LSEG World-Check One

Client and Group Administrators Guide

LSEG RISK INTELLIGENCE

Contents

About this document

Intended readership

For World-Check One clients, selected for the roles of **Client** or **Group Administrator** (**Group Admin**).

In this guide

This guide will walk you through simple steps to completing administrative tasks in World-Check One as a Client or Group Administrator. Learn how to create groups, new roles and users, and configure group search settings.

WORLD-CHECK ONE ADMINISTRATORS

There are **three** types of **administrator** roles in the World-Check system:

LSEG Admin

- Users with this role are **Refinitiv Professional Services** personnel and are the only users allowed to create **new Client accounts**.

Client Admin

- Users with this role belong to the **Client organization** (i.e. not LSEG personnel). Client Admin users can maintain the **primary group** as well as **create child groups**, **users, roles** etc. for the particular account.

Group Admin

- Users with this role belong to the **Client organization** (i.e. not LSEG personnel). Group Admin users can maintain the **group** they administer as well as **create child groups**, **users**, etc. for the particular group.

This guide covers the **Client and Group Administrator** roles.

Client Admin and Group Admin Accesses

The following table indicates what editing rights are afforded to the Client and Group Administrator roles.

	Access All Groups	**Maintain Primary Group**	**Create Parent & Child Groups**	**Maintain Parent & Child Groups**	**Create Users**	**Create & Edit Roles**	**Delete Groups**
Client Admin	Y	Y	Y	Y	Y	Y	Y
Group Admin	N (only those they administer)	N	N	Y	Y	N	Y

GROUPS

The concept of "Groups" was designed originally for clients to be able to group multiple related cases under one umbrella. Among other considerations, group configurations may vary for the following reasons:

As per screening needs

You can create a group with stricter settings for high-risk clients, and another group for low-risk clients.

Organizational hierarchy

Different business units within the same organization can have separate groups and group settings in line with your organization's risk appetite.

Group Allowance Threshold

Although there is no system block on group creation, our technical recommendations would be that no more than **1,000 groups** be created (at an absolute maximum). A higher number of groups may affect general performance, such as load time when reviewing cases in Case Manager, as well as on the initial screening page.

There are **three** sorts of groups in World-Check One:

Primary Group

- A **Primary Group** is **automatically** created when a Client account is set up on World-Check One. It is the **highest group** in the World-Check One group hierarchy and contains the **default settings** that you can use across all other sub-groups (Parent and Child Groups).

Parent Group

- If the Primary Group is the overarching group governing all groups contained below it, then a **Parent group** is a **sub-group** of the Primary group. *You can customise the group settings so that they differ from the default settings within the Primary Group.*

Child Group

- A **Child Group** is the **sub-group of a Parent group** (i.e. the sub-group of a sub-group). Not all Parent Groups need Child Groups. *You can customise the group settings so that they differ from the default settings within the Primary Group.*

This guide covers **all three groups** as they relate to the **Client** and **Group Administrator** roles.

PRIMARY GROUP ACCOUNT

Once you have created your login and gained access to World-Check One, you will land on the **Client Summary** page. The client account will have already been created for you with a **standardised set of default settings**. To manually navigate to the Client Summary page:

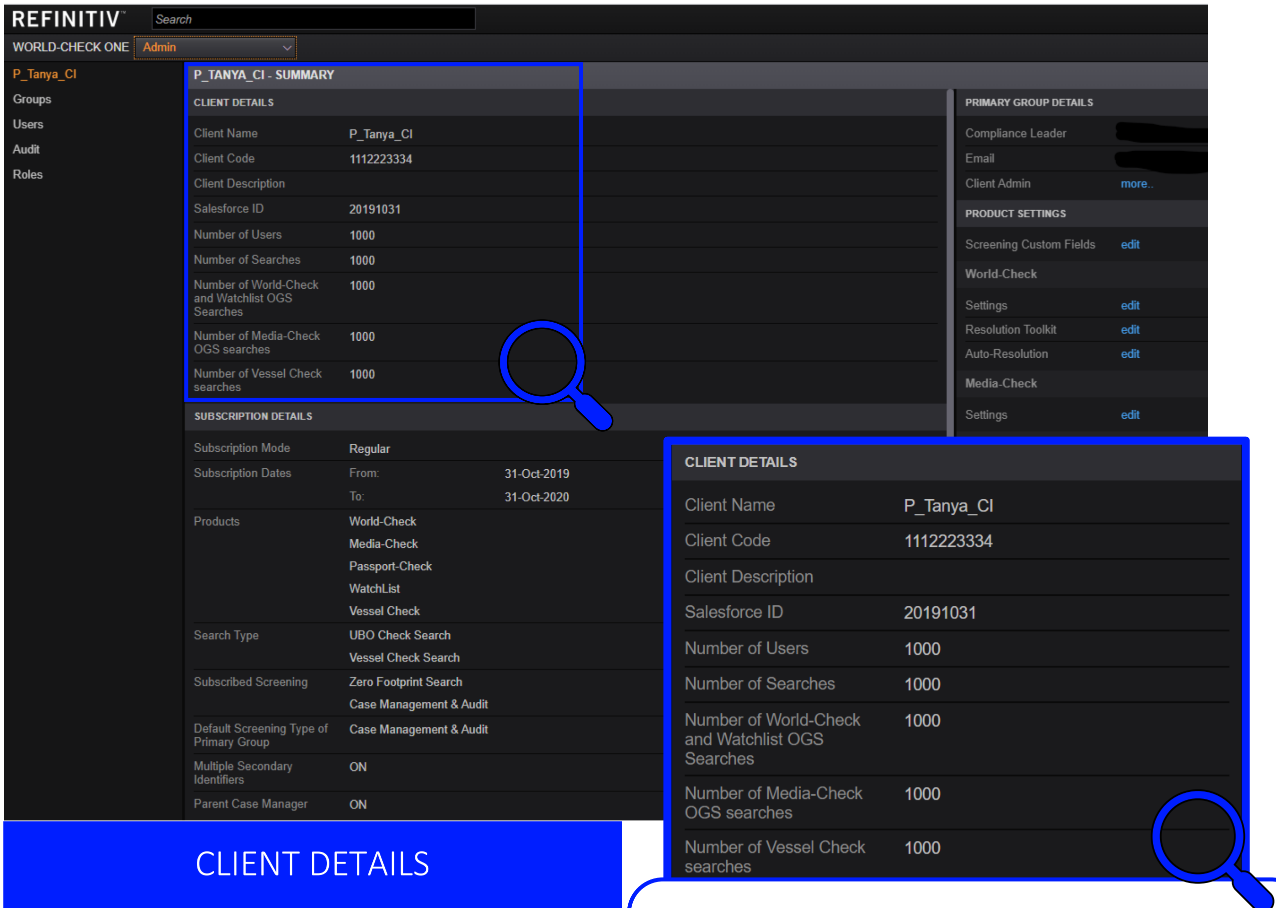
1. Go to **Admin** from the dropdown menu at the top of the screen.

2. A menu will appear in the left-hand panel of the page. Select the **Primary group** (this will be the first item on the menu list). The Client Summary page will appear to the right.

CLIENT SUMMARY PAGE

The Client Summary page provides a broad overview of your **Client details**, **Subscription details**, **Primary Group details**, and additional **features**. You can also edit the **Product Settings**.

Client Summary page:



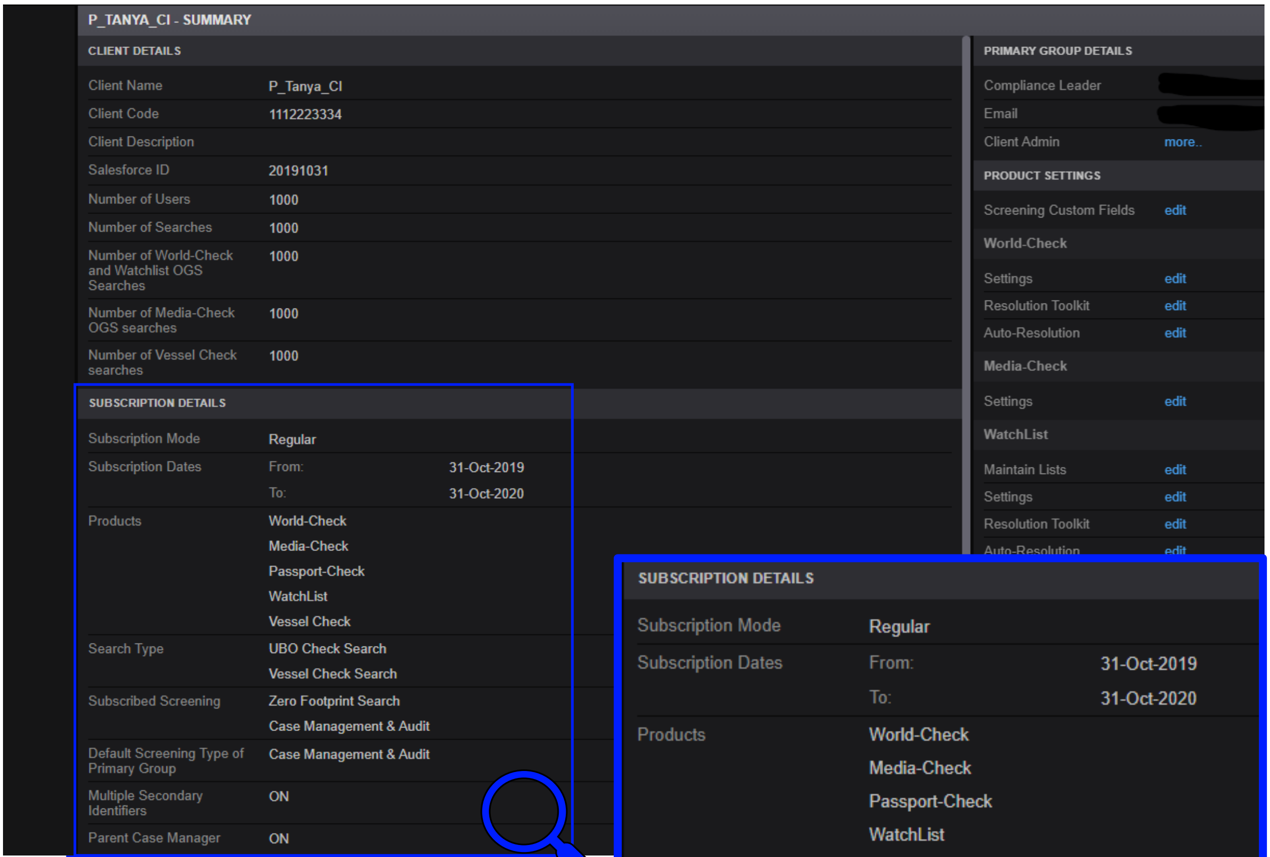
CLIENT DETAILS

Ongoing Screening (OGS): monitors **previously screened** records for any **updates** to the search results (e.g. with OGS turned ON, you will receive notification of an update to an entity appearing on a public sanction record where it did not appear previously).

The **Client Details** section includes:

- **Client Name**
- Unique **Client Code**
- Total **users allowed** under the account
- Total **searches allowed** per contract
- Number of **Ongoing Screening (OGS)** searches allowed per contract for World-Check, Media-Check and Watchlist, as well as number of **Vessel Check** searches.

Client Summary page:

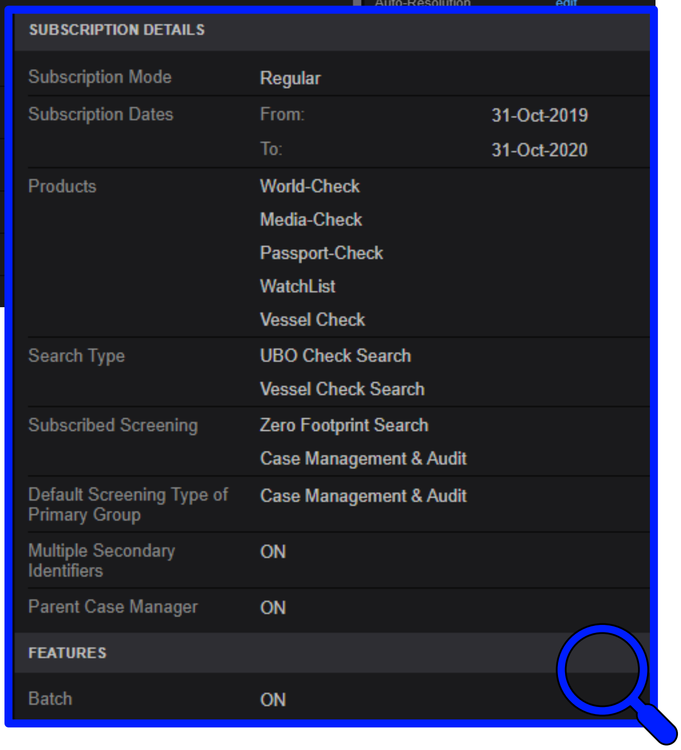


SUBSCRIPTION DETAILS

The Subscription **Details** section includes:

- **Subscription Mode**
- **Subscription dates**
- **Products** active on your account
- Different **search types** (additionally to World-Check)
- **Screening types** subscribed to and the default screening type preference, e.g. Zero Footprint Search.
- This section will also indicate whether **Multiple Secondary Identifiers** and **Parent Case Manager** is turned ON.

Search Type: The search options available will depend on your **account subscription**. In addition to the default World-Check search feature, any other search features active on your account will appear here. In the above example, **UBO Check** and **Vessel Check** are active.

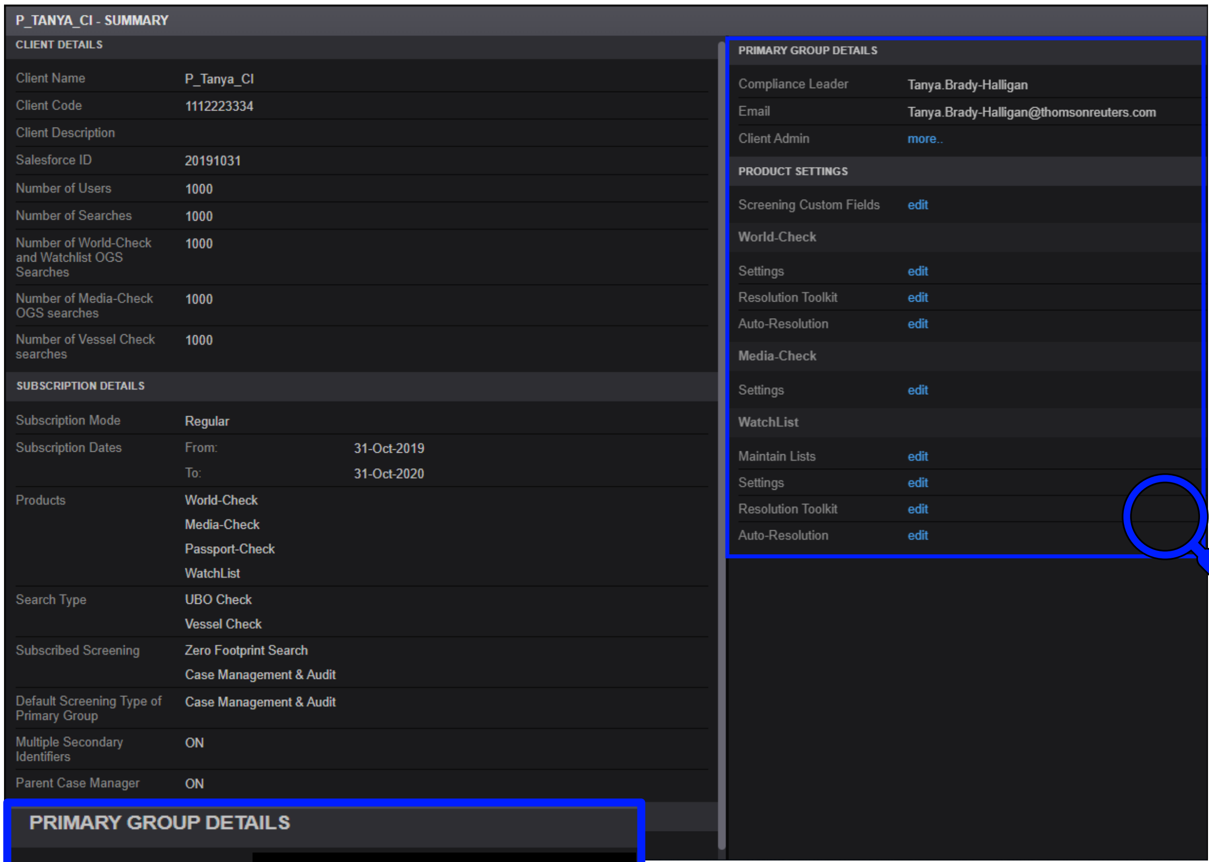


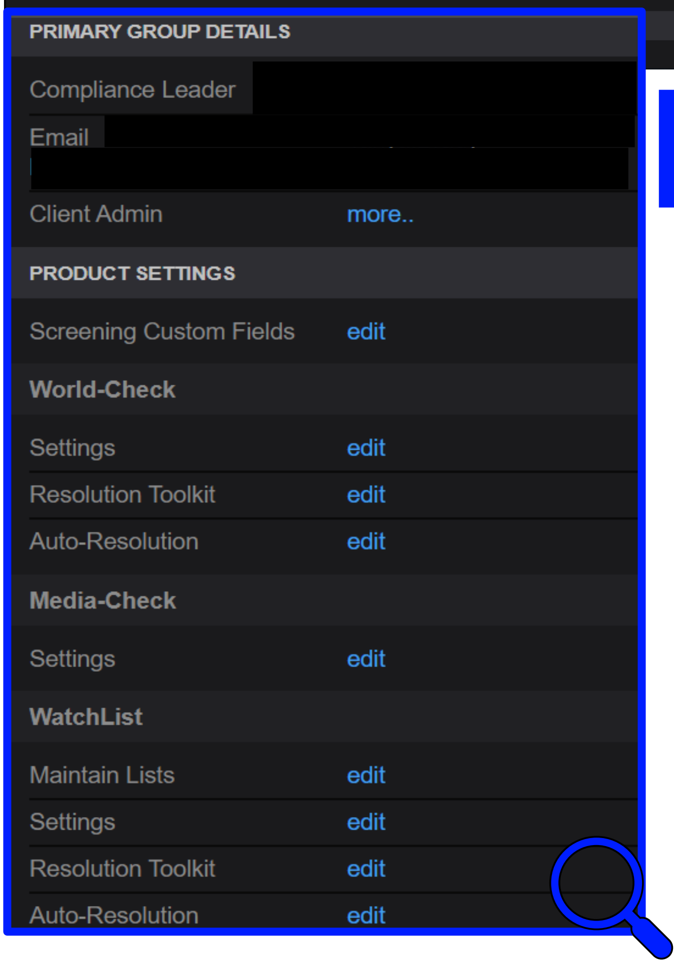
Zero Footprint Search (ZFS): If you have subscribed to this screening type, or set up screening groups with this screening type, you will be able to conduct searches that will **not** be recorded / saved. This option will appear in the left-hand menu panel on the **Screening** page.

Multiple Secondary Identifiers: Secondary Identifiers that allow for multiple entries are **Date of Birth**, **Nationality**, **Registered Country**, **IMO Number, Place of Birth** etc.

Features: Additional features, such as **Batch Screening** are included at subscription level. Batch Screening allows you to **screen records in bulk**.

Client Summary page:





PRIMARY GROUP DETAILS & PRODUCT SETTINGS

The **Primary Group Details** section includes your **Compliance Leader** and email address.

Click **more..** to go the **Group Admin** page to edit Group Administrator settings and make changes on a **primary or child group** level.

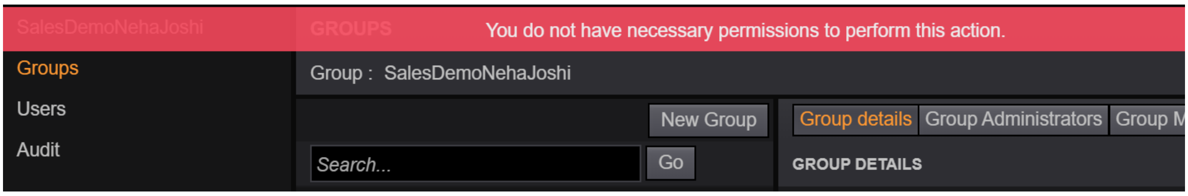
The **Product Settings** section allows you to edit all settings from the **Primary Group** down.

Refer to the Group Settings and Optional Settings sections of this document for more information on the various settings and how to adjust them to suit your organizational needs.

Do I Have Group Administrator Access?

Only the groups that you administer will be accessible to you. Client Administrators, by default, will be able to access all groups. To view the groups you administer, go to the **Group Admin** page:

1. On the **Client Summary** page, from the left-hand panel, select **Groups**.
2. A list of groups you administer will appear.
3. If you are *not* an administrator for the selected group, the following message is displayed:



To gain Group Administrator access

Speak to your **Client Administrator** to request Group Administrator access.

For Client Administrators

To create a new Group Administrator, head to the Create a New User section where you can create a new Group Administrator or edit an existing user's role to allow Group Administrator rights.

Default Settings

The standardised settings will enable your organization to start using World-Check One instantly, without having to make any further changes.

If you are the Client Administrator

Please review and make any changes that would be appropriate for your organization.

If you are not the Client Administrator

Your **Client Administrator** would have already reviewed the settings and made the appropriate changes for the Client and Primary Group. Liaise with your Client Administrator as appropriate.

If you are the Client Administrator of a Primary Group

You will have permission to edit the Primary Group details.

If you are a Group Administrator for a Parent or Child Group

Then you will only have permission to edit the group that you have been assigned to and create child group(s) for that group.

GROUPS

Client Administrators

You will now need to create **screening groups**, **add users**, and create their **roles**. This will ensure that others in your organisation can conduct screening too.

A few things to know before you begin:

- There is only one group to start with: the Client Group. All primary groups and their sub-groups must be created within this group
- The sub-group will inherit all the primary group settings by default
- You, or the user you assign as the Group Administrator to the sub-group, can then change the sub-group settings as desired.

Consider your organization's structure prior to creating sub-groups. In some instances, you may want to keep your primary group as a "template" and set up screening sub-groups to reflect different business needs.

Do you want all users to access all groups?

You can choose to set up all users on the Primary Group. If you want to restrict access to some users, set up sub-groups and only assign users to these groups.

Group Administrators

Group Administrators can only create groups within the groups they administer. Your Client Administrator will assign you as a Group Administrator at their discretion.

Example of Group Setup

The below example follows the setup:

Client Group: 'P_Tanya_CI'

- This is the default group that all other groups must be created under
- Only the Client Administrator has control over this group.

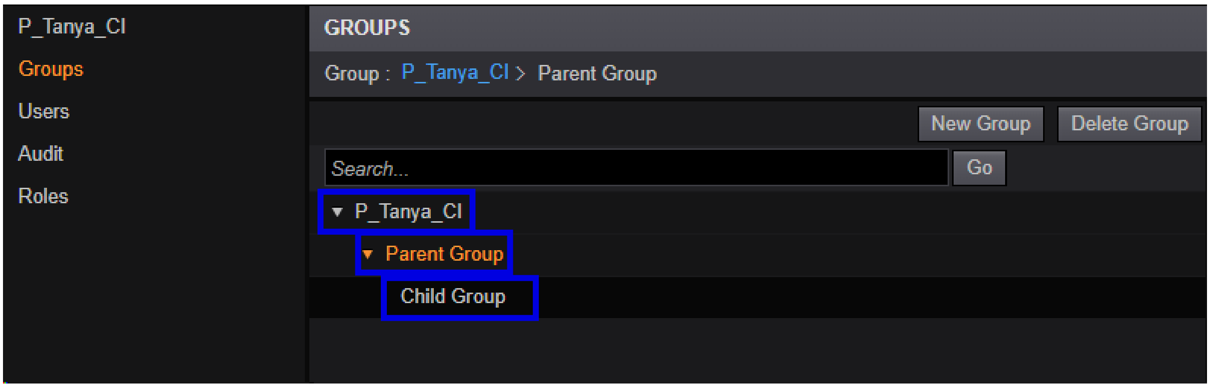
Parent Group

- The Parent Group has been created by the Client Administrator within the Client group, 'P_Tanya_CI.
- The Client Administrator can now assign users and roles to this group, as well as a Group Administrator.
- The group is orange because it has been selected for viewing.

Child Group

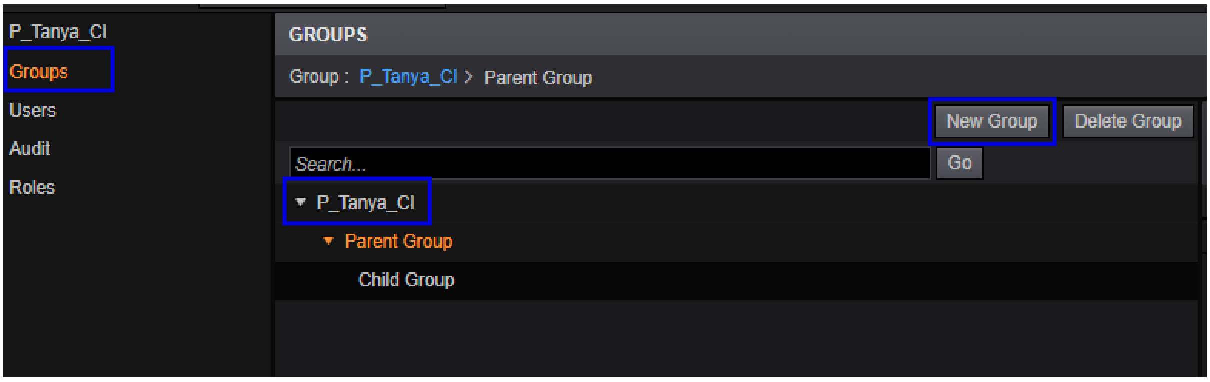
- The Child Group has been created within the Parent Group and is thus a **sub-group**
- This group could be created by either the Client Administrator *or* the Group Administrator.
- Both the Client and Group Administrator can add users to the group and assign roles (although the Group Administrator cannot create new roles for this group- the Group Administrator can only assign existing roles that the Client Administrator has already created).
- Both administrators can assign a Group Administrator to control the new Child Group.

Admin > Groups page > Primary Group example:



CREATE A GROUP

1. Go to the **Admin page** from the dropdown menu at the top of the World-Check page.
2. Once on the Admin page, select **Groups** from the left-hand side menu.
3. For Client Administrators who are setting up their groups for the first time, you will need to select the Client Group (this will be the only group). Otherwise, **select the group you would like to create a new group under**, then click **New Group**:

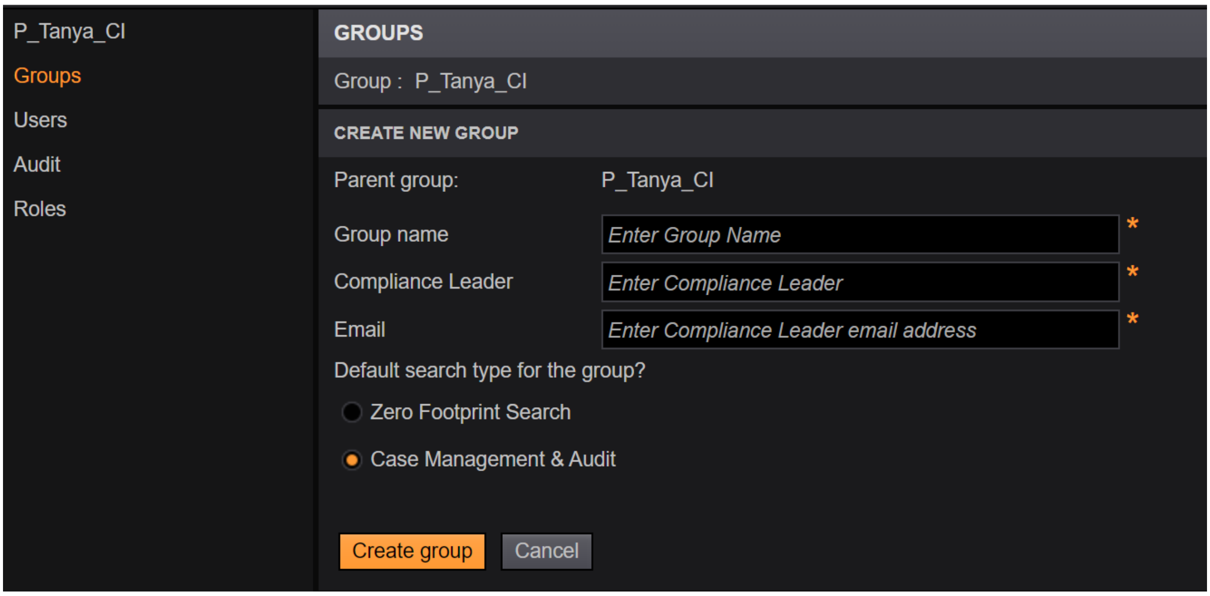


4. On the **Create New Group** page, you will need to enter a **Group Name**, **Compliance Leader name**, and **E-mail address**.
5. You will then be presented with a choice between **Zero Footprint** Search and Case Management and Audit. Choose a preferred search type and click **Create Group**.

Search Types

Zero Footprint Search: no audit trail of screening records will be left behind after conducting a search.

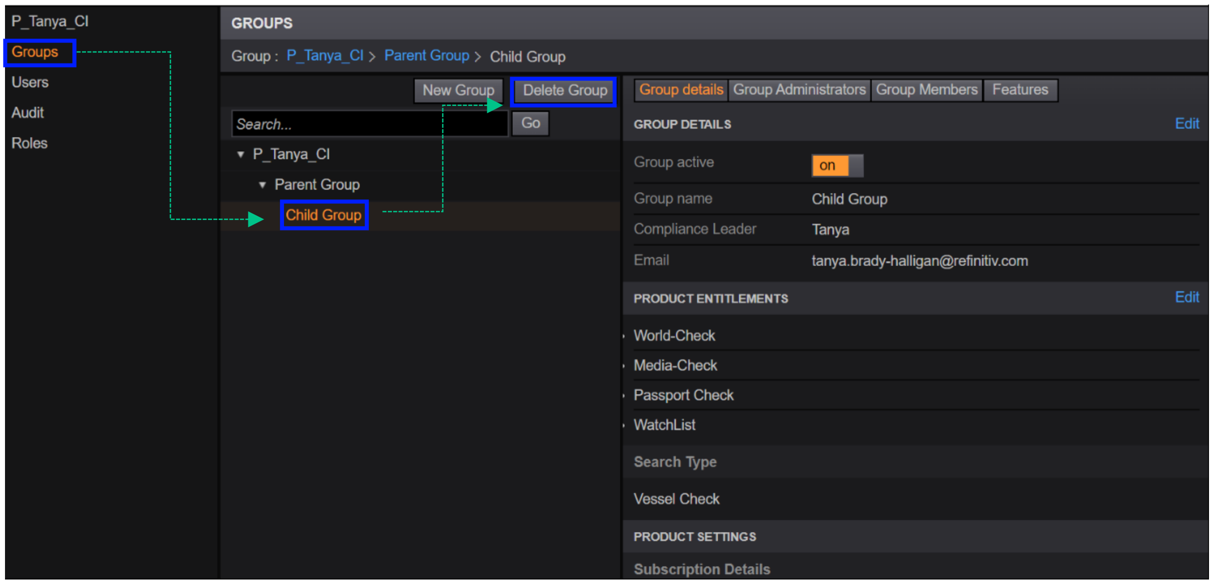
***Case Management and Audit*:** an audit trail of all screenings will be kept, and screening will be saved within Case Manager for later perusal, review, and remediation.



Delete a Group

You can **delete a group** if you no longer require it from the **Group Admin page**.

NOTE: NO active cases should exist within the group. You can delete a group that has archived cases connected to it but doing so will delete these cases permanently.



ROLES

Client Administrators

As a Client Administrator, you are automatically assigned all permissions of a **Group Administrator** for all the **child groups** within your Client/Primary Group.

You can **create your own custom roles** to assign to a user, or use the **pre-defined roles** in the system:

CLIENT_ADMIN

This is the **Client Administrator** and permissions cannot be changed within this role.

GROUP_ADMIN

This is the **Group Administrator** and permissions cannot be changed with in this role.

Case Manager

This is a custom pre-defined role that includes all permissions related to **screening/maintaining a case**. You can edit the Case Manager Role by removing permissions to suit your needs.

Group Administrators

As a Group Administrator, you will be able to add users to the groups you administer and assign to them pre-determined roles that the Client Administrator has created. You will not be able to create custom roles. You can choose to assign Group Administrator to any sub-groups you have created under the group/s you administer.

CREATE A NEW ROLE (Client Administrators only)

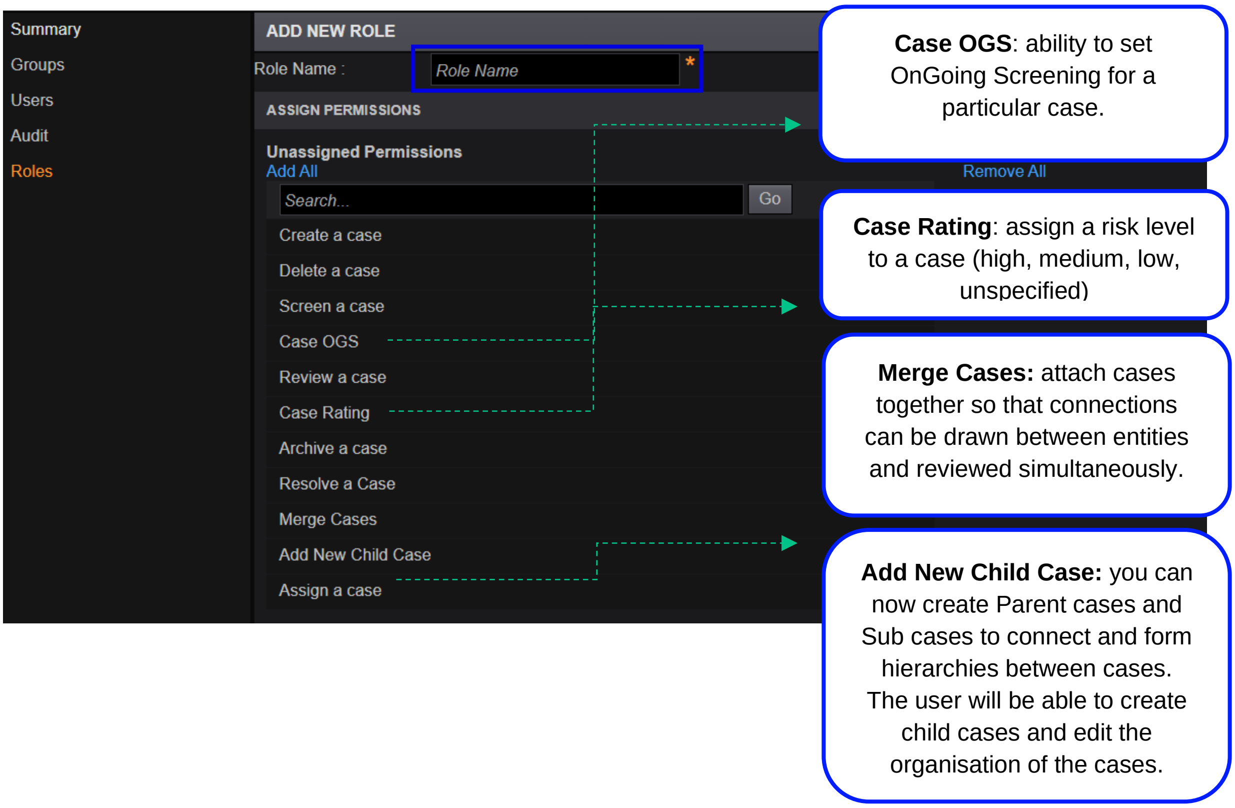
1. Go to **Admin** from the dropdown menu at the top of the World-Check page.

2. From the Admin page, select **Roles** from the left-hand menu, then click **New Roles** at the top right of the page.

3. The **Add New Role page** will appear. Provide a **Role Name** in the **Role Name field box**, then select **Create Role** at the bottom of the page.

4. Click on the desired permissions to add them to a role or select **Add All**. Your selections will appear in the **Assigned Permissions** section. Edit an existing role by deselecting permissions or hit **Remove All**.

Admin > Roles > New Roles:

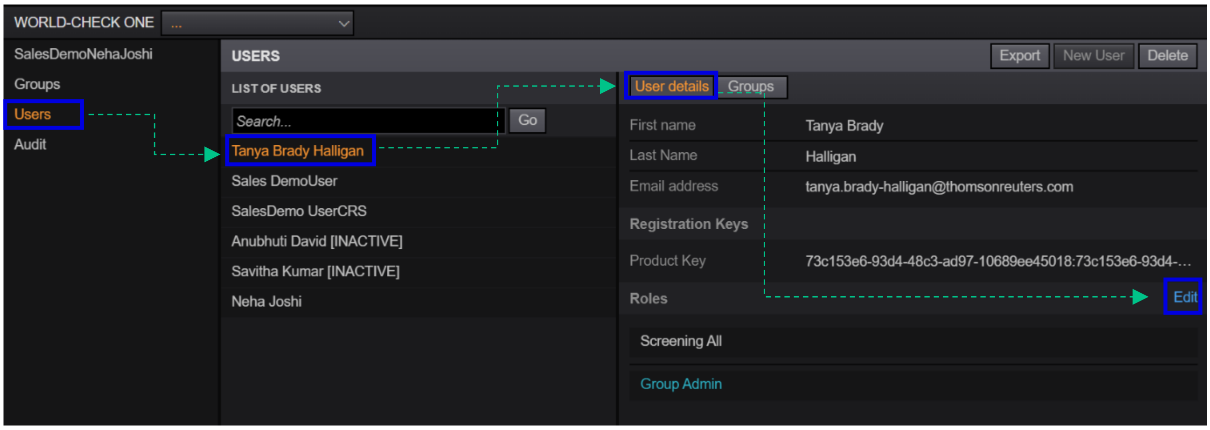


ASSIGN A ROLE

1. Go to the **Admin** page> select **Users** from the left-hand menu.

2. **Search and select** the user desired in the search box. A **Roles** section should appear under the **User details** tab on the right-hand side of the page.

Admin page > Users > User details:



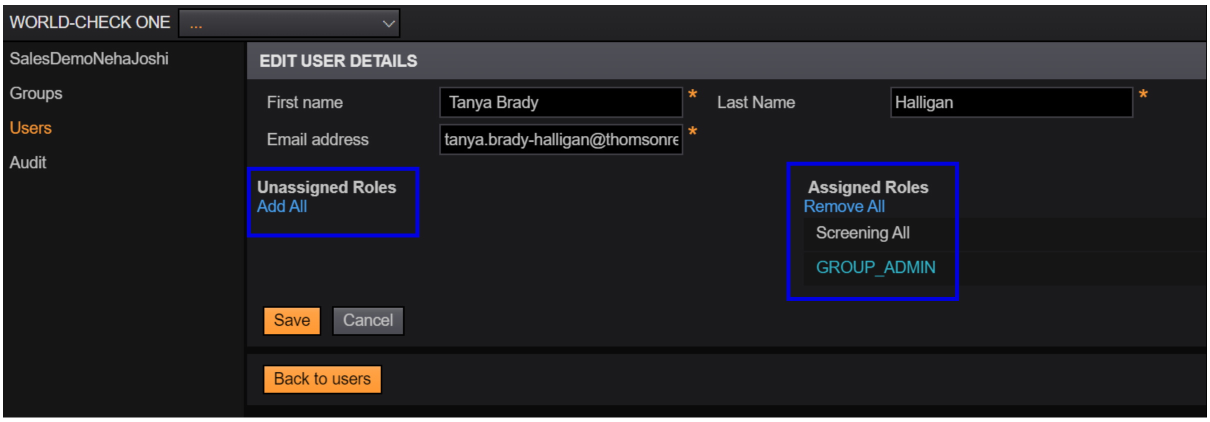
3. Under **Roles**, click **Edit**. You will be presented with the **Edit User Details** page.

4. Under the **Unassigned Roles** section, **click** to select any roles you wish to assign to the user. They will automatically move into the **Assigned Roles** section on the right-hand side. Click **Add All** to assign **all** available roles to a user.

5. To **unassign a role**, **click** on any of the roles listed under the **Assigned Roles** or click **Remove All** to deselect all options.

6. Click **Save**.

Roles > Edit User Details page:



Users

CREATE NEW USERS

Client Administrators

Client Administrators can create users for any all groups.

Group Administrators

As a Group Administrator, you are automatically assigned all permissions of a Group Administrator for all the **child groups** within your Primary Group.

1. Go to **Admin** > select **Users** from the left-hand menu > click **New User** at the top right of the page.

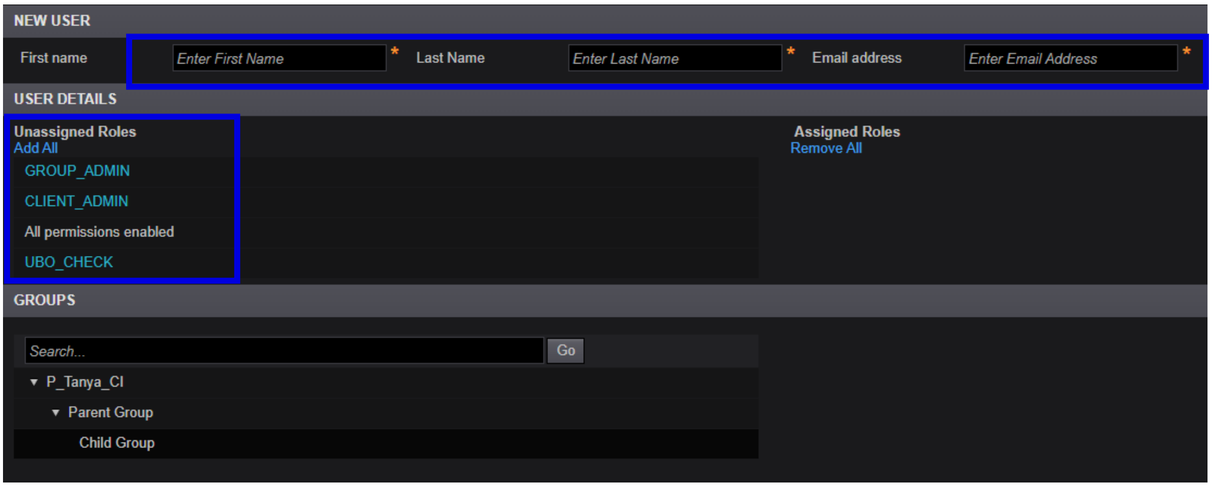
2. Enter the **first name**, **last name**, and **email address** of the new user in the field boxes

3. Add any **Unassigned** Roles by clicking on the role. Click **Add All** to include all roles under the user's name. To **remove** roles, click **Remove All** or select the roles you wish to remove by clicking on them.

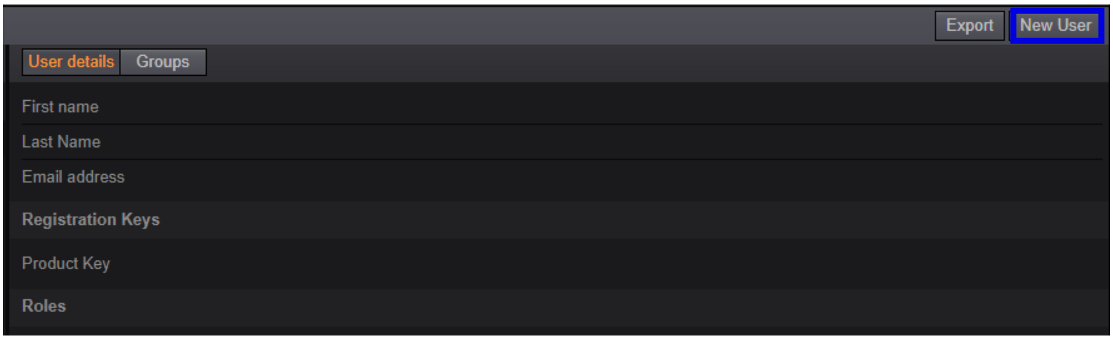
4. Select **Create user** at the bottom of the page.

NOTE: The Group Administrator can assign herself/himself other roles directly if appropriate.

Admin page > Users:



Users > New User:



NOTE: If you have reached the limit of users you can create, the following message will appear.

GROUP SETTINGS

The features in this section instruct you on how to set and adjust the parameters of your Group settings. The following features and what they do will be discussed in more detail: **Product Entitlements** and **Search Type**, **Auto-Include New Data Sources**, **Name Match Settings**, **Name Match Threshold**, and **Sources**.

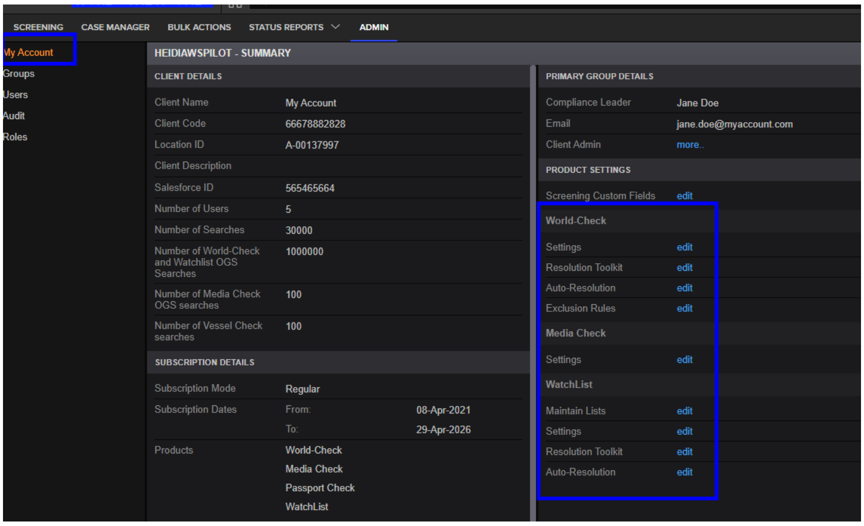
Client Administrators

Configure the settings for all groups from the **Client Summary page**:

1. Choose **Admin** from the dropdown menu. Select the **Primary Group** from the left-hand menu. The **Client Summary page** will appear.

2. Go to the **World-Check** section and hit **Edit** next to **Settings**. Continue reading for more information on each setting.

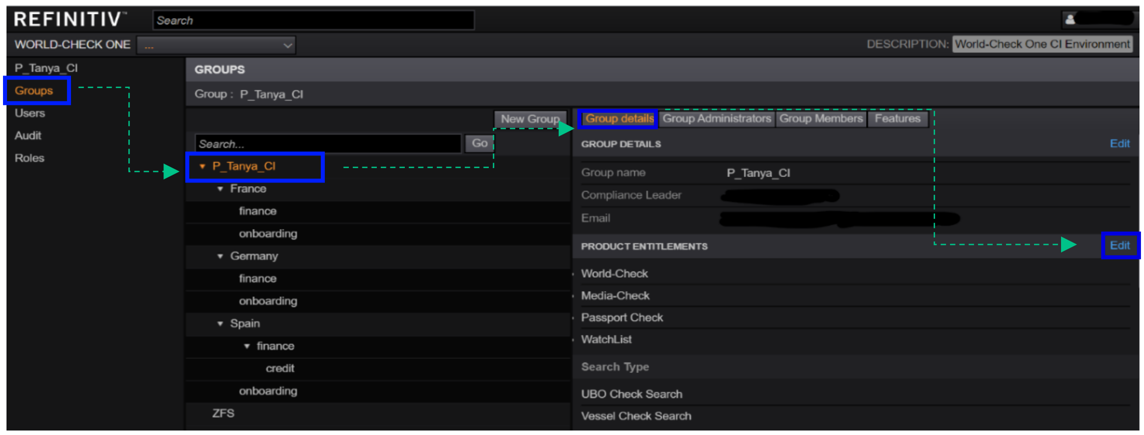
Admin > Client Summary page > World-Check Settings:



Group Administrators

To edit your group's settings, go to the **Group Details** tab from any **Group Admin** page and select **Edit** in the far-right corner of the page.

Group Admin page > Group details:

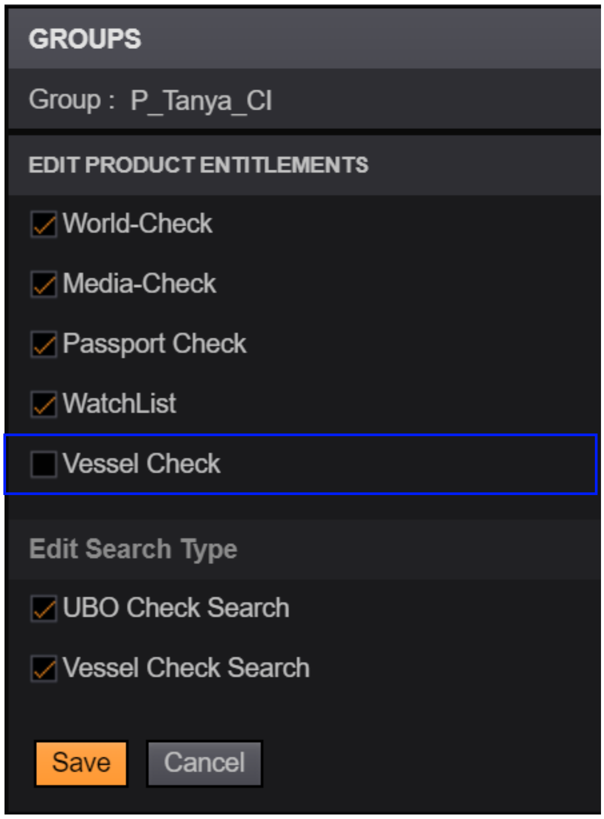


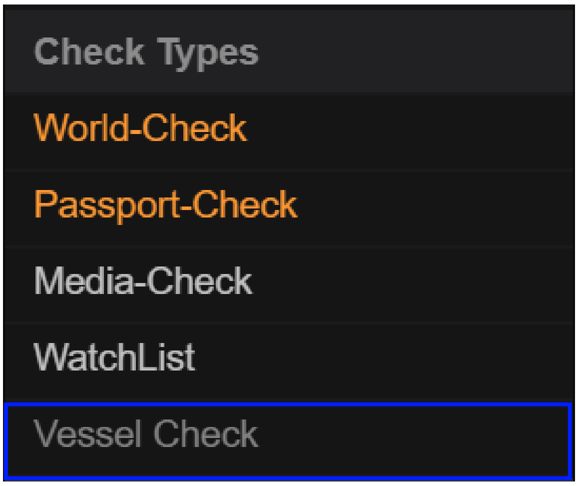
Product Entitlements and Search Type

From the Product Entitlements section, you can **edit the search and screening types** for your selected group. For example, turn on product entitlements for Media-Check and Passport Check, but turn off Vessel Check if that group will only be screening companies and individuals and will not need to search for vessels.

Product Entitlements

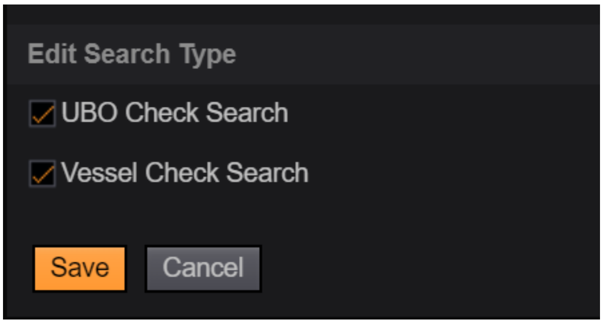
You can edit the product entitlements for World-Check cases here. Any cases that have been **turned OFF** will still appear on the **Screening page** but will be **greyed out** and you will be unable to select that Check Type.

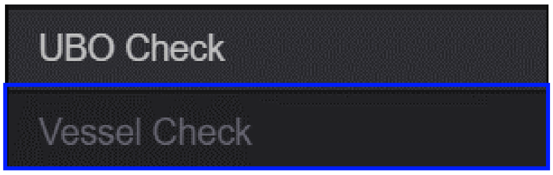




Search Types

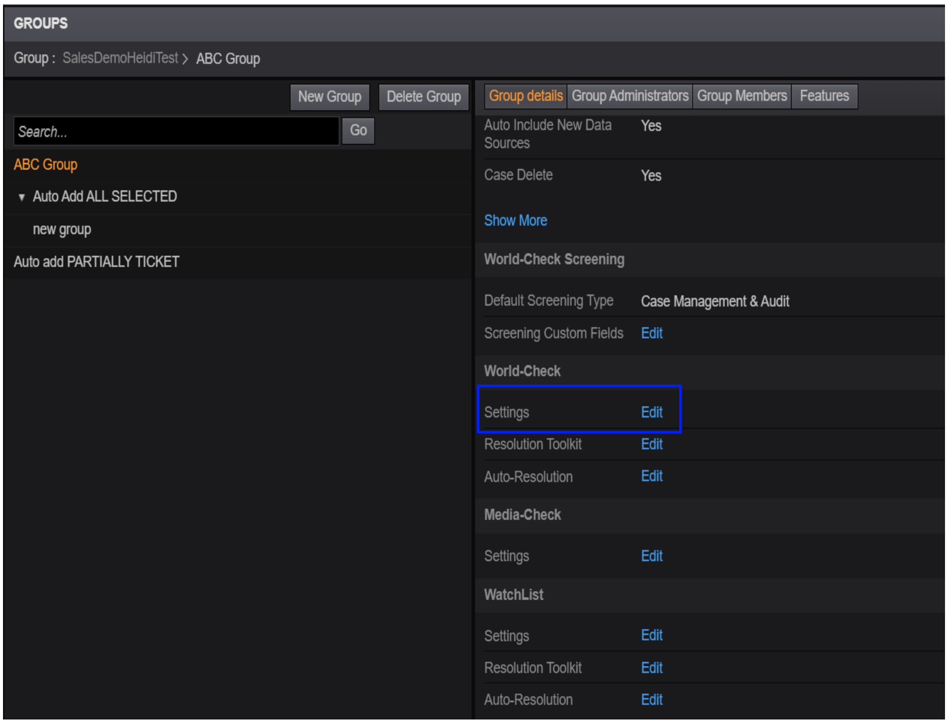
The search types available are **World-Check** (always turned ON by default), **UBO Check**, and **Vessel Check**. You can choose to turn on or off UBO and Vessel Check here depending on whether you would like the case you are screening to be saved as a World-Check case or as a UBO or Vessel case within Case Manager. If turned off, it will be greyed out on the Screening page.



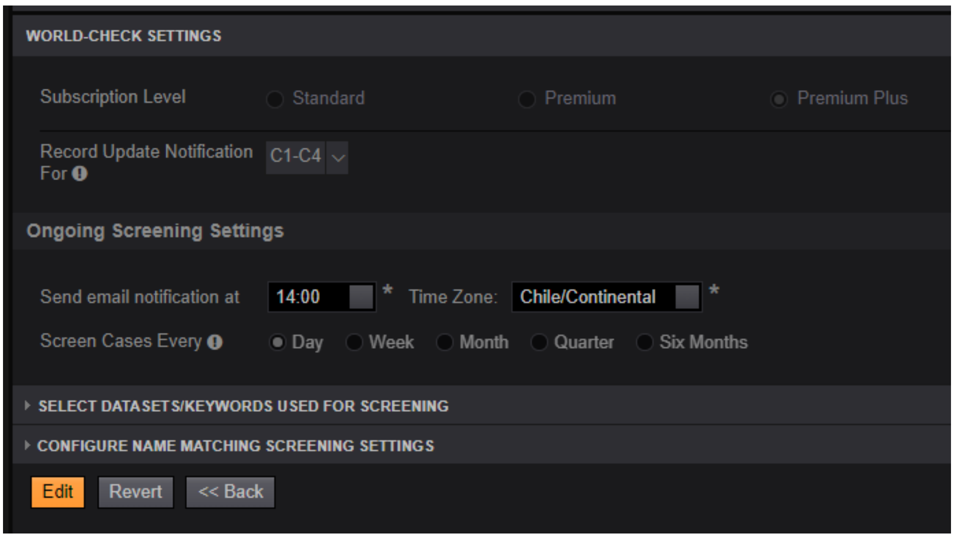


World-Check Screening Group Settings

From the **Group Details** tab, you can also edit the World-Check screening settings for that group. Use the scroll bar on the right-hand side of the page to scroll to the **World-Check** section, then select **Edit** next to **Settings**.



Once selected, you will be directed to the **World-Check Settings** page:

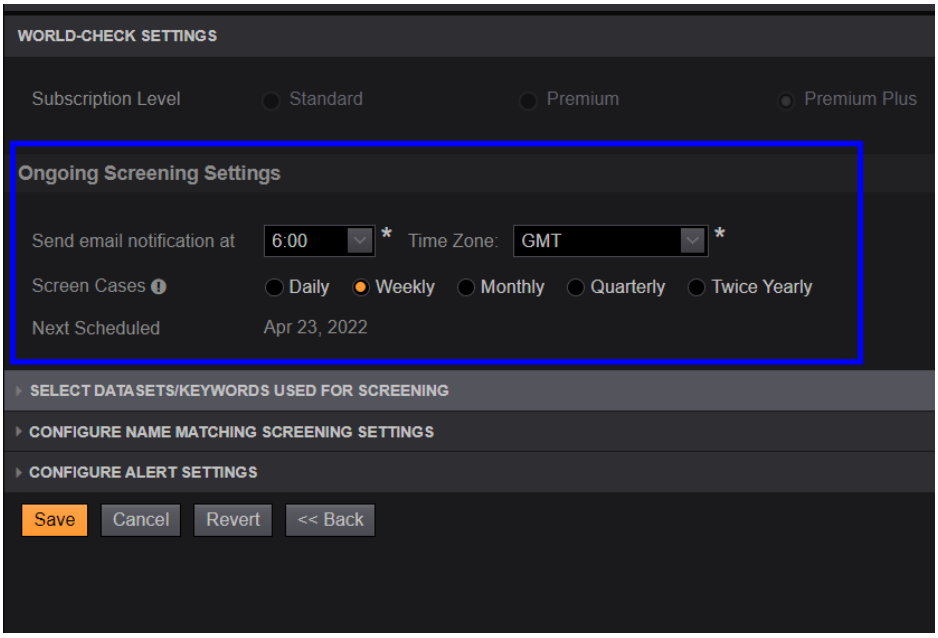


Ongoing Screening Settings

Ongoing Screening (OGS) Settings allows you to set OGS frequency at the group level to daily, weekly, monthly, quarterly or twice-yearly. The schedule for the respective settings is as follows:

How often?	When?
Day	Every day
Week	Every Saturday
Month	First Saturday every month
Quarter	First Saturday every quarter
Twice Yearly	First Saturday of Q1 and Q3

Cases set to Ongoing Screening, regardless of the screening frequency established, will always screen against the OGS Delta using the Ongoing Screening settings. The OGS Delta refers to all new records added or existing records updated since the case last-screened date.



Next Scheduled indicates the programmed date of the next OGS screening based on the group settings.

NOTE: If a record has been updated multiple times since it was last screened, scheduled ogs will pick up the highest update category. For example, if a record had a C1 update followed by a C4 since the last screen date, then you will still receive an update alert even if you exclude C4 updates.

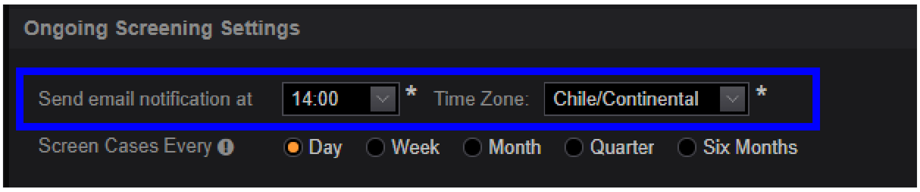
OGS email notification schedule

On the same page, you will find the **OGS email notification** schedule. If you have **Ongoing Screening (OGS)** turned **ON** and would like to receive notifications of any changes to the cases marked for OGS, you can set up the email notification time here.

Select your **time zone** and choose the time you would like to receive emails.

The OGS notification email will indicate the total number of cases per screening Group that had new or updated matches flagged during the latest OGS screening up to the point of the email notification time established for your screening group.

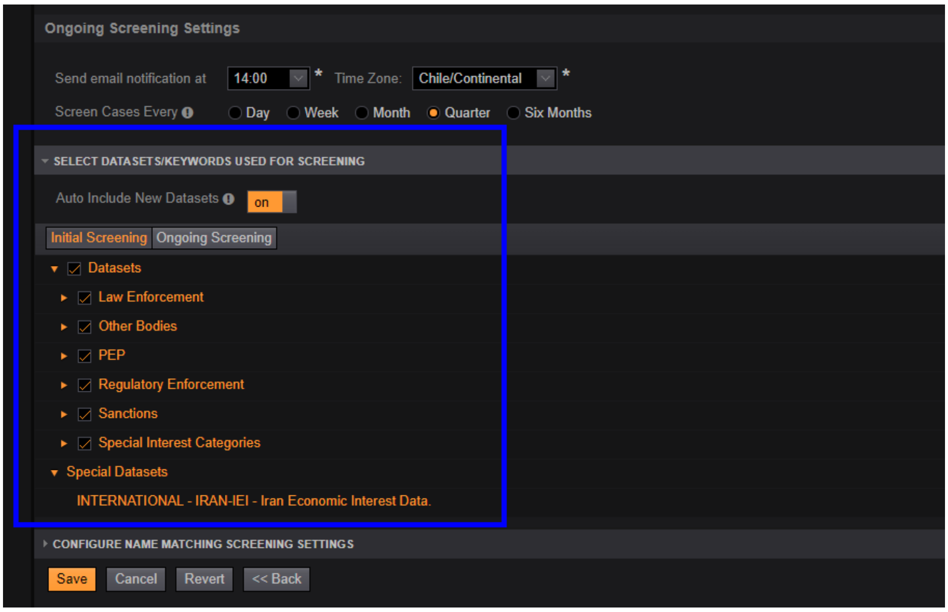
If OGS cases are assigned to specific users, only those users will receive the OGS email alert associated with their assigned cases. For unassigned cases, all users in the screening group will receive a copy of the OGS email notification.



NOTE: Set your email notification **TIME ZONE** to your local time zone to take advantage of ongoing screening efficiency features.

Select Datasets for Screening

Expand this section to enable/disable **Auto-Include New Datasets** and **configure the Dataset selections** for Initial and Ongoing Screening.



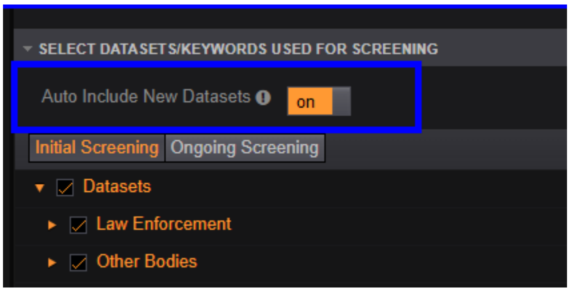
Auto-Include New Datasets

World-Check monitors hundreds of **Sanctions**, **Regulatory** and **Law Enforcement** lists, which are detailed under the Sources section. Datasets also include **PEP** (Politically Exposed Persons), **Other Bodies** and **Special Interest Categories.**

When to turn on Auto Include New Datasets feature

On occasion, the World-Check Research team will add in a new source/list for coverage.

Turn ON Auto-Include New Datasets if you would like any new sources to be automatically included in your screening results. **Turn Auto-Include New Datasets OFF** if you only want to screen selected lists or datasets.



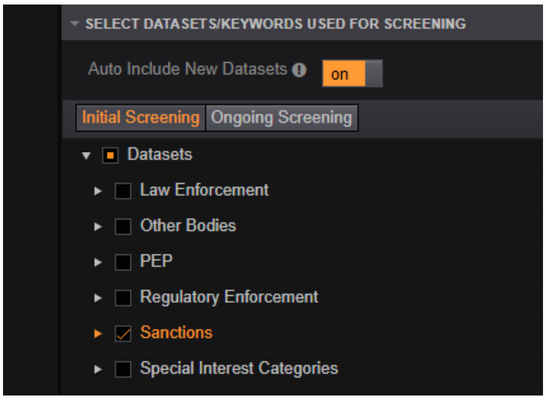
If Auto-Include New Datasets is ON and the relevant source type is selected

Any new data subset/keyword related to the selected dataset(s) will be automatically added to the list your entries are screened against.

Example

In the below example, only the dataset **Sanctions** is selected.

Any new data subset/keyword related to **Sanction** will automatically be added to the list your entry is screened against.



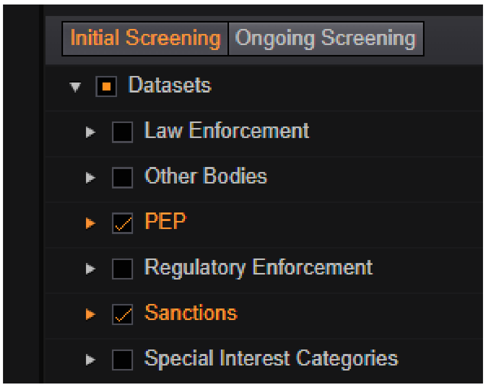
If Auto-Include New Datasets is ON and a specific dataset is not selected

Any new data subset/keyword **unrelated** to the **selected dataset** will **not** be automatically added to the list that your entries are screened against.

Example

In the below example, only **Sanctions** and **PEP** source types are selected.

The new data subset/keyword is related to **Regulatory Enforcement**. It will **not** automatically be added to the list that your entries are screened against as it is not a selected source type.

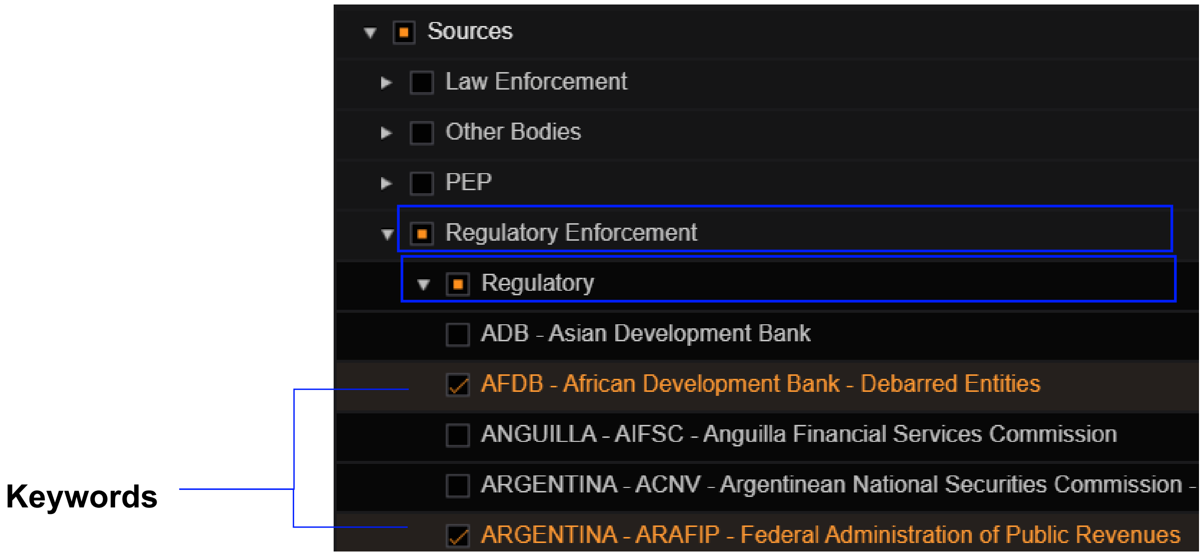


If Auto-Include New Datasets is ON and only some data subsets/keywords are selected from the overall dataset.

If a dataset is selected, but only **some** of the data-subsets/keywords are selected for screening from within that dataset, then any new data-subsets/keywords related to the selected/partially selected datasets will be added for screening.

Example

In the below example, only **some** of the **data subsets/keywords** under the source type, **Regulatory Enforcement**, are selected. When a new Regulatory Enforcement **data subsets/keywords** is added, it will automatically be added to the screening list.



For Client Administrators

The option to **Auto-Include data-sources** is **ON** by default and is set by LSEG Administrators according to your **client subscription** details.

For Group Administrators

The option to **Auto-Include data-sources** would have been set by your **Client Administrator**, but you can change it as appropriate for your group.

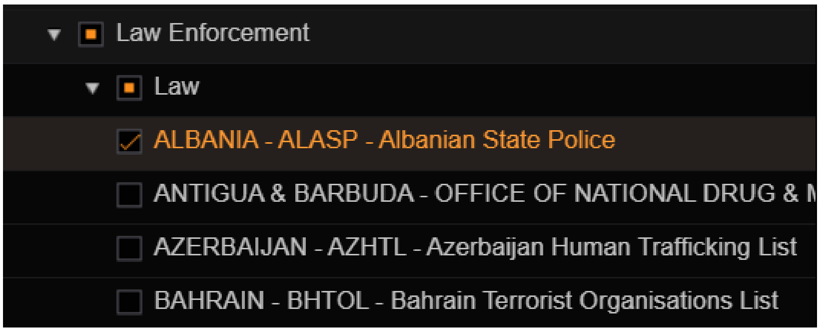
Selecting Datasets for Screening

World-Check records are categorized into one or more of the following datasets: **Law Enforcement, Other Bodies, PEP, Regulatory Enforcement, Sanctions** and **Special Interest Categories.**

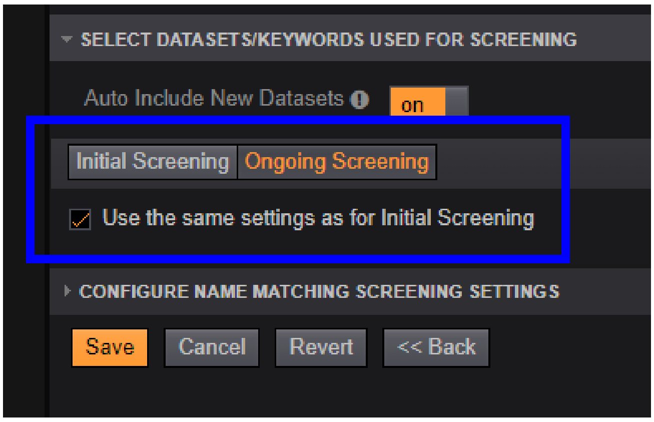
You can choose to select/unselect an entire dataset (i.e. Regulatory Enforcement) from your screening options or drill-down and select/unselect specific data subsets/keywords from within the dataset. For example, select only the **OFAC list** within **Sanctions**.

Example

In the below example, the dataset **Law Enforcement** has been selected for screening. Within this dataset, World-Check monitors the **Albanian State Police list** (World-Check tags this under the data subset/keyword **ALBANIA-ALASP)**.



Dataset selection can be defined for both **Initial** and **Ongoing Screening.** Although recommended best practice for Ongoing Screening configuration would be to "**Use the same settings as for Initial Screening**", it is possible to define a different set of datasets for Initial and Ongoing Screening.



Available Datasets

The below section takes you through the various datasets available to you on World-Check One.

Law Enforcement

This covers Law Enforcement lists and sources monitored and **keyworded** by the Word-Check Research Team (i,e, Interpol). Any World-Check record tagged as **Law Enforcement** would indicate an individual or entity is listed on an official law enforcement public domain site as having met any of the below criteria:

- **Investigated**
- **Charged**
- **Prosecuted**
- **Convicted** or sentenced for a predicate offence
- Individuals **wanted or arrested** by an official law enforcement body such as the police, prosecuting authorities, or criminal courts.

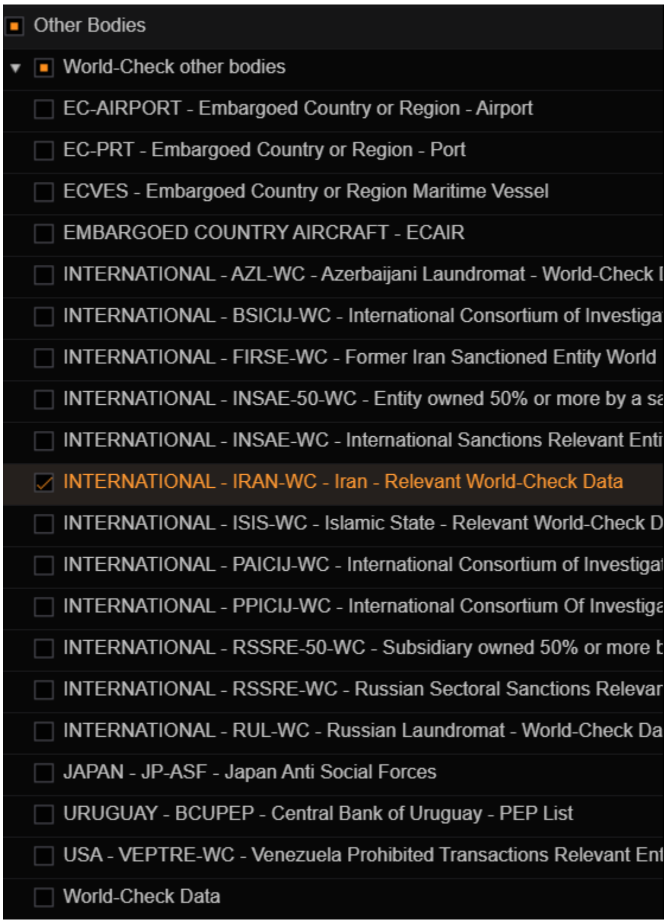
Other Bodies

- **Miscellaneous lists** that are monitored and keyworded by World-Check, such as **JP-ASF: Japan Anti-Social Forces** and which cannot be classified under the **Sanctions**, **Law Enforcement** and **Regulatory Enforcement** datasets.

- **Specific record subsets** keyworded (tagged) by the World-Check Research Team, such as **IRAN-WC: Iran Relevant** World-Check Data.

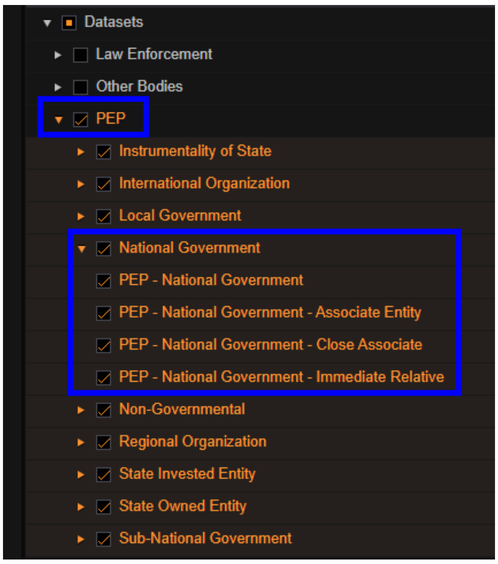
- **Specific record subsets** associated with **Implicit Sanctions** that have been researched and identified by the World-Check Research team, such as **RSSRE-50-WC – Subsidiary owned 50% or more by an OFAC listed Russian Sectoral Sanctioned company**. Records associated with these subsets have been identified through World-Check research as meeting the criteria for implicit sanctions but have not been explicitly identified on official sanctions lists.

- **World-Check Data** is a data subset which contains all records that are not Keyworded or categorized as PEPS but which otherwise fit the inclusion criteria for World-Check. These are typically records covering adverse national/international news media or other non-keyworded sources.



Politically Exposed Persons (PEP)

The World-Check Research team also creates records for **Politically Exposed Persons** (PEP). Under the PEP dataset users can select/deselect various subcategories of PEP (i.e. **PEP-National Government**) as well as for **State Owned Entities** (SOE) and **State Invested Entities** (SIE). More granular selections can also be made under each subcategory. For example, you can choose to screen for all National Government PEPs or drill down further to select/unselect for the PEP-National Government, Associated Entities, Close Associates or Immediate Relatives.



Regulatory Enforcement

This covers **Regulatory Enforcement** lists and sources monitored and keyworded by the World-Check Research Team **(i.e. SEC: Securities and Exchange Commission).** Any World-Check record tagged as **Regulatory Enforcement** indicates that **official regulatory administrative or civil action** has been taken against the individual or entity by a government or independent regulatory agency responsible for the supervision and oversight of specific administrative rules, codes or regulations for breaches of or non-compliance with said rules, codes or regulations.

Sanctions

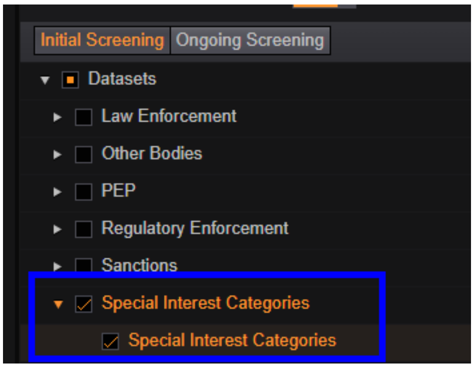
Covers **Sanctions lists**, and sources monitored and keyworded by the World-Check Research Team (i.e. OFAC).

Any World-Check record tagged as **Sanctions** would indicate an individual, entity or group listed on an international, supranational or national sanctions list as subject to restrictive measures, such as:

- an **asset freeze** or block
- an **investment ban**
- restrictions on access to **capital markets**
- to **cease banking** or **business relationships** and activities or related financial sanctions
- **travel bans**, **arms** or **trade embargo**, including counter terrorism sanctions, counter narcotic trafficking sanctions, nuclear proliferation sanctions and country specific sanction programs.

Special Interest Categories

The Special Interest Categories (SICs) are the classification of information obtained from media sources, sanctions or law & regulatory enforcement sources to indicate the nature of alleged or actual offences and/or information relating to the status of explicit & implicit sanctions that may pertain to data subjects in World-Check records. SICs provide more detailed category information concerning the nature of the potential risk associated with existing World-Check records.

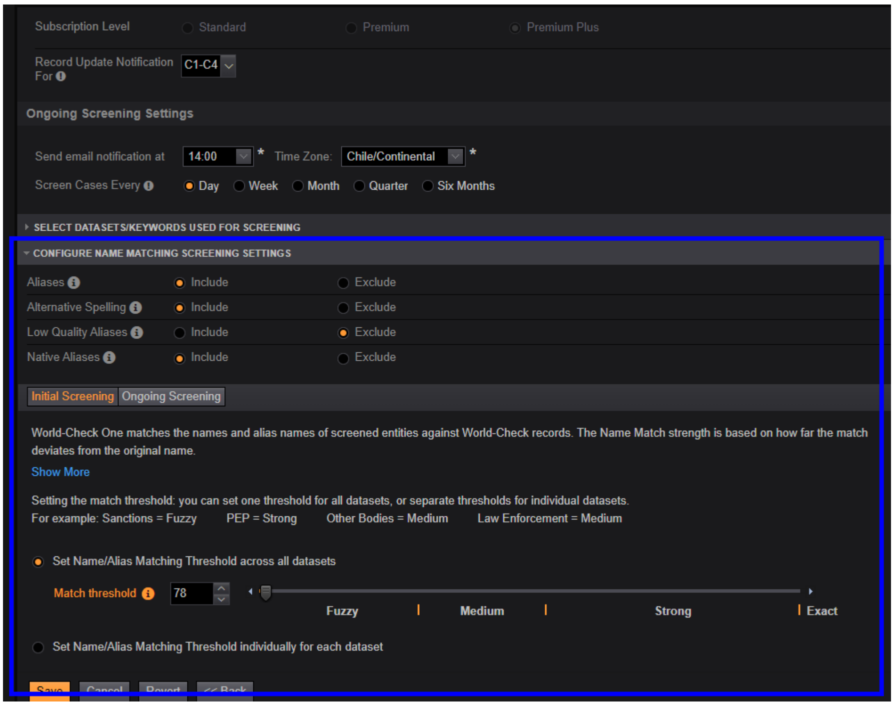


A majority of World-Check records are tagged with SIC, with the exception of a subset of PEP and SOE/SIE records. Currently, users can only select/unselect for the entire Special Interest Categories dataset. However, in future, it will be possible for advanced subscription clients to make more granular selections under the Special Interest Category dataset, for example, selecting for specific SICs such as Fraud, Implicit Sanctions, Human Trafficking, etc.

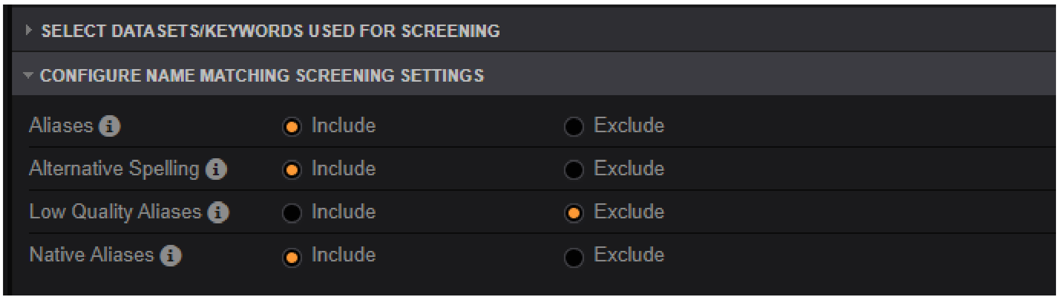
More details on the Special Interest Categories can be found HERE

Configure Name Matching Screening Settings

From the same **World-Check settings** page, you can also edit the default settings to **include** or **exclude: Aliases**, **Alternative Spelling**, **Low Quality Aliases**, and **Native Aliases**.



Use the radio buttons to **include** or **exclude Aliases, Alternative Spellings, Low Quality Aliases** and/or **Native Aliases** from your possible screening matches.



Aliases

When viewing the results returned by Matching Engine from the World-Check screening page, a **Matched Alias** field is included. This feature is designed to **find matches associated with the subject searched**, but where the matched name either **wholly** or **partly differs** from the name searched.

Names that include **alternative spellings**, **foreign characters**, **additional names**, **diminutives** or **company trade names** are all examples of Aliases.

Example

Matched name: Hasan Hussain **Alias name**: Michael Anderson

Alternative Spellings

Include Alias to find matches for names that include **hyphenated spellings**, **diminutives** or where a name normally associated with an individual is being used as a **business** or **trade name**.

Example

Hyphen: Susan Blyde-Smith **Diminutive:** John for Jonathan **Individual name in trade name:** Jones and Jones TM

Native Aliases

Include Native Alias allows you to receive results in the searched name's **original script** or **naming format.** *This feature is only available to **Advanced** (**Premium Plus)** subscription holders.*

When to turn the feature ON

Include Native Alias if you would like to **include results** that match the name searched in **another language** or **format**.

Example

Search for the name **Hong Chen** and **receive results** in **other languages**, **scripts** and **naming formats** e.g. Matching Engine will return 陈红 or Chen Hong**.**

When to turn the feature OFF

The feature will likely not be needed if the name you wish to search meets the following criteria:

- The natural word order of the name is **Given Name**, **Surname**
- The original language of the name is **English**
- You **do not** need seek results that include the name recorded in any other **langauge**, **script** or **word order**

Low Quality Aliases

Include Low Quality Aliases when searching names with irregular naming formats.

When to turn the feature ON

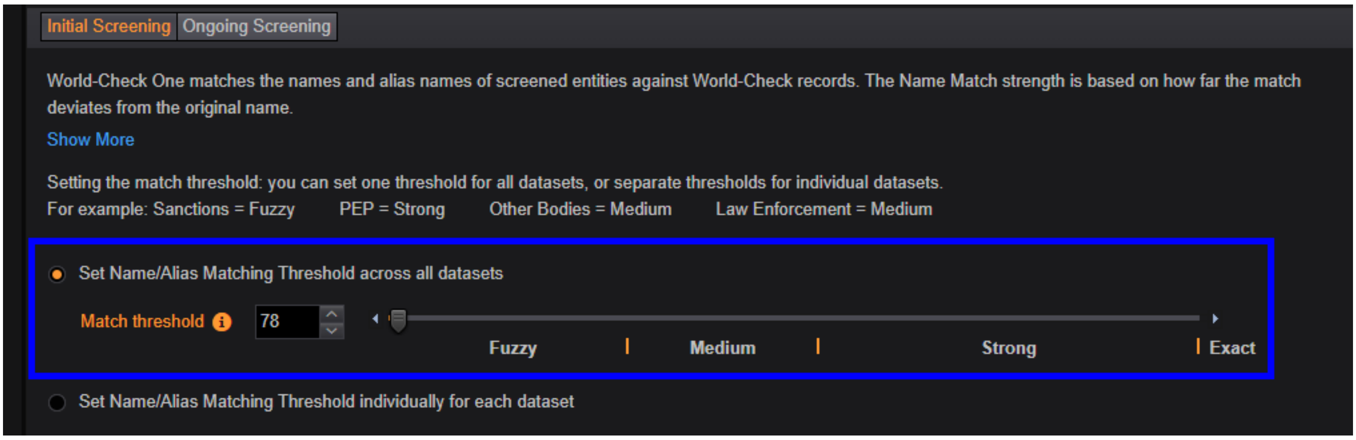
If you wish to **include results** or **search a name** that include **numbers**, **abbreviations** or **nicknames**, **single names** flagged as **low quality** by major sanction lists, or **noms-de-guerres** (e.g. “The Doctor” or “Ahmed the Sudanese”).

Low Quality Aliases	Examples
Numbers	Oleg2
Single Names	JoJo
Noms-de-guerres	The Wolf
Nickname	Jonno

Set Name/Alias Matching Threshold across all datasets

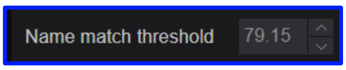
The **Name/Alias Matching Threshold** allows you to control the result set returned by the matching engine (the function that produces and ranks search results for match strength). The name match strength is based on how far the match deviates from the original name screened.

Use the **slider** to adjust the **precision level** of the match recall between the four settings: **Fuzzy**, **Medium**, **Strong**, and **Exact**.



A match threshold set closer to Fuzzy will return a **higher volume** of results a wider range of precision. Do this if you want to capture a wider range of name variations or if you are unsure of the quality of the name details you are screening.

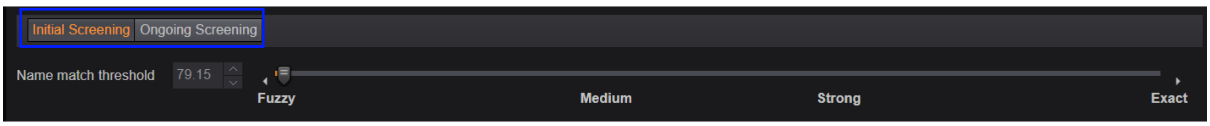
A match threshold set closer to Exact to return fewer, but more precise matches. Do this if you already have a strong idea of the result you are looking for, want fewer results, or are seeking exact matches only.



The Name Match Threshold is also indicated through a score, ranging from **78** (Fuzzy) to **100** (Exact).

Example

In the below example, the slider is set to **Fuzzy**, meaning that all results ranging from **Fuzzy to Exact** will be revealed. If the slider had been moved to **Strong**, then only results ranging from **Strong to Exact** would be revealed.

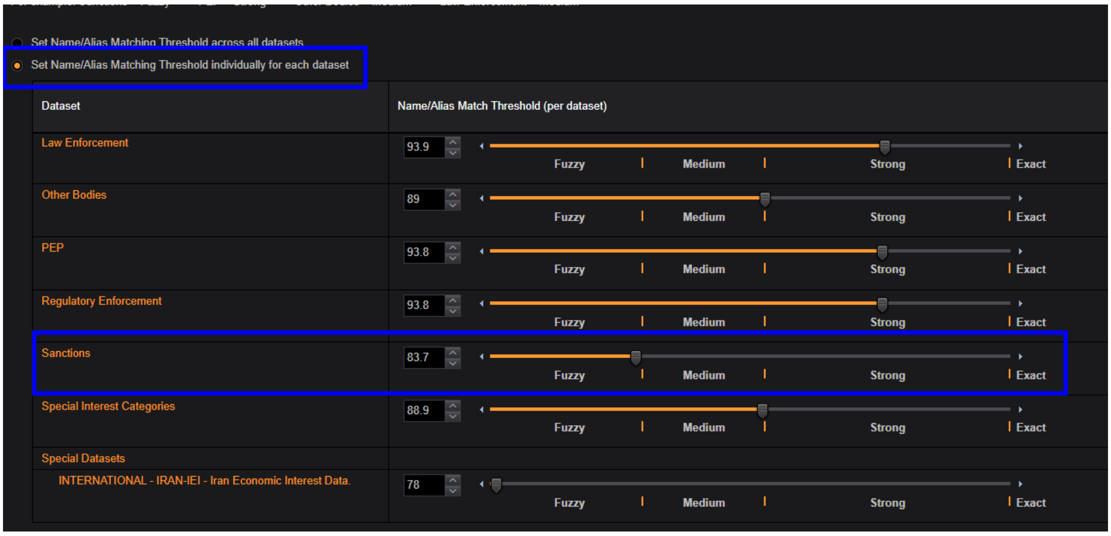


Initial & Ongoing Screening: If you wish to activate **ongoing screening** for batch screens (the process of rescreening previously screened cases at set intervals), then check that the Name Match thresholds for *both* initial and ongoing screening are set to the same threshold. Do this by navigating between the two tabs.

Set Name/Alias Matching Threshold individually for each dataset

A single Name/Alias Matching Threshold can be set for all records screened at the group level or, alternatively, individual Name/Alias Matching thresholds can be set up for each dataset, allowing for a more sophisticated application of a risk-based approach.

Click on the **Set Name/Alias Matching threshold individually for each dataset** option and define the threshold for potential matches associated with each dataset. For example, you may prefer to set a lower threshold for potential Sanctions matches but feel comfortable with a higher threshold for matches associated with other datasets.



NOTE: if a potential match is associated with more than one dataset, the lowest match threshold will apply.

For Client Administrators

You can edit the default **Name/Alias Matching Threshold** for your Primary Group, which will override the default setting.

For Group Administrators

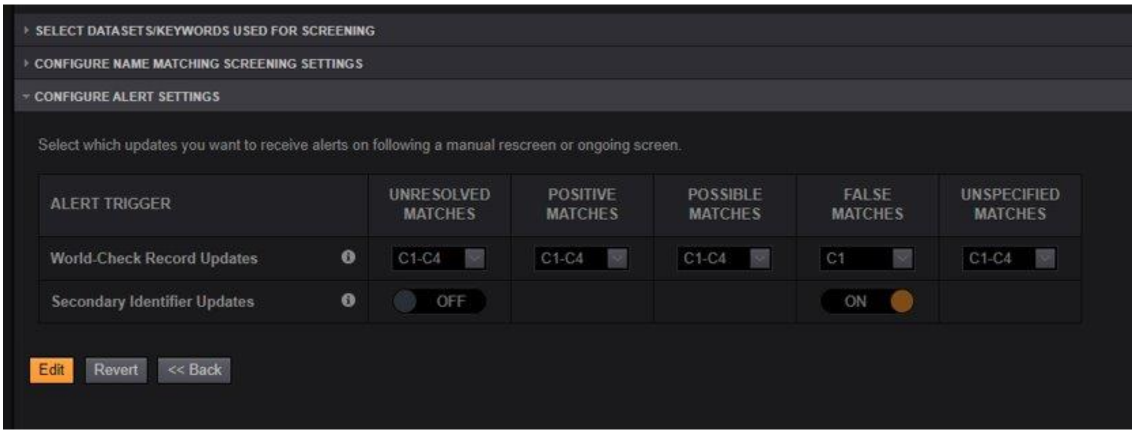
You can edit the default **Name/Alias Matching Threshold** for your appropriate **Group(s)**. This will override the initial settings inherited from your **Parent Group**. Your **Client Administrator** may have adjusted the settings according to what is appropriate for your organization.

Configure Alert Settings

Configure you alert ‘trigger’ settings to align with your organization’s risk appetite and screening requirements, minimizing unnecessary alerts via ongoing screening or manual rescreens.

World-Check Record Updates: Indicate which Update Category(ies) you wish to be alerted to via Ongoing Screening or after manual rescreens for the corresponding Resolution Status (i.e. Unresolved, Positive, Possible. False, Unspecified). Refer to the Update Category Reference Guide for details on the updates that correspond to each Update Category (C1 = Most Critical to C4 = Least Critical)

Secondary Identifier Updates: Indicate if you want to receive alerts on existing Unresolved or False matches due to a secondary ID match following changes made to your case data, such as updates to DOB, Citizenship, Registered Country, etc.)



Revert Group Settings

If you wish to **revert** any settings made to a **sub-group** back to the settings of the **Primary Group**, click **Revert**.

NOTE: Doing this will relink the sub-group and Primary Group back together so that all future changes to the Primary Group settings will automatically apply to the sub-group.

OPTIONAL SETTINGS

The following settings are optional and can be configured at your discretion.

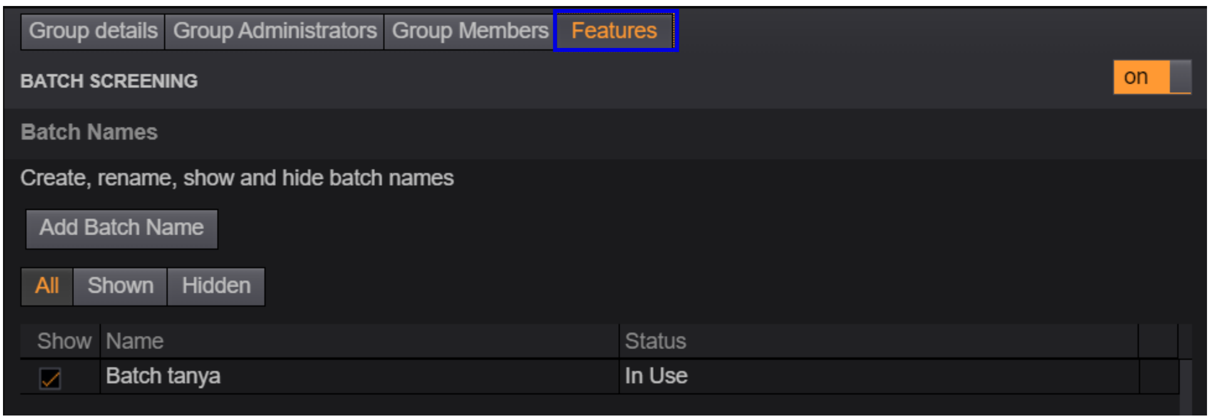
BATCH SCREENING

Batch Screening provides the ability to screen a group of records in one go. This feature is designed to save you time if you have numerous entities that need to be checked.

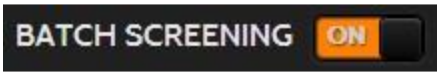
You can check if Batch Screening has been included in your subscription by going to the **Features** section of the Client Summary page. See the Client Summary Page above for more information on this page.

1. Navigate to the **Features** tab from any **Group** summary page within the **Admin** page. The **Batch Screening** settings will be displayed:

Group Summary page:

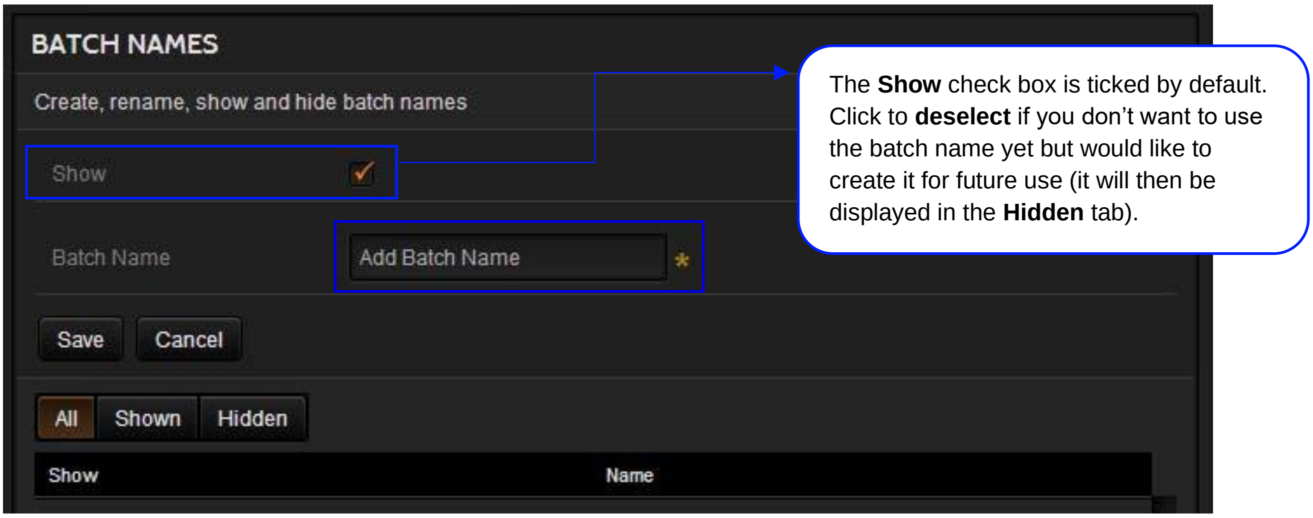


2. Use the toggle to turn batch screening **ON / OFF** according to your needs.



3. Once you have turned Batch Screening **ON**, you will need to add Batch Names. Click **Add Batch Names** to display the **Batch Names** section:

Batch Name section:



4. Enter a **Batch Name**. It may be beneficial to assign a Batch name according to the type of search being conducted. For example, label the Batch **Credit Cards**, **Retail**, **Brokerage**, etc.

5. Click **Save** to save the batch name (you can add more batch names depending on your requirements).

6. The following message will be displayed:

Delete a Batch Name

You can **delete a Batch Name** if you no longer require it. Navigate to the **Features** tab within the **Group Admin page** (ensure that you are in the correct group otherwise the Batch Name will not appear).

NOTE: NO cases should exist within the Batch Name. If there are existing cases, you will **not** be able to delete the Batch Name

CUSTOM FIELDS

Create any **custom fields** you would like to be included in your screening results.

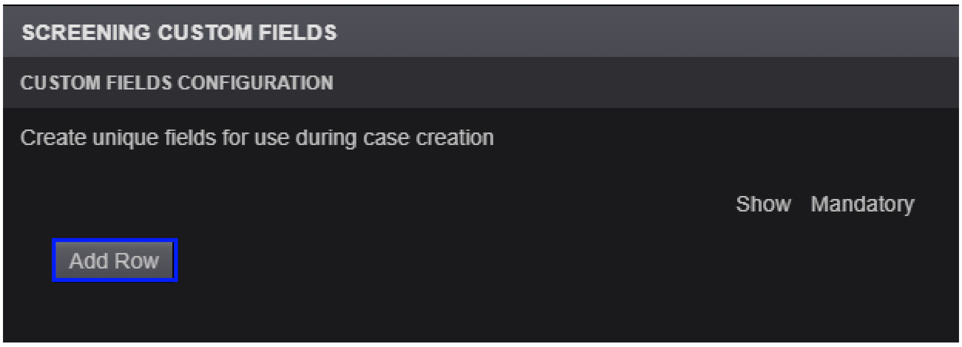
NOTE: Custom fields are **informative fields only;** they capture general information about the case, but **do not affect** the screening results. Follow the below instructions to navigate to the Custom Fields page.

1. Go to **Admin** section and navigate to the **Screening Custom Fields** section on the Summary page. Note that access to the Summary page is exclusive to **Client Admins** and only Client Admins can create/edit custom field names.

2. Click **EDIT** next to Screening Custom Fields.

Default Settings

By default, **no** custom fields will show. Click **Add Row** to begin creating **Custom Fields**.



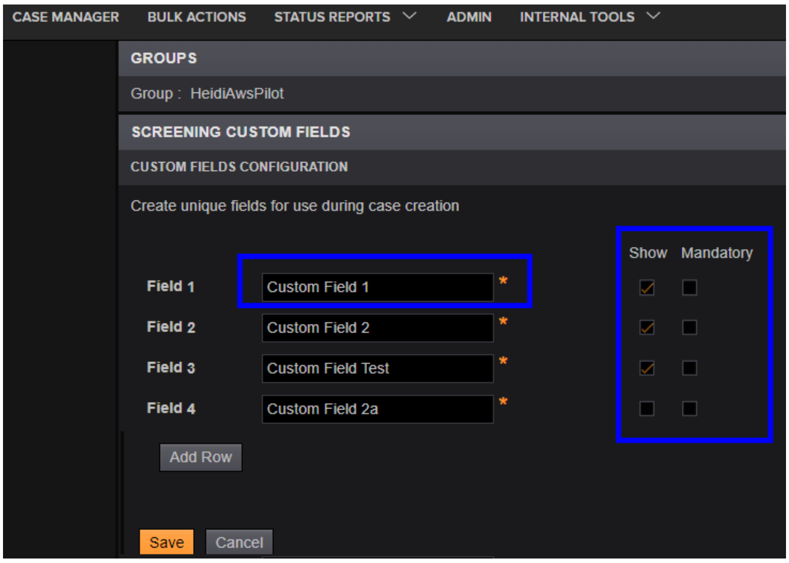
Insert Field Names

Create names for the various Fields you customise.

Show Custom Fields/ Mandatory Fields

Click **Show** to make the fields **visible** in on the relevant group screening page and in your screening results. and select **Mandatory** to make fields **compulsory search factors.**

NOTE: if you choose to make a custom field mandatory, you will **not** be able to leave these fields blank when creating your **Batch Screening template** or when running ad-hoc searches.



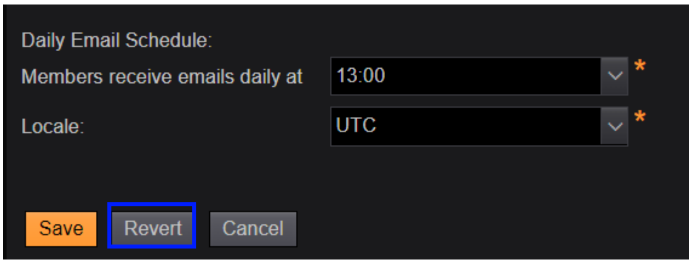
Client Admins administer the creation / edition of the 'Master' list of available custom fields. However, Group Amins can show/hide any of the available Custom Fields on their respective screening subgroups.

Custom fields cannot be deleted; however, they can be hidden or renamed.

Revert Custom Settings

If you wish to **revert** any settings made to a **sub-group** back to the settings of the **Primary Group**, click **Revert**.

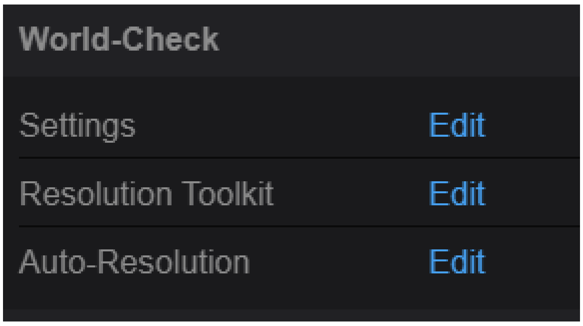
NOTE: Doing this will relink the sub-group and Primary Group back together so that all future changes to the Primary Group settings will automatically apply to the sub-group.



RESOLUTION TOOLKIT CONFIGURATION

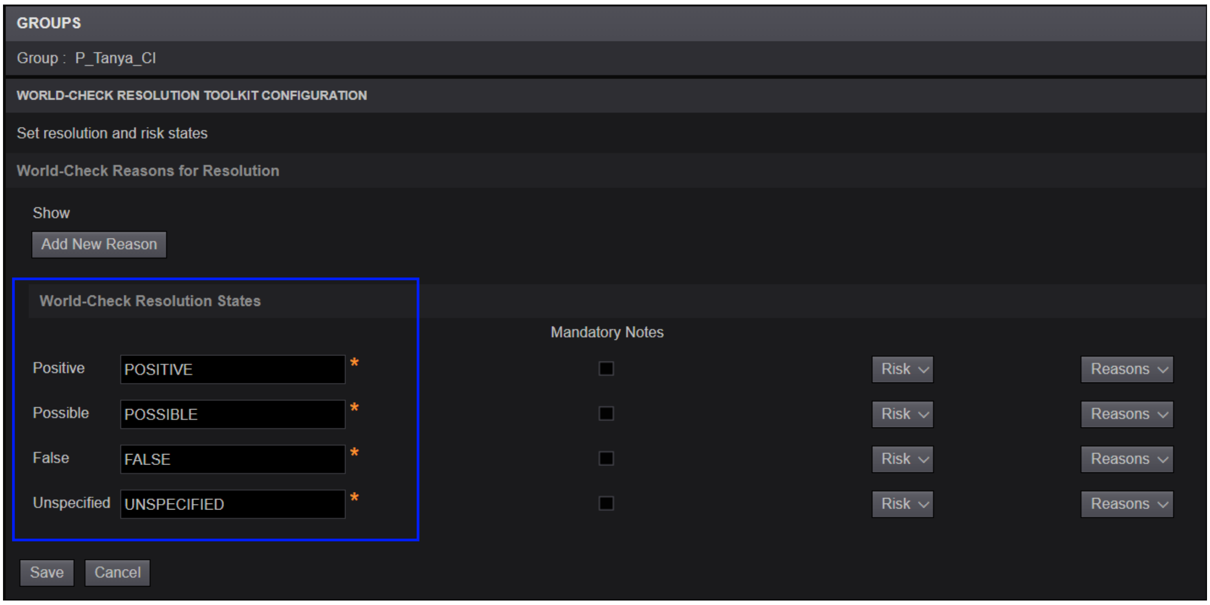
The **Resolution Toolkit Configuration** provides a default set of **Resolution States**, **Risks**, and **Reasons** used for resolving potential matches generated via the screening process. Follow the instructions below to navigate to the correct page:

1. Navigate to the **Admin** from the dropdown menu at the top of the page.
2. Click **Groups** on the left-hand side menu and **select the relevant group**.
3. Navigate to the **Group Details** tab. Scroll to the **World-Check section** and click **Edit** next to **Resolution Toolkit.**



Resolution States

Once on the **Resolution Toolkit Configuration** page, you will be able to edit the default **Resolution States** and label them as preferred. For example, **positive** can be labelled to **full match**, **possible** to **partial match**, **false** to **no match**, and **unspecified** to **unknown**.



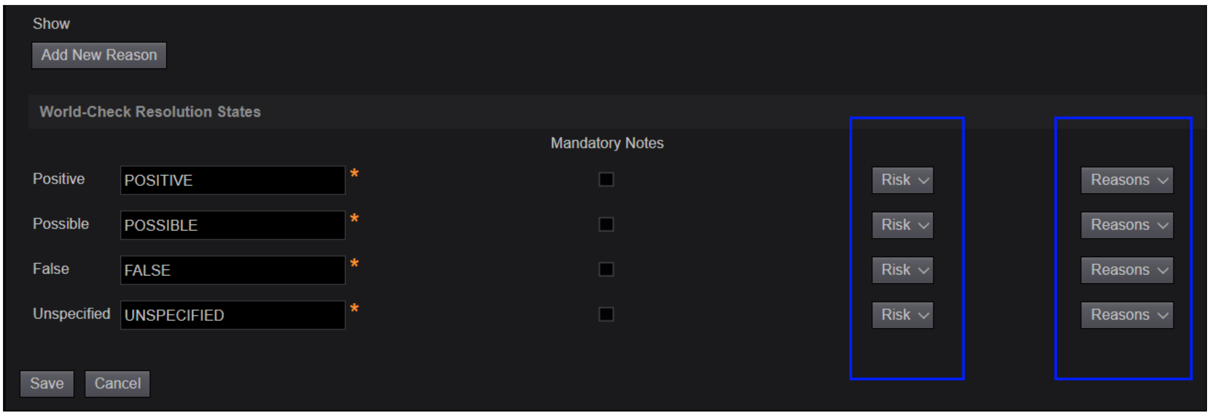
Risk Types

You can select risk levels for each resolution status. For example, assign **positive, possible,** and **false** resolution states as **positive matches** under the risk level, and for unspecified resolution states, assign only the **unknown risk category**.

Reasons

Assign reasons to each resolution state and risk level so that decision makers can better explain the actions taken. To do this, select **Add New Reason**, then fill in the field name.

Group Admin page > Features > Resolution Toolkit:



AUTO-RESOLUTION SETTINGS

When screening an Individual, Organization or Vessel, users have the option to include **secondary identifiers** such as:

Date of Birth, **Nationality**, **Country Location**, **Gender**, **Place of Birth**, **Registered Country** or **IMO number**.

What does the Auto-resolution setting do?

Possible name matches will be **auto-resolved as false** or **removed from the results** if *one* of the **secondary identifiers** entered for screening **does not match** those on the World-Check record. The exception to this logic would be where the **auto-resolution overrides** are applied for matches with an exact Identification number or exact Date of Birth.

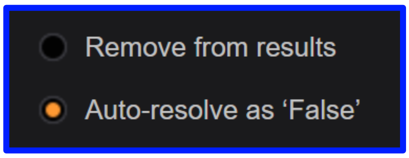
Configure Your Auto-Resolution Settings

Authorised users can set specific rules for the system to follow to **auto-resolve false positives**.

Likewise, authorised users may choose to activate different auto-resolution options for varying secondary identifiers between sources (i.e. a user could activate auto-resolution for **Nationality** under **PEP** matches but **not** for **Sanctions** matches).

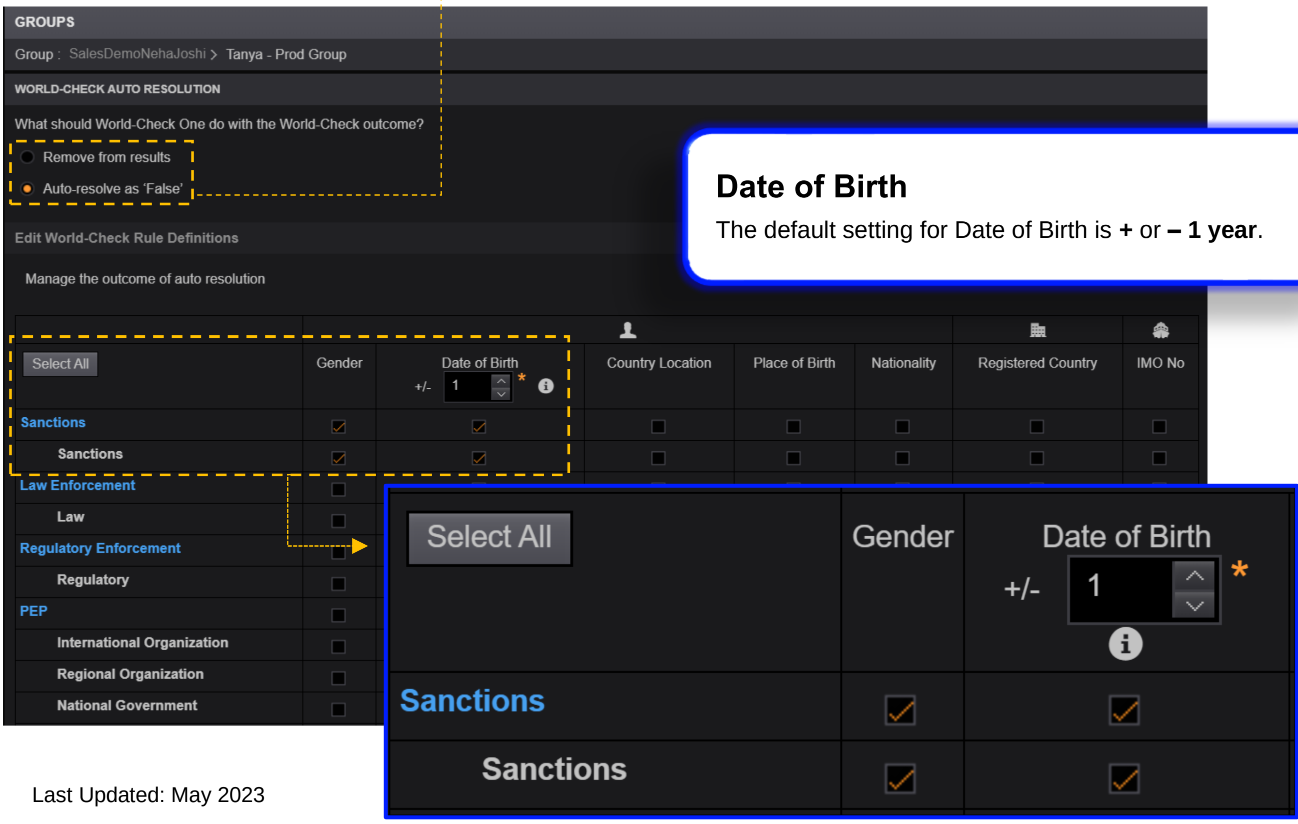
Example

In this example, any **Sanctions** results that list a different g**ender** to that searched- or a will be auto-resolved as **FALSE**, as will any **World-Check Other Bodies** results listing a **Place of Birth** different to that searched.



By default, **ALL** secondary identifiers will be searched against, and **ALL** results will auto-resolve as **FALSE.**

Select **Remove from results** if you do **not** want to see results with secondary identifiers that do not match those entered. E.g. you will **not** see a result where the **name matches** that searched but the **date of birth** is incorrect.

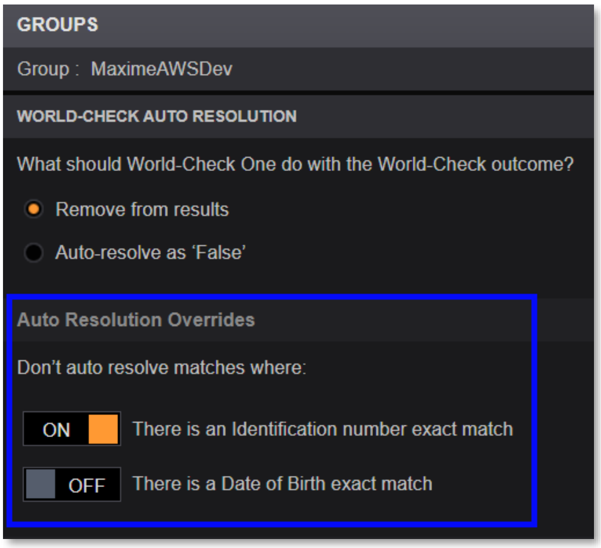


Date of Birth

The default setting for Date of Birth is **+** or **– 1 year**.

How does the Auto-Resolution Overrides option work?

When the override is enabled, matched records that would normally be marked as False due to non-matching secondary identifiers will remain Unresolved if the Identification Number or Date of Birth exactly matches the screened case.



A **Date of Birth Exact match** within the context of the auto-resolution override is determined by the level of detail of the screened DOB:

- If the screened DOB is entered as 1/Jan/2000, the override will only apply to matches with a DOB of 1/Jan/2000.
- If the screened DOB is entered as Jan/2000, the override will only apply to matches with a DOB of xx/Jan/2000.
- If the screened DOB is entered as 2000, the override will only apply to matches with a DOB of xx/xxx/2000.

In each case, the lowest common denominator of the screened DOB is used to determine the exactness of the match.

Here is an example of how the override feature can change the outcome of a match:

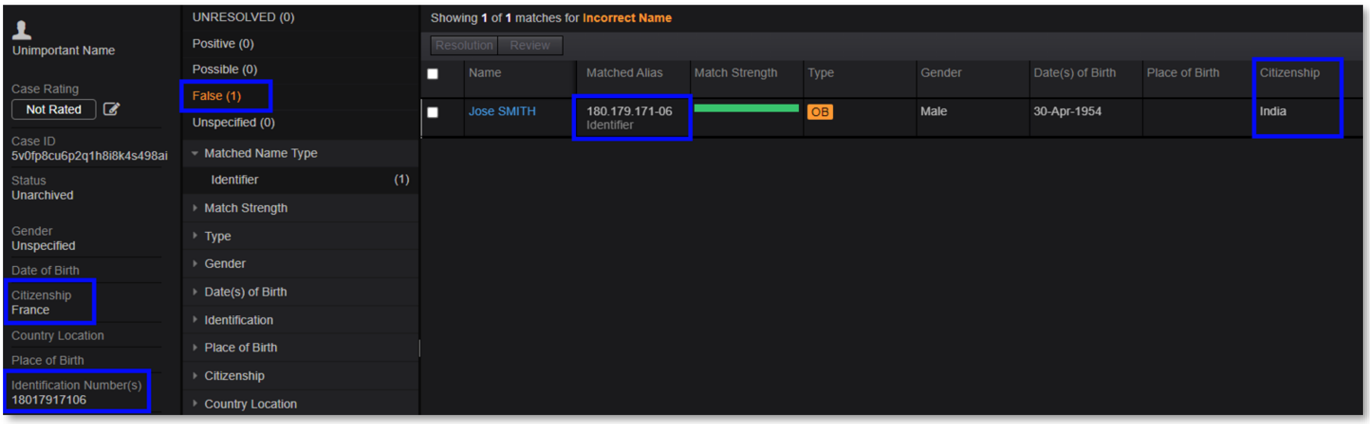
Without the override: False match

With the override: Unresolved match

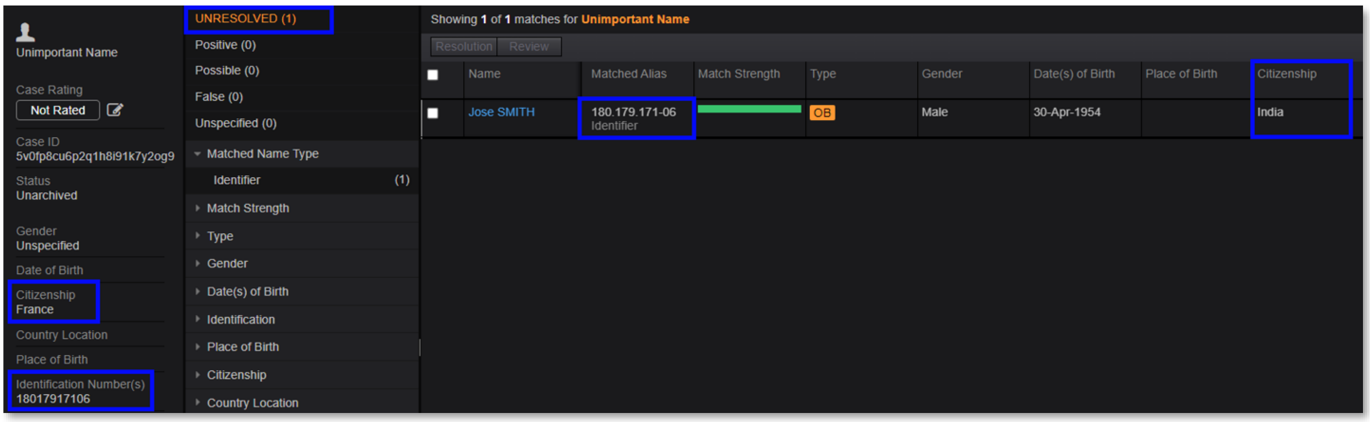
An **Identification number exact match** will be returned **when an exact or near-exact Identification number is found** on a World-Check record, **regardless of the screened name and Match thresholds**. Near-exact ID matches occur when a matching Identification number is found after normalization, which is the process of removing special characters, accents, case differences, and white spaces. Special characters are quotes, slashes, hyphens, periods, commas, underscores, and brackets.

Here is an example of how the override feature can change the outcome of a match:

Without the override: False match



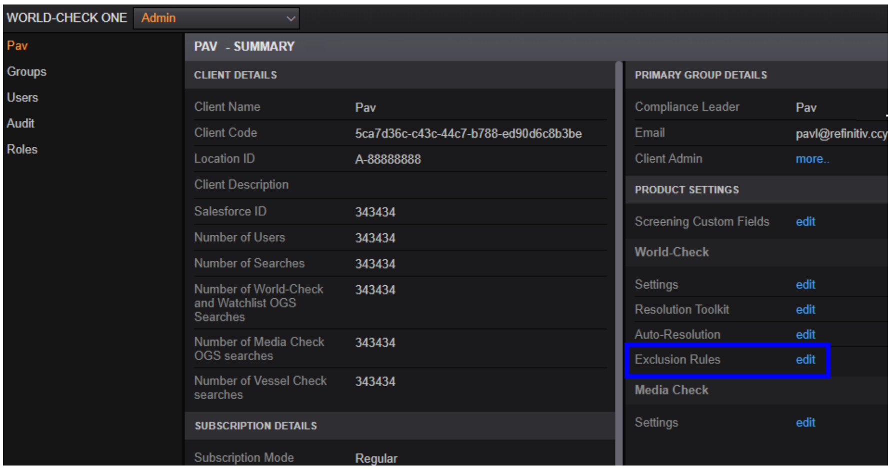
With the override: Unresolved match



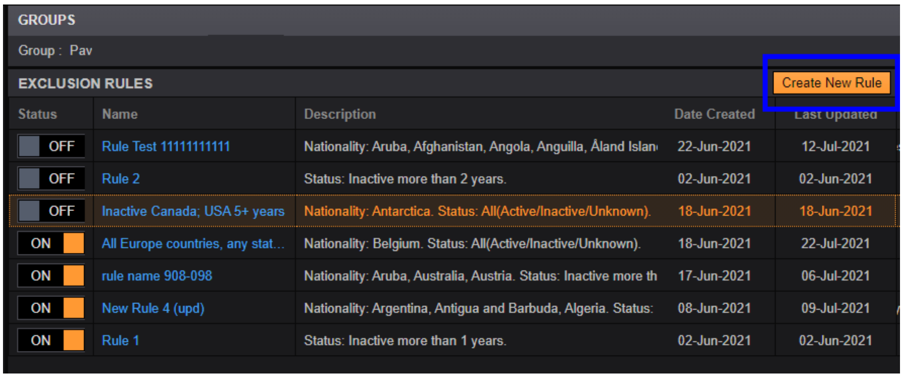
(PEP) EXCLUSION RULES

PEP Exclusion Rules allows users to build rules to exclude PEPs on the basis of Citizenship/Nationality, PEP Sub-Category and overall Standardized Position, PEP Status (Active, Inactive, Unknown) and Period of Inactivity (e.g. inactive more than 5 years).

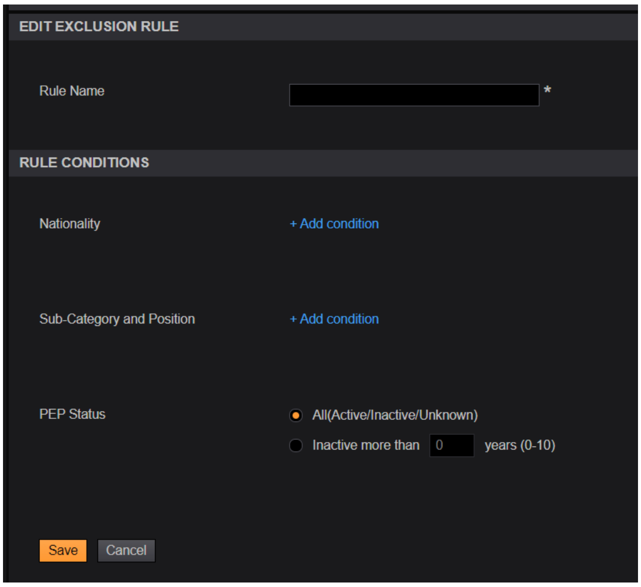
Client Admins can access the **Exclusion Rules** builder from the **Admin** section **Summary** or **Groups** page:



Click on **Edit** and **Create New Rule**



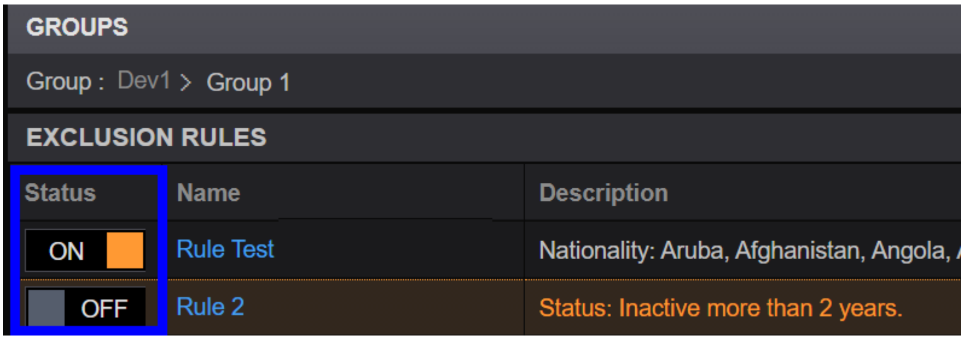
1) Add a **RULE NAME**
2) Select the **CITIZENSHIP(S)/NATIONALITY(IES)** to be excluded (if relevant)
3) Select the **SUB-CATEGORIES** and/or associated **POSITIONS** to be excluded.
4) Indicate whether you wish to exclude based on **PEP STATUS** for the conditions previously selected. You can select **ALL** or only those with Status I**NACTIVE**. If you select Inactive, you can also indicate how long the PEPs should be inactive before excluding.
5) Click on **SAVE** to create the new exclusion rule



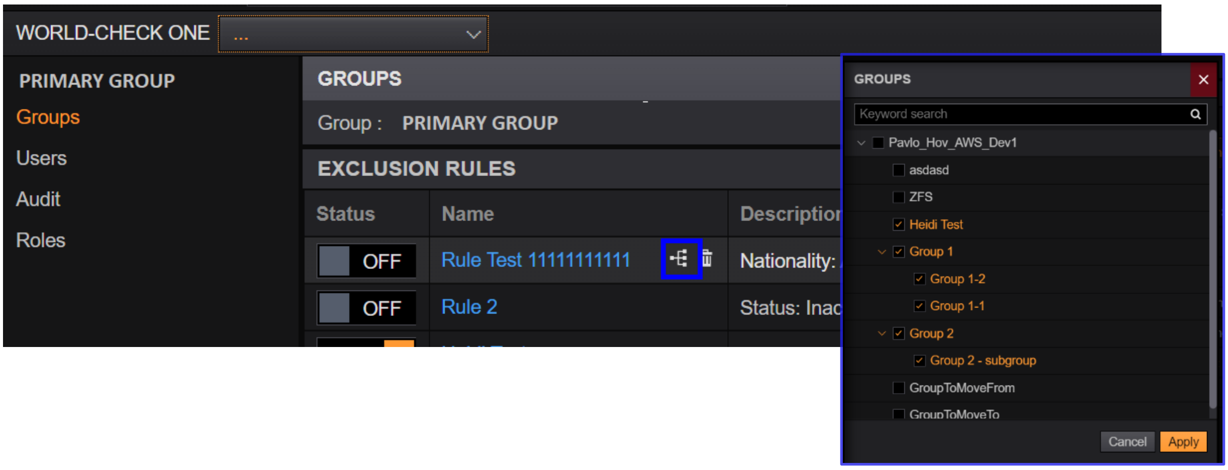
Within a Rule all conditions are based on the & (and) logic. For example, if the rule contains **Nationality/Citizenship:** Canada, **Sub-Category:** PEP-L and **Position:** Candidate, and **PEP Status**: Inactive more than 1 year, you will be excluding all PEPs with Sub-Category PEP Local Government and Position Candidate whose Citizenship is Canada and who have been Inactive for more than 1 year.

Client Admins and Group Admins can activate or deactivate an exclusion rule for a group by toggling the **Status** button next to the rule name to **ON** or **Off.**

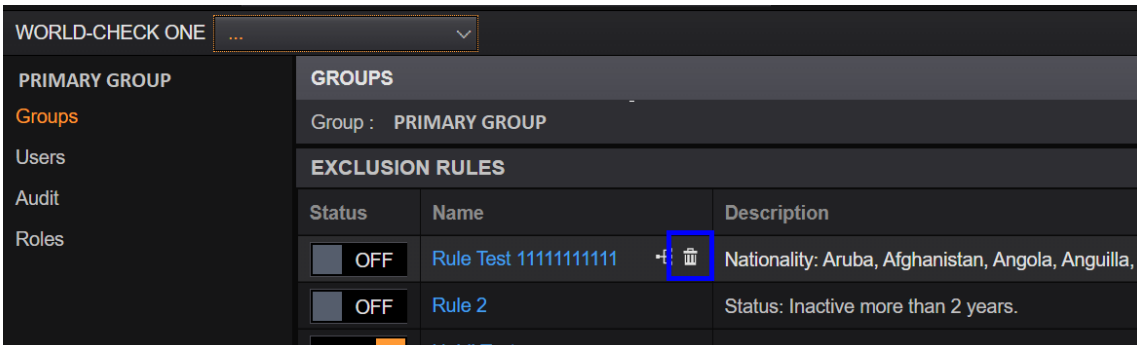
Note: Activating a rule on a Parent group will also activate the rule for any subgroups inheriting exclusion rules. However, once exclusion rules are updated directly on a subgroup, the inheritance link will be broken and any changes to rule status on the parent group level will not affect the subgroup rule status.



Client Admins can use the icon on the Exclusion Rules section on the Primary Group to enable or disable Exclusion Rules from multiple groups at one time.



Client Admins can delete an exclusion rule from the Exclusion Rules section on the Primary Group.



Note: A rule must be disabled from all screening groups before it can be deleted.

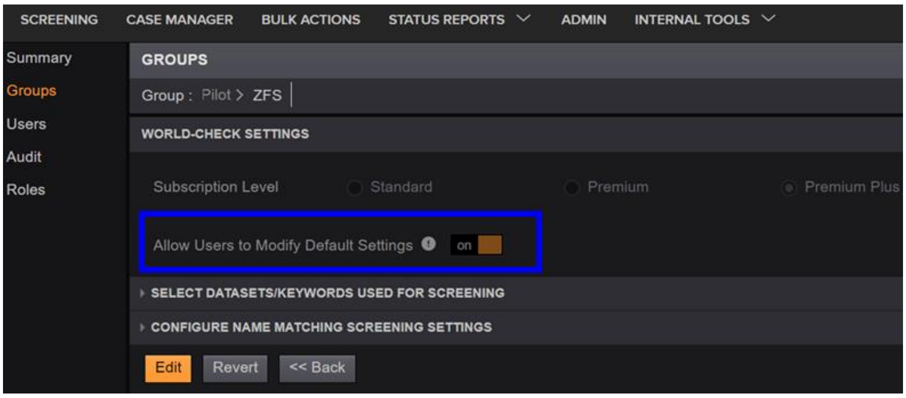
See the PEP EXCLUSION RULES FAQ for more details on Rules creation, PEP Inactivity calculation, etc.

Zero Footprint Screening (ZFS) settings

Zero Footprint Screening (ZFS) group configuration includes many of the same options available to Case Manager & Audit (CMA) groups, with the exception of settings related to Ongoing Screening and Resolution Toolkit. Additionally ZFS group set-up includes some unique features.

Allow Users to Modify Default Settings

Enabling this option (ON) allows users to modify the dataset / keyword selection on a screen-by-screen basis from the ZFS screening page. Disabling (OFF) will ensure the default group settings for datasets / keywords are applied for each screen.



For more information

Read more about our **products** at https://www.refinitiv.com/en/products
For **general support** and to raise a support ticket, go to https://my.refinitiv.com/content/mytr/en/policies/help-and-support.html
For **general sales support**, fill out the form here: https://my.refinitiv.com/content/mytr/en/contactsales.html