional	255 char	Script Name. This only applies to identity verifications for Chinese data sources.
Date of Birth	Optional	10	Enter the individual's date of birth in the format `DD/MM/YYYY`
Client ID	Optional	100 char	Unique identifier for the individual such as Customer Reference Number or Account ID for your own reference.

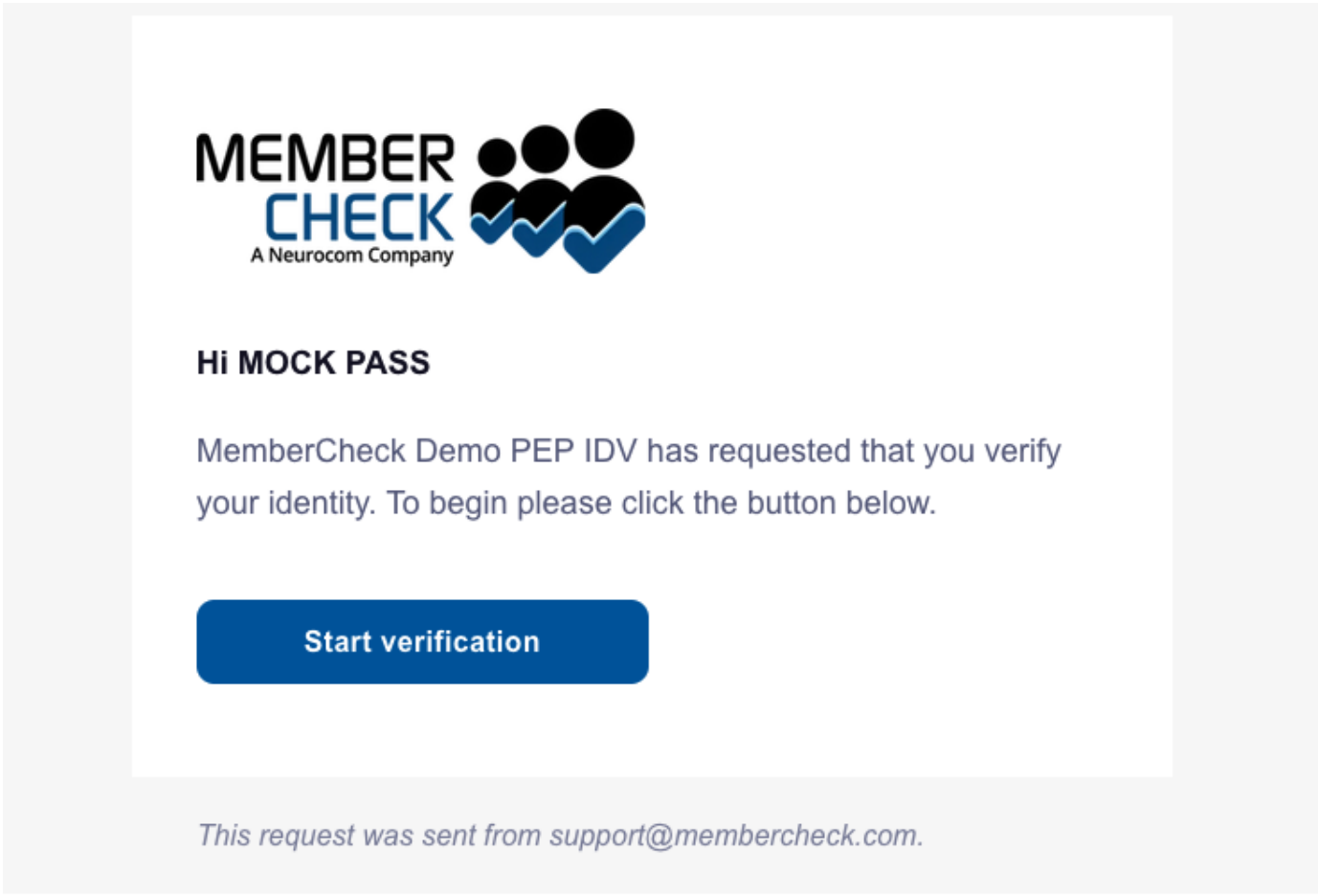
You can run PEP & Sanction or ID Verification scans separately or combine both within a single scan.

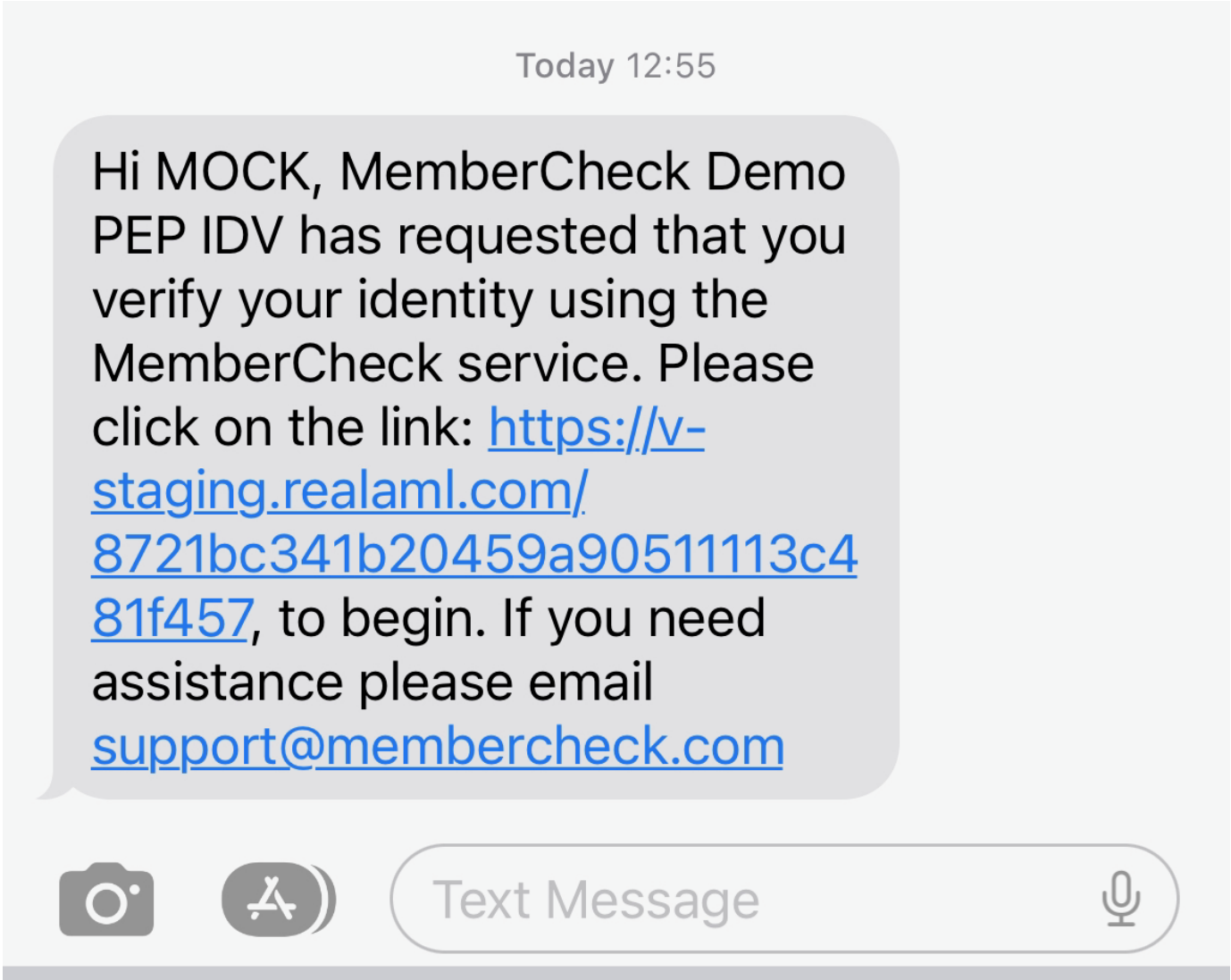
Selecting these scan options will present relevant fields and filters for screening.



If you have opted to send the verification for the individual to complete themselves, the email or SMS will contain your organisation name.

Examples of the Email and SMS received by the individual, "MOCK PASS", to perform the verification from company "MemberCheck Demo PEP IDV":





The **Verification URL** embedded in emails and SMSes is displayed on the screen, which enables you to access the link to the actual verification process. This URL is available for new or recent IDV requests as part of the MemberCheck service upgrade.

Duplicate ID Verification detection

To minimise accidental duplicate scans for ID Verification which may send multiple SMS requests to your customer or applicant to verify themselves, the system has a built-in duplicate detection mechanism. This mechanism will detect for the same name (First, Middle, Last or Full Name) being scanned within a period of 24 hours within your organisation.

You can opt to continue or cancel to stop the duplicate scan.

Getting access to a demo account

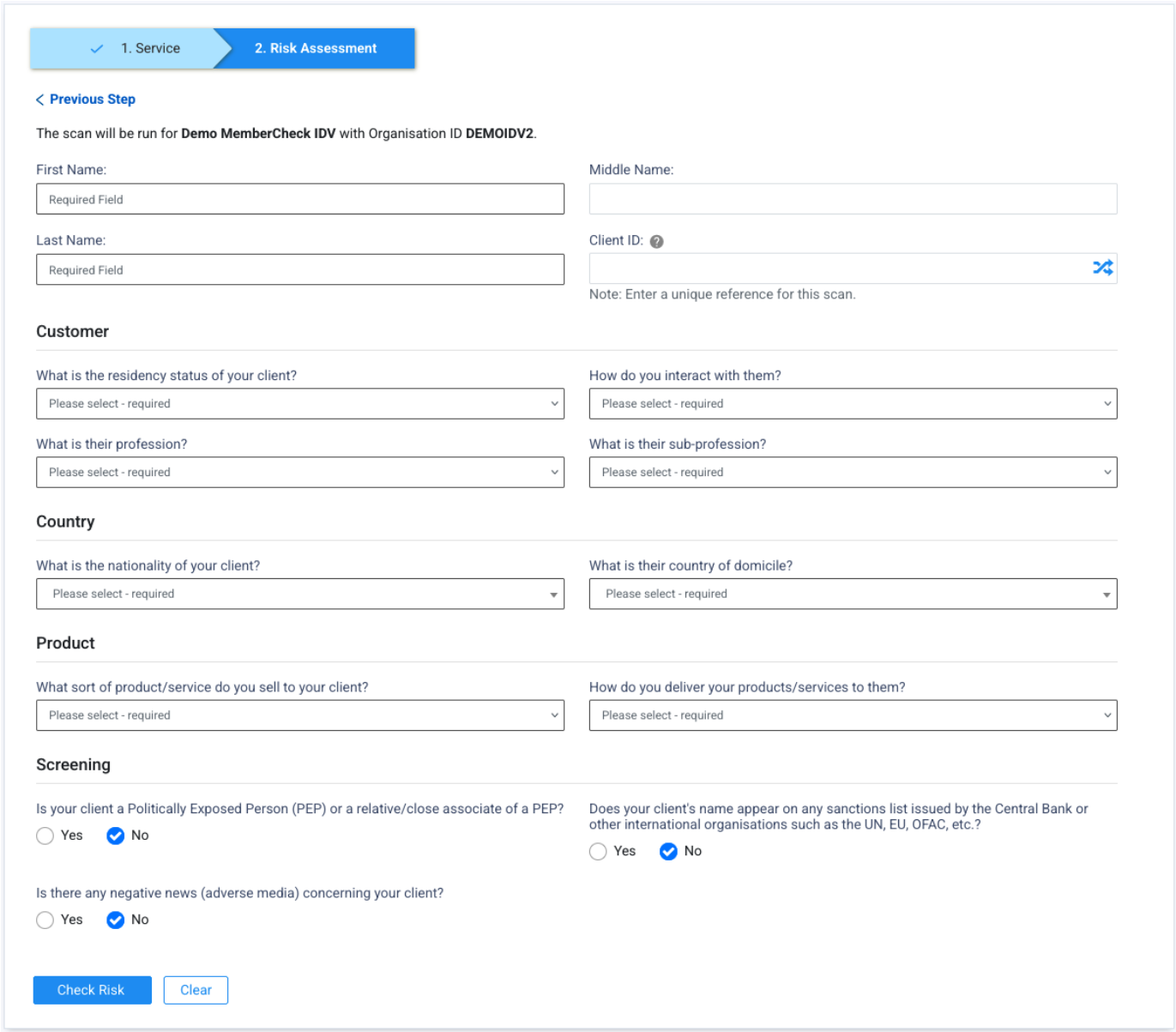
If you would like to trial the ID Verification service, please contact your MemberCheck Account Manager or support@membercheck.com

Risk Assessment

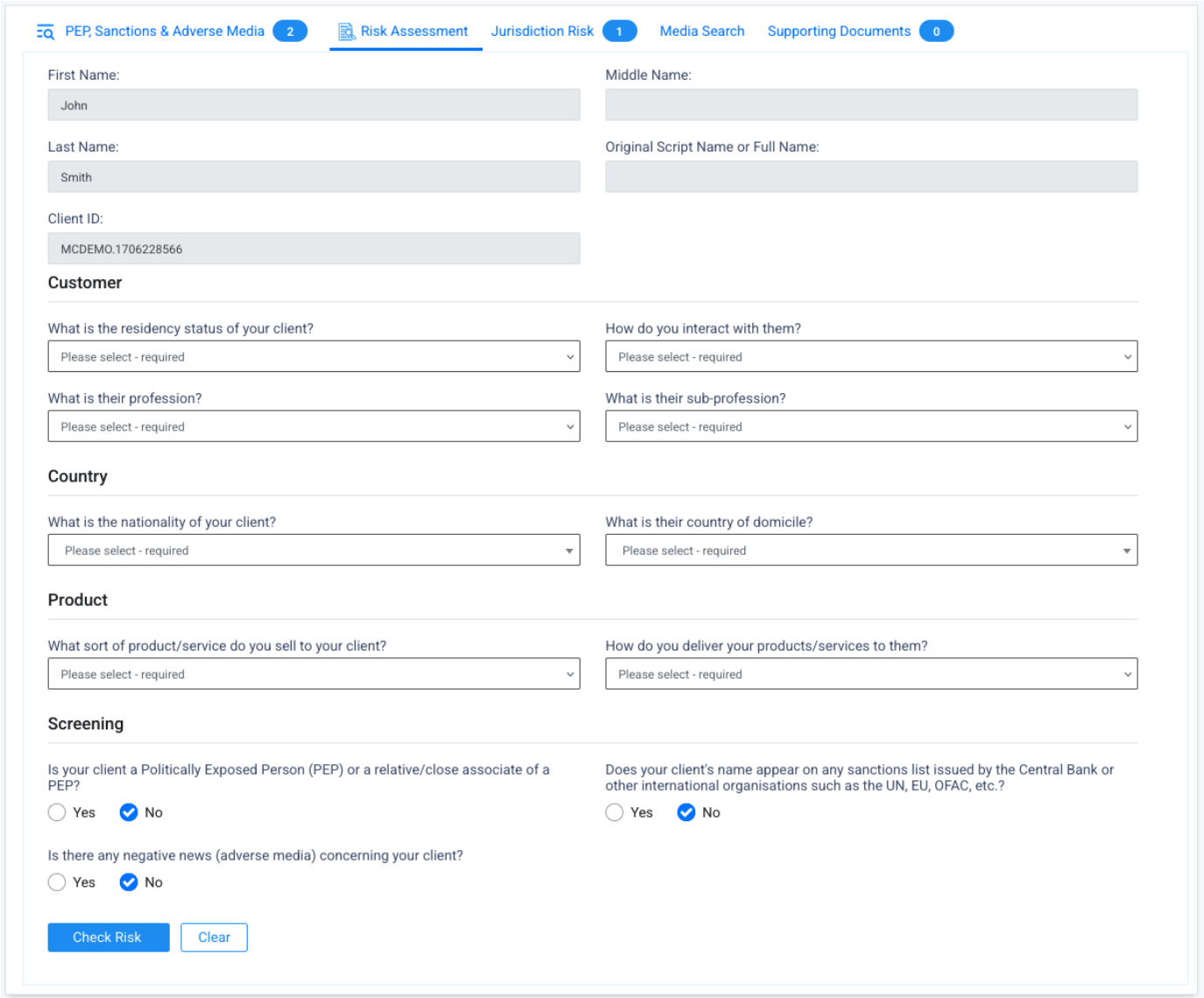
You have the option to perform additional assessment of your customer risk through a simple, structured process. When starting a new screening, you can select this service and answer key questions about your customer, their country of domicile and nationality, products and services offered, and screening outcomes. You will receive a calculated risk score, risk level, and actionable recommendation.

This option is available if your organisation has subscribed to the AML Risk assessment service. When activated, all authorised users of the service with screening permission have access to this feature.

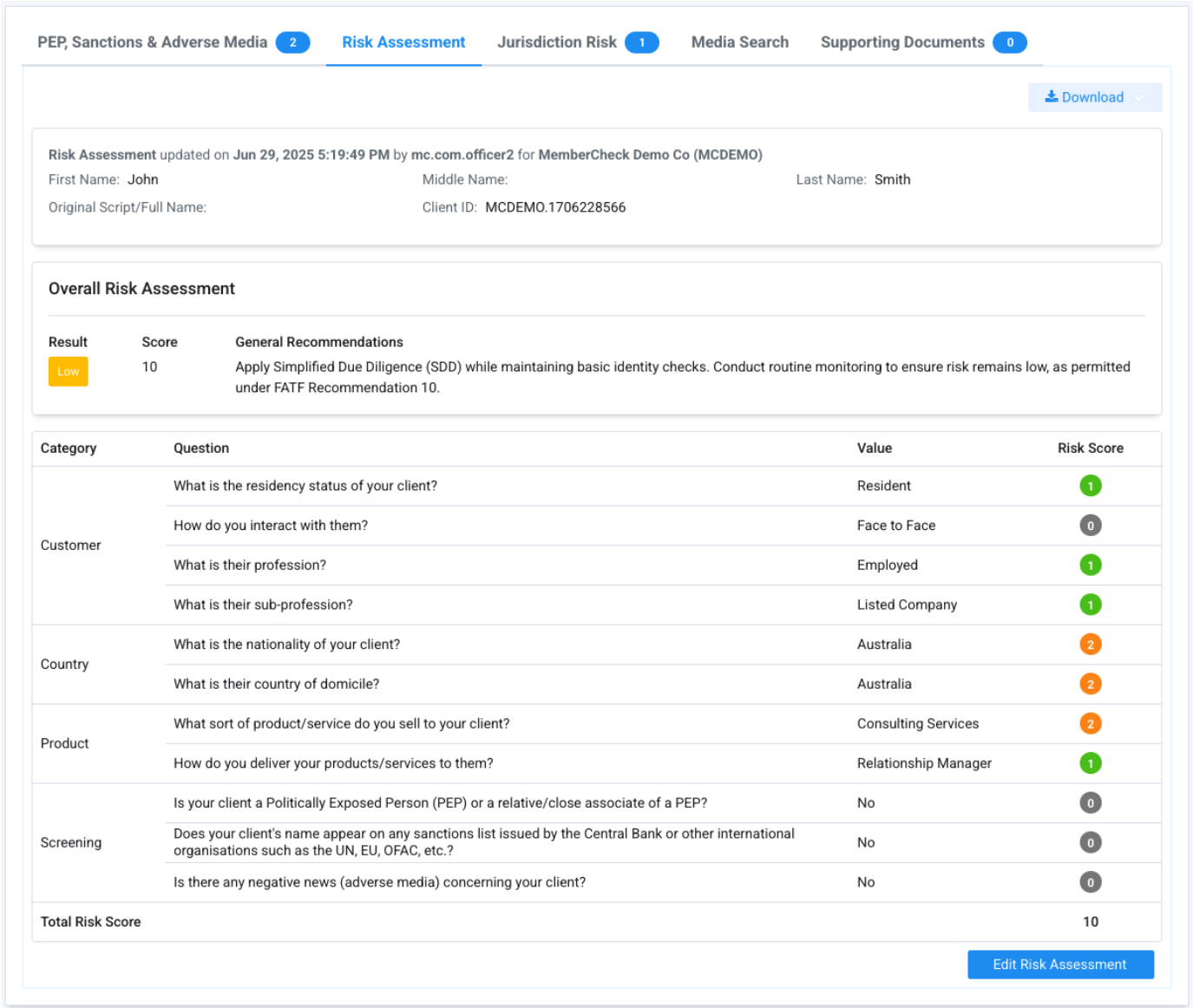
To use this service, simply select the **Risk Assessment** option when you perform a new scan. You can combine this with new PEP & Sanctions scan, ID Verification scan, or run this as a standalone check.



When you combine a Risk Assessment check with a PEP & Sanctions or IDV check, you will see the Risk Assessment tab displayed in the results section for additional information of the customer.



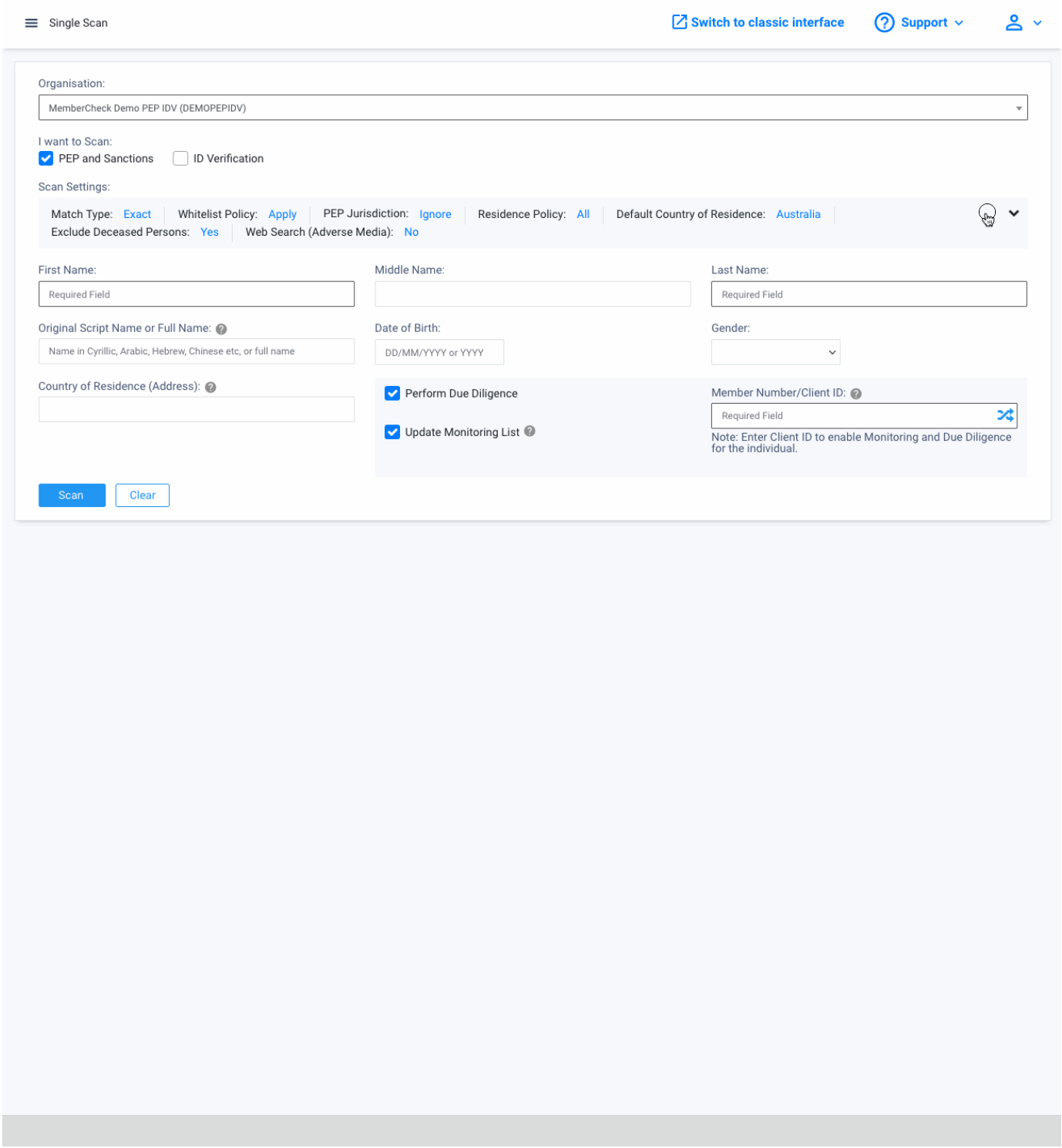
On completion of the questionnaire, you will see the individual scores for each of the questions for transparency and an overall summary of the risk-level and actionable recommendations as a guideline.



Quick How-To Guides

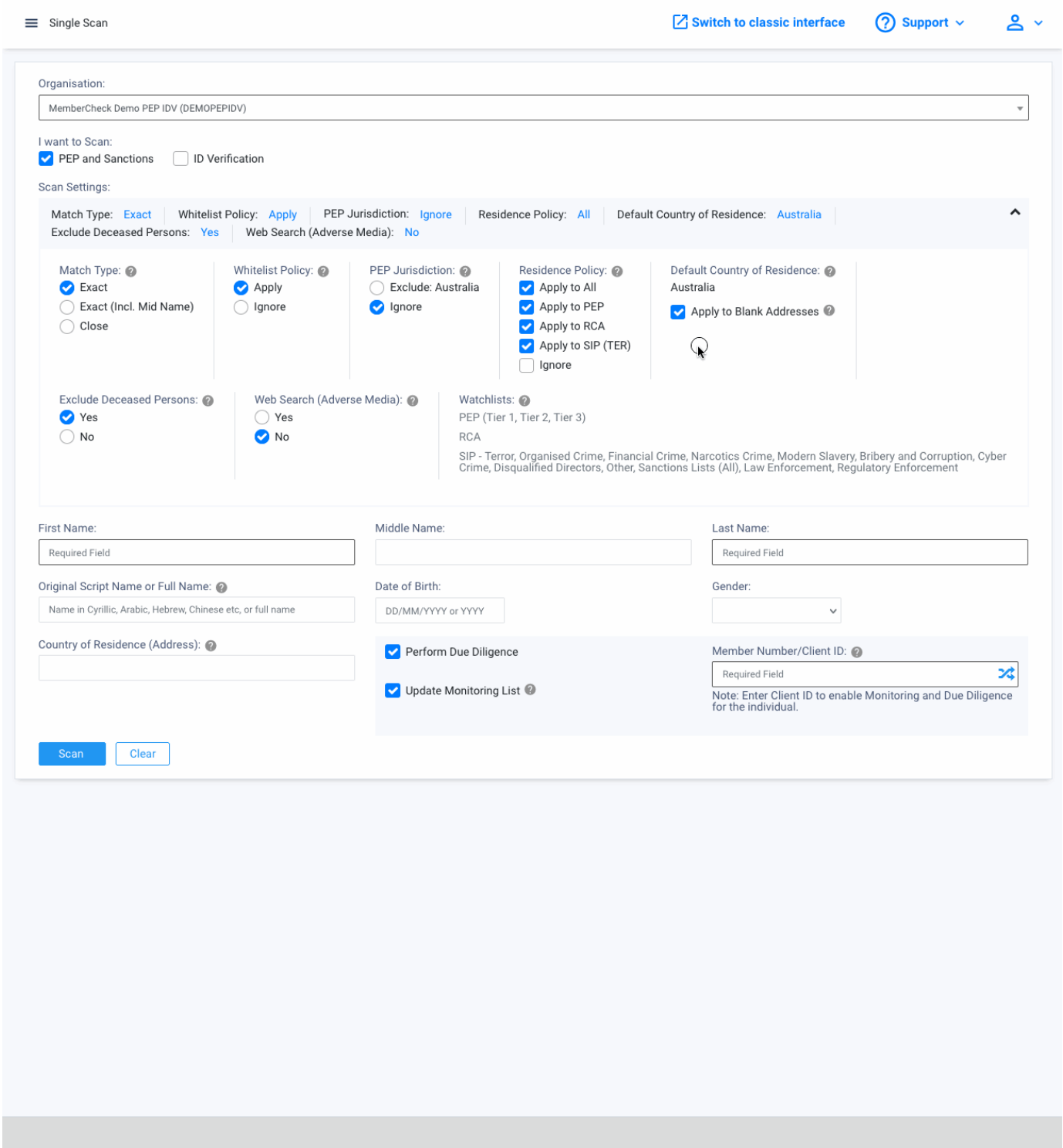
Screen by separate First, Middle and Last Name

Example of screening with **First Name**, **Middle Name**, **Last Name** and with a **Client ID** for monitoring and due diligence for recording of assessed risk.



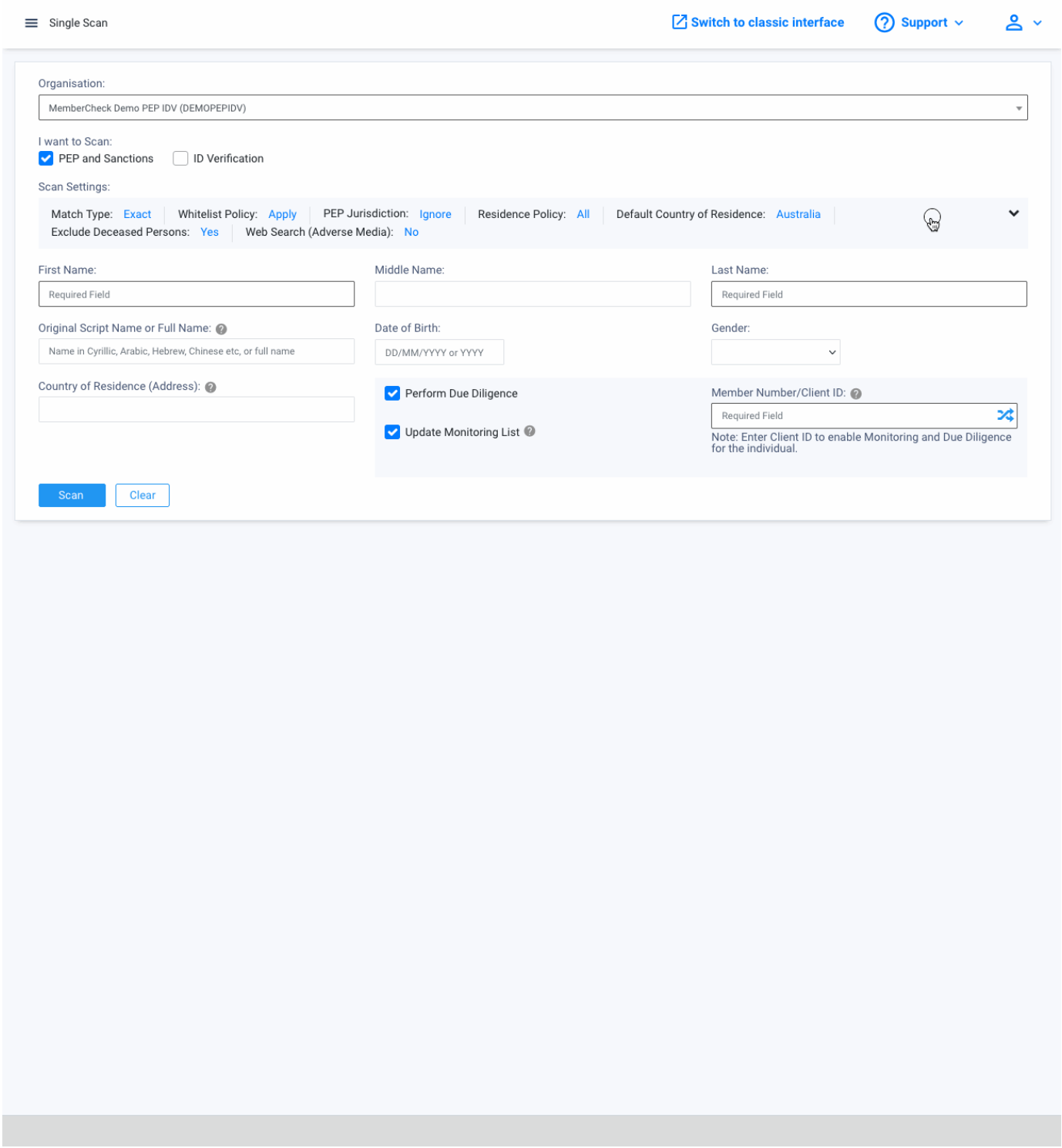
Screen by Full Name

Example of screening with **Full Name** and with a **Client ID** for monitoring and due diligence for recording of assessed risk.



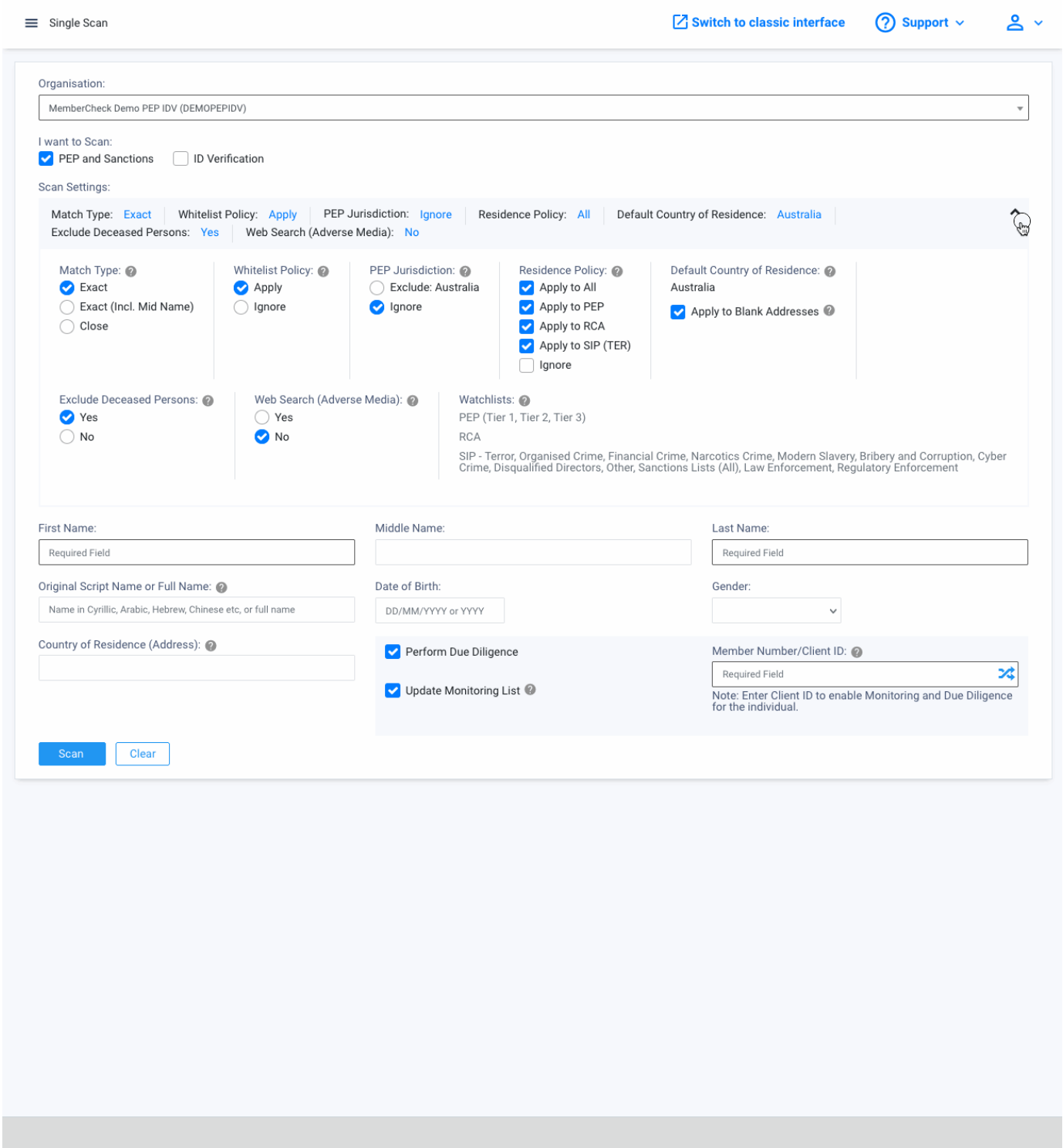
Screen by Original Script Name with additional web search

Example of screening with **Original Script Name** and with a **Client ID** for monitoring and due diligence for recording of assessed risk.



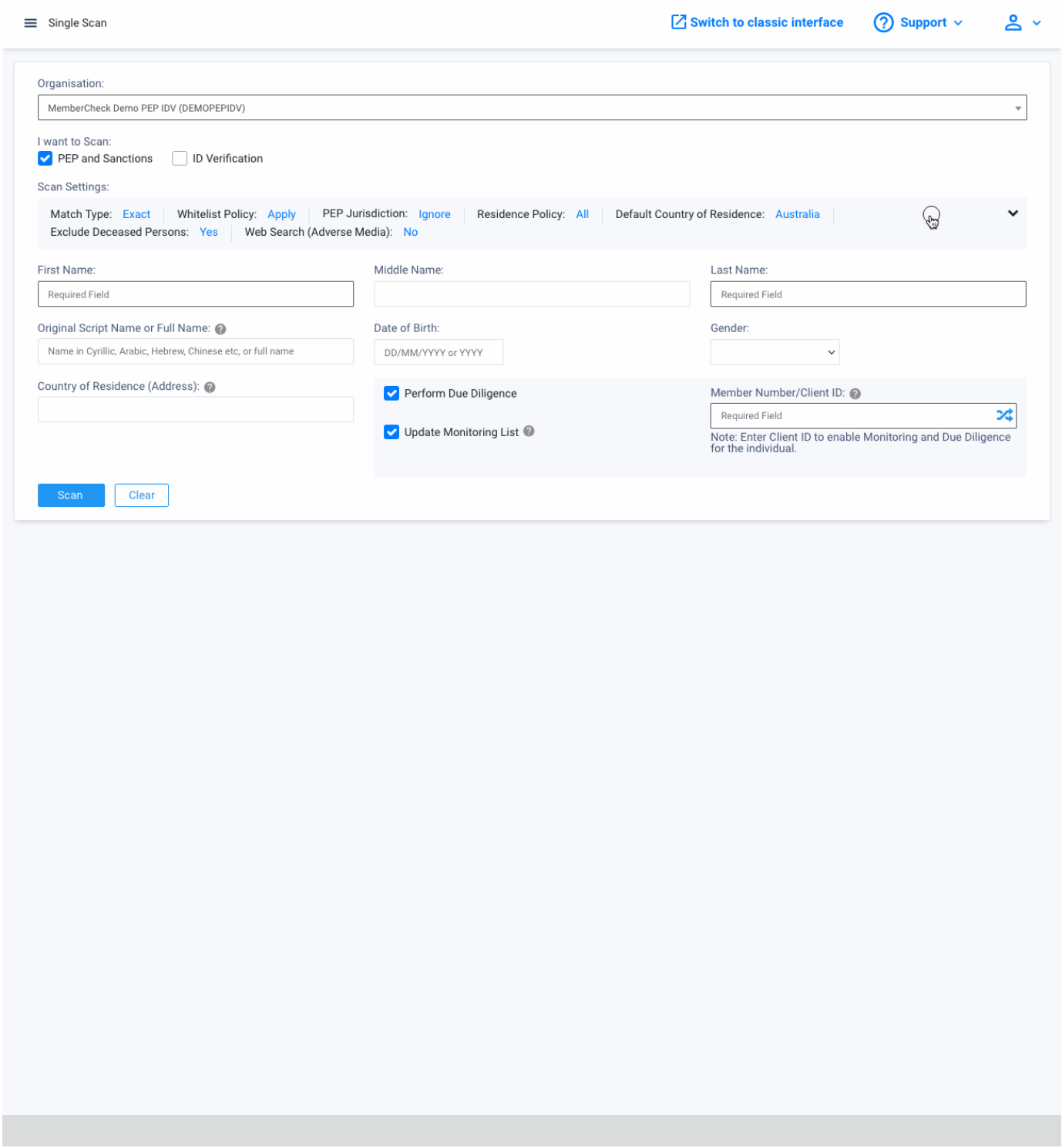
Screen with additional web search

Example of screening with **First Name**, **Last Name** with the option to include additional web search.



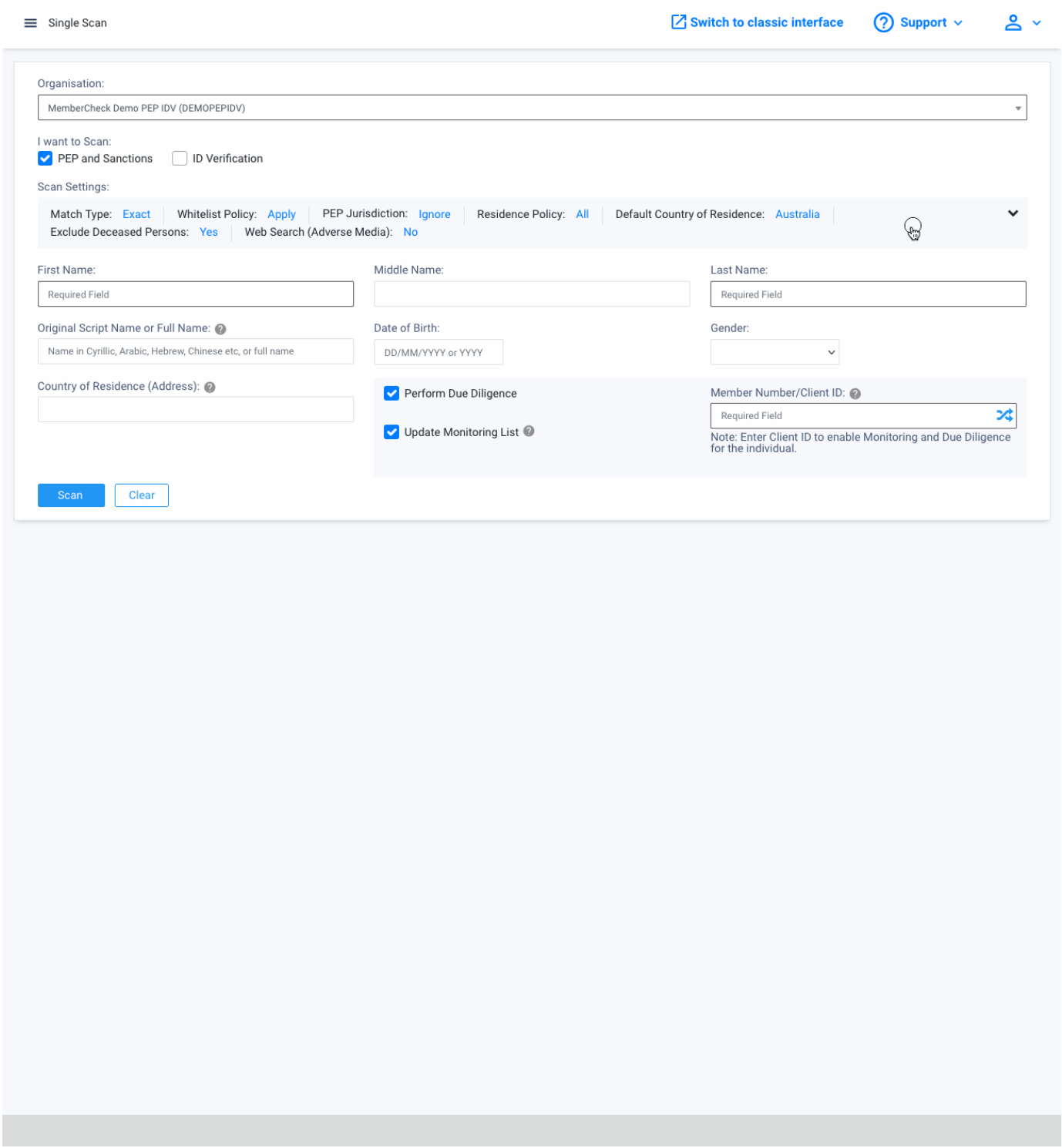
Screen without due diligence or monitoring

Example of screening with **First Name**, **Middle Name**, **Last Name** without monitoring and due diligence for the individual.



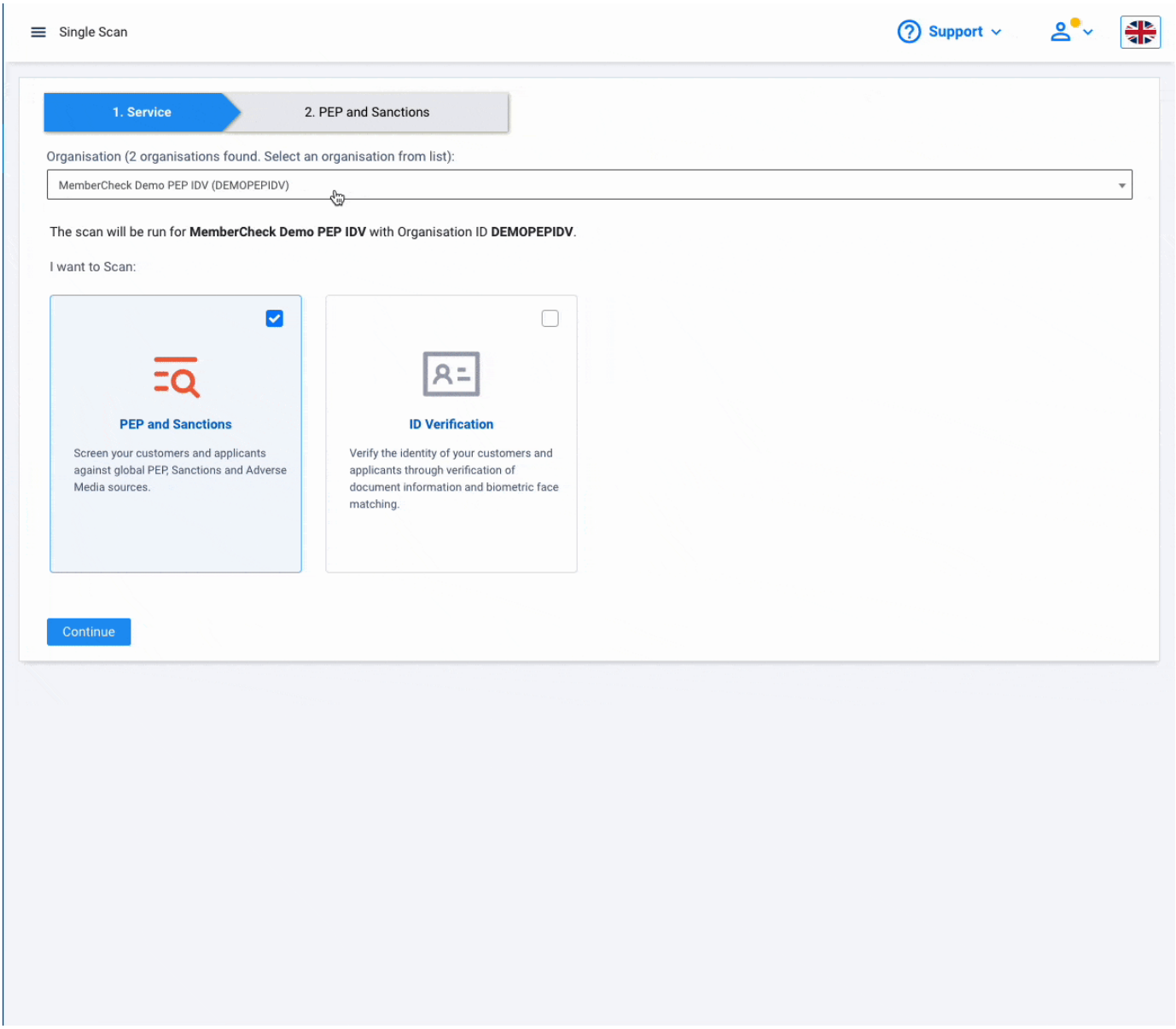
Screen to exclude domestic PEPs

Example of screening with **First Name** and **Last Name** and the exclusion of domestic PEPs, in this example, Australia is defined in the list of countries in **PEP Jurisdiction - Exclude** in Organisation Settings.



Run Customer ID Verification on behalf of the individual

Example of a document verification check (ID Check) on behalf of an individual. This option provides the quickest turnaround time for results. Results sometimes may take up to a few minutes for processing to complete.



Result status of N/A or Not Available

If you only see statuses of `N/A` (not available) and do not see any conclusive results at the bottom of the screen, the verification process may still be in progress. In this case, navigate to the **Scan Results** screen to refresh and view the latest status, noting that it may take some time depending on the data sources and services.

Email Customer ID Verification to the individual

Example of a document verification check (ID Check) request to be sent to the individual to complete via email. Until the individual completes the verification, the status of this will remain as `Pending`

Your browser does not support the video tag.

Common Questions

What if the individual has a mononymous single name?

If the individual only has a mononymous name, you can either:

- A: Enter a dash `-` in the **First Name** field and enter the single name into the **Last Name** field, or
- B: Enter the name into the **Original Script/Full Name** field.

The first approach (A) will return results with profiles where it only contains the mononymous name, or where **Last Name** matches, whereas the latter approach (B) may return additional results where names containing the entered text are returned.

Why can't I change the scan settings?

The Compliance Officer for your organisation may have preset the scan settings based on the organisation's risk and compliance obligations. For any changes to these settings, your Compliance Officer can review these settings at **Administration > Organisations > {Organisation Name} > Settings**.

I do not see any monitoring options during scan

Your organisation or your user account is likely not enabled for the ongoing monitoring service.

Check with your organisation's Compliance Officer for access.

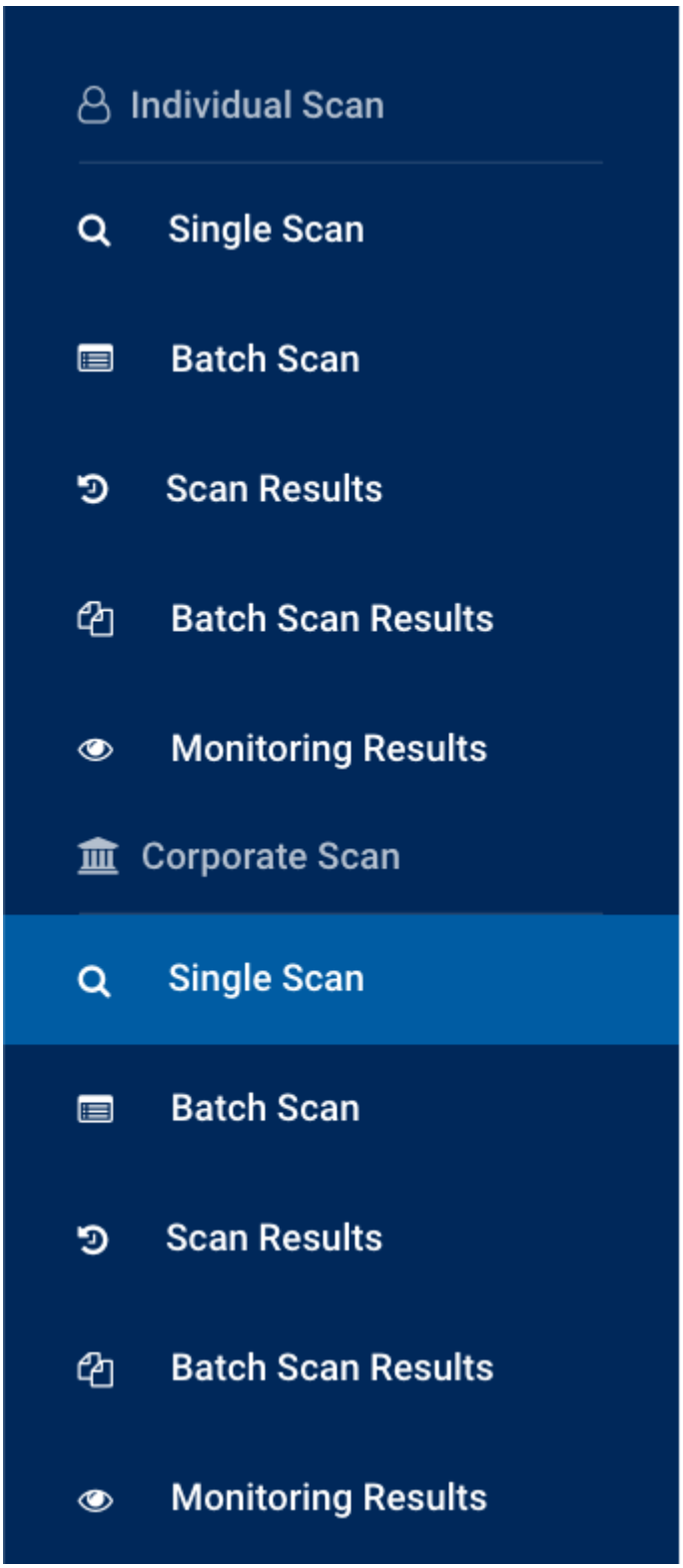
If you are a Compliance Officer or manage the MemberCheck service on behalf of your organisation, get in touch with your MemberCheck Account Manager or at sales@membercheck.com to enquire about this service.

Single Scans of Corporates

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

You can screen for Sanction, Law Enforcement, Regulatory Enforcement and Adverse Media checks for a business or corporate via **Corporate Scan > Single Scan**.



Before Running a Scan

To perform a scan of a business or corporate, you will need to check or select the following before entering details:

1. Organisation

2. Scan service type
3. Scan settings

Organisation

If you are part of a multi-level organisation structure, select the organisation which you would like to run the check for from the drop-down list for **Organisation**.

If you are part of a single level organisation, you do not need to do anything for this step.

Scan Service Type

If your organisation and user account has been enabled with additional scan services, you have the option to select these services such as Know Your Business screening.

By default, `Sanctions and Adverse Media` is selected.

Scan Settings

There are settings provided to manage the scope and coverage of sanction screening as per your organisation's risk level compliance requirements.

Compliance Officers can predetermine and preset these settings or set them to be user defined to enable the settings to be changed during scanning. These settings are defined in the **Organisation Settings**.

Scan Setting Details and Description

Option	Description

Name Match Type	Used to determine how closely a watchlist profile must match the company name before being consi

Stopwords (i.e. incorporated, pty) are ignored and excluded from matching. Special characters (excep punctuation are ignored in `Close` name match scans. Spaces and hyphens are ignored.

Exact

Scan results show matches where the watchlist record name is exactly the same as that entered in th

Close

Scan results show matches where the watchlist record name is matched based on phonetic matchin

Match Rate

If `Close` Name Match Type is selected, this can be used to control the results by setting a match rate

A higher threshold will return results with minor variations in the name whereas a lower threshold will

Example 1: The name `Greenoil` at various thresholds could return these variations:

- **100%**: `Greenoil`
- **80%**: `Greenoil`
- **50%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`
- **30%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`, `Greenall`, `Greenhall`, `Greenwell`, `Green`
- **10%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`, `Greenall`, `Greenhall`, `Greenwell`, `Green` `Cornwall` etc

Example 2: The name `Bayer` at various thresholds:

- **100%**: `Bayer`
- **80%**: `Bayer`
- **50%**: `Bayer`, `Baer`, `Payeer`
- **30%**: `Bayer`, `Baer`, `Payeer`, `Bauer`, `Beyer`, `Bower`, `Buyer`, `Beer`, `Veier`
- **10%**: `Bayer`, `Baer`, `Payeer`, `Bauer`, `Beyer`, `Bower`, `Buyer`, `Beer`, `Veier`, `Bayard`, `Barre`, `Bea`

Whitelist Policy	If Due Diligence has previously been carried out, profiles marked as `No Match` are whitelisted, and ca eliminate match results previously determined to not be a true match. This option requires an `Client ID` to be associated with the company during scanning for identifica The options are: • `Apply` : Whitelisted profiles marked as `No Match` for the company being scanned are excluded a • `Ignore` : Display all results regardless of previous due diligence decisions.
Country of Operation Policy	Used for matching the Country of the company with the locations associated with the matching profil field when scanning for the corporate entity. The options are: • `Apply to All` : Apply the matching of country. • `Ignore` : Display all results regardless of whether the country matches with the profiles.
Default Country of Operation	Used for nominating a Country of Operation where a country cannot be identified. For addresses whic **Operation** has been nominated, it will be automatically assigned to the corporate entity as the Countr This setting is defined by the Compliance Officer in the **Organisation Settings**.
Apply to blank Addresses	Used in conjunction with **Country of Operation Policy** and **Default Country of Operation**. This is used found in any of the Locations in the matching entity's profile. This option applies the preset Default Country of Operation to blank addresses during Sanction scans

Web Search (Adverse Media)	Extend the search for additional adverse media on Google. The options are: • `Yes` : Run the scan on available search engines for adverse media. • `No` : Do not run additional adverse media search.
Advanced Media Search	Perform advanced media search for recent news articles. This option provides additional AML/CTF re Sanctions profiles. Results may include article title, source name, date of publication, author and artic The options are: • `Yes` : Run the scan for recent news media. • `No` : Do not run scans for recent news media.
FATF Jurisdiction Risk	Perform additional search to include technical compliance and effectiveness ratings, based on FATF The options are: • `Yes` : Include FATF Jurisdiction Risk rating information. • `No` : Do not include FATF Jurisdiction Risk rating information.
Watchlists	Scope of watchlist categories applied for the new scan. The available options are based on the Orgar The **Compliance Officer** can edit the list in **Organisation Settings** as well lock the editing of the list.

Running a Single Scan

Sanction and Adverse Media screening

To start screening a company, the following are necessary information:

- **Company Name**
- **Client ID** (check conditions below)

Optional

- **Registration Number**
- **Country of Operation**

> **Client ID**
>
> Formerly "Entity Number". A unique reference number or profile name for the company is required if you want to add the company for ongoing monitoring or perform due diligence.
>
> You may use a Company Reference or Account ID or a profile name to keep track of this entity.
>
> In cases where a company may be allocated an account number in the future, such as new clients for example, an arbitrary number should not be allocated. The prospect or company number that will be allocated to the company when they become a 'new client' should be used as the Client ID for scanning purposes. This way, due diligence decisions will be allocated to the account and subsequently the whitelist will also be appropriately applied to that Client ID.

Providing Scan Information

You can provide information of the company in the following fields:

Field	Required	Field Limit	Description

Company Name	Mandatory	255 char	This field is *Mandatory*. Text which falls within the stopwords will be ignored e.g. `incorporated` and `pty`. Stopwords can be customised within the **Organisation administration settings**. Wildcard search is supported if you are uncertain of the company suffix. Append the asterisk (`*`) to the end of the company name.
Registration Number	Optional	100 char	Company's unique identifier including Business Registration Number, OFAC Unique ID, SIC Number, DUNS number, VAT/Tax Number, and IMO number for shipping vessels. The **Registration Number** entered will be used in the matching process and Company Name matches will be returned if the Registration Number is contained in the watchlist record or if the record does not contain any identifiers to minimise the risk of overlooking potential matches.
Country of Operation (Address)	Optional	Batch File and API: 255 char	Select the country of operation or registration from the drop-down list. You can select up to 5 countries. Only profiles with locations matching all entered countries will be returned. Results may include profiles with no location data.

Client ID	Conditional	100 char	Unique identifier for the company such as Company Reference Number or Account Number or profile name. This unique ID is associated with due diligence decisions and ongoing monitoring updates. Retaining the same Client ID for the company will assist with tracking of changes. This field is mandatory if the **Compliance Officer** has enabled the update monitoring list feature or if you have elected to record due diligence decisions and monitoring. If you do not have a Client ID to uniquely identify and track the company, you are welcome to use the auto-generate function to suggest an identifier (🔀).

Wildcard search for Company Names

If you are uncertain of the official or full entity name including the suffix, or if there are additional branch or division information which may be included in the company name, you may use the wildcard search by appending an asterisk (`*`) to the end of the name.

For example, searching for **Bank of America *** will match with the following profiles:

- `Bank of America`
- `Bank of America Corporation`
- `Bank of America Hawaii`
- `Bank of America Investment Services`
- `Bank of America N.A.`
- `Bank of America, National Association` etc.

Know Your Business

The Know Your Business verification consists of 2 processes: Know Your Business (verify company details) and Ultimate Beneficial Owner (identify shareholders and beneficial owners of the business).

To run a business check for a company, you will need the following to get started:

- **Company Name** or business **Registration Number**
- **Jurisdiction of Registry (Country or Country-State)**

> **Searching by Registration Number**
>
> The ability to search by Registration Number is dependent on the jurisdiction registry and is not within the control of MemberCheck.

Providing Scan Information

You can provide information of the individual in the following fields:

Field	Required	Field Limit	Description
Country	Required	-	Jurisdiction or Country where the business is registered in.
State	Mandatory	-	Some countries have different jurisdictions separated by state e.g. United States - Alaska, Canada - British Columbia etc
Company Name	Conditional	255 char	Name of business. This field is *Mandatory*, unless you are entering a **Registration Number**.
Registration Number	Conditional	100 char	Business registration number. This field is *Mandatory*, unless you are entering a **Company Name**.

You can run the Sanction scans or Know Your Business scans separately or together within a single scan.

After running a scan for Know Your Business and having identified the correct profile matching your search, you will need to request for the relevant information for your verification to complete the KYB scan:

- Request for the specific documents - All historical documents available of the business from the jurisdiction registry will be available for selection.
- Request for company details and UBO - Enhanced profile details including shareholders and beneficial owners.

> **Ensure you complete the KYB process**
>
> If you do not complete either of these 2 actions above, you will only be able to view the company searched without any supporting information or evidence for verification.

1. Search for a company

After searching for a company, you will be presented with company profiles matching your search.

2. Request for documentation

Once you have identified the company record you are searching for, select **View Document** to see a list of available documents from the jurisdiction registry. Each document will display the associated cost where you can request and download the document.

Sample reports of the various types of documents can be previewed before purchasing. Where sample reports are available, you will see a pop-up tooltip when hovering your mouse over the Document Title. Click on the Document Title to preview the PDF.

> **Document availability**
>
> Most of these documents may take some time to be delivered from the registry. Please give this process some time before checking the **Scan Results** screen for access to the documents.

3. Request for company details and UBO

Within each company profile, there is the option to request for additional company details that contain shareholders and beneficial owners. Select **Get Details and UBO** to request the enhanced company profile.

Availability of UBO information

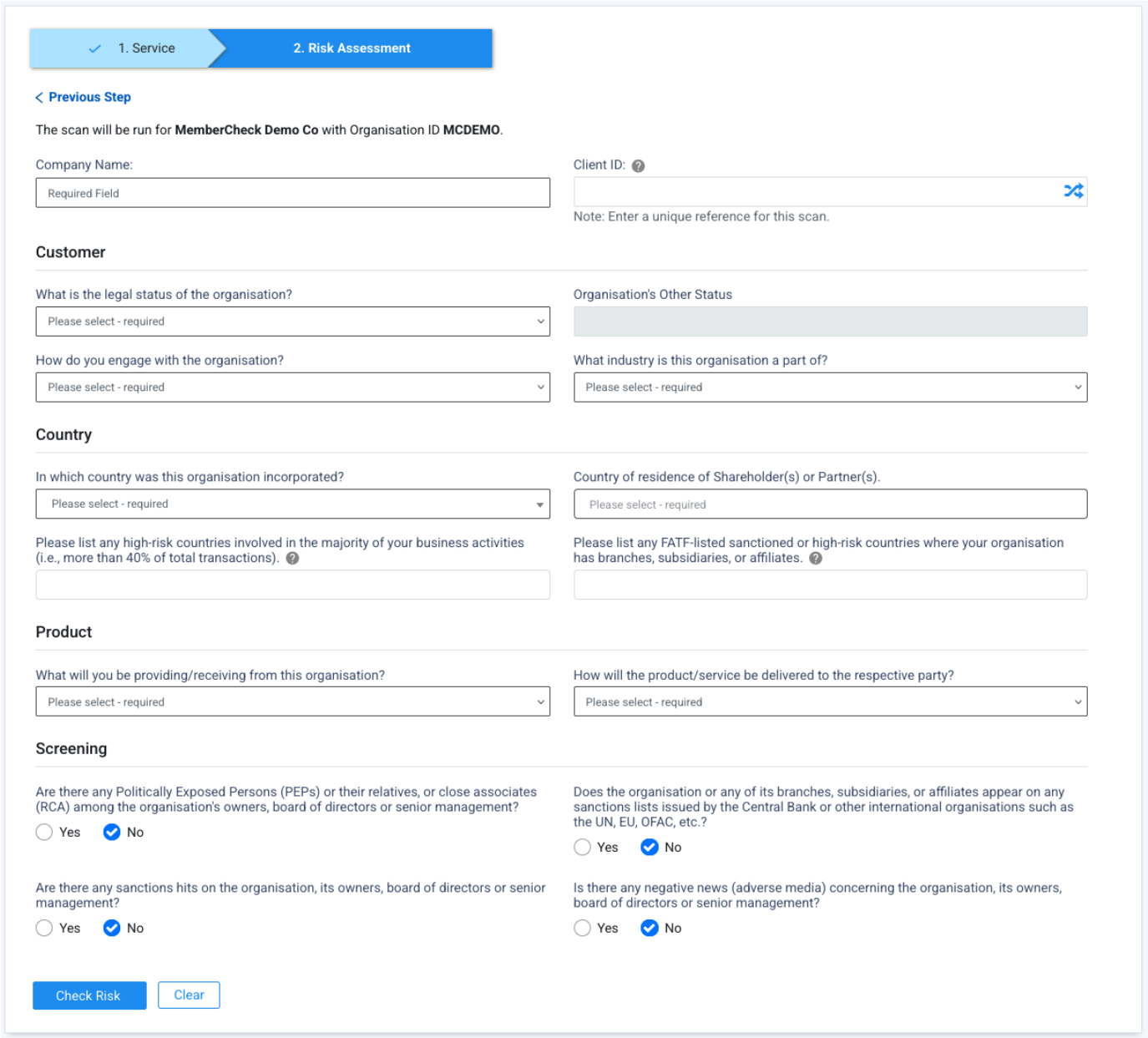
Though we strive to provide this information for as many jurisdictions as possible, it may not be available for all, and there could be instances where it is unavailable.

Risk Assessment

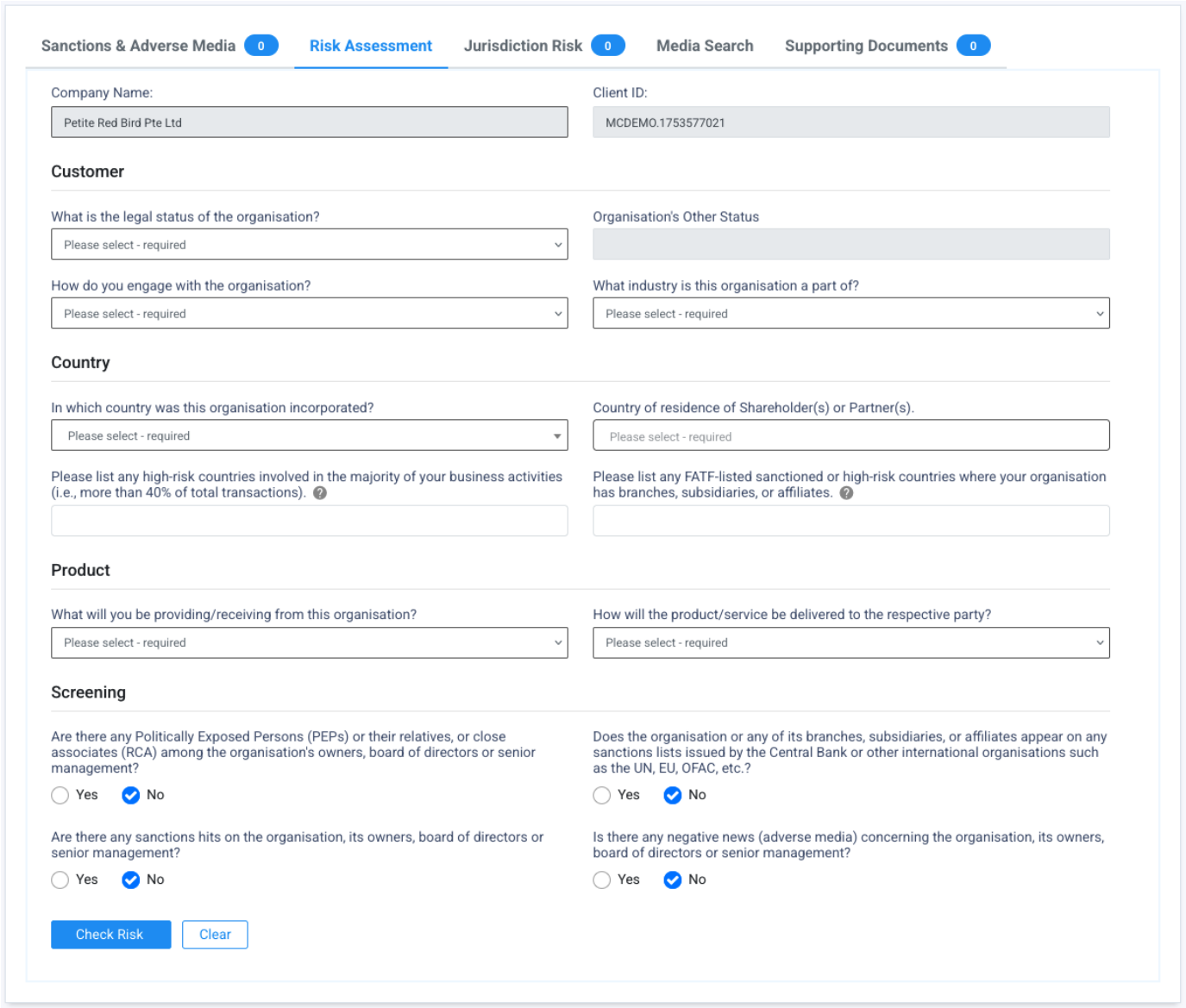
You have the option to perform additional assessment of your customer risk through a simple, structured process. When starting a new screening, you can select this service and answer key questions about the organisation including their country of incorporation, residence of shareholders/partners and identification of high-risk countries for business activities, products and services offered, and screening outcomes. You will receive a calculated risk score, risk level, and actionable recommendation.

This option is available if your organisation has subscribed to the AML Risk assessment service. When activated, all authorised users of the service with screening permission have access to this feature.

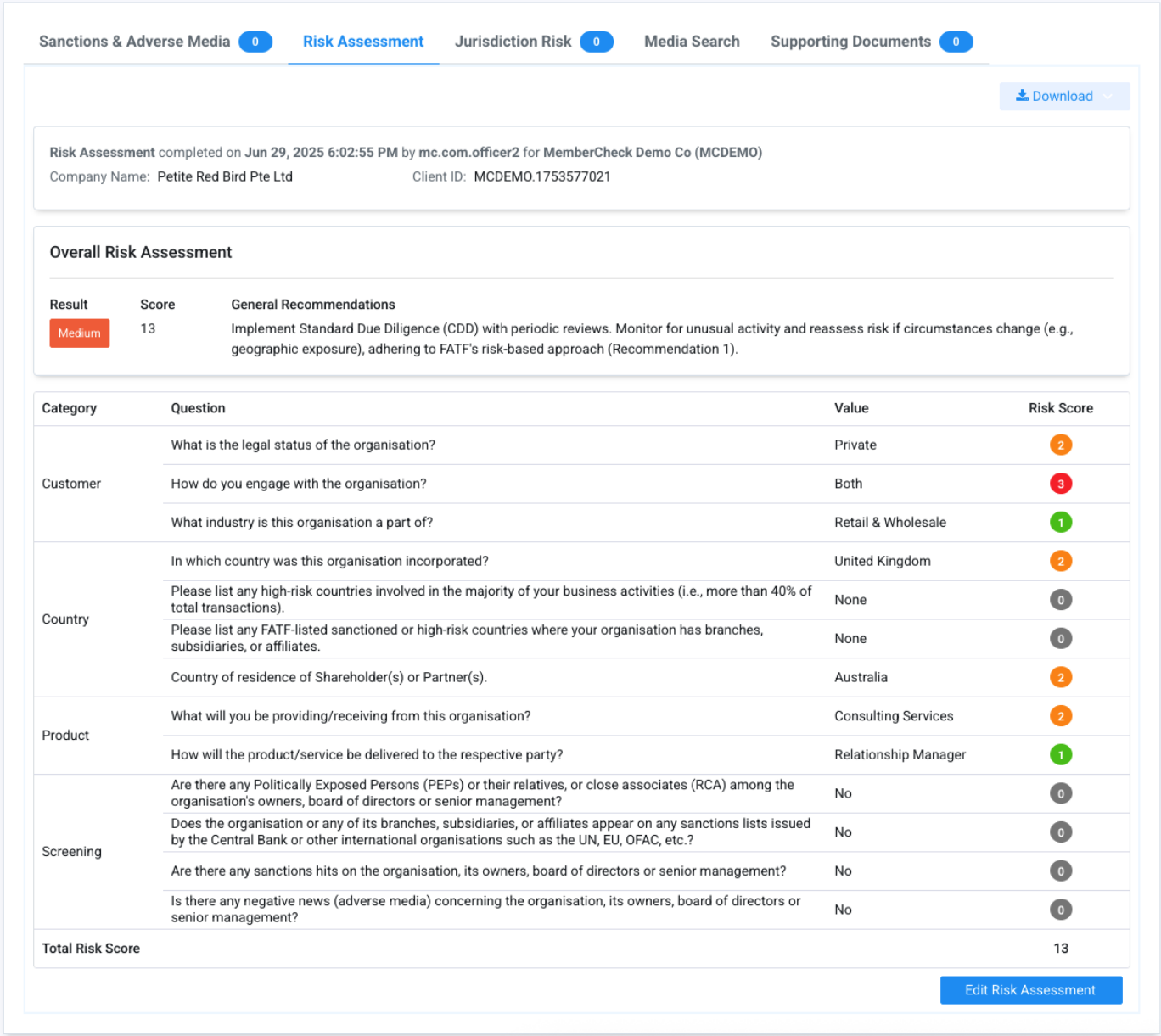
To use this service, simply select the **Risk Assessment** option when you perform a new scan. You can combine this with new Sanctions & Adverse Media scan, Know Your Business scan, or run this as a standalone check.



When you combine a Risk Assessment check with a Sanctions & Adverse Media or KYB check, you will see the Risk Assessment tab displayed in the results section for additional information of the customer.



On completion of the questionnaire, you will see the individual scores for each of the questions for transparency and an overall summary of the risk-level and actionable recommendations as a guideline.



Quick How-To Guides

Screen by Company Name and Registration Number

Your browser does not support the video tag.

Screen by Company Name with additional web search and jurisdiction risk check

Your browser does not support the video tag.

Run a Know Your Business check

Run a business check to verify and understand the company using the Know Your Business (KYB) and Ultimate Beneficial Owner (UBO) features.

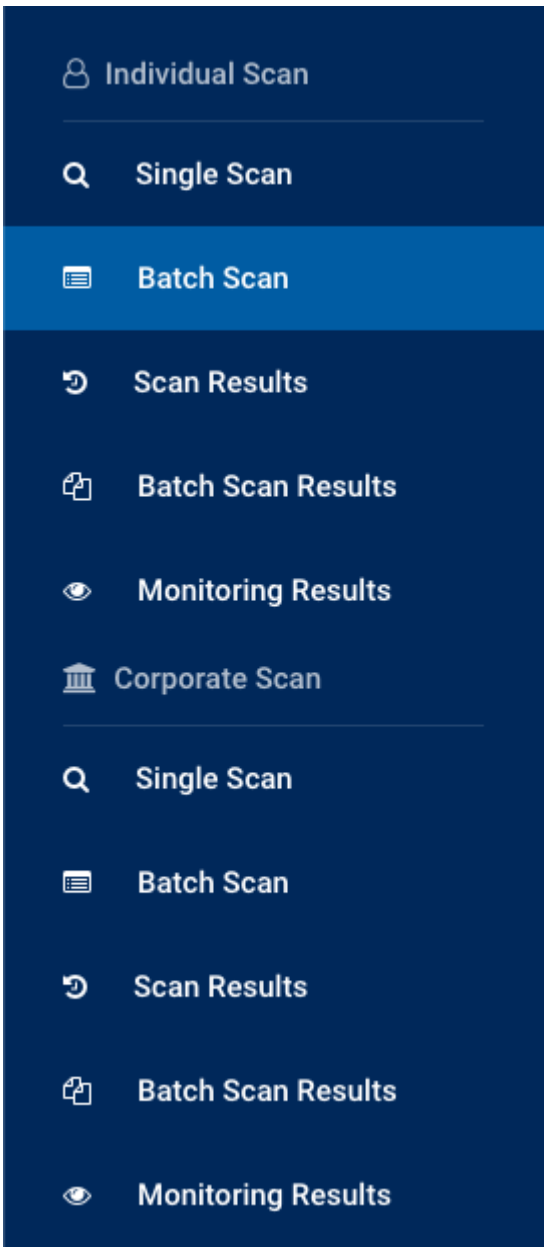
Your browser does not support the video tag.

Batch Scans for Individuals

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

You can screen for PEP & Sanction, Law Enforcement, Regulatory Enforcement and Adverse Media checks for individuals in volume via **Individual Scan > Batch Scan**.



Before Running a Scan

To perform a batch scan of individuals, you will need to check or select the following, and have your CSV or XML batch file prepared:

1. Organisation
2. Scan settings
3. Batch file in **CSV** or **XML** format (UTF-8 encoded recommended)

CSV or XML batch file templates

To help you get started, you can download CSV and XML templates and sample batch files here.

CSV vs structured spreadsheets

CSV (Comma-Separated Values) and structure spreadsheet files (e.g. XLSX from Microsoft Excel) are both used to store tabular data, but serve different purposes. CSV files are simple, plain-text files with data separated by commas, making them universally compatible across different systems and applications. In contrast, XLSX files are more complex, supporting advanced features like formatting, formulas, and multiple worksheets. When importing data into our system, using the standard CSV format ensures clean, straightforward data transfer, preventing potential import errors caused by complex spreadsheet elements.

Organisation

If you are part of a multi-level organisation structure, select the organisation which you would like to run the check for from the drop-down list for **Organisation**.

If you are part of a single level organisation, you do not need to do anything for this step.

Scan Settings

There are multiple settings provided to manage the scope and coverage of PEP & Sanction screening as per your organisation's risk level compliance requirements.

Compliance Officers can predetermine and preset these settings or set them to be user defined to enable the settings to be changed during scanning. These settings are defined in the Organisation Settings.

Scan Setting Details and Description

Option	Description

Name Match Type	Used to determine how closely a watchlist profile must match a person's name before being consider The options are `Exact`, `Exact (Including Middle Name)` or `Close`.

Exact

Scan results return matches where the First and Last Name match exactly. Middle names are also tal
Middle Name matching does not eliminate watchlist entities with no middle name. Scan results inclu

- The First and Middle and Last Name match exactly.
- The First and Last Name match exactly and the watchlist record Middle Name contains the Midd
- The First and Last Name match exactly and the watchlist record has no Middle Name.
- The First and Last Name match exactly and the Middle Name does not match.

Exact (Including Middle Name)

- The First and Middle and Last Name match exactly.
- The First and Last Name match exactly and the watchlist record Middle Name contains the Midd
- The First and Last Name match exactly and the watchlist record has no Middle Name.

Close

- The First Name and Last Name match based on a phonetic matching algorithm (similar soundin searching (spelling variations). Middle Names are ignored.

DOB Tolerance (Years)	Used to enable tolerance of date of birth variations based on years. This value applies to both before birthdate. Specifying this tolerance disregards the specific day and month to return matches within th You will only see this option if your Compliance Officer has enabled this setting for your organisation.

Match Rate

If `Close` Name Match Type is selected, this can be used to control the results by setting a match rate

A higher threshold will return results with minor variations whereas a lower threshold will return large sound of the name.

Example: The name `John` at various thresholds:

- **100%**: `John`.
- **80%**: `John`, `Johnnie`, `Johnny`.
- **50%**: `John`, `Johnnie`, `Johnny`, `Jon`, `Joan`, `Jonah`, `Jean`, `Jan`, `Joanne`, `Joanna`, `Janie`, `Gena`,
- **1%**: `John`, `Johnnie`, `Johnny`, `Jon`, `Joan`, `Jonah`, `Jean`, `Jan`, `Joanne`, `Joanna`, `Janie`, `Gena`, `Jayne`, `Juan` etc.

Example: The first name and last name `Richard JOHN` at various thresholds (asterisk indicates existe middle name or last name and may not contain `Richard` or `John`):

- **100%**: `Richard JOHN`, `Richard * JOHN`, `John RICHARD`, `John * RICHARD`, `Richard John *`.
- **80%**: `Richard JOHN`, `Richard * JOHN`, `John RICHARDS`, `John * RICHARDS`, `John RICHARDSON`, `John REICHARDT`.
- **50%**: `Richard JOHN`, `Richard * JOHN`, `Richard John *`, `John Richard *`, `John * RICHARD`, `John * RICHARDS`, `John RICHARDSON`, `John * RICHARDSON`, `John REICHARDT`, `Jon RICHARDS`, `Johnny RICHARDSON`, `* John RICHARDS`, `John ROCHARD`, `Joan RICHARDS` etc.
- **1%**: `Richard JOHN`, `Richard * JOHN`, `Richard John *`, `* Richard JOHN`, `John Richard *`, `John RICHARDS`, `John * RICHARDS`, `John RICHARDSON`, `John * RICHARDSON`, `John REICHARDT`, `Jon RICHARDSON` `Johnny RICHARDS`, `Johnny RICHARDSON`, `* John RICHARDS`, `John ROCHARD`, `Joan RICHARD`, `Joanne RICHARD`, `Joanne RICHARDS`, `Joanne RICHARDSON`, `Richard JANE`, `Jayne RICH` `Jean-Pierre RICHARD`, `Jean-paul RICHARD`, `June RICHARD`, `June RICHARDS`, `June RICHARDSON` `Richard GENAO`, `Richard GIANNI`. `Juan RICHARTE` etc.

Whitelist Policy	If Due Diligence has previously been carried out, profiles marked as `No Match` are whitelisted, and ca excluded from being returned. This can help eliminate match results previously determined to not be This option requires a `Client ID` to be associated with the person. The options are: • `Apply` : Whitelisted profiles marked as `No Match` for the person being scanned are excluded and • `Ignore` : Display all results regardless of previous due diligence decisions.
(Country of) Residence Policy	Used for matching the Country in the Address of the person with the locations associated with the ma requires the Country to be specified in the Address field when scanning for the person. The options are: • `Apply to All` : Apply the matching of country to all profiles for all categories. • `Apply to PEP` : Apply the matching of country only to profiles with the category `PEP` (Politically I • `Apply to POI` : Apply the matching of country only to profiles with the category `POI` (Profile of I • `Apply to RCA` : Apply the matching of country only to profiles with the category `RCA` (Relatives c • `Apply to SIP (incl.TER)` : Apply the matching of country only to profiles with the category `SIP` Person), which includes `Terrorism` . • `Ignore` : Display all results regardless of whether the country matches with the profiles. If you want to apply the defined PEP Jurisdiction Inclusion or Exclusion list, do not check `Apply`

Default Country of Residence	Used for nominating a Country of Residence for an individual's address where a country cannot be ide which are not blank but do not contain an identifiable country, if a **Default Country of Residence** has b be automatically assigned to the individual as the Country of Residence. This setting is defined by the Compliance Officer in the **Organisation Settings**.
Apply to blank Addresses	Used in conjunction with **Residence Policy** and **Default Country of Residence**, this is used for elimina where the individual's Country of Residence is not found in any of the Locations in the matching entity This option applies the preset Default Country of Residence to blank addresses during PEP and Sanc
PEP Jurisdiction	This setting filters PEP and RCA profiles based on defined jurisdictions for inclusion or exclusion, and filtering domestic PEPs. To use this setting, ensure `Apply to PEP` in the **Residence Policy** is unchecked. The settings available are based on the organisation settings defined by the Compliance Officer and c or Include: • `Exclude` : Exclude from matching, PEPs and RCAs with locations within the defined PEP Jurisdic • `Include` : Include in matching, PEPs and RCAs with locations within the defined PEP Jurisdiction • `Ignore` : Ignore any exclusion or inclusion of PEP jurisdictions. If no jurisdictions are defined, this will behave the same way as `Ignore` .

Exclude Deceased Persons	Used for eliminating match results where the person is recorded as deceased. The options are: • `Yes` : Exclude deceased persons from matching results. • `No` : Include deceased persons in matching results.
FATF Jurisdiction Risk	Perform additional search to include technical compliance and effectiveness ratings, based on FATF countries linked to matched profiles. The options are: • `Yes` : Include FATF Jurisdiction Risk rating information. • `No` : Do not include FATF Jurisdiction Risk rating information.
Watchlists	Scope of watchlist categories applied for the new scan. The available options are based on the Orgar The **Compliance Officer** can edit the list in **Organisation Settings** as well lock the editing of the list.

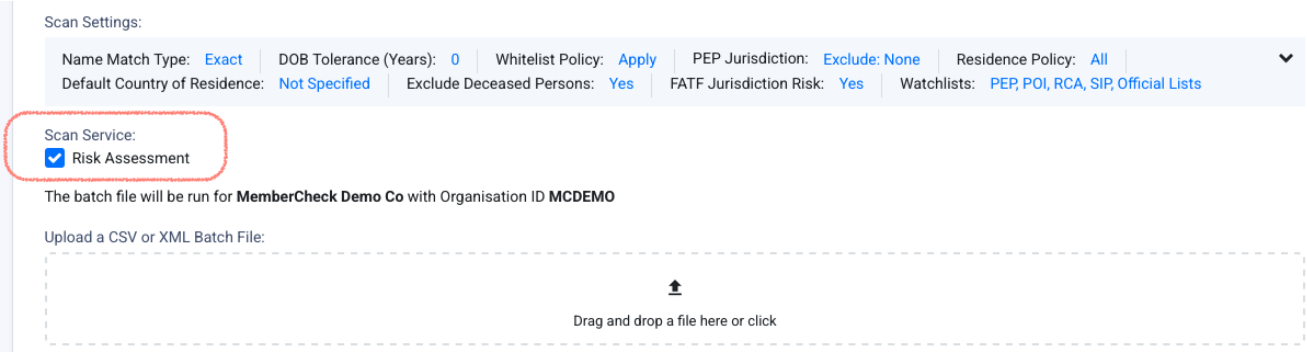
Scan Service

You have the option to perform AML risk assessments of your customers through a simple, structured process. When starting a new batch scan, you can select the service during the batch file upload screen. This will activate the Risk Assessment tab in the Batch Scan Results screen on completion of the batch processing.

This option is available if your organisation has subscribed to the AML Risk assessment service. When activated, all authorised users of the service with screening permission have access to this feature.

Accessing Risk Assessment check for batch scans

You must select the **Risk Assessment** scan service at the start of the batch file processing in order to use this feature. Otherwise, this tab will not be visible in the **Scan Results** or **Batch Scan Results** screens.



Preparing Your Batch File

Please refer to the section Batch Files for details of the batch file formatting.

Running a Batch Scan

To start screening for multiple individuals using a batch file, the following are necessary information:

- **Organisation ID**
- **First Name and Last Name** or **Full Name** or **Original Script Name**
- **Client ID** (check conditions below)
- **Date of Birth** (check conditions below)

Client ID

Formerly "Member Number". A unique reference identifier or profile name for the individual is required if you want to add the person for ongoing monitoring or perform due diligence.

You may use a Customer Reference or Client Account ID or any unique identifier for the person.

In cases where individuals do not have and never will have a Client ID, such as staff for example, arbitrary Client IDs can be used and prefixed by a letter, or letters, to distinguish them from your regular client base.

In cases where individuals may be allocated a Client ID in the future, such as new clients for example, an arbitrary number should not be allocated. The client number that will be allocated to the individual when they become a 'new client' should be used as the Client ID for scanning purposes. In this way, due diligence decisions will be allocated to the real client identifier and subsequently the whitelist will also be appropriately applied to that Client ID.

Date of Birth

The Date of Birth will be required during scanning if your **Compliance Officer** has enabled this feature in the **Organisation Settings > Ignore Blank DOB**.

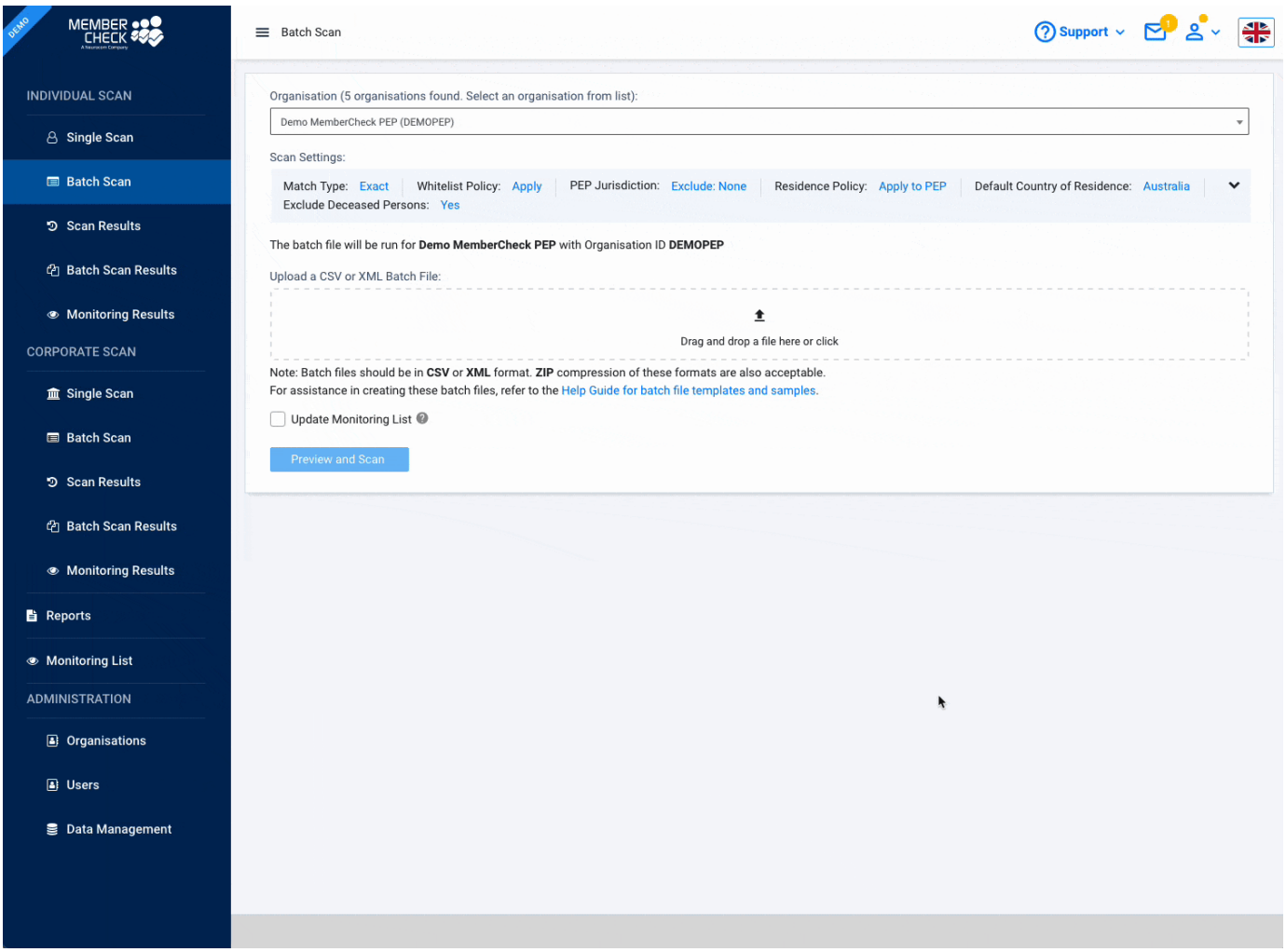
The more information you are able to provide for the person will enable more targetted matches and improve the results returned.

Batch files are processed asynchronously. Once the system has completed the upload, it will process the file in the background, enabling you to navigate to other areas of the site, or start uploading another batch file.

Quick How-To Guides

Upload and scan batch file

Upload a CSV, XML or ZIP of the batch file and preview the contents of the file before running the scan. The formatting of the batch file will be validated during this process.



Duplicate entries and Client ID detection in batch files

Preprocessing of batch files include detection of duplicate entries and Client IDs **within the same batch file**. If the batch validation setting is turned off, duplicate entries will be ignored and excluded from processing. If the validation setting is turned on, the system will not proceed until the duplicates are removed or corrected.

Your browser does not support the video tag.

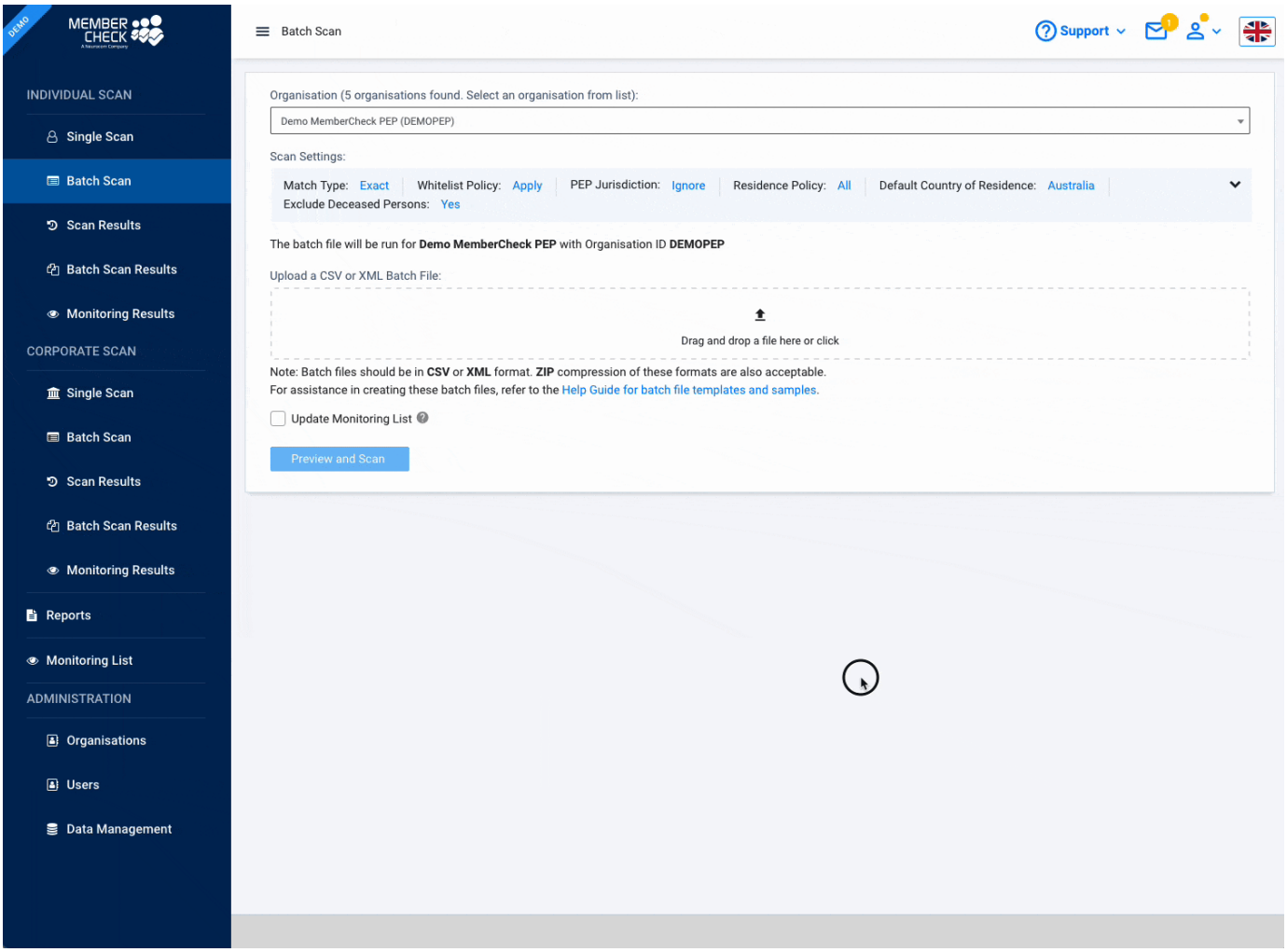
Errors with batch file

Upload a batch file (CSV, XML or ZIP of CSV or XML file) and preview the contents of the file before running the scan.

If there are formatting issues with the batch file, these specific cells will be highlighted for correction in your CSV or XML file, or the source which generated the files. Duplicate entries and Client IDs are also detected and highlighted for your attention. From this screen, you may choose **Close** to stop the batch scan process until the file is corrected, or **Scan Anyway** to ignore the problematic entries and proceed with the scan.

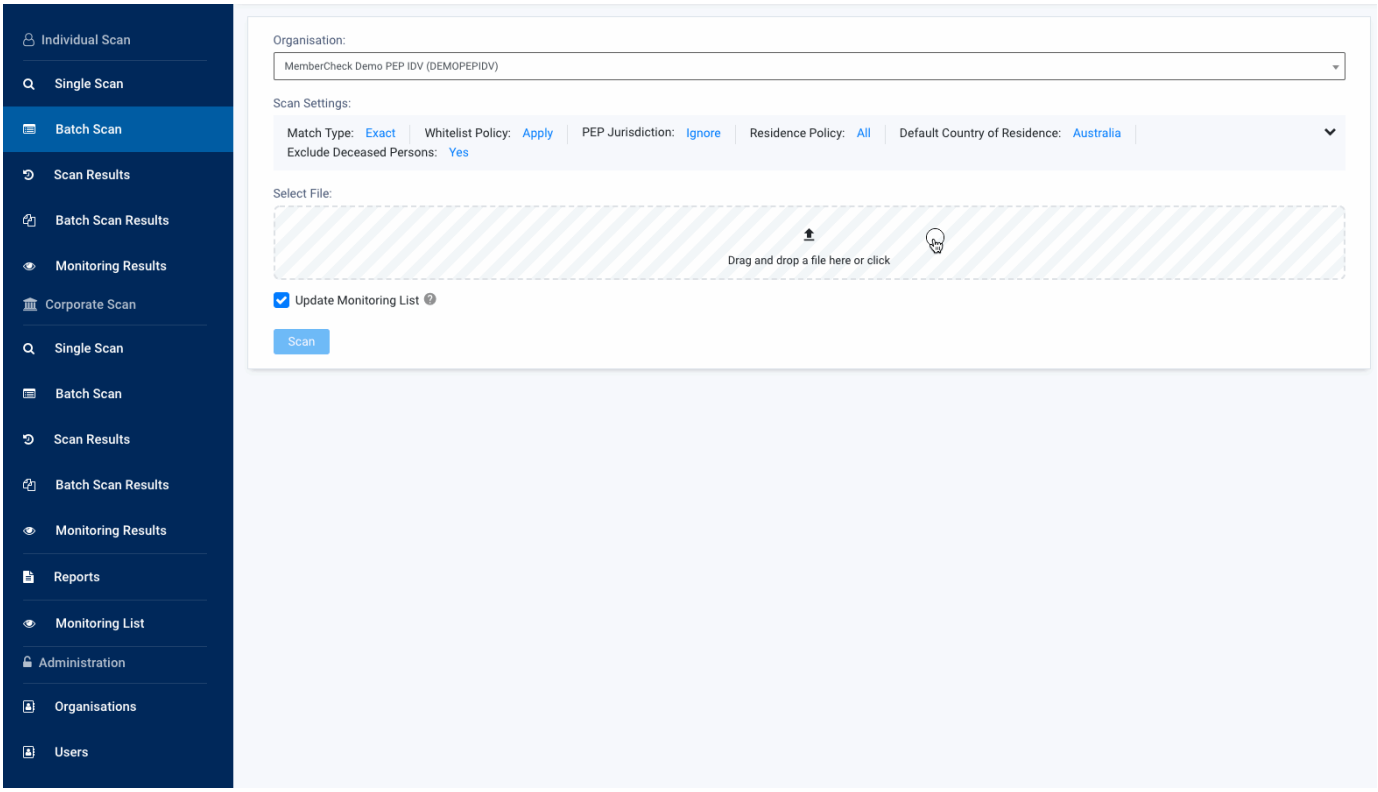
Batch file validation

- Please note that the batch file validation is limited to formatting checks only, and does not check for validity of contents.
- Duplicate entries found within the batch file will not allow the system to proceed until they are removed or corrected.
- If you are unable to proceed to scan the erroneous batch file, your organisation settings may be stopping you from doing so. Please check the **Batch Setting** as described in **Administration > Manage Organisation**



View results of batch scan

On completion of the batch scan you may opt to run another batch scan if you have multiple files or view results of the batch scan. Results of batch scans are available in **Individual Scan > Batch Scan Results**



Common Questions

Why can't I change the scan settings?

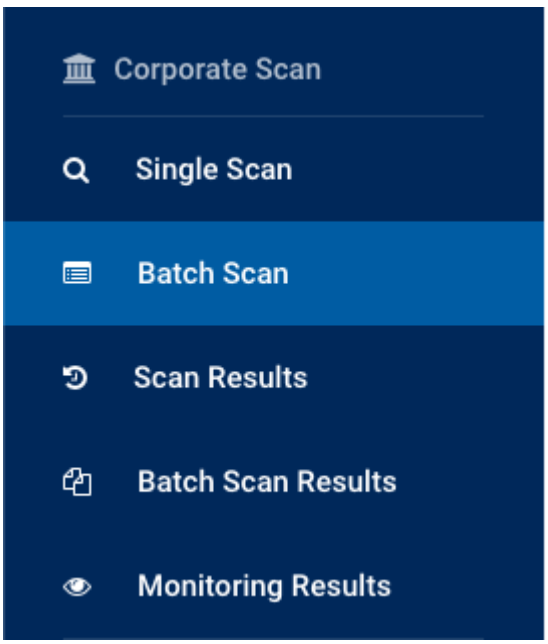
The Compliance Officer for your organisation may have preset the scan settings based on the organisation's risk and compliance obligations. For any changes to these settings, your Compliance Officer can review these settings at **Administration > Organisations > {Organisation Name} > Settings**.

Batch Scans for Corporates

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	✎	✎	✎	✕	✕

You can screen for Sanction, Law Enforcement, Regulatory Enforcement and Adverse Media checks for companies in volume via **Corporate Scan > Batch Scan**.



Before Running a Scan

To perform a batch scan of companies, you will need to check or select the following, and have your CSV or XML batch file prepared:

1. Organisation
2. Scan settings
3. Batch file in **CSV** or **XML** format (UTF-8 encoded recommended)

CSV or XML batch file templates

To help you get started, you can download CSV and XML templates and sample batch files here.

CSV vs structured spreadsheets

CSV (Comma-Separated Values) and structure spreadsheet files (e.g. XLSX from Microsoft Excel) are both used to store tabular data, but serve different purposes. CSV files are simple, plain-text files with data separated by commas, making them universally compatible across different systems and applications. In contrast, XLSX files are more complex, supporting advanced features like formatting, formulas, and multiple worksheets. When importing data into our system, using the standard CSV format ensures clean, straightforward data transfer, preventing potential import errors caused by complex spreadsheet elements.

Organisation

If you are part of a multi-level organisation structure, select the organisation which you would like to run the check for from the drop-down list for **Organisation**.

If you are part of a single level organisation, you do not need to do anything for this step.

Scan Settings

There are multiple settings provided to manage the scope and coverage of Sanction screening as per your organisation's risk level compliance requirements.

Compliance Officers can predetermine and preset these settings or set them to be user defined to enable the settings to be changed during scanning. These settings are defined in the **Organisation Settings**.

Scan Setting Details and Description

Option	Description

Name Match Type	Used to determine how closely a watchlist profile must match a company's name before being consic The options are `Exact` or `Close`. **Exact** Scan results return matches where the Company Name matches exactly. **Close** Scan results show matches where the watchlist record name is matched based on phonetic matchin

Match Rate

If `Close` Name Match Type is selected, this can be used to control the results by setting a match rate

A higher threshold will return results with minor variations whereas a lower threshold will return large

Example 1: The name `Greenoil` at various thresholds could return these variations:

- **100%**: `Greenoil`
- **80%**: `Greenoil`
- **50%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`
- **30%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`, `Greenall`, `Greenhall`, `Greenwell`, `Green`
- **10%**: `Greenoil`, `Greenwill`, `Greenlay`, `Greenhill`, `Greenall`, `Greenhall`, `Greenwell`, `Green` `Cornwall` etc

Example 2: The name `Bayer` at various thresholds:

- **100%**: `Bayer`
- **80%**: `Bayer`
- **50%**: `Bayer`, `Baer`, `Payeer`
- **30%**: `Bayer`, `Baer`, `Payeer`, `Bauer`, `Beyer`, `Bower`, `Buyer`, `Beer`, `Veier` etc
- **10%**: `Bayer`, `Baer`, `Payeer`, `Bauer`, `Beyer`, `Bower`, `Buyer`, `Beer`, `Veier`, `Bayard`, `Barre`, `Bea`

Whitelist Policy	If Due Diligence has previously been carried out, profiles marked as `No Match` are whitelisted, and ca results previously determined to not be a true match. This option requires a `Client ID` to be associated with the company. The options are: • `Apply` : Whitelisted profiles marked as `No Match` for the company being scanned are excluded a • `Ignore` : Display all results regardless of previous due diligence decisions.
FATF Jurisdiction Risk	Perform additional search to include technical compliance and effectiveness ratings, based on FATF The options are: • `Yes` : Include FATF Jurisdiction Risk rating information. • `No` : Do not include FATF Jurisdiction Risk rating information.
Watchlists	Scope of watchlist categories applied for the new scan. The available options are based on the Orgar The **Compliance Officer** can edit the list in **Organisation Settings** as well lock the editing of the list.

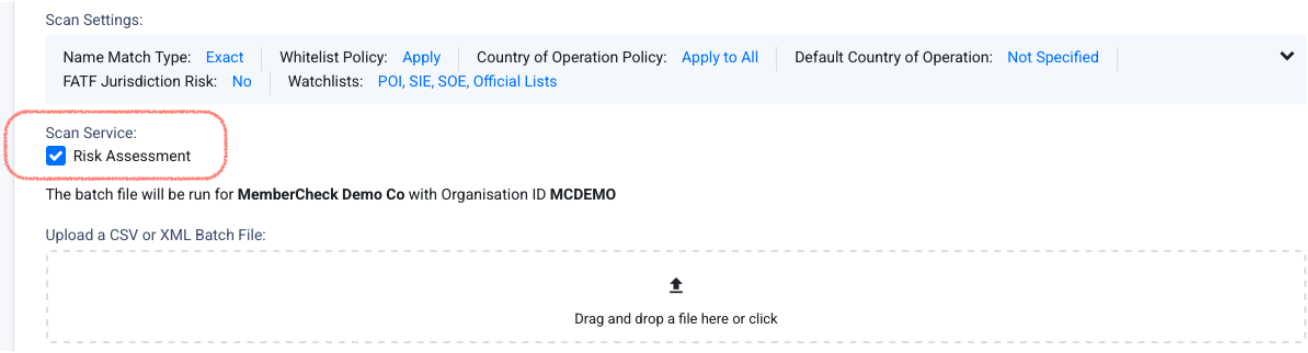
Scan Service

You have the option to perform AML risk assessments of your customers through a simple, structured process. When starting a new batch scan, you can select the service during the batch file upload screen. This will activate the Risk Assessment tab in the Batch Scan Results screen on completion of the batch processing.

This option is available if your organisation has subscribed to the AML Risk assessment service. When activated, all authorised users of the service with screening permission have access to this feature.

Accessing Risk Assessment check for batch scans

You must select the **Risk Assessment** scan service at the start of the batch file processing in order to use this feature. Otherwise, this tab will not be visible in the **Scan Results** or **Batch Scan Results** screens.



Preparing Your Batch File

Please refer to the section Batch Files for details of the batch file formatting.

Running a Batch Scan

To start screening for multiple individuals using a batch file, the following are necessary information:

- **Organisation ID**
- **Company Last Name**
- **Client ID** (check conditions below)

Optional:

- **Registration Number**

Client ID

Formerly "Entity Number". A unique reference identifier or profile name for the company is required if you want to add the record for ongoing monitoring or perform due diligence.

You may use a Company Reference or Account ID or any unique identifier for the company.

In cases where the company may be allocated an account number in the future, such as new clients for example, an arbitrary number should not be allocated. The company account number that will be allocated to the company when they become a 'new client' should be used as the Client ID for scanning purposes. In this way, due diligence decisions will be allocated to the real account number and subsequently the whitelist will also be appropriately applied to that Client ID.

Batch files are processed asynchronously. Once the system has completed the upload, it will process the file in the background, enabling you to navigate to other areas of the site, or start uploading another batch file.

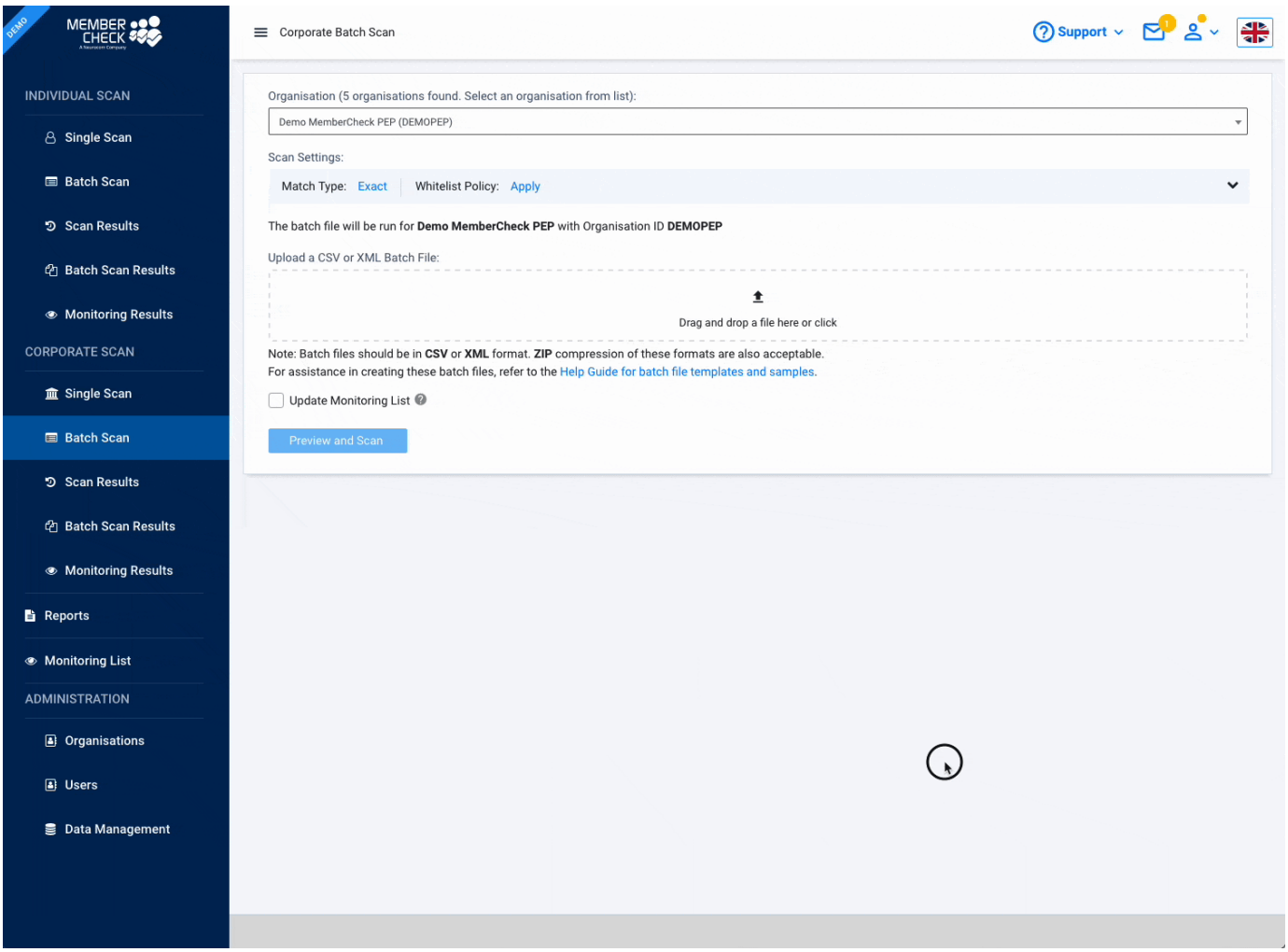
There is a protection mechanism in place which will detect if the same batch file name has been processed in the organisation within the last 12 months to warn of duplicate batch processing, whereby you can continue to proceed or cancel the duplicate batch scan.

Please refer to the section Batch Files for details of the batch file formatting.

Quick How-To Guides

Upload and scan batch file

Upload a CSV, XML or ZIP of the batch file and preview the contents of the file before running the scan. The formatting of the batch file will be validated during this process.



Duplicate entries and Client ID detection in batch files

Preprocessing of batch files include detection of duplicate entries and Client IDs **within the same batch file**. If the batch validation setting is turned off, duplicate entries will be ignored and excluded from processing. If the validation setting is turned on, the system will not proceed until the duplicates are removed or corrected.

Your browser does not support the video tag.

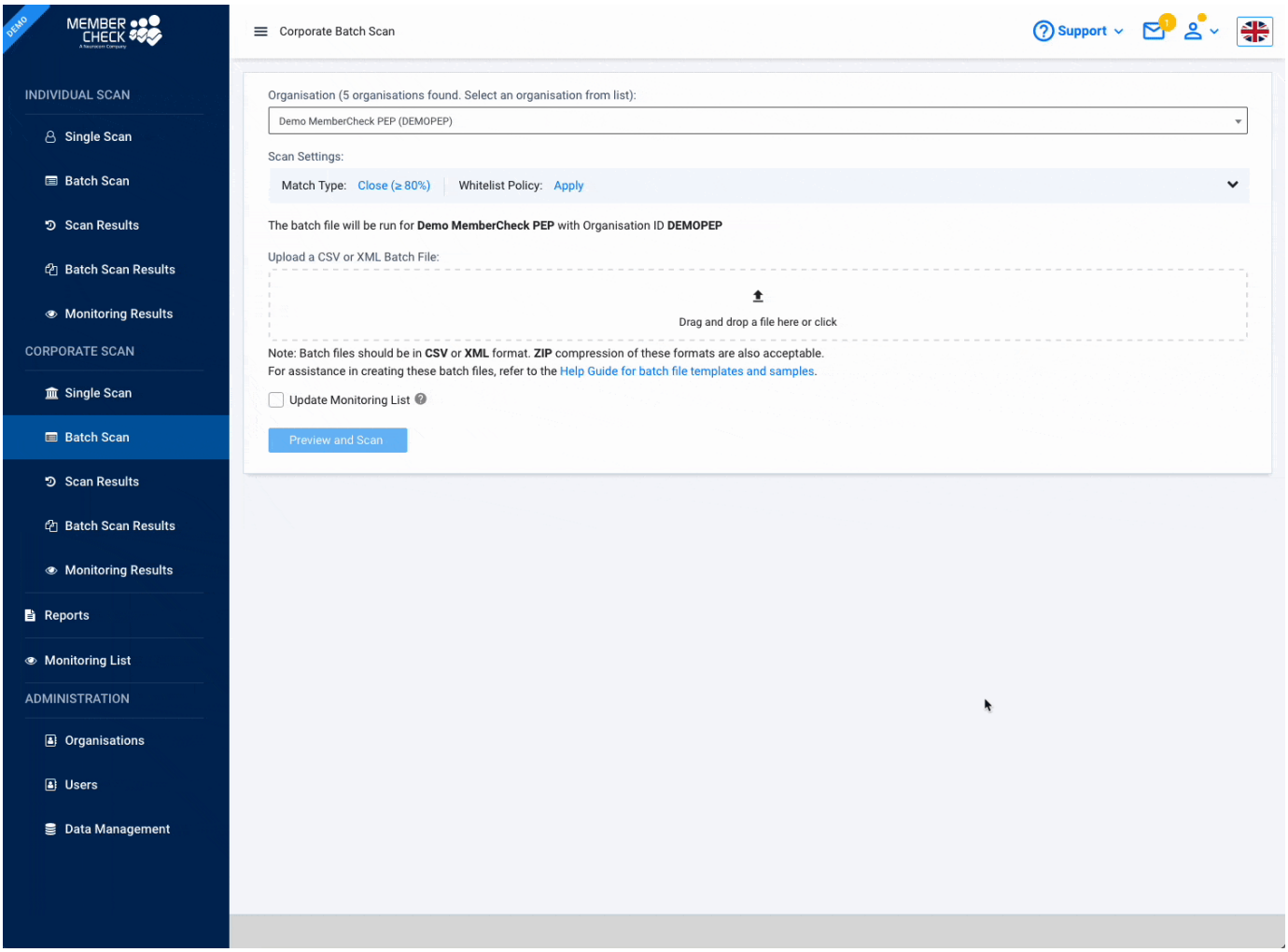
Errors with batch file

Upload a batch file (CSV, XML or ZIP of CSV or XML file) and preview the contents of the file before running the scan. If there are formatting issues with the batch file, these specific cells will be highlighted for correction in your CSV or XML file, or the source which generated the files.

From this screen, you may choose **Close** to stop the batch scan process until the file is corrected, or **Scan Anyway** to ignore the problematic entries and proceed with the scan.

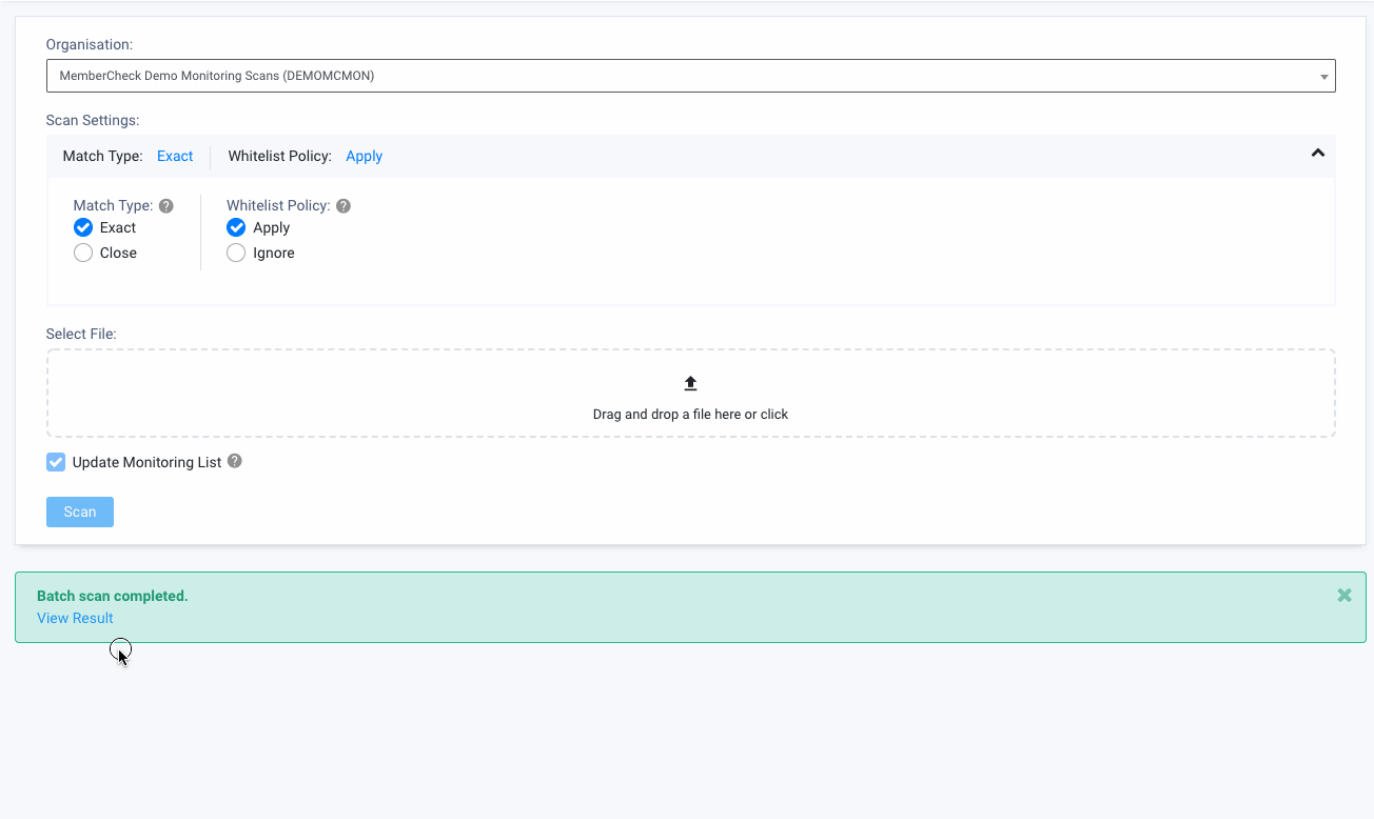
Batch file validation

- Please note that the batch file validation is limited to formatting checks only, and does not check for validity of contents.
- If you are unable to proceed to scan the erroneous batch file, your organisation settings may be stopping you from doing so. Please check the **Batch Setting** as described in **Administration > Manage Organisation**



View results of batch scan

On completion of the batch scan you may opt to run another batch scan if you have multiple files or view results of the batch scan. Results of batch scans are available in **Individual Scan > Batch Scan Results**



Common Questions

Why can't I change the scan settings?

The Compliance Officer for your organisation may have preset the scan settings based on the organisation's risk and compliance obligations. For any changes to these settings, your Compliance Officer can review these settings at **Administration > Organisations > {Organisation Name} > Settings**.

Monitoring Results

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

Ongoing Monitoring

Ongoing monitoring is integrated into the existing individual and corporate scan processes for a convenient way to access and manage monitoring of individuals and corporate entities, review outcome of monitoring scans and perform risk assessment for due diligence.

Monitoring Results are separated for Individuals and Corporates and can be accessed via **Scan Results** and **Monitoring Results**.

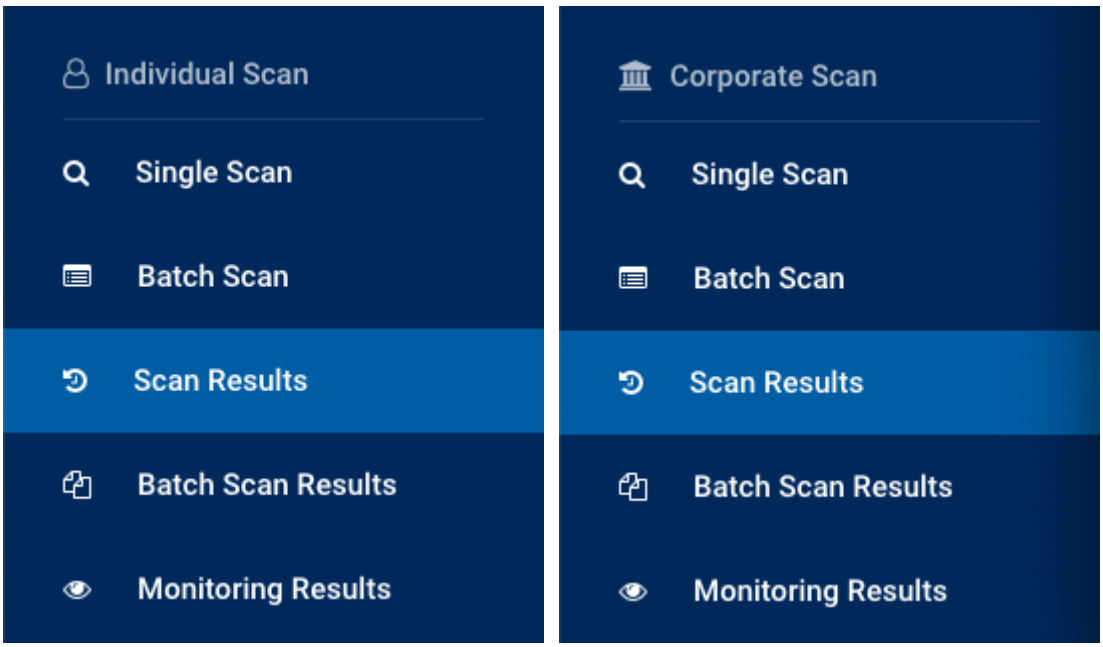
Detected changes in profiles which match monitored individuals or corporate entities will indicate the type of change (new matched profile, updated profile details of matches, or removed matches). These notifications are independent of any due diligence decisions performed unless the whitelist policy setting has been applied for the monitoring setting.

Notifications of detected changes can be configured to be emailed or notified via API. These monitoring settings are described in greater detail at **Manage Organisations**

Viewing Changes for Individuals and Corporates

Monitoring Scan Results for specific entities

To view results of the automated monitoring scans for individuals, use **Individual Scan > Scan Results** or for companies, use **Corporate Scan > Scan Results**. You can filter and view the monitoring changes from a high level or filter to view changes for a specific individual.



Monitoring Scan Activities

There are two types of ongoing monitoring scan activities performed by the system automatically:

- **Monitoring Scans** - detects changes in monitored entities against the frequently updated watchlists on a regular basis and displays the differences in the watchlist profile from when the ongoing process schedule is last run.
- **Monitoring Rescans** - runs a scan of the monitored entities against the entire watchlist database and returns matches found. This process does not detect and highlight changes in the profiles returned. This process runs on the anniversary of the subscription renewal date for all active entities in the **Monitoring List**.

Monitoring Status of Matches

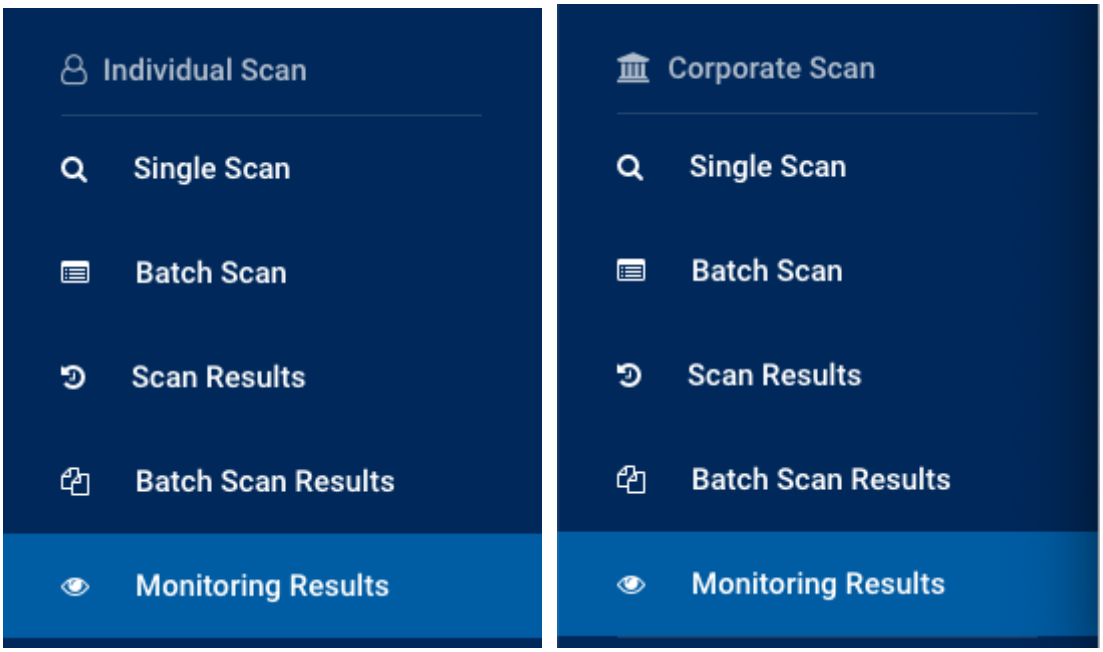
You can filter the monitoring statuses to assist with your prioritisation and escalation of due diligence and risk assessment.

Status	Icon	Description
New Matches		Automatic monitoring scans where a new match was found for the individual or company ("entity"). This may be due to new profiles being added to the watchlists, or updated watchlist profile information which now matches with the monitored entity.

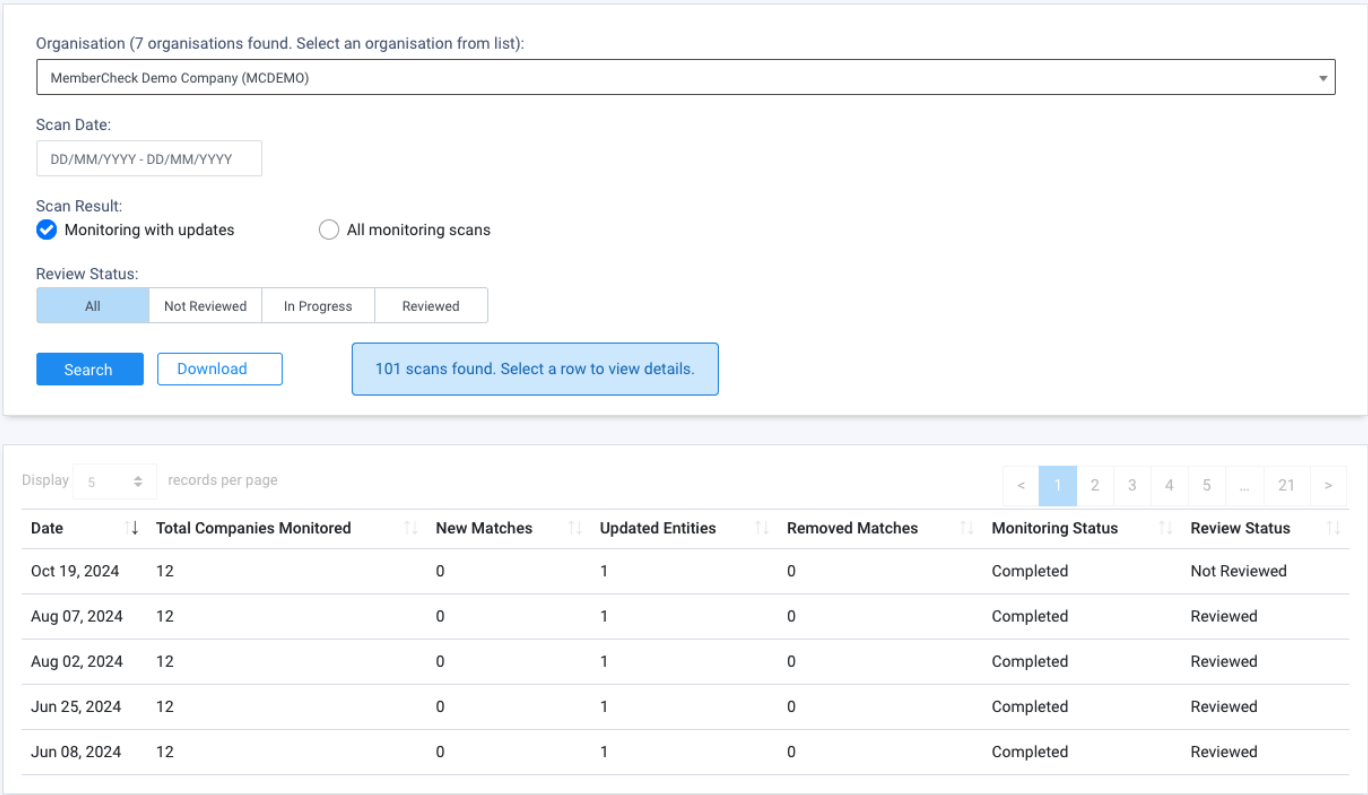
Updated Matches	🟡	Automatic monitoring scans where the profile of an existing match for the entity has been updated, or updated profile in the watchlist now matches the monitored entity.
Removed Matches	🟢	Automatic monitoring scans where an existing match no longer applies to the entity due to removal of the profile from the watchlists.
No Changes		Automatic monitoring scans where no changes were found for the monitored entity.

Monitoring Results

For an overview of the monitoring scan activities, which can be run `Daily`, `Weekly`, `Fortnightly`, `Quarterly` or `Semi Annually`, use **Individual Scan > Monitoring Results** or **Corporate Scan > Monitoring Results** for individuals and companies respectively. This provides an overview of the number of entities being monitored and the results. You can drill down to view detailed changes for a monitored individual or corporate similar to **Scan Results**.



By default, only monitoring scans which contain changes in matched results are displayed in the list (`Monitoring with updates`). To view a full list of all monitoring activities, select the option `All monitoring scans` .



Date	Total Companies Monitored	New Matches	Updated Entities	Removed Matches	Monitoring Status	Review Status
Oct 19, 2024	12	0	1	0	Completed	Not Reviewed
Aug 07, 2024	12	0	1	0	Completed	Reviewed
Aug 02, 2024	12	0	1	0	Completed	Reviewed
Jun 25, 2024	12	0	1	0	Completed	Reviewed
Jun 08, 2024	12	0	1	0	Completed	Reviewed

Review Status

The Compliance Officer can turn on ongoing monitoring results view to see the optional **Review Status** information via **Administration > Organisation > Monitoring Settings**.

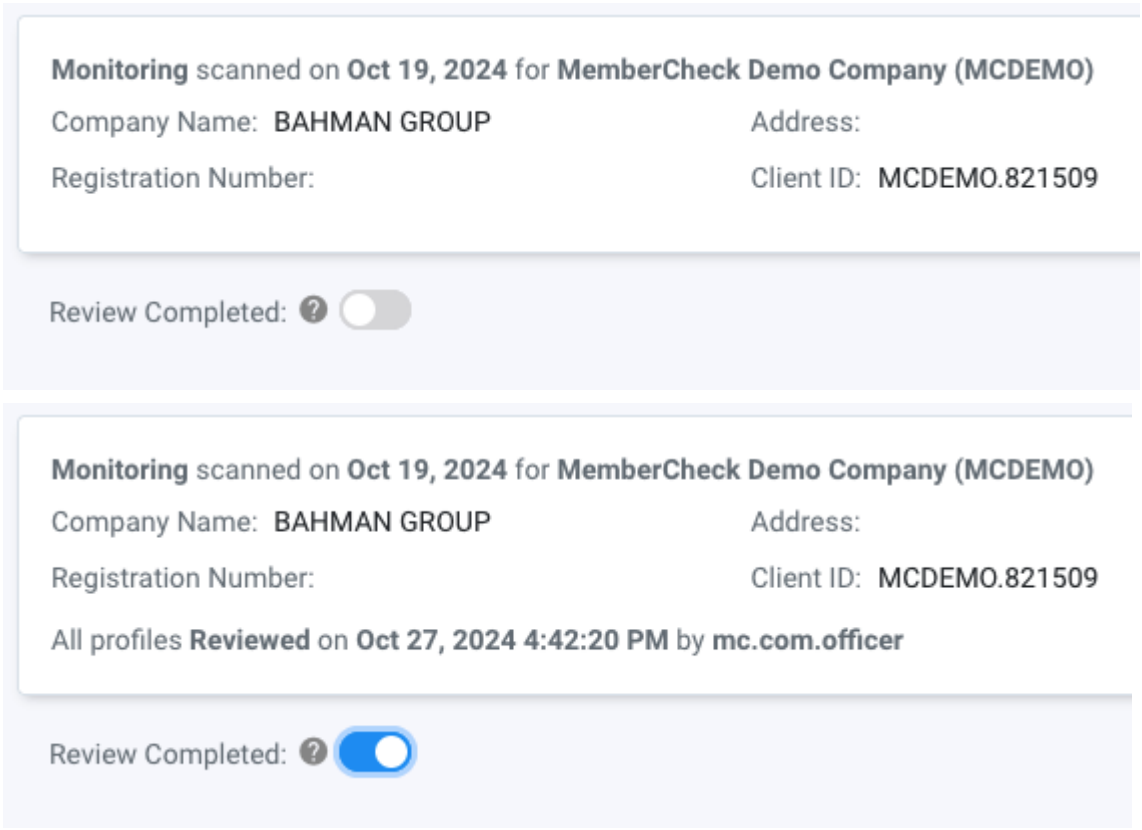
Column Name	Description
Date	Date the monitoring process was run.
Total Individuals/Companies Monitored	Total number of active monitored entities in the Monitoring List on the day of scan.
New Matches	Number of new results which match the monitored entity.
Updated Entities	Number of matched results with changes in the profile which still match the monitored entity.
Removed Matches	Number of results which no longer match the monitored entity.

Monitoring Status	Status of the monitoring process. Statuses can be: • `Completed` - process completed • `In progress` - currently running • `Error` - service error.
Review Status	Status of the ongoing monitoring review, which can be: • `Not Reviewed` - Review has not started • `In progress` - Shows reviewed entities versus total changed entities (e.g. 5/10) • `Reviewed` - All changes have been assessed.

You may select a row for the day the monitoring scan was run to view detailed information of the results of the monitoring scan and the scan settings and policies applied.

To track the progress of assessments of changed profiles, you can toggle the **Review Completed** switch to indicate you have completed the review of all profiles that have been changed in the monitoring check.

Toggle the **Review Completed** switch after you have reviewed all profile changes from the monitoring check to help track progress of review.



This will update the

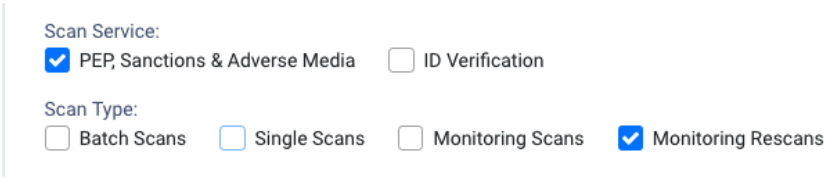
Monitoring Rescan

In addition to continuous monitoring of entities against the daily updated watchlist, an annual rescan is performed for all active monitored entities in the **Monitoring List** on the date of Subscription Renewal. This is an automated process to proactively ensure compliance with regulations, mitigate financial and reputational risk and reduce the likelihood of inadvertent engagement with sanctioned parties.

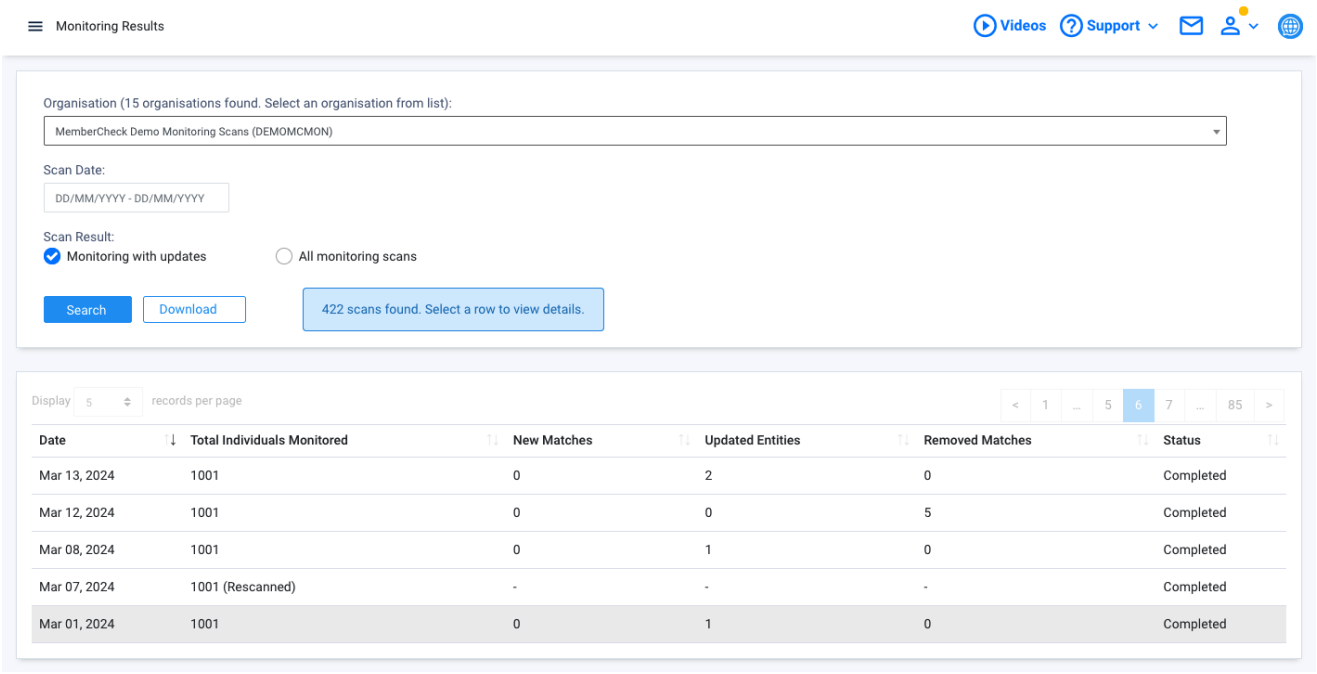
The rescan process checks against the entire watchlist database and may disregard any whitelisting and due diligence decisions depending on the whitelist policy in the organisation monitoring setting. This process reports on whether the entity has a `Match` or `No Match`, and does not report on changes to the profile e.g. new, updated or removed matches.

The outcome of the rescan can be viewed via the following screens:

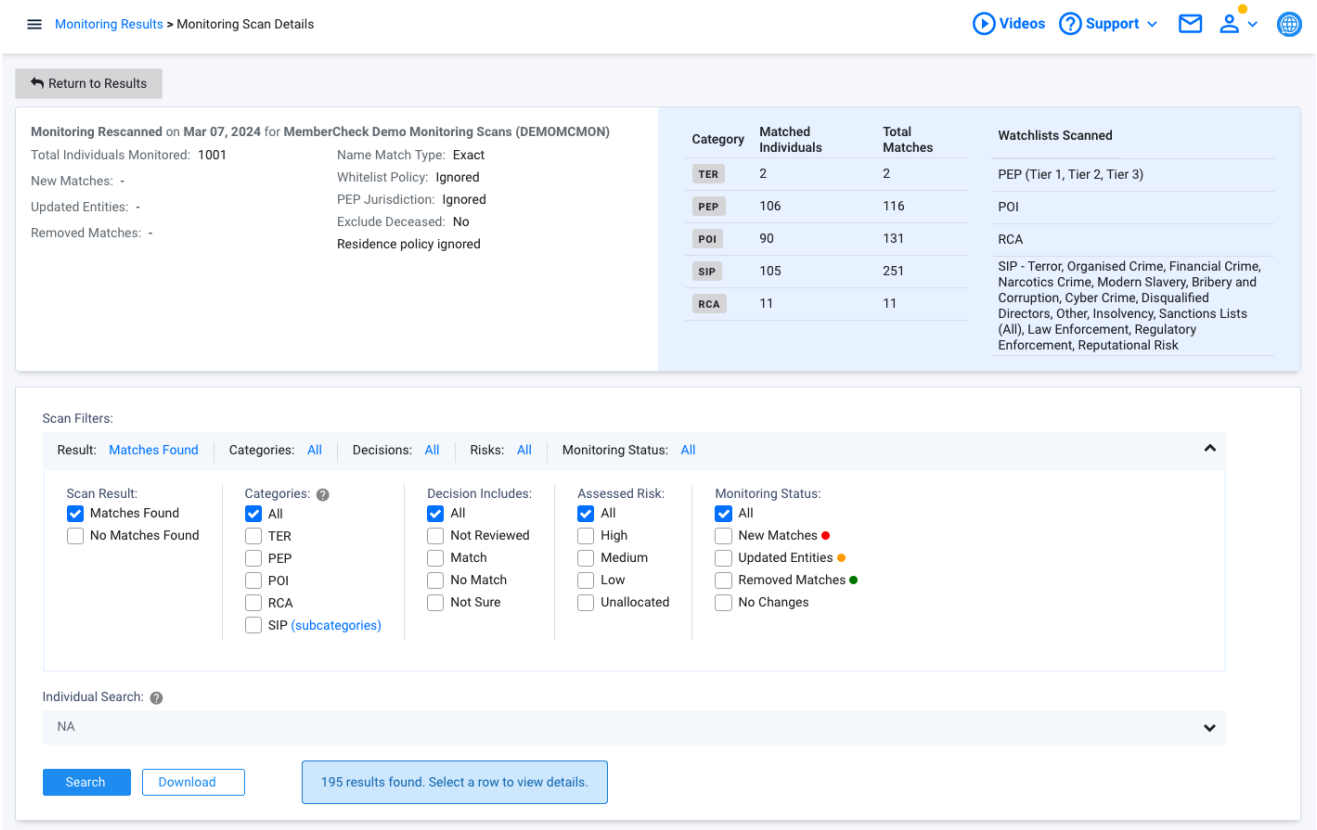
- **Scan Results** - Select `Monitoring Rescans` in the scan type filter



- **Monitoring Results** - this activity will be displayed in the list as "Rescanned".



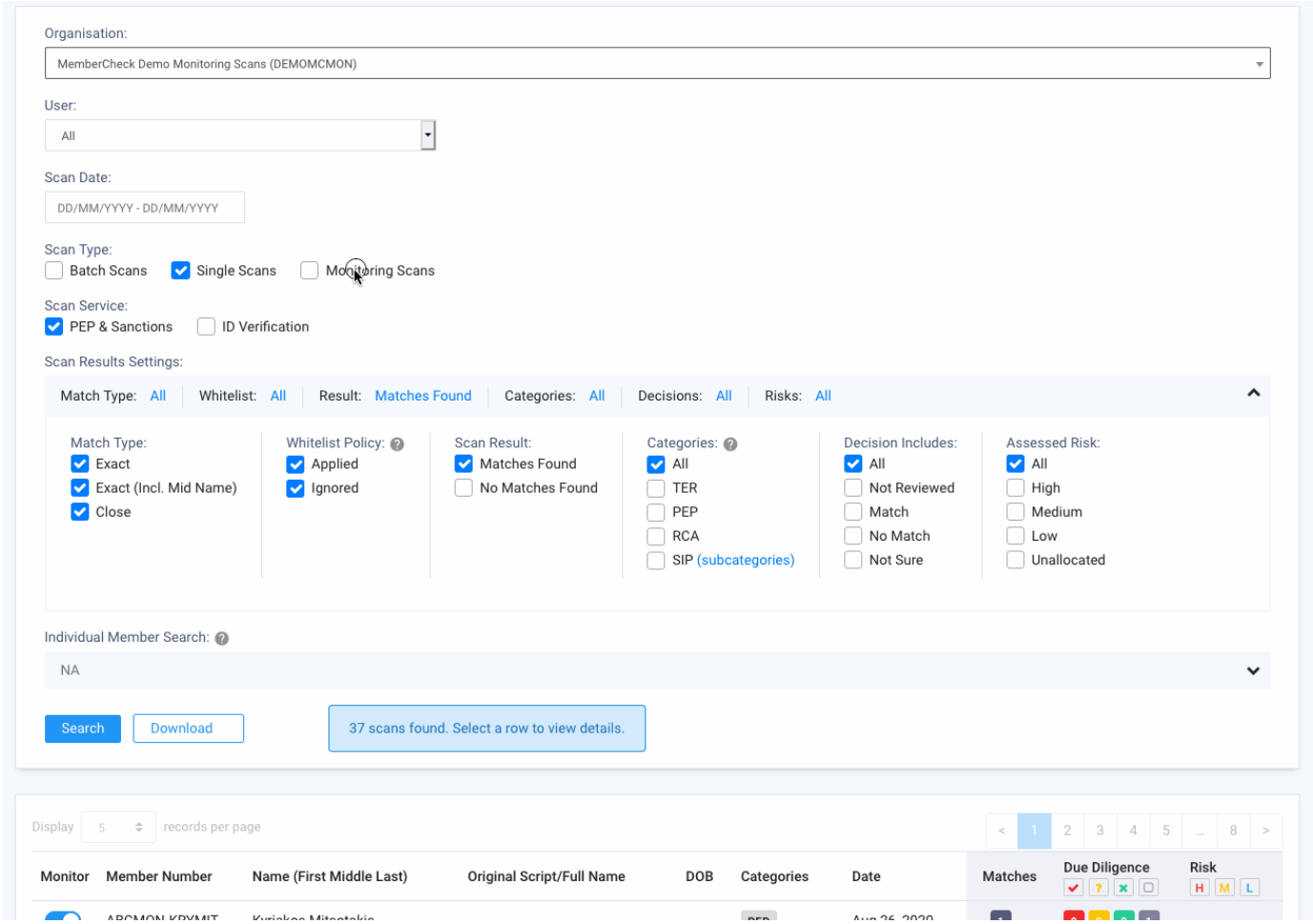
Click on the row to view detailed results of the rescan:



How-To Guides

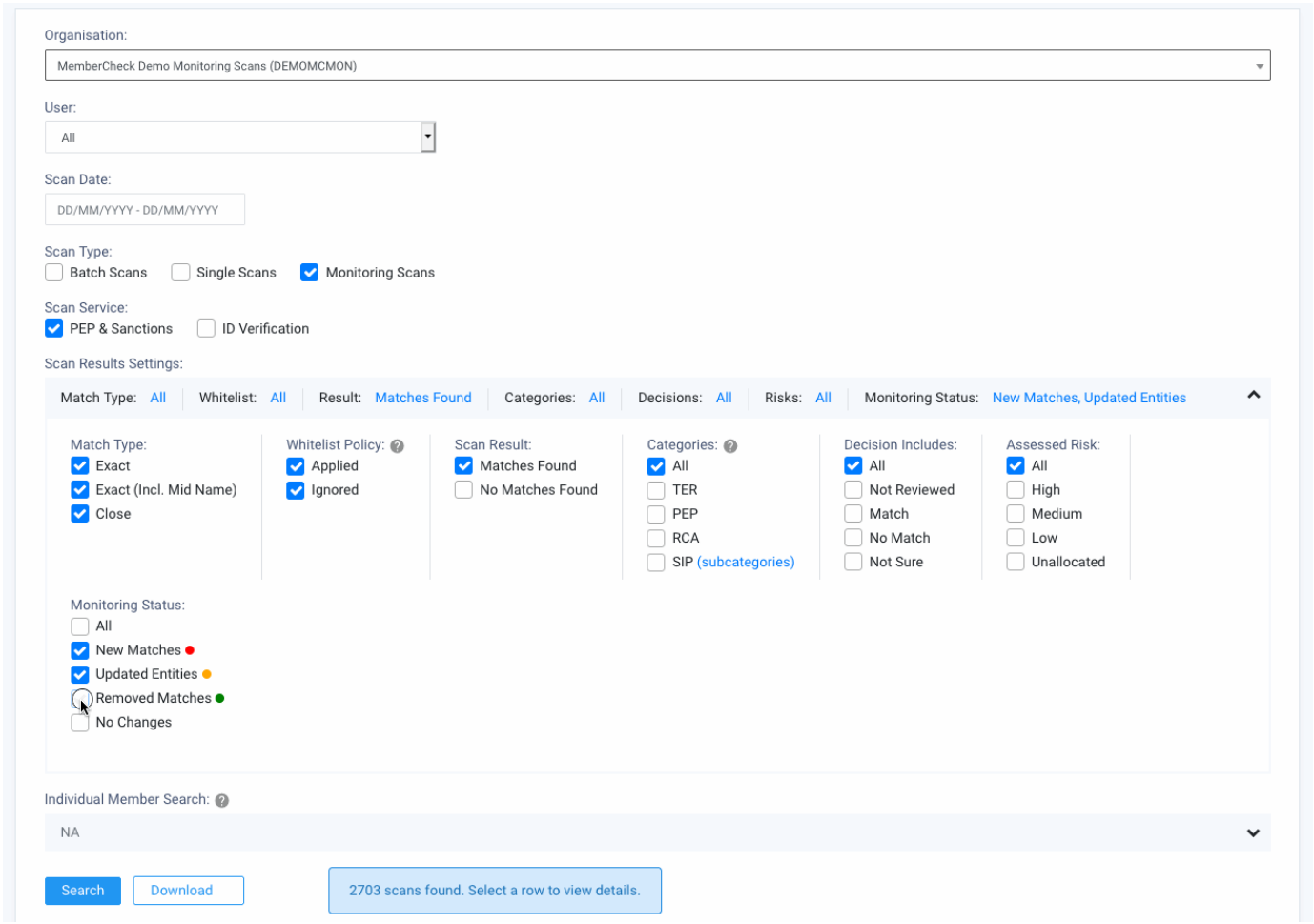
View all monitored individuals

To view *all monitored individuals*, within **Scan Results**, you can simply select to filter **Scan Type** for `Monitoring Scans`.



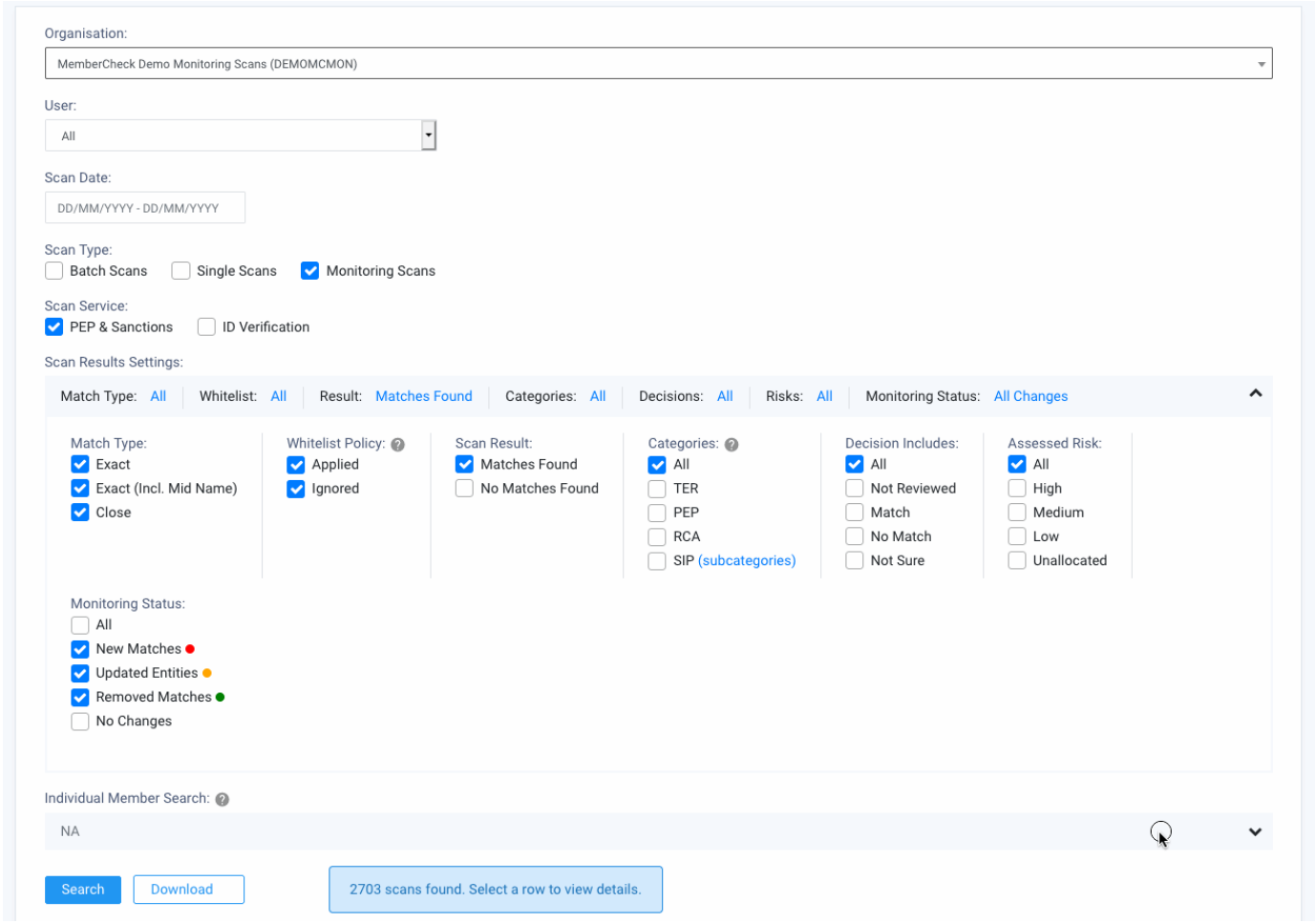
View monitored individuals with specific outcomes

To view *all monitored individuals with specific outcomes*, you can select the relevant **Monitoring Status** by `New Matches`, `Updated Entities`, `Removed Matches`.



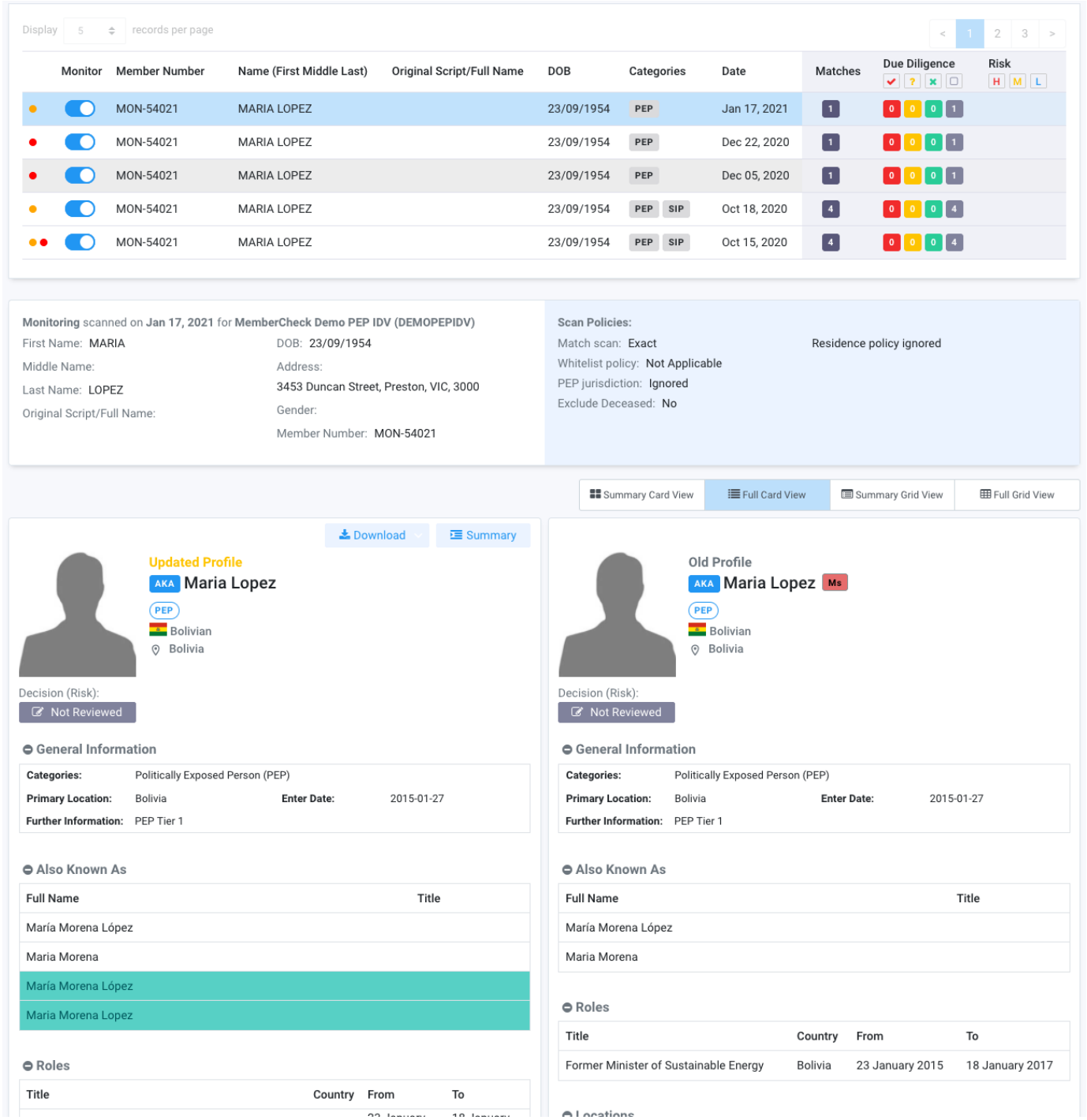
View specific monitored individual

To view all changes for a specific individual, you can specify the unique identifier for the individual in **Client ID**.



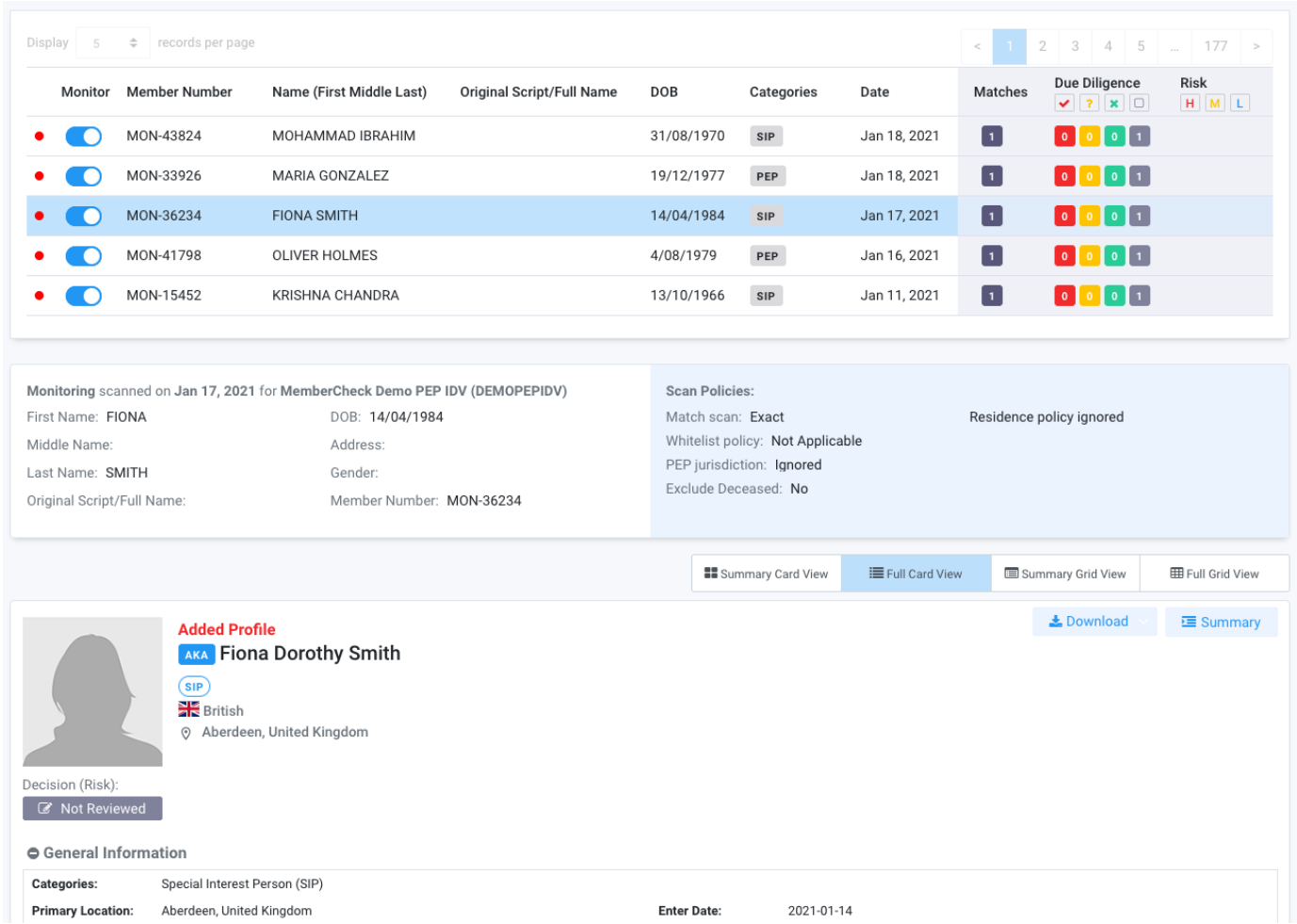
Compare updated profile information

Select an entry to view the matching profile. If the monitoring scan has flagged a matching profile as updated, these changes are highlighted and displayed on the left-hand side which contains the latest profile information.



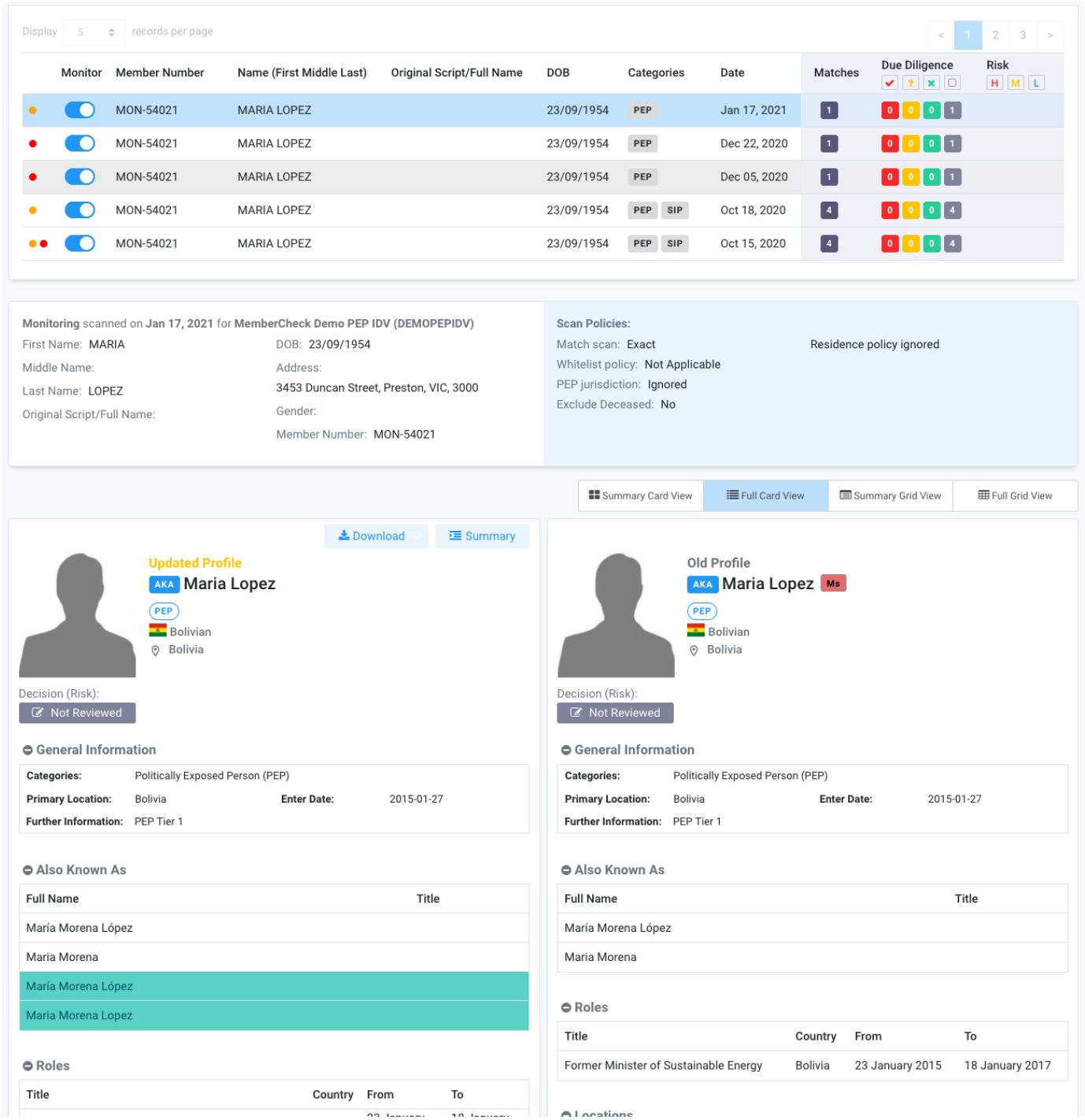
View New Matches

Example of a new profile being added to the watchlist that has triggered a new match:



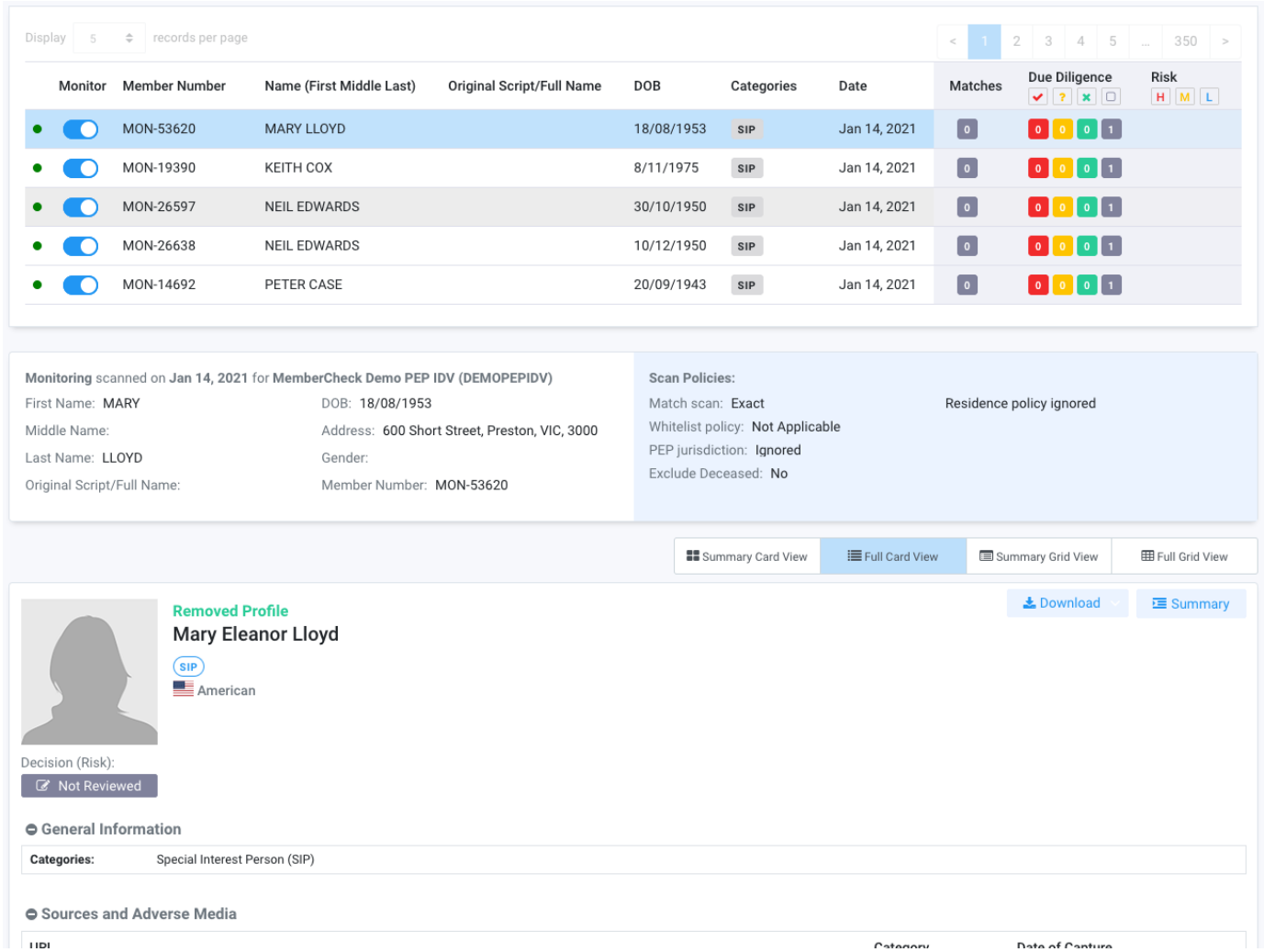
View Updated Entities

Example of an existing match that has an updated profile in the latest watchlist. A side by side comparison of the new (left side) and previous (right side) profile is displayed for review and due diligence:



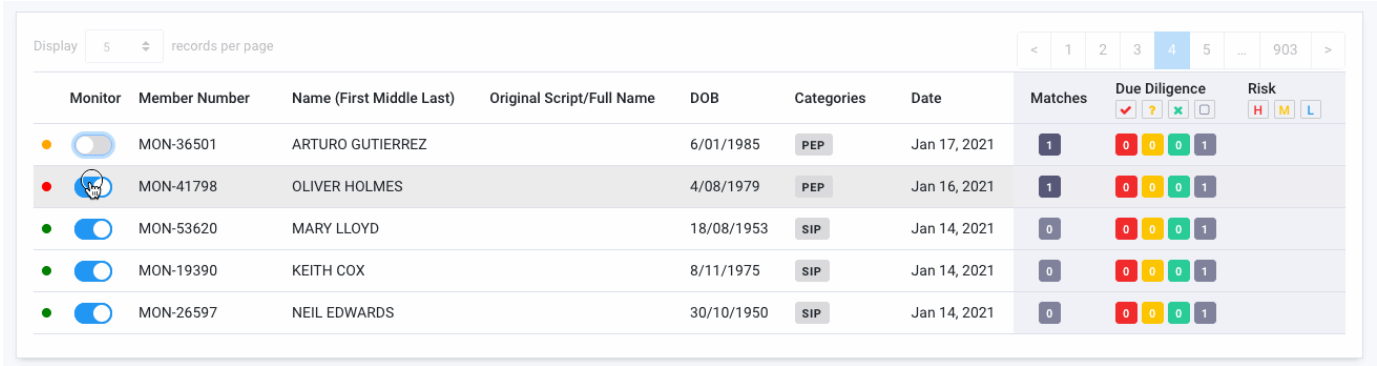
View Removed Matches

An example where a previously matched profile has been removed from the watchlists that has triggered a **No Match** result:



Enable and Disable Monitoring

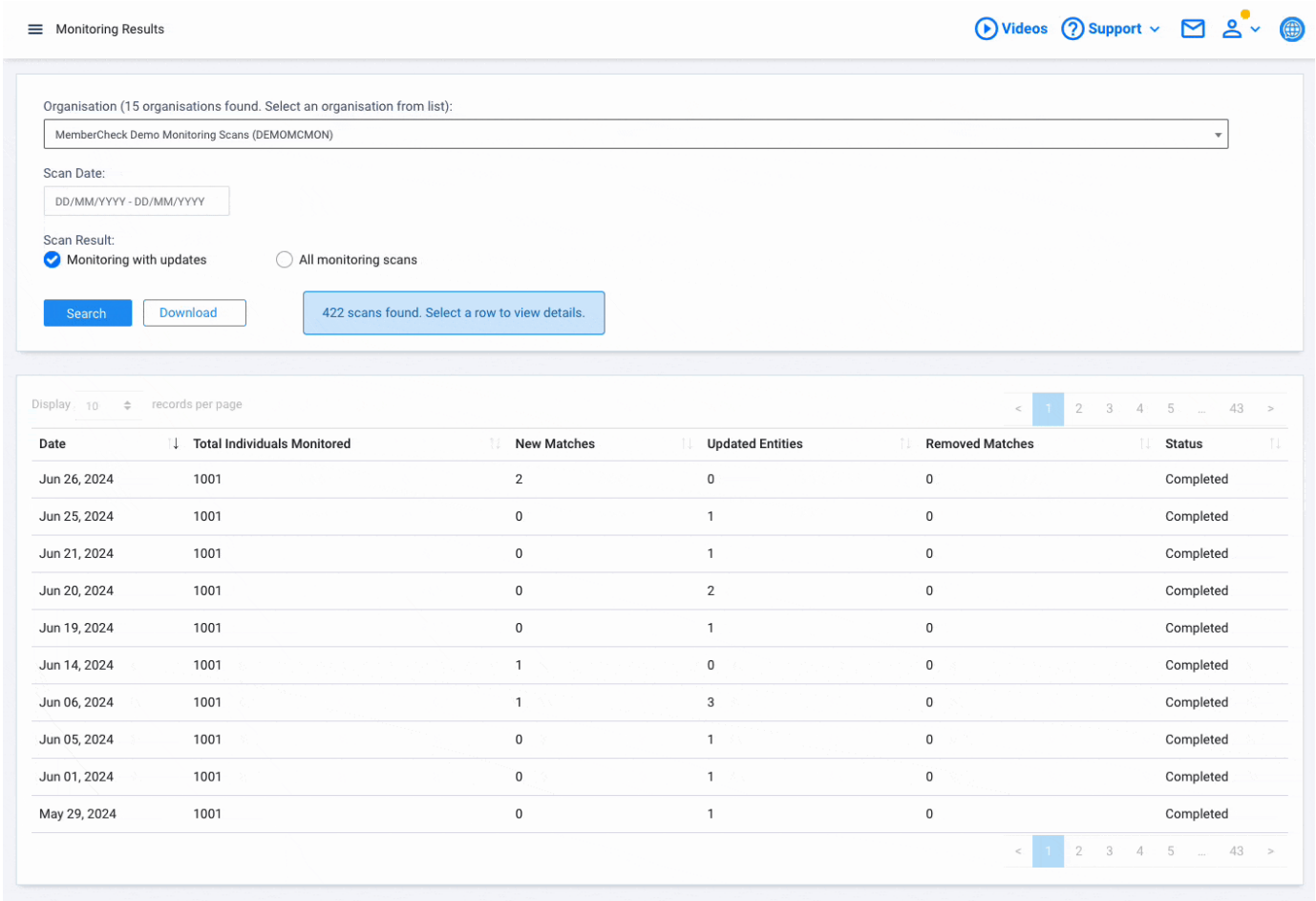
Monitoring for individuals and companies can be enabled or disabled by toggling the switch button in the Monitor column.



Individuals and companies enabled for monitoring will appear in the **Monitoring List**.

If you enable monitoring for an individual or company with an existing entry in the Monitoring List (same Client ID) you will be prompted to confirm replacement of the existing entry in the Monitoring List.

Viewing All Monitoring Scans or Updates only

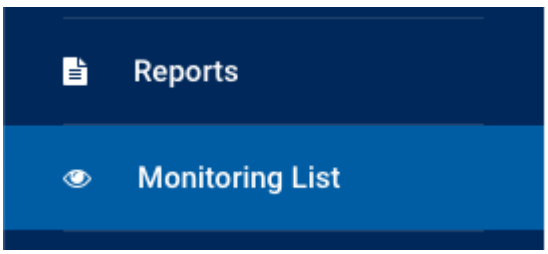


Monitoring List

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	✎	👁	✕	👁	👁

Monitoring List enables you to view, search and manage the monitoring of individuals and corporates ("entities").



Individuals and Corporates are listed separately in the **Monitoring List**. Select **List Type** to jump between views.

The following Individual details are available:

Field	Description
Checkbox	Ability to select one or more entities to enable monitoring, pause monitoring or remove from the Monitoring List entirely.
Monitor	Toggle switch to indicate if the associated individual is being actively monitored or not. Only active entities are monitored in the continuous monitoring and monitoring rescan processes. monitoring of the individual is active monitoring of the individual is paused

Client ID	Client ID (or Customer Reference or Client/Account ID or unique profile name) of scanned individual. Client IDs are unique.
First Name	First Name of scanned individual.
Middle Name	Middle Name of scanned individual.
Last Name	Last Name of scanned individual.
Original Script Name/Full Name	Original Script Name or Full Name of scanned individual.
DOB	Date of birth of scanned individual.
Address	Address of scanned individual.
Added By	Name of user who added the individual for monitoring.
Date Added	Date the individual was first added to the Monitoring List.

The following Corporate details are available:

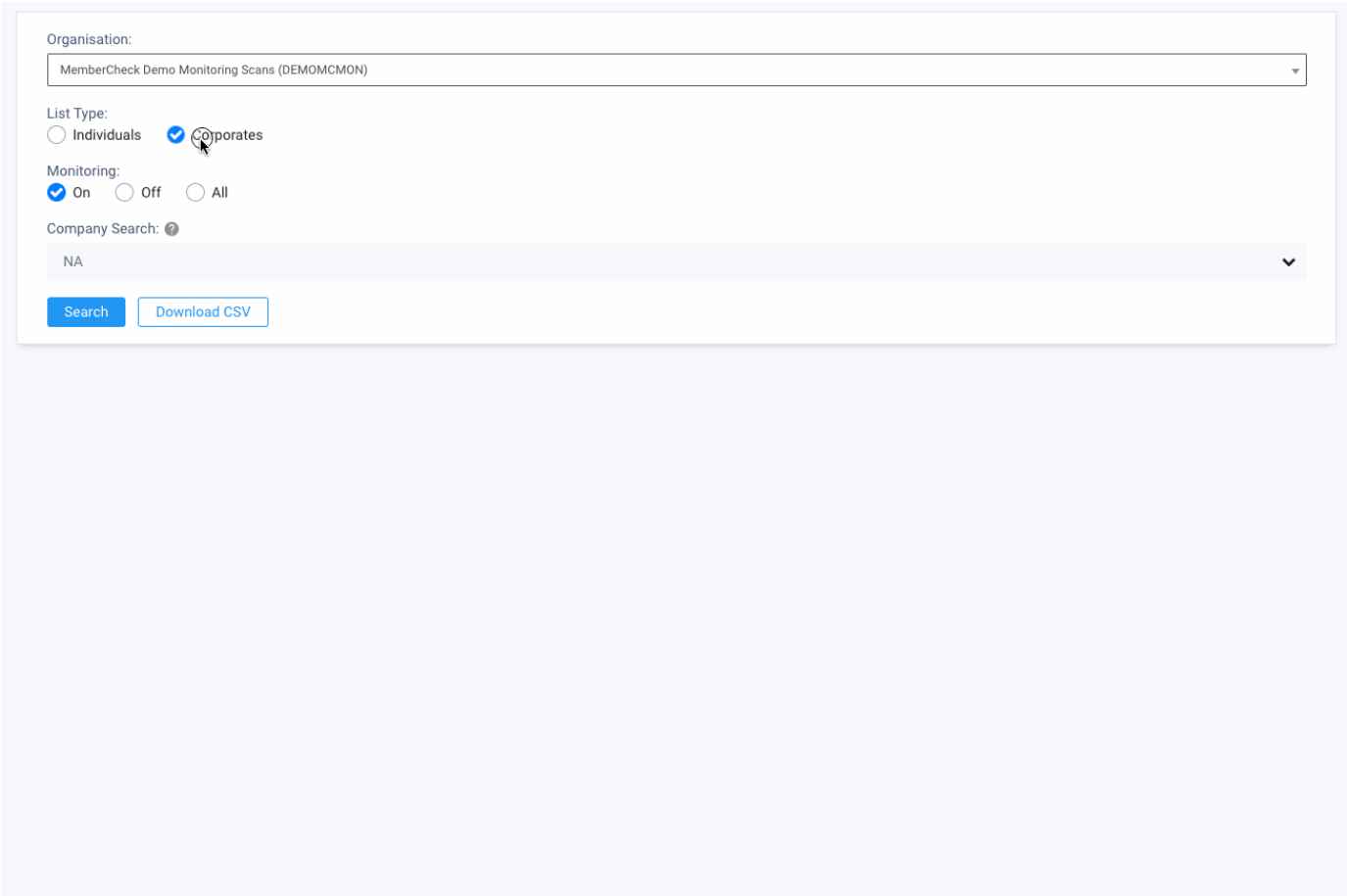
Field	Description
Checkbox	Ability to select one or more entities to enable monitoring, pause monitoring or remove from the Monitoring List entirely.
Monitor	Toggle switch to indicate if the associated entity is being actively monitored or not.  monitoring of the corporate entity is active monitoring of the corporate entity is paused
Client ID	Client ID (or Company Reference or Client/Account ID or profile name) of scanned corporate entity. Client IDs must be unique.
Company Name	Company Name of scanned corporate entity.
Registration Number	Company registration number, e.g ABN, ACN, NZBN, CRN, RN etc of scanned corporate entity.

Address	Address of scanned corporate entity.
Added By	Name of user who added the corporate entity for monitoring.
Date Added	Date the corporate entity was first added to the Monitoring List.

Quick How-To Guides

Switch between Individuals and Corporate Monitoring Lists

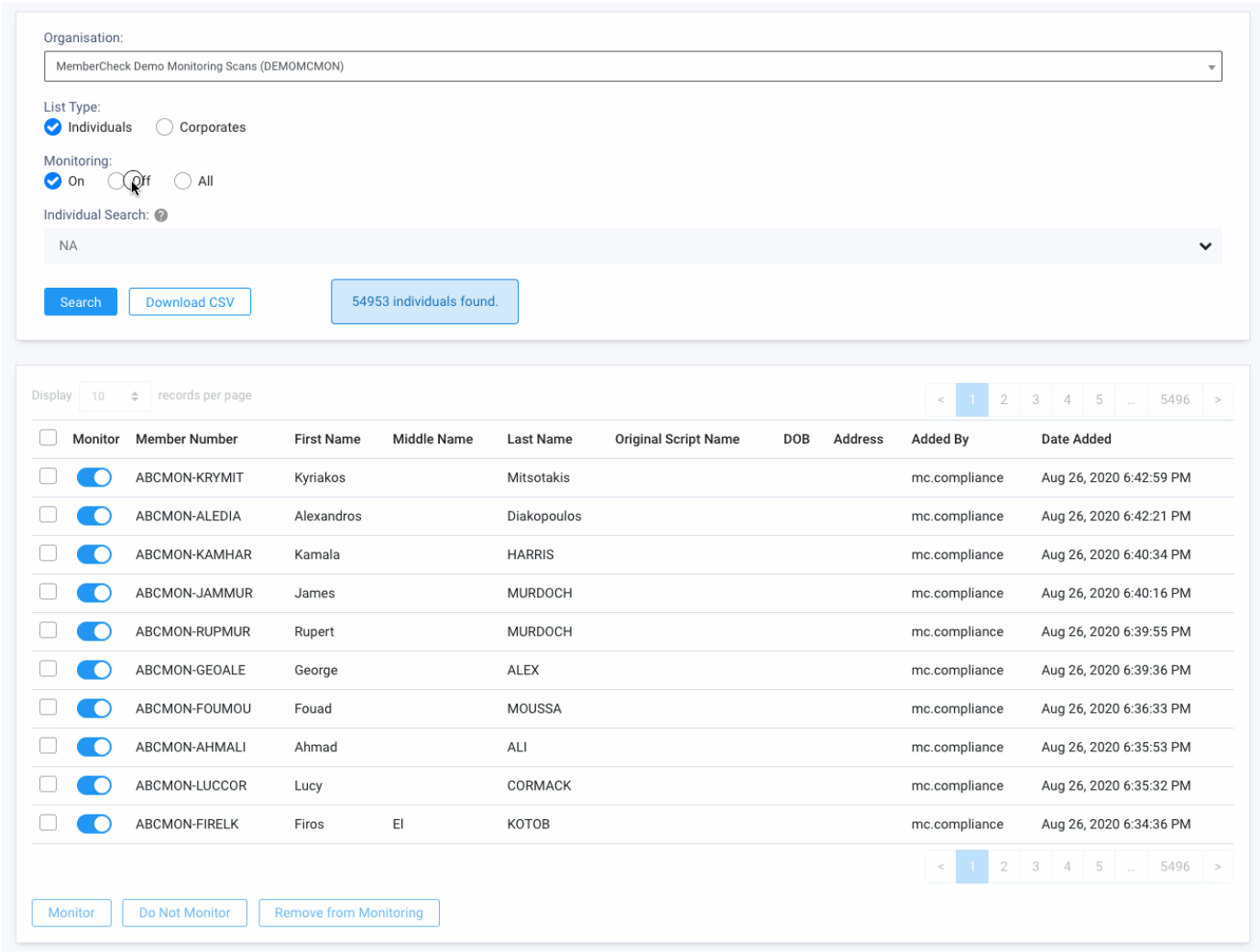
Individuals and Corporates are listed separately in the **Monitoring List**. Select **List Type** to jump between views.



View Active and Paused Monitoring of Individuals and Corporates

All entities enabled for ongoing monitoring are displayed in the **Monitoring List**. This list may include entities added to the Monitoring List but paused (`Off`) from being actively monitored

until a time when they are removed from the Monitoring List entirely, or re-enabled to resume monitoring (`On`).

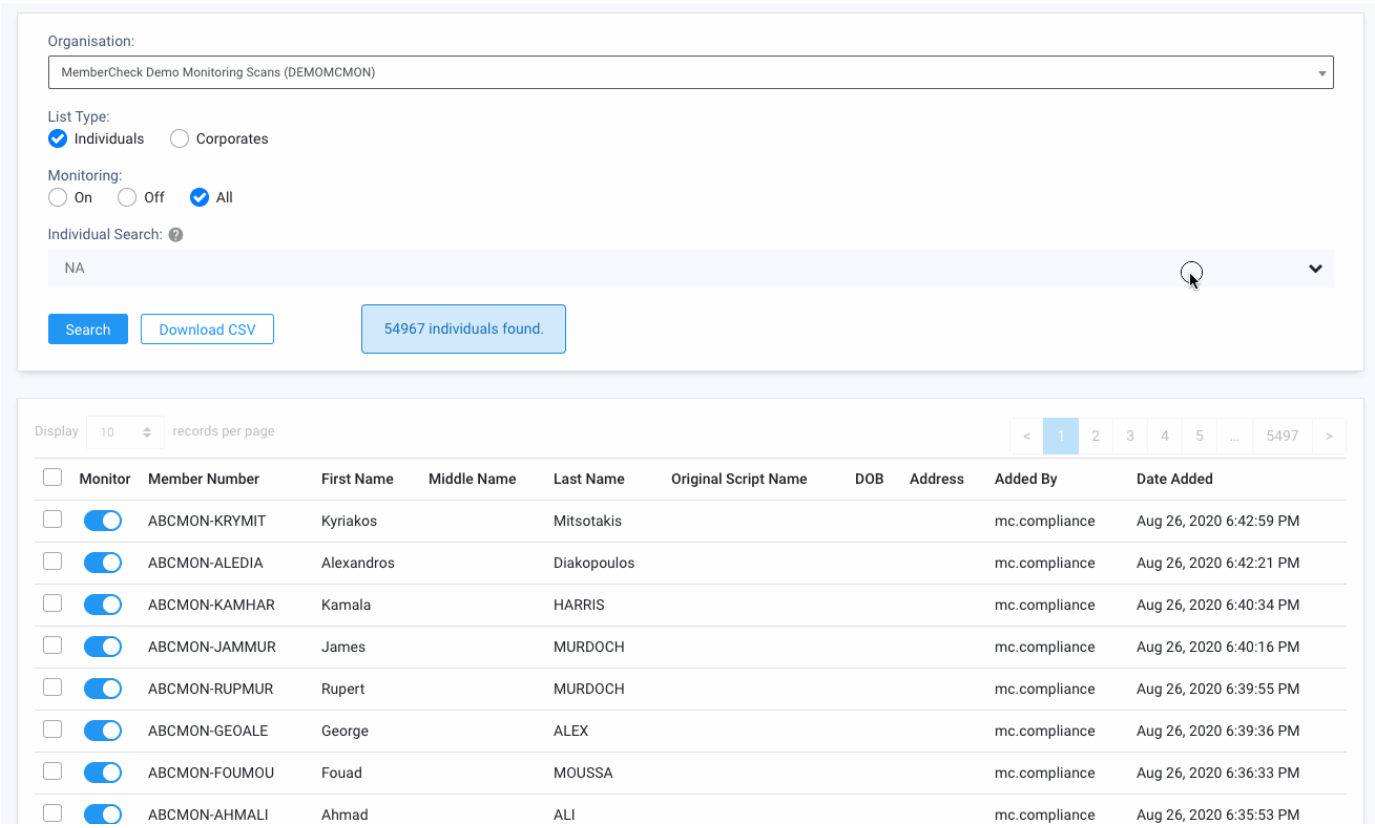


Automated annual rescans

All actively monitored entities in the Monitoring List are rescanned against the entire watchlist database (excluding custom watchlists) on the renewal date of your subscription. This does not include paused items.

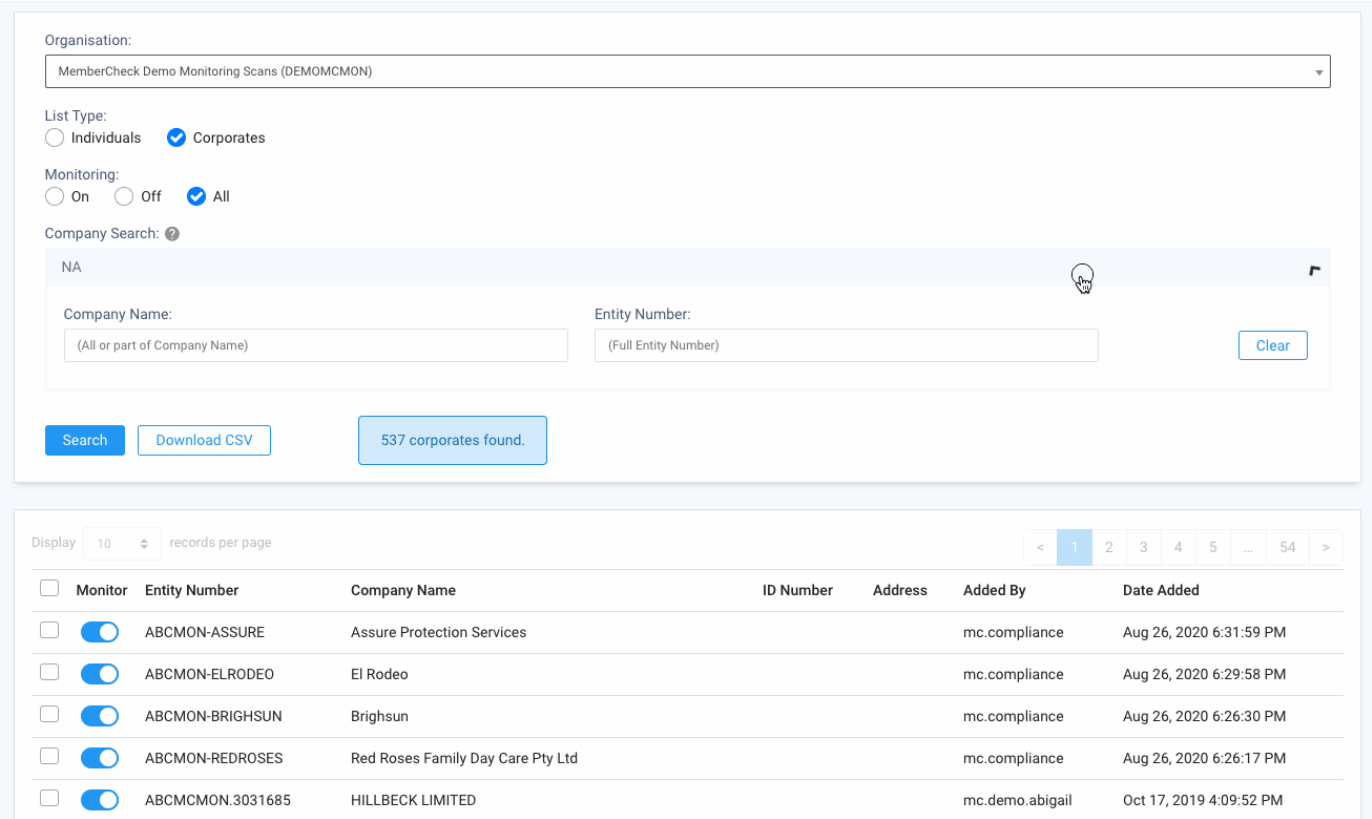
You have the option to remove all entities from the Monitoring List before your subscription expires. See Automatically clear Monitoring List on subscription renewal below for details.

Searching for a specific Individual

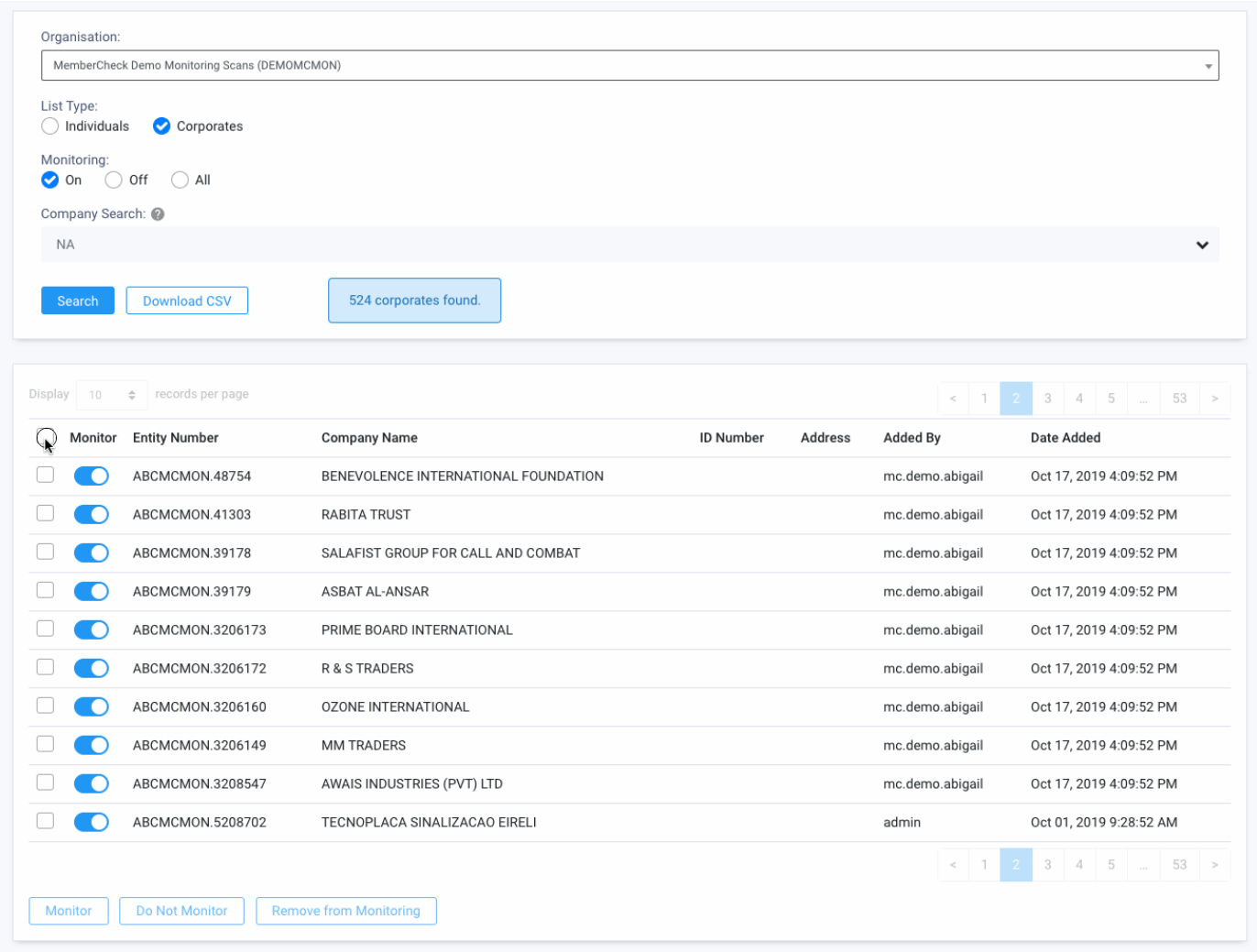


Monitor	Member Number	First Name	Middle Name	Last Name	Original Script Name	DOB	Address	Added By	Date Added
	ABCMON-KRYMIT	Kyriakos		Mitsotakis				mc.compliance	Aug 26, 2020 6:42:59 PM
	ABCMON-ALEDIA	Alexandros		Diakopoulos				mc.compliance	Aug 26, 2020 6:42:21 PM
	ABCMON-KAMHAR	Kamala		HARRIS				mc.compliance	Aug 26, 2020 6:40:34 PM
	ABCMON-JAMMUR	James		MURDOCH				mc.compliance	Aug 26, 2020 6:40:16 PM
	ABCMON-RUPMUR	Rupert		MURDOCH				mc.compliance	Aug 26, 2020 6:39:55 PM
	ABCMON-GEOALE	George		ALEX				mc.compliance	Aug 26, 2020 6:39:36 PM
	ABCMON-FOUMOU	Fouad		MOUSSA				mc.compliance	Aug 26, 2020 6:36:33 PM
	ABCMON-AHMALI	Ahmad		ALI				mc.compliance	Aug 26, 2020 6:35:53 PM

Searching for a specific Corporate



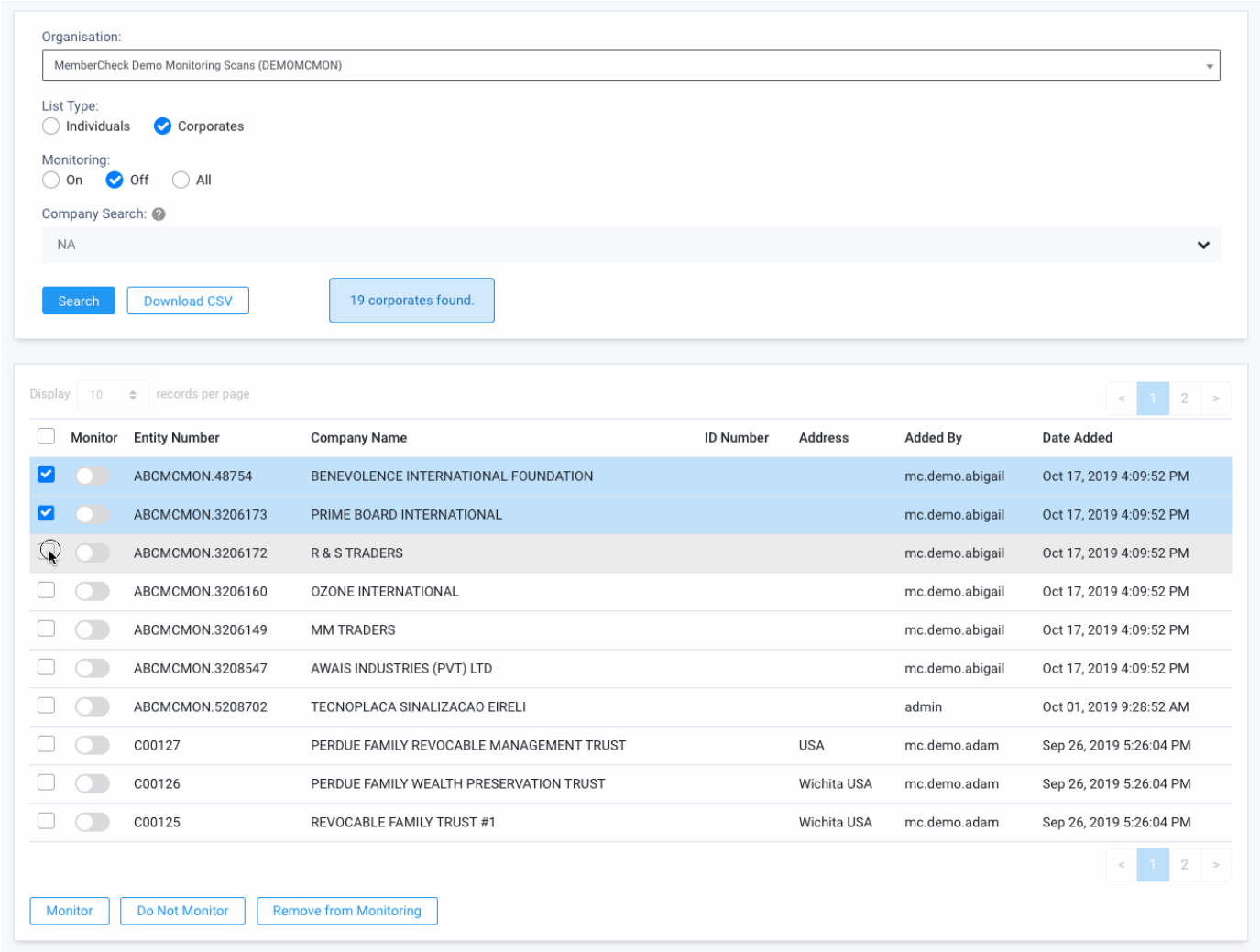
Pause Monitoring for Corporate (or Individual)



Remove Corporate (or Individual) from Monitoring List

Entities which can easily be toggled off to pause from monitoring. However if you do not want an entity to be monitored at all (e.g. due to changes in your organisation membership), you can remove an entity entirely from the Monitoring List. Entities which are both actively monitored or paused can be removed from the Monitoring List.

Removal of entities from the Monitoring List does not affect scan history of the entity. Additionally, removed entities can be added back to the Monitoring List from **Scan Results**.

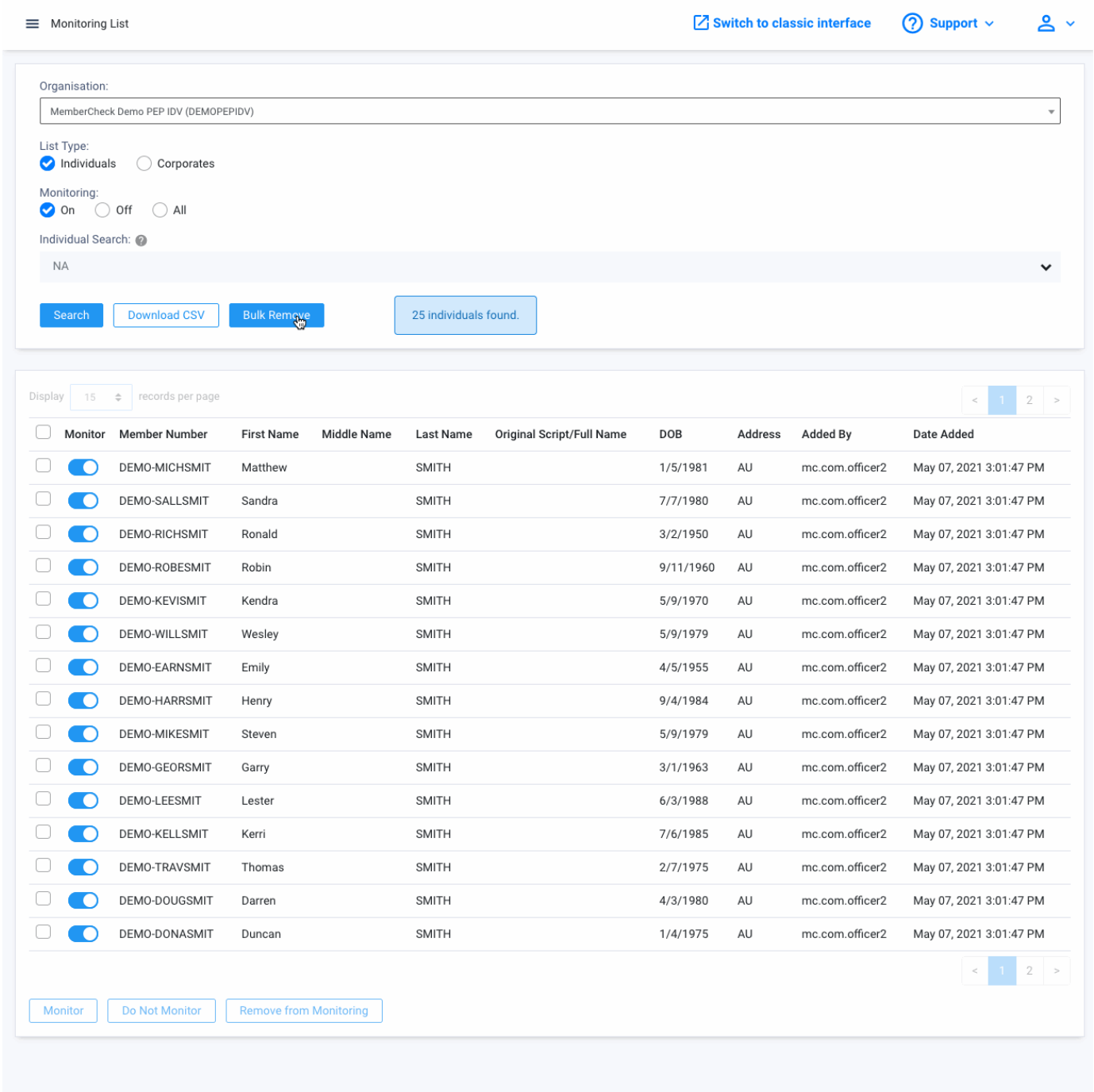


Bulk remove Individual (or Corporate) from Monitoring List

Multiple entities can be removed from being monitored in bulk (e.g. due to changes in your organisation membership).

Entities which are both actively monitored or paused can be removed from the Monitoring List using the **Bulk Remove** feature. Simply select the **List Type** and enter a list of Client IDs in the text box provided. A maximum of 10,000 entries can be removed at once within the text box.

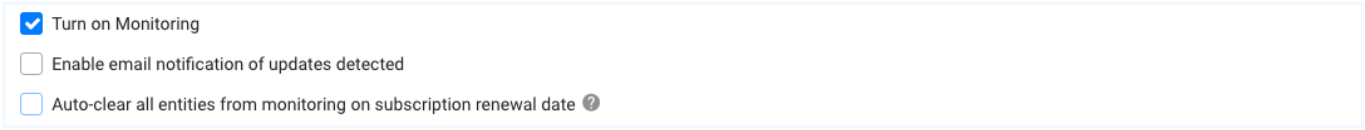
Removal of entities from the Monitoring List does not affect scan history of the entity. Additionally, removed entities can be added back to the Monitoring List from **Scan Results**.



Automatically clear Monitoring List on subscription renewal

Depending on your organisation requirements, you can clear the Monitoring List of ***all*** entities on renewal of your organisation subscription account. To do so, the **Compliance Officer** can select the option in **Administration > Organisations > Monitoring Settings** > `Auto-clear all entities from monitoring on subscription renewal date`.

Ongoing Monitoring:



Scan Results for Individuals

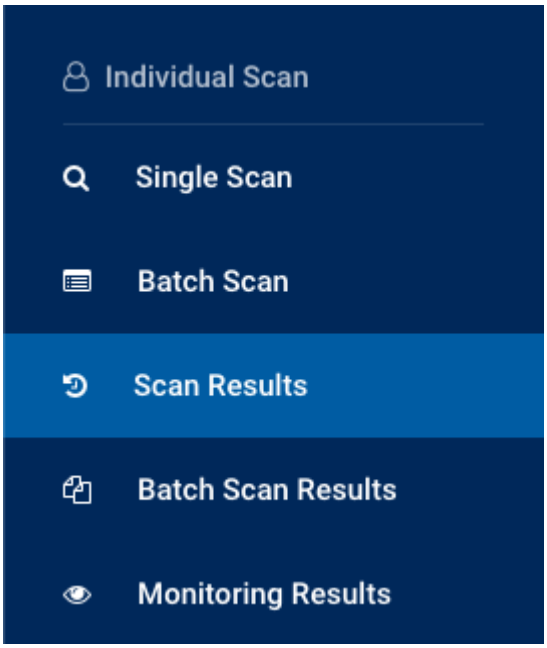
Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
👁	👁	👁	✕	👁	👁

Standard User Permissions

Whilst **Compliance Officers**, **Advanced Users** and **Auditors** have access to view scan results performed by all users associated with the organisation, **Standard Users** are able to only view scan results performed by themselves.

Individual Scan > Scan Results displays the match results for the individuals screened from both Single and Batch scans, and includes ID Verification scans, Monitoring scans and Monitoring Rescans, if available.



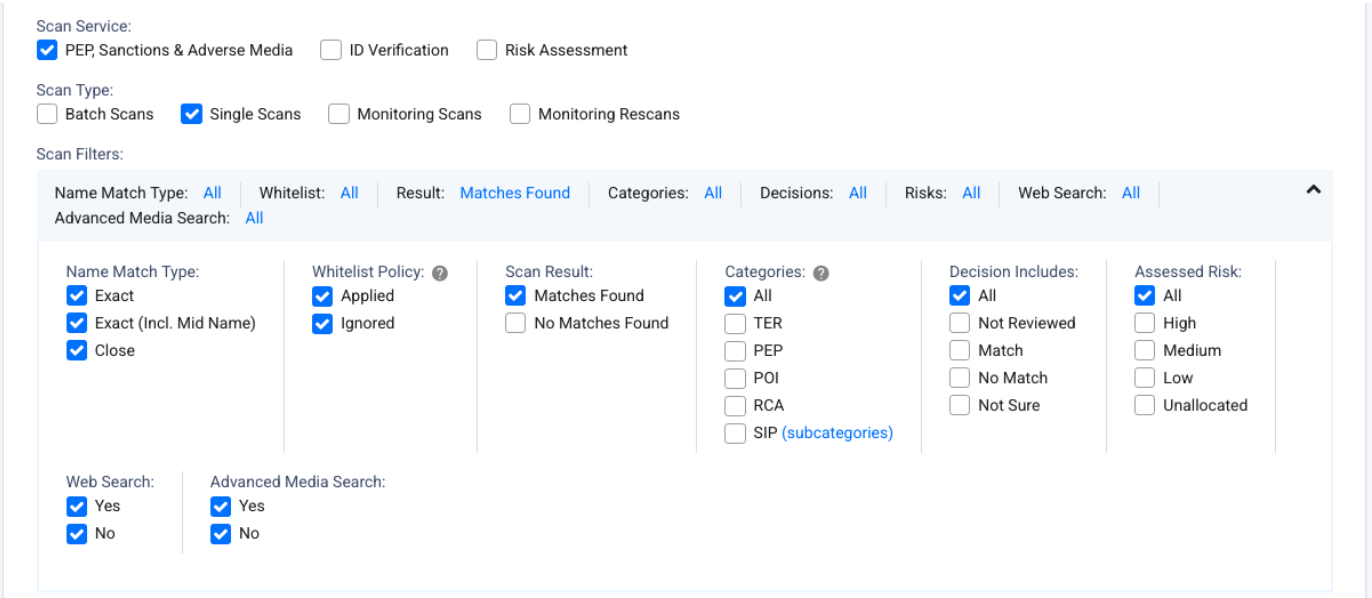
By default, it lists **Single Scan** results of **PEP & Sanctions** for **Matches Found** only. You can change the filters to expand or refine the scan results displayed using the options available for

Scan Date, **Scan Service**, **Scan Type**, **Scan Filters**, **Due Diligence Decisions** and **Individual Search** for a person or persons.

If you are part of a multi-level organisation or if you have multiple users associated with your organisation account, you can additionally filter by **Organisation** and **Users** who have performed the scans.

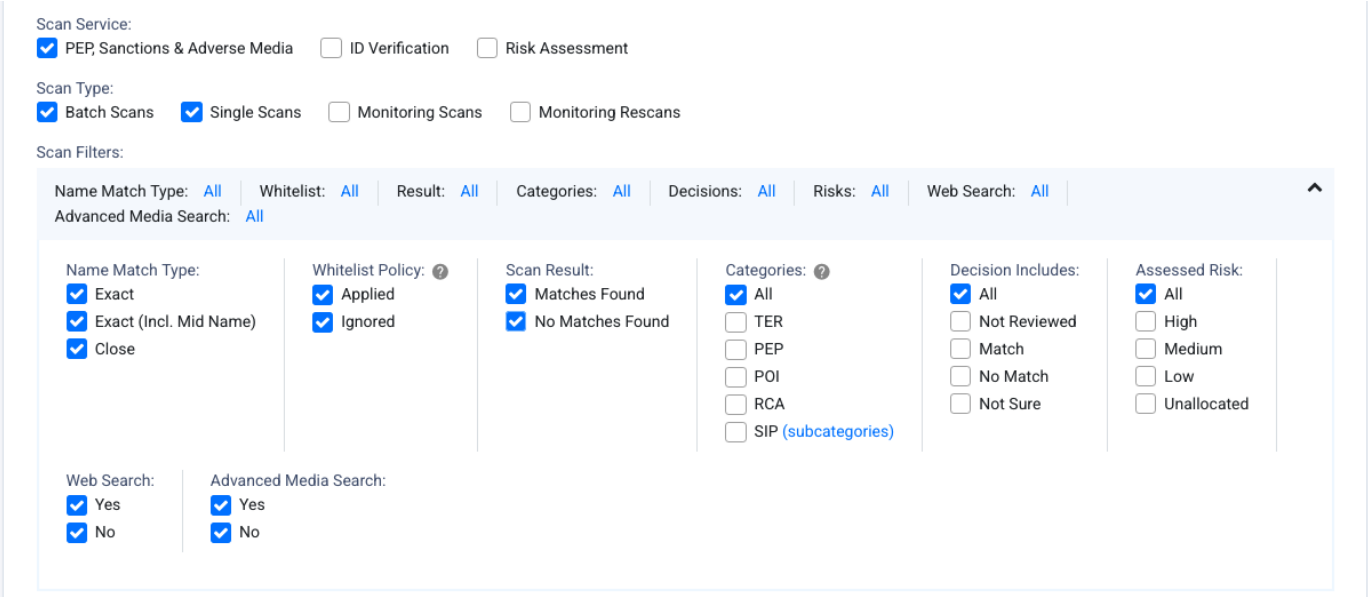
Scan Filters to filter by scan settings and results:

Default filter settings where scans with `No Matches Found` are excluded in **Scan Result**.



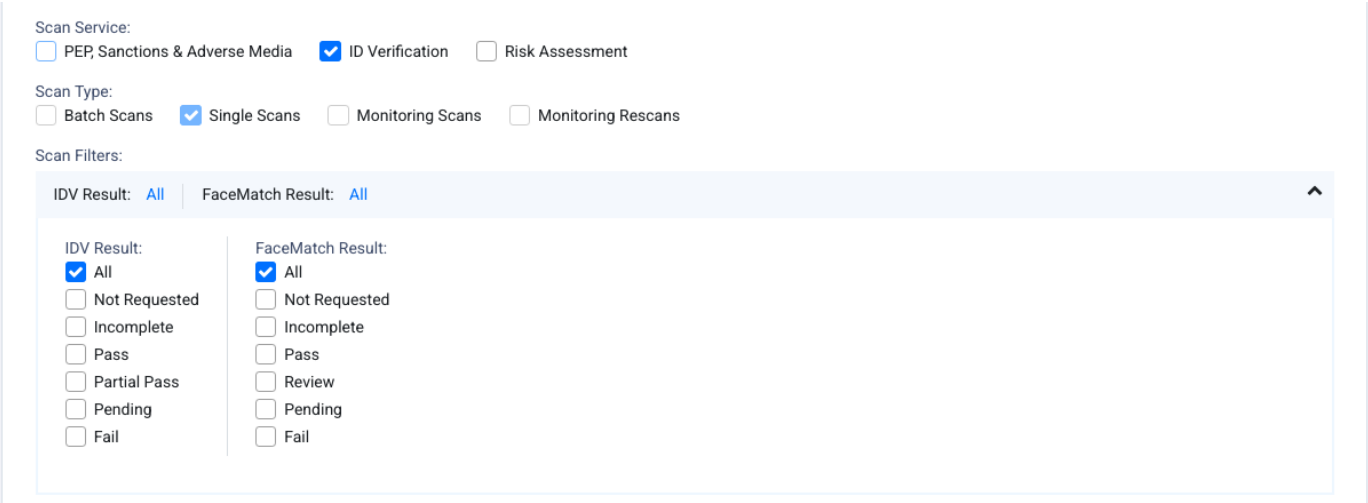
Scan Result Settings for all scans regardless of match results:

Note that both `Single Scans` and `Batch Scans` are selected. Both `Matches Found` and `No Matches Found` are selected.



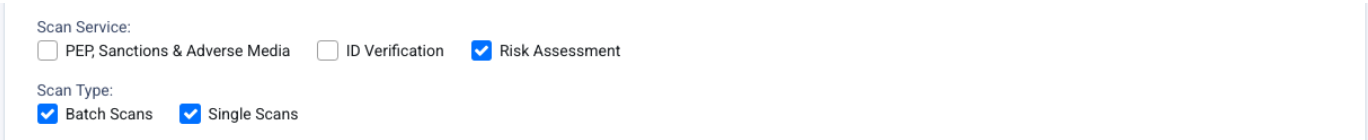
Scan Result Settings when ID Verification is selected:

Filter ID Verification scans based on the outcome of **IDV Result** (ID Check) and **FaceMatch Result** biometric screening.



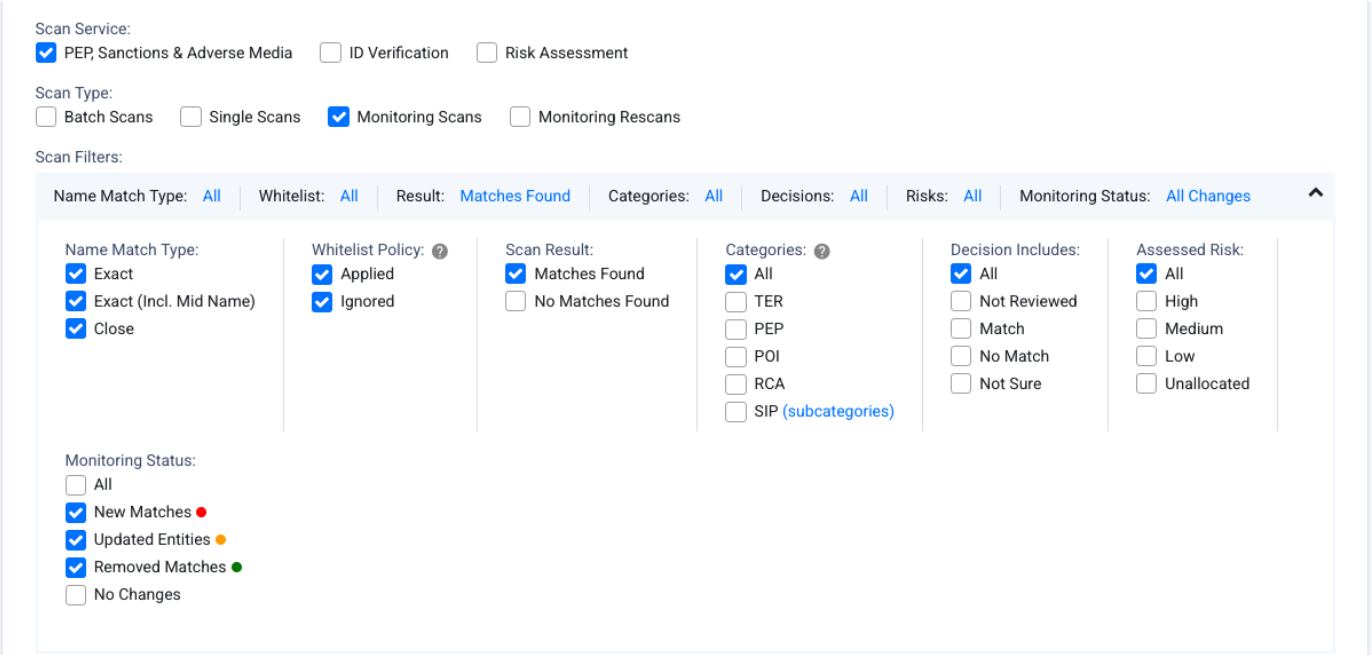
Scan Result Settings when AML Risk Assessment is selected:

Filter scans with Risk Assessment enabled during screening. This refers to the AML Risk Assessment questionnaire completed based on customer information, country, product or services offered and outcome of screening.



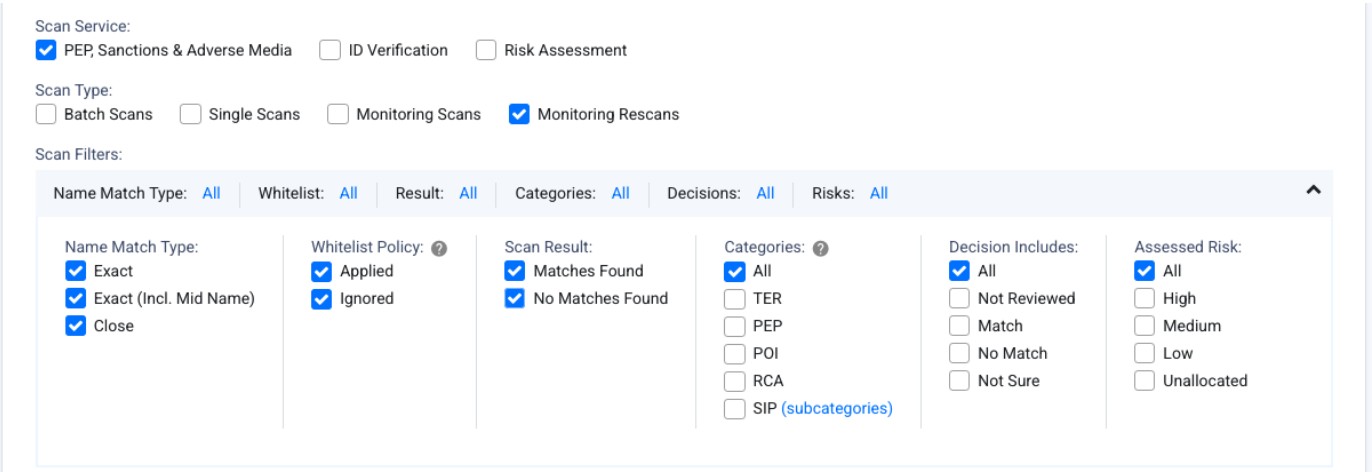
Scan Result Settings when Monitoring Scans is selected:

Filter scans based on the outcome of ongoing monitoring and type of detected change.



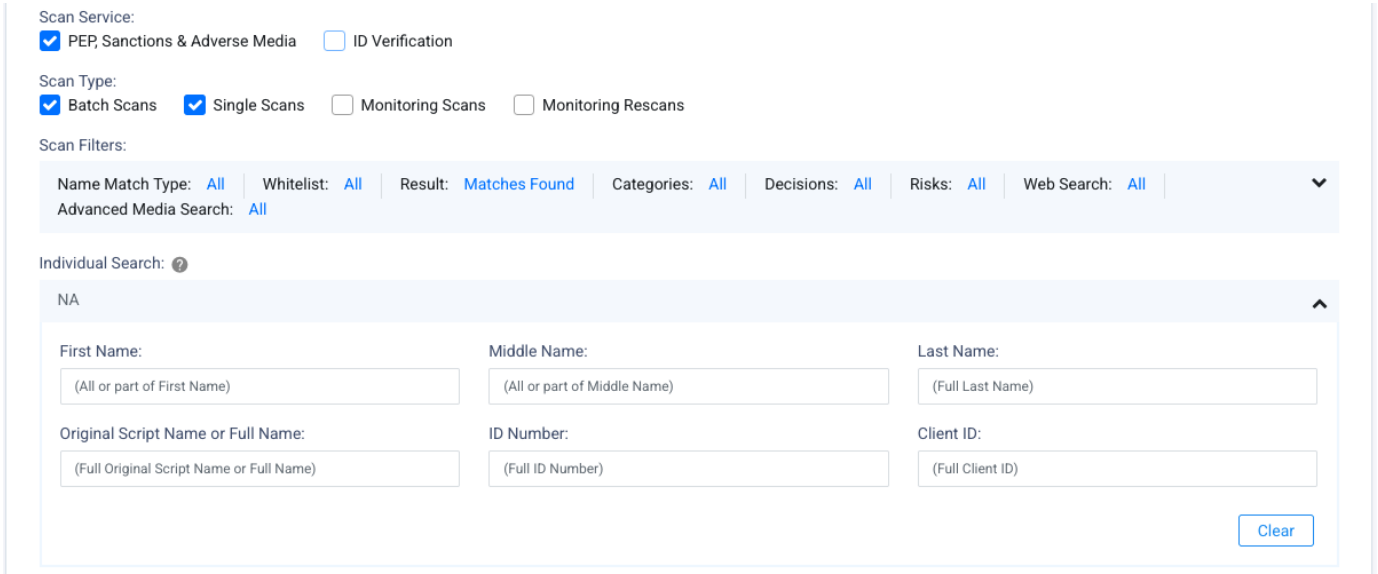
Scan Result Settings when Monitoring Rescans is selected:

Filter for rescans where actively monitored entities are rescanned against the full database on day of account subscription renewal.



Individual Search to filter by individuals scanned:

Expand the **Individual Search** panel to search for a specific individual in Batch and/or Single Scans.



Searching and Filtering Scan Results

Scan Result Settings:

Fields	Description
Name Match Type	Filter by name Match Type used during scans. The options are `Exact`, `Exact (Including Middle Name)` and `Close`. By default, all options are selected.
Whitelist Policy	Filter if whitelist policy was applied during the scan. Profiles marked as `No Match` are whitelisted and excluded from being returned and displayed again. The options are: `Apply` and `Ignore`. By default, all options are selected
Scan Result	Filter by the outcome of the scan. Options are `Matches Found` and `No Matches Found`. By default, `Matches Found` is selected.

Categories	Filter results by the major category type of the matching profile. The categories are: `TER` (Terrorism), `PEP` (Politically Exposed Person), `POI` (Profile of Interest), `RCA` (Relatives or Close Associates of PEP), `SIP` (Special Interest Person). SIPs have filters for additional subcategories such as `Sanctions Lists`, `Law Enforcement`, `Regulatory Enforcement`, `Organised Crime` etc. By default, `All` categories are selected.
Decision Includes	Filter results by due diligence decisions applied to the matching profile. The decisions available are: `Not Reviewed`, `Match`, `No Match` and `Not Sure`. By default, `All` decisions are selected.
Assessed Risk	Filter results by due diligence risk assessments applied to the matching profile. The assessed risk options are: `High`, `Medium`, `Low` and `Unallocated`. By default, `All` assessed risk levels are selected.
Web Search	Filter results where additional web search for adverse media was performed. The options are: `Yes` and `No`. By default, `All` options are selected.

Advanced Media Search	Filter results where additional advanced media search for latest news articles was performed. The options are: `Yes` and `No`. By default, `All` options are selected.

The full list of categories and subcategories are described in List Categories.

ID Verification Scan Result Settings:

Fields	Description
IDV Result	Filter by result of ID Verification. The options are `All`, `Not Requested`, `Incomplete`, `Pass`, `Partial Pass`, `Pending` and `Fail`. By default, the `All` option is selected.
FaceMatch Result	Filter by result of biometric face matching for ID Verification. The options are `All`, `Not Requested`, `Incomplete`, `Pass`, `Review`, `Pending` and `Fail`. By default, the `All` option is selected.

Individual Search:

For a quick and specific search of an individual screened, use the **Individual Search** panel.

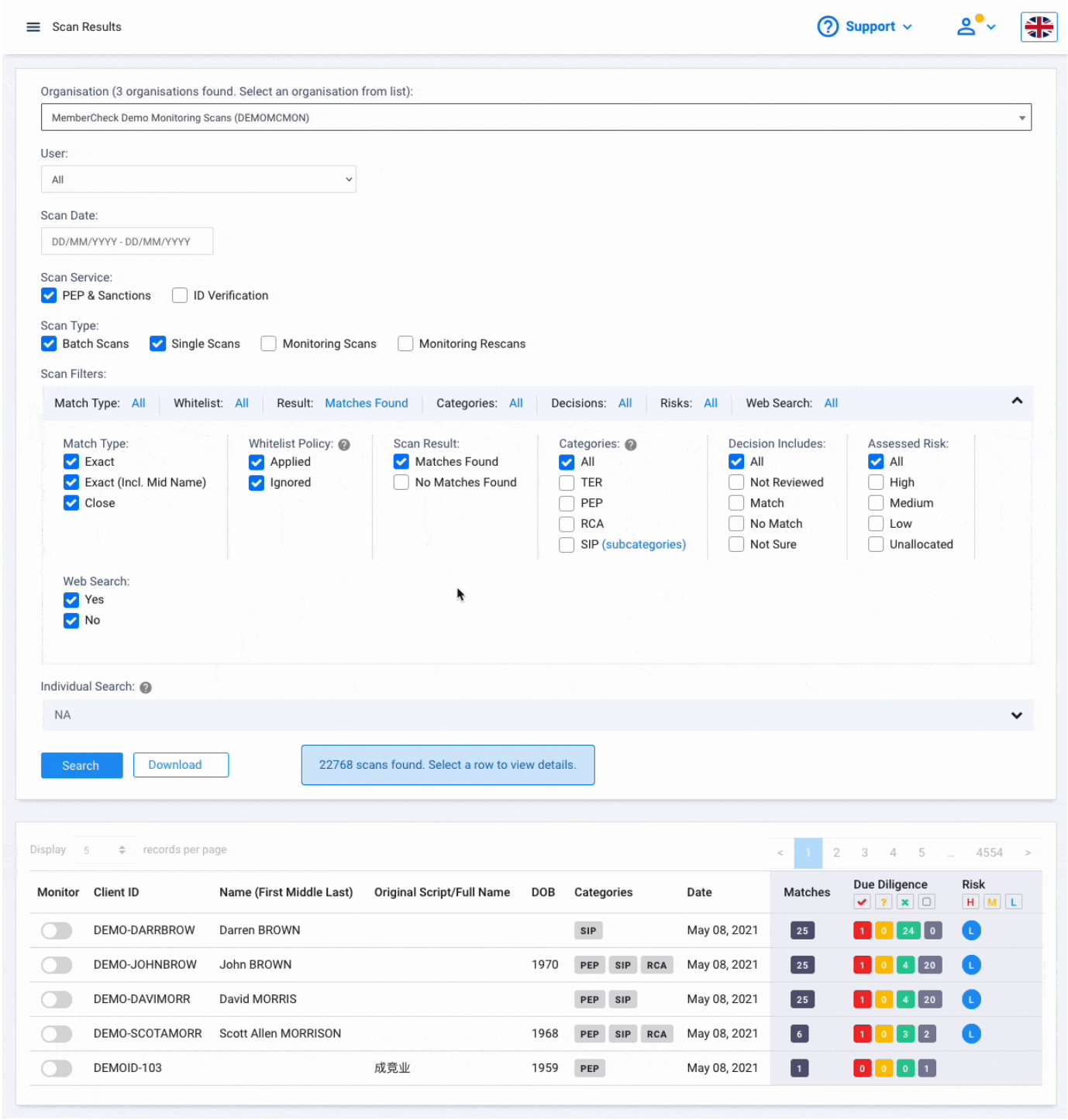
To search for fields where contents exist, use an asterisk (`*`).

Fields	Description

First Name	Search results by the First Name entered during scan. Search supports full or partial matching. Example: `Joh` returns `Joh`, `John`, `Johnny` etc.
Middle Name	Search results by the Middle Name entered during scan. Search supports full or partial matching.
Last Name	Search results by the Last Name entered during scan. Search supports full matching only.
Original Script Name or Full Name	Search results by the Original Script Name or Full Name entered during scan. Latin-based text are not case-sensitive and the exact full name in the correct order should be used. For original script text, it must be entered exactly as screened, including casing. Example: If you have screened with the **Full Name** `Renée DUMAS`, this can be found when filtering for `Renée Dumas` or `renée dumas` but not with `Renee Dumas.` or `Dumas Renée`
Client ID	Search results by Client ID entered during scan. Search supports exact full matching only.

Filtering scans by categories and subcategories:

Special Interest Persons (SIP) are further categorised into subcategories. See descriptions of the **SIP subcategories**.



Viewing Scan Results

Scan results of individuals screened are summarised as follows. Results are displayed in chronological order from most recent first.

The table below contains all possible columns. What is viewed on-screen is dependent on the **Scan Service** selected:

Field	Description
Monitor	If a **Client ID** has been assigned to the individual during scanning, a toggle switch to enable or disable monitoring is displayed.
Client ID	The unique identifier or profile name assigned to the individual during scanning.
Name (First Middle Last)	The name entered during screening, combining First, Middle and Last Name.
Original Script Name/Full Name	The non-Latin Original Script Name or Latin-based Full Name entered during screening.
DOB	Date of Birth or Year of Birth entered during screening.
ID Number	Identifier for the individual entered during screening.
Categories	Major categories of matched profiles. These can be one or any combination of the following: • `TER` : Special Interest Persons - exposure or associations with terrorist related activities. • `PEP` : Politically Exposed Persons • `POI` : Profiles of Interest • `RCA` : Relatives or Close Associates of PEPs. • `SIP` : Special Interest Person - People on Sanctions, Regulatory Enforcement, Law Enforcement lists, and Adverse Media sources. • A blank Category indicates that no matches were found.
Date	Date the scan was run.
Matches	Number of matching profiles for the scanned individual. `0` indicates no matches found.

Due Diligence	Number of due diligence decisions made against the matching profiles based on the decision types: Match Not Sure No Match Not Reviewed
Risk	Assessed risks assigned to matching profiles: High Medium Low
Comment	Remark or comment associated with the due diligence decision.
IDV+	Online ID verification status of individual's Name, DOB and Address against verified sources: • `Not Requested` : Identity document verification not requested • `Incomplete` : Identity document verification request not completed by a member of your organisation. Incomplete processes are not able to be resumed at this point in time. • `Pass` : Data is able to be fully verified • `Partial` : Data is able to be partially verified • `Fail` : Data is unable to be verified • `Pending` : Verification by the individual not yet started or incomplete.

FaceMatch[+]	Biometric face matching of the individual including liveness detection, facial recognition and data extraction using OCR (optical character recognition): • `Not Requested` : Facial matching verification not requested • `Incomplete` : Facial matching verification request not completed by a member of your organisation. Incomplete processes are not able to be resumed at this point in time. • `Pass` : Biometric is able to be fully verified • `Review` : Biometric is partially verified and should be reviewed • `Fail` : Biometric does not match and is unable to be verified • `Pending` : Biometric verification by the individual not yet complete.

[+] These are available if your organisation has subscribed to the **ID Verification** service and if the ID Verification Scan Service is selected.

Risk Assessment

If the AML Risk Assessment service was selected during screening, this tab will be displayed. If you have previously provided answers to the questionnaire, the overall results will be displayed. Else, a list of questions will be prompted to enable you to enter the information.

FATF Jurisdiction Risk

If the FATF Jurisdiction Risk option was selected during scan, you will see an additional tab containing information about the country associated with the matched profile, if available.

FATF Black List and Grey List

For countries that are identified in the FATF Black List and Grey List, these are tagged within the profile scan results, regardless of whether the Jurisdiction Risk option has been selected.

Web Search for adverse media

If the Web Search or Advanced Media Search options were selected for additional adverse media checks, you will see an additional tab with the media results.

For **Advanced Media Search**, the 30 most recent news articles from around the globe are returned with details of the title, publication date, source name, author, article readership and word count.

For **Web Search**, the first 10 most relevant results are displayed.

All links will open up to a new browser tab.

Compromised Information

If an email address was entered for the Individual during the PEP, sanction and adverse media check, you will see an additional tab with a list of sites with known data breaches for the email address.

Viewing Scan Result Details

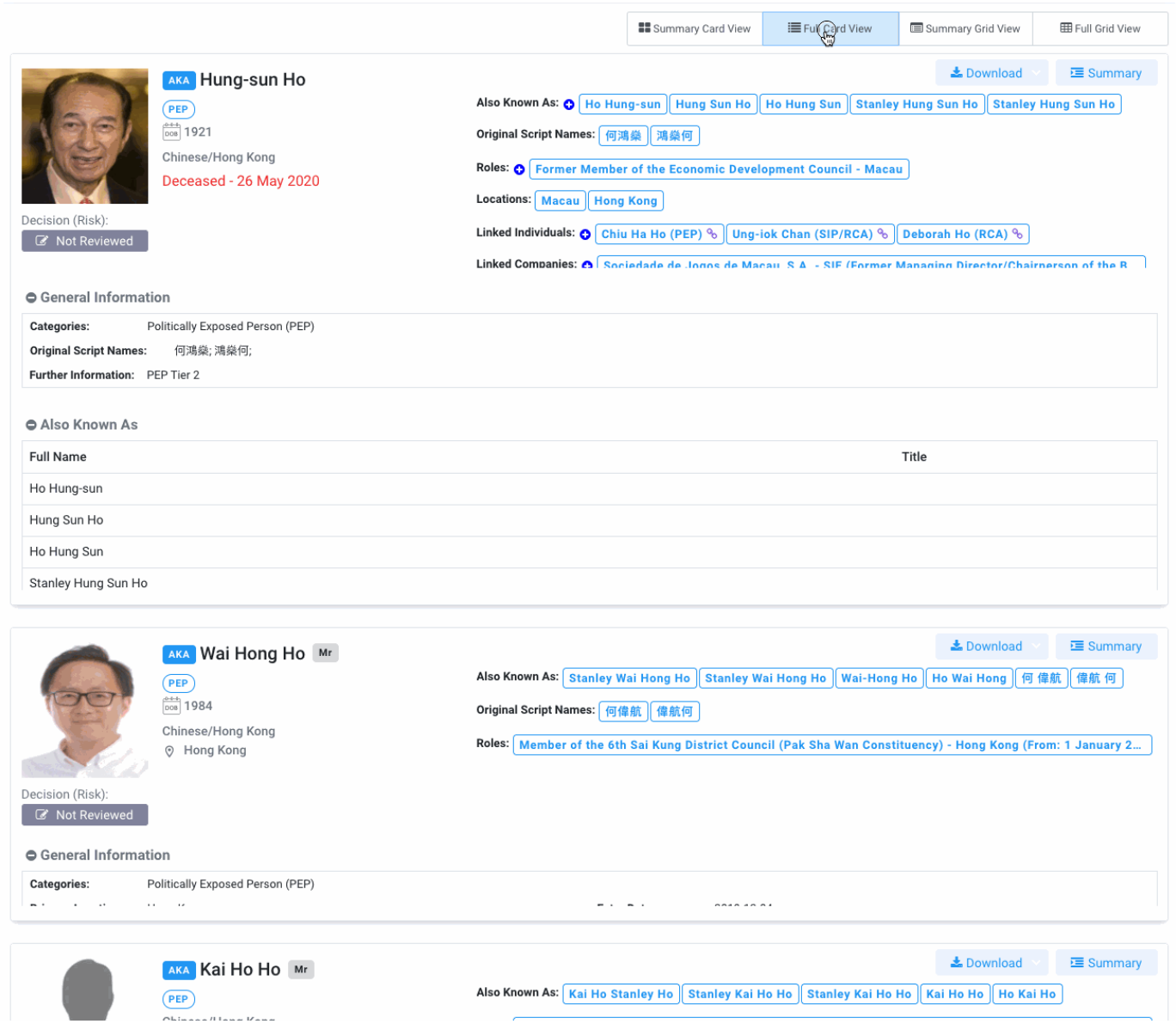
Matching profile information are displayed in **card** or **grid** format with either a **summary** or **full** detailed card view of the profile.

Click on a scan result record to view details of matching profiles:

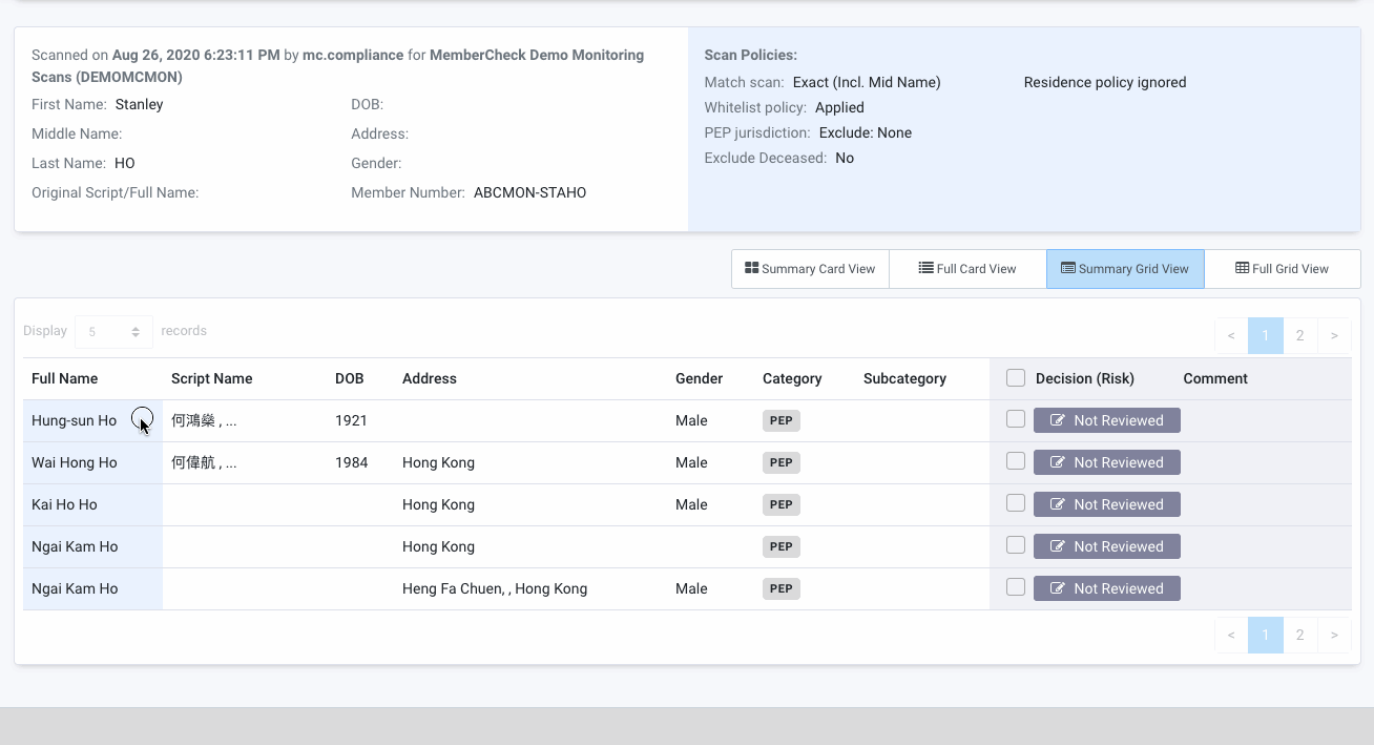
Card views provide a quick look into the matching profile with the high level summary with the options to expand to view details.

Grid views provide an additional table with summarised profile details with an overview and comparison of results. Where information in the profiles match with the scanned individual, cells are highlighted to indicate full match or partial match.

Card view



Grid view



Detailed information of profiles are displayed in the cards and may include:

Fields	Description
Profile Details	Key profile information: • Full Name • Category e.g. `PEP`, `POI`, `SIP`, `RCA`, `TER` • Date or Year of Birth • Nationality • Primary country or location • Deceased Date, if applicable • Due diligence decision and risk level assessment • `Tax haven` and `Sanction` indicators based on the primary country of residence.

General Information	• Categories of the profile e.g. `Politically Exposed Person (PEP)`, `Special Interest Person (SIP) - Regulatory Enforcement` • Original Script Name • The date the record was last reviewed or updated • Further information and profile notes PEPs are further categorised into tiers based on the level of risk exposure. See below for **description of PEP Tiers**.
Also Known As	• Name - aliases or other names associated with the individual • Type - type of name variation e.g. original script name, name spelling variation, shortened name, maiden name, nickname, previous name, fake name.
Roles	This is only available for PEP profiles: • Title - represents the job Role of the PEP in the particular PEP position • Country - represents the country of the government for the political position • Segment - the category of in scope positions for the PEP for a particular country • Status - represents whether the particular role is `Current` or `Former`. There can be more than one `Current` and `Former` roles held by the PEP. • From - represents the Start date of the term of office in the particular role, where available • To - represents the End date of the term of office in the particular role, where available.

Important Dates	For each Date: • Type - e.g. Date of Birth, Deceased Date • Date
Locations	All registered or known locations associated with the individual: • Country • City • Address • Type e.g. place of birth, residential, business, previous residential, previous business
Official Lists	Name of Sanction List this profile appears in. • Name - name of the official Sanctions list e.g. Office of Foreign Asset Control • Category - category of the official list • Measures - list of measures enforced by the official list e.g. asset freeze, travel ban • Origin - country or region of the official list • Type - type of sanction classified by the official list • Status - status of the entity on the official list i.e. `current` or `former`.

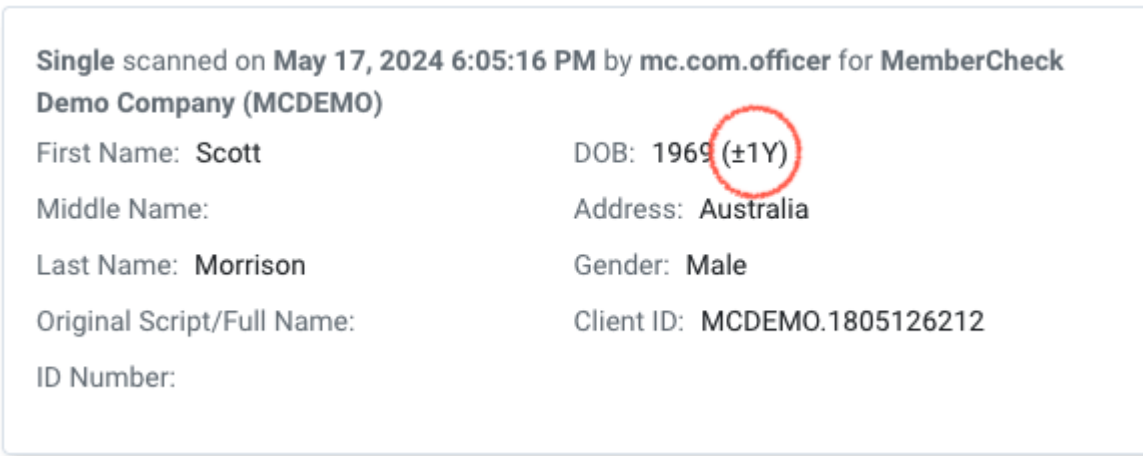
Identifiers	List of ID numbers or tax number of the individual. • Type - type of identifier e.g. tax number, national ID, passport number, OFAC unique ID, SECO unique ID • Value
Sources and Adverse Media	For each Source: • URL - link to the source of information regarding the entity • Category - category type of source e.g. `PEP`, `Sanction`, `Adverse Media`, `Law Enforcement`, `ID/V` (ID Verification) • Date of Capture - date the source article was recorded. This may contain multiple dates where the source was reviewed and recorded. • Info - additional information on the publication e.g. publication date, credibility, language of the article, title and summary, if available

 Links to news articles may be out of date or broken depending on how recently they have been reviewed. Some source articles contain cached PDF copies.
If the cached PDF is available, this is provided as a hyperlink in **Date of Capture** . For copyrighted sources which may not be accessible, you can check for availability of the copyright material. If available, the data of capture will change to a hyperlink to download the PDF. Availability of cached materials and copyright PDFs are dependent on your data source subscription.

Linked Individuals	List of persons associated with the organisation. • Full Name • Category e.g. `PEP` , `RCA` • Description Click on the name of a **Linked Individual** to view further information of the person.
Linked Companies	Lists any associations with businesses and companies such as founder, executive, associate, shareholder, adviser of the company. • Name • Categories e.g. `SIE` • Description Click on a **Linked Company** to view further information of the company.

Date of Birth variations

Where a scan was performed with a date of birth tolerance applied, this will be indicated in the summary of the scan as well as within the result reports:



Where a record was found due to the tolerance in DOB and is not the exact DOB or YOB, an indicator will be displayed next to the Date of Birth information of the profile:

Something amiss with the profile data?

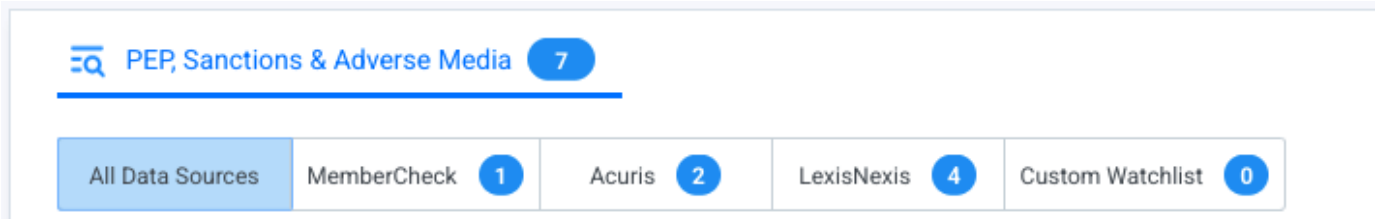
If the information in the existing profile data appears to be outdated, incomplete or unclear as to reasons for being listed in the watchlist, you can report this profile directly to the MemberCheck team for review. See tip on how to **report profile for review**.

Profile Categories

Refer to List Categories for a full list of the definitions of the main categories and subcategories.

Data Source of Profile

The service provides access to multiple database sources to ensure broader coverage for clients requiring additional information. If your organisation has subscribed to multiple PEP and sanctions data sources, the profiles will display the source of the data. You can filter these by selecting specific segment names.



Viewing Profile Risk Levels

Where an organisation has configured its Risk Settings, the recommended risk levels will be displayed for PEP & Sanctions profile matches. The risk levels are based on the current organisation settings.

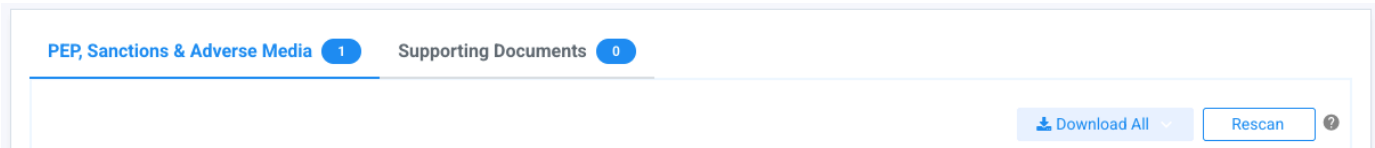
To view the risk levels of linked Individuals and Companies to the matched profile, click the **Calculate Risk Levels** button next to these sections. The results are retrieved based on the latest organisation risk settings and are not persistent in the scan history.

Rescanning an Individual

A **Rescan** feature is available for individuals previously scanned for PEP, Sanctions and Adverse Media, and applies for scans that resulted in matches and no matches. This feature allows for a new scan to be performed without the need to re-enter the individual's details, enabling you to check for the latest updates.

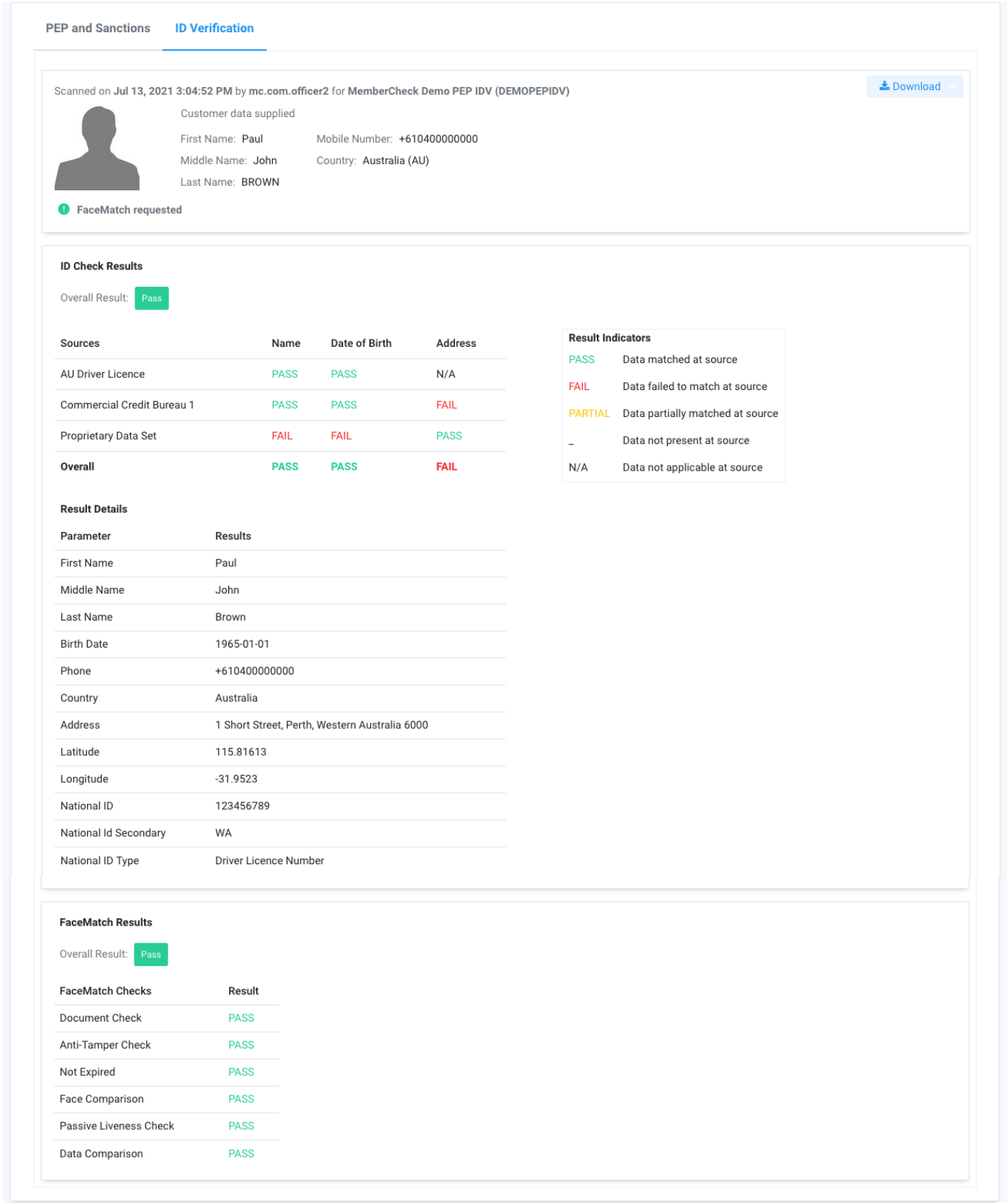
Initiating a rescan will commence a new scan using the individual's existing details. The previous scan policies and settings will be applied during this process, with the exception of the watchlists, which will be determined by the organisation's current list access scope.

Rescan activities count toward the organisation's scan activity and usage.



ID Verification

If ID Verification was included in the screening, additional information will be displayed for the individual scanned.



Detailed information of individual's data and biometric matching results vary between country sources used for verification and generally includes:

Fields	Description

ID Check Results	Overall data matching result based on successful verification against 2 or more independent sources. Includes list of sources used for data matching of individual's Name, Date of Birth and Address.
Identity Check Verification Results	Details entered by the individual or customer for verification including document type for verification e.g. Passport number, Driver Licence number, Government or Tax ID number, Health Card number, Visa number, Vehicle Plate number, Voter ID number etc. These document verification types vary based on country selected for verification.
FaceMatch Check Results	Verification results of biometric matching including: • Document check • Anti-Tamper check • Verification document not expired • Face comparison • Passive liveness check • Data comparison • Screen Replay attack check
FaceMatch Comparison	Photos of documentation used for verification including a liveness video, where available.

A **Verification URL** is available for IDV requests which enables you to access the link to the actual verification process. This URL is available for new or recent IDV requests as part of the MemberCheck service upgrade.

To keep a copy of the report of the results, you can click on the **Download** button to save as PDF, Word or Excel. Please note that the ability to enlarge photos and viewing of the Liveness video is only available online and is not included in the downloadable report.

Downloading Reports

For record keeping and for purposes of auditing for your organisation, you can download reports of your screening activities and the associated results in PDF, Word, Excel and CSV formats. Where large volumes of data are downloadable, the application may only offer download in CSV format.

This option is available through the **Download** button in all screens where download of reports are available.

In the **Scan Results** screen, the Download button offers the ability to:

- Preview PDF report before download
- Export as PDF
- Export as Word
- Export as Excel
- Export as CSV
- Export Results Summary report.

The **Download All** button enables you to download a report of all profile matches for a screened entity. The consolidated report contains an extract of the key details of the profiles such as the applied scan settings and policies, name, date of birth, address, gender, due diligence decisions, and the category and subcategory of the profile record.

The **Results Summary report** option enables you to download a summary of all the profiles of matched results for your PEP and Sanction screening, and is available in both the **Scan Results** and **Batch Scan Results** screens. This report is available in CSV format only and is compressed and downloaded as a ZIP file. The ZIP file is secured and password protected using the email address of the person who generated this report. If you have initiated the download of this report, the password to the ZIP file will be your registered email address in the application and entered as lower case. To check which email address you have registered in the system, you can review the information in **My Profile**.

Email Address to unlock Results Summary Report

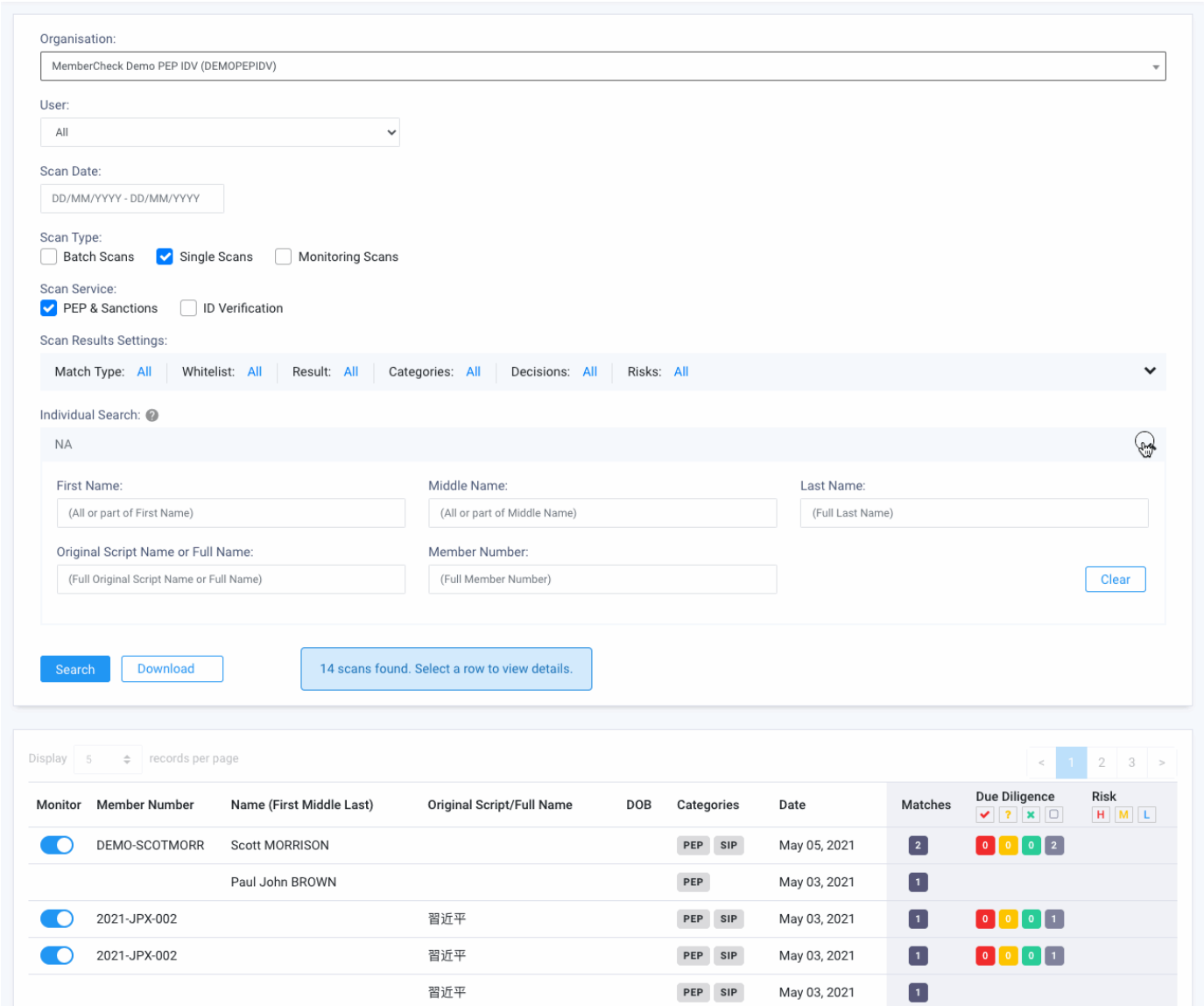
If the email address has different casing such as `UserName@domain-name.com` then the password to unlock the ZIP file will be `username@domain-name.com`

Availability of reports during trials and demos

If you are trialling the service on a demo environment, only the PDF and CSV options are available.

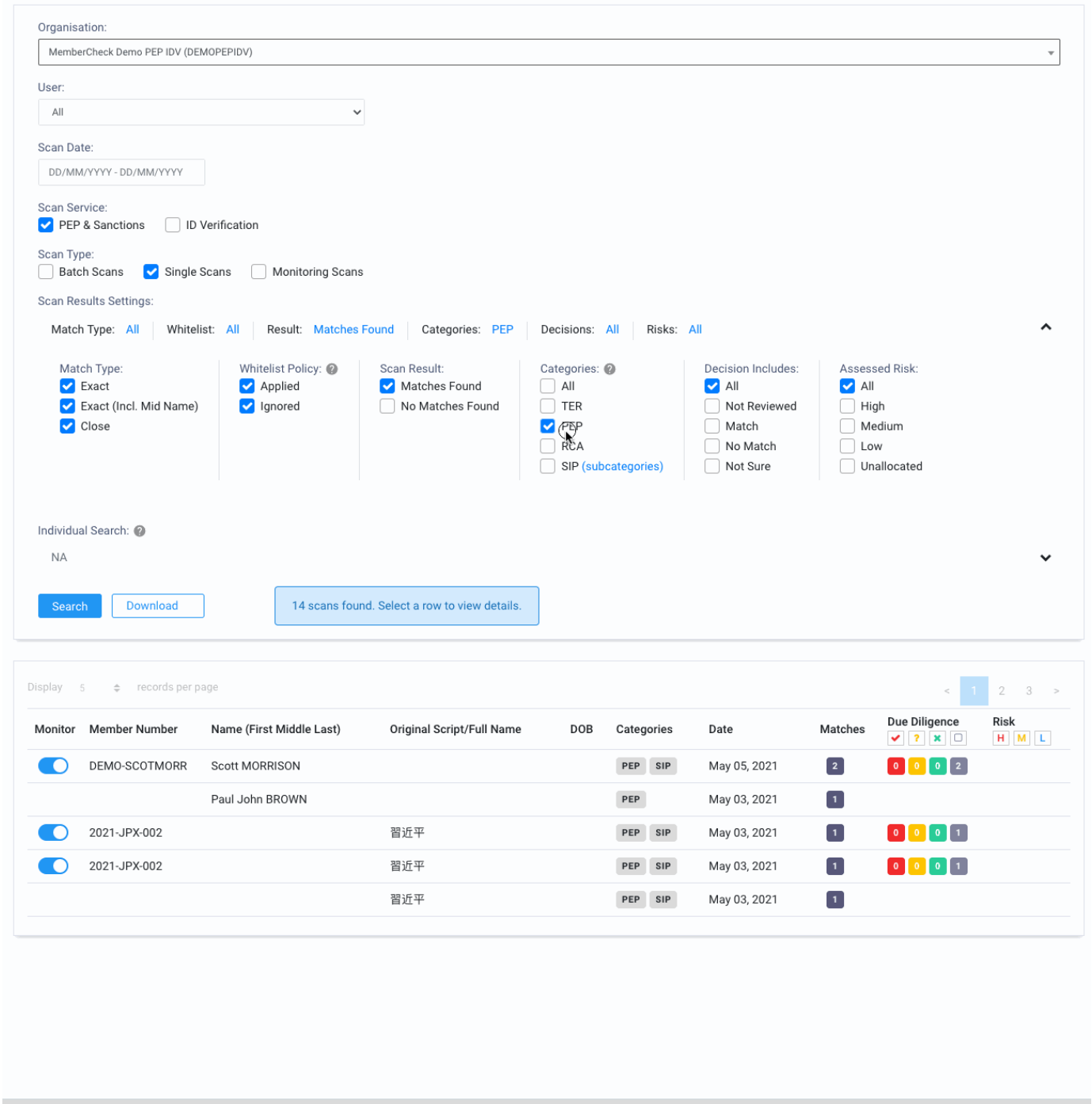
Quick How-To Guides

Filtering for all results with Original Script Name or Full Name

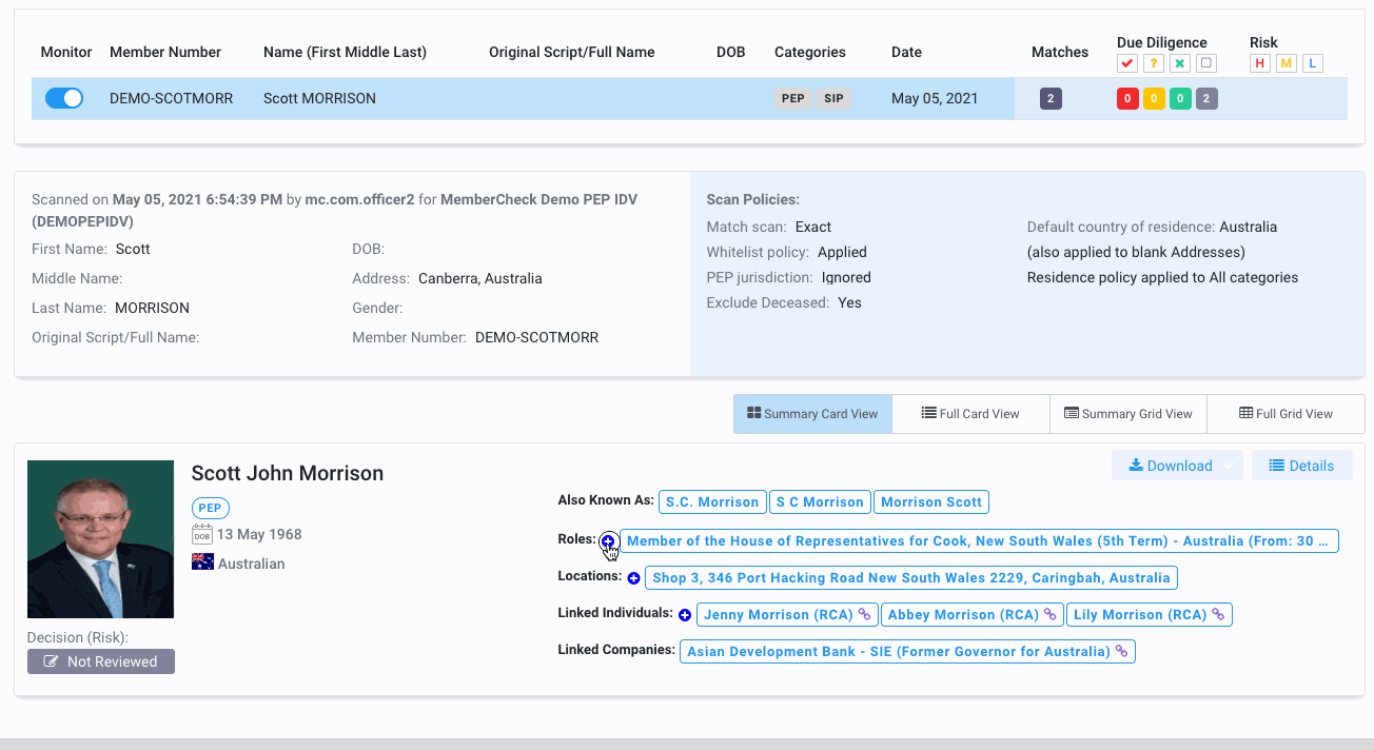


Filtering results by Category

The Category filter only displays the matching profiles with the same category. It does not affect the overall number of matches in the scan result summary.

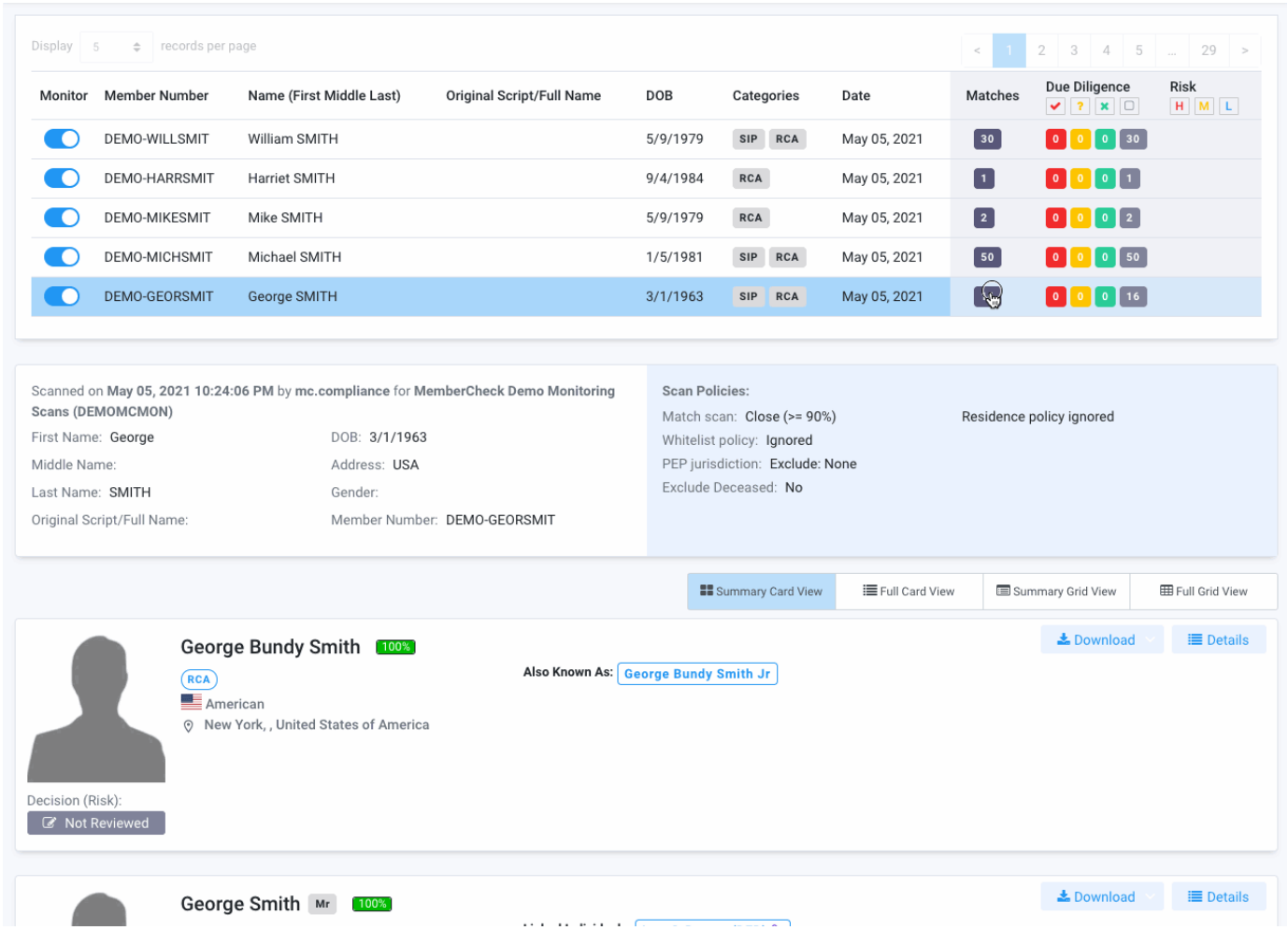


Viewing profile information in card summary mode



Card and Grid views

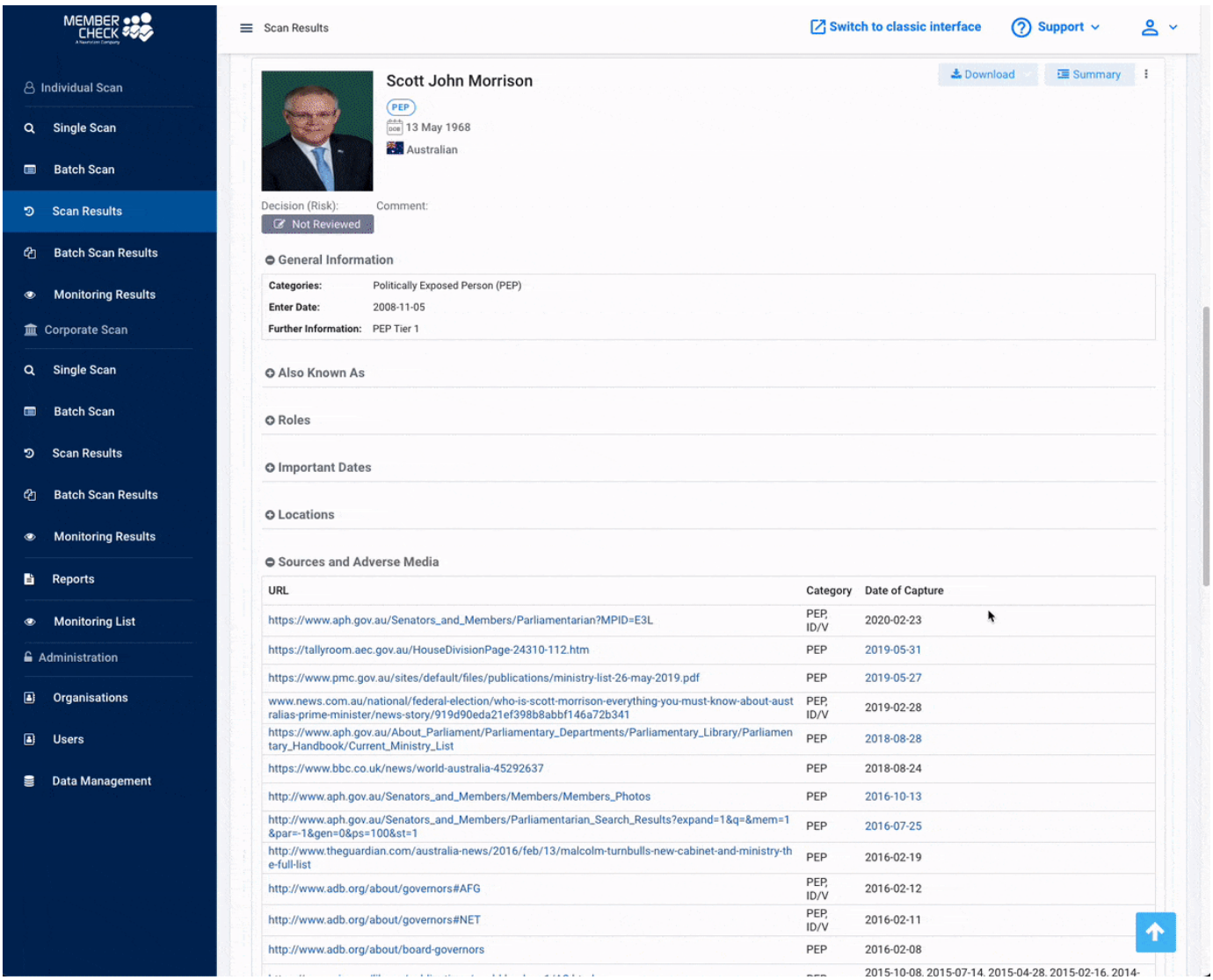
The card view is useful for quick access to the matching profiles to view details, however for larger number of matching profiles, the grid view provides an overview of the key information of the matching profiles. The grid view also provides the option to perform due diligence risk assessment in bulk.



Viewing Cached Sources and Adverse Media

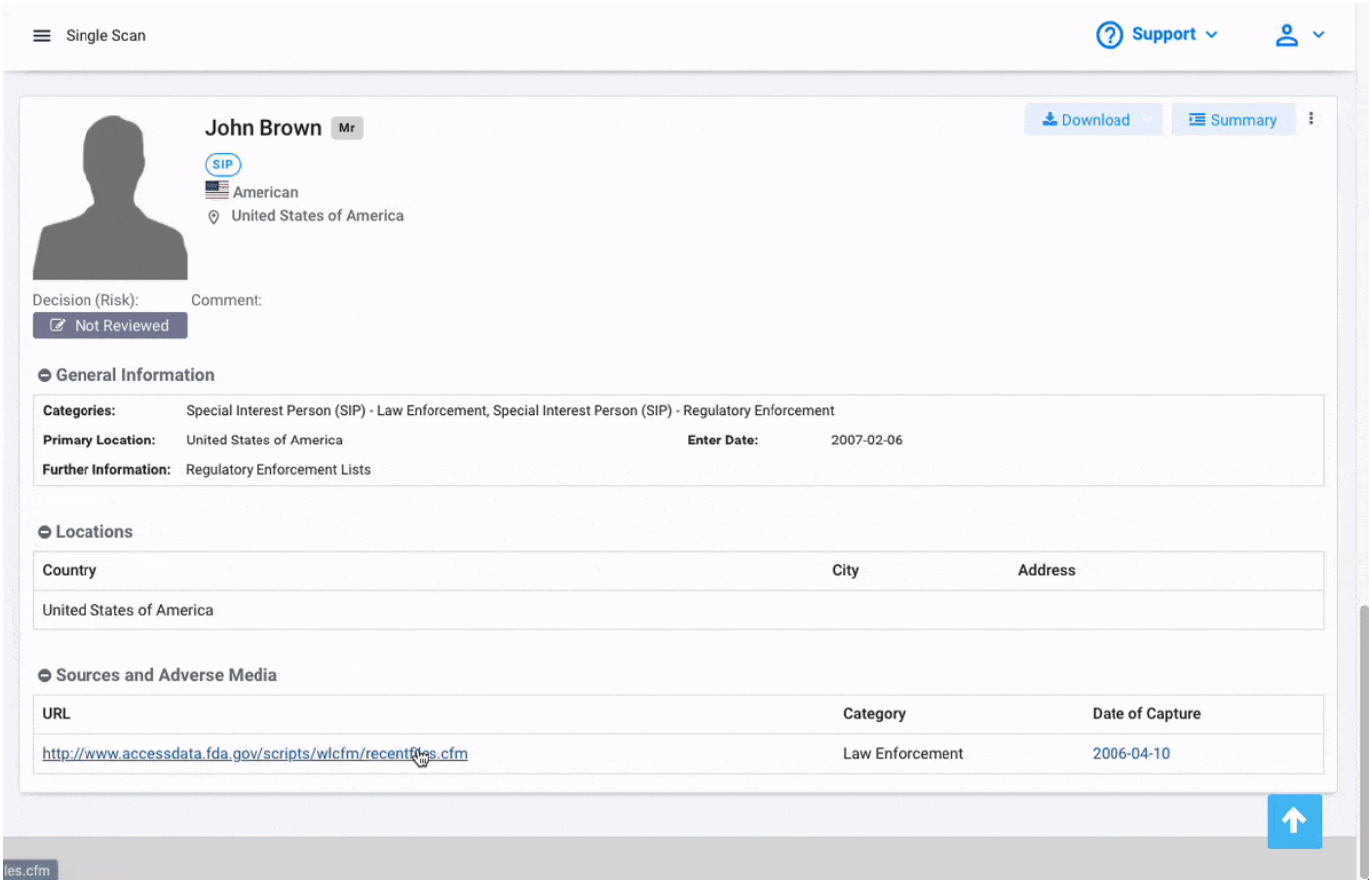
Sources and adverse media links can be archived, moved, removed and changed causing broken links in the original URL. Where available, a PDF copy of the article is cached and made available with the date of the captured snapshot.

To access this, look for hyperlinked dates in **Date of Capture**



Report profile for review

Directly report profile data issues or submit questions about a specific profile. Expand the options for the profile and select the most appropriate Subject and enter your comment or query. If wish to report a profile to be outdated, please include details with hyperlinks to publicly available sources or official lists for review.



Request Copyright Media

For copyrighted media sources, you'll see a question mark against the PDF icon. If the source link is not accessible or the cached PDF is not available, you can request for the copyrighted sources by clicking on the date with the question mark icon. This will request and download a copy of the media, and the link will be available for up to 15 minutes.

Your browser does not support the video tag.

Viewing risk levels of profile and linked entities

Recommended risk level of matched profile is displayed based on the current organisation risk setting. To view the risk levels of associated Individuals and Companies, click on the **Calculate Risk Levels** button.

Your browser does not support the video tag.

Scan Results for Corporates

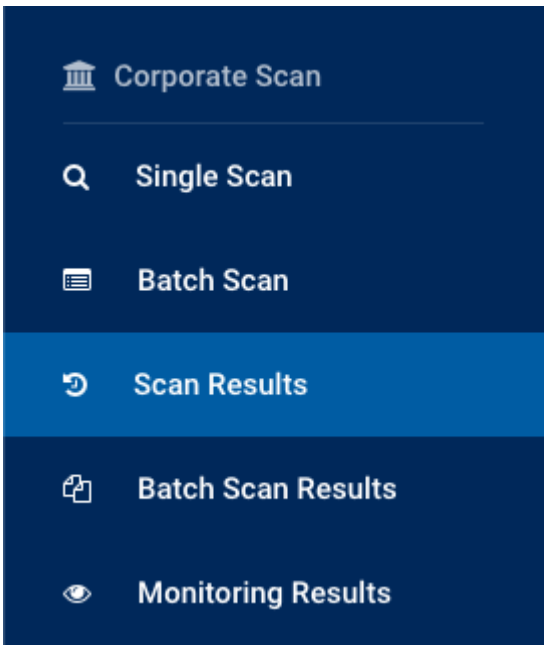
Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
👁	👁	👁	✕	👁	👁

Standard User Permissions

Whilst **Compliance Officers**, **Advanced Users** and **Auditors** have access to view scan results performed by all users associated with the organisation, **Standard Users** are able to only view scan results performed by themselves.

Corporate Scan > Scan Results displays the match results for the companies screened.

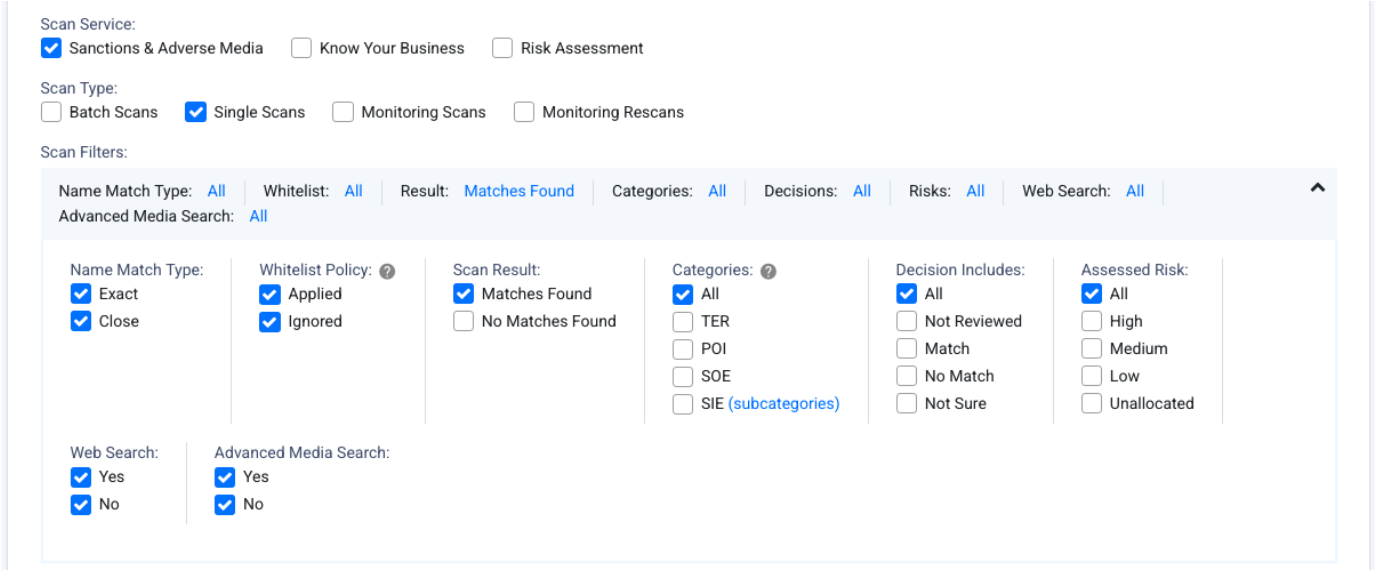


By default, it lists **Single Scan** results for Sanction and Adverse Media **Matches Found** only. You can change the filters to expand or further refine the scan results displayed using the options available for **Scan Service**, **Scan Type**, **Scan Result Settings** and **Company Search**.

If you are part of a multi-level organisation or if you have multiple users associated with your organisation account, you can additionally filter by **Organisation** and **Users** who have performed the scans.

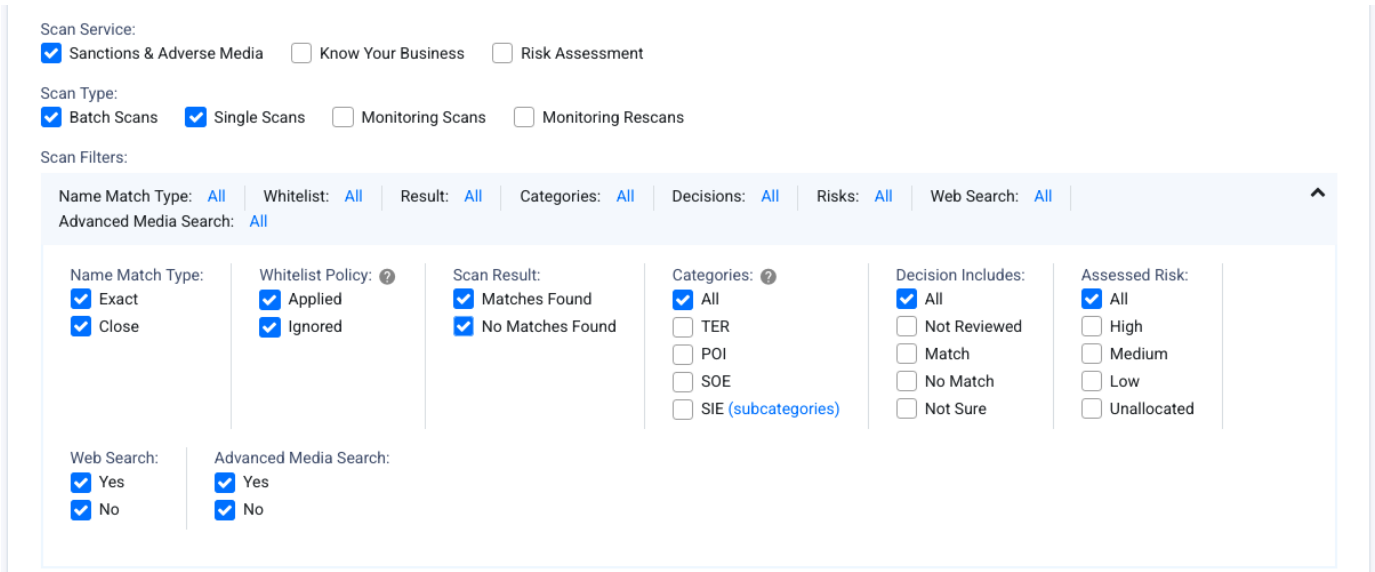
Scan Results Settings to filter by scan settings and results:

Default filter settings where scans with `No Matches Found` are excluded in **Scan Result**.



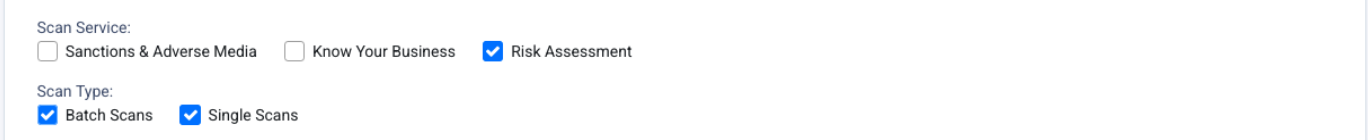
Scan Result Settings for all scans regardless of match results:

Note that both `Single Scans` and `Batch Scans` are selected. Both `Matches Found` and `No Matches Found` are selected.



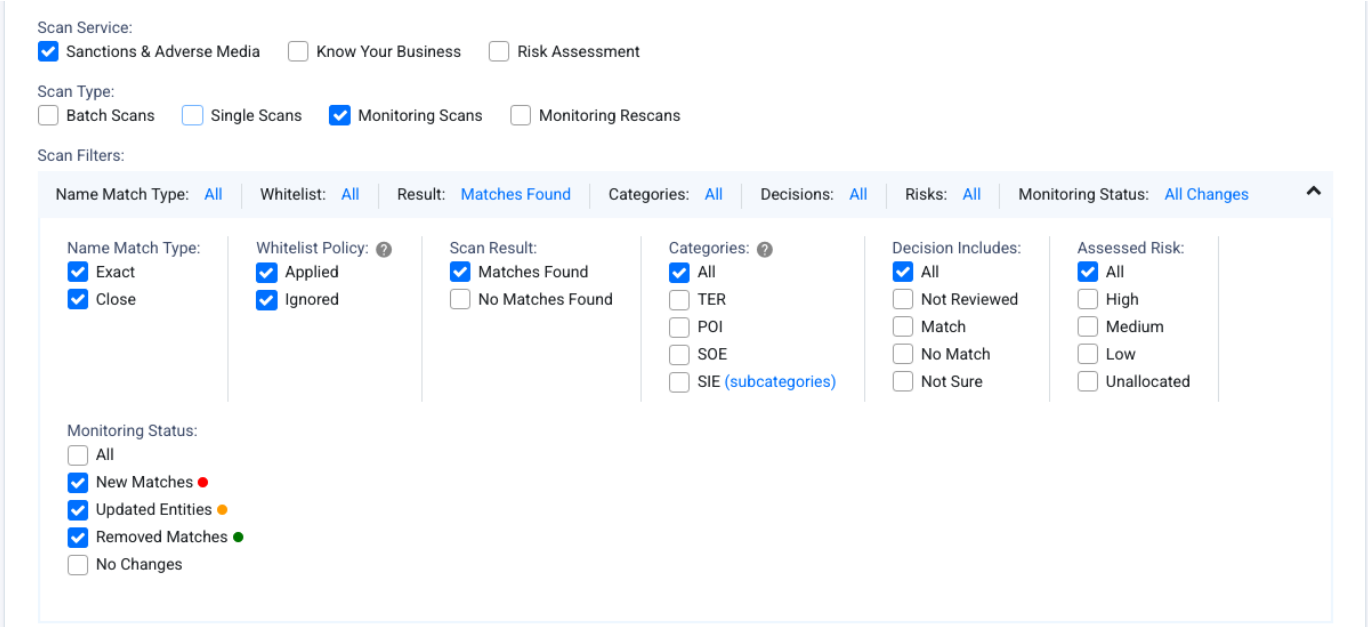
Scan Result Settings when AML Risk Assessment is selected:

Filter scans with Risk Assessment enabled during screening. This refers to the AML Risk Assessment questionnaire completed based on customer information, country, product or services offered and outcome of screening.



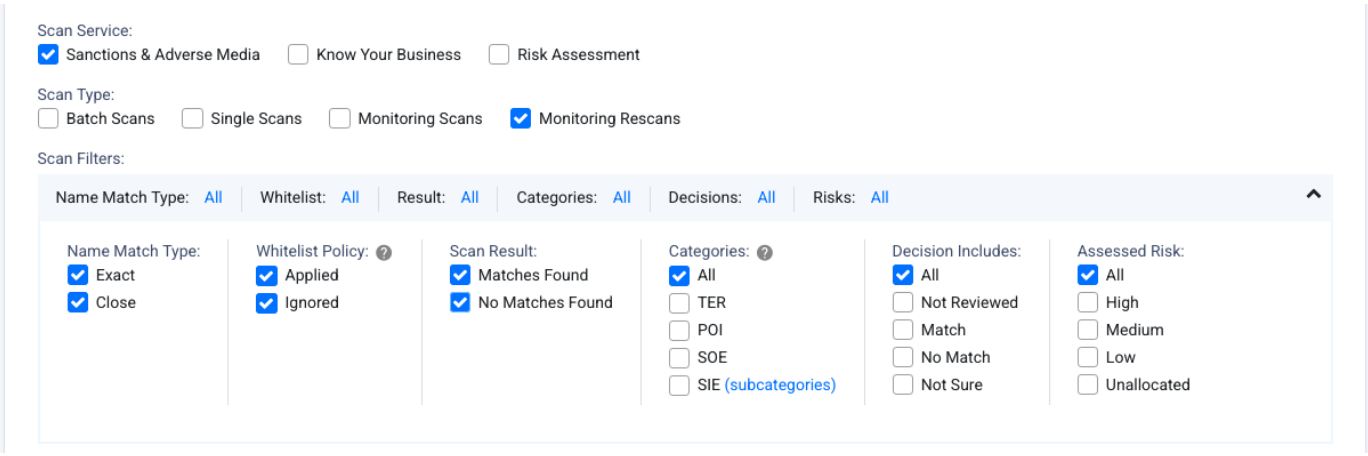
Scan Result Settings when Monitoring Scans is selected:

Filter scans based on the outcome of ongoing monitoring and type of detected change.



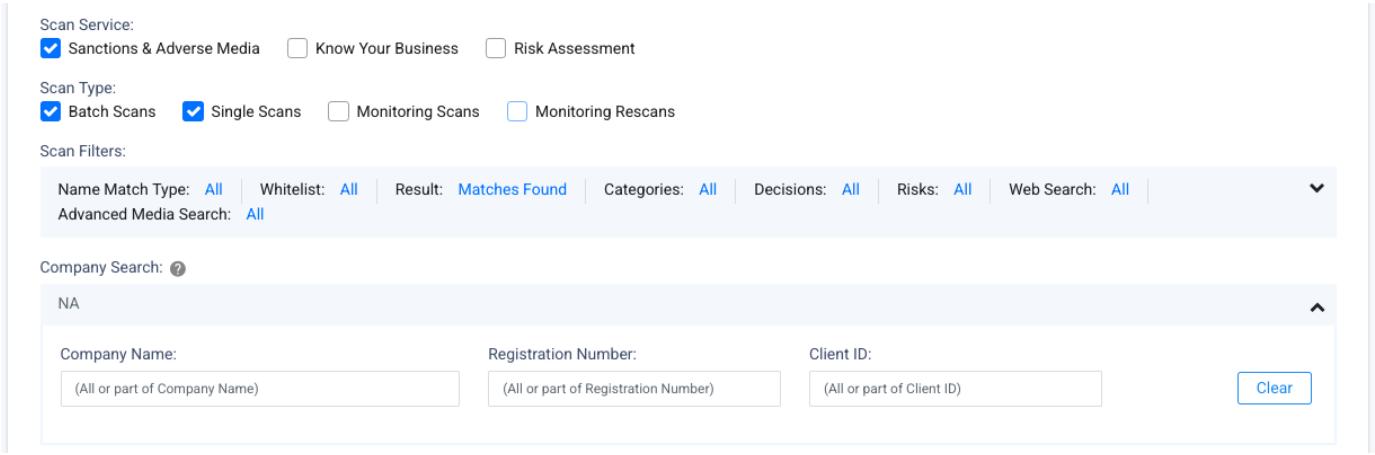
Scan Result Settings when Monitoring Rescans is selected:

Filter for rescans where actively monitored entities are rescanned against the full database on day of account subscription renewal.



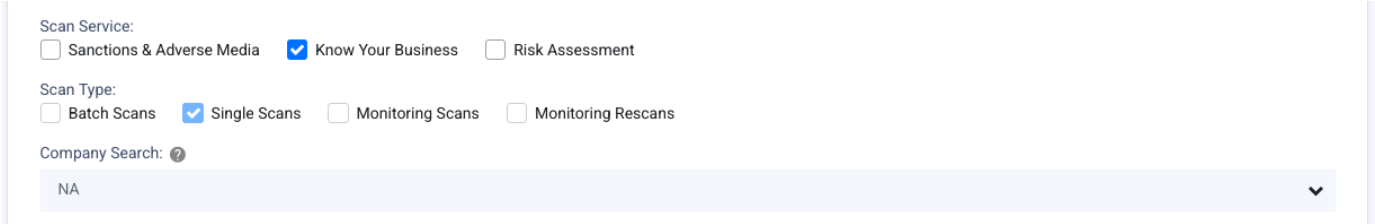
Company Search to filter by companies scanned:

Search for a specific company in Batch and/or Single Scans.



Filtering for Know Your Business checks:

Filter scans for all Know Your Business checks, which are conducted via Single Scans only.



Searching and Filtering Scan Results

Scan Result Settings:

Fields	Description
Name Match Type	Filter by the Name Match Type used during scans. The options are `Exact` and `Close`. By default, all options are selected.

Whitelist Policy	Filter if whitelist policy was applied during the scan. Profiles marked as `No Match` are whitelisted and excluded from being returned and displayed again. The options are: `Apply` and `Ignore`. By default, all options are selected
Scan Result	Filter by the outcome of the scan. Options are `Matches Found` and `No Matches Found`. By default, `Matches Found` is selected.
Categories	Filter results by the major category type of the matching profile. The categories are: `TER` (Terrorism), `POI` (Profile of Interest), `SOE` (State Owned Enterprise), `SIE` (Special Interest Entity). SIEs have filters for additional subcategories such as `Sanctions Lists`, `Law Enforcement`, `Regulatory Enforcement`, `Organised Crime` etc. By default, `All` categories are selected.
Decision Includes	Filter results by due diligence decisions applied to the matching profile. The decisions available are: `Not Reviewed`, `Match`, `No Match` and `Not Sure`. By default, `All` decisions are selected.
Assessed Risk	Filter results by due diligence risk assessments applied to the matching profile. The assessed risk options are: `High`, `Medium`, `Low` and `Unallocated`. By default, `All` assessed risk levels are selected.

Web Search	Filter results where additional web search for adverse media was performed. The options are: `Yes` and `No`. By default, `All` options are selected.
Advanced Media Search	Filter results where additional advanced media search for latest news articles was performed. The options are: `Yes` and `No`. By default, `All` options are selected.

The full list of categories and subcategories are described in List Categories.

Company Search:

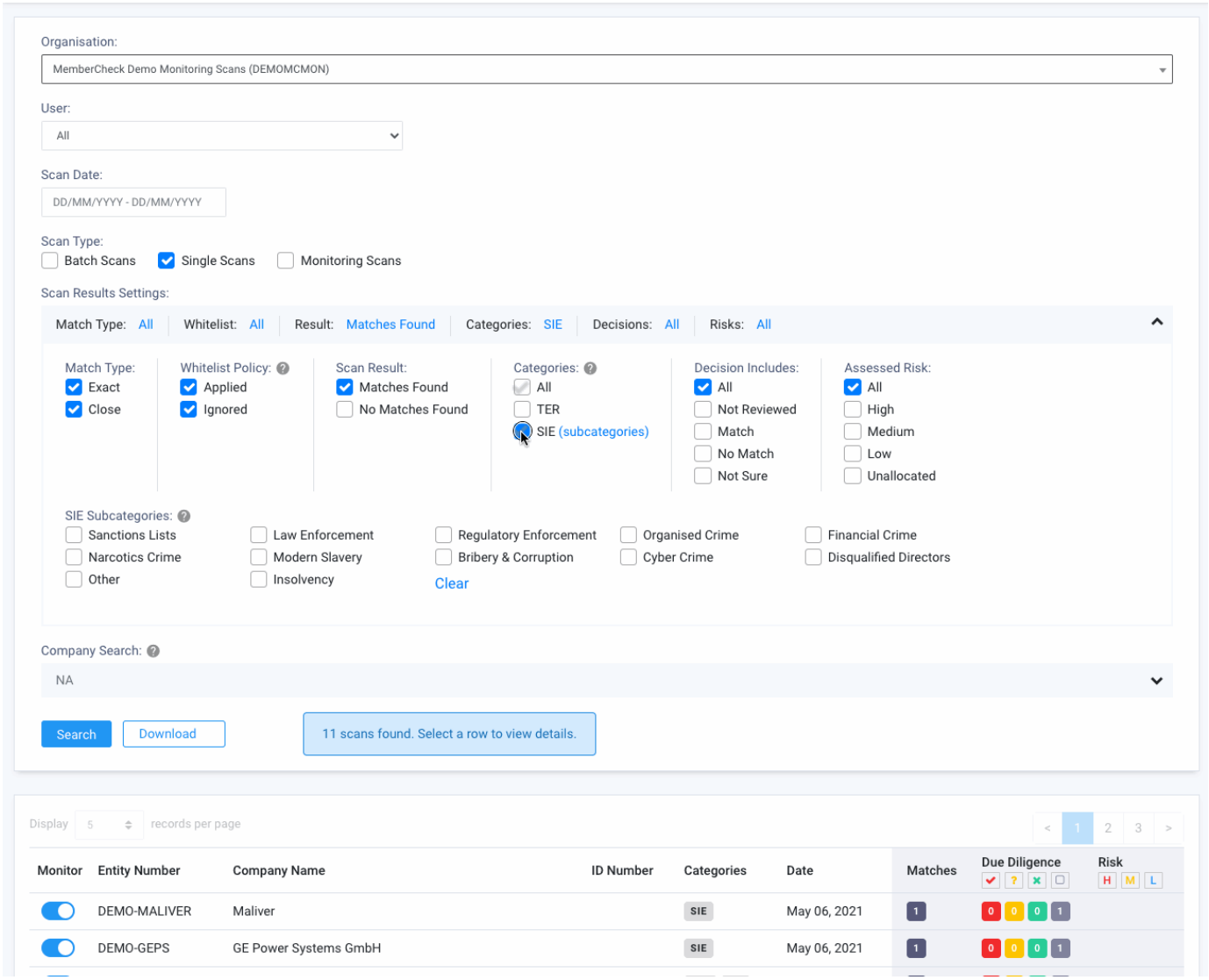
For a quick and specific search of the company scanned, use the **Company Search** panel.

To search for fields where contents exist, use an asterisk (`*`).

Fields	Description
Company Name	Search results by the Company Name entered during scan. Search supports full or partial matching. Example: `com` returns `Company`, `Computer Whizz`, `The Company` etc.
Registration Number	Search results by the Registration Number entered during scan. Search supports full and partial matching.
Client ID	Search results by Client ID entered during scan. Search supports full and partial matching.

Filtering scans by categories and subcategories:

Special Interest Entities (SIE) are further categorised into subcategories. Descriptions of the **SIE subcategories** are described below.



Viewing Scan Results

Scan results of companies screened are summarised as follows. Results are displayed in chronological order from most recent first.

The table below contains all possible columns. On-screen visibility depends on the selected **Scan Service**:

Field	Description
Monitor	If an **Client ID** has been assigned to the company during scanning, a toggle switch to enable or disable monitoring is displayed.
Client ID	The unique identifier assigned to the company during scanning.

Company Name	The name entered during screening.
Registration Number	The company registration number entered during screening.
Categories	Major categories of matched profiles. These can be one or any combination of the following: • `TER` : Special Interest Entity - exposure or associations with terrorist related activities. • `POI` : Profile of Interest - exposure or associations with terrorist related activities. • `SIE` : Special Interest Entity - Organisations on Sanctions, Regulatory Enforcement, Law Enforcement lists, and Adverse Media sources. • A blank Category indicates that no matches were found.
Date	Date the scan was run.
Documents	Number of registry documents requested. This may be `0` or more depending on whether you have requested for any registry documents.
Enhanced Profile	Number of enhanced profile data (UBO) requested. This may be `0`, `1` or more depending on whether you have requested for the UBO, and for 1 company record or multiple company records.
Matches	Number of matching profiles for the scanned company. `0` indicates no matches found.

Due Diligence	Number of due diligence decisions made against the matching profiles based on the decision types: Match Not Sure No Match Not Reviewed
Risk	Assessed risks assigned to matching profiles: High Medium Low
Comment	Remark or comment associated with the due diligence decision.

Viewing Profile Risk Levels

Where an organisation has configured its Risk Settings, the recommended risk levels will be displayed for Sanctions and Adverse Media profile matches. The risk levels are based on the current organisation settings.

To view the risk levels of linked Individuals and Companies to the matched profile, click the **Calculate Risk Levels** button next to these sections. The results are retrieved based on the latest organisation risk settings and are not persistent in the scan history.

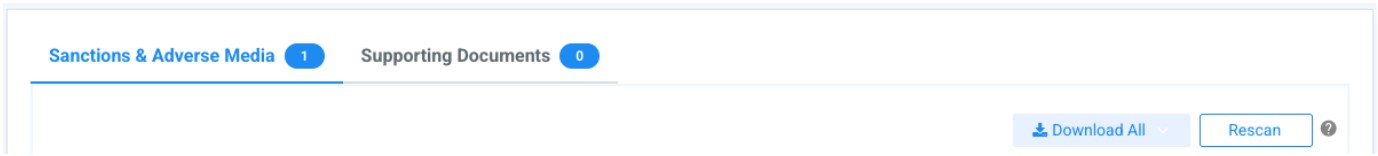
Rescanning a Corporate Entity

A **Rescan** feature is available for companies previously scanned for Sanctions and Adverse Media, and applies for scans that resulted in matches and no matches. This feature allows for a

new scan to be performed without the need to re-enter the company's details, enabling you to check for the latest updates.

Initiating a rescan will commence a new scan using the company's existing details. The previous scan policies and settings will be applied during this process, with the exception of the watchlists, which will be determined by the organisation's current list access scope.

Rescan activities count toward the organisation's scan activity and usage.

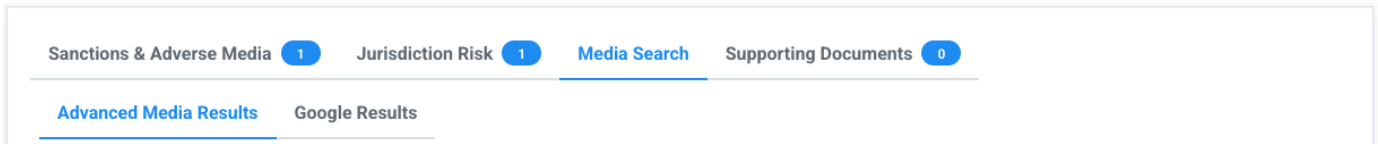


Know Your Business check

If the business check for Know Your Business was selected for screening, you will see an additional tab for the KYB results.

Web Search and Advanced Media Search

If the Web Search or Advanced Media Search options were selected for additional adverse media checks, you will see an additional tab with the media results.



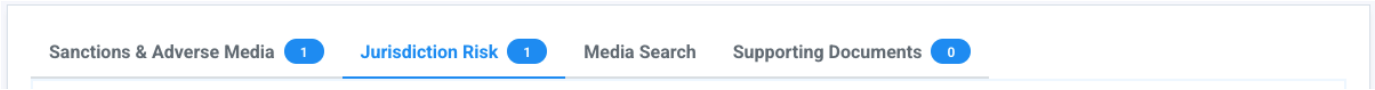
For **Advanced Media Search**, the 30 most recent news articles from around the globe are returned with details of the title, publication date, source name, author, article readership and word count.

For **Web Search**, the first 10 most relevant results are displayed.

All links will open up to a new browser tab.

FATF Jurisdiction Risk

If the FATF Jurisdiction Risk option was selected during scan, you will see an additional tab containing information about the country associated with the matched profile, if available.



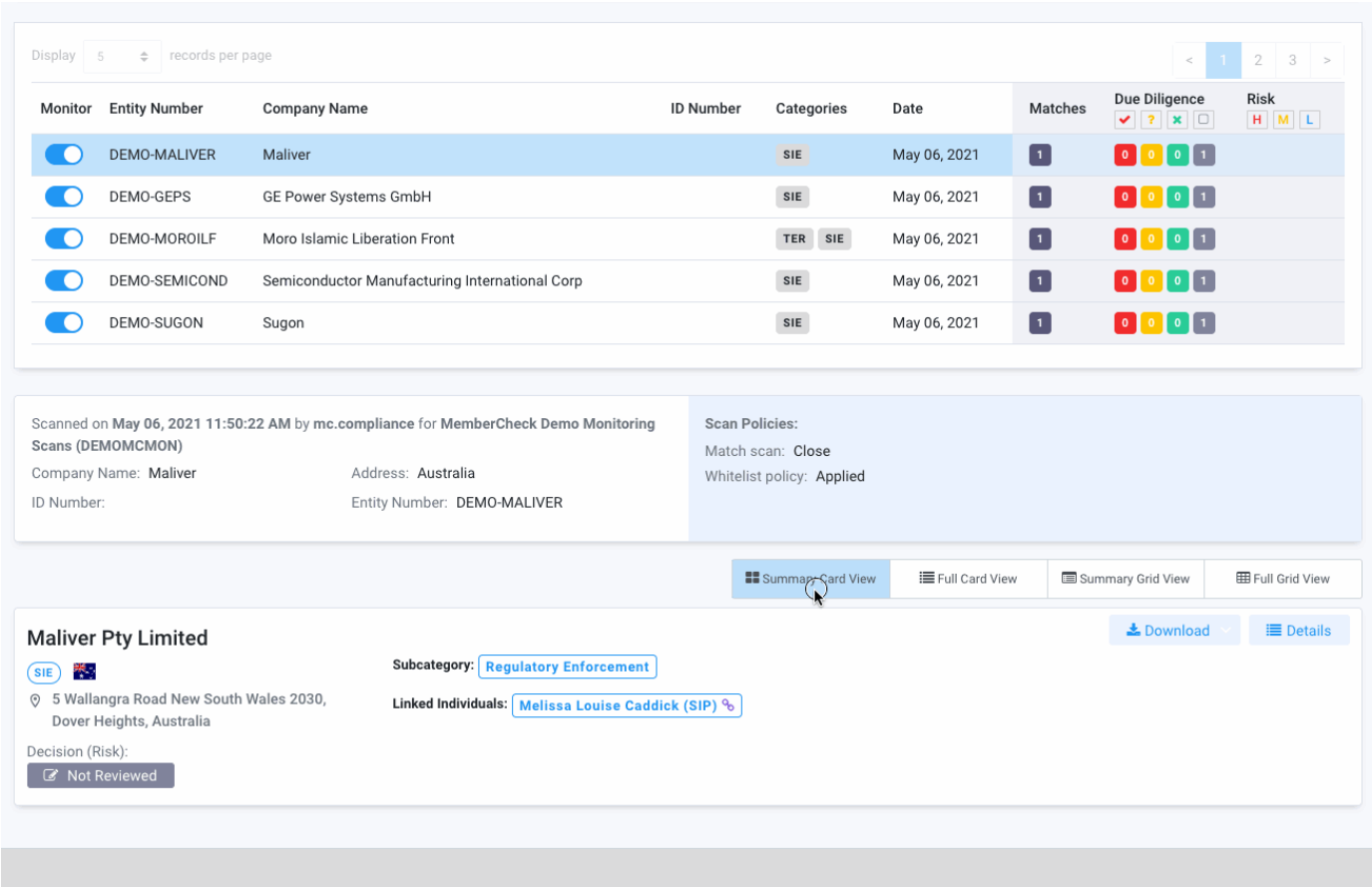
Viewing Scan Result Details

Matching profile information for Sanction and Adverse Media are displayed in **card** or **grid** format with either a **summary** or **full** detailed card view of the profile.

Click on a scan result record to view details of matching profiles:

Card views provide a quick look into the matching profile with the high level summary with the options to expand to view details.

Grid views provide an additional table with summarised profile details with an overview and comparison of results. Where information in the profiles match with the scanned company, cells are highlighted to indicate full match or partial match.



Detailed information of profiles are displayed in the cards and may include:

Fields	Description

Profile Details	Key profile information: • Company Name • Category e.g. `SIE`, `TER` • Country or location • Due diligence decision and risk level assessment • `Tax haven` and `Sanction` indicators based on the primary location of the company.
General Information	• Categories of the profile e.g. `Special Interest Entity (SIE) - Regulatory Enforcement` • Business Type - type of business e.g. privately-held company, publicly-traded company, charitable organisation, bank • Activities - description of core activities or services provided • The date the record was last reviewed or updated • Further information and profile notes
Also Known As	• Name - aliases or other names associated with the organisation • Type - type of name variation e.g. original script name, name spelling variation, name abbreviation, previous name, brand name, fake name.

Locations	All registered or known locations associated with the organisation: • Country • City • Address • Type e.g. registered, operating, previous, branch office, representative office, headquarters
Official Lists	Name of Sanction List this profile appears in. • Name - Name of the official Sanctions list e.g. Office of Foreign Asset Control • Category - category of the official list • Measures - list of measures enforced by the official list e.g. asset freeze, travel ban • Origin - country or region of the official list • Type - type of sanction classified by the official list • Status - status of the entity on the official list i.e. `current` or `former`.
Identifiers	List of registration and ID numbers of the company. • Type - type of identifier e.g. DUNS number, business registration number, business registration date, tax number, OFAC unique ID, SECO unique ID • Value

Sources and Adverse Media	Links to online sources and adverse media for the profile. • URL - link to the source of information regarding the entity • Category - category type of source e.g. `Sanction`, `Adverse Media`, `Law Enforcement`, `ID/V` (ID Verification) etc • Date of Capture - date the source article was recorded. This may contain multiple dates where the source was reviewed and recorded. • Info - additional information on the publication e.g. publication date, credibility, language of the article, title and summary, if available  Links to news articles may be out of date or broken depending on how recently they have been reviewed. Some source articles contain cached PDF copies. If the cached PDF is available, this is provided as a hyperlink in **Date of Capture** . For copyrighted sources which may not be accessible, you can check for availability of the copyright material. If available, the data of capture will change to a hyperlink to download the PDF. Availability of cached materials and copyright PDFs are dependent on your data source subscription.
Linked Individuals	Individuals associated with the entity with a description of the relationship. • Full Name • Category e.g. `PEP`, `RCA` • Description  Click on a **Linked Individual** to view further information of the person.

Linked Companies	Lists of organisations associated or affiliated with the entity with a description of the relationship. • Name • Category e.g. `SIE` • Description

Click on a **Linked Company** to view further information of the company.

Something amiss with the profile data?

If the information in the profile data appears to be outdated, incomplete or unclear as to reasons for being listed in the watchlist, you can report this profile directly to the MemberCheck team for review. See tip on how to **report profile for review**.

Know Your Business profiles are also viewable in **card** or **grid** view with an additional **document view** of requested documents for the company.

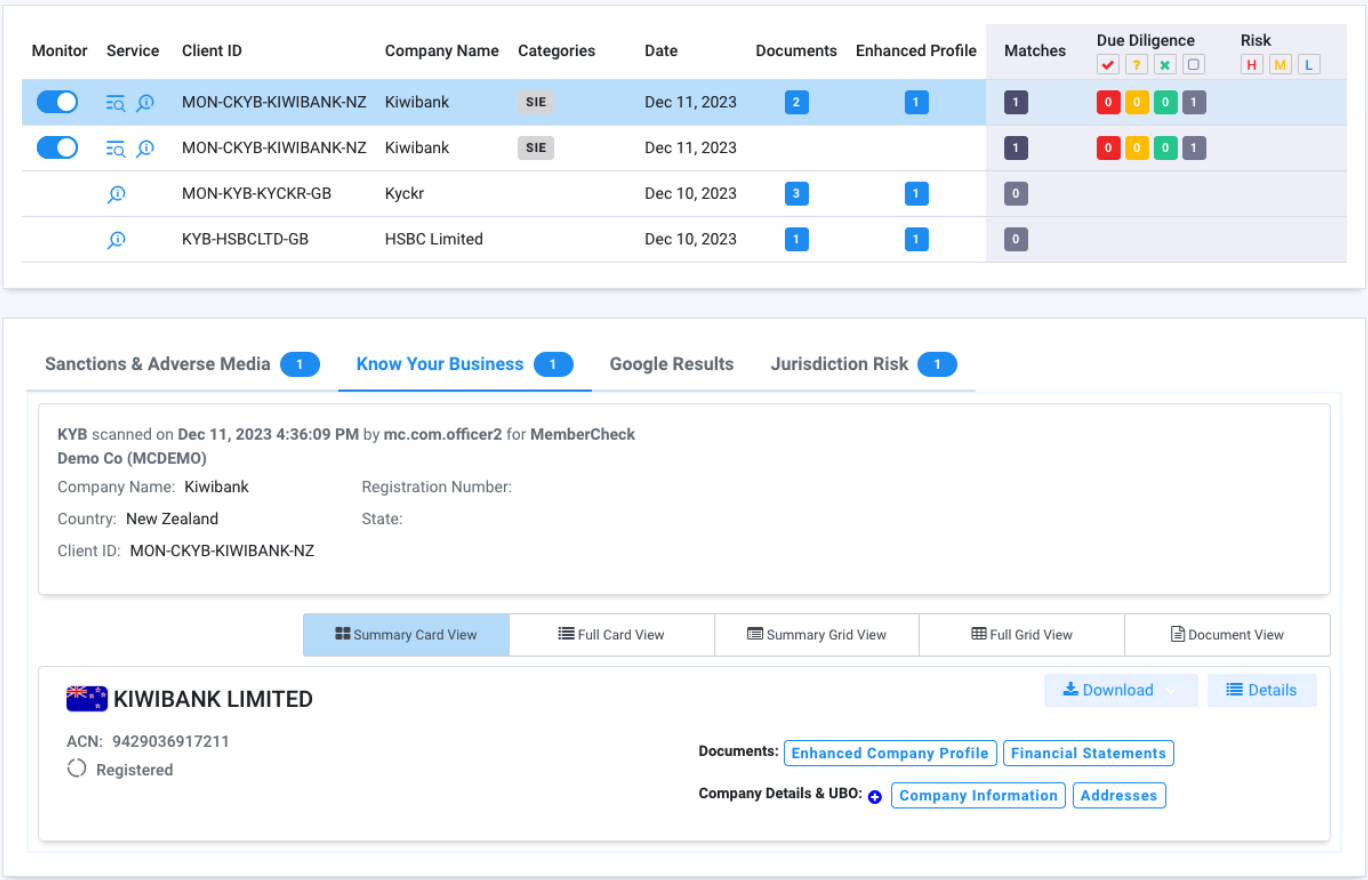
Your browser does not support the video tag.

Profile Categories

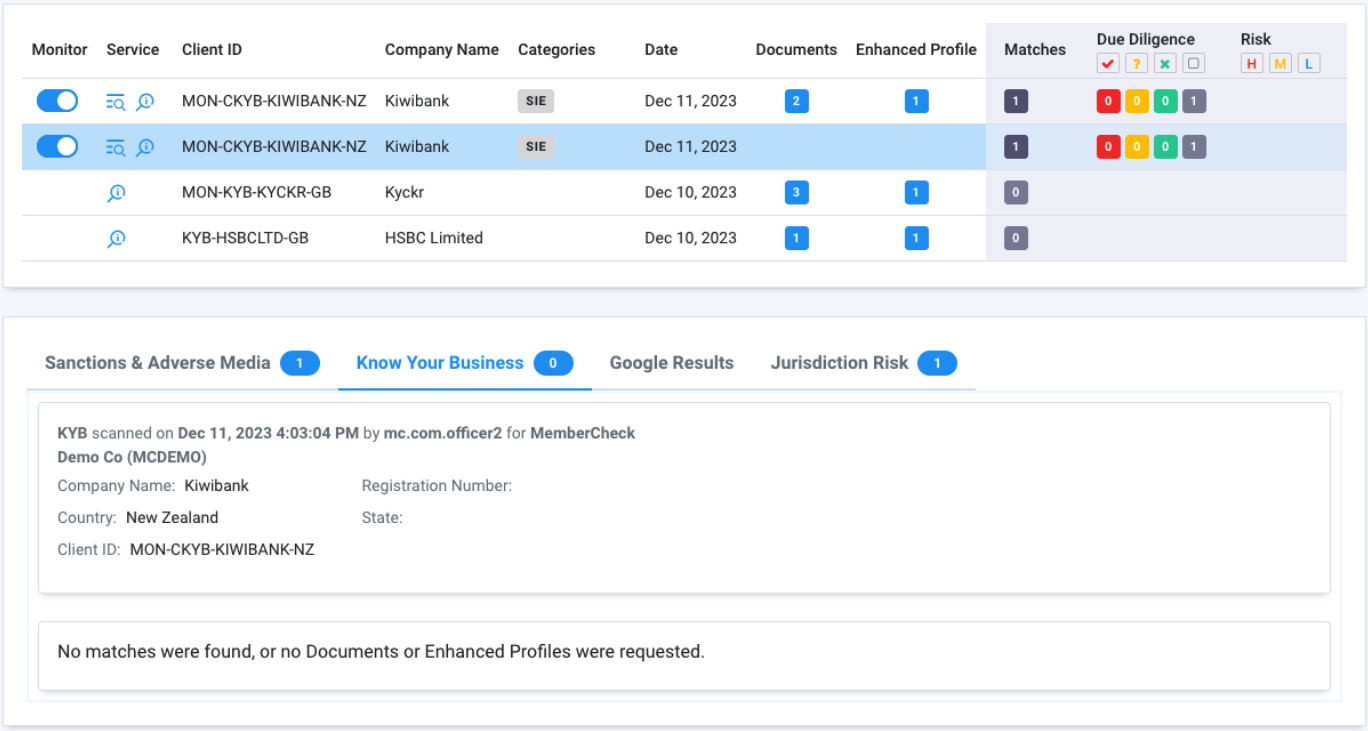
Refer to List Categories for a full list of the definitions of the main categories and subcategories.

Know Your Business checks

If a business check was included in the screening, additional information will be displayed for the company scanned.



If no company profile was found, or no documents or UBO were requested, the **Documents** and **Enhanced Profile** columns will be empty.



Detailed information of the business check may vary between registry jurisdictions and generally includes:

Fields	Description
Company Summary	High-level identification of the business including company name, registration number and status of registration.
Documents	List of requested documents and the status of delivery. Delivery of documents range from near real time to 7 days.
Company Information	Company details including legal and registration details.
Addresses	List of registered addresses
Directors and Shareholders	List of representatives such as shareholders, directors and secretaries, the type of entity (`Person` or `Company`), role, percentage of holdings, address and appointment date.
Ultimate Beneficial Owner(s)	Individual(s) identified as the ultimate beneficial owner including name, nationality, address, and date of birth.

Downloading Reports

For record keeping and for purposes of auditing for your organisation, you can download reports of your screening activities and the associated results. All reports are available in PDF format. Some reports are also available in Word, Excel and CSV formats. Where large volumes of data are downloadable, the application may only offer download in CSV format.

This option is available through the **Download** button in all screens where download of reports are available.

In the **Scan Results** screen, the Download button offers the ability to:

- Preview PDF report before download
- Export as PDF
- Export as Word
- Export as Excel

- Export as CSV
- Export Results Summary report.

The **Download All** button enables you to download a report of all profile matches for a screened entity. The consolidated report contains an extract of the key details of the profiles such as the applied scan settings and policies, name, address, due diligence decisions, and the category and subcategory of the profile record.

For **Know Your Business** checks, the following download options are available:

- Preview PDF report of the business check activity
- Export as PDF of the business check activity
- Download documents of requested from the jurisdiction registry
- Download Enhanced Company Profile of the UBO check

The **Results Summary report** option enables you to download a summary of all the profiles of matched results for your Sanction screening, and is available in both the **Scan Results** and **Batch Scan Results** screens. This report is available in CSV format only and is compressed and downloaded as a ZIP file. The ZIP file is secured and password protected using the email address of the person who generated this report. If you have initiated the download of this report, the password to the ZIP file will be your registered email address in the application and entered as lower case. To check which email address you have registered in the system, you can review the information in **My Profile**.

Email Address to unlock Results Summary Report

If the email address has different casing such as `UserName@domain-name.com` then the password to unlock the ZIP file will be `username@domain-name.com`

Availability of reports during trials and demos

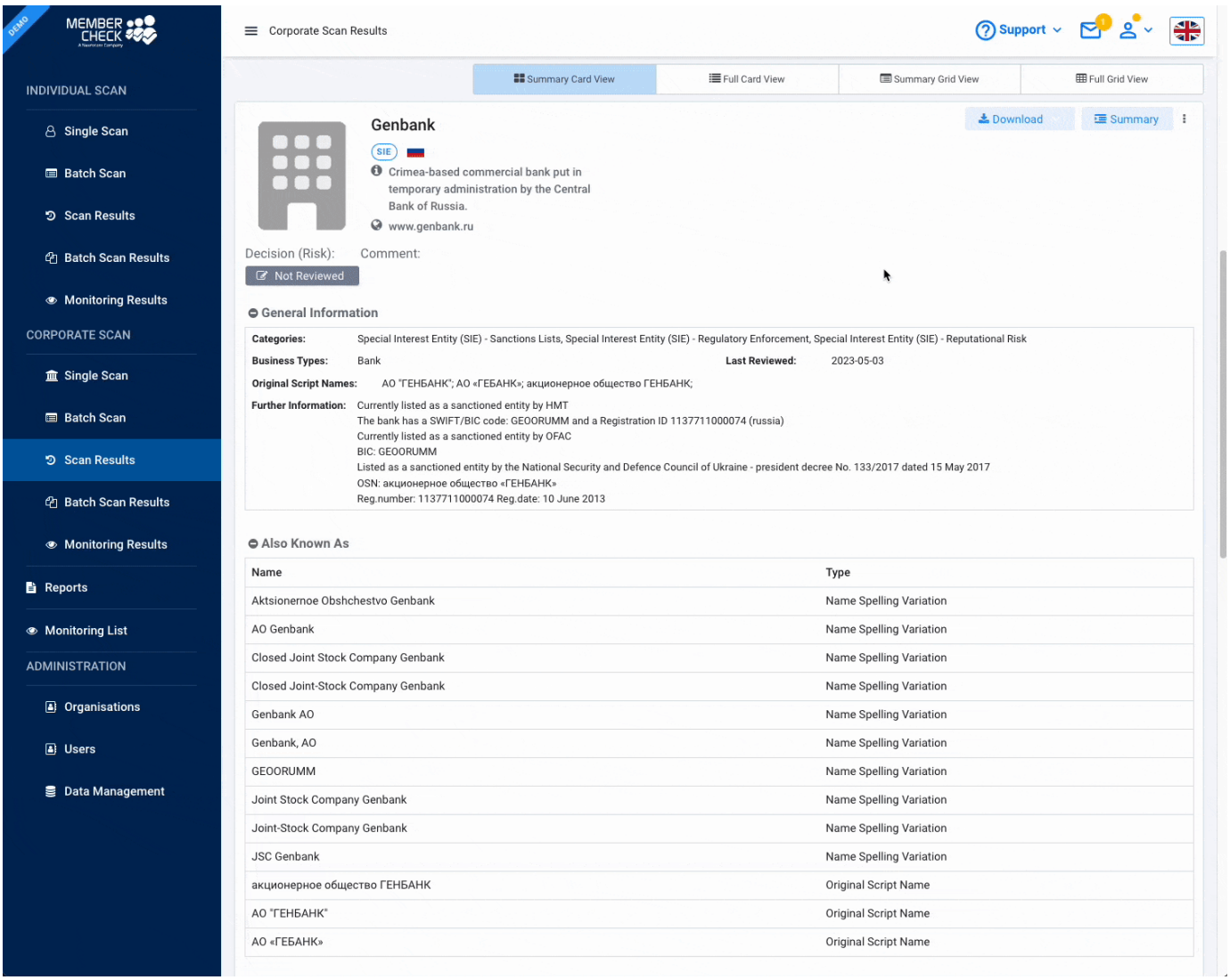
If you are trialling the service on a demo environment, only the PDF and CSV options are available.

Quick How-To Guides

Viewing Cached Sources and Adverse Media

Sources and adverse media links can be archived, moved, removed and changed causing broken links in the original URL. Where available, a PDF copy of the article is cached and made available with the date of the captured snapshot.

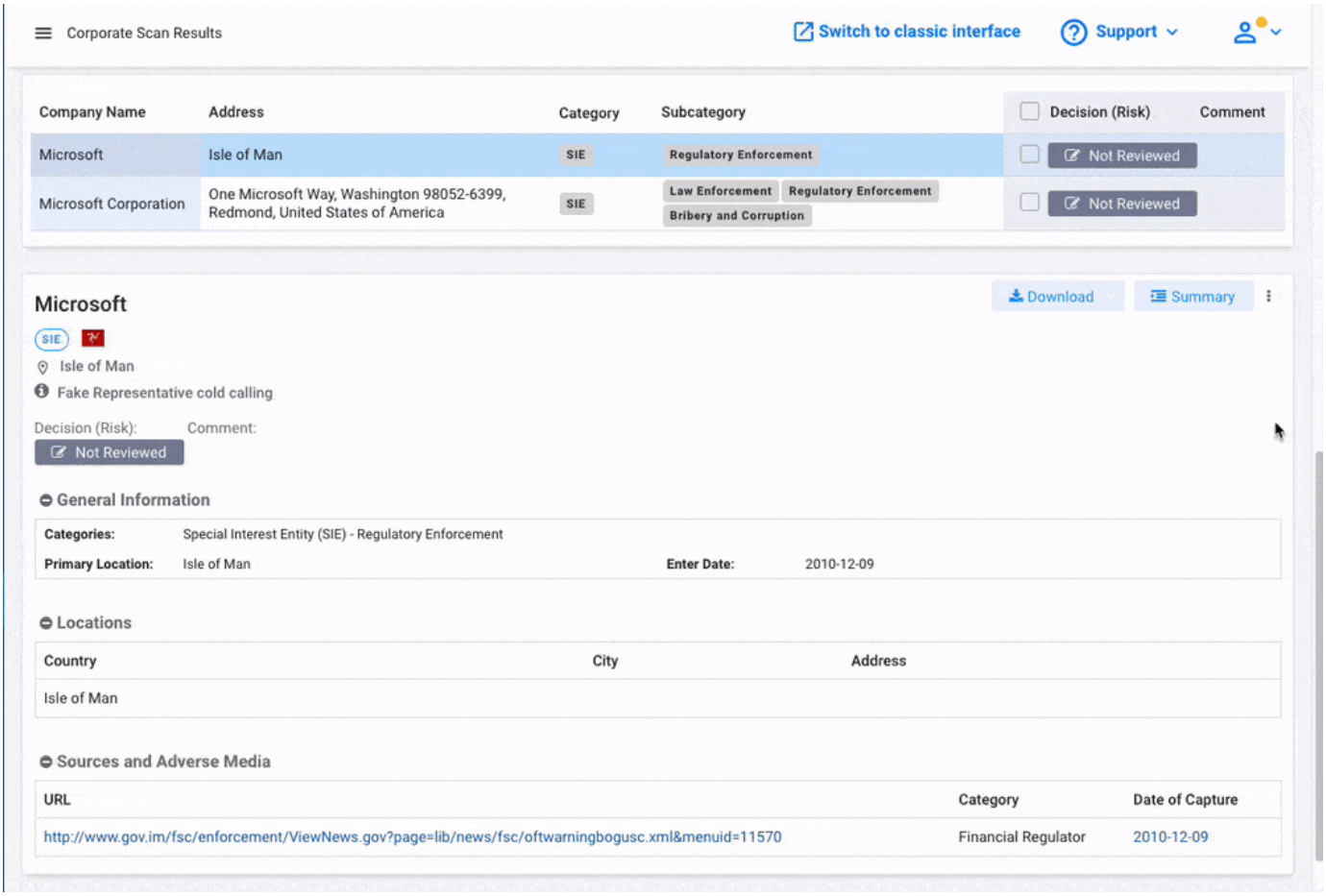
To access this, look for hyperlinked dates in **Date of Capture**



Report profile for review

Directly report profile data issues or submit questions about a specific profile. Expand the options for the profile and select the most appropriate Subject and enter your comment or query.

If wish to report a profile to be outdated, please include details with hyperlinks to publicly available sources or official lists for review.



Viewing risk levels of profile and linked entities

Recommended risk level of matched profile is displayed based on the current organisation risk setting. To view the risk levels of associated Individuals and Companies, click on the **Calculate Risk Levels** button.

Your browser does not support the video tag.

Batch Scan Results

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

Standard User Permissions

Whilst **Compliance Officers**, **Advanced Users** and **Auditors** have access to view scan results performed by all users associated with the organisation, **Standard Users** are able to only view scan results performed by themselves.

Results of batch scans are separated for Individuals and Corporates and can be accessed via **Batch Scan Results**.

Batch files uploaded via the web application and API are visible on this screen with an overview of:

- Date of upload
- Batch file name
- Number of entities in the batch file
- Number of entities with matches found against the watchlists
- Total number of profile matches
- Status of the batch scan.

Select the batch file row to view detailed information of the batch scan.

In the Batch Scan Details screen, you can see a summary of the results of the batch file:

- Screening policies applied
- Number of entities with matches
- Total number of profile matches per category

- Category of watchlists scanned

By default, only entities with matches found are displayed. To view all entities in the batch file, change the **Scan Filters** accordingly.

Searching and Filtering Scan Results

Scan Filters

Fields	Description
Scan Result	Filter by matches found or not. By default, `Matches Found` is selected.
Categories	Filter by category of the profile. By default, `All` is selected.
Decisions	Filter by due diligence decisions applied, if any. By default, `All` is selected.
Assessed Risk	Filter by the level of risk applied, if any. By default, `All` is selected.

For a quick and specific search of the entity screened, use the **Individual Search** or **Company Search** panel, depending on the entity type. To search for fields where contents exist, use an asterisk (`*`).

Add Entity to Monitoring List

If your organisation has ongoing monitoring enabled, you will be able to see the **Monitor** toggle switch against each entity with a Client ID in your batch scan. You can toggle the switch for each entity individually or apply to all entries in the batch file to add in bulk. To add all entries in the batch file to the Monitoring List, click the button at the bottom of the screen, `Monitor Batch File` .

Similarly, to remove all entries in a batch scan from the Monitoring List, click on the button `Remove Monitoring of Batch File`.

> **Client ID required for monitoring**
>
> Only entities with a **Client ID** can be added to the Monitoring List.

Your browser does not support the video tag.

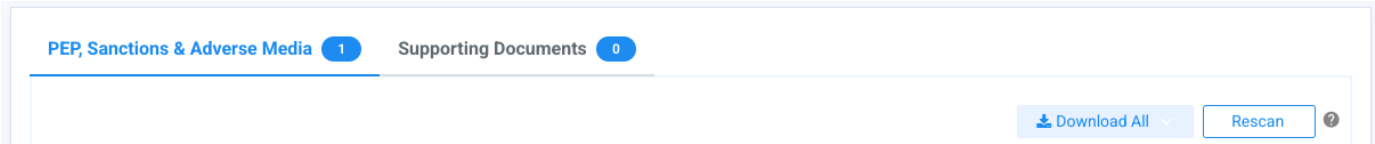
Rescanning an Individual or Corporate Entity

A **Rescan** feature is available for individuals and companies previously scanned for PEP, Sanctions and Adverse Media within the batch scan. This applies for individual entities within the batch scan that resulted in matches and no matches. This feature allows for a new granular scan to be performed without the need to re-enter the individual's details, enabling you to check for the latest updates.

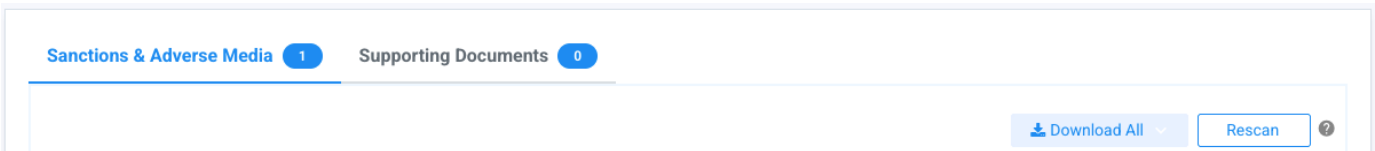
Initiating a rescan will commence a new scan using the entity's existing details. The current scan policies and settings will be applied during this process, with the exception of the watchlists, which will be determined by the organisation's current list access scope.

Rescan activities count toward the organisation's scan activity and usage.

Rescan option for individuals:



Rescan option for companies:



Due Diligence

Permissions

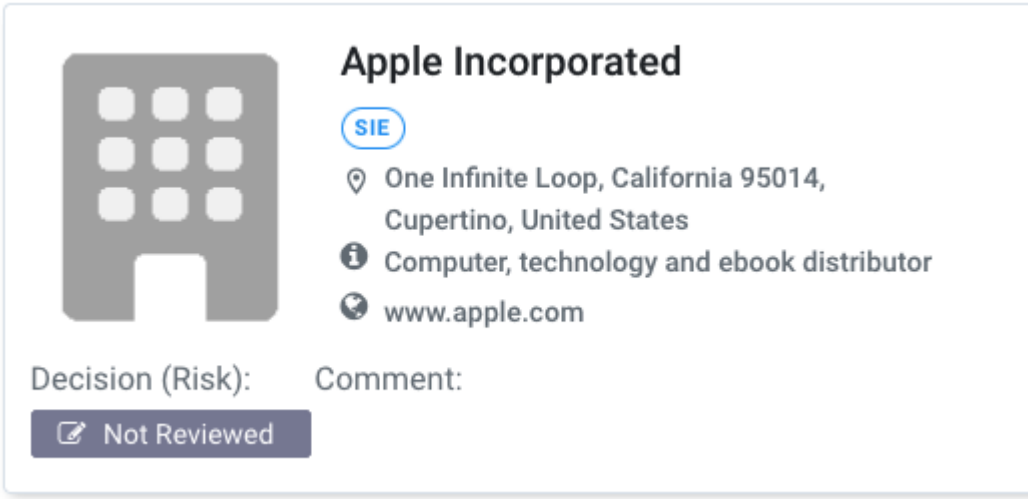
Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	✎	✎	✕	✕	👁

> ✎ **Standard User Permissions**
>
> Whilst **Compliance Officers**, **Advanced Users** and **Standard Users** can perform due diligence and risk level assessments, **Standard Users** are able to assess and make due diligence decisions on scan results performed by themselves.

Recording Due Diligence and Risk Level Assessments

You can record due diligence decisions, add notes and risk level assessments against matched profiles for both individual and corporate entities scanned for your organisation. This process is integrated into the screening process and is accessible via **Individual Scan > Scan Results** and **Corporate Scan > Scan Results**.

If you have included a unique reference Client ID during screening, you will see a button for the **Decision (Risk)** and **Comment** beneath the profile image.



By default, all results are flagged as **Not Reviewed** until a decision is applied. The options available are as follows:

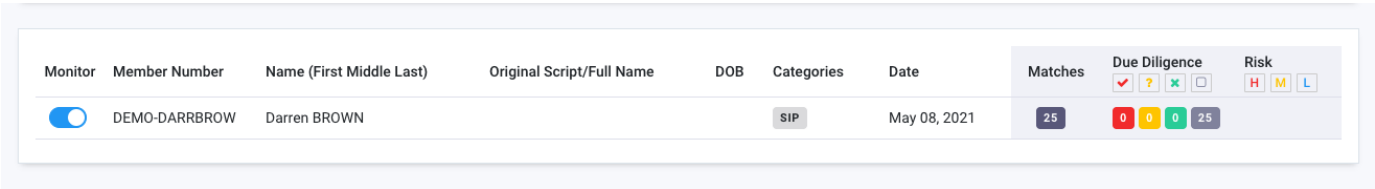
Status	Icon	Description
Not Reviewed		Default status until a decision is applied. The number in the box indicates the number of matches for the individual or company entity which are not reviewed.
Match		The number in the box indicates the number of matches for the entity which are recorded as match.
Unsure		The number in the box indicates the number of matches for the entity which are recorded as unsure.
No Match		The number in the box indicates the number of matches for the entity which are recorded as no match.
High		Indicates at least 1 recorded high risk level profile. Risk level applies to **Matched** and **Not Sure** decisions only.
Medium		Indicates at least 1 recorded medium risk level profile. Risk level applies to **Matched** and **Not Sure** decisions only.

Low		Indicates at least 1 recorded low risk level profile. Risk level applies to **Matched** and **Not Sure** decisions only.

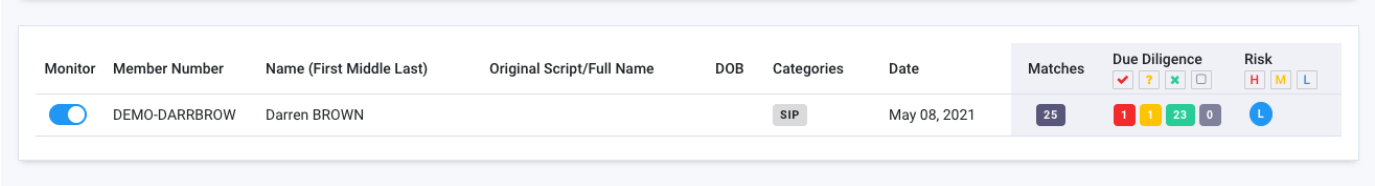
Understanding the Due Diligence Summary

Example of an individual scan which resulted in **25 matching profiles** and all matching profiles have not yet been reviewed:

Before due diligence:



After due diligence:

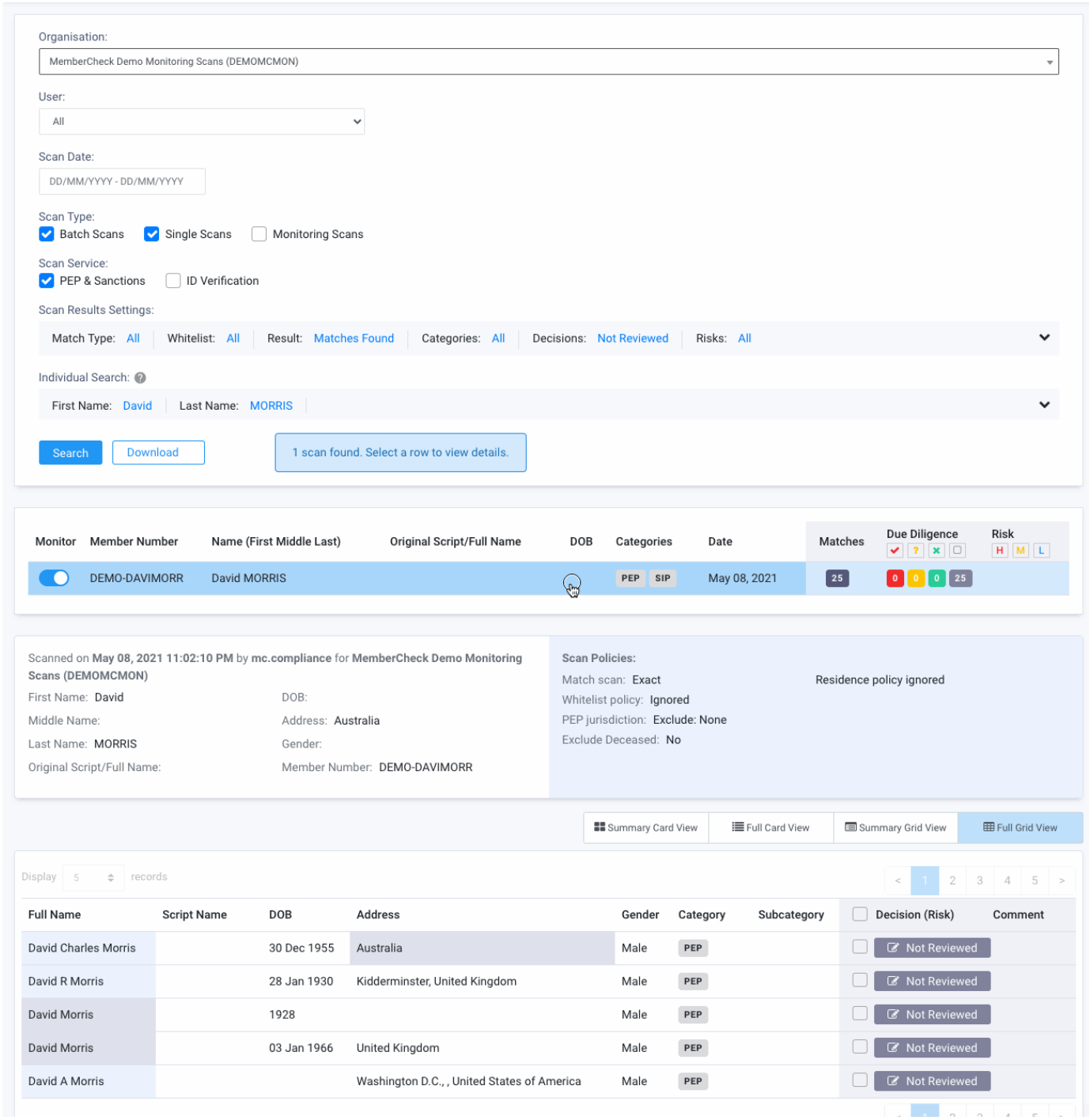


On completion of due diligence, this was found that **23 profiles are not true matches**, **1 profile cannot be certain of a match** and **1 matched profile**. The assessed risk level for this individual is considered **low risk**:

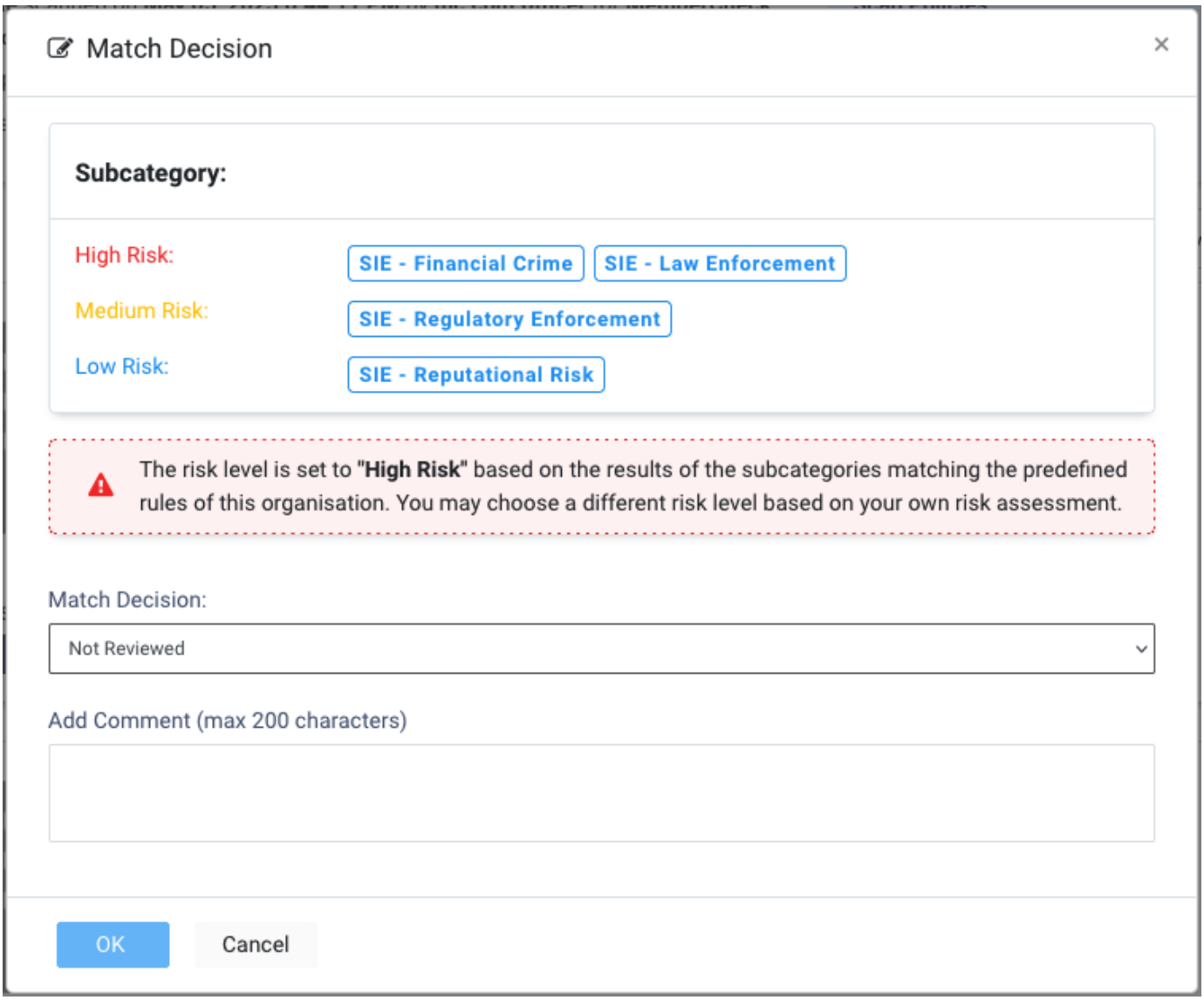
Add Due Diligence Decisions to Matched Profiles

Due diligence decisions, risk level assessments and comments can be applied to a single profile or multiple profiles at once.

You can also replace with a new decision against the profile by adding a new match decision. A history of the decisions will be retained for auditing purposes.



If your organisation has predefined risk levels set, the associated risk levels are displayed as a guideline with a recommended risk score. You may elect the risk level based on your own risk assessment.



The Compliance Officer can define the risk levels for the categories and subcategories within the Organisation administration screens. Refer to Risk Settings for details.

Supporting Documentation

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	✎	✎	✕	👁	👁

> ✎ **Data Entry Operator Permissions**
>
> **Data Entry Operators** have access to add supporting documents but are not able to view any of the scan results.

You can upload, and securely store and manage the necessary documentation for the source of funds (SoF) or source of wealth (SoW) of screened entities (PEP & Sanctions screening, ID Verification, and Know Your Business verification). This enables all necessary documents to be kept in a centralised, secure location, enhancing compliance and audit readiness.

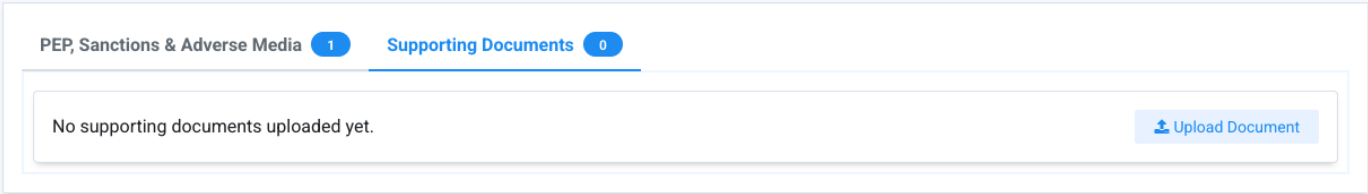
Supported file formats (size up to 5 MB):

- PDF
- JPG/JPEG
- PNG
- GIF
- TIF/TIFF

You can upload a ZIP of the above formats if your file size is too large.

Uploading Supporting Documents

You can upload **up to 10 documents** for a screened entity. The **Supporting Documents** tab is available from **Single Scan**, **Scan Results** and **Batch Scan Results** screens for both Individual and Corporate entities.



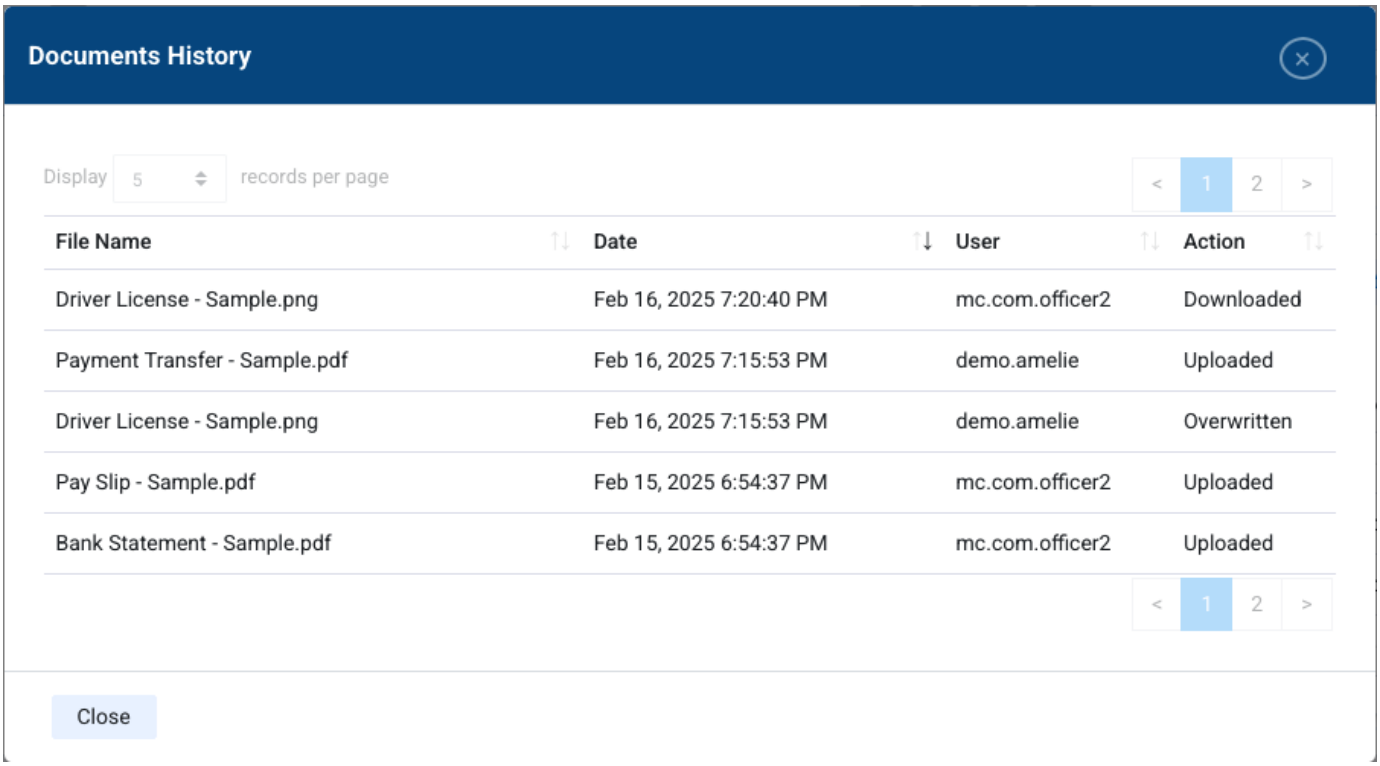
You can categorise the uploaded documents with one of the preset values such as `Proof of Identity`, `Proof of Address`, `Financial Statements` etc. for ease of identification.

If you or any of your team members attempt to upload a document with the same file name for the screened entity, the system will prompt for confirmation to overwrite the existing document.

Managing Supporting Documents

Uploaded documents can be previewed and downloaded based on your permission access rights.

You can view an audit history of supporting document activities through **Documents History** which include statuses for `Uploaded`, `Downloaded` , `Overwritten` and `Deleted`.



Deleting Supporting Documents

Uploaded documents can be deleted based on your permission access rights.

Important Note

Deleted or Overwritten documents cannot be restored

Documents that are deleted or replaced are permanent and cannot be restored.

Quick How-to Guides

Upload supporting documentation

Upload necessary documentation for Source of Funds (SoF) and Sources of Wealth (SoW) with the scanned entity for a centralised view for compliance and audit readiness.

Your browser does not support the video tag.

Manage Organisation and Suborganisations

Permissions

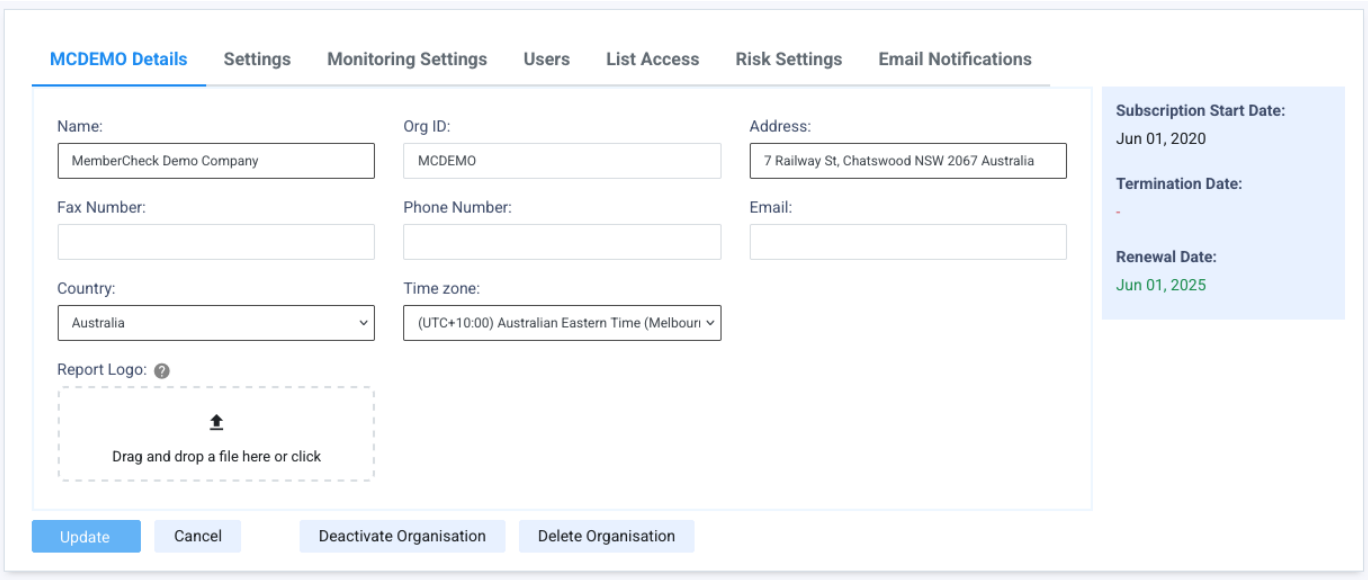
Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
✎	👁	✕	✕	✕	👁

The **Compliance Officer** can edit organisation and scan settings for their organisation and suborganisations. You may like to add multiple suborganisations under your parent organisation for different departments or for specific scan criteria and scope for PEP & Sanction screening.

Organisation Details

The **Details** tab allows you to view or edit the following details for the organisation selected from the **Organisation List**:

> **Reseller accounts**
>
> If you are a Compliance Officer of a reseller account, you have the ability to set and edit the subscription dates.



Field	Required	Character Limit	Description
Name	Mandatory	100	Legal name of the organisation. If you change the name of your parent organisation, please notify support@membercheck.com so that we can update our records.
Org ID	Mandatory	20	Unique identifier for the selected organisation. Your parent organisation Org ID will be assigned to you during enrolment. For suborganisations, you can assign your own Org ID or allow the system to automatically assign an Org ID. The **Org ID** is key to identifying the organisation you are scanning for in batch files and API requests.
Address	Mandatory	499	Address of the organisation or head office. Free format
Fax Number	Optional	50	Free format.
Phone Number	Optional	50	Free format.
Email	Conditional	125	Organisation email or email address to receive scan notifications if no Compliance Officer is assigned and no specific Notification Email Addresses are provided in **Email Notifications** tab.
Country	Mandatory	-	Country where the organisation is based. This affects the Time zone used for the organisation.

Time zone	Mandatory	-	Time zone is automatically set based on the selected **Country**, however it can be changed to cater for different regions with different time zone settings. This time zone will be used for all dates and times displayed for the organisation, with the exception of the Activity Report, which is based on Australian Eastern Standard/Daylight Saving Time (UTC +10/11). Time zone is displayed against the **Last Login** date and time on the MemberCheck banner, for reference For users that are assigned to an organisation belonging to a group of organisations with different time zones, the time zone displayed against the **Last Login** date and time will be that of the group's parent organisation.
Report Logo	Optional	-	An organisation logo can be uploaded to be included for display in exported reports (PDF, Excel, Word). Supported formats: `gif`, `jpg` and `png`. Maximum logo dimensions (pixels): `150` width, `100` height. Maximum file size: `100 KB`.

Scan Settings

The default `User Defined` option enables the users to select the scan criteria prior to scanning and offers the greatest flexibility.

MCDEMO Details | Settings | Monitoring Settings | Users | List Access | Risk Settings | Email Notifications

Batch Setting

Batch Validation

(•) On ( ) Off

Individual Scan Settings

Default Name Match Type:

( ) Exact ( ) Exact (Incl. Middle Name) ( ) Close

(•) User Defined

Close Name Match Rate (%):

( ) ≥ 80 (•) User Defined (defaults to 80%)

Whitelist Policy:

( ) Apply ( ) Ignore (•) User Defined

Country of Residence Policy:

[ ] Apply to All [ ] Apply to PEP [ ] Apply to POI

[ ] Apply to RCA [ ] Apply to SIP (incl. TER) [ ] Ignore

[x] User Defined

Default Country of Residence/Operation:

Apply Country of Residence to Blank Addresses:

( ) Yes ( ) No (•) User Defined

PEP Jurisdiction Policy:

( ) Apply ( ) Ignore (•) User Defined

PEP Jurisdiction Countries:

(•) Exclude from screening:

( ) Include in screening:

Exclude Deceased Persons:

( ) Yes ( ) No (•) User Defined

Web Search:

Note: Applies to Single Scans only

( ) Yes ( ) No (•) User Defined

Advanced Media Search:

Note: Applies to Single Scans only

( ) Yes ( ) No (•) User Defined

FATF Jurisdiction Risk:

( ) Yes ( ) No (•) User Defined

Corporate Scan Settings

Default Name Match Type:

( ) Exact ( ) Close (•) User Defined

Close Name Match Rate (%):

( ) ≥ 80 (•) User Defined (defaults to 80%)

Whitelist Policy:

( ) Apply ( ) Ignore (•) User Defined

Country of Operation Policy:

( ) Apply to All ( ) Ignore (•) User Defined

Default Country of Operation:

N/A

Apply Default Country to Blank Addresses:

( ) Yes ( ) No (•) User Defined

Web Search:

Note: Applies to Single Scans only

( ) Yes ( ) No (•) User Defined

Advanced Media Search:

Note: Applies to Single Scans only

( ) Yes ( ) No (•) User Defined

FATF Jurisdiction Risk:

( ) Yes ( ) No (•) User Defined

Stopwords (comma-separated): Reset to Default

Incorporated, Proprietary Limited, Private Limited, Pty Ltd, Pte Ltd, Limited Liability Company, Public Limited Company, Public Company Limited, Public Limited, Aktiebolag, Anpartsselskab, Sociedad de Responsabilidad Limitada, Societa A Responsabilita Limitata, Société à Responsabilité Limitée, Gesellschaft mit beschrankter Haftung, Aktiengesellschaft, Societe Anonyme, Sociedad Anonima, Sendirian Berhad, Sdn Bhd, Berhad, Kabushiki Kaisha, Joint Stock Company, Open Joint Stock Company, Open Joint-Stock Company, Private Limited Company, Company Private Limited, Company (Private) Limited, Co Ltd, S.R.L., S.A.R.L, SARL, SP. z o.o., SA/NV, NV/SA, LLC, PLC, Kft, Ltda, Ltd, PAO, CJSC, PJSC, DMCC, FZCO, FZE, BV, AB, AG, ApS, SIA, d.o.o., Oü, Oy, K.K.

Limit Scan results (1-200):

Exact Match: 100 Close Name Match: 200

IDV Scan Settings

[x] Enable Global FaceMatch

Batch Setting

Field	Required	Description
Batch Validation	Mandatory	A setting that determines if batch file validation is performed prior to scanning. Options are: `On` - Default. Any batch file with incorrect formatting or containing invalid data will be rejected and the batch scan will show an error, and a status of the Error will be displayed against the scan in the Batch Scan History. `Off` - Any batch file with incorrect formatting or containing invalid data will be accepted and the batch scan will be completed by ignoring the incorrectly formatted or invalid data.

Individual Scan Settings

Setting options to `User Defined` enables the user or API client to specify their preference during screening.

Field	Required	Description

Default Name Match Type	Mandatory	A setting that defines the default name match type across the organisation for all sc The options are `Exact`, `Exact (Including Middle Name)`, `Close` or `User Defined` **Exact** Scan results show matches where the First and Last Name match exactly. Middle na Middle Name matching does not eliminate watchlist entities with no middle name. S • The First and Middle and Last Name match exactly. • The First and Last Name match exactly and the watchlist record Middle Name c • The First and Last Name match exactly and the watchlist record has no Middle N • The First and Last Name match exactly and the Middle Name does not match. **Exact (Including Middle Name)** • The First and Middle and Last Name match exactly. • The First and Last Name match exactly and the watchlist record Middle Name c • The First and Last Name match exactly and the watchlist record has no Middle N **Close** • The First Name and Last Name match based on a phonetic matching algorithm Names are ignored.

Close Name Match Rate	Mandatory	Applicable for Close name matches only. Improves relevance of scan results by setti threshold. Options are: `1 - 100` % - Refines the scan results to display only name matches with a match rate entered. Accepted values are between 1 and 100. `User Defined` - Default. The user can specify a threshold at the time the scan is per equal to 80% if no value is entered. Example: The name `John` at various thresholds: • **100%**: `John` . • **80%**: `John` , `Johnnie` , `Johnny` . • **50%**: `John` , `Johnnie` , `Johnny` , `Jon` , `Joan` , `Jonah` , `Jean` , `Jan` , `Joanne` , `Joanna` • **1%**: `John` , `Johnnie` , `Johnny` , `Jon` , `Joan` , `Jonah` , `Jean` , `Jan` , `Joanne` , `Joanna` , `Jayne` , `Juan` etc.
Whitelist Policy	Mandatory	A setting that ensures previous due diligence decisions, i.e, an individual is determin into account in future scans. Therefore, previous match results will not be returned a Options are: `Apply` - Watchlist entity matches previously classified as No Match are excluded fro `Ignore` - All watchlist entities matching the scanned individual are displayed. Previo shown.

Country of Residence Policy	Mandatory	A setting, for individual scans, which allows matches to be ignored if the individual's that of the matching watchlist entity. This rule can be applied to selected category m Options are: `Apply to All` - All watchlist entity matches where the individual's Country of Reside locations are excluded from the scan results. This includes `Apply to PEP`, `Apply t` settings. `Apply to PEP` - PEP (Politically Exposed Persons) watchlist entity matches where th different to the PEP's locations are excluded from the scan results. `Apply to RCA` - RCA (Relatives or Close Associates) watchlist entity matches where the RCA's Country of Residence are excluded from the scan results. `Apply to SIP (incl. TER)` - SIP (Special Interest Person) watchlist entity matches Residence is different to the SIP's locations are excluded from the scan results. `Ignore` - Country of Residence Match Policy is not applied.

Default Country of Residence	Mandatory	Used for nominating a Country of Residence for the individual's address where a cou To utilise the Country of Residence Policy, a country needs to be identified in the mer addresses, which are not blank but do not contain an identifiable country, if a **Default** nominated, it will be automatically assigned to the member as the Country of Reside For **MemberCheck users outside Australia**, selecting a **Default Country of Residence** to the address of a member where a country does not already exist in the member's r For **Australian MemberCheck users**, selecting `Australia` as the **Default Country of** Country of Residence to member addresses that do not contain a `State` or "Australi The default setting is `Not specified`, which has no impact on member scans.  Default Country of Residence should be set once and not changed as no record i  Only a Compliance Officer can select a **Default Country of Residence**, it cannot
Apply Country of Residence to Blank Addresses	Mandatory	Used in conjunction with **Country of Residence Policy** and **Default Country of Reside** Default Country of Residence is used where Member addresses are blank during PEF Including a Country of Residence during PEP and Sanction scans helps to eliminate a provides a catchall if Member addresses do not contain any information. Options are: `Yes` - Applies specified Default Country of Residence for all blank Member addresse `No` - No changes to blank Member addresses.

PEP Jurisdiction Policy	Mandatory	This setting determines whether to exclude or include PEPs and their RCAs based or specified exclusion or inclusion list. The default which is set by the scanning organisation's Compliance Officer is `Exclud` specified in **Exclude from screening** field). Options are: `Apply` - Exclude or include PEPs and RCAs based on defined **PEP Jurisdiction Coun** `Ignore` - Disregard jurisdiction-based exclusions or inclusions for PEPs and RCAs. `User Defined` - Allow users to choose whether to apply jurisdiction-based exclusion them. If no country is defined in **PEP Jurisdiction Countries** in the fields below, this is t
PEP Jurisdiction Countries	Optional	Options are: • **Exclude from screening**: Allows you to specify countries to exclude from the sca domestic PEPs. • **Include in screening**: Allows you to specify countries to include within the scan r Your obligations under the appropriate AML/CTF or AMC/CFT legislation should dete choose to explicitly include or exclude. To apply the PEP Jurisdiction policy to explicitly include or exclude the defined c the **Residence Policy** should be unchecked, as this will override the PEP Jurisdiction return PEP and RCA profiles that match the country defined during screening.

Exclude Deceased Persons	Mandatory	Allows you to specify if deceased persons are to be excluded from the scan results. Options are: `Yes` - exclude profiles where the person is tagged as deceased. `No` - include profiles where the person is tagged as deceased.
Web Search	Mandatory	Allows you to specify if a search on the Google search engine should be included dur Options are: `Yes` - run a web search during screening. `No` - do not include a web search. This is the default setting.
Advanced Media Search	Mandatory	Allows you to specify if an advanced search for the latest news articles should be inc Options are: `Yes` - run a search on articles during screening. `No` - do not include the search. This is the default setting.
FATF Jurisdiction Risk	Mandatory	Allows you to specify if a jurisdiction search which includes technical compliance an recommendations, should be included during screening. Options are: `Yes` - run a jurisdiction risk check during screening. `No` - do not include the risk check. This is the default setting.

Original Script/Full Name Search	Mandatory	A setting, which when turned `On`, provides an additional **Original Script Name** or **Full** allow single and batch scanning of a person's name in its original script (e.g. Arabic, Japanese, Thai and other non-Latin/Roman scripts). Options are: `On` - Name matching is performed based on **First** and **Middle** and **Last Name** and **Or** `Off` - Name matching is performed based on **First** and **Middle** and **Last Name**.
Ignore Blank DOB Policy	Mandatory	A setting, which when turned `On`, enforces DOB to be entered during screening and a entity does not have a DOB to be eliminated. Options are: `On` - Eliminates match results where the date of birth is blank for either the member When this option is `On`, a watchlist entity that could be a true match may be eliminat of birth. `Off` - DOB is optional. If a valid Date of Birth (DD/MM/YYYY) is entered, the Scan Re incomplete or no Date of Birth.
Ignore Blank Nationality	Mandatory	A setting, which when turned `On`, enforces nationality to be entered during screening watchlist entity does not have a nationality to be eliminated. Options are: `On` - Eliminates match results where the nationality or citizenship is blank for the me When this option is `On`, a watchlist entity that could be a true match may be eliminat information. `Off` - Default. Nationality is optional during screening. Results will include profiles m well as no known nationality to minimise potential match exclusions.

DOB and YOB Tolerance (Years)	Mandatory	A setting which allows for date of birth variations in the results returned with a tolera individual's date of birth. Enabling this variation will ignore the specific day and mont against the year only. Supports a maximum of `9` years of variation. Options are: `On` - preset allowance of [X] years variation. This will be applied during screening an `Off` - No variation allowed. `User Defined` - the tolerance setting can be enabled and adjusted during screening. This is turned off by default.
Limit Scan Results	Mandatory	Set limits on the maximum number of scan results returned for `Exact` and `Close` n Defaults to `100` for Exact name match type and `200` for Close name match type. Ac

Corporate Scan Settings

Field	Required	Description
Default Name Match Type	Mandatory	A setting that defines the default name match type across the organisation for all sc Options are: `Exact` - The corporate data entered into the system will only result in a match shoul `Close` - The corporate data entered into the system will result in a match should the

Close Name Match Rate	Mandatory	Applicable for Close name match type only. Adjust relevance of scan results by settir (somewhat similar sounding name). Options are: Match rate - Define the closeness of name matching. Scan results will return matche `100` . Setting this rate will apply to all scans performed within the organisation accou `User Defined` - Default. The user can specify a threshold at the time the scan is per value is entered. Example 1: The name `Greenoil` at various thresholds with the variations returned: • **100%**: `Greenoil` • **80%**: `Greenoil` • **50%**: `Greenoil` , `Greenwill` , `Greenlay` , `Greenhill` • **30%**: `Greenoil` , `Greenwill` , `Greenlay` , `Greenhill` , `Greenall` , `Greenhall` , `Gr` • **10%**: `Greenoil` , `Greenwill` , `Greenlay` , `Greenhill` , `Greenall` , `Greenhall` , `Gr` `Cornwall` etc Example 2: The name `Bayer` at various thresholds: • **100%**: `Bayer` • **80%**: `Bayer` • **50%**: `Bayer` , `Baer` , `Payeer` • **30%**: `Bayer` , `Baer` , `Payeer` , `Bauer` , `Beyer` , `Bower` , `Buyer` , `Beer` , `Veier` etc

Whitelist Policy	Mandatory	A setting that ensures previous due diligence decisions, i.e, a member is determined will not be returned as a match. Options are: `Apply` - Member and watchlist entity matches previously classified, after due diligen `Ignore` - All watchlist entities matching the scanned member are displayed. Previou
Country of Operation Policy	Mandatory	A setting which allows matches to be ignored if the corporate entity's Country of Ope Options are: `Apply to All` - All watchlist entity matches where the corporate's Country of Operat `Ignore` - Country of Operation Match Policy is not applied.
Apply Default Country to Blank Address	Mandatory	Used in conjunction with **Country of Operation Policy** and **Default Country of Operati** country locations are blank during screening. Including a Country of Operation helps to target and filter relevant results. This optior Options are: `Yes` - Applies specified Default Country of Operation for all blank addresses during s `No` - No changes to blank Corporate addresses.

Web Search	Mandatory	Allows you to specify if a search on the Google search engine should be included dur Options are: `Yes` - run a web search during screening. `No` - do not include a web search. This is the default setting.
Advanced Media Search	Mandatory	Allows you to specify if an advanced search for the latest news articles should be inc Options are: `Yes` - run a search on articles during screening. `No` - do not include the search. This is the default setting.
FATF Jurisdiction Risk	Mandatory	Allows you to specify if a jurisdiction search which includes technical compliance an Options are: `Yes` - run a jurisdiction risk check during screening. `No` - do not include the risk check. This is the default setting.
Stopwords	Optional	List of words or phrases to be ignored for Corporate scans. By default, this contains The system default is available if you choose to use this, or customise this to cater t On occasion, we may update the system default to improve the searchability for our on **Reset to Default**.

Limit Scan Results	Mandatory	Set limits on the maximum number of scan results returned for `Exact` and `Close` n Defaults to `100` for Exact name match type and `200` for Close name match type. Ac

> **Customisation of company stopwords**
>
> When customising your company or entity stopwords, be careful not to include common words or suffixes which may also form part of an organisation name, as this may return more results for matches which are irrelevant.

Watchlists Settings

Field	Required	Description
Select Watchlist Categories	Mandatory	A setting which when turned `On`, enables users to customise the scope of screening from the list of selected watchlist categories when performing a new scan. Options are: `Yes` - Default. Allows the user to change the watchlist categories for new scans. `No` - Watchlist categories cannot be changed during screening.

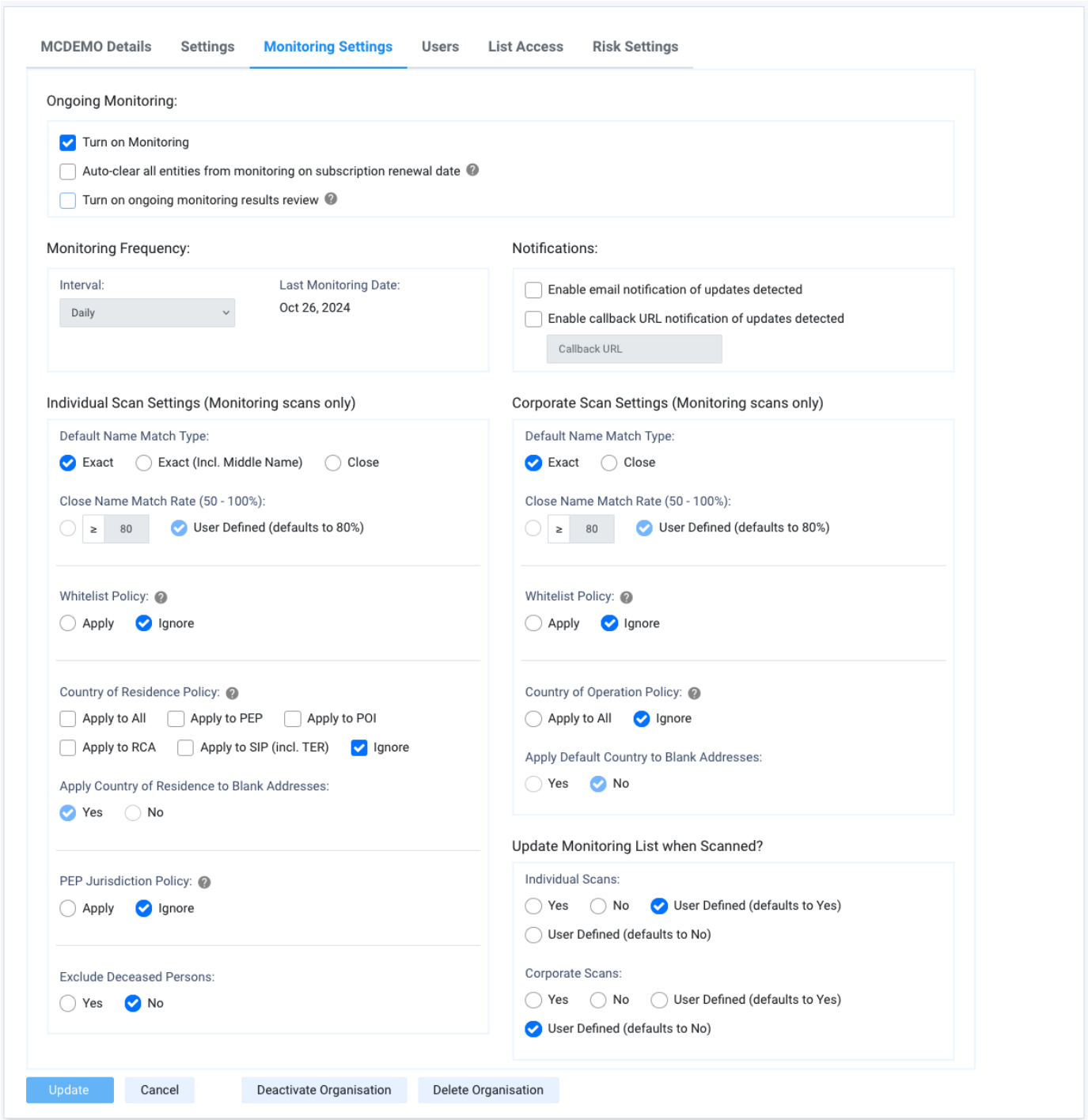
IDV Scan Settings

Field	Required	Description

Enable Global FaceMatch	Optional	Disable or enable the global FaceMatch screening (biometric facial matching against government-issued documents). By default, this option is enabled if your organisation is subscribed to the IDV service. Turning this off will verify identities using ID Check only (verification against official and commercial sources at the following **list of supported countries**. If you would like to verify using the global FaceMatch only, please reach out to your Account Manager or Support.
Available Countries	Read only	A list of countries enabled for your organisation for ID Verification. This list of verification sources applies to all suborganisations and cannot be customised.
Default Country	Optional	Set a default country if you would like a pre-selected country to appear in the field **Country of Verification** in **Single Scan**. This provides a pre-selected value, but does not restrict the user from selecting a different country for verification. This may be useful if the majority of the verification sources are the same.

Monitoring Settings

Define scan setting options for ongoing monitoring. These can be set to be the same as **Settings** or adjusted to cater for variations depending on your organisation's AML/CTF obligations.



Some additional features to note:

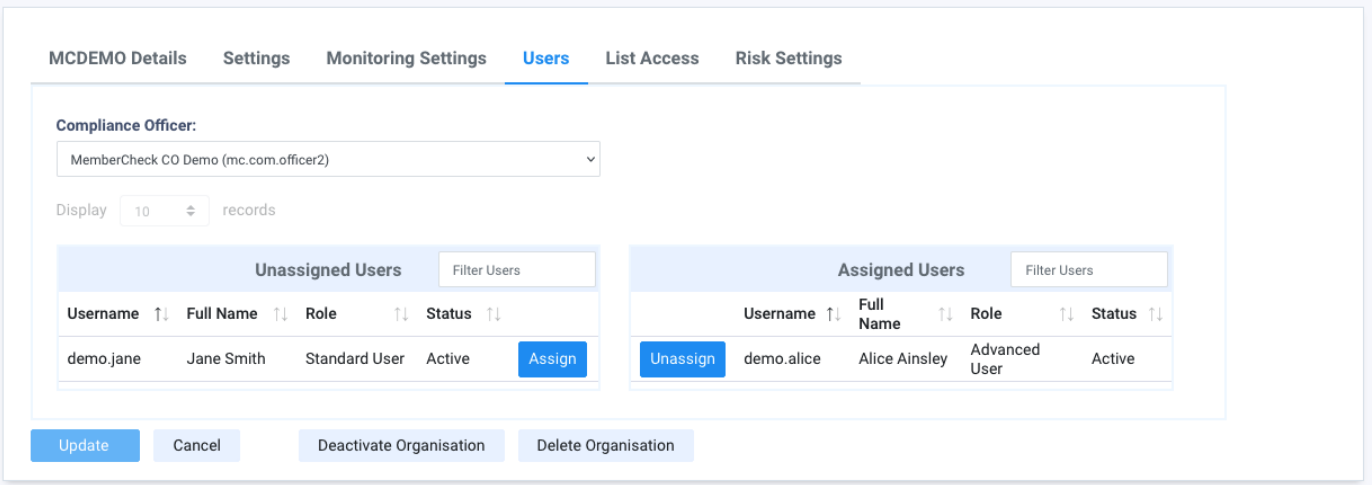
Field	Description
Turn on Monitoring	Check this option to enable ongoing monitoring for your organisation. This is not checked by default.

Auto-clear all entities from monitoring on subscription renewal date	On the first day of subscription renewal, all active entities in the Monitoring List are rescanned. Check this option to automatically clear all entities from the Monitoring List on the first day of subscription renewal. This is not checked or enabled by default.
Turn on ongoing monitoring results review	Check this option to enable tracking of ongoing monitoring review within Monitoring Results screens. This is not checked or enabled by default.
Monitoring Frequency	Displays the preset interval for ongoing monitoring for your organisation account and the date the process was last run. These values are read-only and can be: `Daily`, `Weekly`, `Fortnightly`, `Monthly`, `Quarterly` and `Semi Annually`. To change the interval to reduce the frequency of ongoing monitoring, please contact your Account Manager or MemberCheck Support.
Enable email notifications of monitoring updates	Check this option to receive email notifications if changes are detected in the watchlist which may affect monitored individuals and or companies. Emails will be sent to the Compliance Officer or Organisation Email. This is not checked or enabled by default.
Last Monitoring Date	Displays the date the ongoing monitoring was last run for the organisation or suborganisation account.
Enable callback URL notification of updates detected	Check this option to receive API notifications if changes are detected in the watchlist which may affect monitored individuals and or companies. The specified callback URL must be available via GET method without authentication. For detailed usage of the callback URL, refer to **FAQ** This is not checked or enabled by default.

Update Monitoring List for New Individual Scan	Preference for adding new individual scans (single, batch and API) to the Monitoring List. Options are: `Yes` - Automatically add all scans to the Monitoring List. Users are not able to change this option during scans. `No` - Do not add scans to the Monitoring List. Users are not able to change this option during scans. `User Defined (defaults to Yes)` - Add scans to the Monitoring List. User is able to change this before running a scan, batch scan or via API request. `User Defined (defaults to No)` - Do not add scans to the Monitoring List. User is able to change this before running a scan or batch scan or via API request.
Update Monitoring List for New Corporate Scan	Preference for adding corporate scans (single, batch and API) to the Monitoring List. Options are: `Yes` - Automatically add all scans to the Monitoring List. Users are not able to change this option during scans. `No` - Do not add scans to the Monitoring List. Users are not able to change this option during scans. `User Defined (defaults to Yes)` - Add scans to the Monitoring List. User is able to change this before running a scan, batch scan or via API request. `User Defined (defaults to No)` - Do not add scans to the Monitoring List. User is able to change this before running a scan or batch scan or via API request.

Users

The **Users** tab allows you to view or edit the following details, for the organisation selected from the **Organisation List**.



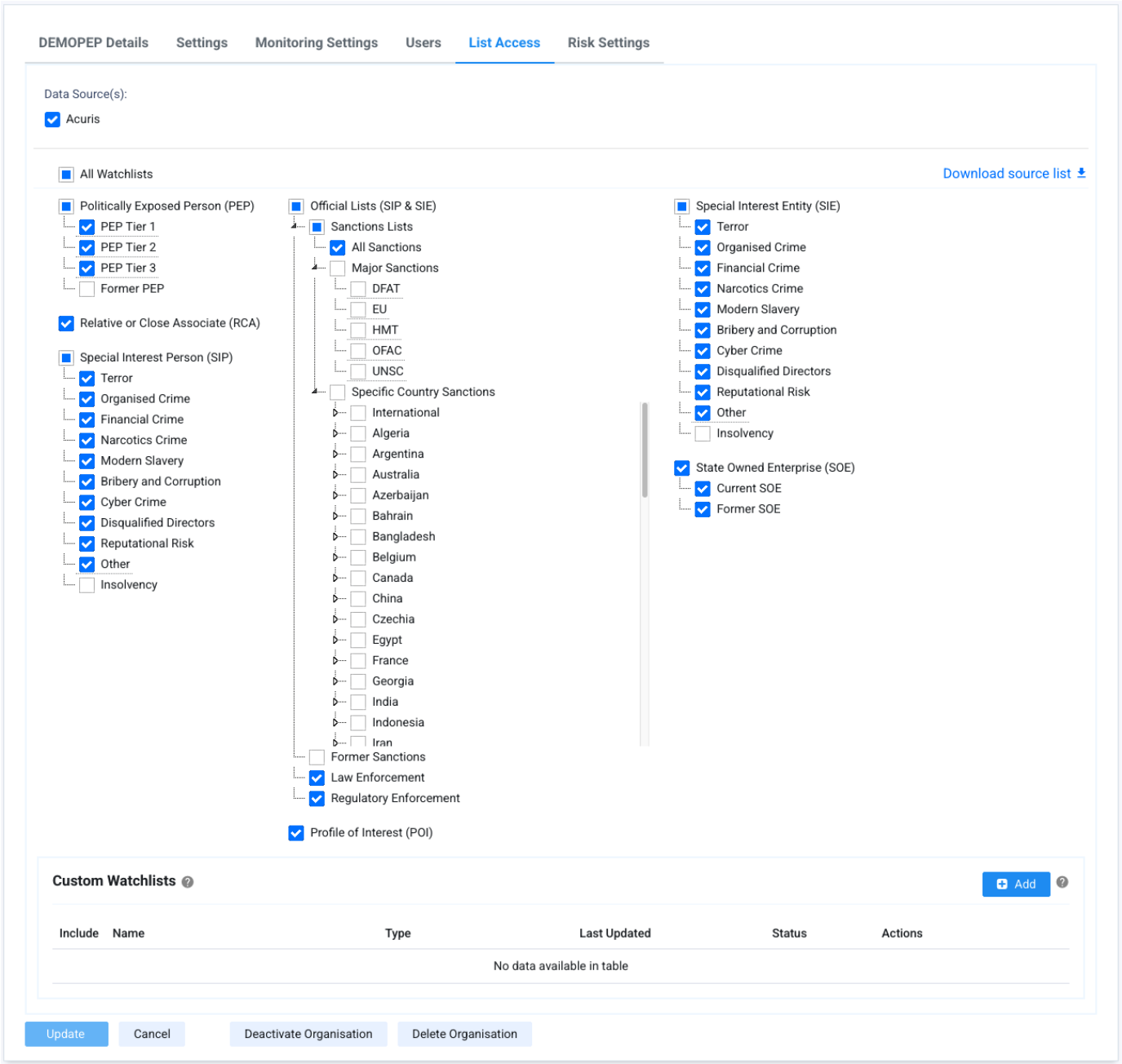
Field	Description
Compliance Officer	Name of the assigned Compliance Officer for the selected Organisation. Compliance Officers in suborganisations are also available for selection in the list.
Unassigned Users	List of users associated with the primary organisation which are not assigned to the selected organisation or suborganisation.
Assigned Users	List of users assigned to the selected organisation or suborganisation.

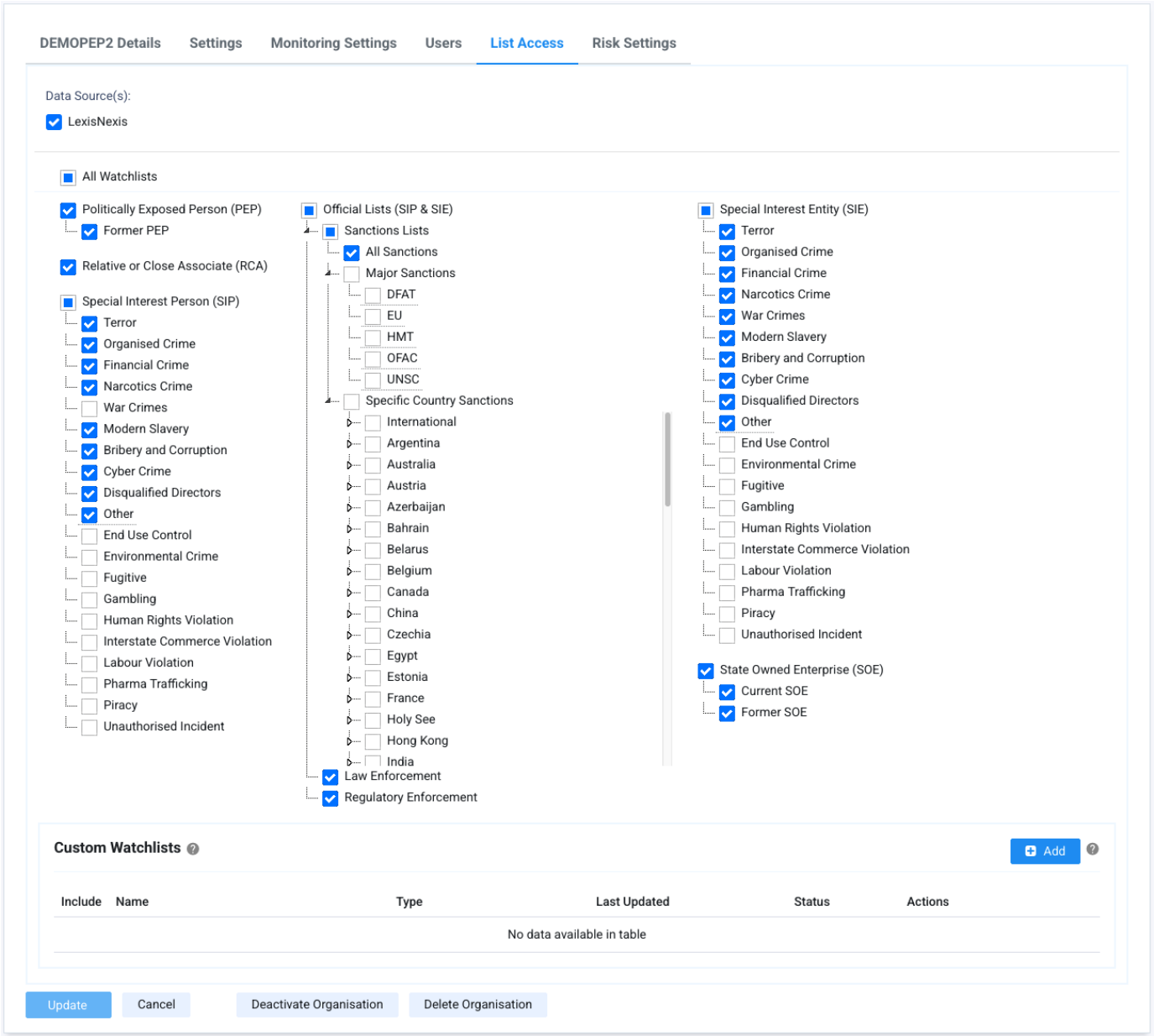
List Access

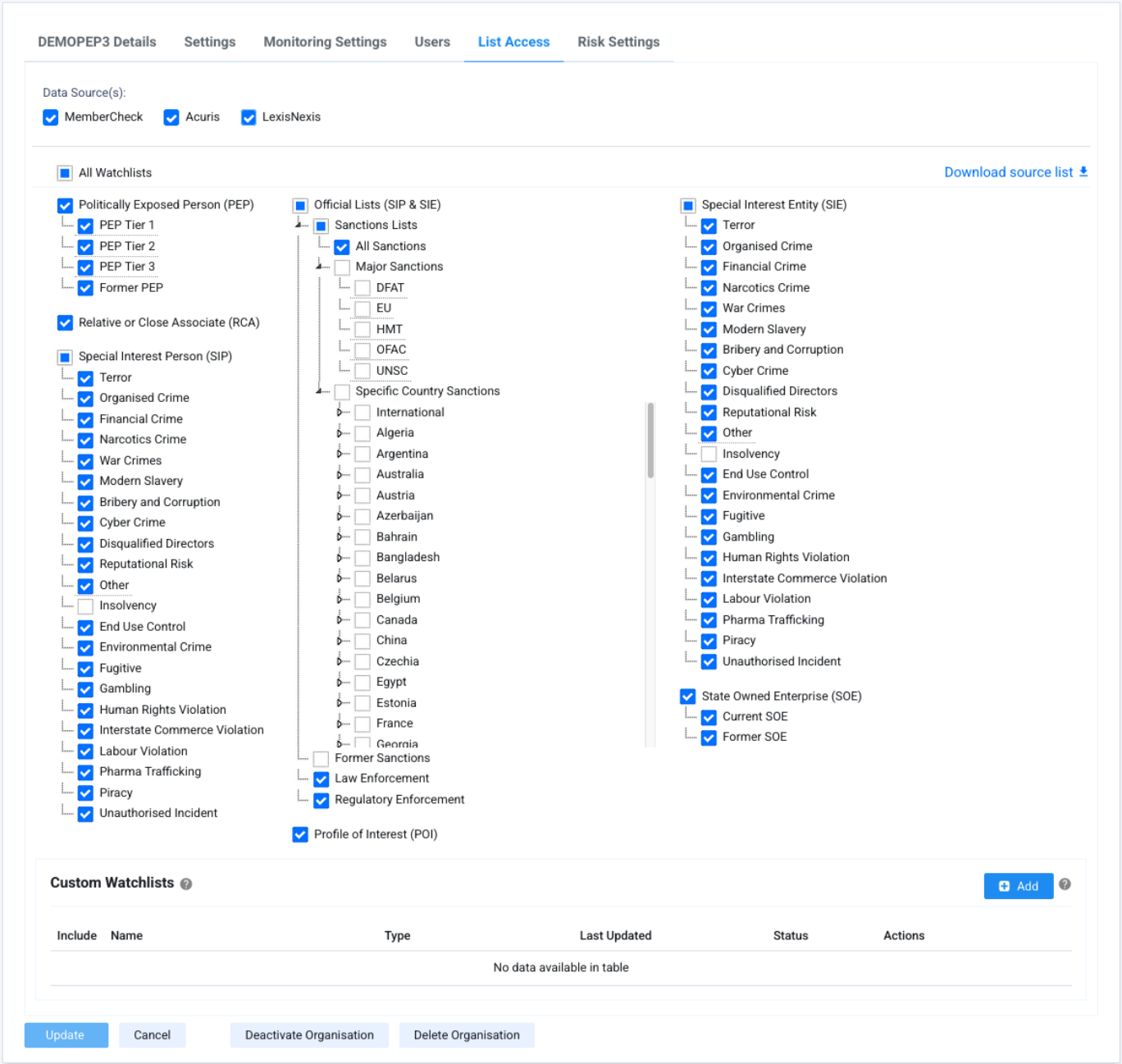
The **List Access** tab enables you to view and configure the scope of PEP and Sanctions screening for the chosen organisation or suborganisation.

You can tailor the screening scope at both the category and subcategory levels, including specific country sanctions lists or major international sanctions lists, and specific sanctions lists by country. These settings can be independently configured for different suborganisations.

Examples of the standard setup for organisations based on the selected data source:







Refer to List Categories for a full list of the definitions of all the main categories and subcategories available in the system. Your subscription may provide access to some and not all of these categories and subcategories.

A detailed list of sources utilised in the system for Sanctions, Regulatory Enforcement and Law Enforcement are available for your download and reference via **Download source list** on this screen.

Custom Watchlists

You can include any specific watchlists or blacklists for your organisation to extend the PEP and Sanction screening.

For details on adding your own lists, refer to **Manage Custom Watchlists**

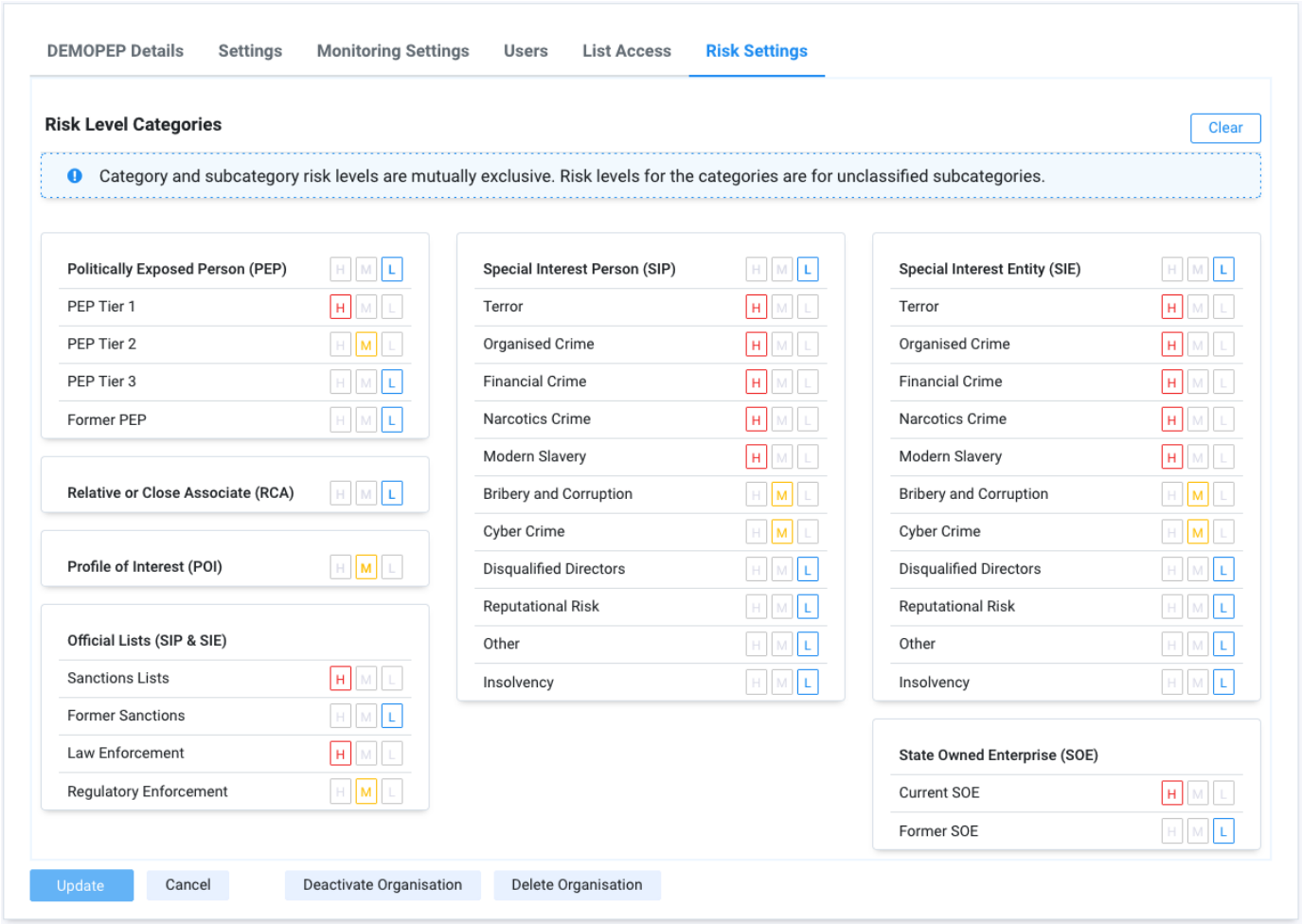
Risk Settings

The **Risk Settings** tab enables you to standardise risk levels for PEP and Sanction categories and subcategories across your organisation.

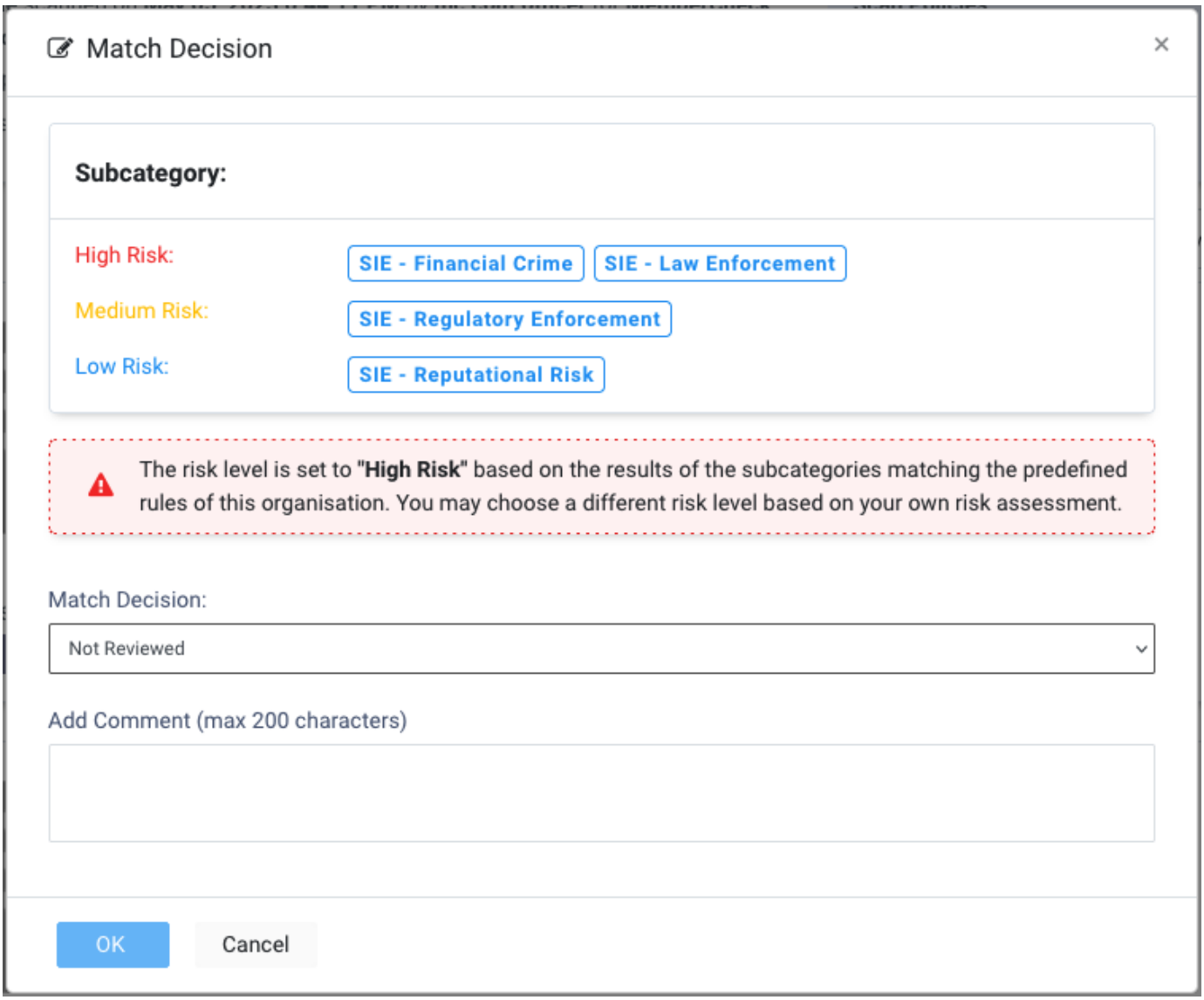
Set `High`, `Medium` or `Low` risk levels for any combination of categories and subcategories. These pre-defined levels are then displayed as recommended risk scores during due diligence workflows, but are not enforced.

Category risk levels apply to any unclassified subcategories under them. However, an explicitly set subcategory level takes precedence over its parent category level.

The overall risk score shown reflects the highest associated category/subcategory level for that profile.



An example of how this would be viewed within the scan result due diligence workflow:



Email Notifications

The **Email Notifications** tab enables you to configure how your Organisation receives email notifications from the MemberCheck system. Tailoring these notifications ensures that the relevant personnel are informed about specific events according to your Organisation's needs.

Field	Description

Send Notification Emails to	Opt to send system email notifications to the assigned Compliance Officers, or specify the email addresses designated to receive the system notifications. You can add up to five distinct email addresses. This address field is separate from the primary Organisation Email address. Emails will be sent to the designated Compliance Officer(s). If specific Notification Email Addresses are provided, they will be used. If no Compliance Officer is assigned and no Notification Email Address(es) have been specified, notifications will be sent to the Organisation Email address as a backup.
Email Preferences	List of events that trigger emails from the system. Some events are not able to be switched off as these are important information affecting the Organisation's subscription, and have been listed here for reference.

Daily limit for Single Scan emails

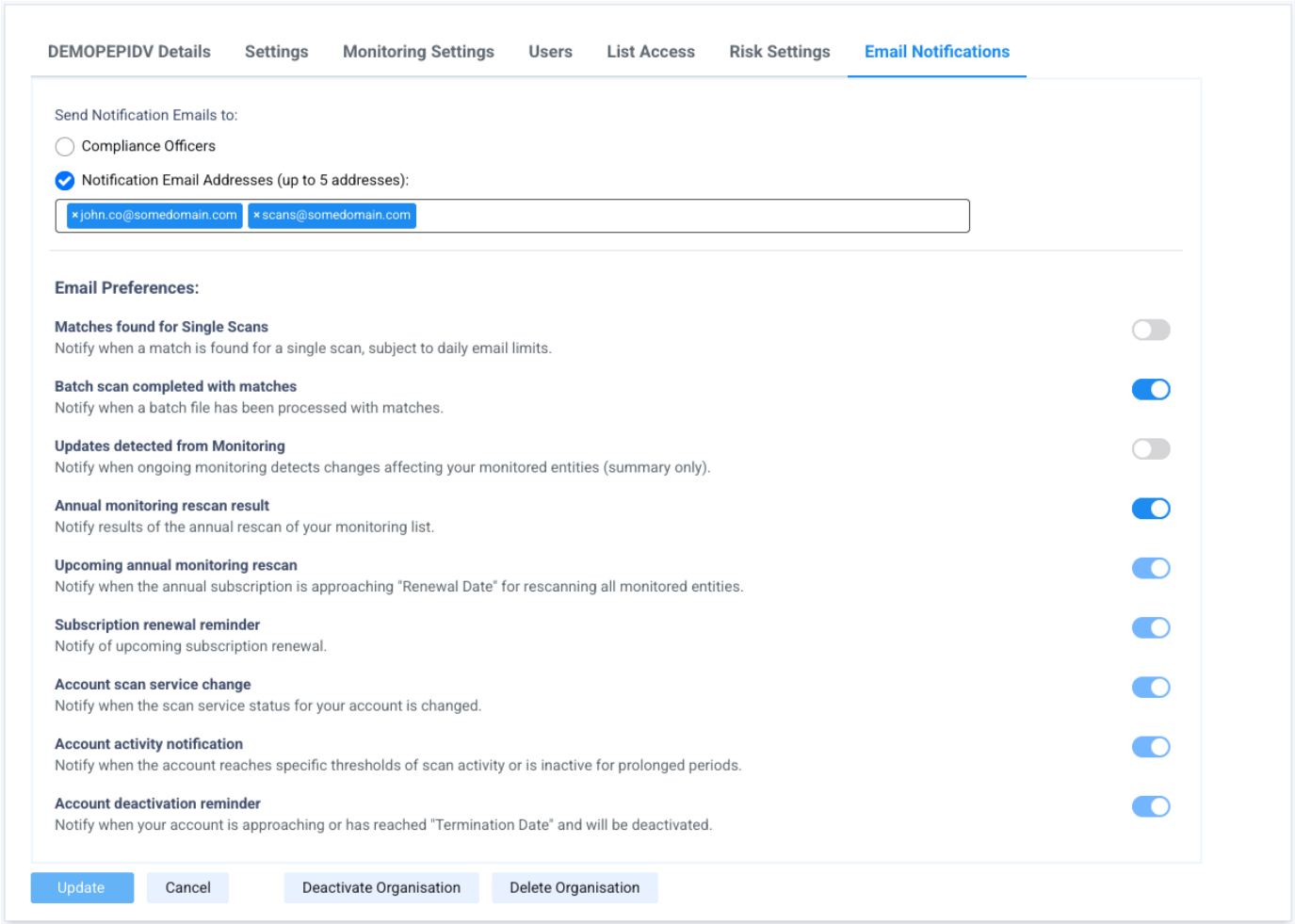
Please note that a daily email quota applies per Organisation for **Single Scans** to ensure that you receive important notifications without potential interruption from email providers or being overwhelmed by emails.

The daily quota is `100` emails, but may be adjusted based on the load and usage.

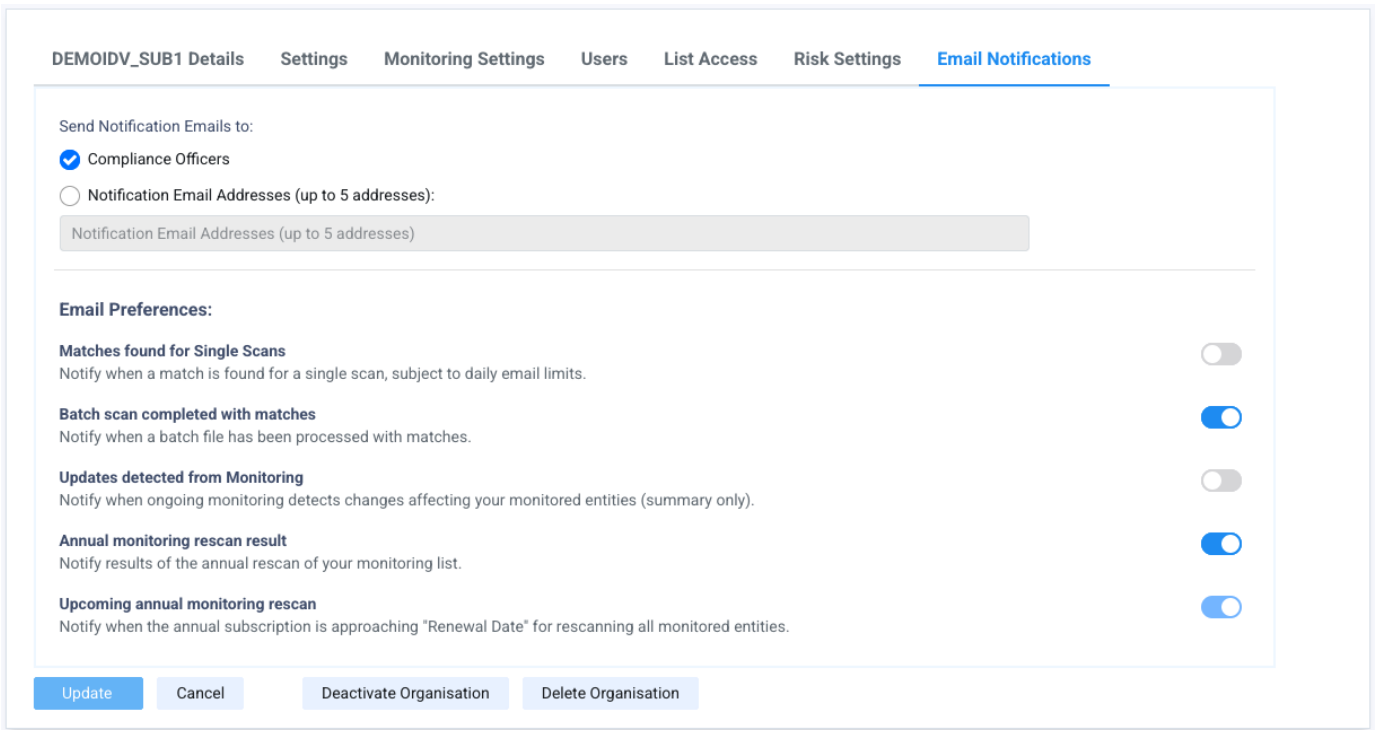
System Email Information

Please be aware that users will receive emails triggered automatically by the system for important events such as subscription renewal reminders, monitoring rescan reminders, password resets, and other critical system communications necessary for service operation and account management.

Email notification settings for a root parent organisation:



Email notification settings for a suborganisation organisation:



Deactivate Organisation

For organisations that are no longer used but require retention of historical scan results and reports, you may deactivate the suborganisation or organisation. Deactivated organisations remain accessible for historical information but will not allow new scans or monitoring.

> **Users must be assigned to at least 1 active organisation**
>
> Please note that all users must have at least 1 active organisation assigned to their account to access MemberCheck.

Delete Organisation

For unused organisations and suborganisations without historical scans, you can deactivate or delete them.

To delete organisations with historical data, run Data Management to erase it first. Reassign or unassign all users associated with the organisation or suborganisation before deleting the account. For security, only organisations with no users or historical data can be deleted.

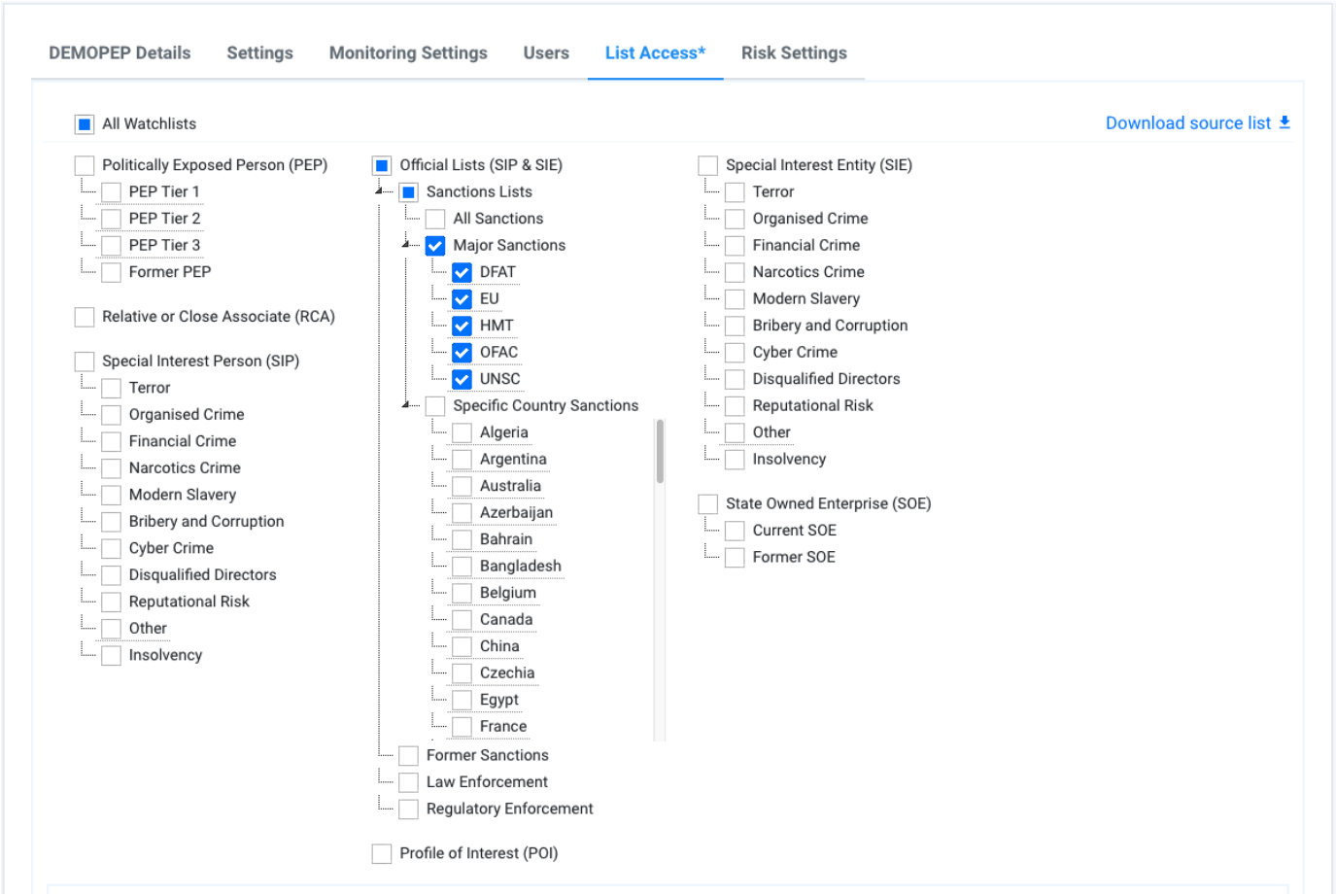
Deleted accounts cannot be restored.

> **Users must be assigned to at least 1 active organisation**
>
> Please note that all users must have at least 1 active organisation assigned to their account to access MemberCheck.

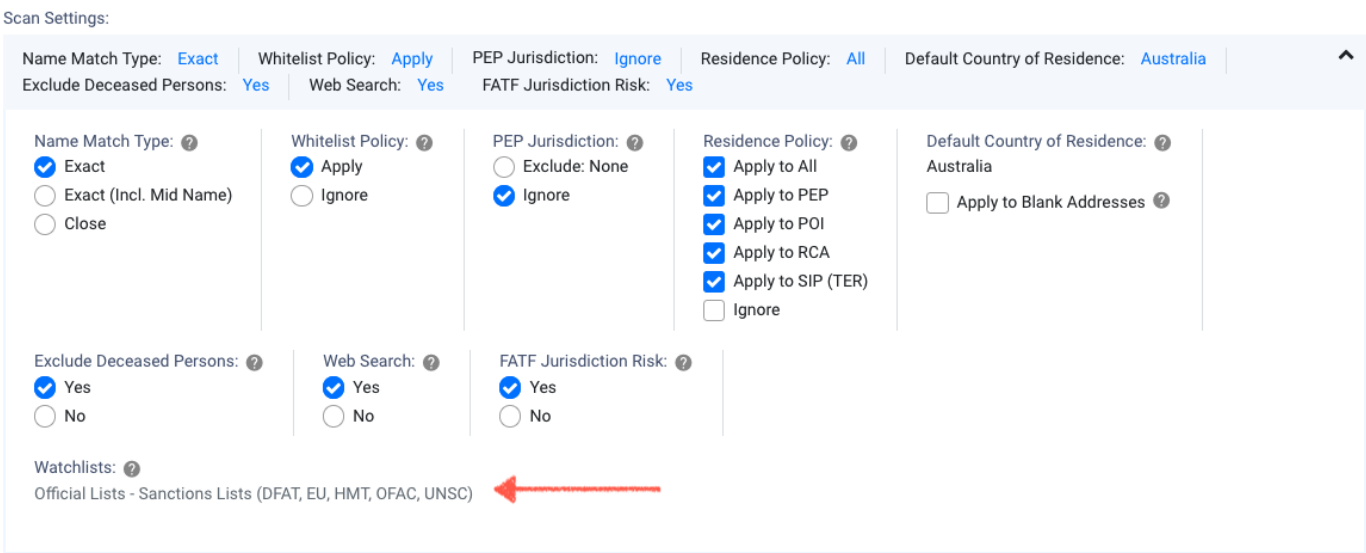
Quick How-To Guides

Screen against major sanctions lists only

Example of List Access setup to screen against the major sanctions only.

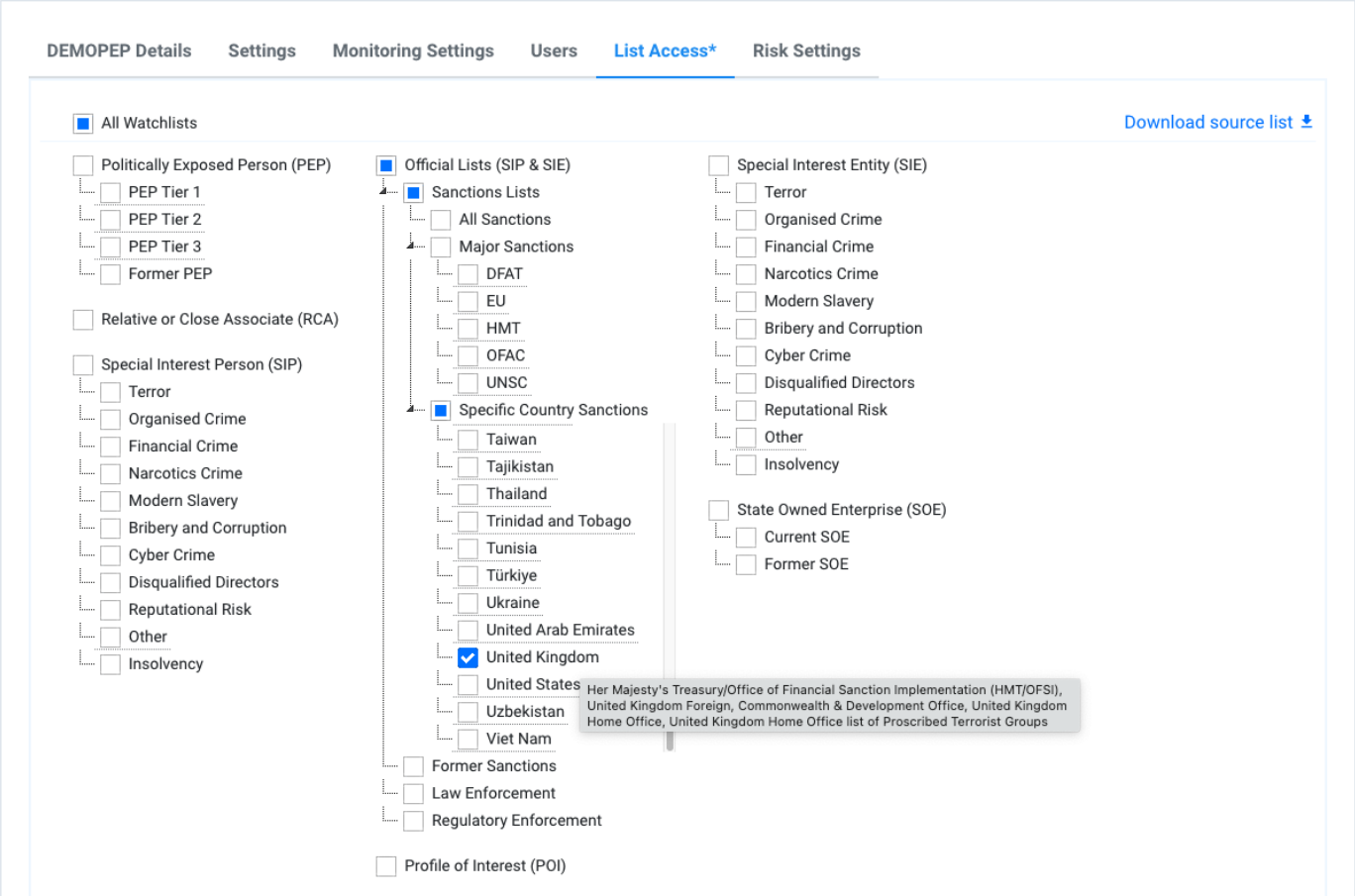


The selected sanctions will be displayed during screening:

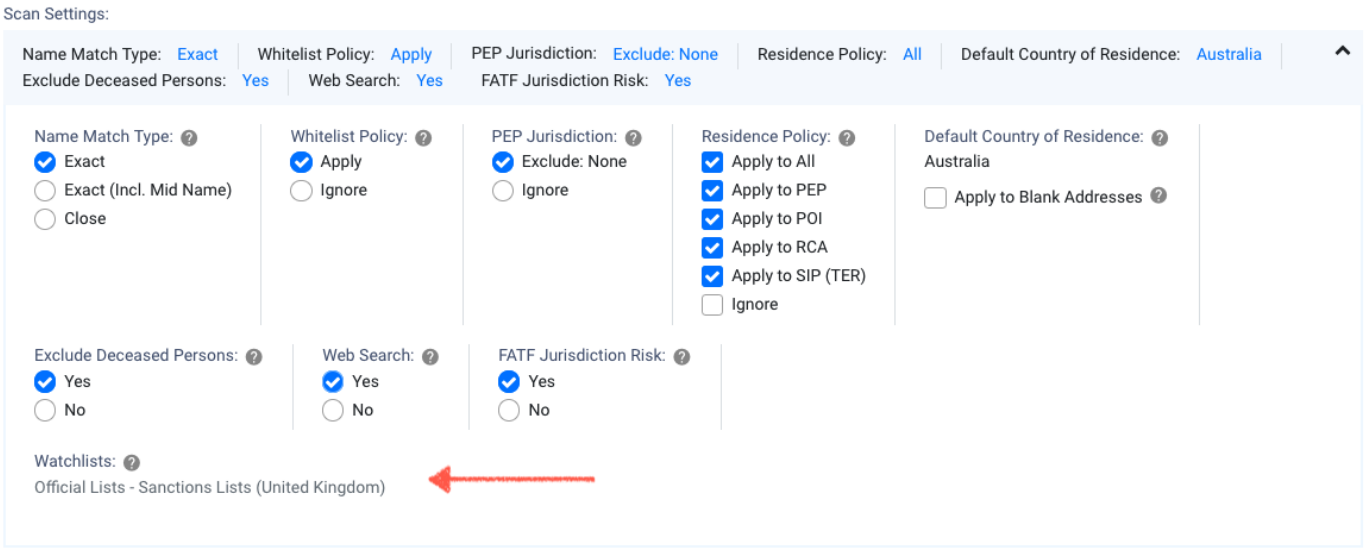


Screen against the United Kingdom sanctions lists only

Example of List Access setup to screen against the United Kingdom sanctions only. You can view the list of sanctions on mouse hover over the country jurisdiction.

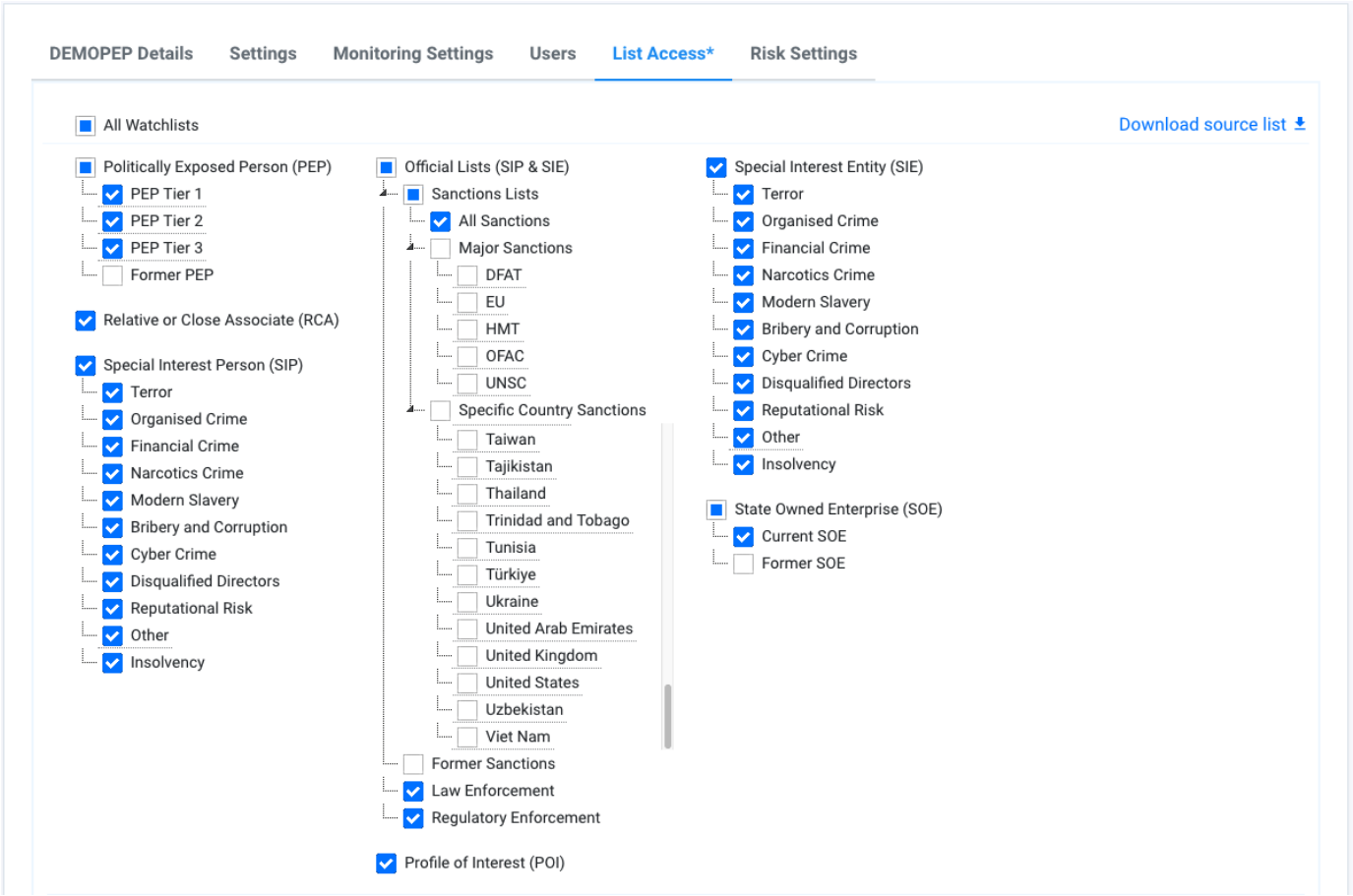


The selected sanctions will be displayed during screening:

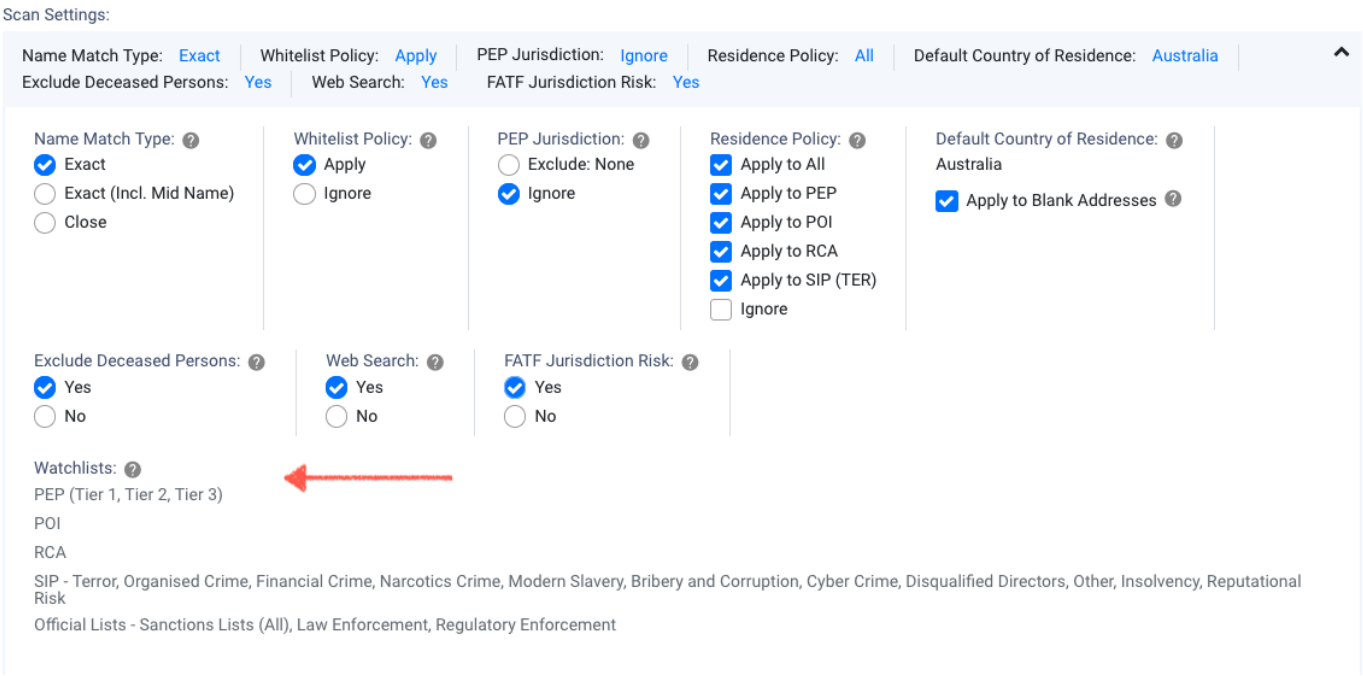


Screen against all watchlists

Example of List Access setup to screen against all watchlists.



The selected watchlists will be displayed during screening:



Manage Users

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

Key Elements

- User details
- Assigned organisation
- Role and Access Rights
- API Access Key

A user can be assigned to one or multiple organisations and suborganisations. To create a user account, you must assign an organisation or suborganisation to the user, else they will be unable to login to access the service.

A user account can be associated to a single role which applies to the entire organisation hierarchy. If a user plays different roles for different suborganisations, we would recommend they be created with multiple user accounts with their own unique usernames and email addresses with the specific roles for the associated suborganisation. Each user account must have a unique **Username** and **Email**.

Each organisation can have up to 3 **Compliance Officers** , and a **Compliance Officer** can be assigned to multiple organisations or suborganisations.

Roles and Access Rights

For a summary of the permissions available to the various user roles, refer to **Overview > User Roles**.

User Roles offer a quick and easy way to allocate permissions for users. Access rights provide additional fine-tuning of a user's access to the features. Access rights are dependent on the user role selected, and you may see different permissions displayed based on the **User Role** selected.

Access Rights	Description
Single Scan	Permission to perform single scans for individuals.
Scan Results	Permission to view scan results.
Batch Scan	Permission to perform batch scans for individuals.
Batch Scan Results	Permission to view batch scan results
Corporates	Access to Corporate scan functionality. This is used in addition to the above permissions to enable the user to run corporate scans, view corporate scan results, run corporate batch scans and view corporate batch scan results.
Due Diligence Decisions	Permission to perform due diligence decisions. The user may be able to view the final match decision but is not able to view history of due diligence decisions and comments.
Due Diligence Report	Permission to view the Due Diligence Reports for individuals and corporates.
Activity Report	Permission to view the Activity Reports for individuals and corporates.
Organisation Management	Permission to manage organisation settings. This applies to Compliance Officers of a suborganisation.
Data Management	Permission to remove scan data. This applies to Compliance Officers of a suborganisation.
Monitoring	Permission to access the ongoing monitoring features including adding scans to the monitoring list.
Dashboard	Permission to view the organisation dashboard.
ID Verification Service	Permission to screen for Identity Verification (IDV) in Individual Single Scan. This does not restrict the ability to view IDV results if `Scan Results` permission is enabled. This is visible if the organisation has been activated for the IDV service and the user role permits screening.

Know Your Business Service	Permission to screen for Know Your Business (KYB) in Corporate Single Scan. This does not restrict the ability to view KYB results if `Scan Results` permission is enabled. This is visible if the organisation has been activated for the KYB service and the user role permits screening.

User Account Statuses

User accounts will have one of the following statuses:

Status	Description
Pending	Account pending user activation. User must set up password and security question/answer to activate. For API only accounts, this can remain Pending and will not affect the API key access.
Active	Account is active and web access is available to the service.
Inactive	Account is deactivated and will not be able to access the service.
Locked	Account is/was locked due to multiple failed login attempts. Locked accounts are automatically unlocked after a period of time, however the status remains as `Locked` for the attention of the Compliance Officer.

API Access Key

Your access to the MemberCheck service includes API access.

To integrate with MemberCheck's API, generate an API key for each user that requires access. Users can create one API key at a time in their profile's **API Access Key** field.

Separate user and system accounts for API

As API Keys are associated with user accounts, having a separate user account with its own API Key for your production system reduces the risk of impact if the individual user's account is deactivated if they were ever to leave your company.

API Keys are specific to environments

The API keys are different for the Demo and Production environments. If you have accounts in both environments, please use the environment specific key to enable your requests to be successfully authenticated and authorised. Also check the API URL relevant to the location of your account.

Deactivate User Account

Users who have left the organisation or no longer need MemberCheck access can be deactivated. This helps improve security and management of access.

Delete User Account

For pending user accounts or user accounts which do not have any associated historical scans, you can delete these to help improve security and management of access.

Deleted accounts cannot be restored.

Users must be assigned to at least 1 active organisation

Please note that all users must have at least 1 active organisation assigned to their account to access MemberCheck.

Single Sign-On

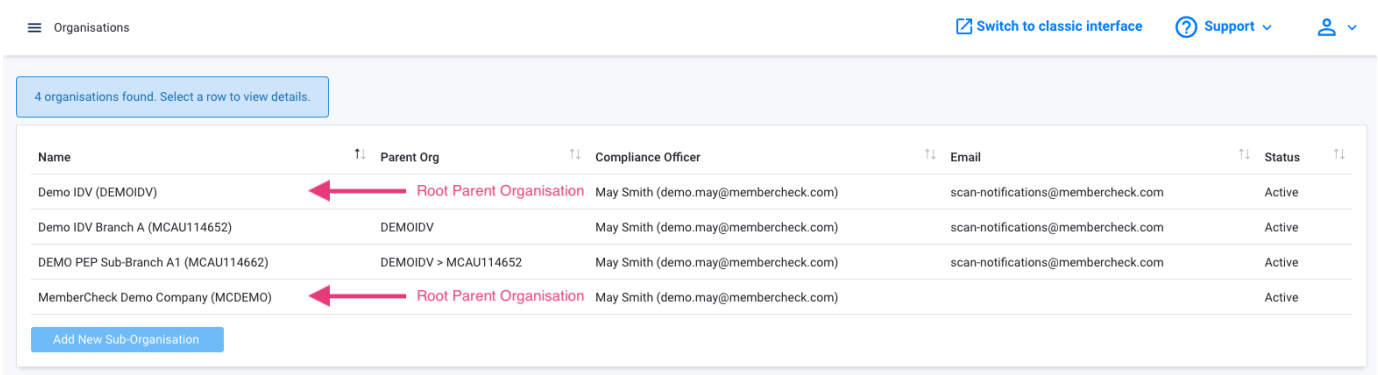
The service supports enterprise-level single sign-on with OpenID Connect (OIDC) and SAML authentication protocols. The integration requires some configuration by the client as well as the MemberCheck team. If you would like to integrate your organisation's identity provider for SSO, please reach out to your Account Manager or the MemberCheck Support team for more details.

Custom Watchlists

Custom watchlists are managed within the Organisation's **List Access** tab and is only available to the **Compliance Officer**. Custom watchlists enables you to expand on the available sources provided by MemberCheck, making this a versatile solution for clients who have specific blacklists for screening.

Whether you have a single-level organisation or part of a multi-level organisation, the **Compliance Officer** at every organisation and suborganisation level can upload and manage their own custom watchlists. These custom watchlists can be enabled for inclusion in PEP & Sanction screening for suborganisations.

Example of a multi-level organisation where the root parent organisation displays a blank for **Parent Org**:

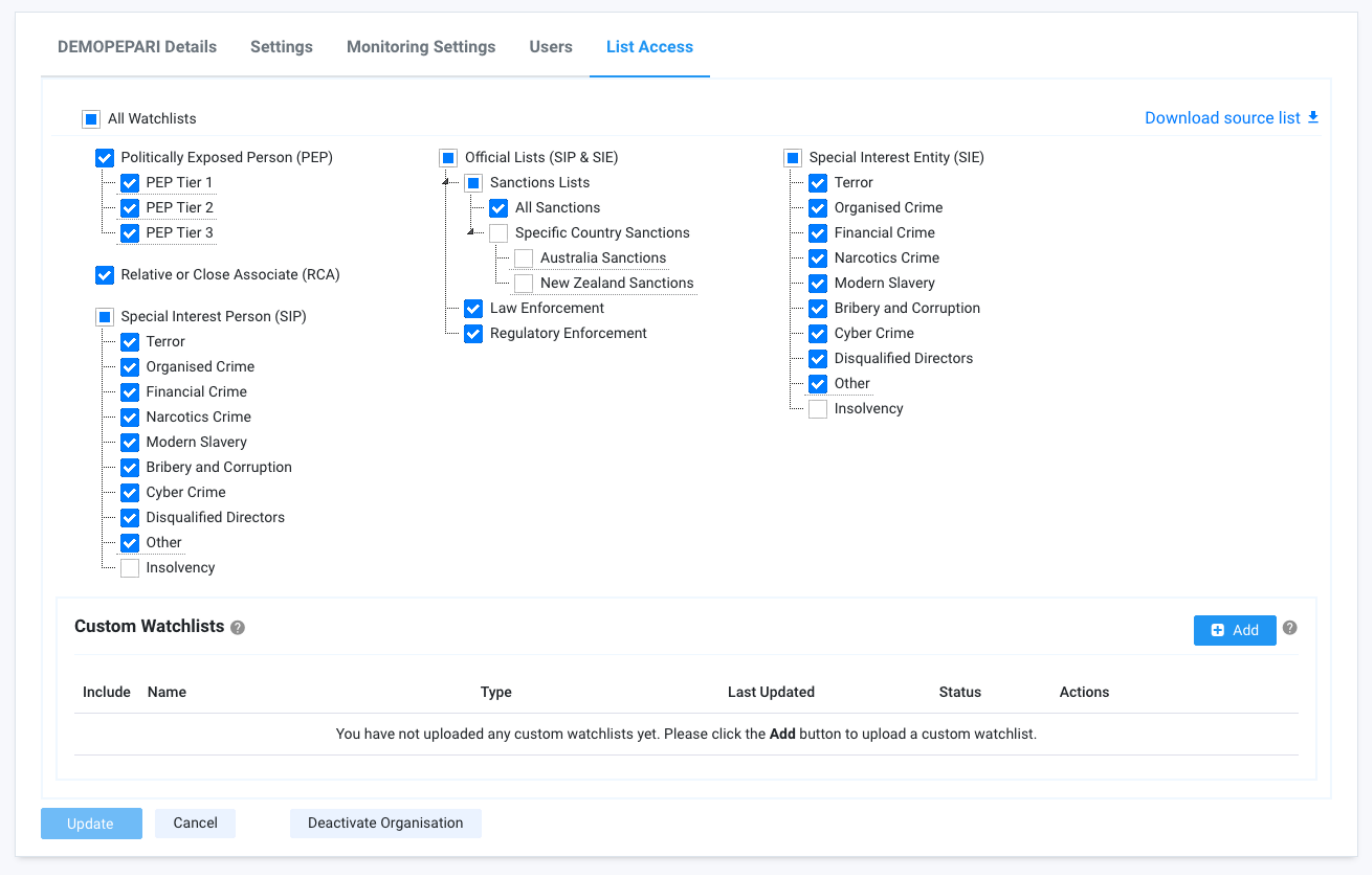


Adding a Custom Watchlist

You can add new custom watchlists within the **List Access** tab of your selected organisation.

> **Custom Watchlist formatting and samples**
>
> Before uploading the custom watchlist, please check **Custom WatchList Templates** for information on structuring the watchlists as well as access available samples to help get you started.

The default screen where no custom watchlists are set up yet:



You can create a custom watchlist to contain:

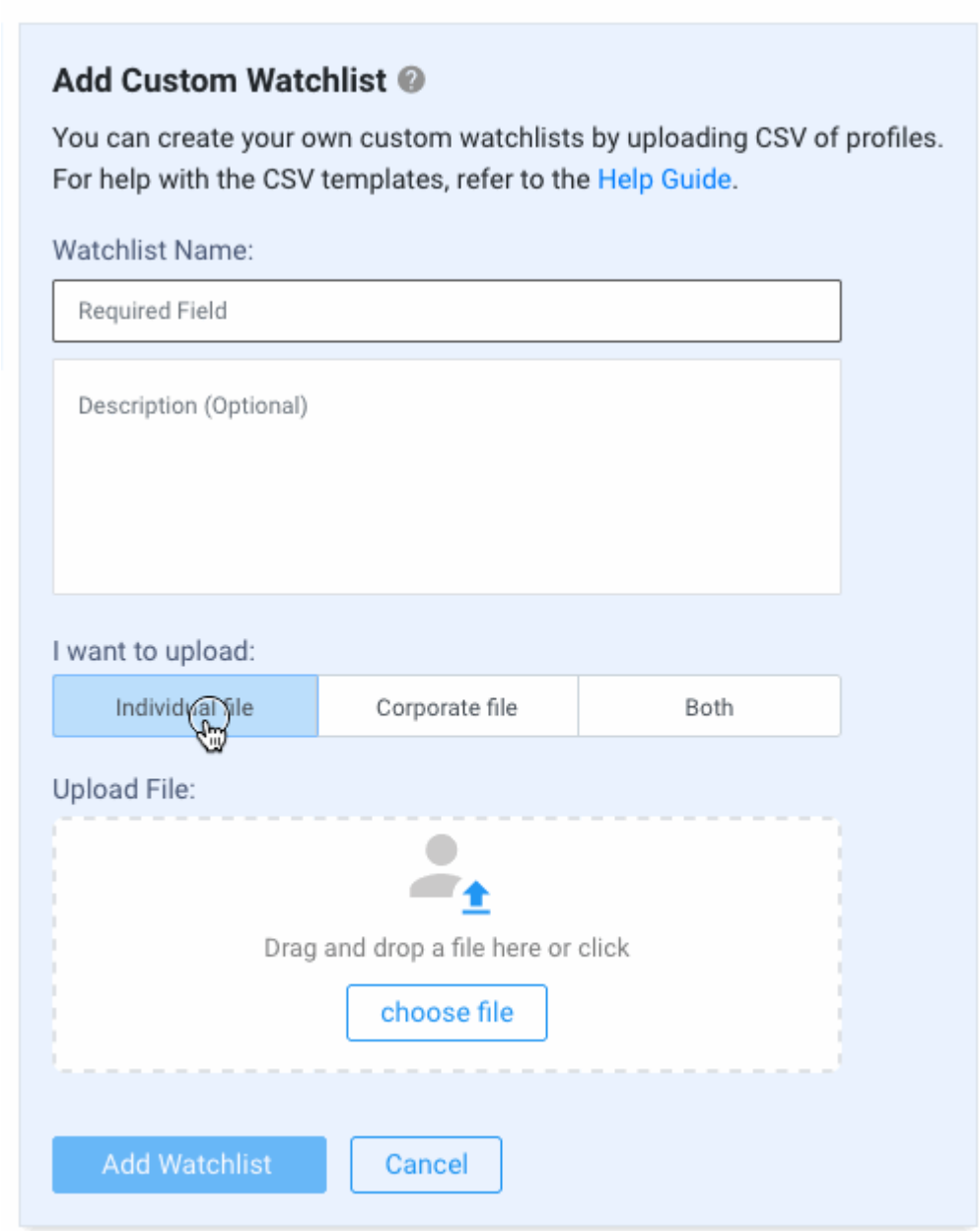
- Individual profiles only
- Corporate profiles only
- Both types of profiles.

The formatting of the CSV for Individuals and Corporates are different and require that these are maintained in separate CSVs.

Field	Required	Character Limit	Description
Watchlist Name	Mandatory	50	Name of the watchlist for easy identification.
Description	Optional	500	Description of the watchlist.

Upload Watchlist Type	Mandatory	-	Select the type of watchlist you would like to upload. Options are: `Individual file` - Select this option to upload a single CSV of Individual profiles. `Corporate file` - Select this option to upload a single CSV of Corporate profiles. `Both` - Select this option to upload the 2 CSV files of both types of profiles.
Upload File	Mandatory	-	Upload CSV of Individual and/or Corporate profiles.

Depending on which option you have selected for upload, you may see the following panes.



Combine or separate watchlists for Individuals and Corporates?

The system provides for both approaches depending on your preference and availability of organisation data. You may prefer to maintain both types of profiles within the same custom watchlist or maintain separate watchlists for Individuals and Corporates.

Please note that you can only remove and delete the CSV file by removing the Custom Watchlist. You are not able to select individual CSV files within the custom watchlist to remove. This may assist you in your decision to main combined or separate watchlists for the different entities.

Large file for uploads

If you have a large sized CSV file, you can compress this file and upload the ZIP file which allows up to 30 MB.

Editing a Custom Watchlist

You can edit the custom watchlist to change the following:

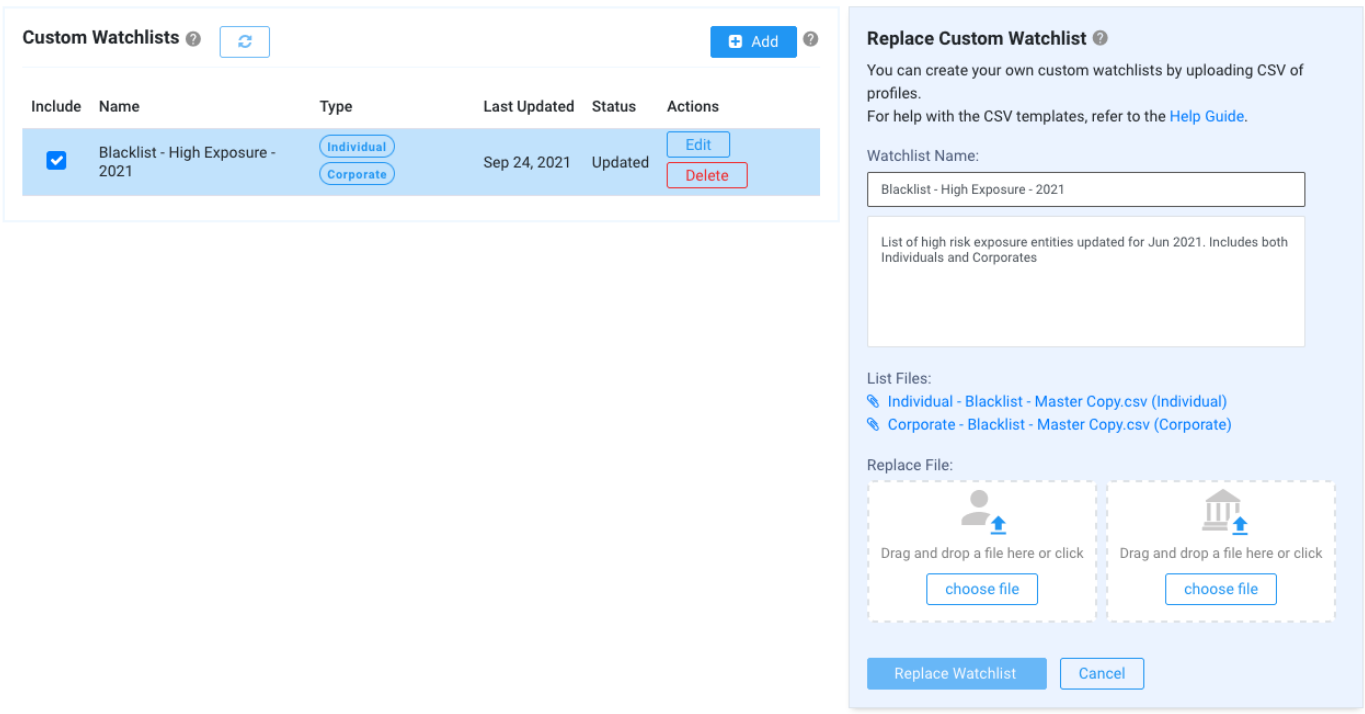
- Change Watchlist Name
- Change Watchlist Description
- Upload updated replacement CSV files

When you select an existing custom watchlist or the associated `Edit` button, the **Replace Custom Watchlist** pane is displayed with options to upload both Individual and Corporate profiles. This option enables you to extend the custom watchlist to include both types of entity profiles, regardless of whether you had initially only uploaded profiles for a single type of entity.

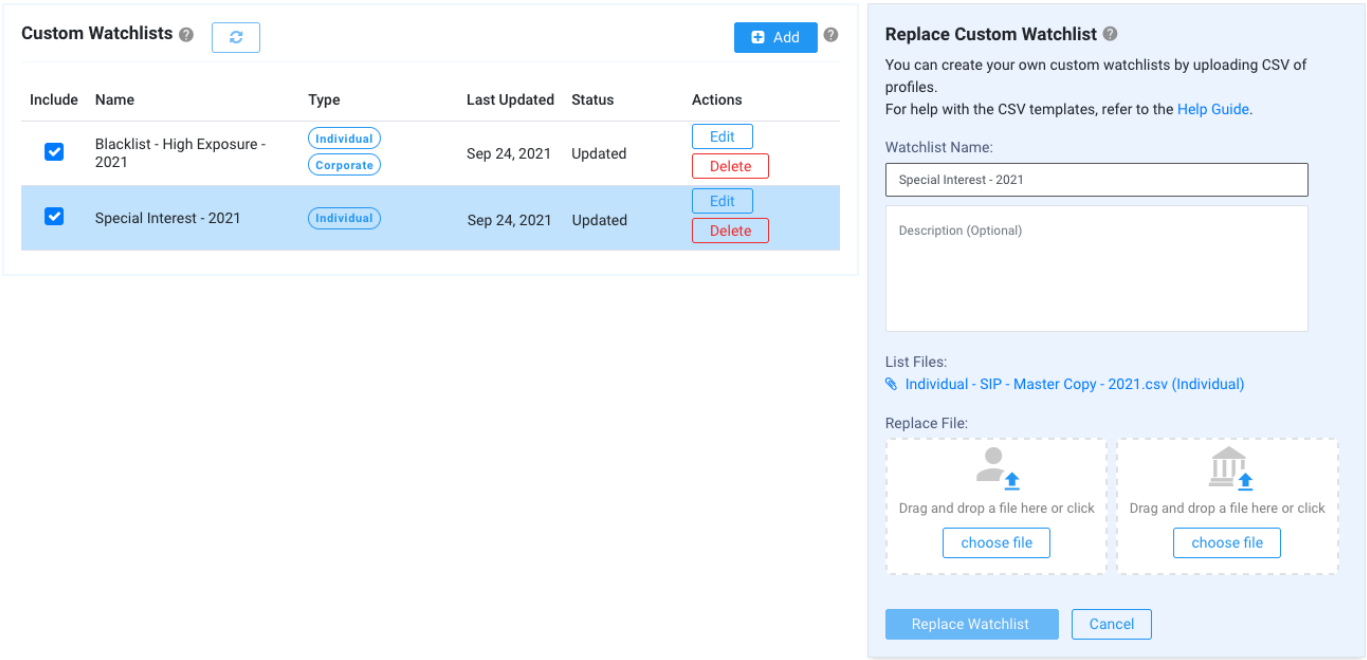
To update your custom watchlists with new profiles, changed profile details, or removal of profiles, select the required watchlist and upload the latest CSV into the relevant Individual and/or Corporate file upload boxes to replace the existing data.

Within this pane, you can download the latest uploaded CSV files for reference.

Example of editing a custom watchlist with both Individual and Corporate profiles:



Example of editing a custom watchlist with only Individual profiles:



Screening against the Custom Watchlist

When a custom watchlist is added, it is activated for the organisation or suborganisation it was uploaded for only. Any associated suborganisations inherit access to the custom watchlists, however, it is not activated by default.

The Compliance Officer for the suborganisation and the Compliance Officer for the parent organisation can opt to enable the custom watchlists. It is not possible to hide the custom watchlists within the organisation hierarchy.

To include the custom watchlists in the PEP and Sanction screening process, simply select the checkbox under **Include** against the associated custom watchlist entry. To exclude the custom watchlist from being included in the screening, simply deselect the checkbox.

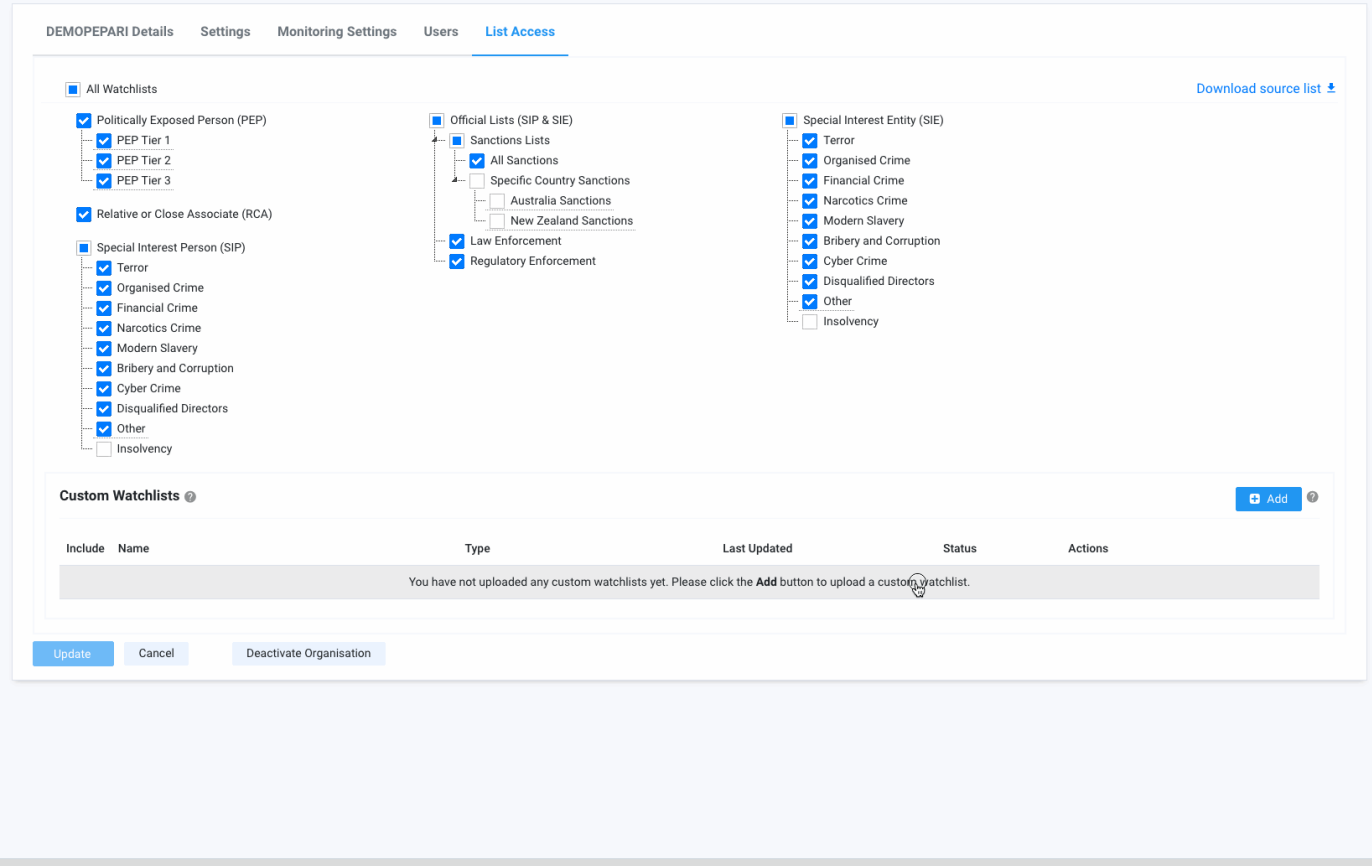
Deleting a Custom Watchlist

To remove profiles uploaded in the custom watchlist, you can delete the custom watchlist entry. If you have both Individual and Corporate profiles combined in the single custom watchlist, deleting of the custom watchlist will remove both types of profiles as you cannot select the CSVs separately to remove.

Quick How-To Guides

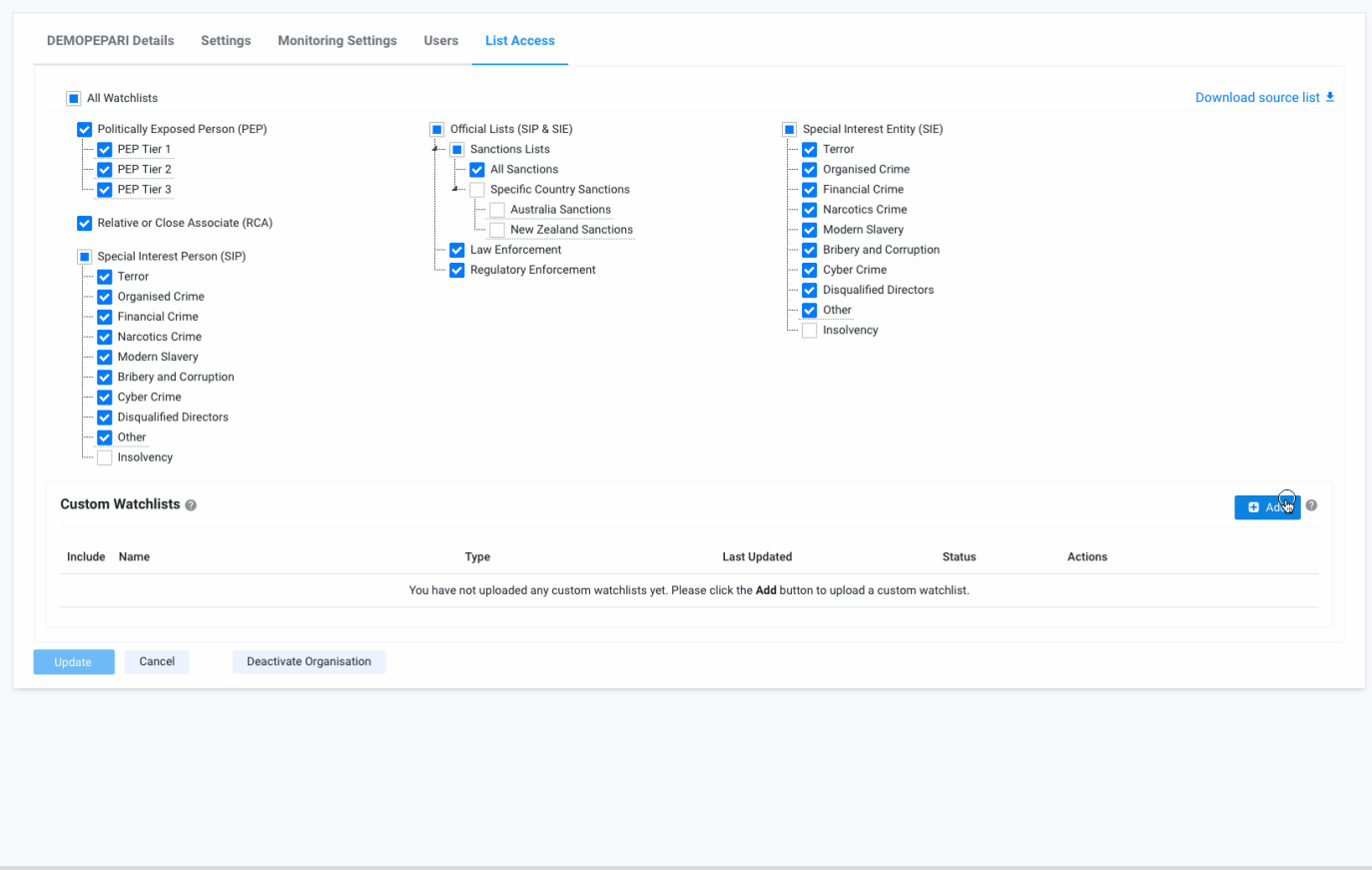
Add a new custom watchlist of Individual profiles

Example of creating a new custom watchlist of Individual profiles.



Add a new custom watchlist of both Individual and Corporate profiles

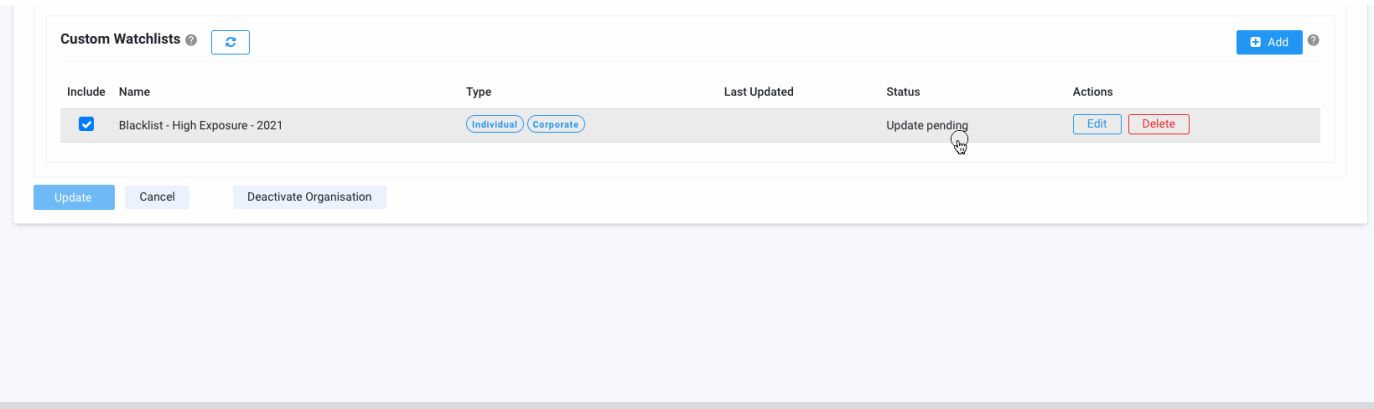
Example of creating a new custom watchlist of both Individual and Corporate profiles.



Refresh custom watchlist

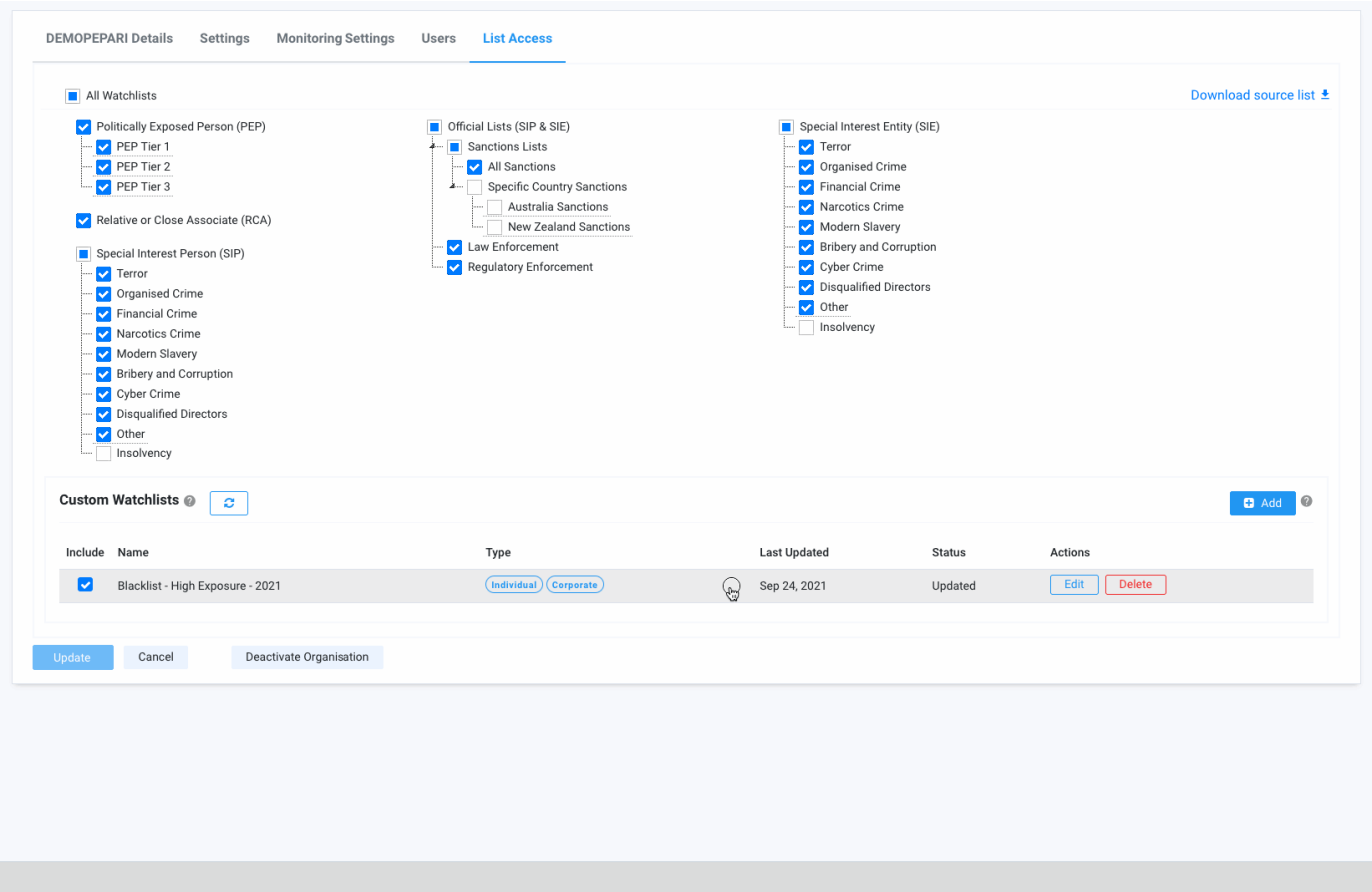
The creation, update or removal of a watchlist may take some time between minutes to hours, depending on the volume of data and the load activity on the server.

You can click on the refresh icon next to the Custom Watchlist to refresh the screen to display the latest status.

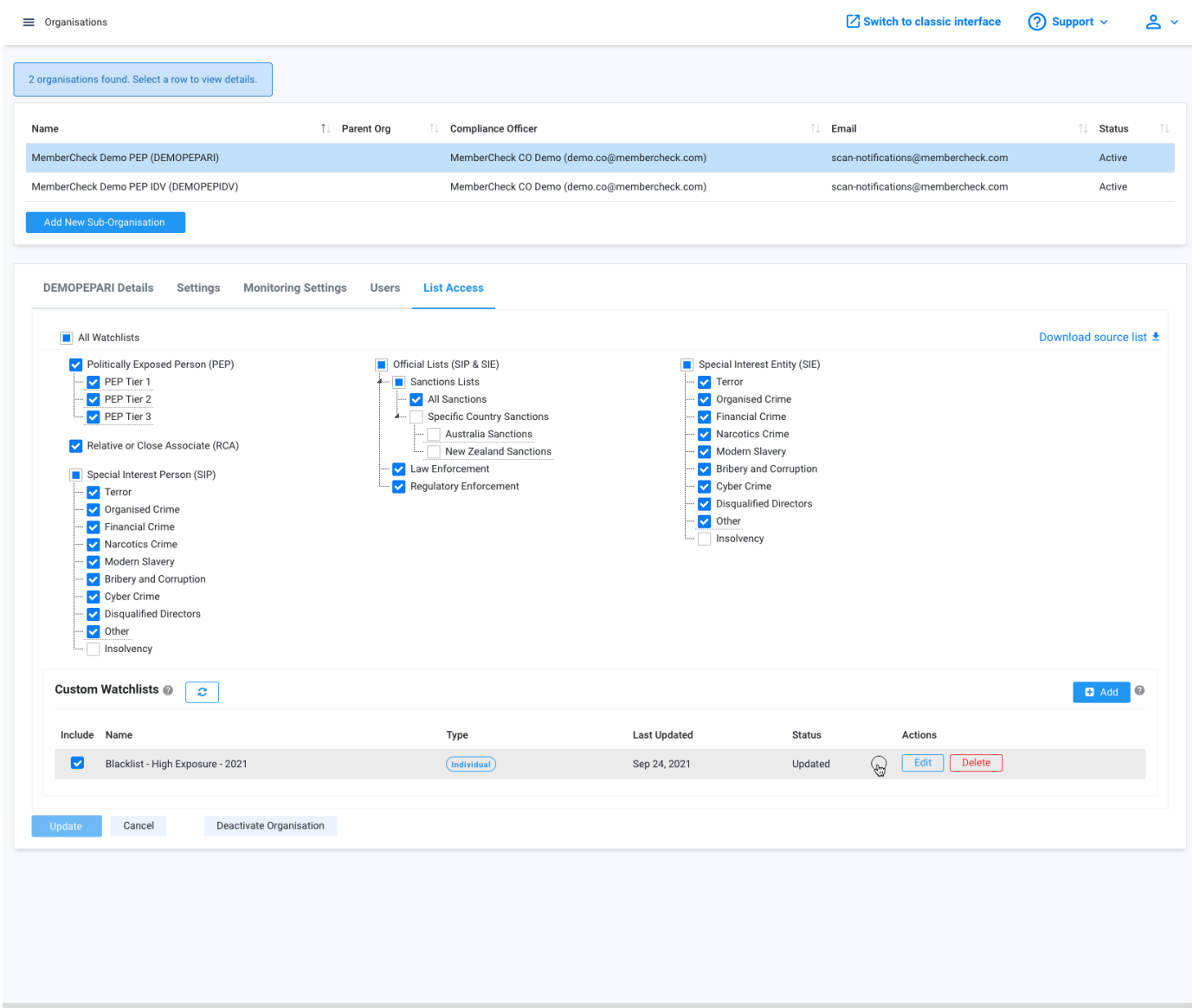


Edit an existing custom watchlist

Example of updating the watchlist of Corporate profiles.



Delete a custom watchlist



Watchlist Categories

Within the service, profile records in watchlists are categorised into the following main categories and subcategories. The availability of these categories and subcategories depends on your subscription to the relevant data sources.

Categories for Individuals

Politically Exposed Person (PEP) Tiers

Individuals who hold prominent public positions and may be at a higher risk for corruption.

PEPs may be further categorised into 3 different tiers depending on their level of risk exposure:

Category	Description

PEP Tier 1	Represents: • Head of state and their deputies • Head and members of government (national level in unitary states; sub-federal/state level in federations; supranational level European Commission, Europe Council) and their deputies • Heads and top commanders of the armed forces - armed forces joint command members, commanders of the main branches of the armed forces • Members of the legislature (national level in unitary states; sub-federal/state level in federations; supranational level European Parliament) • Heads and members of last-instance courts (supreme, constitutional, high, European Court of Justice, specialised courts) • Heads and members of central banks and court of auditors (national level in unitary states; sub-federal/state level in federations; supranational level European Court of Auditors) • Party leaders and executive council members (Parties represented in the national parliament of unitary states and in the federal and sub-federal parliaments in federations)

PEP Tier 2	Represents: • Senior diplomats (ambassadors, high-commissioners, charge d'affaires, permanent representatives) • Heads and board members of the executive bodies of international organisations established by treaty (the highest governing bodies of ARI list of organisations) • Members of the board of directors of SOEs, top executives (C-level) • Senior officials (e.g. high-ranking civil servants, director generals, directors, heads of units) of agencies and boards appointed by the head of state, the government (cabinet and ministries) and the parliament • Members of executive (e.g. governor, prefect) bodies at sub-national level in unitary states and below sub-federal level in federal jurisdictions • Members of legislative (e.g. aldermen, councillors) bodies at sub-national level in unitary states and below sub-federal level in federal jurisdictions • Mayor of capital city and large municipalities (megapolis) • Judges, justices, magistrates, prosecutors, attorneys in courts with jurisdiction at sub-national level in unitary states and below the sub-federal level in federations • Commanders of major national military units (battalions, brigades, flotillas, bases)
PEP Tier 3	Represents: • Middle ranking diplomats (minister-counsellors, councillors, 1st Secretaries and 2nd Secretaries) and low-ranking diplomats (attaché) • Mayor, council member and senior officials of medium to small municipality.
Former PEP	Defined as the natural persons who served in a relevant PEP position within the past 12 months (or a longer period as defined by the national PEP definition)

Relatives and Close Associates (RCA)

Relatives or Close Associates refer to individuals who have a close relationship with a politically exposed person (PEP). This can include family members such as spouses, children, parents, siblings, as well as close friends, business associates, and other individuals who have a significant connection to the PEP.

Profile of Interest (POI)

Profile of Interest is a category designed to capture legacy data of PEPs who served on relevant PEP positions more than 12 months ago, as well as legacy data of profiles which no longer fits the new Reputational Risk Exposure methodology. This includes individuals whose appointments have not been reinstated for a period of 10 years after their status was updated to `Former PEP`.

Special Interest Persons (SIP)

Special Interest Persons refer to individuals who have been identified as being involved in activities that may pose a higher risk for money laundering, terrorism financing or various financial related crimes. These are grouped into the following subcategories.

Category	Description
Sanctions Lists	Persons appearing on official financial sanctions lists who are involved, or suspected of being involved, in illegal activities.
Law Enforcement	Persons appearing on an official law enforcement public domain site as either wanted, investigated, or arrested by an official law enforcement body or the police; or individuals or entities charged, prosecuted, convicted and/or sentenced by a competent criminal court that constitutes a criminal act.
Regulatory Enforcement	Persons listed on an official regulatory enforcement public domain site against whom official regulatory administrative action has been taken by a government or independent regulatory agency responsible for the supervision and oversight of specific administrative regulations or rules for breaches of said rules and regulations.
Bribery & Corruption	Persons involved or alleged to have been involved in criminal activity relating to bribery and corruption, including being bribed, bribing another person (including facilitation payments), bribing a foreign public official, failure of a relevant commercial organisation to prevent bribery, and corrupt practices.

Cyber Crime	Persons involved or alleged to have been involved in criminal activity relating to cybercrime, including identity theft, scams, hacking, and credit card or payment fraud.
Disqualified Directors	Individuals that have been disqualified as acting as company directors (for UK only).
End Use Control	An end use control incident occurs when an entity involved in exporting dual-use or military technology, which has both commercial and military applications, poses a heightened risk of breaching non-proliferation rules. End users, typically foreign entities that ultimately utilise these exported items, may not be intermediaries but could be purchasers or financiers..
Environmental Crime	An environmental crime incident involves individuals or groups attempting, committing, or conspiring to systematically and wilfully engage in illegal acts that directly harm the environment for personal gain. These acts exploit, damage, trade, or steal natural resources, violating international, local, or extraterritorial environmental laws. A key aspect is the organised, systemic approach to wrongfully contaminate the atmosphere, soil, or water with harmful substances, securing financial advantages through profit or cost avoidance. Such pollution is likely to adversely affect the natural environment or life. A key aspect is the organised, systemic approach to wrongfully contaminate the atmosphere, soil, or water with harmful substances, securing financial advantages through profit or cost avoidance. Such pollution is likely to adversely affect the natural environment or life. Examples include dumping industrial waste in water bodies, illicitly trading hazardous waste, trafficking endangered species, smuggling ozone-depleting substances, and illegal logging. The category also covers incidents determined by courts to be criminally negligent acts.
Financial Crime	Persons involved or alleged to have been involved in criminal activity relating to financial crime, including financial and non-financial fraud, money laundering, tax offences, embezzlement, counterfeiting of currency, high-value theft and robbery, insider trading, unexplained wealth orders / interim assets freeze, and failure to comply with relevant financial regulations.
Fugitive	A fugitive incident involves a person who flees a jurisdiction or prison to avoid arrest, prosecution for a crime, imprisonment, or to avoid giving testimony in any criminal proceeding.

Gambling	A gambling operation incident involves individuals or groups attempting, committing, or conspiring to conduct, finance, manage, supervise, direct, or own part of an illegal, organised gambling business. These operations, also known as illegal gaming, demonstrate a systemic approach likely to involve illicit fund flows through the financial system, posing heightened abuse risks. They may further organised crime, terrorism financing, or other AML predicate offences. Unorganised or low-risk gambling operations are excluded.
Human Rights Violation	A human rights violation incident involves individuals or groups attempting, committing, or conspiring to violate fundamental rights established by international agreements, conventions, customs, or national laws. These rights, acknowledged by authoritative institutions like governments, the UN, EU, or NGOs, include life, freedom from torture, fair trial, assembly, religion, expression, and freedom from slavery or arbitrary arrest. This category also encompasses crimes against humanity, where individuals or groups knowingly participate in widespread, systematic attacks against civilians, as directed by organisations or states. Examples include apartheid, forced population transfers, enforced disappearances, enslavement, extermination, genocide, murder, persecution based on group identity, sexual violence, and torture. Such violations often further political destabilisation, terrorism, conflicts, or organised crime, posing elevated financial system abuse risks.
Insolvency	Individuals that have been declared as bankrupt or insolvent (for UK and Ireland only).
Interstate Commerce Violation	An interstate commerce incident involves an individual or a group that attempts, commits, or conspires to unlawfully purchase, sell, or exchange of commodities, money or goods through transport by land or water in contravention of interstate laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject. Interstate commerce includes the movement of goods and services across U.S. state borders.
Labour Violation	A labour violation incident involves individuals or groups attempting, committing, or conspiring to violate laws that define and protect employee rights from employer retaliation. These violations include interfering with employee rights or labour organisation formation, discriminating in hiring or tenure, influencing union membership, refusing collective bargaining, violating child labour laws, and breaching labour laws to secure financial advantages. Key criteria are wilful intent for material gain and likelihood of illicit fund flows through the financial system, posing heightened abuse risks. The category excludes violations that are unlikely to involve such flows and civil labour claims.

Modern Slavery	Persons involved or alleged to have been involved in criminal activity relating to modern slavery, including human trafficking and exploitation, labour trafficking and exploitation, and sex trafficking and exploitation.
Narcotics Crime	Persons involved or alleged to have been involved in criminal activity relating to narcotics, including production, trafficking and distribution of drugs.
Organised Crime	Persons involved or alleged to have been involved in criminal activity relating to organised crime, including illicit arms trafficking, smuggling or illicit trafficking in goods, and organised crime groups, gangs and syndicates.
Pharma Tracking	A pharmaceutical products trafficking incident involves individuals or groups attempting, committing, or conspiring to engage in the organised, systemic manufacture, trade, transport, and distribution of fake, stolen, or illicit medicines and medical devices. This activity contravenes international laws, local jurisdiction's prescribed laws, or any applicable extraterritorial laws. The category excludes single instances of selling pharmaceutical products and small-scale prescription drug sales.
Piracy	A piracy incident involves individuals or groups attempting, committing, or conspiring to engage in criminal acts of violence, detention, or depredation. These acts, perpetrated by crew or passengers of a private ship or aircraft, are directed against another vessel or its persons or property on the high seas for private benefit. The category includes incidents outside a state's sovereign maritime borders, under universal jurisdiction where states or international organisations can claim criminal jurisdiction regardless of the crime's location. It specifically includes maritime piracy in international waters and incidents involving vessels at sea or on rivers.
Reputational Risk	Individuals that have been involved or alleged to have been involved in activities which exposes a risk in reputation.
Unauthorised Incident	An unauthorised incident involves entities not officially permitted, approved, or licensed by a regulatory authority to practice, sell, advise, provide services, or engage in other regulated activities within a specified jurisdiction.

War Crime	A war crime incident involves individuals or groups that have been indicted, wanted, accused, or charged by national governments or international organisations for attempting, committing, or conspiring to violate laws, treaties, customs, or practices governing military or armed conflict between international and non-international states or parties. This consolidated category also includes incidents involving unlawful manufacture, possession, sale, delivery, display, use, threat to use, or making readily accessible CBRN (chemical, biological, radiological, or nuclear) weapons or high explosives. These weapons of mass destruction (WMDs), also known as ABC (atomic, biological, or chemical) weapons, are capable of high-order destruction, causing death or serious harm to large numbers of people, or mass destruction to human-made or natural structures. Examples of war crimes include atrocities against persons or property, murder or ill-treatment of civilians, prisoners of war, or hostages, biological experiments, plunder, wanton destruction of cities, and unjustified devastation. War crimes may be committed by government forces, irregular forces, political leaders, judiciary members, or industrialists.
Other	Individuals involved with other alleged offences related to any of the above categories but without evidence of official action by relevant national or foreign authorities.
Custom Watchlist	Individuals that have been listed in your organisation's self managed custom watchlist.

Terror/Terrorism (TER)

Terrorism encompasses acts of politically or socially motivated violence perpetrated by individuals, organised groups, or lone actors who aim to influence governmental or international organisational policies and populations through fear and coercion. This includes domestic extremism, state-sponsored violence, and ideologically driven attacks across both single and multiple territories. Key identifiers include: membership in recognised terrorist organisations, involvement in activities dangerous to human life or property, and actions intended to further specific political or social objectives.

Former PEP

Former PEPs are individuals who have previously held a prominent public function, typically a senior role, but no longer does. Despite leaving office, these individuals may still pose a risk due to their potential for corruption and the informal influence they retain.

There is no globally accepted timeframe for how long someone retains their PEP status, with some jurisdictions, like the EU, mandating a minimum of 12 months. Other institutions, such as

the FATF, advocate for an open-ended, risk-based approach that considers factors like the individual's previous role, potential for continued influence, and the level of corruption in their country.

Categories for Corporates

Profile of Interest (POI)

Profile of Interest is a category designed to capture legacy data of profiles which no longer fits the new Reputational Risk Exposure methodology.

Special Interest Entities (SIE)

Special Interest Entities refer to organisations that have been identified as being involved in activities that may pose a higher risk for money laundering, terrorism financing or various financial related crimes. These are grouped into the following subcategories.

Category	Description
Sanctions Lists	Entities appearing on official financial sanctions lists what are involved, or suspected of being involved, in illegal activities.
Law Enforcement	Entities appearing on an official law enforcement public domain site as either wanted, investigated, or arrested by an official law enforcement body or the police; or individuals or entities charged, prosecuted, convicted and/or sentenced by a competent criminal court that constitutes a criminal act.
Regulatory Enforcement	Entities listed on an official regulatory enforcement public domain site against whom official regulatory administrative action has been taken by a government or independent regulatory agency responsible for the supervision and oversight of specific administrative regulations or rules for breaches of said rules and regulations.
Bribery & Corruption	Entities involved or alleged to have been involved in criminal activity relating to bribery and corruption, including being bribed, bribing another person (including facilitation payments), bribing a foreign public official, failure of a relevant commercial organisation to prevent bribery, and corrupt practices.
Cyber Crime	Entities involved or alleged to have been involved in criminal activity relating to cybercrime, including identity theft, scams, hacking, and credit card or payment fraud.

Disqualified Directors	Entities that are associated with company directors who have been disqualified or professionally suspended (for UK only).
End Use Control	An end use control incident occurs when an entity involved in exporting dual-use or military technology, which has both commercial and military applications, poses a heightened risk of breaching non-proliferation rules. End users, typically foreign entities that ultimately utilise these exported items, may not be intermediaries but could be purchasers or financiers..
Environmental Crime	An environmental crime incident involves individuals or groups attempting, committing, or conspiring to systematically and wilfully engage in illegal acts that directly harm the environment for personal gain. These acts exploit, damage, trade, or steal natural resources, violating international, local, or extraterritorial environmental laws. A key aspect is the organised, systemic approach to wrongfully contaminate the atmosphere, soil, or water with harmful substances, securing financial advantages through profit or cost avoidance. Such pollution is likely to adversely affect the natural environment or life. A key aspect is the organised, systemic approach to wrongfully contaminate the atmosphere, soil, or water with harmful substances, securing financial advantages through profit or cost avoidance. Such pollution is likely to adversely affect the natural environment or life. Examples include dumping industrial waste in water bodies, illicitly trading hazardous waste, trafficking endangered species, smuggling ozone-depleting substances, and illegal logging. The category also covers incidents determined by courts to be criminally negligent acts.
Financial Crime	Entities involved or alleged to have been involved in criminal activity relating to financial crime, including financial and non-financial fraud, money laundering, tax offences, embezzlement, counterfeiting of currency, high-value theft and robbery, insider trading, unexplained wealth orders / interim assets freeze, and failure to comply with relevant financial regulations.
Fugitive	A fugitive incident involves a person who flees a jurisdiction or prison to avoid arrest, prosecution for a crime, imprisonment, or to avoid giving testimony in any criminal proceeding.
Gambling	A gambling operation incident involves individuals or groups attempting, committing, or conspiring to conduct, finance, manage, supervise, direct, or own part of an illegal, organised gambling business. These operations, also known as illegal gaming, demonstrate a systemic approach likely to involve illicit fund flows through the financial system, posing heightened abuse risks. They may further organised crime, terrorism financing, or other AML predicate offences. Unorganised or low-risk gambling operations are excluded.

Human Rights Violation	A human rights violation incident involves individuals or groups attempting, committing, or conspiring to violate fundamental rights established by international agreements, conventions, customs, or national laws. These rights, acknowledged by authoritative institutions like governments, the UN, EU, or NGOs, include life, freedom from torture, fair trial, assembly, religion, expression, and freedom from slavery or arbitrary arrest. This category also encompasses crimes against humanity, where individuals or groups knowingly participate in widespread, systematic attacks against civilians, as directed by organisations or states. Examples include apartheid, forced population transfers, enforced disappearances, enslavement, extermination, genocide, murder, persecution based on group identity, sexual violence, and torture. Such violations often further political destabilisation, terrorism, conflicts, or organised crime, posing elevated financial system abuse risks.
Insolvency	Entities that have been declared as bankrupt or insolvent (for UK and Ireland only).
Interstate Commerce Violation	An interstate commerce incident involves an individual or a group that attempts, commits, or conspires to unlawfully purchase, sell, or exchange of commodities, money or goods through transport by land or water in contravention of interstate laws and regulations, the prescribed laws of the subject legal jurisdiction, or in violation of any extraterritorial laws to which the entity is subject. Interstate commerce includes the movement of goods and services across U.S. state borders.
Labour Violation	A labour violation incident involves individuals or groups attempting, committing, or conspiring to violate laws that define and protect employee rights from employer retaliation. These violations include interfering with employee rights or labour organisation formation, discriminating in hiring or tenure, influencing union membership, refusing collective bargaining, violating child labour laws, and breaching labour laws to secure financial advantages. Key criteria are wilful intent for material gain and likelihood of illicit fund flows through the financial system, posing heightened abuse risks. The category excludes violations that are unlikely to involve such flows and civil labour claims.
Modern Slavery	Entities involved or alleged to have been involved in criminal activity relating to modern slavery, including human trafficking and exploitation, labour trafficking and exploitation, and sex trafficking and exploitation.
Narcotics Crime	Entities involved or alleged to have been involved in criminal activity relating to narcotics, including production, trafficking and distribution of drugs.

Organised Crime	Entities involved or alleged to have been involved in criminal activity relating to organised crime, including illicit arms trafficking, smuggling or illicit trafficking in goods, and organised crime groups, gangs and syndicates.
Other	Entities involved with other alleged offences related to any of the above categories but without evidence of official action by relevant national or foreign authorities.
Pharma Tracking	A pharmaceutical products trafficking incident involves individuals or groups attempting, committing, or conspiring to engage in the organised, systemic manufacture, trade, transport, and distribution of fake, stolen, or illicit medicines and medical devices. This activity contravenes international laws, local jurisdiction's prescribed laws, or any applicable extraterritorial laws. The category excludes single instances of selling pharmaceutical products and small-scale prescription drug sales.
Piracy	A piracy incident involves individuals or groups attempting, committing, or conspiring to engage in criminal acts of violence, detention, or depredation. These acts, perpetrated by crew or passengers of a private ship or aircraft, are directed against another vessel or its persons or property on the high seas for private benefit. The category includes incidents outside a state's sovereign maritime borders, under universal jurisdiction where states or international organisations can claim criminal jurisdiction regardless of the crime's location. It specifically includes maritime piracy in international waters and incidents involving vessels at sea or on rivers.
Reputational Risk	Entities involved or alleged to have been involved in activities which exposes a risk in reputation.
Unauthorised Incident	An unauthorised incident involves entities not officially permitted, approved, or licensed by a regulatory authority to practice, sell, advise, provide services, or engage in other regulated activities within a specified jurisdiction.

War Crime	A war crime incident involves individuals or groups that have been indicted, wanted, accused, or charged by national governments or international organisations for attempting, committing, or conspiring to violate laws, treaties, customs, or practices governing military or armed conflict between international and non-international states or parties. This consolidated category also includes incidents involving unlawful manufacture, possession, sale, delivery, display, use, threat to use, or making readily accessible CBRN (chemical, biological, radiological, or nuclear) weapons or high explosives. These weapons of mass destruction (WMDs), also known as ABC (atomic, biological, or chemical) weapons, are capable of high-order destruction, causing death or serious harm to large numbers of people, or mass destruction to human-made or natural structures. Examples of war crimes include atrocities against persons or property, murder or ill-treatment of civilians, prisoners of war, or hostages, biological experiments, plunder, wanton destruction of cities, and unjustified devastation. War crimes may be committed by government forces, irregular forces, political leaders, judiciary members, or industrialists.
Custom Watchlist	Entities that have been listed in your organisation's self managed custom watchlist.

Terror/Terrorism (TER)

Terrorism encompasses acts of politically or socially motivated violence perpetrated by individuals, organised groups, or lone actors who aim to influence governmental or international organisational policies and populations through fear and coercion. This includes domestic extremism, state-sponsored violence, and ideologically driven attacks across both single and multiple territories. Key identifiers include: membership in recognised terrorist organisations, involvement in activities dangerous to human life or property, and actions intended to further specific political or social objectives.

State Owned Enterprises (SOE)

A State-Owned Enterprise is a government-owned corporate entity recognised by national law, where the state holds full, majority, or significant minority ownership. SOEs include joint stock companies, limited liability companies, and statutory corporations engaged in economic activities, often with government representation on their boards. Defined by the OECD, this classification helps meet Anti-Money Laundering (AML) compliance, as board members of SOEs may qualify as Politically Exposed Persons (PEPs) based on the level of state control.

Former State Owned Enterprises

The Former SOE category includes entities that were previously owned or controlled by a government but have since undergone privatisation, restructuring, or other changes in ownership status. These entities may no longer be under direct state control or influence, yet their historical background as SOEs can still provide valuable context for monitoring and analysis purposes.

Consolidated Categories

Official watchlist consisting of Sanctions, Financial Regulation and Law Enforcement which apply to both Individual and Corporate entities:

Official Lists (SIP & SIE)

Category	Description

`Sanction Lists`

Sanctions are restrictive measures imposed by an international body, multilateral agency, or national government to achieve a desired outcome. They can be imposed on a regime, organisation or individual. Sanctions range from multilateral programmes, such as those imposed by the UN or EU, to unilateral sanctions enacted by individual nations like Australia, Japan, and Switzerland. These are divided into the following levels for screening scope:

- All Sanctions Lists
- Major Sanctions Lists
    - DFAT - Department of Foreign Affairs and Trade
    - EU - European Union Council
    - HMT - Her Majesty's Treasury/Office of Financial Sanction Implementation
    - OFAC - Office of Foreign Assets Control
    - UNSC - United Nations Security Council
- International sanctions lists e.g. Consolidated Sanctions List, Asian Development Bank
- Sanctions by country e.g. Australia, New Zealand, Japan
- Sanctions lists by country e.g. Austrac, Australian National Security, New Zealand Police Force, Japan Ministry of Finance etc.

`Law Enforcement`

Persons or entities appearing on an official law enforcement public domain site as either wanted, investigated, or arrested by an official law enforcement body or the police; or individuals or entities charged, prosecuted, convicted and/or sentenced by a competent criminal court that constitutes a criminal act.

`Regulatory Enforcement`	Persons or entities listed on an official regulatory enforcement public domain site against whom official regulatory administrative action has been taken by a government or independent regulatory agency responsible for the supervision and oversight of specific administrative regulations or rules for breaches of said rules and regulations.

Former Sanctions

The Former Sanctions category encompasses entities that were once listed on international, regional or national sanctions lists but have since been removed from active sanction status due to various reasons such as compliance with imposed conditions, resolution of conflicts, or changes in geopolitical situations. These entities, although no longer subject to restrictive measures, may still be of interest for monitoring purposes given their historical involvement in activities that led to their initial listing.

Reports

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
					

Permissions

Compliance Officers and **Auditors** have access to view reports for all associated organisations, active and disabled.

Advanced Users, **Standard Users** and **Billing Officers** have access to view reports for all associated organisations which are active.

Report Types

The following reports are available in the system.

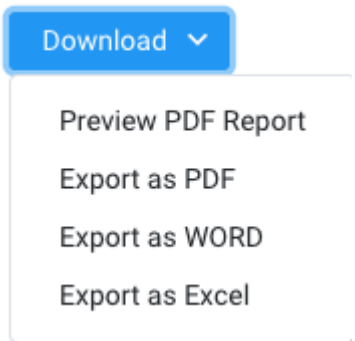
Report Name	Section	Description
Organisation Activity	Reports	Scan activities per day for the selected organisation. The report includes number of scans for both PEP & Sanctions, ID Verification and Know Your Business. The annual Monitoring Rescan activities are also included in this report. This report is generated overnight and does not include scan activities of the current day.

Organisation Group Activity	Reports	Summary of total number of scans for one or more selected organisation. The report includes activities for both PEP & Sanctions, ID Verification and Know Your Business. This report is generated overnight and does not include scan activities of the current day.
Monitoring	Reports	Ongoing monitoring activities per day/fortnight/week/month/ quarter/semi-annual for both individuals and corporates. This schedule is based on your agreed subscription frequency. The report includes number of individuals and corporates being monitored on a regular basis and the number of detected changes to profiles affecting monitored entities.
Monitoring Group Summary	Reports	Overview of the number of active items in the monitoring list and monitoring rescan within the defined date range. The report includes the number of lowest, highest and average number of actively monitored entities in the monitoring list as well as the number of items screened for the annual monitoring rescan if exists within the period.
Individual Due Diligence	Reports	A report of due diligence decisions and comments recorded against individual scan matches. This applies to PEP & Sanctions scans only.
Corporate Due Diligence	Reports	A report of due diligence decisions and comments recorded against company scan matches.
Business and UBO Check Activity Report	Reports	A report for Know Your Business checks including requested documents and enhanced company profiles, request dates, associated delivery statuses, and prices.

Results Summary Report	Scan Results (Individuals and Corporates)	A report containing a summary of all profile matches returned and the associated due diligence decisions. This report is only available in CSV format.

To view the reports, select the **Report Type**, select an **Organisation or suborganisation** from the available list and the period of activity. The **Activity Date** defaults to "year to date".

For a quick view of the report contents, select from **Download** the option `Preview PDF Report`. You may also opt to download a copy as PDF, Word or Excel.



Screening Activity Details and Results

For record keeping and for purposes of auditing for your organisation, you can download reports of your screening activities and the associated results, and lists of monitored entities. The reports can be downloaded in PDF, Word, Excel and CSV formats. Where large volumes of data are downloadable, the application may only offer download in CSV format.

The report download options are available as a **Download** button throughout the application within the **Scan Results**, **Batch Scan Results**, **Monitoring Results** and **Monitoring List** screens.

Data Management

Permissions

Compliance Officer	Advanced User	Standard User	Data Entry Operator	Billing Officer	Auditor
	✕	✕	✕	✕	✕

The **Compliance Officer** can remove historical scan data and whitelists for the organisation.

It is recommended that *before deleting any data* from the system, you have downloaded all the relevant reports for audit management. Data deleted from the system is permanent and cannot be retrieved.

Options for data deletion

Within **Data Management**, you can select to delete the following types of data for your organisation:

Option	Description
1 - **ID Verification scan data only**	This options enables you to delete all historical ID Verification only scans. This option is only visible if your organisation has subscribed to the ID Verification service.
2 - **KYB scan data only**	This options enables you to delete all historical Know Your Business only scans.
3 - **Selected Single Scan data**	This options enables you to filter and select specific individual or corporate scans for deletion. If your organisation has subscribed to **ID Verification**, this option will also enable you to remove ID Verification scans.

4 - **Selected PEP & Sanctions Batch Scan data**	This options enables you to individually select from a list of individual or corporate batch scans for deletion.
5 - **PEP & Sanction data, where No Matches were found from single and batch scan information**	If you choose to delete only data that had no matches, it is recommended that prior to deletion, you download a Full Report for all batch scans that have been run so that you can keep a record of all members that have been scanned whether they lead to a match or no match.
6 - **All Single Scan, Batch Scan and whitelist data**	This option deletes **all scan data including single scan data, batch scan data and all whitelist information**. **Scan Results** and **Batch Scan Results** will show no scans found. Matches previously added to the whitelist will also be deleted. If your organisation has subscribed to **ID Verification**, this option will also remove all ID Verification scan information. If you choose to delete all scan and whitelist information, it is recommended that prior to deletion, you run the appropriate Individual and Corporate Due Diligence Reports so that you can keep a record of all due diligence decisions recorded. Entities in the Monitoring List will continue to be monitored and are unaffected.
7 - **All Single Scan, Batch Scan, whitelist and Monitoring List data**	This option deletes **all scan data including single scan data, batch scan data, all whitelist information and monitored entities**. **Scan Results** and **Batch Scan Results** will show no scans found. Matches previously added to the whitelist will also be deleted. **Monitoring List** will also be emptied. If your organisation has subscribed to **ID Verification** and **Know Your Business**, this option will also remove these scan information. If you choose to delete all scan and whitelist information, it is recommended that prior to deletion, you run the appropriate Individual and Corporate Due Diligence Reports so that you can keep a record of all due diligence decisions recorded.
8 - **Selected Supporting Document data only**	The option to delete Supporting Documents associated with Individual and Corporate entities. You can filter documents for deletion by scan type and scan service for Batch and Single scans.

9 - **Risk Assessment scans data only**	This option deletes all stand alone historical AML Risk Assessment Checks. This does not include Risk Assessment Checks associated with PEP and Sanctions, IDV or KYB scans. This option is only visible if your organisation has subscribed to the AML Risk Assessment Check service.

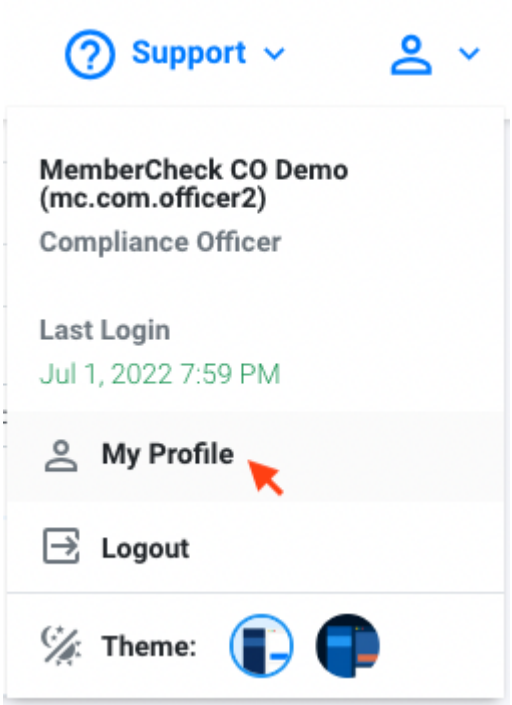
Once you have completed due diligence on a batch file it is recommended that you delete selected batch data (option 4) or only data that lead to no matches (option 5), to comply with National Privacy Principles.

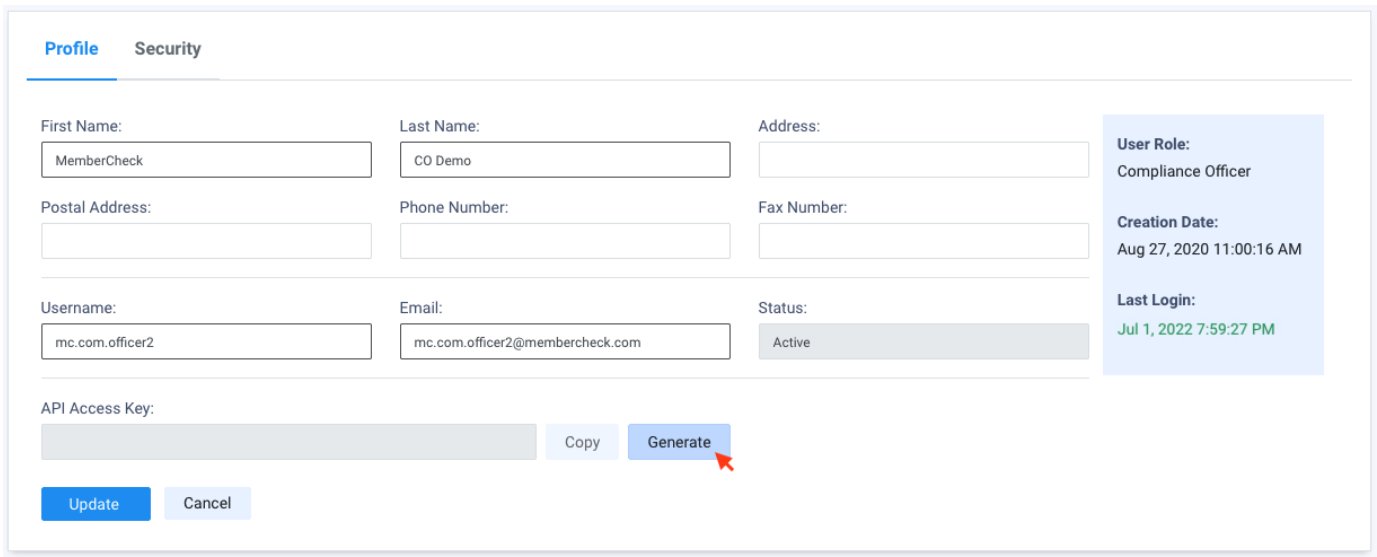
Deleting scan data means that there will be no record of it in the **Scan Results**, **Batch Scan Results** or **Monitoring Results**. Whitelist entries are only retained if you choose to delete selected batches (option 4) or only data that lead to no matches (option 5).

API Key

Generate Your Own API Key

All users are able to generate an API key for their own accounts via **My Profile** screen after logging in.



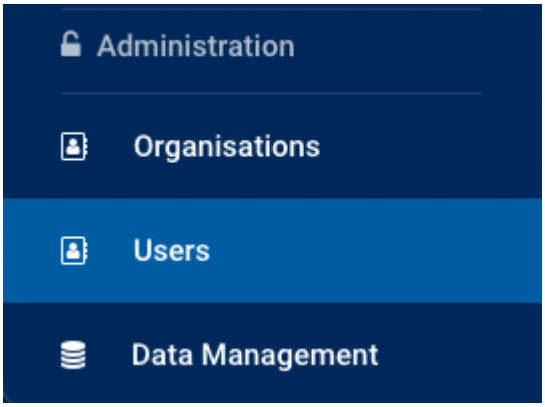


Once your API Access Key has been generated, click on **Update** to save the changes to your profile.

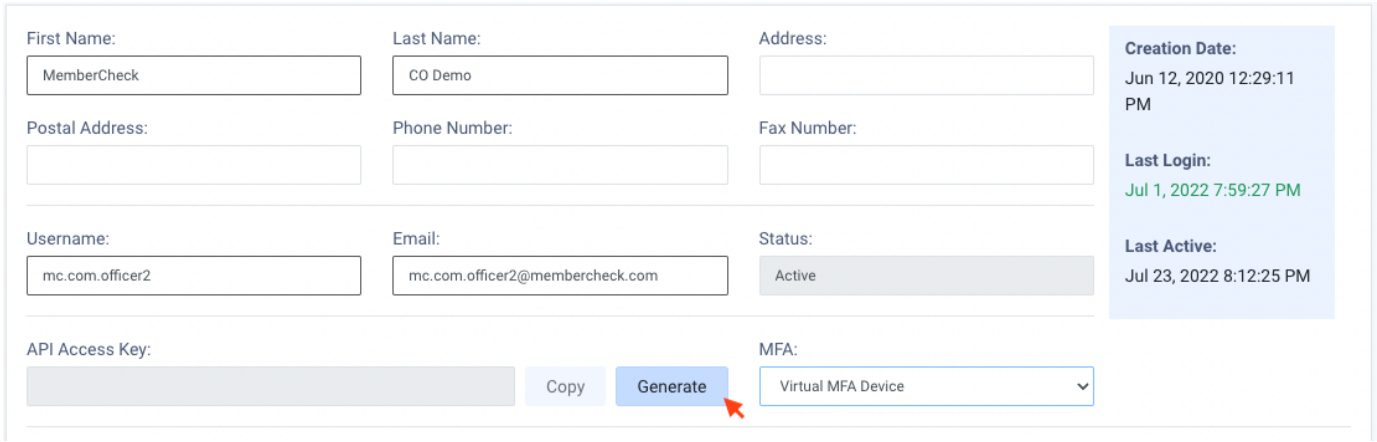
Generate API Key for another account

A **Compliance Officer** can generate an API Key for any user account assigned to their organisation or suborganisation.

This can be managed through **Administration > User**.



Once you have selected the required user account to view the profile details, click **Generate** for **API Access Key**.



Once your API Access Key has been generated, click on **Update** to save the changes to your profile.

Dedicated user accounts for API access only

You may like to consider using a dedicated user account for your systems to minimise any disruptions relating to an individual user's account. For example, when a staff member leaves the company and their account is deactivated.

Important Note

API keys are different for the Demo and Production environments and within different regions. If you have accounts in both environments, please use the environment specific key to ensure your requests are able to be authenticated and authorised.

Batch File Templates and Samples

Templates

Batch scans for **Individuals** and **Corporates** are separate due to their different schema and contents.

The **templates** and **sample** batch files have been provided to assist you in preparing your batch files, and you will need to make some minor adjustments to appropriate the files for your organisation.

Description	Download Template	
Batch file template for Individuals	CSV	XML
Batch file template for Corporates	CSV	XML
All batch file templates (Individuals and Corporates)	ZIP	

Sample Batch Files

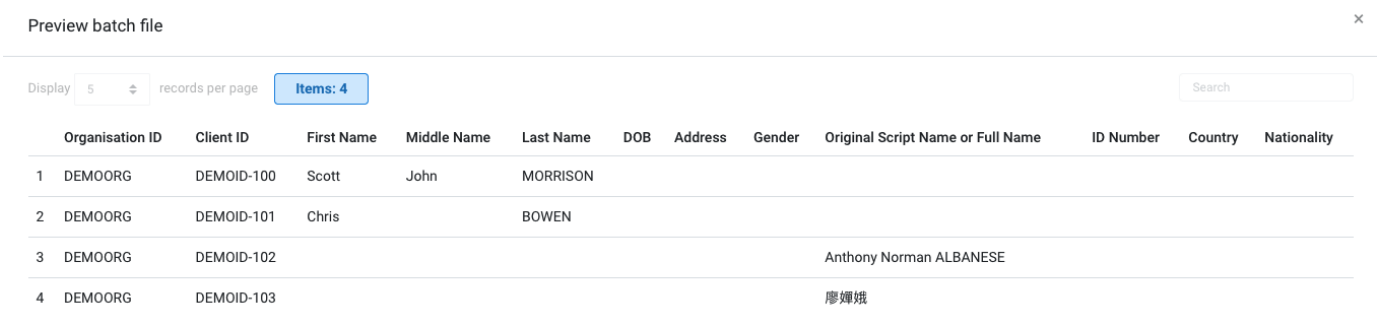
For a quick start, you can download the sample CSV and XML batch files which contain sample text and preset fields.

> ⚠ **Before running the sample batch file you will need to ...**
>
> Please replace the generic Org ID `DEMOORG` in the sample batch with the **Org ID** assigned to you during enrolment.

To ensure the file formatting and encoding is retained, we recommend editing these sample files via a text editor rather than Excel or Numbers as these applications can change the formatting and structure of the CSV files.

Individual Sample Batch Files

Minimum requirements for due diligence or monitoring:


Preview batch file

Display 5 records per page Items: 4 Search

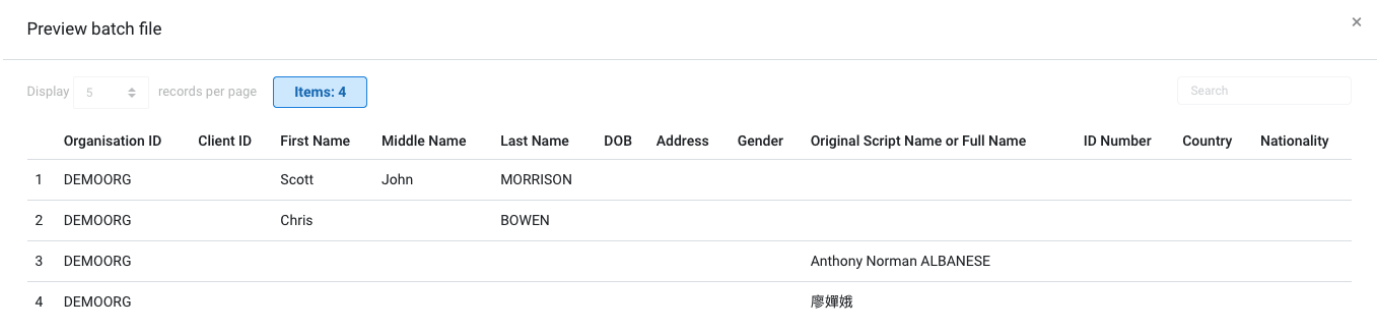
	Organisation ID	Client ID	First Name	Middle Name	Last Name	DOB	Address	Gender	Original Script Name or Full Name	ID Number	Country	Nationality
1	DEMOORG	DEMOID-100	Scott	John	MORRISON							
2	DEMOORG	DEMOID-101	Chris		BOWEN							
3	DEMOORG	DEMOID-102							Anthony Norman ALBANESE			
4	DEMOORG	DEMOID-103							廖嫦娥			

Type of Data Required	Download Sample
	CSV XML

- Org ID
- Client ID
- First Name and Last Name
- Original Script Name
- Full Name

You must include either **First Name and Last Name**, or **Original Script Name or Full Name**. If you are not able to separate the First and Last Names, you can enter the individual's Full Name into the **Original Script Name or Full Name** field.

Minimum requirements (no due diligence or monitoring):


Preview batch file

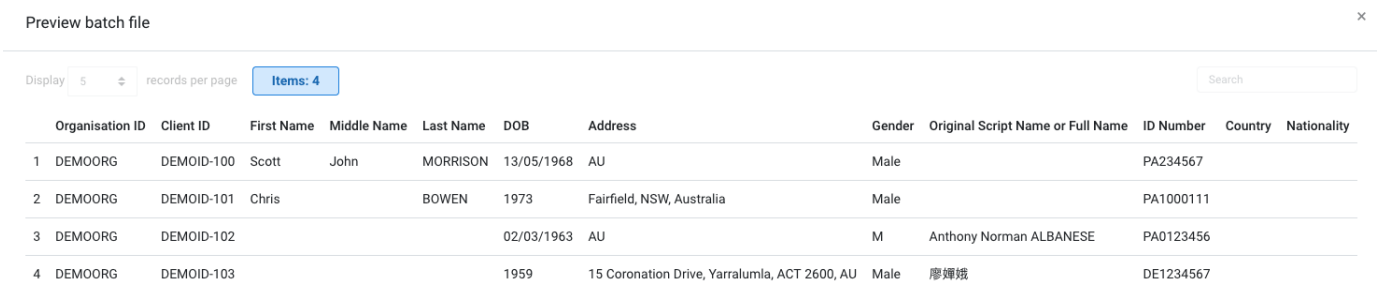
Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	First Name	Middle Name	Last Name	DOB	Address	Gender	Original Script Name or Full Name	ID Number	Country	Nationality
1	DEMOORG		Scott	John	MORRISON							
2	DEMOORG		Chris		BOWEN							
3	DEMOORG								Anthony Norman ALBANESE			
4	DEMOORG								廖嫦娥			

Type of Data Required	Download Sample
• Org ID • First Name and Last Name • Original Script Name • Full Name	CSV XML

You must include either **First Name and Last Name**, or **Original Script Name or Full Name**. If you are not able to separate the First and Last Names, you can enter the individual's Full Name into the **Original Script Name or Full Name** field.

Additional member details with Gender, Original Script Names/Full Name and ID Number:


Preview batch file

Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	First Name	Middle Name	Last Name	DOB	Address	Gender	Original Script Name or Full Name	ID Number	Country	Nationality
1	DEMOORG	DEMOID-100	Scott	John	MORRISON	13/05/1968	AU	Male		PA234567		
2	DEMOORG	DEMOID-101	Chris		BOWEN	1973	Fairfield, NSW, Australia	Male		PA1000111		
3	DEMOORG	DEMOID-102				02/03/1963	AU	M	Anthony Norman ALBANESE	PA0123456		
4	DEMOORG	DEMOID-103				1959	15 Coronation Drive, Yarralumla, ACT 2600, AU	Male	廖嬋娥	DE1234567		

Type of Data Required	Download Sample

CSV XML

- Org ID
- Client ID
- First Name and Last Name
- Date of Birth
- Address
- Gender
- Script Name or Full Name
- ID Number

You must include either **First Name and Last Name**, or **Original Script Name or Full Name**. If you are not able to separate the First and Last Names, you can enter the individual's Full Name into the **Original Script Name or Full Name** field.

Full member details with multiple Countries of Residence and Nationalities:

Preview batch file

Display 5 records per page Items: 5 Search

	Organisation ID	Client ID	First Name	Middle Name	Last Name	DOB	Address	Gender	Original Script Name or Full Name	ID Number	Country	Nationality
1	DEMOORG	DEMOID-100	Scott	John	MORRISON	13/5/1968	AU	Male		PA234567		AU
2	DEMOORG	DEMOID-101	Chris		BOWEN	1973	Fairfield, NSW, Australia	Male		PA1000111		AU
3	DEMOORG	DEMOID-102				2/3/1963		M	Anthony Norman ALBANESE	PA0123456	AU	AU
4	DEMOORG	DEMOID-103				1959	15 Coronation Drive, Yarralumla, ACT 2600	Male	廖嫦娥	DE1234567	AU;CN	CN
5	DEMOORG	DEMOID-104	Benjamin		Smith			Male			FR;GB	CA;US

Type of Data Required	Download Sample

CSV XML

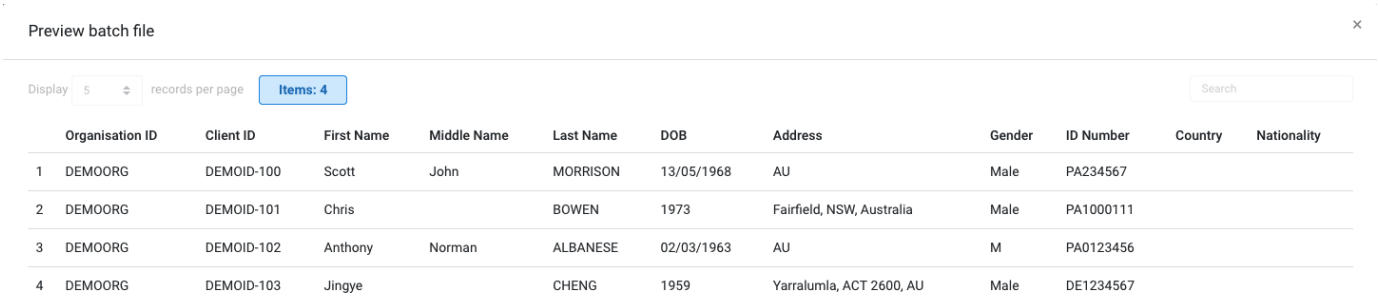
- Org ID
- Client ID
- First Name and Last Name
- Date of Birth
- Address
- Gender
- Script Name or Full Name
- ID Number
- Country of Residence (up to 5)
- Nationality (up to 5)

You must include either **First Name and Last Name**, or **Original Script Name or Full Name**. If you are not able to separate the First and Last Names, you can enter the individual's Full Name into the **Original Script Name or Full Name** field.

Original Script Search or Full Name not enabled for your organisation

If your organisation does not have the **Original Script Search/Full Name** setting activated, the **Original Script Name/Full Name** field should not be included from your batch files.

Full member details with Gender and ID Number (excluding Original Script Name/Full Name):



Preview batch file

Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	First Name	Middle Name	Last Name	DOB	Address	Gender	ID Number	Country	Nationality
1	DEMOORG	DEMOID-100	Scott	John	MORRISON	13/05/1968	AU	Male	PA234567		
2	DEMOORG	DEMOID-101	Chris		BOWEN	1973	Fairfield, NSW, Australia	Male	PA1000111		
3	DEMOORG	DEMOID-102	Anthony	Norman	ALBANESE	02/03/1963	AU	M	PA0123456		
4	DEMOORG	DEMOID-103	Jingye		CHENG	1959	Yarralumla, ACT 2600, AU	Male	DE1234567		

Type of Data Required	Download Sample
	CSV XML

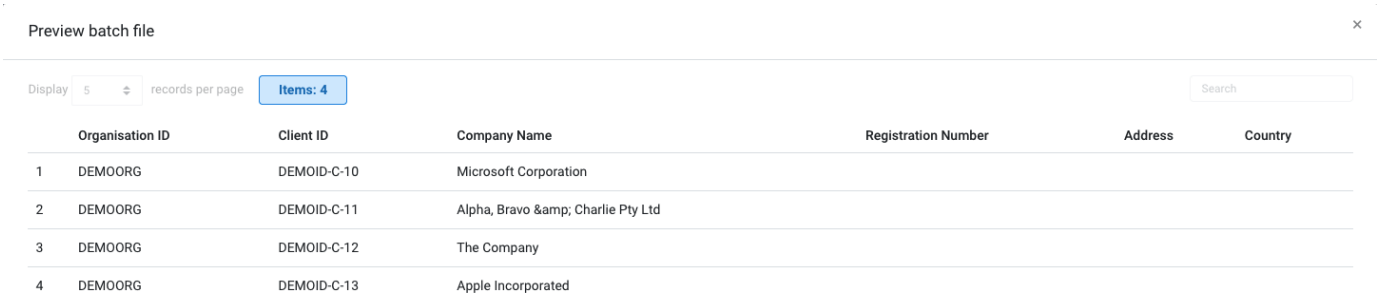
- Org ID
- Client ID
- First Name and Last Name
- Date of Birth
- Address
- Gender
- ID Number

Original Script Search/Full Name setting

To check if your organisation has this setting enabled, check out this FAQ or get in contact with your Compliance Officer.

Corporate Sample Batch Files

Minimum requirements for due diligence and monitoring:


Preview batch file

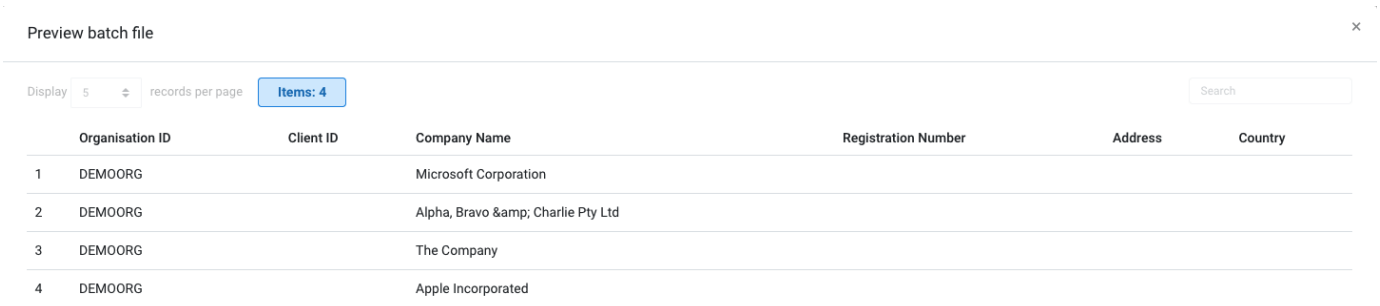
Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	Company Name	Registration Number	Address	Country
1	DEMOORG	DEMOID-C-10	Microsoft Corporation			
2	DEMOORG	DEMOID-C-11	Alpha, Bravo & Charlie Pty Ltd			
3	DEMOORG	DEMOID-C-12	The Company			
4	DEMOORG	DEMOID-C-13	Apple Incorporated			

Type of Data Required	Download Sample
	CSV XML

- Org ID
- Client ID
- Company Name

Minimum requirements (no due diligence or monitoring):


Preview batch file

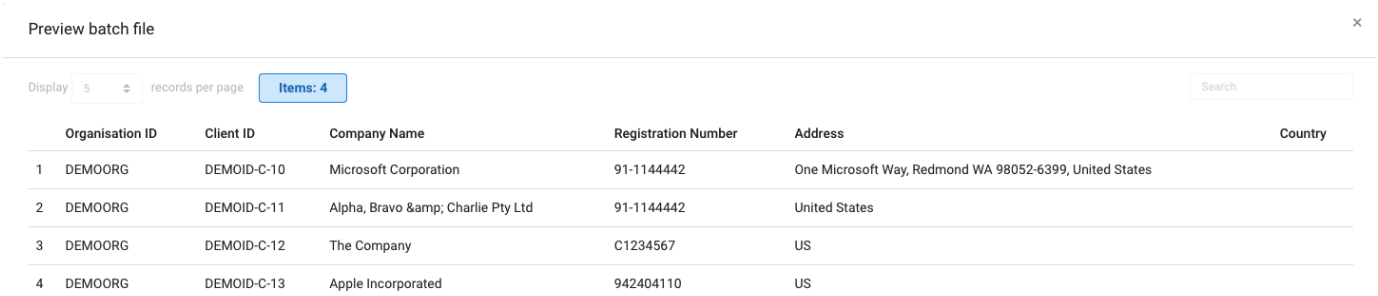
Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	Company Name	Registration Number	Address	Country
1	DEMOORG		Microsoft Corporation			
2	DEMOORG		Alpha, Bravo & Charlie Pty Ltd			
3	DEMOORG		The Company			
4	DEMOORG		Apple Incorporated			

Type of Data Required	Download Sample
	CSV XML

- Org ID
- Company Name

Full company details:



Preview batch file

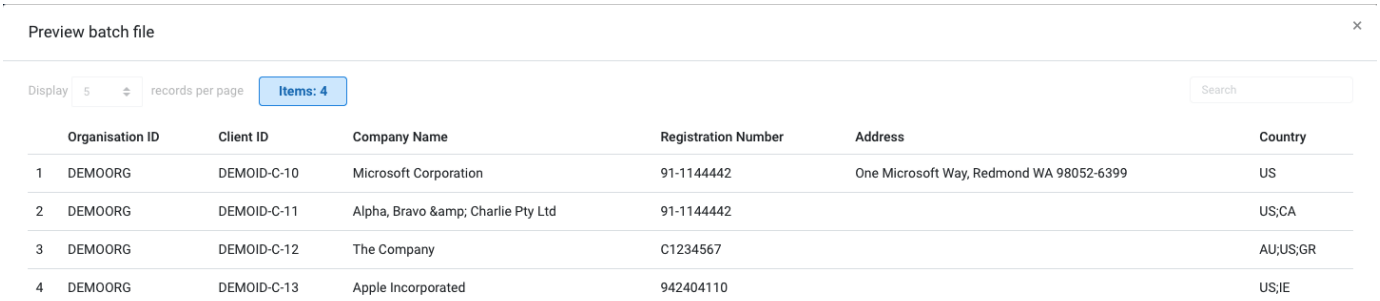
Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	Company Name	Registration Number	Address	Country
1	DEMOORG	DEMOID-C-10	Microsoft Corporation	91-1144442	One Microsoft Way, Redmond WA 98052-6399, United States	
2	DEMOORG	DEMOID-C-11	Alpha, Bravo & Charlie Pty Ltd	91-1144442	United States	
3	DEMOORG	DEMOID-C-12	The Company	C1234567	US	
4	DEMOORG	DEMOID-C-13	Apple Incorporated	942404110	US	

Type of Data Required	Download Sample
	CSV XML

- Org ID
- Client ID
- Company Name
- Registration Number
- Address/Country

Company details with multiple operating locations:



Preview batch file

Display 5 records per page Items: 4 Search

	Organisation ID	Client ID	Company Name	Registration Number	Address	Country
1	DEMOORG	DEMOID-C-10	Microsoft Corporation	91-1144442	One Microsoft Way, Redmond WA 98052-6399	US
2	DEMOORG	DEMOID-C-11	Alpha, Bravo & Charlie Pty Ltd	91-1144442		US;CA
3	DEMOORG	DEMOID-C-12	The Company	C1234567		AU;US;GR
4	DEMOORG	DEMOID-C-13	Apple Incorporated	942404110		US;IE

Type of Data Required	Download Sample

	CSV	XML

- Org ID
- Client ID
- Company Name
- Registration Number
- Address/Country
- Countries

CSV Batch Files Explained

A CSV (comma separated values) file is a text file containing records and fields delimited with commas. You can create a CSV file containing multiple records where each line records represents a profile. The CSV file follows a specific format and specific order of fields.

- Each line of the file represents a record (details of one individual or entity)
- Each line of the profile starts with your assigned Organisation ID. This information is available in your account enrolment email or within the Organisation Details if you have appropriate access.
- Headings are optional in the CSV. If included, the first line must start with `OrgId` to be recognised.
- Each line is terminated with a carriage return and line feed, `CRLF` or `\r\n`.
- The sequence order of the fields are important as they will be processed as specific types of information
- Details containing commas (e.g. addresses, company names etc.) should be enclosed with double quotes (`"`)
- Special symbols should be replaced by HTML characters e.g. `&` should be written as `&`

- Each line is separated or delimited by commas without spaces in between fields. The commas are necessary to differentiate the sequence of fields. Do not remove the commas even if fields are empty
- Batch files containing original script, umlauts or diacritics should be saved in UTF-8 encoding to preserve the information.

Batch files for **Individuals** and **Corporates** are separate and different due to their different structure and contents.

Individuals

Based on your organisation settings, the requirements for the minimum information required to be included in the batch file may differ.

Additional information may be required as a minimum for the batch file to be processed if for example:

- **Date of Birth** is required if **Ignore Blank DOB** is enabled
- **Client ID** is required if **Ongoing Monitoring** is enabled

If your organisation has **Default Country** specified and **Apply Blank Address** enabled, leaving the **Address** field blank will default to the specified country.

The order of the fields in the CSV file are important and are as follows:

Field	Order	Required	Character Limit	Remarks
OrgID	**1**	Mandatory	20	The **OrgID** associated with the organisation or suborganisation you are scanning against. This is assigned to your organisation during enrolment. If unsure, please contact your organisation's **Compliance Officer**.
ClientID	**2**	Conditional	100	Unique identifier for the individual such as Customer Reference Number. This is required for due diligence decisions and for ongoing monitoring.

FirstName	**3**	Mandatory	255	First name or Given name of the individual. This field is required unless you are entering an Original Script Name or Full Name. If the person has a single mononymous name, enter a dash (`-`) in this field and the mononymous name into **LastName**.
MiddleName	**4**	Optional	255	If the individual has multiple middle names, enter all middle names separated by spaces.
LastName	**5**	Mandatory	255	Last Name or Surname or Family Name of the individual. If the individual has a single mononymous name, enter the name in this field.
DateofBirth	**6**	Conditional	10	This is Required if **Ignore Blank DOB** is enabled for the organisation by the Compliance Officer. Supported formats: `DD/MM/YYYY` or `YYYY`
Address	**7**	Optional	255	You may enter the full address enclosed in double quotes, or just the Country. Only the Country in the address field will be used for matching.
Gender	**8**	Optional	20	The application will recognise: `Female` , `F` , `Male` , or `M` .
OriginalScriptName	**9**	Optional	255	Non-Latin-based original script name such as Cyrillic, Hebrew, Chinese, Korean, Arabic etc, or Latin-based full name if unable to identify and separate by First and Last Names.
IDNumber	**10**	Optional	100	Identifier for the individual such as Passport Number, National ID, VAT/Tax Number, Professional Registration Number.

Country	**11**	Optional	15	ISO 3166-1 alpha-2 code equivalent for the country of residence. Use semicolon (;) to separate values. Supports up to 5 countries.
Nationality	**12**	Optional	15	ISO 3166-1 alpha-2 country code equivalent for the individual's nationality or citizenship. Use semicolon (;) to separate values. Supports up to 5 countries.

An example of a CSV batch file viewed in a spreadsheet e.g. MS Excel

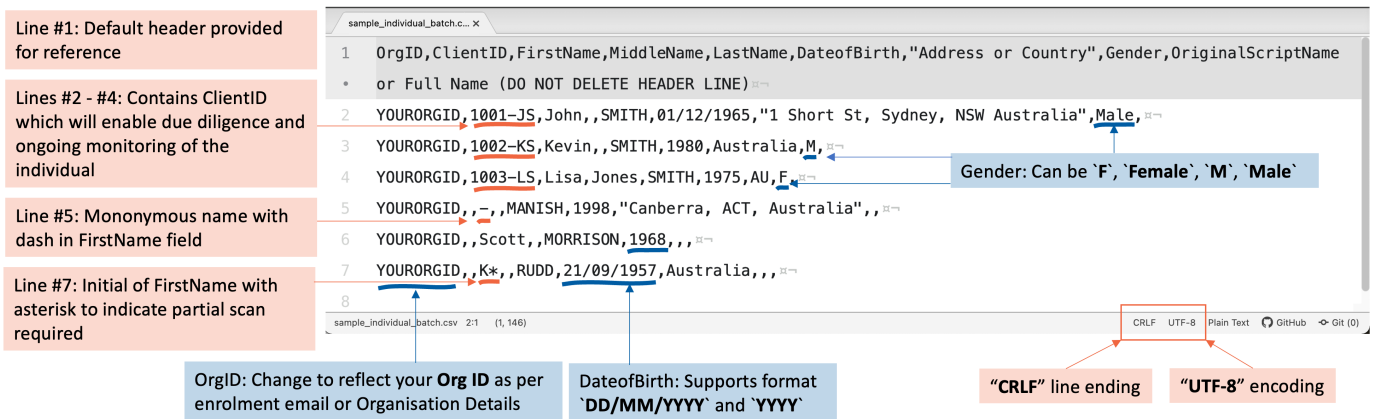
	A	B	C	D	E	F	G	H	I	J	K	L
1	OrgID (DO NOT DELETE HEADER)	ClientID	FirstName	MiddleName	LastName	DateofBirth	Address or Country	Gender	OriginalScriptName or Full Name	IDNumber	Countries, up to 5 separated by semicolon (;)	Nationality, up to 5 separated by semicolon (;)
2	DEMOORG	DEMOID-100	Scott	John	MORRISON	13/5/1968	AU	Male		PA234567		AU
3	DEMOORG	DEMOID-101	Chris		BOWEN	1973	Fairfield, NSW, Australia	Male		PA1000111		AU
4	DEMOORG	DEMOID-102				2/3/1963		M	Anthony Norman ALBANESE	PA0123456	AU	AU
5	DEMOORG	DEMOID-103				1959	15 Coronation Drive, Yarralumla, ACT 2600	Male	廖嬋娥	DE1234567	AU;CN	CN
6	DEMOORG	DEMOID-104	Benjamin		Smith			Male			FR;GB	CA;US

An example of a CSV batch file viewed in a text editor e.g. Atom. Some advanced text editors can provide greater insight to the structure and encoding of a CSV file compared to Excel spreadsheet.

sample_batch_individual_...

```
1  OrgID (DO NOT DELETE HEADER),ClientID,FirstName,MiddleName,LastName,DateofBirth,Address or
•  Country,Gender,OriginalScriptName or Full Name,IDNumber,"Countries, up to 5 separated by semicolon
•  (;)","Nationality, up to 5 separated by semicolon (;)"
2  DEMOORG,DEMOID-100,Scott,John,MORRISON,13/5/1968,AU,Male,,PA234567,,AU
3  DEMOORG,DEMOID-101,Chris,,BOWEN,1973,"Fairfield, NSW, Australia",Male,,PA1000111,,AU
4  DEMOORG,DEMOID-102,,,,2/3/1963,,M,Anthony Norman ALBANESE,PA0123456,AU,AU
5  DEMOORG,DEMOID-103,,,,1959,"15 Coronation Drive, Yarralumla, ACT 2600",Male,廖嬋娥,DE1234567,AU;CN,CN
6  DEMOORG,DEMOID-104,Benjamin,,Smith,,,Male,,,FR;GB,CA;US
```

The key elements of the CSV batch file:



Corporates

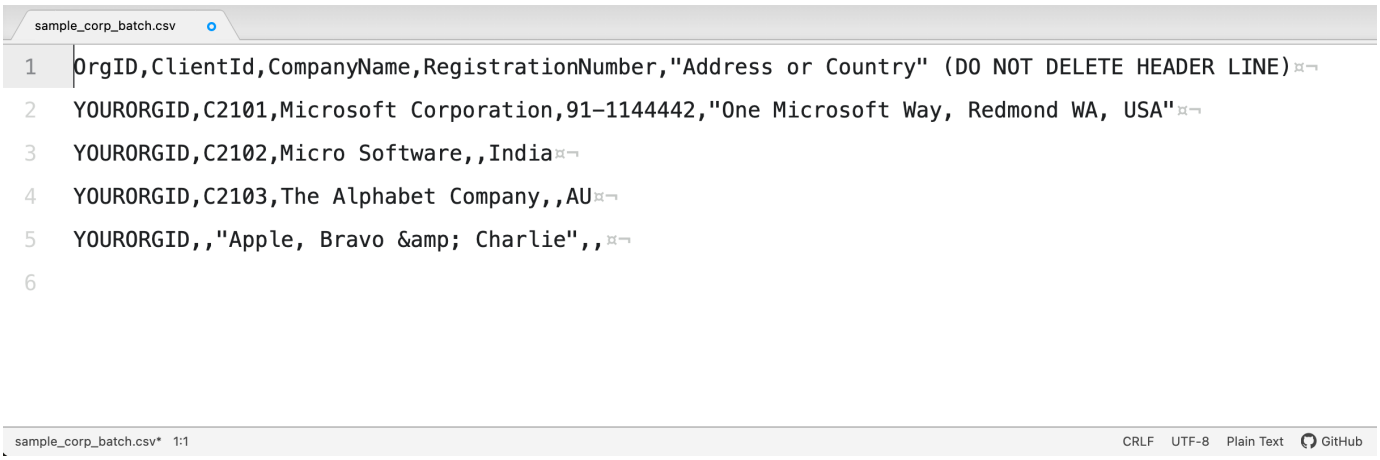
The order of the fields in the CSV file are as follows:

Field	Order	Required	Character Limit	Remarks
OrgID	**1**	Mandatory	20	The **OrgID** associated with the organisation or suborganisation you are scanning against. This is assigned to your organisation during enrolment. If unsure, please contact your organisation's **Compliance Officer**.
ClientID	**2**	Optional		Unique identifier for the company such as Company Reference Number or Account Number. This is Required for due diligence decisions.
CompanyName	**3**	Mandatory	255	Name of company.
RegistrationNumber	**4**	Optional	100	Company's registration number such as ABN, ACN, NZBN, CRN, RN or equivalent.
Address	**5**	Optional	255	The company's country of operation or registration. Enter the ISO 3166-1 2-letter country code, or the country name. You can also enter the full address (there are no restrictions imposed on the address format). Only the country component will be used for comparing country of operation or registration when the Country of Operation policy is applied during scanning.
Country	**16**	Optional	15	ISO 3166-1 alpha-2 code equivalent for the country of operation. Use semicolon (`;`) to separate values. Supports up to 5 countries.

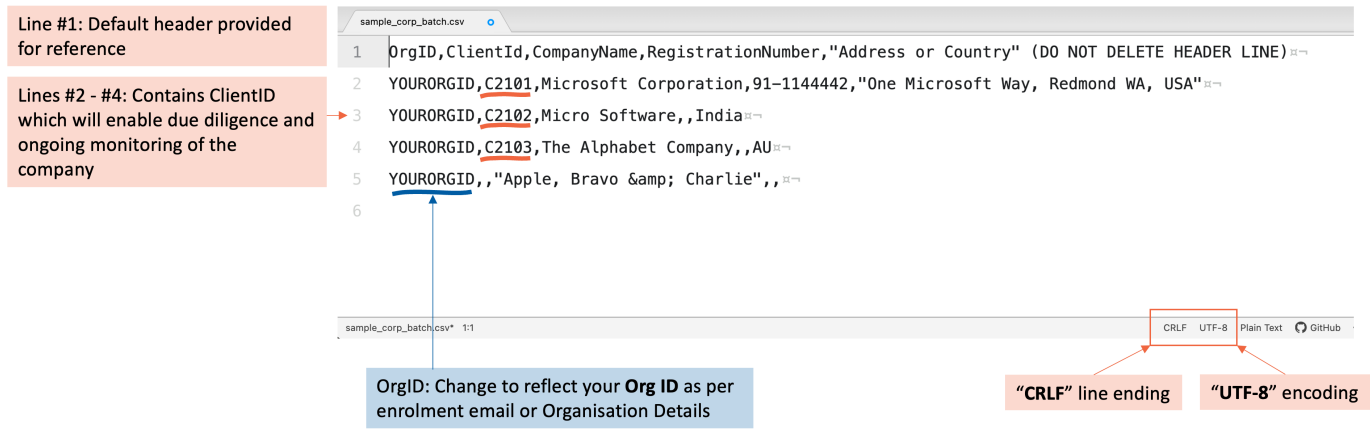
An example of a CSV viewed in a spreadsheet e.g. MS Excel

	A	B	C	D	E	F
1	OrgID (DO NOT DELETE HEADER)	ClientID	CompanyName	RegistrationNumber	Address or Country	Countries, up to 5 separated by semicolon (;)
2	DEMOORG	DEMOID-C-10	Microsoft Corporation	91-1144442	One Microsoft Way, Redmond WA 98052-6399	US
3	DEMOORG	DEMOID-C-11	Alpha, Bravo & Charlie Pty Ltd	91-1144442		US;CA
4	DEMOORG	DEMOID-C-12	The Company	C1234567		AU;US;GR
5	DEMOORG	DEMOID-C-13	Apple Incorporated	942404110		US;IE
6	DEMOORG	DEMOID-C-14	Micro Software		IN	

An example of a CSV batch file viewed in a text editor e.g. Pulsar. Some advanced text editors can provide greater insight to the structure and encoding of a CSV file compared to Excel spreadsheet.



The key elements of the CSV batch file:



'Null' names or strings

Due to a technicality in the processing of CSV files within the system, the string "NULL" (`N-U-L-L`) should be avoided as this will be ignored by the system. To enter this as a name or string text, use `"Null"` or `"null"` (`N-u-l-l` or `n-u-l-l`) to avoid all uppercase.

XML Batch Files Explained

Individuals

The batch XML file can be validated against the following DTD.

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT InputList (Person+)><!ELEMENT Person (OrgID, MemberNumber?, ClientID?,
FirstName, MiddleName?, Surname, DOB?, Address?, Gender?, ScriptNameFullName?,
IDNumber?)>
<!ELEMENT OrgID (#PCDATA)>
<!ELEMENT MemberNumber (#PCDATA)> <!-- superseded by ClientID -->
<!ELEMENT ClientID (#PCDATA)>
<!ELEMENT FirstName (#PCDATA)>
<!ELEMENT MiddleName (#PCDATA)>
<!ELEMENT Surname (#PCDATA)>
<!ELEMENT DOB (#PCDATA)>
<!ELEMENT Address (#PCDATA)>
<!ELEMENT Gender (#PCDATA)>
<!ELEMENT OriginalName (#PCDATA)> <!-- (if Original Script Search is enabled) -->
<!ELEMENT ScriptNameFullName (#PCDATA)> <!-- (if Original Script Search is
enabled) -->
<!ELEMENT IDNumber (#PCDATA)>
<!ELEMENT Country (#PCDATA)>
<!ELEMENT Nationality (#PCDATA)>
```

The format of the XML file may be similar to the following example where we have the full address in `Address`:

```
<?xml version="1.0" encoding="utf-8" ?>
<InputList>
    <Person>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-100</ClientID>
        <FirstName>John</FirstName>
        <MiddleName>Andrew</MiddleName>
        <Surname>SMITH</Surname>
        <DOB>13/05/1968</DOB>
        <Address>1 Short Street, Sydney, 2000 NSW, Australia</Address>
        <Gender>Male</Gender>
        <ScriptNameFullName></ScriptNameFullName>
        <IDNumber>M1234567</IDNumber>
    </Person>
</InputList>
```

This can be simplified using the ISO 3166-1 2-letter country code in `Address`:

```
<?xml version="1.0" encoding="utf-8" ?>
<InputList>
    <Person>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-100</ClientID>
        <FirstName>John</FirstName>
        <MiddleName>Andrew</MiddleName>
        <Surname>SMITH</Surname>
        <DOB>13/05/1968</DOB>
        <Address>AU</Address>
        <Gender>Male</Gender>
        <ScriptNameFullName></ScriptNameFullName>
        <IDNumber>M1234567</IDNumber>
    </Person>
</InputList>
```

For dual citizenship:

```
<?xml version="1.0" encoding="utf-8" ?>
<InputList>
    <Person>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-100</ClientID>
        <FirstName>John</FirstName>
        <MiddleName>Andrew</MiddleName>
        <Surname>SMITH</Surname>
        <DOB>13/05/1968</DOB>
        <Address>AU</Address>
        <Gender>Male</Gender>
        <ScriptNameFullName></ScriptNameFullName>
        <IDNumber>M1234567</IDNumber>
        <Nationality>AU;GB</Nationality>
    </Person>
</InputList>
```

For multiple country of residences:

```
<?xml version="1.0" encoding="utf-8" ?>
<InputList>
    <Person>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-100</ClientID>
        <FirstName>John</FirstName>
        <MiddleName>Andrew</MiddleName>
        <Surname>SMITH</Surname>
        <DOB>13/05/1968</DOB>
        <Address>AU</Address>
        <Gender>Male</Gender>
```

```
        <ScriptNameFullName></ScriptNameFullName>
        <IDNumber>M1234567</IDNumber>
        <Country>CA;US;FR</Country>
    </Person>
</InputList>
```

Corporates

The batch XML file can be validated against the following DTD.

```
<?xml version="1.0" encoding="UTF-8"?>
   <!ELEMENT InputList (Company+)>
   <!ELEMENT Company (OrgID, EmployerNumber?, ClientID?, CompanyName, IDNumber?,
RegistrationNumber?, Address?)>
   <!ELEMENT OrgID (#PCDATA)>
   <!ELEMENT EmployerNumber (#PCDATA)> <!-- superseded by ClientId -->
   <!ELEMENT ClientID (#PCDATA)>
   <!ELEMENT CompanyName (#PCDATA)>
   <!ELEMENT IDNumber (#PCDATA)> <!-- superseded by RegistrationNumber -->
   <!ELEMENT RegistrationNumber (#PCDATA)>
   <!ELEMENT Address (#PCDATA)>
   <!ELEMENT Country (#PCDATA)>
```

The format of the XML file may be similar to the following example where we have the full address in `Address`:

```
<?xml version="1.0" encoding="utf-8" ?>
   <InputList>
    <Company>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-C-100</ClientID>
        <CompanyName>ABC Corporation</CompanyName>
        <RegistrationNumber>12 345 678 012</RegistrationNumber>
        <Address>One Alphabet Way, Sydney, 2000, NSW, Australia</Address>
    </Company>
   </InputList>
```

This can be simplified using the ISO 3166-1 2-letter country code in `Address`, and the spaces removed from the ABN in `RegistrationNumber`:

```
<?xml version="1.0" encoding="utf-8" ?>
   <InputList>
    <Company>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-C-100</ClientID>
```

```
        <CompanyName>ABC Corporation</CompanyName>
        <RegistrationNumber>12345678012</RegistrationNumber>
        <Address>AU</Address>
     </Company>
    </InputList>
```

Example with multiple countries of operation:

```
<?xml version="1.0" encoding="utf-8" ?>
   <InputList>
    <Company>
        <OrgID>DEMOORG</OrgID>
        <ClientID>DEMOID-C-100</ClientID>
        <CompanyName>ABC Corporation</CompanyName>
        <RegistrationNumber>12345678012</RegistrationNumber>
        <Country>AU;JP;US</Country>
    </Company>
   </InputList>
```

Common Questions

Batch file not able to be processed

If a batch file is not able to be processed, please check if the following are applicable to your batch file **Encoding and formatting**:

- The file has `UTF-8` encoding
- Line breaks for each record is separated by carriage return and line feed e.g. `CRLF` or `\r\n`
- Ampersands should be replaced with HTML format e.g. `&`
- The OrgID in the profile records refers to your own organisation. The header should not be changed.

Should I use Excel or a text editor to view a batch file?

Both options provide different advantages and can be used to complement each other.

Viewing the CSV batch file via a spreadsheet such as MS Excel will provide a quick overview of the contents of the CSV file and if contents are listed under the correct fields or columns. However, it does not provide detailed information on the encoding, or type of line breaks used in the file, or if there are correct number of specified fields in a row. Additionally, Excel may have some limitations on the size of the contents of a cell.

An advanced text editor e.g. *Atom*, *Notepad++*, *Sublime Text*, to name a few, provides detailed insights to the encoding and structure of the CSV file, the explicit number of fields per row, and the ability to control and change the encoding of the file and line breaks. However, it may be a bit more challenging to obtain an overview of the contents compared to a spreadsheet.

Therefore, it is not unusual to use Excel for an initial review of the contents of the batch file. If troubleshooting is required, the use of advanced text editors can be used for more detailed investigation into the batch file.

Custom Watchlist Templates and Samples

MemberCheck supports custom watchlist to enable you to extend the PEP and Sanction screening to include any blacklist or specific lists applicable to your organisation.

The custom watchlist templates for **Individuals** and **Corporates** require separate CSVs due to their different structure and schema.

The sample templates have been provided to assist you in preparing your own files.

Templates

Example	Download Sample
Custom watchlist for individual profiles	CSV
Custom watchlist for corporate profiles	CSV

Individual Custom Watchlist

The fields in the CSV file for individual entities are as follows:

Field	Required	Remarks
UniqueID	Mandatory	The unique identifier for the entity for tracking within the system.
Names	Mandatory	Name of the entity including variations in spelling and aliases. Supports multiple names.
DOBs	Optional	Full date of birth or year of birth. Supports multiple dates.
Gender	Optional	Gender of the profile.
Addresses	Optional	Registered or known locations associated with the entity. Supports multiple addresses.

LinkedIndividuals	Optional	Other individuals associated with this entity. Supports multiple unique identifiers (`UniqueID`) of profiles defined in the same custom watchlist.
LinkedCompanies	Optional	Other business entities associated with this entity. Supports multiple unique identifiers (`UniqueID`) of profiles defined in the corporate custom watchlist.

Formatting and Samples

The first row of the CSV contains the header.
Please keep the items in the header and ensure the contents match the sequence of the header items.

Some fields support array of multiple values, for example: Names, Date of Birth, Addresses, Linked Individuals and Linked Companies. For multiple values in the array, each set of data should be separated by semicolon (`;`) and text containing commas (`,`) should be enclosed with double quotes (`"`).

The first value in the array of multiple values are considered primary data and will be displayed as the main data in the result profile.

Details of supported formats and examples:

Field	Supported Formats	Examples
UniqueID	Up to 10 digits	Unique identifier from 1 up to 10 digits: • `1` • `10001` • `100001` • `200001`

Names	Up to 255 characters per name. Supported name formats: • FirstName,MiddleName,LastName • FirstName,LastName • FirstName LastName • OriginalScriptName For mononymous names, please enter dash (`-`) for the FirstName and the actual name in the LastName. See example for `Suharto` in the next column.	Single name: • `"Charles,Montgomery,Burns"` • `"Charles, Burns"` • `Charles Burns` • `- Suharto` • `習近平` Multiple names: • `"Charles,Montgomery,Burns; Monty,Burns; Charlie Burns"` • `"Jinping XI; 習近平; 近平習"`

DOBs	Supported date formats: • DD-MM-YYYY • DD/MM/YYYY • DD MMM YYYY • YYYY-MM-DD • YYYY/MM/DD • YYYY	Single date: • `20-04-1960` • `20/04/1960` • `20 APR 1960` • `1960-04-20` • `1960/04/20` • `1960` Multiple dates: • `1960; 1961; 01/01/1961` • `"1950-04-01; 1950-04-02"`
Gender	Supported gender values: • Female • Male For "Unspecified" gender, please leave blank.	• `Female` • `female` • `Male` • `male`

Addresses

Address contains 6 specific components separated by commas (`,`).

The country component is essential to enable screening by Country of Residence. Other components are not used in the screening but provide more detailed information for the profile.

Leave the components blank if you do not have information.

- Building name
- Street address
- City
- State or County
- Postal or Zip code
- **Country**

Single location:

- `",,,,,MU"`
- `",,Notting Hill,London,,GB"`
- `",213/100 Railway Street,Chatswood,NSW, AU"`
- `"Building A, 213/100 Railway Street, Chatswood, NSW, 2067, AU"`
- `"Character Building, 742 Evergreen Terrace, Springfield, Oregon,, US"`

Multiple locations:

- `",,Port Louis,,,MU; ,,Pretoria,,,ZA; ,,Maputo,,,`
- `",,Notting Hill,London,,GB; ,,Canberra, ACT,, AU; ,,Arlington, Virginia,,US"`
- `"Character Building, 742 Evergreen Terrace, Springfield, Oregon,, US; ,,San Angelo,Texas,,US"`

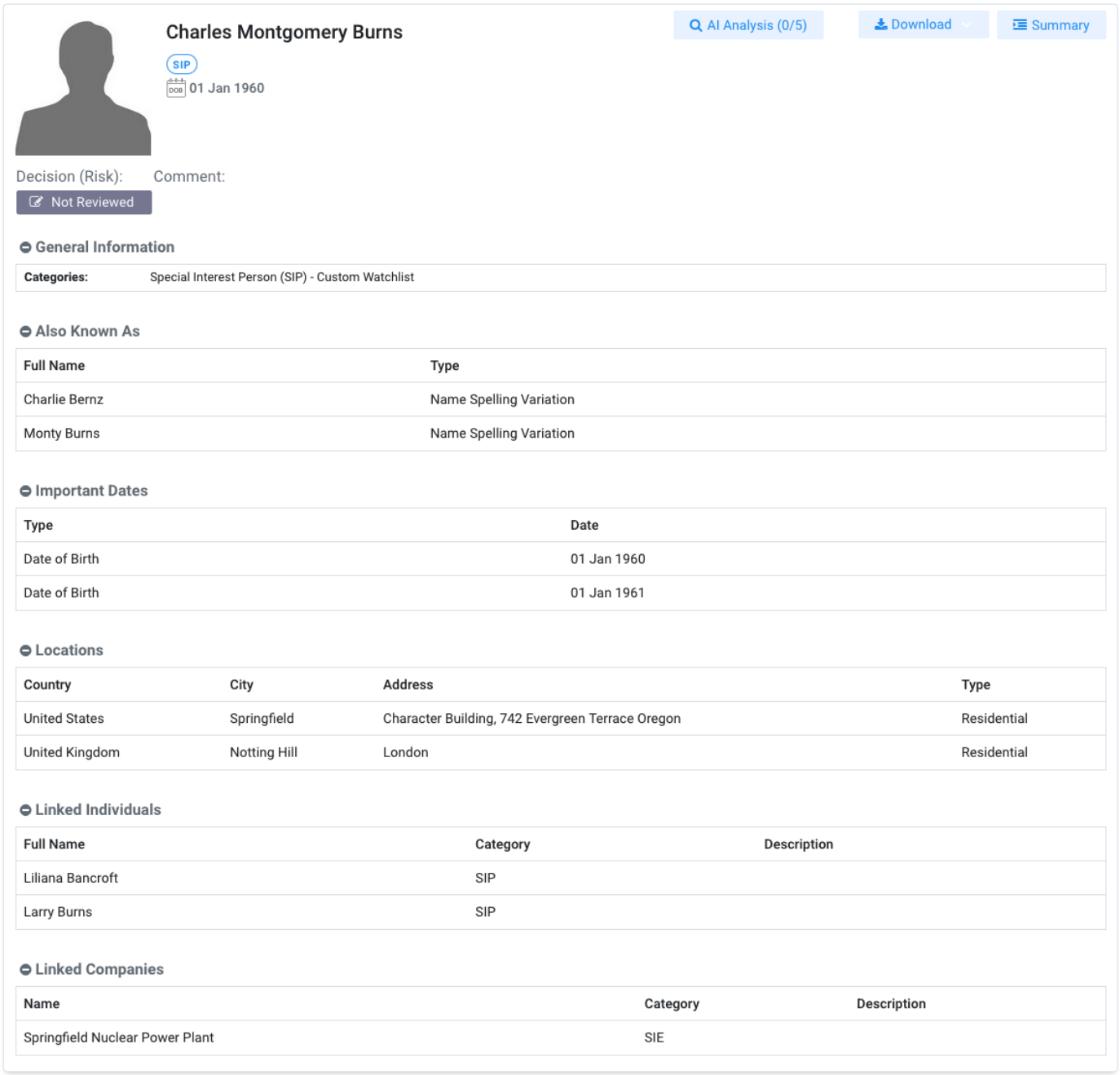
Note: To minimise incompatibilities with variations country name spelling, we recommend using the IS 3166-1 2-letter code for country names.

LinkedIndividuals	The unique identifier (**UniqueID**) of the individual(s) associated with this entity. Ensure the unique identifier refers to an existing profile in the same custom watchlist.	Single associated individual: • `10001` Multiple associated individuals: • `10001;10002;10335`
LinkedCompanies	The unique identifier (**UniqueID**) of the business entity associated with this entity. Ensure the unique identifier refers to an existing profile in the corporate custom watchlist to be uploaded together with the individual custom watchlist.	Single associated company: • `50001` Multiple associated individuals: • `50001;50002`

Example of CSV content

```
UniqueID,Names,Gender,DOBs,"Addresses (Building,Street
address,City,State,Postal code,Country)",LinkedIndividuals,LinkedCompanies
1001,"Charles, Montgomery, Burns; Monty Burns; Charlie Bernz",Male,
1960-01-01;01/01/1961,"Character Building, 742 Evergreen Terrace,
Springfield, Oregon,,US; ,,Notting Hill,London,,GB",1002;1003,5001
1002,"Liliana, Bancroft;Liliana, Lily, Bancroft;Lily, Bancroft",Female,
1955,",,,,,US",1001,
1003,Larry Burns, Male,1940-01-01;1939-12-31,",,,Oregon,,US",1001,
1004,Clifford Burns,Male,28/12/1980,",,San Angelo,Texas,,US",,5002
1005,- Suharto;- Soeharto,Male,,",,,,,ID",,
```

Screening for `Charles Burns` would return the following profile from the sample custom watchlist:



Charles Montgomery Burns

AI Analysis (0/5) Download Summary

SIP

DOB 01 Jan 1960

Decision (Risk): Comment:

Not Reviewed

General Information

Categories:	Special Interest Person (SIP) - Custom Watchlist

Also Known As

Full Name	Type
Charlie Bernz	Name Spelling Variation
Monty Burns	Name Spelling Variation

Important Dates

Type	Date
Date of Birth	01 Jan 1960
Date of Birth	01 Jan 1961

Locations

Country	City	Address	Type
United States	Springfield	Character Building, 742 Evergreen Terrace Oregon	Residential
United Kingdom	Notting Hill	London	Residential

Linked Individuals

Full Name	Category	Description
Liliana Bancroft	SIP	
Larry Burns	SIP	

Linked Companies

Name	Category	Description
Springfield Nuclear Power Plant	SIE	

Corporate Custom Watchlist

The fields in the CSV file for corporate entities are as follows:

Field	Required	Remarks
UniqueID	Mandatory	The unique identifier for the entity for tracking within the system.
Names	Mandatory	Name of the entity including variations in spelling and aliases. Supports multiple names.

Addresses	Optional	Registered or known locations associated with the entity. Supports multiple addresses.
LinkedIndividuals	Optional	Other individuals associated with this entity. Supports multiple unique identifiers (`UniqueID`) of profiles defined in the Individuals custom watchlist.
LinkedCompanies	Optional	Other business entities associated with this entity. Supports multiple unique identifiers (`UniqueID`) of profiles defined in the same custom watchlist.

Formatting and Samples

The first row of the CSV contains the header.
Please keep the items in the header and ensure the contents match the sequence of the header items.

Some fields support array of multiple values, for example: Names, Addresses, Linked Individuals, and Linked Companies. For multiple values in the array, each set of data should be separated by semicolon (`;`) and text containing commas (`,`) should be enclosed with double quotes (`"`).

The first value in the array of multiple values are considered primary data and will be displayed as the main data in the result profile.

Details of supported formats and examples:

Field	Supported Formats	Examples
UniqueID	Up to 10 digits	Unique identifier from 1 up to 10 digits: • `1` • `10001` • `100001` • `200001`

Names	Up to 255 characters per name. Supported name formats: • CompanyName • OriginalScriptName	Single name: • `"AB & C Alphabet Company"` • `"Alpha, Bravo & Charlie Pty. Ltd."` • `Springfield Nuclear Power Plant` • `颐州烟草` Multiple names: • `"AB & C Alphabet Company; ABC Alphabet Company; The Alpha Bet Incorporated; The Company"` • `"China Tobacco Industrial Company Ltd; 颐州烟草"`

Addresses

Address contains 6 specific components separated by commas (`,`).

The country component is essential to enable screening by Country of Residence. Other components are not used in the screening but provide more detailed information for the profile.

Leave the components blank if you do not have information.

- Building
- Street address
- City
- State or County
- Postal or Zip code
- **Country**

Single location:

- `",,,,,MU"`
- `",,Notting Hill,London,,GB"`
- `",213/100 Railway Street,Chatswood,NSW,, AU"`
- `"Building A, 213/100 Railway Street, Chatswood, NSW, 2067, AU"`
- `"Tower A, 1002 Evergreen Terrace, Springfield, Oregon,, US"`

Multiple locations:

- `",,Port Louis,,,MU; ,,Pretoria,,,ZA; ,,Maputo,,,MZ"`
- `",,Notting Hill,London,,GB; ,,Canberra, ACT,, AU; ,,Arlington, Virginia,,US"`
- `"Tower A, 1002 Evergreen Terrace, Springfield, Oregon,, US; ,,San Angelo,Texas,,US"`

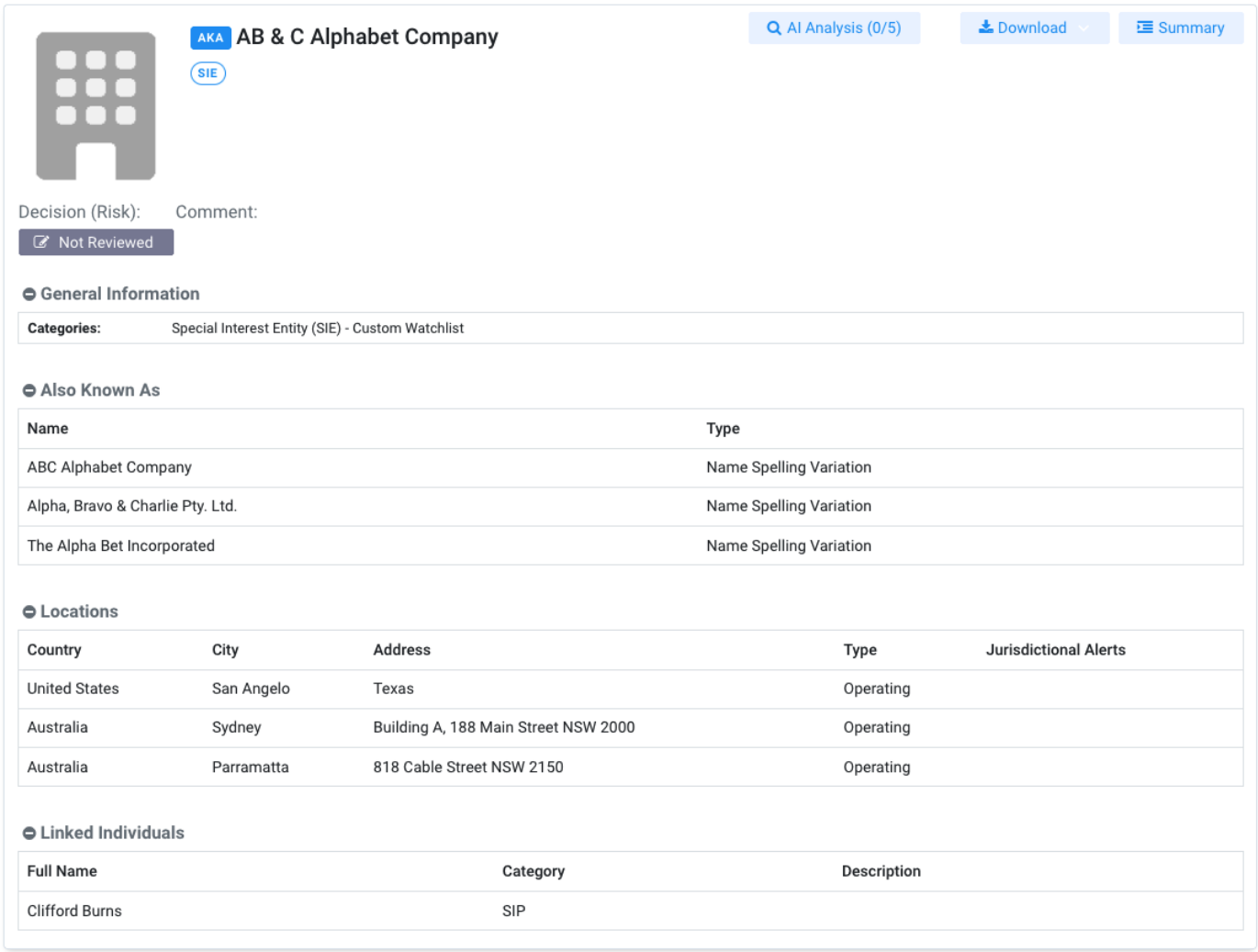
Note: To minimise incompatibilities with variations in country name spelling, we recommend using the ISO 3166-1 2-letter code for country names.

LinkedIndividuals	The unique identifier (**UniqueID**) of the individual(s) associated with this entity. Ensure the unique identifier refers to an existing profile in the Individuals custom watchlist to be uploaded together with the corporate custom watchlist.	Single associated individual: • `10001` Multiple associated individuals: • `10001;10002;10335`
LinkedCompanies	The unique identifier (**UniqueID**) of the business entity associated with this entity. Ensure the unique identifier refers to an existing profile in the same corporate custom watchlist.	Single associated company: • `50001` Multiple associated individuals: • `50001;50002`

Example of CSV content

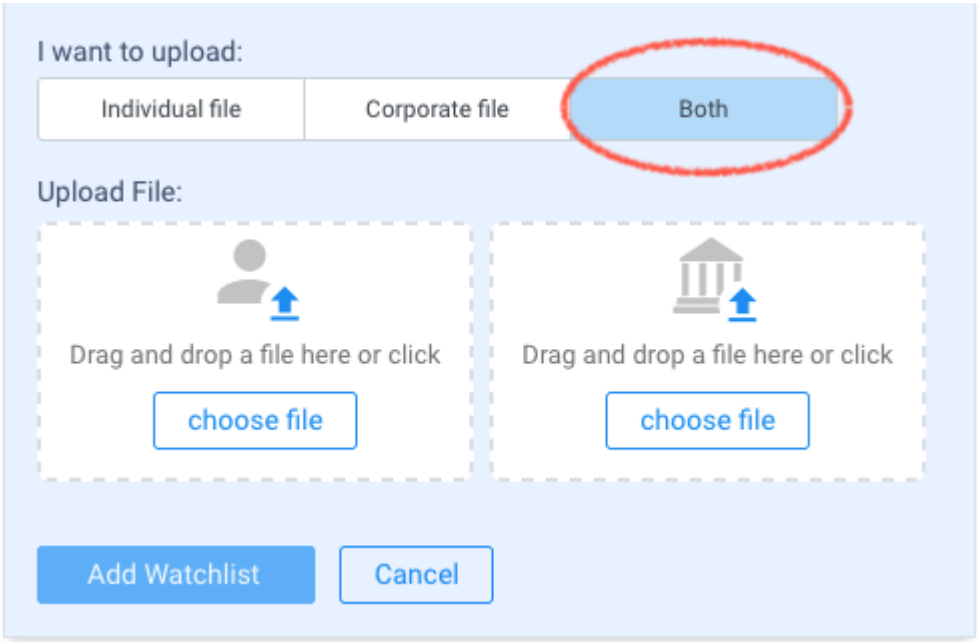
```
UniqueID,Names,"Addresses (Building,Street address,City,State,Postal
code,Country)",LinkedIndividuals,LinkedCompanies
5001,Springfield Nuclear Power Plant,",,Springfield,Oregon,,US",1001,
5002,"AB & C Alphabet Company; ABC Alphabet Company; The Alpha Bet
Incorporated; Alpha, Bravo & Charlie Pty. Ltd.",",,San Angelo,Texas,,US;
Building A, 188 Main Street, Sydney, NSW, 2000, AU; ,818 Cable Street,
Parramatta, NSW, 2150, AU",1004,
5003,Lumosyn Innovations Pty Ltd; ルモシン・イノベーションズ; 露莫森新,",,
Kunming, Yunnan Province,, CN",,5004
5004,Nexara Technologies; Teknologi Nexara; ネクサラテクノロジーズ,",,,,,ID",,
5003
```

Screening for `ABC Alphabet Company` would return the following profile from the sample custom watchlist:



Cross-linking Individuals and Corporates

To cross-link profiles in the Individual and Corporate custom watchlists, you need to upload both files together. Uploading these files separately will not be able to create the associated relationships.



Encoding and formatting

For the best compatibility and success of processing the CSV custom watchlists, please ensure you apply the following to your CSVs:

- The file has `UTF-8` encoding
- Line breaks for each record is separated by carriage return and line feed e.g. `CRLF` or `\r\n`
- Each set of data within multiple-value array should be separated by semicolon (`;`)
- Values containing commas (`,`) should be enclosed with double quotes (`"`)
- Dates should follow any of the supported formats as provided above.

Watch out for date formats in spreadsheets

Be mindful of date format changes when using spreadsheets. If you're editing and saving custom watchlists, ensure the date formats stay consistent. For instance, Excel might automatically reformat dates based on your system's settings.

Similar to batch files, you can use a text editor to review contents and formatting, if required.

API Integration

API Testing

Most of the API methods require authentication and requires an API Access Key or Bearer token. All API scans performed in the Developer Centre will count towards the Organisation scan count.

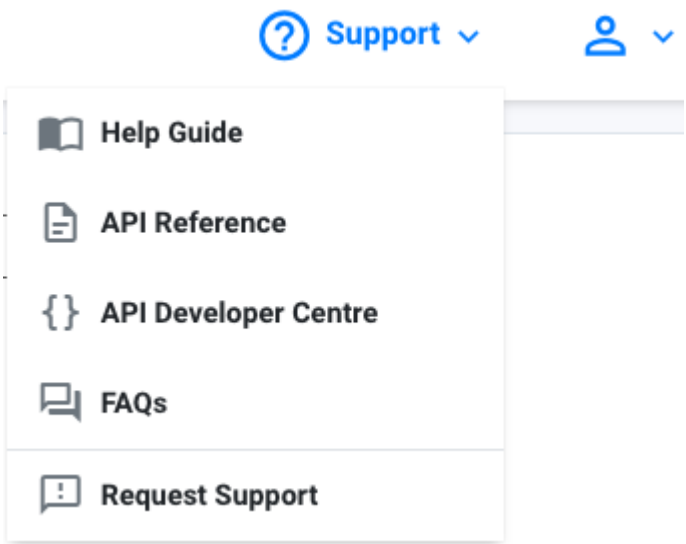
If you need to test the API without impacting on the organisation scan count, please contact your Account Manager or support@membercheck.com with this request.

API V2

API Documentation V2: https://api.membercheck.com/docs/index.html

API Developer Centre V2: https://api.membercheck.com/swagger/index.html

The API V2 documentation and developer centre (Swagger) is also available within the application under the **Support** menu item.



All examples in the API reference documentation refer to the default Demo URL. To send requests to a different environment in a different region, change the URL domain and check that your API key for your account is correct for the specific region and environment.

Default Demo URL: `https://demo.api.membercheck.com/api/v2`

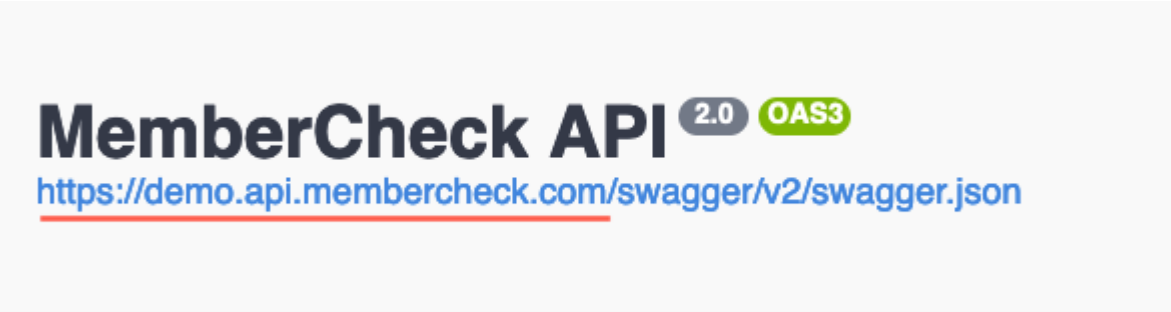
Production URL (Australia): `https://api.membercheck.com/api/v2`

Production URL (Germany): `https://api.eu.membercheck.com/api/v2`

Production URL (Indonesia): `https://api.id.membercheck.com/api/v2`

Production URL (GCC): `https://api.z.membercheck.com/api/v2`

The API domains are specific to the service region. You can find the API domain for your account within the **API Developer Centre**, accessible via the **Support** menu once you have logged in to the web application.



API Keys

The API keys are different for the Demo and Production environments. If you have accounts in both environments, please use the environment specific key to enable your requests to be successfully authenticated and authorised.

For information on generating an API Key for your account or another user account, please refer to the guide in API Keys.

API V1 (Classic) - decommissioned

> **Sunsetting API Classic V1**
>
> The API Classic V1 has been deprecated and decommissioned as of **May 7, 2023**.

The Classic API V1 documentation is available at the following link for historical reference purposes only:

API Documentation V1: https://app.membercheck.net/docs/index.html

FAQ

Login

- Unable to recognise username or password

Screening Names

- Screen an individual by the Original Script name
- Screen a person's Full Name instead of separating by First and Last Name
- Original Script Name or Full Name field not visible
- Screen by mononymous names (single names)
- Screening for translated names
- Options to reduce the number of false matches in Individual scans
- What does Close Name Match apply to?
- Search for a date of birth or year of birth within a range

Unique Client Identifier

- What is a Client ID and why is it important
- What if I don't have a Client ID?

Scan Results

- View or download a list of matches with specific decisions for audit
- What names are covered under Also Known As?
- Numerical codes appearing within the Original Script Names
- Accessing cached PDFs of adverse media links
- Accessing copyright adverse media
- Tax Haven and jurisdiction risk indicators in the profiles

- Profile Categories of PEP, POI, RCA and SIP

Due Diligence

- No options available to apply due diligence decisions
- Determining if an Individual or Corporate is a true match or a false match

Batch Files

- Limit of batch file sizes
- Possible reasons for failing batch files

Ongoing Monitoring

- Procedure for ongoing monitoring service
- No option to monitor Individuals and Corporates even though my account has Ongoing Monitoring activated
- Changes detected from automated ongoing monitoring
- Notification of detected changes via API Callback URL or email
- Enable Ongoing Monitoring for my account
- Monitoring Scan vs Monitoring Rescan

Identity Verification (IDV)

- List of countries supported for ID Verification

Watchlists

- Watchlists coverage for PEP & Sanctions scan
- Custom watchlists

Administration

- Change email recipient for scan notifications
- Change of the parent Organisation's Compliance Officer
- Compliance Officer limit on organisations

Testing services

- Dummy test profiles for trialling services

API

- API rate limits

Unable to recognise my username or password

MemberCheck operates in multiple regions worldwide, giving clients data sovereignty in their chosen location. Logins for each region are provided via distinct URLs in the account activation emails. These URLs are provided here for reference.

Region	Link
Asia Pacific (Australia)	https://app.membercheck.com
Asia Pacific (Indonesia)	https://app.id.membercheck.com
Europe (Germany)	https://app.eu.membercheck.com
Middle East (Oman)	https://app.z.membercheck.com

Screen an individual by the Original Script name

You can search by the Original Script Name (e.g. Arabic, Chinese, Cyrillic, Korean, Japanese, Thai and other non-Latin/Roman scripts). The **Original Script Search or Full Name** is an option that can be enabled by the Compliance Officer for the organisation as an additional search field.

The non-Latin script name must be entered into the **Original Script Name or Full Name** field to search against the Original Script Name in the watchlist record. There is no script conversion applied to the name fields (`First Name` , `Middle Name` , `Last Name`).

Example of **screening by Original Script Name**.

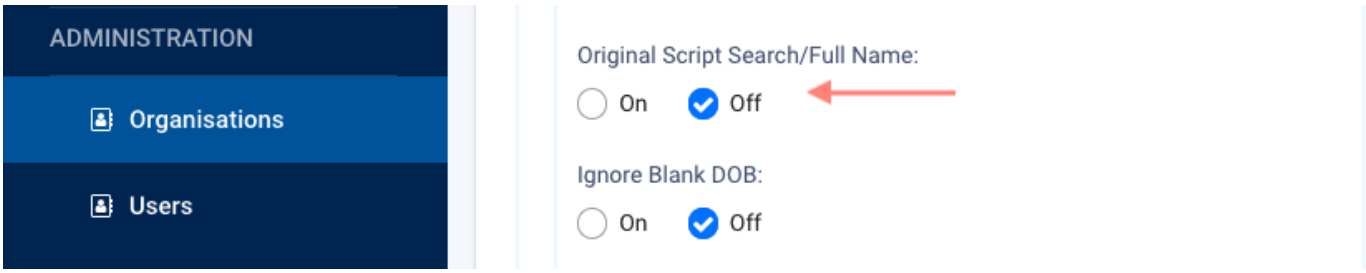
Screen a person's Full Name instead of separating by First and Last Name

If you are not able to separate the individual's name by First Name (or Given Name) and Last Name (or Family Name), you can search by the Full Name. Enter the full name into the **Original Script Name or Full Name** field. You can enter the name with the last/family name at the beginning or the end, e.g. `XI Jinping` or `Jinping XI`

Example of **screening by Full Name**.

Original Script Name or Full Name field not visible

If you are not able to view the **Original Script Name or Full Name** field in the **Single Scan** screen for Individuals, it is likely that your organisation settings has not enabled this option. Please check with your organisation's Compliance Officer to check this setting within the **Administration > Organisations** settings.



Screen by mononymous names (single names)

Where your customer or applicant has a single mononymous name, you can enter the name into the **Last Name** field. You must enter a dash (`-`) within the **First Name** field to indicate it is a mononym.

Screening for translated names

There are things that you can do to optimise your screening for translated names. We suggest screening with `Close` match with a match rate of `80%` for names that are translated into English and may have variations of spelling.

Options to reduce the number of false matches in Individual scans

MemberCheck is not able to provide any recommendations on your organisation's scan settings for your AML/CTF obligation. However, you can refer to the following information to assist you with optimising your scan settings to reduce false positives.

As the **Compliance Officer**, it is important to review and set up the scan settings in **Administration > Organisations > Settings** to exclude or filter scans which are not relevant.

The following settings and policies should be reviewed:

- **Default Country of Residence** and **Country of Residence Policy** for Individual screening

These 2 settings work in combination to enable the system to match the Member's country of residence against the watchlists. Where a member's country of residence is not able to be identified during a PEP & Sanctions scan, the Default Country of Residence defined by the CO will be used. Similarly, you can set the Default Country of Residence to be used in the event the member's country of residence is blank using the option `Apply to Blank Addresses` .

- **Default Country of Operation** and **Country of Operation Policy** for Corporate screening

Similar to above, these 2 settings work in combination to enable the system to match the company's country of operation against the watchlists. Where a country of operation is not able

to be identified during a Sanctions scan, the Default Country of Operation defined by the CO will be used.

- **Ignore Blank DOB**

Enabling this setting will enforce matching against date of birth of the member. This will require a DOB or YOB to be entered during PEP & Sanctions scanning, and the system will only return results where there is a match against the DOB. Where profiles in the watchlists do not contain DOB, these profiles will not be returned in the results.

- **Close Name Match Rate**

Close Name Match Rate sets the results returned based on the similarity of the names by assigning a percentage where `100%` is very close with minimal variations and `1%` being loosely similar. The default Close name match rate recommended by the system is `80%`, however the Compliance Officer may specify a different Close Match Rate to be applied for all scans, or leave the closeness of the name matching up to the user during scan. The match rate is only applied to the names and does not include date of birth or other data of the profile.

A reasonable close name match rate should be considered during scanning as a low Close Name Match Rate could return a large number of results containing all types of variations of the entered name.

For more information on these fields and their impact, please refer to **Customise Scan Settings**.

What does Close Name Match apply to?

The Close Name Match scan type and Close Name Match Rates in PEP, Sanction and Adverse Media screening only applies to the name fields such as First Name, Last Name and Full Name for Latin-based names. Currently, the close matching of names does not include Original Script Name (non-Latin based text e.g. Arabic, Cyrillic, Chinese, Korean etc.).

Close Name Match does not include other factors such as Date of Birth or Year of Birth.

How do I search for a date of birth or year of birth within a range?

You can specify a tolerance value for Date of Birth or Year of Birth during screening. If you do not see this option, or you are not able to change the number of years, the Compliance Officer for your Organisation may have turned this off or set a specific value based on screening policies.

What is a Client ID and why is it important

Client ID, formerly "Member Number" for Individuals or "Entity Number" for Companies, is the organisation’s unique identifier used to distinguish the individual being scanned (e.g. client reference, account number or profile name given during scanning). A Client ID is required for recording due diligence decisions, reporting and reconciliation, as well as ongoing monitoring of an Individual.

Similarly, a Client ID is required for recording due diligence decisions, reporting and reconciliation, as well as ongoing monitoring of a Corporate entity.

What if I don't have a Client ID?

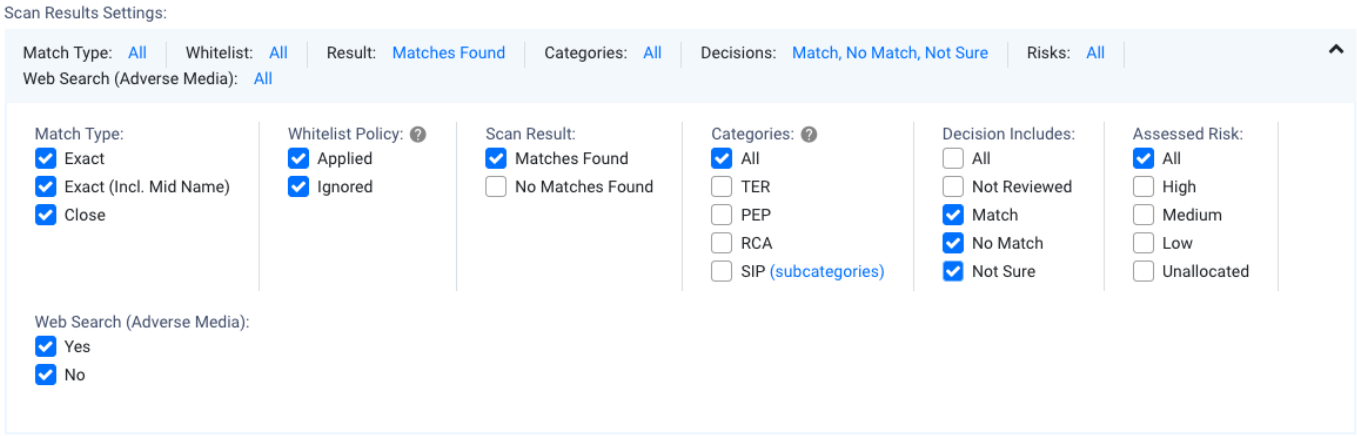
Client ID (e.g. client reference, account number or profile name given during scanning) is the organisation’s unique identifier used to distinguish the individual being scanned. It is used for recording due diligence decisions, reporting and reconciliation.

In cases where individuals do not have and never will have a Client ID, such as staff for example, arbitrary Client IDs can be used and prefixed by a letter, or letters, to distinguish them from your regular client base.

In cases where individuals may be allocated a Client ID in the future, such as new clients for example, an arbitrary number should not be allocated. The client identifier that will be allocated to the individual when they become a 'new client' should be used as the Client ID for scanning and tracking purposes. In this way, due diligence decisions will be allocated to the real client identifier and subsequently the whitelist will also be appropriately applied to that Client ID.

View or download a list of matches with specific decisions for audit

You can use a combination of options in the **Scan Result Settings** panel in **Scan Results** to filter the view and download the results for your organisation's record keeping.



- Go to **Scan Results** for either Individual or Corporate
- Specify a date range or leave blank to report on all scans
- Select the Scan Types **Batch** and **Single Scans** to ensure you have covered both types of scans
- Select the appropriate **Decisions** options e.g. `Match`, `No Match`, `Not Sure`, `Not Reviewed`
- To download the screened entities, click the `Download` button to preview or export the report as an Excel, PDF, Word or CSV file.
- To download the profiles which match the screened entities, click the `Download` button and select `Results Summary Report`.

You may be asked to present a record of screening performed and the due diligence conducted for your business. To do so, you can filter and download reports based on the specific decisions of `Match` and `No Match`.

What names appear under Also Known As?

This section of the profile record contains AKAs (Also Known As), FKAs (Formerly Known As) and aliases for both Individual and Corporate entity profiles. For Individuals, it may contain aliases, maiden names, variations of spelling of names, and original script names. It contains names which differ partially or completely from the name contained in the primary name fields, or names in addition to the name contained in the primary name fields.

Numerical codes appearing within the Original Script Names

For Chinese names, some may include the 'Chinese Commercial Codes' applicable to the name. These codes, which are four-digit numbers from `0000` to `9999`, have a one-to-one relationship with the corresponding Chinese characters and are searchable. For example, `5045 6602 1627` is equivalent to 習近平.

Accessing cached PDFs of adverse media links

This is applicable to specific data source subscriptions.

URLs to sources and adverse media links can be archived, moved, removed and changed causing broken links in the original URL. Where available, a PDF copy of the article is cached and made available with the date of the captured snapshot. To access this, look for hyperlinked dates in **Date of Capture**.

Where are there multiple dates with hyperlinks for the same article or publication, these are multiple snapshots taken at the various dates indicated.

Sources and Adverse Media

URL	Category	Date of Capture
https://privycouncil.independent.gov.uk/privy-council/privy-council-members/	PEP	2021-05-31
https://www.wsj.com/articles/afiniti-names-david-cameron-as-advisory-board-chairman-11559300400?mod=searchresults&page=1&pos=3	PEP, ID/V	2019-09-27
https://www.afiniti.com/team/david-cameron	PEP, ID/V	2019-09-27
http://www.winstonchurchill.org/about/whos-who/honorary-members	PEP	2016-05-23
http://cartertoneducationaltrust.weebly.com/about-us.html	PEP	2016-05-23
http://www.abdabs-yt.co.uk/	PEP	2016-05-23
http://www.youngepilepsy.org.uk/about-us/who-we-are/president-and-vice-presidents/	PEP	2016-05-23
https://www.epilepsysociety.org.uk/president-and-vice-presidents#.V0LIU_krLIU	PEP	2016-05-23
http://www.parliamentaryrecord.com/content/profiles/mp/David-Cameron/Witney/661	PEP, ID/V	2010-07-21
http://www.parliament.uk/biographies/david-cameron/25752	PEP, ID/V	2010-07-21, 2010-06-24
http://www.number10.gov.uk/news/topstorynews/2010/05/her-majestys-government-49840	PEP	2010-05-21
http://news.bbc.co.uk/1/hi/uk_politics/election_2010/8675705.stm	PEP, ID/V	2010-05-13, 2010-05-12

Accessing copyright adverse media

This is applicable to specific data source subscriptions.

Copyright sources which are not accessible via the URL can be requested. Click on the date of capture, and if available, the date will change to a link to download the PDF of the copyrighted material.

Please note that this link is available for up to 15 minutes. After expiry, the request will need to be submitted again.

A question mark is indicative of copyrighted material:

	Category	Date of Capture	
	PEP	2024-01-08 ?	Info

Click on the date to check if the copyright material is available. If so, the date of capture will change to a link for download:

	Category	Date of Capture	
	PEP	2024-01-08	Info

Tax Haven and jurisdiction risk indicators in the profiles

The profiles provide indicators when an individual's primary country of residence or a business's primary country is on the FATF black list, FATF grey list or tax haven lists.

The tax haven list includes the top 10 countries from the Corporate Tax Haven Index (CTHI) and WorldData.info compiled from:

- FATF: Financial Action Task Force's black and grey lists
- EU: EU List of Non-Cooperative Countries and Territories
- IMF: International Monetary Fund blacklist
- Oxfam: Corporate Tax Havens list

The term 'tax haven' lacks a universally accepted definition, as there is no absolute measure determining when a country qualifies as one. Countries may be considered tax havens if they provide favourable tax conditions that incentivize foreign individuals or companies to shelter assets or income. Though subjective, the designation relies on factors like low or no taxes on foreign earnings, strict bank secrecy laws, and limited transparency requirements. As a result, the distinction remains unclear, as characteristics considered when labelling jurisdictions as tax havens continuously evolve.

Profile Categories of PEP, POI, RCA and SIP

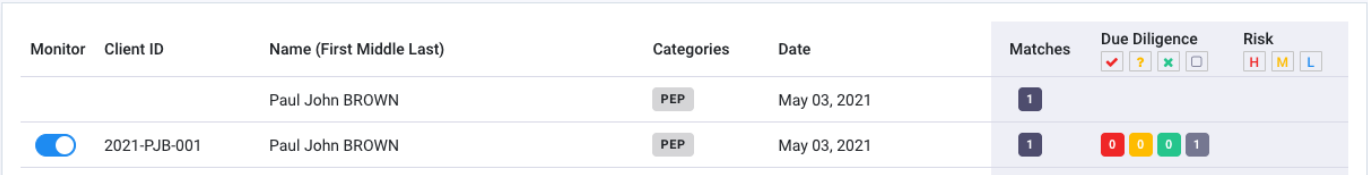
The description of the categories and subcategories available for profiles can be viewed at Profile Categories for Individuals and Profile Categories for Corporate Entities

No options available to apply due diligence decisions

You will need to have associated a **Client ID** with the Individual or Corporate entity during scans. A Client ID is required if you would like to perform due diligence on the matches returned for both single scans and batch scans.

Once the Client ID is included during the scan, the options to include due diligence decisions with assessed risk levels for matched profiles will be available to you.

Example where an Individual is assigned with a Client ID and another without a Client ID:



If you have applied the Client ID during screening and can verify that the Client ID is assigned to the Individual or Corporate entity, but still unable to view the due diligence options, your user account may not be enabled with `Due Diligence Decisions` access rights. In this case, please contact the Compliance Officer for your organisation to activate this permission.

Determining if an individual or corporate is a true match or a false match

If you are having difficulty determining if an entity is a true match or a false match:

- Record the Match Decision as “Not Sure” until additional information is provided that enables a more definitive decision to be made.
- Allocate a Risk, either `Low`, `Medium` or `High`, based on the profile. Check to see what activities the entity may have been involved in, in the past. Also check for any current or expired orders.
- Monitor the entity's transactions for a period to determine if any activity is suspicious.
- Based on the above information, conduct enhanced due diligence if you determine that it is required, i.e. “obtain information about the source of wealth or funds of the customer or beneficial owner and take reasonable steps to verify the source of that wealth”.
- If still unsure, seek assistance from your compliance and legal team.

If you would like information or assistance to conduct enhanced due diligence (EDD), please reach out to your Account Manager or the team at sales@membercheck.com.

Limit of batch file sizes

The file size upload limit for a single batch file is **30 MB**.

For faster and successful uploads of batch files, especially large file sizes, we recommend compressing the CSV or XML file into ZIP for upload. Each ZIP file should only contain a single CSV or XML file.

Possible reasons for failing batch files

There are 3 supported formats for batch file scanning, **CSV**, **XML** and compressed **ZIP** containing a single CSV or XML file. Batch files can be performed via the MemberCheck web application and via REST API.

> **Sample batch file templates to get you started**
>
> Sample templates of the CSV and XML batch files are available in for your download to help you get started.

CSV format batch files

Refer to the following sections for details and examples of the CSV fields and formatting:

- Individual CSV Batch Files
- Corporate CSV Batch Files

When using CSVs, please take note of the following factors which may invalidate your file:

For Individual batch files:

- Check that all mandatory fields are included
- A single individual entity should be contained in a single row/line.

> **Use a text editor to view formatting and invisible characters**
>
> You can use Notepad++ for Windows, or Atom for Mac or Linux or alternative preferred text editors to view if the number of fields are correct for each row as well as invisible characters such as new line characters or carriage return characters.

- Do not add spaces between field separators
- Remove any trailing spaces at the end of the line/row
- Do not include footers or blank lines/rows in the file
- Batch files containing diacritics and original script name should be UTF-8 encoded
- Commas are required to separate all fields even if they are blank. There should be a minimum of 7 fields

> **Record with only FirstName, LastName (no ClientID, MiddleName, DateofBirth or Address)**
>
> OrgID,,FirstName,,LastName,,

- Multiple names in **First Name**, **Middle Name** or **Last Name** should be separated by a blank space

> **First Name and Last Name contains multiple names**
>
> OrgID,ClientID,**Anne Marie**,**Sarah**,**Van Hallen**,DateofBirth,Address

- First Names and Middle Names can be combined in **FirstName**, with **MiddleName** left blank.

Combine First and Middle Name into FirstName

OrgID,ClientID,**Anne Marie Sarah**,,Van Hallen,DateofBirth,Address

- Single or mononymous name should be added to the **LastName**. **FirstName** should include a dash (`-`)

Dash in FirstName, single name in LastName

OrgID,ClientID,**-**,,**SUHARTO**,,

- If the Address contains commas (,) to distinguish them from the commas used to separate the fields, the address should be enclosed in double quotes

Multiple lines or commas in Address

OrgID,ClientID,FirstName,MiddleName,LastName,DateofBirth,**"7 Railway Street, Chatswood, NSW Australia"**

XML format batch files

Refer to the following sections for details of the data type definition to ensure your XML are well-formed and valid:

- Individual XML Batch Files
- Corporate XML Batch Files

RESTful API

If your MemberCheck subscription includes access to API, you can access the RESTful API documentation in **Main Menu > API**. This link is available to all user roles within the organisation.

Procedure for ongoing monitoring service

An overview of the ongoing monitoring procedure from registration, usage, monitoring and renewal process.

Step	Action	Details
Step 1: Sign Up	Register for a 12-month subscription to access the MemberCheck monitoring services	Upon signing up, you will gain access to a pre-defined number of scans which you can use to screen names against our AML watchlists.
Step 2: Use of Scans	Utilise your allocated scans to screen individuals and entities.	Add names to your monitoring lists, which will be monitored on a daily basis to ensure compliance with AML regulations. Note: The number of scans and the frequency of monitoring can be adjusted based on your needs and regulatory requirements. Please contact your account manager for more information.
Step 3: Pre-Renewal Notification	Be aware of upcoming subscription renewal.	You will receive notifications alerting you that your subscription renewal is approaching, usually 3 months and another at 1 month before the renewal date.
Step 4: Review Monitoring List	Check your current monitoring list for accuracy.	Prior to renewal, review the monitoring list to ensure there are no duplicates and that it only includes active customers. Remove any individuals or entities that are no longer relevant to your operations.
Step 5: Renewal and Rescreening	Automated renewal and rescreening of names on the monitoring list.	On the renewal date, all names that are active on the monitoring list will be automatically rescreened. This scan counts towards your scan usage for the new subscription term.
Step 6: Continuous Monitoring	Continue the monitoring process.	The monitoring and rescreening process will repeat each subscription term, ensuring ongoing compliance and vigilance.

No option to monitor Individuals and Corporates even though my account has Ongoing Monitoring activated

If your organisation and user account have ongoing monitoring activated and permissions enabled respectively, you will be able to add Individuals and Corporates to the Monitoring List during PEP & Sanction scans.

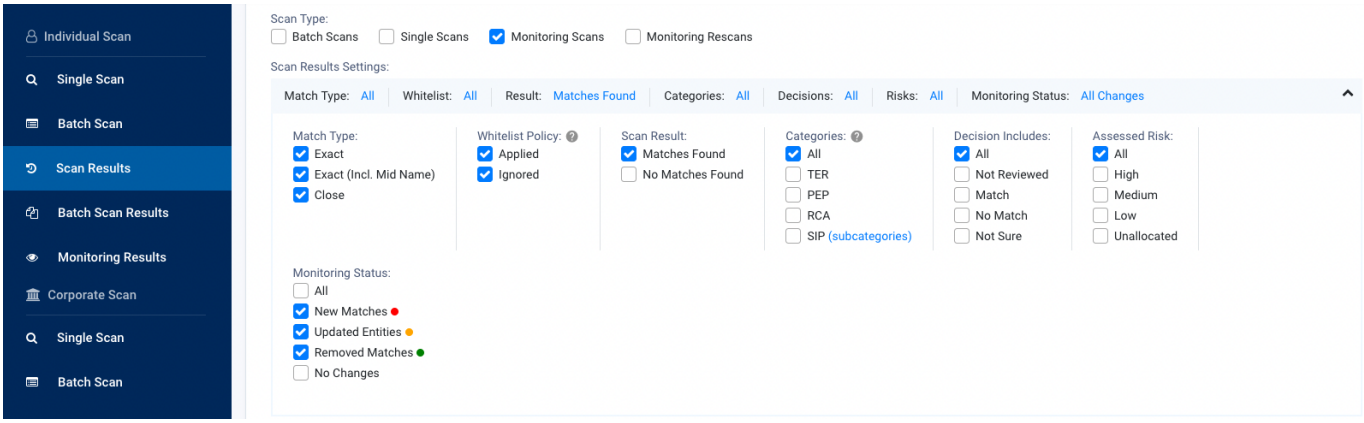
You will need to associate a unique **Client ID** with the Individual or Company during the screening process for Single Scans or Batch Scans. This cannot be added post-screening. Depending on your organisation settings, once the **Client ID** is assigned, the Individual or Company can then be added to the Monitoring List.

Examples of a Single Scan where users are given the option to update the Monitoring List during screening:

Examples where the organisation has preset the Monitoring List option to be enabled or disabled and cannot be changed during screening:

Changes detected from automated ongoing monitoring

Ongoing monitoring checks for Individuals and Corporate entities in the organisation and suborganisation Monitoring List on a regular basis. Any changes in the profile information may trigger a new match, an update to the match, or removal of a match. These are reflected in the monitoring status such as a `New Matches`, `Updated Entities` or `Removed Matches` and are reported in the **Scan Results and Monitoring Results** screens.



Notification of detected changes via email and API Callback

You may select the methods to receive notification of detected changes. Supported methods are email and API callback URL. By default, email notification is disabled, and can be switched on.

Notifications can be sent via **email** to the Compliance Officer or the specified email address based on the preference in **Administration > Organisations > Email Notifications**.

Notifications can also be sent via **API** through the callback URL defined in the **Administration > Organisations > Monitoring Settings**.

> **Callback URL**
>
> The specified callback URL must be available via the GET method and should not require authentication.

You can specify a URL for the MemberCheck system to notify you via API for any detected changes.

The following parameters will be included in the callback URL query:

- **ClientId**: The Client ID (unique identifier) of the monitored entity.

- **entityType**: The type of monitored entity. It could be `Individual` or `Corporate`.
- **type**: Type of detected change. It could be one of `Added`, `Updated`, or `Deleted`.
- **scanId**: The scan identifier is used to retrieve details of the monitoring scan.

For example, if the callback URL is set to `https://yourdomain.com/api/notification`, the returned callback URL may look like:

- `https://yourdomain.com/api/notification?clientId=ID.1150&entityType=Individual&type=Updated&scanId=1022922`
- `https://yourdomain.com/api/notification?clientId=ID.428&entityType=Corporate&type=Added&scanId=229215`
- `https://yourdomain.com/api/notification?clientId=ID.350&entityType=Corporate&type=Deleted&scanId=229210`

Use **scanId** in `GET /api/v2/member-scans/single/{id}` or `GET /api/v2/corp-scans/single/{id}` for Individual and Corporate entities respectively.

Enable Ongoing Monitoring for my account

Ongoing Monitoring is an additional service in MemberCheck. This is activated during enrolment as part of the subscription agreement.

If you already have an account and would like to activate this service, please contact your Account Manager or at sales@membercheck.com.

Monitoring Scan vs Monitoring Rescan

There are two types of monitoring scans:

- **Monitoring Scans** - detects changes in monitored entities against the frequently updated watchlists on a regular basis and displays the differences in the watchlist profile from when the ongoing process schedule is last run.
- **Monitoring Rescans** - runs on the anniversary of the subscription renewal to scan the monitored entities against the entire watchlist database and returns matches found. This process does not detect and highlight changes in the profiles returned.

The difference between a Monitoring Scan and Monitoring Rescan is the former checks the entities in the Monitoring List against smaller and regularly updated profiles that are updated, newly added or removed from watchlists. The latter checks the entities in the Monitoring List against the entire database watchlist.

You may find that Monitoring Rescans have picked up more matches whereas the Ongoing Monitoring Scan did not. This would be due to profiles that exists in the database but are not new or updated recently to trigger the ongoing monitoring detection mechanism.

Therefore, `New Matches`, `Updated Entities` and `Removed Matches` only applies to Monitoring Scans whereas these statuses are displayed with `-` for Monitoring Rescan activities.

Example below displays both Monitoring Scan and Monitoring Rescan activities:

Date	Total Individuals Monitored	Individuals Checked	New Matches	Updated Entities	Removed Matches	Status
Jul 01, 2022	7	7 (Rescanned)	-	-	-	Completed
Jun 14, 2022	7	1	0	1	0	Completed
Jun 11, 2022	7	1	0	1	0	Completed
Jun 10, 2022	7	1	0	1	0	Completed
Jun 08, 2022	7	2	0	1	0	Completed

List of countries supported for ID Verification

The Identity Verification process contains 2 different types of verification:

- FaceMatch - self-verification using biometric facial matching against government-issued documentation.
- ID Check - verify documentation information against reputable data sources.

The customer self-verification biometric facial verification (FaceMatch) supports various types of documents (e.g. passports, driver license, ID Cards etc.) in over **200 countries**.

The list of countries supported for ID Check (document verification) are:

Country	Country Code	Pre-registration Required?
Australia	`AU`	Optional

Austria	AT	No
Brazil	BR	No
Canada	CA	Yes
China	CN	No
Denmark	DK	No
Finland	FI	No
France	FR	No
Germany	DE	No
India	IN	No
Italy	IT	No
Mexico	MX	No
Netherlands	NL	No
New Zealand	NZ	Optional
Norway	NO	No
South Africa	ZA	No
Spain	ES	No
Sweden	SE	No
Switzerland	CH	No
United Kingdom	GB	No
United States	US	No

Country sources that require pre-registration can be applied online via MemberCheck. Country sources where pre-registration is indicated as `Optional` would enable you to have access to additional data sources, but is not mandatory to get started. Please enquire with your Account Manager or sales@membercheck.com for further information.

> **Removal of countries with poor pass rates**
>
> The following countries have been removed from the list for document verification due to poor pass rates:
>
> - Jun 23, 2023: Hong Kong (`HK`)
> - Apr 10, 2024: Singapore (`SG`)

Watchlists coverage for PEP & Sanctions scan

For a comprehensive list of sanctions, financial regulatory and law enforcement source lists covered by the system, these are available within the **Administration > Organisation > List Access** screen. This is available to `Compliance Officer` and `Advanced User` roles.

Should you have any questions about the coverage of specific lists, please reach out to support@membercheck.com.

Custom watchlists

You can extend the available watchlists in the service to include additional custom watchlists of your own for use within your organisation hierarchy. These custom lists may be region-specific lists, industry-specific lists, or any blacklists specific for your organisation.

The file size upload limit for a single custom watchlist file is **30 MB**.

For faster and successful uploads of files, we recommend compressing the CSV file into ZIP for upload. Each ZIP file should only contain a single CSV file.

For details on creating your custom watchlists or accessing the sample templates, refer to Custom Watchlists

Change email recipient for scan notifications

Scan related activities and notifications are emailed to the Compliance Officer(s) by default. To change this setting, the Compliance Officer can specify an alternate email address to receive scan notifications.

The Compliance Officer can change the preference in the **Email Notifications** screen to enter the preferred email address (supports up to 5 unique email addresses) in **Administration > Organisations**.

Change of the parent Organisation's Compliance Officer

Please have the director of the company, with the **director's role and company signature**, email MemberCheck Support (**support@membercheck.com**) to authorise the change of Compliance Officer. The following details should be provided in the email:

1. Authorisation to change Compliance Officer
2. Confirmation to **deactivate** or **change the role** of the outgoing Compliance Officer
3. Full name and email address of the new Compliance Officer.

If the outgoing Compliance Officer user account is to be retained, the role will be changed to `Advanced User`.

Compliance Officer limit on organisations

Effective 24 August 2024, the service has been upgraded to allow up to three Compliance Officers per organisation or suborganisation, up from the previous limit of one. This change offers clients greater flexibility in configuring and utilising their organisational accounts within the service.

Dummy test profiles for trialling the services

There are no available preset dummy data which can be used within the trial environment, however we can offer the following suggestions to preview the various services offered.

PEP and Sanctions

To trial the **PEP & Sanction** screening service, we would recommend testing with a well known political figure or special interest person, such as the president or prime minister of your country to sample the data.

Ongoing Monitoring

To sample the ongoing monitoring detection, we would recommend testing with an entity that is trending in the current news which are highly likely to generate adverse media and sanction list updates. If you are unable to do so, please contact our Support team.

Customer Identity Verification

As of Dec 7, 2022, dummy profiles for use in the trial service for identity verification are no longer available. This change will shift the trial service to be more aligned with the production service.

You can request for a temporary trial account on the **MemberCheck Demo** environment to preview the service via the web application and API.

If you would like to trial any of these services, please contact your MemberCheck Account Manager or support@membercheck.com.

API rate limits

API requests are rate limited based on the type of request e.g. POST, GET, PUT, DELETE.

If you exceed this limit, the system will return a HTTP `429` response code for too many requests.

Request Type	Rate limit per 5 minutes
POST	2,000
GET/PUT/DELETE	720

If you are an enterprise client with high-volume transactions or require support for short-term traffic surges and are unable to throttle your traffic, please contact your Account Manager to discuss your specific business needs.

Further Assistance

If you have any question which are not covered in this help site, please email us at support@membercheck.com.

Supporting Documentation and Resources

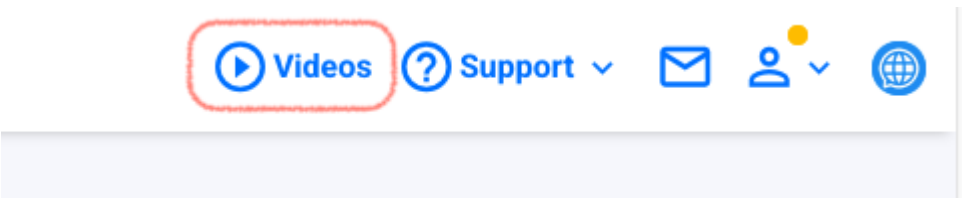
Watchlists and Methodologies

	Document	Description
PDF	**Sanctions Source List**	Source list of Sanctions covered by MemberCheck.
PDF	**Financial Regulatory and Law Enforcement Source List**	Source list of Financial Regulatory and Law Enforcement covered by MemberCheck.
PDF	**Approach to defining PEPs, Business and SOEs**	Approach to the definition of Politically Exposed Persons (PEPs), Businesses and State Owned Enterprises (SOEs).
PDF	**PEP Methodology: Approach to defining PEPs**	Detailed methodology to the definition and tiers for Politically Exposed Persons (PEPs).

Videos

Getting Started

Videos to help you get started are available at https://video-tutorials.membercheck.com. This page is protected and a password can be found via the MemberCheck dashboard application.



ID Verification Overview

This video gives an overview of ID Verification options of running the verification on behalf of a customer, or sending the link to the customer via email or SMS for self-completion.

Release Notes

Release 10.4.2

Released: Jul 27, 2025

Change	Application Section	Description
Enhancement	Scan Results, Batch Scan Results - Individual & Corporate	Increase visibility of PEP & Sanctions risk levels of profiles based on an organisation's current risk settings for categories and subcategories. This extends to linked Individuals and Companies.
Enhancement	Single Scans, Batch Scans - Individual & Corporate	Improve the handling of Arabic name variations in prefixes (e.g., .and compound prefix names (ه,ة ,.suffixes (e.g ,(إ,أ,ا
Enhancement	Single Scans, Batch Scans - Individual & Corporate	Improve recall and match rates for screening by Full Names for Latin-based names.
Enhancement	Data Management	Add new filter, Scan Type, to Supporting Documents, for more granular document management.
Enhancement	Single Scans - Individual	Add new field for Script Name or Full Name for stand alone Risk Assessment Check. Previously, only First, Middle and Last Name were supported.
Change	Reports	Add the timestamp of report generation to all report headers.
Fix	Scan Results - Individual & Corporate	Display results even if an associated service is deactivated. Previously, details of results were not accessible if any of the combined ID Verification, Know Your Business, or Risk Assessment Check services were deactivated.
Fix	Organisation Administration	Resolve issues in creating suborganisations.

Release 10.4.1

Released: Jun 28, 2025

Change	Application Section	Description
Feature	Single Scans, Batch Scans - Individual & Corporate	Introducing **AML Risk Assessment**. Answer key questions about your customer including country, product and services offered, and screening outcomes to view the calculated risk score, risk level and actionable recommendations.
Enhancement	General	Support for Chinese (simplified) language within the web user interface.
Enhancement	Organisation administration	Ability to enable the organisation or suborganisation access to ID Check or FaceMatch only. By default, the IDV service allows access to both.
Enhancement	Scan Result reports - Corporate	Add Country column/field in **Export as CSV** and **Corporate Scan History** reports.
Enhancement	Reports	KYB only - Enhanced company profile activities are now reflected in the **Business and UBO Activity Report** to provide a more complete view of all KYB activities and costs.

Release 10.4

Released: Jun 1, 2025

Change	Application Section	Description
Feature	Single Scans - Individual & Corporate	Introducing **Advanced Media Search**. This can be selected during PEP and Sanctions screening for additional AML/CTF specific news related to the person or entity.
Enhancement	Organisation Administration - Settings	Compliance Officers can define the organisation screening preferences to include or exclude Web Search, Advanced Media Search and FATF Jurisdiction Risk for all users.

Enhancement	Organisation Administration - List Access	Access the latest Financial Regulatory, Law Enforcement and Sanctions source lists for all subscribed data sources within the **List Access** screen. This is available to Compliance Officers and Advanced User roles.
Enhancement	Single Scans - Individual	Add **Client ID** for **IDV only** scans to enable recording of an account number or customer reference number for the individual person.
Change	Scan Results, Batch Scan Results - Individual & Corporate	Change label names for FATF Jurisdiction Risk tags to reflect FATF Black and Grey lists more clearly.
Change	Scan Results - Corporate	Remove references to the monitoring status within reports containing KYB only scan activities due to irrelevance.
Fix	Single Scans - Individual	IDV Global FaceMatch has been fixed to refresh and display relevant form fields.

Release 10.3.4

Released: Apr 13, 2025

Change	Application Section	Description
Enhancement	Scan Results - Individual & Corporate	A Rescan button has been added to the Scan Results screens for all previously scanned individuals and entities for PEP, Sanctions and Adverse Media, allowing you to trigger a new PEP or Sanctions scan using existing details without manual re-entry. Rescans count towards the organisation scan activity.
Enhancement	Organisation Administration	Compliance Officers can select specific events for email notifications and view a list of all event triggers for the organisation. A new option for single scan events has been added and is disabled by default. There is a daily maximum limit of `100` single scan email notifications per organisation. Notifications can be sent to the multiple email addresses (maximum of `5`) or continue to be sent to the Compliance Officers by default. The custom multiple email address supersedes the Organisation Email functionality.

Enhancement	Single Scans, Batch Scans - Individual & Corporate	Enhance the PEP, Sanctions and Adverse Media search algorithm to handle spaces in corporate and individual names, ensuring that searches with variations in spacing return accurate results to improve true positive matches.
Enhancement	Single Scan, Scan Results - Individual	IDV only - view the verification URL sent to the end-user via the web UI and API. This is useful for integrating IDV into your own workflows and for troubleshooting.
Change	Single Scans - Corporate	KYB only - Changes to the supported countries and jurisdictions.
Fix	Batch Scans - Individual & Corporate	Fix for persistent feedback prompt on completion of Batch scans.
Fix	General	Feedback bar misaligned in Arabic language dashboard.
Fix	General	Some organisations with multiple Compliance Officers where some are inactive may have experienced issues with active Compliance Officers receiving scan email notifications.

Release 10.3.3

Released: Feb 16, 2025

Change	Application Section	Description
Feature	Single Scan, Scan Results - Individual & Corporate	Upload and securely store documentation for source of funds (SoF) or source of wealth (SoW) of screened entities. This enables all necessary documents to be kept in a centralised, secure location, enhancing compliance and audit readiness.
Enhancement	Dashboard	Overview of scan usage and remaining credits to provide insight to track progress of the organisation's scan usage. This applies to parent organisation view only.
Enhancement	Single Scan, Scan Results - Individual & Corporate	Retrieve copyright media assets. Where sources and adverse media are copyrighted and the URL is not accessible or cached PDFs are not available, you can request for a copy of the copyrighted material.

Enhancement	Scan Results, Batch Scan Results - Individual & Corporate	Option to download a consolidated report of key details for all matches for a screened entity. This is useful for scans which return multiple profiles, allowing you to record the data more efficiently.
Change	Single Scans, Scan Results - Individual	Added and changed the nationality values to reflect more common usage or spelling. Added: `Curaçaon`; Changed: `Argentinian` for Argentina, `Sint Maarteners` for Sint Maarten, `Jersey people` for Jersey.
Fix	General	Fix download mechanism to enable download of larger volume of entries for Exception Report and Full Report for batch scans.

Release 10.3.2

Released: Jan 19, 2025

Change	Application Section	Description
Enhancement	Organisation Administration	Custom watchlist support is now available for all data source subscriptions.
Enhancement	General	Clients subscribed to multiple data sources can now filter scan results in the web UI by data source type.
Enhancement	General	Notification emails for scan usage are triggered when usage hits predefined thresholds (30%, 50%, 70%, and 100%) to help clients track and understand their usage progress.
Enhancement	General	Additional feedback dialog and button added for ease of our clients to submit feedback and sentiment of the workflow and information presented in the service so we can provide meaningful and impactful enhancements for our customers.
Change	Single Scans - Individual	Matching for multiple nationalities changed from `AND` to `OR` logic to ensure better coverage and no potential matches are missed by returning profiles which match any of the entered nationalities.
Change	Scan Results - Individual & Corporate	FATF grey list updated to reflect changes up to October 2024.

Change	Scan Results - Individual	Changed the nationality value from `Emirian` to `Emirati` in scan results and API responses, reflecting more common usage of the latter term.
Fix	Data Management	Fixed an issue where selecting "All PEP & Sanctions scan data where No Matches were found " also removed KYB results and documents.

Release 10.3.1

Released: Dec 7, 2025

Change	Application Section	Description
Fix	General	Fix missing PEP & Sanction watchlist coverage notes in scan results and reports for GCC service.

Release 10.3

Released: Dec 1, 2024

Change	Application Section	Description
Feature	General	Subscribe to multiple PEP & Sanctions datasets simultaneously. To access multiple datasets, contact your Account Manager for information.
Feature	Single Scans, Batch Scans - Individual	Screen by nationality for PEP, Sanctions and Adverse Media. This allows screening for dual and multiple citizenship (up to 5).
Enhancement	Single Scans, Batch Scans - Individual	Country of residence expanded to support up to 5 countries. Only profiles matching all locations will be returned.
Enhancement	Single Scan, Batch Scan - Individual & Corporate	Granular scope of PEP & Sanctions screening by category (PEP, RCA, SIP, SIE, SOE etc.) during screening. Previously, the scope of screening is set by the Compliance Officer and applied across to the organisation or suborganisation.

Enhancement	Monitoring Result, Scan Results	Detailed profile report enhanced to improve the layout including the last monitored date and monitoring review status.
Enhancement	Batch Scan Results - Individual & Corporate	Simplify the ability to add batch file entries to the Monitoring List.
Fix	General	Change CSV download mechanism to enable download of larger volume of entries such as Monitoring Lists and scan results.

Release 10.2

Released: Oct 27, 2024

Change	Application Section	Description
Feature	Organisation Administration, Monitoring Results - Individual & Corporate	Track profile updates that have been assessed in the ongoing monitoring process. Turn on this option within Organisation Administration to see the features in the Monitoring Results.
Enhancement	Organisation Administration	Enhance List Access to enable selection of former PEP and former sanctioned entities for more granular scope of screening. These are not selected by default.
Enhancement	Organisation Administration	Enhance List Access to enable granular selection of current and former SOEs (State Owned Enterprise) for improved categorisation and refined screening scope. These were previously categorised as `SIE`.
Enhancement	Data Management	New option added to extend deletion of all historical scan data including entities in the Monitoring List, `All Single Scan, Batch Scan, whitelist and Monitoring List data`.
Enhancement	General	The MemberCheck proprietary data, `Emerald` updated to include data for the origin or source country of the watchlist.
Fix	User Administration	Fix issue when creating new user accounts in the French language.

Fix	General	Fix for duplicate display of Compliance Officers in **Organisation > Users** administration screen for some organisations.

Release 10.1.3

Released: Sep 29, 2024

Change	Application Section	Description
Change	System	Change database character set to support all Unicode characters (utf8mb4).
Fix	Scan Results - Individual & Corporate	Fixed "Export to CSV reports" to reflect filtered results in UI.
Fix	Scan Results - Individual & Corporate	Fix to not display duplicate Client ID warning prompt when details of the monitored entity is the same.

Release 10.1.2

Released: Aug 24, 2024

Change	Application Section	Description
Enhancement	Organisation Administration	Enhance **List Access** to enable selection of specific jurisdiction countries for sanction screening.
Enhancement	General	All organisations and suborganisations can now be assigned up to 3 compliance officers.
Enhancement	Dashboard	Monitoring activities and the number of monitored entities are now visible in the Dashboard.
Change	Single Scan - Individual & Corporate	Changed the duplicate Client ID warning system to detect any attempt to add an existing Client ID to the monitoring list, regardless of whether the associated details match or differ.

Change	Single Scan, Scan Results, Batch Scan, Batch Scan Results - Individual & Corporate	Modified the ID Number screening process to return results even when profiles lack identifiers, thereby reducing the risk of overlooking potential matches. Previously, only profiles with a matching identifier were returned.
Change	Single Scan - Corporate	KYB - Remove `South Africa` from the list of supported countries due to a change at the KYB provider.
Fix	Monitoring Scan Reports - Individual & Corporate	Amendment to the monitoring status exported in Excel reports to be displayed in a separate cell rather than combined with Client ID
Fix	Single Scan, Batch Scan - Individual & Corporate	LexisNexis data only - Fix issue with inconsistent country naming conventions, ensuring proper identification of all countries during location-based screening processes. Countries affected are `Åland Islands`, `Bonaire`, `Sint Eustatius and Saba`, `Brunei Darussalam`, `Cabo Verde`, `Cocos (Keeling) Islands`, `Congo`, `Czechia`, `Eswatini`, `Hong Kong`, `Macao`, `Myanmar`, `North Macedonia`, `Palestine`, `Pitcairn`, `Saint Helena, Ascension and Tristan da Cunha`, `Saint Barthélemy`, `Saint Martin`, `South Georgia and South Sandwich Islands`, `Syrian Arab Republic`, `Taiwan`, `Türkiye`, `U.S. Virgin Islands`, `Viet Nam`.

Release 10.1.1

Released: Jul 28, 2024

Change	Application Section	Description
Enhancement	Organisation Administration	Ability to specify and customise sanction screening to major sanction lists: DFAT, EU, HMT, OFAC and UNSC.
Enhancement	Organisation Administration	Support option to upload CSV custom watchlist in compressed ZIP format to optimise on speed of uploads.
Enhancement	Scan Result Reports - Individual & Corporate	Include the monitoring status (Yes or No) of the individual or corporate entity within reports.
Enhancement	Dashboard	Include Monitoring Rescan activity in Dashboard.

Change	Scan Results - Individual & Corporate	FATF grey list updated to reflect changes up to June 2024.
Change	Password Reset	Simplify the password reset process to remove the need for clients to authenticate themselves in order to initiate the reset. This is in-line with OWASP best practices.

Release 10.1

Released: Jun 30, 2024

Change	Application Section	Description
Enhancement	Login	Include service region links for ease of access to the separate regions.
Enhancement	Monitoring	Option to apply the whitelist policy on continuous monitoring and monitoring rescans to ignore profiles marked as `No Match`.
Enhancement	Reports	New **Monitoring Group Summary Report** to provide an overview of monitoring activities for multiple organisations.
Enhancement	Reports	**Monitoring Report** updated to include numbers for Monitoring Rescan activities.
Enhancement	Administration - Users	Define access to utilise or screen for Know Your Business (KYB) and Identity Verification (IDV) per user account. By default, this is enabled for users where the service is activated for the organisation.
Change	Monitoring Results	Simplify the web interface and email communications to remove the interim process for entities checked column. There are no changes to the monitoring process.

Change	Dashboard	Include all elements of KYB and IDV activities that incur costs in the dashboard. Previously, numbers for these services represented the screened names. For KYB, the new numbers include elements for **documents** and **enhanced company profiles**. For IDV, the new numbers include elements for **ID Check** and **FaceMatch**.
Fix	Batch Scan Results - Corporate	Fix missing elements of scan activity (organisation name and person who performed the scan) in the **Corporate Batch Scan Full Report**.
Fix	Scan Results - Individual & Corporate	Fix caching issue where specifically large batch files screened with whitelist policy applied returned matches flagged as `No Match`.

Release 10.0

Released: Jun 2, 2024

Change	Application Section	Description
Feature	General	Support multiple PEP and Sanction datasets. Two additional datasets have been added to the service, `LexisNexis WorldCompliance` and MemberCheck's proprietary dataset, `Emerald`. This rollout enables clients to choose a single dataset of their choice. In our product roadmap, we will enable clients to opt for multiple datasets simultaneously. For more information on the datasets and the impact on your subscription, contact your Account Manager to discuss.
Change	Login	Change in system messages returned for unsuccessful login to include checking of region.
Change	Login	Display the region name of the service to help users identify the correct service for their user accounts.
Fix	Single Scan - Corporate	Know Your Business (KYB) - Change to company search to include all entered words. Previously company suffixes were ignored.

Fix	Scan Results - Individual & Corporate	Fix issue to the monitor toggle to reflect the correct status of the monitored entity.

Release 9.6

Released: May 19, 2024

Change	Application Section	Description
Enhancement	Single Scan - Individual, Administration - Organisation	Allowance of date of birth variations with an adjustable tolerance of [x] years either side of an individual's date of birth or year or birth. Supports a maximum tolerance of 9 years.
Enhancement	Result Summary Report (CSV)	CSV report enhanced to include additional information of profiles with the new columns `Subcategories`, `Nationality` and `Sources & Adverse Media`
Change	Scan Results, Batch Scan Results - Individual	Match rate calculation for Close Match screening by Full Name now returns a more accurate match rate taking into account all words in the name.
Fix	Dashboard	Number for Web Search service corrected to include Corporate web search scans.
Fix	Reports	IDV only - The **Organisation Activity Report** and **Organisation Group Activity Report** updated to include a new category for `Global FaceMatch` scans.

Release 9.5.1

Released: Apr 28, 2024

Change	Application Section	Description
Enhancement	ID Verification	ID Verification FaceMatch option expanded to support over 200 countries.

Enhancement	Reports	More details of IDV and KYB related activities added to the **Group Activity Report**.
Enhancement	Monitoring	The continuous monitoring process has been updated to detect and match on `gender`.
Change	Single Scan, Administration Organisation	Include `Kosovo` in country list to support some exceptional screening needs for this jurisdiction.

Release 9.5

Released: Mar 17, 2024

Change	Application Section	Description
Feature	Dashboard	Provide visibility into the scan usage for the organisation, with an overview of the breakdown of the major services used.
Feature	Organisation Administration	Compliance Officers can now set standardised `High`, `Medium`, `Low` risk level recommendations for all profile categories and subcategories under the new tab **Risk Settings** tab. These pre-configured risk levels are displayed during the due diligence workflows to guide - but not enforce - assessments organisation-wide.

Release 9.4.3

Released: Mar 10, 2024

Change	Application Section	Description
Enhancement	Scan Results - Individual & Corporate	Official Lists within the entity profile now include the **Status** of the sanction lists in the web interface, which can contain both current and former states. The API updated to include the former state (`false`).
Enhancement	Single Scan - Corporate	Our business check service for KYB now supports the jurisdiction of **Malta**.

Change	Scan Results - Individual & Corporate	Include Google web search results in PEP & Sanction result report to provide supplementary adverse media information.
Change	Single Scan, Batch Scan, Scan Results - Individual & Corporate	UI label change from **Match Type** to **Name Match Type** to clarify the scope of close match screening to the name.
Fix	Administration - Organisation	Fixed time zone mapping on selection of Country in the drop-down list for Organisation profile details.
Fix	Batch file validation	Fixed an error with incorrect line terminators (must be CRLF (ASCII `\r\n`) instead of LF (ASCII `\n`)), preventing any lines from being recognised during the batch file import process.

Release 9.4.2

Released: Feb 17, 2024

Change	Application Section	Description
Enhancement	Batch Scan - Individual & Corporate	Duplicate entries and Client IDs in batch files are detected and displayed in the batch file preview before scanning. If the batch validation setting is turned off, duplicate entries are ignored and excluded from scanning.
Enhancement	Organisation administration	Compliance Officers are able to delete user accounts and organisation accounts which are unused or have no historical scan activities.
Change	General	The fuzzy name matching process is now separated from Elasticsearch to provide greater control and improve performance of `Close` match scans for batches and ongoing monitoring.
Change	Single Scan Results, Batch Scan Results - Individual & Corporate	`Tax haven` and `Sanctioned` jurisdiction indicators have been expanded to cover other aspects of the profile. These now cover the person's primary location and nationality, and for corporates, the primary and registered locations.

Change	Single Scan Results, Batch Scan Results - Individual & Corporate, Administration Organisation	Update country list names to reflect latest standard ISO 3166-2. Note: The common names North Korea (`KP`) and South Korea (`KR`) have been retained. • Removed: Abkhazia, South Ossetia, Tibet, Turkish Republic of Northern Cyprus, Kosovo, Netherlands Antilles, Serbia and Montenegro, Macedonia. • Added: Åland Islands (`AX`), Bonaire, Sint Eustatius and Saba (`BQ`), French Southern Territories (`TF`), North Macedonia (`MK`), United States Minor Outlying Islands (`UM`)
Fix	Single Scan Results, Batch Scan Results - Individual & Corporate	Improved handling of malformed URLs in Adverse Media source links.
Fix	Single Scan - Individual & Corporate	Fix for **Country** drop down lists which were not loading in some instances.

Release 9.4.1

Released: Dec 23, 2023

Change	Application Section	Description
Change	Single Scan Results, Batch Scan Results - Individual & Corporate	Scope of tax haven countries limited to top 10 most notorious based on the Corporate Tax Haven Index (CTHI).
Change	Single Scan Results, Batch Scan Results - Individual	Documentation for tax haven indicator for individuals have been corrected to refer to the "primary country of residence" instead of "country of nationality".
Fix	Monitoring Results - Corporate	Preview and download of reports for Corporate monitoring results have been fixed to enable reports to be generated and downloaded.

Release 9.4

Released: Dec 10, 2023

Change	Application Section	Description
Feature	Single Scan - Corporate	Business check service for Know Your Business (KYB) and Ultimate Beneficial Owner (UBO) verifications. Search for a company and select from available registry documents for KYB verification. Optionally, request for the company enhanced profile containing detailed company information, associated directors, shareholders and ultimate beneficial owners. These may incur additional charges, and you are only charged for the specific information requested.
Feature	Reports	New report for KYB and UBO activities with a list of requested documents or UBO requests, and the associated costs and status of document delivery.
Feature	Single Scan Results, Batch Scan Results - Individual & Corporate	Display new indicators where an individual's country of nationality or a business's primary location has operations in countries considered as **tax haven** or **sanctioned**, based on WorldData.info data compiled from various sources including FATF, IMF, EU and Oxfam.
Enhancement	Menu bar	New **Video** link in the top right menu. Links to a library of "how-to" videos with more in-depth details of various features of the application.
Feature - Experimental	Single Scan Results, Batch Scan Results - Individual & Corporate	Integration with OpenAI ChatGPT for analysis of individual and corporate profiles. This is currently available to a limited number of clients and will be made available to a wider scope of users in due time.
Change	General	Improve cache management in the database.

Release 9.3.5

Released: Oct 1, 2023

Change	Application Section	Description

Feature	Single Scan, Batch Scan - Corporate	Supports wildcard (`*`) search for partial names e.g. `Bank of Ame*` can return results of `Bank of America`, `Bank of America Corporation`, `Bank of America Investment Services` etc.
Feature	Single Scan, Batch Scan - Corporate, Organisation administration	Expand list of default company stopwords and the ability for organisations to manage their own stopwords. Compliance Officers can manage this in **Organisation Settings**.
Enhancement	Organisation administration	Expand custom watchlist to enable the Compliance Officer of a suborganisation to upload and manage their own Custom Watchlists. This was previously limited to the root parent organisation to manage for all suborganisations.
Enhancement	Scan Results - Individual	Remove case-sensitivity when searching for Latin-based text in **Full Name** search field in **Scan Results - Individual Search**.
Enhancement	General	Support for Arabic language within the web user interface.
Fix	Single Scan, Batch Scan - Corporate	Web interface updated to reflect the minimum company name length supported in API of `1` character.
Fix	Organisation administration	*Applies to Oman service only.* Fix for custom watchlist administration where the list was not able to be removed for the organisation.

Release 9.3.4

Released: August 6, 2023

Change	Application Section	Description
Feature	Single Scan - Corporate, Batch Scan - Corporate	Inclusion of text-to-number translations for company profiles to expand the variation of company name screening when using `Close` match. For example, a company name on the watchlist "Company 55 Limited" can be found using `Close` match type with "Company Fifty Five Limited" or "Company Fifty-Five Limited".
Enhancement	Data Management	Added new option for more granular data deletion of single scan results for Individuals and Corporates. This option is available to Compliance Officers only.

Change	User Management	Added validation during user administration management to prevent orphaned user accounts when not linked to any organisation. All users must be assigned to at least 1 organisation. This feature is available to Compliance Officers only.
Fix	Data Management	Running data management process to remove large number of scan results and whitelist data sometimes returned timeout errors. Fix to improve efficiency of process.

Release 9.3.3

Released: June 25, 2023

Change	Application Section	Description
Feature	Single Scan, Batch Scan - Individual & Corporate	Introducing Jurisdiction Risk ratings. Opt-in to include this information during single scans or batch scans to view the technical compliance and effectiveness ratings for relevant countries based on FATF recommendations.
Enhancement	Single Scan - Individual, Batch Scan - Individual	New field **ID Number** to enable screening with an identifier (e.g. Passport Number, National ID, VAT/Tax Number).
Enhancement	Single Scan - Corporate, Batch Scan - Corporate	Replaced the Address field for corporate scans with Country of Operation (Address) drop down list to enable screening for country of operation or registration using a standard input. For batch files and API requests, the full address of the corporate entity is still accepted but only the country name or country code (ISO 3166-1 2-letter code) will be used for screening.
Enhancement	Group Activity Report	Added a search field to quickly find an organisation to generate a report. This is useful for multi-level organisations or for resellers managing multiple organisations where the list can be long.
Fix	Scan Results - Corporate, Batch Scan Results - Corporate	Filtering by `SIE` subcategories sometimes returned no match found for existing profiles. This now correctly displays the filtered profiles.

Fix	Scan Results, Batch Scan Results	Improve handling of malformatted URLs in Sources and Adverse Media for PEP and Sanctioned profiles for individuals and companies. Malformatted URLs may not be able to be fixed for existing links, however, these can be reviewed on a case by case basis.

Release 9.3.2

Released: May 28, 2023

Change	Application Section	Description
Enhancement	Single Scan - Corporate, Batch Scan - Corporate	Improved corporate screening by incorporating fuzzy matching for better searchability of name spelling variations.
Enhancement	Batch Scan - Individual & Corporate	Batch scan workflow includes a preview of the formatting of the batch file before scanning. This applies to the web UI only.
Enhancement	Scan Results Reports	New screenings for PEP and sanctions will now show watchlist categories in reports for better auditing.
Enhancement	ID Verification	Display completion timestamps for Quick ID and FaceMatch verifications in the web UI, reports, and API for reference.
Enhancement	Reports	Reports now feature a modern design consistent with the web interface, incorporating additional PEP, Sanction, and Adverse Media information from version **9.3.1**.
Change	Compromised Information report	Separated the Compromised Information report from the PEP, Sanction, and Adverse Media scan result report for improved clarity.

Release 9.3.1

Released: May 7, 2023

Change	Application Section	Description

Enhancement	Watchlist data	PEP, sanction and adverse media profiles expanded with • additional details for PEP roles, publication information of adverse media sources, official lists and location types • support for multiple images of the individual or corporate entity, where available.
Enhancement	Single Scan - Corporate, Batch Scan - Corporate	Include close match rate threshold to enable adjustment of the closeness of screening of names, ranging from `100`% (almost exact names) to `1`% (somewhat similar sounding names).
Enhancement	Single Scan - Corporate, Batch Scan - Corporate	Improve search by business registration/reference number to return more targetted results and reduce false matches.
Enhancement	Single Scan - Individual, Batch Scan - Individual	Adjustment to the fuzzy matching algorithm to improve relevance and reduce false matches for name screening.
Change	Monitoring List	A limit of `10,000` rows applied to the web interface text area for bulk removal of Monitoring List entities. This does not apply to the API requests, which is dependent on existing API rate limits in the service.
Change	Reports	Reports generated in the Demo environments have been restricted to PDF format and highlights the use for trial purposes only.
Fix	Organisation Activity Report	Fix scan count for PEP & Sanctions service. IDV scan counts were previously combined within Individual Scans section of the report.

Release 9.3

Released: February 26, 2023

Change	Application Section	Description

Enhancement	Watchlist data	The database for PEP, sanctions and adverse media profiles have been expanded to contain more detailed information. The API has been updated to include the additional information. Please refer to the **API Change Log** in this Help Guide, or the relevant API documentation for details. The web user interface will be further enhanced in the coming months to reflect the new information and structure.
Enhancement	Single Scan, Batch Scan, Scan Results, Batch Scan Results, Organisation List Access	Inclusion of a new category for "Profile of Interest" (`POI`). This category will be enabled by default in the organisation **List Access** tab.
Enhancement	Single Scan, Batch Scan, Scan Results, Batch Scan Results, Organisation List Access	Inclusion of a new subcategory, "Reputational Risk", under Special Interest Person (`SIP`) and Special Interest Entity (`SIE`). This subcategory will be enabled if you have selected `SIP` or `SIE` in the organisation **List Access** tab.
Enhancement	Scan Results - Individual, Batch Scan Results - Individual	Profiles where multiple dates for the same event e.g. date of birth, deceased dates etc. are displayed in the **Important Dates** section.
Enhancement	Scan Results, Batch Scan Results	Sources and adverse media categories have changed and includes `Profile of Interest` and `Reputational Risk Exposure`. `ID/V` is now `Identity`.
Enhancement	Scan Results, Batch Scan Results	A new section, **Identifiers**, lists a variety of ID numbers and unique IDs recorded for the individual or corporate entity. These IDs were previously within the general notes in **Further Information**. These identifiers include business registration numbers, OFAC unique IDs, VAT/Tax numbers, BIC numbers, IMO numbers etc.
Enhancement	Single Scan - Corporate	Change in the Corporate scanning to take advantage of the new identifiers. Entering a **Registration Number** during corporate screening will exclude all profiles which do not have an identifier, or if the identifier does not match from being returned as a potential match. This will produce more targetted results and reduce false matches.
Enhancement	General	Service and product updates will be visible in the new **Notifications** section in the top menu. This central area enables web users to view and manage messages relating to the service.

Change	Scan Results, Batch Scan Results	The **Enter Date** for a profile has been replaced by **Last Reviewed** which provides the date the profile record was last reviewed or updated.
Fix	Monitoring List	Bulk removal of monitoring items from monitoring list fixed. This was previously displaying an error when more than 25 items were in the request.

Release 9.2.1

Released: February 12, 2023

Change	Application Section	Description
Feature	Compromised Data check	Enter an individual's email address during PEP, sanction and adverse media screening to check if the member's data has been compromised in known data breaches.
Enhancement	API	IDV - API expanded to enable document verification (ID Check), or biometric facial matching (FaceMatch), or both. Previously FaceMatch could only be performed together with an ID Check.
Enhancement	API	IDV - API expanded to enable email of the verification request to individuals. Previously, individuals could only receive SMS of the verification link.
Change	IDV	If the process to run the FaceMatch verification on behalf of the individual on the web application was interrupted, the FaceMatch status was previously flagged as `Pending`. This is now changed to `Incomplete` to more accurately reflect the status.
Change	Scan Result reports, API	For scans with IDV only screening, null references to the irrelevant PEP and Sanction labels have been removed to clean up the reports and response body in the API.
Fix	Monitoring Results	Viewing of historical profiles which have been removed from the watchlist database in some circumstances were returning an error. Correct display of the profile details of the removed entities.

Change	Application Section	Description
Fix	Monitoring Results	Profiles which were marked as 'removed matches' only in ongoing monitoring were not displaying the details of the profile. These were previously displaying "individual not found" in profile details.

Release 9.2

Released: December 10, 2022

Change	Application Section	Description
Enhancement	Single Scan	IDV - Expanded to enable document verification (ID Check), or biometric facial matching (FaceMatch), or both. Previously FaceMatch could only be performed together with an ID Check**. *See note below.*
Enhancement	Single Scan	IDV - Added capability to email customer identity verification to individuals, as well as running the document verification on the individual's behalf. Previously, individuals could only receive SMS of the verification link**. *See note below.*
Enhancement	Scan Results	IDV - Images of biometric facial matching and documents included in the scan results for review and verification.
Enhancement	Single Scan, Batch Scan, Organisation Administration	New option to enable inclusion of specific jurisdictions or countries for PEP screening. Previously, there was only the option to exclude specific jurisdictions for PEPs. This is configurable within the organisation administration settings.
Enhancement	Administration	Automated deactivation of Organisation and associated user accounts upon expiry or termination of subscription. The Compliance Officer of an organisation will receive an email to notify of deactivation.
Enhancement	API	Inclusion of a liveness check for the API service which will enable clients to easily check the liveness and status of the API service. Please refer to the API Reference documentation for details at https://api.membercheck.com/docs/index.html?#membercheck-api-health-check.

Change	Application Section	Description
Change	Single Scan - Individuals	Changes to the screening workflow to improve and simplify the selection of services before commencing screening, in anticipation of new services to be introduced in the near future.
Change	Single Scan, Batch Scan	Close Match - Addition of phonetic matching algorithms to improve the relevance and fuzzy matching of names for Individual entities.
Change	General	Various improvements and optimisation within the application to improve responsiveness.

** Note: This is currently only available via the Web UI. API functionality will be made available soon.

Release 9.1.2

Released: October 1, 2022

Change	Application Section	Description
Enhancement	General	Support for French language within the web user interface.
Enhancement	Organisation Administration	Additional options for frequency of Ongoing Monitoring, `Daily`, `Weekly`, `Fortnightly`, `Monthly`, `Quarterly` and `Semi Annually` (see Note below).
Change	User Administration	Increase number of organisations able to be assigned to a user account.
Change	General	Various label changes to the UI to improve comprehension of features.
Fix	Monitoring Results	Monitoring Rescan activities can now be viewed within `Monitoring with updates` if there are updates resulting from the annual rescan.
Fix	Batch Scan	Improve error handling of CSV batch files that contained headers only without any individual or corporate screening contents.

Change	Application Section	Description
Fix	Scan Results	Fix to display flags for some nationalities which were not appearing in the profile of the matched results.

Changing the ongoing monitoring frequency

Note: Contact your Account Manager or support@membercheck.com if you would like more information on changing the frequency of the ongoing monitoring service for your organisation account.

Release 9.1.1

Released: July 23, 2022

Change	Application Section	Description
Enhancement	Scan Results	Expand downloadable `Results Summary Report` to include unique client reference, **Client ID**.
Change	Scan Results	Updated message prompt when downloading `Results Summary Report` to clarify the use of the email address in lower case as the password for secured ZIP file.
Change	Single Scan, Batch Scan	Scanning by **First Name** and **Last Name** by `Close Match` previously returned results where First and Last Names were interchanged to return potential matches where the order of the names were uncertain or may vary. This has been changed to only display results in the specific order as entered. Where the order of names for First and Last Name is uncertain, enter the name into **Full Name** field instead for an expanded search for greater potential matches.
Change	Single Scan, Scan Results	Close match scanning of names which exactly match the names entered for Individuals are now displayed at the top of the list of results for improved visibility of returned results.
Change	New User Account	New User accounts created on login will be prompted to specify a security question and answer, which are used for verification during password reset. This is currently optional but is highly recommended that users complete this process.

Release 9.1

Released: May 15, 2022

Change	Application Section	Description
Enhancement	Due Diligence Decisions	All due diligence decisions including Decision, Risk level and Comments are displayed in all reports containing due diligence decisions. Previously all Comments and only the latest Decision and Risk levels were retained and displayed
Enhancement	Scan Results	Ability to directly report issues or questions relating to profile details of Individuals or Corporates to MemberCheck Support team to improve quality of data in the watchlists. Predefined reports include profile data incompleteness or inaccuracies, request for more detailed information of a profile, or reasons for profile being listed in the watchlists
Enhancement	General	Resellers of MemberCheck are able to advise if they would like to display their logo in the main menu of the application. Only horizontal/landscape logo designs are supported at the moment
Fix	Individual - Single Scan, Batch Scan	Fix for `Close` match screening of mononymous names. This was previously unable to return results. `Exact` matching for mononymous names is unaffected
Fix	Individual - Single Scan, Batch Scan	Changes to **Full Name** search to reduce false matches and improve relevance. All names entered in **Full Name** will search for occurrences of all the names entered. Note: Screening by **Full Name** with `Exact` or `Exact (incl. Mid Name)` match will return the same results as full name does not differentiate the Middle Name
Fix	Monitoring List	Enable CSV download of large volumes of entries within the **Monitoring List**. The **Download CSV** button was previously erroring for downloads of over 1 million entries

Release 9.0

Released: December 11, 2021

Change	Description
Enhancement	Support partial search on **First Name** of an individual. Where only initials are available, use an asterisk (`*`) after the initial e.g. `K*` . For partial or incomplete first names, use an asterisk after the name prefix e.g. `Ken*`
Enhancement	Expand **Results Summary Report** to include the latest due diligence decisions. This report in CSV format is available for both single and batch scans for Individuals and Corporates
Enhancement	IDV - Detect and warn of duplicate requests for ID verification of the same name within 24 hours
Enhancement	Organisation Administration - Support for `Reseller` organisations. Compliance Officer of a reseller organisation can manage and track the Subscription Start Dates and Termination Dates of their clients (suborgs)
Enhancement	System notifications - Important account information such as subscription renewal reminders are automatically sent out to the Compliance Officer of the root parent organisation on behalf of the Account Manager
Enhancement	Various enhancements and optimisation in the backend databases to improve scan response time and retrieval of scan results
Change	The default HTTP 404 error page has been given a facelift with helpful links to help the user navigate back to the site and help guide
Fix	Organisation User management - Remove irrelevant message displayed within User administration list where no users are assigned

Release 8.4

Released: September 25, 2021

Change	Description
Feature	Extend PEP & Sanction screening to support **Custom Watchlists**. Create one or more custom watchlists by uploading CSV files of Individual and Corporate profiles via **List Access**.
Enhancement	**Activity Reports** include separate Web Search (adverse media) scan activities to provide more information for reporting.

Change	Description
Enhancement	New status `Pending` for user accounts which have not yet completed the account set up to differentiate from the default status of `Active` users.
Enhancement	Within user's **Profile** screen, change button label for API Access Key from `Reset` to `Generate` for clarity of function. Inclusion of a `Copy` button to enable ease of copying of the API Access Key.
Enhancement	Unsaved settings detected in Administration and Profile screens will prompt to confirm to discard changes to minimise loss of configuration changes.
Change	Email notifications of scan activity and system reminders will be sent from `donotreply@membercheck.com` instead of `admin@membercheck.com`.
Fix	**Ongoing monitoring** change highlights extended to include changes detected in the addition or removal of cached URLs in **Date of Capture** of the adverse media.
Fix	Fixed possible minor variation where a large number of scan results are returned for `Close match` type scans performed with `Full Name` search.

Release 8.3.1

Released: September 4, 2021

Change	Description
Enhancement	Ability to download a report immediately for Single Scans which do not return matches. Additional message displayed in results panel where no results are found for combined screening of PEP & Sanction and web search.
Fix	Various fixes and changes to the backend for Log reports.

Release 8.3

Released: August 29, 2021

Change	Description
Enhancement	Support secure exporting of additional report containing summary of profiles returned for Single and Batch Scans. The CSV report is compressed and downloadable in a password protected ZIP file. Password is the email address of the user who generated the report. Report is available for download as **Results Summary Report**.
Enhancement	Reports section has been updated to simplify the selection of reports and includes descriptions to improve usability.
Enhancement	Improve the relevance of web search results returned for Google searches.
Change	Email address validation expanded to support additional top level domains.
Change	Email notifications of scans results sent from the Modern UI has changed in the display order. Links to the Modern UI is displayed before Classic UI.
Fix	`Full Report` and `Exception Report` of batch results have been cleaned up to display the number of profiles in the major categories of PEP, RCA, SIP, SIE.
Fix	Various fixes to the validation of XML batch files.

Release 8.2

Released: August 15, 2021

Change	Description
Feature	Option to extend PEP and Sanction screening to include a web search on Google for adverse media for **Single Scans**. Option is available within **Scan Settings** panel. API - API clients can enable this setting with the new optional property `includeWebSearch` .
Enhancement	IDV - New verification source for `Singapore` .
Enhancement	Added option to quickly generate a suggested new **Client ID** (previously Member Number and Entity Number) during Single Scans. This is available within the UI only.

Change	Description
Enhancement	Inclusion of a document containing source lists used for PEP & Sanction screening within the organisation **List Access**. The same document is also available in this help guide ***Resources*** section.
Change	Relabel fields **Member Number** and **Entity Number** in Individual and Corporate Scans to **Client ID** to reflect the purpose of the field more accurately. API - a new separate property `clientId` is available and recommended for use over the existing properties `memberNumber` and `entityNumber` which will be deprecated in the future. These however will continue to be available until further notice.
Change	Protect users from over clicking buttons and performing duplicate tasks by displaying a progress icon within the pressed button.
Change	Protect users from processing duplicate batch scans. If the same batch file name is identified as being scanned within the last 12 months, a prompt is displayed for the user to proceed or cancel. API - API clients are able to set if duplicate batch file names are allowed to be processed with the new optional property `allowDuplicateFileName` .
Change	We have received positive and encouraging feedback on the application and are happy to remove the "PREVIEW" status from the modern interface.
Fix	Error in handling new user account setup after expiry of the registration link.

Release 8.1.1

Released: July 18, 2021

Change	Description
Enhancement	Support monitoring notifications of detected changes via API callback URL defined by the Compliance Officer.
Enhancement	Distinguish monitoring rescan activities in **Monitoring Results**.

Change	Description
Change	Change "monitoring with updates" filter to only display and notify activities with new, updated or removed results. Changes in `Monitoring with updates` filter in **Monitoring Results** and trigger for ongoing monitoring notifications.
Change	Update of icons to reflect the updated modern user interface including browser favicons, due diligence icons in Reports, and light and dark themes.
Fix	Error in allowing multiple COs to be assigned to suborganisations causing multiple suborganisations to be displayed in Organisation list. Fix to enforce single CO per suborganisation.
Fix	Error in sending Monitoring Rescan Emails if no Corporate entity exists in Monitoring List.

Release 8.1

Released: June 27, 2021

Change	Description
Feature	Identity Verification includes biometric face matching, an optional feature in **Single Scan**.
Feature	Actively monitored entities will be rescanned on first day of renewed subscription.
Feature	Ability to bulk remove multiple entities in **Monitoring List**.
Enhancement	Display watchlist categories for new scans for scope of PEP & Sanction scan by expanding the scan settings in **Single Scan**.
Enhancement	Organisation subscription and renewal dates displayed in **Organisation** details.
Enhancement	API - First release of the new version of API v2 to integrate with modern UI. **API Reference** and **Developer Centre** can be accessed via the **Support** menu item.

Release 8.0.1

Released: June 6, 2021

Change	Description
Feature	Screen for both PEP & Sanction and ID Verification with a single click within **Single Scan**.
Feature	Option to select specific nation of `Australia` and `New Zealand` for targetted sanction scans within **List Access**.
Feature	ID Verification now includes `China` as an additional source. Supported countries: Australia, New Zealand, Austria, Brazil, Canada, China, Denmark, Finland, France, Germany, India, Italy, Mexico, Netherlands, Norway, South Africa, Sweden, Switzerland, United Kingdom and United States.
Enhancement	Option to preview Reports before downloading as PDF, Word or Excel format.
Change	Hide columns in **Scan Results** where no data is available for the page view.
Fix	User login times to reflect organisation timezone.
Fix	Enable creation of suborganisations for client accounts where monitoring is not enabled.
Fix	Fix display of original script text in PDF reports. Previously displaying "box" symbols.

Release 8.0

Released: May 9, 2021

Change	Description
Feature	Improved and modernised user interface.
Feature	Supports screening by **Full Name** for PEP & Sanction.
Enhancement	IDV - Countries for ID Verification now extends beyond Australia and New Zealand to include Austria, Brazil, Canada, Denmark, Finland, France, Germany, India, Italy, Mexico, Netherlands, Norway, South Africa, Sweden, Switzerland, United Kingdom and United States.

Release Notes for MemberCheck Classic

To view the list of changes in the MemberCheck Classic interface, you can refer to the **Release Notes** available at https://help2.membercheck.com.

API Change Log

Deprecated

Fields deprecated or scheduled for deprecation, and will be decommissioned (removed).

Name	API Schema	Deprecation Date	Decommission Date
`enterDate`	Entity EntityCorp	26 Feb 2023	TBA
`title`	Entity	26 Feb 2023	TBA
`NameDetail.title`	Entity	26 Feb 2023	TBA
`xmlFurtherInformation`	Entity EntityCorp	26 Feb 2023	TBA
`image`	Entity	30 Jun 2024	TBA
`originalScriptNames`	Entity EntityCorp	30 Jun 2024	TBA
`dates_Urls`	Source	30 Jun 2024	TBA
`membersChecked`	MonitoringScanHistoryLog MonitoringScanResults	30 Jun 2024	TBA
`companiesChecked`	CorpMonitoringScanHistoryLog CorpMonitoringScanResults	30 Jun 2024	TBA

Release 10.4.2

Released: Jul 27, 2025

Name	API Schema	Description

`scriptNameFullName`	`aml-risk/member-scans`	New input parameter to enable entry of Script Name or Latin-based Full Name for the standalone Risk Assessment Check.

`member-scans/single/results/{id}/linked-individuals/risk-levels`
 	
`member-scans/single/results/{id}/linked-companies/risk-levels`
 	
`corp-scans/single/results/{id}/linked-individuals/risk-levels`
 	
`corp-scans/single/results/{id}/linked-companies/risk-levels`
		New methods to retrieve the recommended risk level of an associated individual or corporate entity based on the organisation risk settings of categories and subcategories.

`suggestedRisk`	`POST member-scans/single`
	
	`POST member-scans/single/{id}/rescan`
	
	`GET member-scans/single/{id}`
	
	`POST corp-scans/single`
	
	`POST corp-scans/single/{id}/rescan`
	
	`GET corp-scans/single/{id}`
		New parameter returning the recommended risk level of the matched profile based on the organisation risk settings of categories and subcategories.

`exactMidName`	`POST corp-scans/single`
	
	`GET corp-scans/single`
	
	`GET corp-scans/single/report`
		Removed supported value for `matchType` for screening and filtering of Corporate entities as this relates to Individual entities.

Release 10.4.1

Released: Jun 28, 2025

Name	API Schema	Description

	`aml-risk/member-scans`
	`aml-risk/member-scans/{scanId}`
	`aml-risk/member-scans/{scanId}/report`
	`aml-risk/corp-scans`
	`aml-risk/corp-scans/{scanId}`
	`aml-risk/corp-scans/{scanId}/report`
		New methods to perform and retrieve reports of the AML risk check for individuals and corporate entities.

	`reports/aml-risk-activity`	New method to download report of AML Risk check activities.

	`member-scans/single`
	`member-scans/single/{id}/rescan`
	`member-scans/batch`
	`member-scans/single/{id}`
	`corp-scans/single`
	`corp-scans/single/{id}/rescan`
	`corp-scans/batch`
	`corp-scans/single/{id}`
		New parameter `includeRiskAssessment` for Risk Assessment Check.

`member-scans/single`
`member-scans/single/report`
`corp-scans/single`
`corp-scans/single/report`
	New parameter `amlRiskLevel` to indicate AML Risk Level result. New value `RiskAssessment` for parameter `scanService`.

`member-scans/batch/{id}`
`member-scans/monitoring/{id}`
`corp-scans/batch/{id}`
`corp-scans/monitoring/{id}`
	New parameter `amlRiskLevel` to indicate AML Risk Level result.

`data-management/scans/count` `data-management/scans`	New value for input parameter `scanType` to reflect the Risk Assessment Check.

`data-management/member-scans`
`data-management/member-documents`
`data-management/corp-scans`
`data-management/corp-documents`
	New value for input parameter `scanService` to reflect the Risk Assessment Check

Release 10.4

Released: Jun 1, 2025

Name	API Schema	Description
`includeAdvancedMedia`	ScanInputParam CorpScanInputParam	New input parameter to include advanced media search of news articles for the entity during screening.

`advancedMediaResults`	ScanResult CorpScanResult	New parameter that returns the advanced media results.
`advancedMediaSearch`	OrgDetails.memberScanSettings OrgDetails.corporateScanSettings	New parameter that returns the advanced media search default setting (Yes/No) for the scan.
`advancedMediaSearch`	ScanHistoryDetail.scanResult CorpScanHistoryDetail.scanResult	New parameter that returns the advanced media results.

`webSearch`
 	
`advancedMediaSearch`
 	
`fatfJurisdictionRisk`
	OrgDetails.memberScanSettings
	
	OrgDetails.corporateScanSettings
		New parameters that return the default setting (Yes/No) for the scan for web search (Google), advanced media search and FATF jurisdiction risk search.

`includeAdvancedMedia`	`GET /api/v2/member-scans/single`
	
	`GET /api/v2/member-scans/single/report`
	
	`GET /api/v2/corp-scans/single`
	
	`GET /api/v2/corp-scans/single/report`
		New parameter to filter results where advanced media search was included during screening.

`member-scans/advanced-media/bookmark`
 	
`corp-scans/advanced-media/bookmark`
		New method to add or remove bookmarks for advanced media articles within the MemberCheck UI.

`clientId`	IDVInputParam	New parameter that enables you to record an Account or Customer Reference Number for the ID Verification scan to help search and identify the screened individual.

Release 10.3.4

Released: Apr 13, 2025

Name	API Schema	Description
`id-verification/single2`		New method to initiate a new ID Verification request that returns a Verification URL to the verification process.

`member-scans/single/{id}/rescan`
 	
`corp-scans/single/{id}/rescan`
		New methods to run a new scan using previously entered details of the entity and scan policies, with the exception of the watchlist, which will be determined by the organisation's current list access scope.
		
		Rescan requests count toward the organisation's scan activity and usage.

Release 10.3.3

Released: Feb 16, 2025

Name	API Schema	Description

`id`
 	
`isCopyrighted`
	scanResult.matchedEntities.resultEntity.sourceDetails	New response parameter for source and adverse media to help identify and indicate if a source media is copyrighted. This `id` is used in the new methods to request for the asset URL of the copyrighted media.
		
		This is available for Acuris data source only.

`member-scans/single/results/{id}/sources/{sourceId}/asset-url`
 	
`corp-scans/single/results/{id}/sources/{sourceId}/asset-url`
	New methods. Where a source or adverse media is copyrighted and the cached PDF is not available, you can call this to get the asset file URL of a specific source of the matched member, company, linked individual or linked company to download as PDF. It is recommended to only use this request if the URL is broken or the cached PDF is not available.
	
	This is available for Acuris data source only.

`lookup-values/document-types`	New method to retrieve the complete list of document types for the Supporting Document feature.

`member-scans/single/{id}/documents`
 	
`member-scans/single/{id}/documents/{documentId}/download`
 	
`member-scans/single/{id}/documents/{documentId}/pin`
 	
`member-scans/single/{id}/documents/{documentId}`
 	
`member-scans/single/{id}/documents/history`
	New methods for upload, list, download and delete supporting documents for Individual (member) scans.

`corp-scans/single/{id}/documents`
 	
`corp-scans/single/{id}/documents/{documentId}/download`
 	
`corp-scans/single/{id}/documents/{documentId}/pin`
 	
`corp-scans/single/{id}/documents/{documentId}`
 	
`corp-scans/single/{id}/documents/history`
	New methods for upload, list, download and delete supporting documents for Corporate scans.

`id-verification/single/{id}/documents`
`id-verification/single/{id}/documents/{documentId}/download`
`id-verification/single/{id}/documents/{documentId}/pin`
`id-verification/single/{id}/documents/{documentId}`
`id-verification/single/{id}/documents/history`
	New methods for upload, list, download and delete supporting documents for ID verification.

`kyb/single/{id}/documents`
`kyb/single/{id}/documents/{documentId}/download`
`kyb/single/{id}/documents/{documentId}/pin`
`kyb/single/{id}/documents/{documentId}`
`kyb/single/{id}/documents/history`
	New methods for upload, list, download and delete supporting documents for Know Your Business scans.

`data-management/member-documents`
`data-management/corp-documents`
`data-management/single-scans/documents`
`data-management/documents`
	New methods to search and remove supporting documents.

Release 10.3

Released: Dec 1, 2024

Name	API Schema	Description
`GET organisations/new`		Temporarily removed.

`watchlists`	ScanInputParam CorpScanInputParam BatchScanInputParam CorpBatchScanInputParam	New input parameter used for setting the watchlist scope for screening. If this is NULL or undefined, the organisation's list access settings will be used by default.
`isWatchlistActive`	OrgDetails	Indicates if the watchlist selection option is enabled for user selection during screening.
`country`	ScanInputParam CorpScanInputParam	New input parameter to match for country of residence for individual or operation for corporates. Separate from Address and supports up to 5 countries. Format should be based on ISO 3166-1 alpha-2.
`nationality`	ScanInputParam	New input parameter to match for nationality or citizenship. Supports up to 5 nationalities. Format should be based on ISO 3166-1 alpha-2.
`country`	MonitoringListMemberItem MonitoringListCorpItem	Returns the country scanned for the entity.
`nationality`	MonitoringListMemberItem	Returns the nationality scanned for the individual person.
`IsIgnoreBlankNationalityActive`	OrgDetails.memberScanSettings	Returns the status of the ignore blank nationality match setting. When turned on, nationality is enforced during screening.

`member-scans/batch/{id}/monitor/enable`
 	
`member-scans/batch/{id}/monitor/disable`
 	
`corp-scans/batch/{id}/monitor/enable`
 	
`corp-scans/batch/{id}/monitor/disable`
		Add (enable) or remove (disable) Member or Corporate batch scans from monitoring.

`lastMonitored`	MonitoringListMemberItem MonitoringListCorpItem	New parameter of the last monitored date of the entity.

`lastMonitoredFrom`
 	
`lastMonitoredTo`
	MonitoringListMemberItem
	
	MonitoringListCorpItem
	
	monitoring-lists/member/report
	
	monitoring-lists/corp/report
		New input parameter to search for last monitored date.

Release 10.2

Released: Oct 27, 2024

Name	API Schema	Description

`member-scans/single/{id}/monitor/review`
 	
`corp-scans/single/{id}/monitor/review`
		If Monitoring Review has been enabled for th organisation by the Compliance Officer via th Organisation Administration UI, you can set re status to track assessment of profile updates ongoing monitoring. Check for the organisati monitoring review status via `monitoringSettings.monitoringReviewEnab` `GET organisations/{id}`.

`reviewStatus`	MonitoringScanHistoryLog CorpMonitoringScanHistoryLog	New optional input parameter to filter for mor review status.

`reviewStatus`
 	
`membersReviewed`
 	
`companiesReviewed`
	MonitoringScanHistoryLog
	
	CorpMonitoringScanHistoryLog
		Returns the overall monitoring review status monitoring event with the number of entities completed review for In Progress assessmen

`monitoringReviewStatus`
 	
`monitoringReviewSummary`
	ScanHistoryDetail.scanResult
	
	CorpScanHistoryDetail.scanResult
		Returns the completed review status of the monitored entity with detected changes. Sum contains the **date time** and **username** to indic user who has marked the assessment as con for auditing references.

`category`	CorpScanHistoryLog	New value `SOE` added to category for State C Enterprise entities.
`scanType`		New value `AllWithMonitoring` added to sca in `GET data-management/scans/count` and `DELETE data-management/scans`.
`subCategory`		New values added for former PEP and former sanctions in `GET member-scans/single` and `corp-scans/single`
`lookup-values/sso-url/{token}`	SsoSettings	New method to return the Single Sign-On (SS login and logout URLs

`identity`
 	
`clientId`
	UserDetails.userSsoSettings	The unique identity (e.g. email address) of th and the unique key of the Identity Provider.

Release 10.1

Released: Jun 30, 2024

Name	API Schema	Description
`whitelistPolicy`	orgDetails.monitoringSettings.memberScanSettings orgDetails.monitoringSettings.corporateScanSettings	Returns the monitoring whitelist policy setting if due diligence decisions are applied or ignored for continuous monitoring and monitoring rescans.

Release 9.6

Released: May 19, 2024

Name	API Schema	Description

`dobTolerance`	ScanInputParam BatchScanInputParam	New parameter to specify the number of years allowed for variations in the birthdate. Note: The organisation administration settings must have the policy enabled.

Release 9.5

Released: Mar 17, 2024

Name	API Schema	Description

`category`
 	
`subcategory`
 	
`risk`
 	
`overallRisk`
	RiskResult	New method to retrieve organisation-wide defined risk levels, and overall risk score, for the specific scan result. The risk levels are set by the Compliance Officer within the application Administration screens.

Release 9.4.2

Released: Feb 18, 2024

Name	API Schema	Description

`companyProfileAvailable`
 	
`productAvailable`
	KYBCountryResult	New parameters to indicate if the enhanced company details (including UBO) and registry documents are available for the country jurisdiction.

`companyProfileAvailable`
 	
`productAvailable`
	KYBStateResult	New parameters to indicate if the enhanced company details (including UBO) and registry documents are available for the country-state jurisdiction.

`nationalitiesCodes`	ScanResult.matchedEntities	2-letter country code of nationality based on ISO 3166-2 standard.
`taxHavenCountryResult`	ScanResult.matchedEntities CorpScanResult.matchedEntities	Indicator of tax haven jurisdiction.
`sanctionedCountryResult`	ScanResult.matchedEntities CorpScanResult.matchedEntities	Indicator of sanctioned jurisdiction.

`isPrimaryLocation`
 	
`countryCode`
 	
`comment`
 	
`url`
	ScanResult.matchedEntities.
	taxHavenCountryResults
	
	CorpScanResult.matchedEntities.
	taxHavenCountryResults
	
	ScanResult.matchedEntities.
	resultEntity.taxHavenCountryResults
	
	CorpScanResult.matchedEntities.
	resultEntity.taxHavenCountryResults
	
	ScanResult.matchedEntities.
	monitoredOldEntity.taxHavenCountryResults
	
	CorpScanResult.matchedEntities.
	monitoredOldEntity.taxHavenCountryResults
		Additional information of the tax haven jurisdiction and if it applies to the primary location of the entity.

`isPrimaryLocation`
`countryCode`
`comment`
`url`
`isBlackList`
`isGreyList`
	ScanResult.matchedEntities.sanctionedCountryResults
	CorpScanResult.matchedEntities.sanctionedCountryResults
	ScanResult.matchedEntities.resultEntity.sanctionedCountryResults
	CorpScanResult.matchedEntities.resultEntity.sanctionedCountryResults
	ScanResult.matchedEntities.monitoredOldEntity.sanctionedCountryResults
	CorpScanResult.matchedEntities.monitoredOldEntity.sanctionedCountryResults
		Additional information of the sanctioned jurisdiction and if it applies to the primary location of the entity.

`scanService`	ScanHistoryDetail.scanParam CorpScanHistoryDetail.scanParam	New parameter returns the type of scan service.

Release 9.4

Released: Dec 10, 2023

Name	API Schema	Description
`comment` `url`	ScanResult.matchedEntities.taxHavenCountryResult CorpScanResult.matchedEntities.taxHavenCountryResult	New parameters to indicate if the individual's primary country of residence or a company's primary address is considered a tax haven country.

`comment`
`url`
`isBlackList`
`isGreyList`
	ScanResult.matchedEntities.
	sanctionedCountryResult
	CorpScanResult.matchedEntities.
	sanctionedCountryResult
		New parameters to indicate if the individual's primary country of residence or a company's primary address is considered a sanctioned country, and the associated FATF lists. Countries in the "black list" are considered high risk jurisdictions and "grey lists" are countries under increased monitoring.

`isAIAnalysisActive`	OrgInfo OrgDetails	Indicates if the **AI Analysis** service is enabled for organisation.
`isKybActive`	OrgInfo OrgDetails.corporateScanSettings	Indicates if the **Business check** service (KYB) is enabled for organisation.
`aiAnalysisQuestionCount`	ScanResult.matchedEntities CorpScanResult.matchedEntities	Returns the number of remaining questions or credits for AI queries on a profile.
`member-scans/single/results/{id}/questions` `member-scans/single/results/{id}/questions/{questionId}`		New methods available in Individual scans to perform AI Analysis of profiles.
`corp-scans/single/results/{id}/questions` `corp-scans/single/results/{id}/questions/{questionId}`		New methods available in Corporate scans to perform AI Analysis of profiles.

`kyb/countries`
`kyb/countries/{countryCode}/states`
`kyb/company`
`kyb/{scanId}/company/profile`
`kyb/{scanId}/products`
`kyb/{scanId}/products/order`
`kyb/{scanId}/products/status`
`kyb/{scanId}/products/{productId}/file`
`kyb/{scanId}`
`kyb/{scanId}/company/{companyId}/report`
`kyb/{scanId}/products/file`
`kyb/{scanId}/company/{companyId}/products/file`
`kyb/{scanId}/products/sample/{productTitle}/file`
`kyb/{scanId}/company/{companyId}/profile/report`
`kyb/{scanId}/company/profile/charge`
`kyb/{scanId}/products/report`
		New methods available in business-ubo-checks to support business verifications for Know Your Business (KYB) and Ultimate Beneficial Owner (UBO).

`reports/business-ubo-activity`		New method to download report of KYB and UBO activities.
`scanType`	data-management/scans data-management/corp-scans data-management/scans/count	Support for KYB scan type.

`countryCode`
`registrationNumberSearch`
`allowDuplicateKYBScan`
	CorpScanInputParam.kybParam	New parameters for Business check service (KYB).

`KYBCountry`	CorpScanInputParamHistory	Country or country-state code for KYB scan
`KYBScanResult`	CorpScanResult	Results returned for KYB scan

`KYBProductsCount`
`KYBCompanyProfileCount`
`IsPaS`
`IsKYB`
`ScanService`
	CorpScanHistoryLog	Returns KYB related information for KYB scans.

Release 9.3.4

Released: August 6, 2023

Name	API Schema	Description
`data-management/member-scans`		New method to return a list of Individual scan results and the associated `scanId`. This provides a subset of functionality to `member-scans/single` but is specifically catered for API user accounts with **data management** permissions.
`data-management/corp-scans`		New method to return a list of Corporate scan results and the associated `scanId`. This provides a subset of functionality to `corp-scans/single` but is specifically catered for API user accounts with **data management** permissions.
`data-management/single-scans`		New method to delete at a granular level, single scan results for Individual and Corporate entities. This includes **PEP, Sanctions & Adverse Media** and **ID Verification** results.

Release 9.3.3

Released: June 25, 2023

Name	API Schema	Description
`idNumber`	ScanInputParam	Optionally include an ID Number (e.g. Passport Number, National ID, VAT/Tax Number, Professional Registration ID) for screening of the individual to exclude matches that does not contain the entered ID Number.
`includeJurisdictionRisk`	ScanInputParam BatchScanInputParam CorpScanInputParam CorpBatchScanInputParam	Option to search for FATF jurisdiction risk rating and information for countries associated with matched profiles.
`fatfJurisdictionRiskResult.jurisdiction`	ScanResult CorpScanResult	Country name of FATF jurisdiction.
`fatfJurisdictionRiskResult.effectivenessScore`	ScanResult CorpScanResult	Effectiveness score to which the country's measures are effective based on the ratings against the 11 immediate outcomes from FATF.
`fatfJurisdictionRiskResult.effectivenessLevel`	ScanResult CorpScanResult	Level of effectiveness of the country's measures.
`fatfJurisdictionRiskResult.complianceScore`	ScanResult CorpScanResult	Compliance score to which the country's implementation of technical requirements of the 40 FATF Recommendations.
`fatfJurisdictionRiskResult.complianceLevel`	ScanResult CorpScanResult	Level of compliance of the country's technical implementation.
`fatfJurisdictionRiskResult.comments`	ScanResult CorpScanResult	Summary of compliance with FATF recommendations.
`fatfJurisdictionRiskResult.fatfCompliance`	ScanResult CorpScanResult	Status of compliance.

`fatfJurisdictionRiskResult.fatfComplianceNotes`	ScanResult CorpScanResult	Notes on compliance shortcomings.
`fatfJurisdictionRiskResult.fatfEffectiveness`	ScanResult CorpScanResult	Level of effectiveness of the country's measures.
`fatfJurisdictionRiskResult.fatfEffectivenessNotes`	ScanResult CorpScanResult	Notes on effectiveness shortcomings.
`fatfJurisdictionRiskResult.fatfEffectivenessSubtitles`	ScanResult CorpScanResult	Overall level of effectiveness of the country's measures.
`fatfJurisdictionRiskResult.countryCode`	ScanResult CorpScanResult	Two-letter country code.

Release 9.3.1

Released: May 7, 2023

Name	API Schema	Description
`closeMatchRateThreshold`	CorpScanInputParam CorpBatchScanInputParam	Specify the close match rate threshold for entity screening (from `100`% for very close to `1`% for somewhat similar). This is optional and defaults to `80`% if not specified.
`closeMatchRateThreshold`	CorpScanInputParamHistory CorpBatchScanResults CorpMonitoringScanResults	Returns Close Match Rate threshold applied during screening.
`matchRate`	CorpScanEntity	Returns percentage rate of the matching name of the entity profile.

Release 9.3

Released: February 26, 2023

Name	API Schema	Description

`title`	Entity	Removed parameter.
`NameDetail.title`	Entity	Removed parameter.
`disqualifiedDirectors`	Entity	New parameter for a list of disqualifications for the profile.
`nationalities`	Entity	New parameter with the nationalities of the profile.
`placeOfBirth`	Entity	New parameter for the birthplace for the profile.
`generalInfo`	Entity	Parameter changed to only return the nationality for an individual.
`generalInfo`	EntityCorp	Parameter changed to return additional information for the company, where available.
`enterDate`	Entity EntityCorp	Removed parameter.
`xmlFurtherInformation`	Entity EntityCorp	Removed parameter.
`identifiers`	Entity EntityCorp	New parameter for a list of registration or ID numbers for the profile.
`images`	Entity EntityCorp	New parameter with a list of pictures available for the profile.
`lastReviewed`	Entity EntityCorp	New parameter of date the profile record was last reviewed or updated.
`profileOfInterest`	Entity EntityCorp	New parameter with detailed profile of interests for the profile.
`category`	Entity EntityCorp	Parameter includes the new "POI" category of the profile.
`categories`	Entity EntityCorp	Parameter includes the new "POI" category of the profile.
`countryCode`	Location	New parameter for the country code of the location.

`type`	Location	New parameter for the location type.
`category`	OfficialList	New parameter for the watchlist category of the official list.
`measures`	OfficialList	New parameter with a list of measures enforced by the official list.
`origin`	OfficialList	New parameter of the country or region of the official list.
`types`	OfficialList	New parameter of the type of sanction classified by the official list.
`segment`	Role	New parameter of the category of in scope positions for the PEP for a particular country.
`status`	Role	New parameter of the status of the associated role held by the PEP.
`details`	Source	New parameter with a list of details for the captured source and adverse media.
`categories`	Source	Changes in the returned values for the category of the source and adverse media.
`nameType`	NameDetail CorpNameDetail	Change in returned values. Expanded to include more details.
`description1`	Description	Parameter includes the new "POI" reference for the profile.
`description2`	Description	Parameter includes the new "Reputational Risk" reference for the profile.
`category`	AssociatePerson AssociateCorp	Parameter includes the new "POI" reference for the profile.

Release 9.2.1

Released: February 12, 2023

Name	API Schema	Description

`emailAddress`	IDVInputParam	New parameter to enable the ID Verification request link to be sent to the individual's email address.
`birthDate`	IDVInputParam	New parameter for the individuals birthdate for ID Verification, if available. Date format: DD/MM/YYYY.
`idvSubType`	IDVInputParam	New parameter to specify the delivery method and ID Verification type e.g. email/SMS the ID Check, FaceMatch or both.
`dataBreachCheckParam.emailAddress`	ScanInputParam	New parameter to include the individual's email address to run a compromised information check against a list of known data breaches.
`dataBreachCheckResults`	ScanResult	New parameter in response body containing a list of email breaches found, if an email address was provided in `dataBreachCheckParam.emailAddress`.

Release 9.2

Released: December 10, 2022

Name	API Schema	Description
`isPepJurisdictionExclude`	ScanInputParamHistory BatchScanResults MonitoringScanResults	New parameter to either include or exclude one or more countries for the PEP Jurisdiction policy.
`pepJurisdictionCountries`	ScanInputParamHistory BatchScanResults MonitoringScanResults	New parameter to specify one or more countries for inclusion or exclusion for PEP Jurisdiction.
`pepJurisdictionExclude`	ScanInputParamHistory BatchScanResults MonitoringScanResults	Decommission parameter.

Release 9.1.2

Released: October 1, 2022

Name	API Schema	Description
`dates`	Source	Decommission parameter. Replaced by `dates_Urls`
`dates_Urls`	Source	New parameter replacing `dates` to include link to cached PDF of URL, if available.