Oracle ® Watchlist Screening

Oracle Watchlist Screening Implementation Guide

Version 12.2.1

September 2016

Table of Contents

Chapter 1: Introduction

This document details the steps required to install Oracle Watchlist Screening and to configure it to your requirements.

These instructions assume the reader has a good understanding of OEDQ and knowledge of Sanctions, PEP and EDD screening requirements.

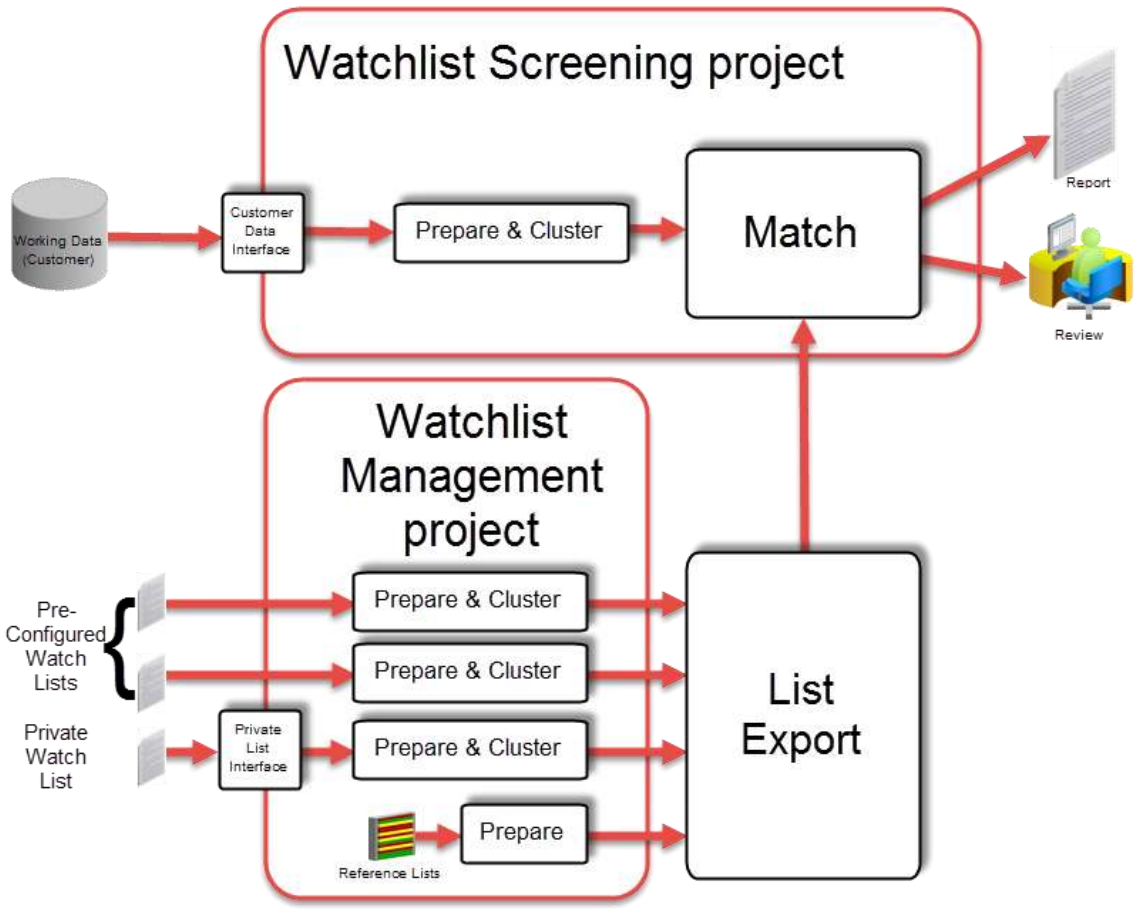
Oracle Watchlist Screening consists of:

- Two OEDQ projects: one for managing watch list data and the other for screening working data;
- A **config.zip** file containing a number of components that must be installed alongside and in some cases over existing OEDQ components;
- A user application for performing real-time screening and reviewing potential matches identified by the screening processes.

The case source and workflows supplied with Oracle Watchlist Screening can be extended, customized and duplicated to match your screening requirements. In addition, multiple, customized copies of the screening project itself can be installed on the same OEDQ server.

1.1 Architecture Overview

The diagram below gives a high level overview of the Oracle Watchlist Screening architecture:



Chapter 2: Installation

The solution uses custom widgets (pre-configured processors), gadgets (match extensions), selection functions and database connectors to extend the functionality of OEDQ. These components are collectively referred to as *extensions*, and are provided as Java Archive (JAR) files. Also, a set of online help files and a customized version of the Case Management extended attributes file (**flags.xml**) are provided as part of Oracle Watchlist Screening.

2.1 Installing the Oracle Watchlist Screening Components

The Oracle Watchlist Screening distribution contains a **config.zip** file. This file must be extracted over your OEDQ instance's local **config** folder in order to install new folders and extensions required for Oracle Watchlist Screening to function.

The OEDQ Config Folder:
Your OEDQ instance's **config** folder might not be named 'config'. The choice of the config folder's name is made when OEDQ is installed - in some cases a name is automatically allocated. OEDQ release 11g and later has both a 'base' and a 'local' config folder. The base config folder is often called '**oedqhome**', and the local config folder is often called '**oedqlocalhome**'. In some cases, dots or underscores may be inserted into these names (for example: 'oedq_local_home'). You need to unzip the **config.zip** file over your OEDQ instance's local config folder. Whenever you see a file path in this document that begins with **config**, this always refers to your OEDQ instance's **local** config folder.

Note:

- If the OEDQ server uses a different landing area path from that set during installation (i.e. config/landingarea), the landingarea folder created when the config.zip is extracted must be copied over the existing landingarea folder.
- If the **flags.xml** file in the **config/casemanagement** folder of the OEDQ distribution has been customized, you can preserve the changes made by copying the local file to a folder outside the config folder first. After completing the steps detailed in Import Case Source and Workflows below, add new attributes in the new **flags.xml** file to the customized file. Then copy the customized file back into the **config/casemanagement** folder, overwriting the new file).

When the **config.zip** file has been extracted, stop and re-start the OEDQ Application Server service before proceeding to the next installation stage.

2.2 Import Oracle Watchlist Screening Case Source and Workflows

This section describes the steps required to install the Case Management configuration in Oracle Watchlist Screening.

The next steps require the use of the Case Management Administration tool, which you should be able to access from the OEDQ Launchpad. If it is not visible, follow the steps described in 2.4.2 : Publish Applications to the Launchpad.

1. Use the Case Management Administration Case Source Administration tool to import the following from the **casesources** folder in the Oracle Watchlist Screening distribution.
   - sentry-case-source.dxic
2. Use the Case Management Administration Workflow Administration tool to import the case workflow and one of the two available alert workflows from the **casesources** folder in the Oracle Watchlist Screening distribution. These are:
   - sentry-alert-workflow.dxic
   - sentry-alert-workflow-basic.dxic
   - sentry-case-workflow.dxic

For further information on workflows see See "Case and Alert Workflows".

Note that you will also need to import pre-configured filters and reports. This is covered in a later section of this guide: Importing Case Management Filters and Reports.

2.3 Importing the Oracle Watchlist Screening Projects

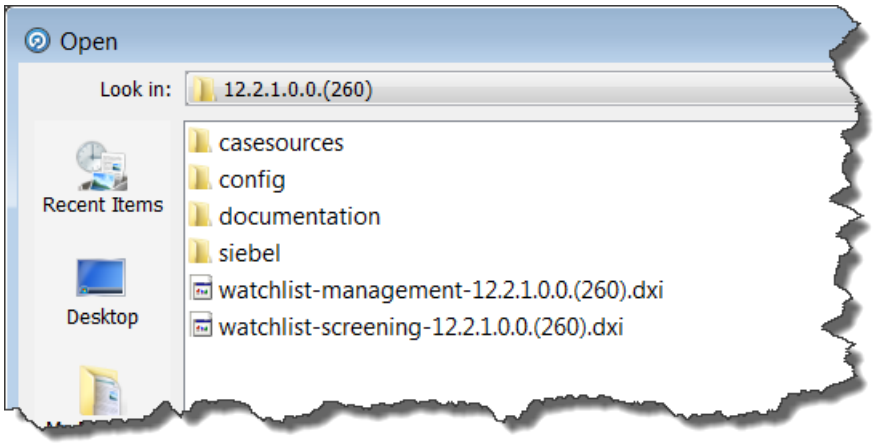
Oracle Watchlist Screening includes two OEDQ package (**.dxi**) files. The file names and their roles are detailed in the following table:

Package name	Project Name	Description
watchlist-management-<*version*>.dxi	Watchlist Management	Contains jobs and processes for handling watch list data. This includes downloading, preparing and exporting the data for use in the screening processes.
watchlist-screening-<*version*>.dxi	Watchlist Screening	Contains jobs, processes and Web services for handling customer data. This includes data quality analysis and data screening.

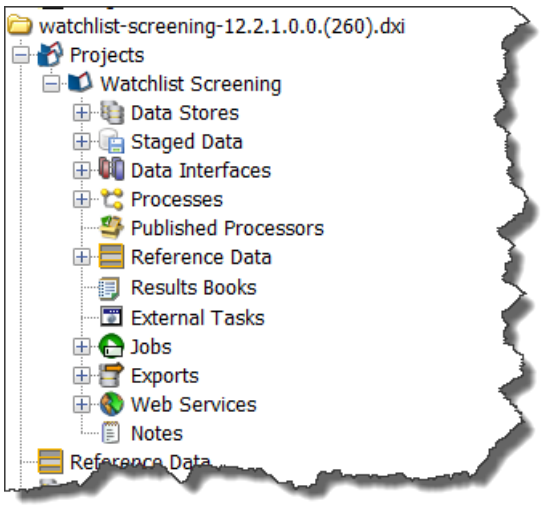
Each of the package files needs to be imported into OEDQ by using the following process:

1. Open the package file in OEDQ using the **File > Open Package File**... menu option.

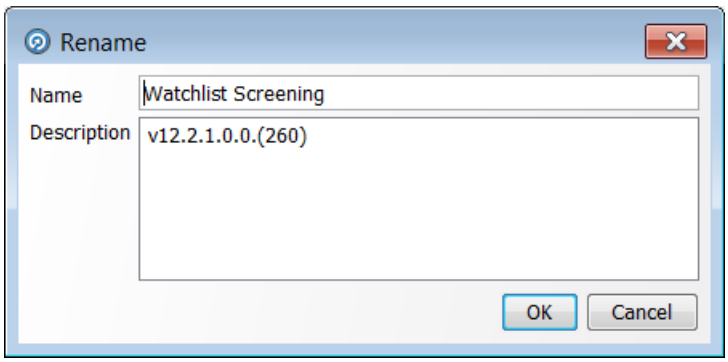
2. Select the package file from your distribution and click **Open**.



The package file and its contents will be displayed in the OEDQ project browser:



3. Drag and drop the project from the package file in the project browser to the **Projects** folder on your server. This will create a copy of the project on your deployment server. Rename the project to something suitable for the implementation (if required) and give it a meaningful description:



If you rename your screening project, make a note of the name as it will be required when configuring the Oracle Watchlist Screening User Application.

2.3.1 Installing multiple copies of the Watchlist Screening project

In some cases, it may not be possible to encapsulate all the screening requirements of an organization in a single instance of the Watchlist Screening project. For example:

- Regulatory requirements may mandate the use of different watch lists in different geographical locations;
- Different business units may require different, customized case or alert workflows.

Where this is the case, the Watchlist Screening project may be copied onto the server multiple times and configured for each discrete set of requirements.

Each project in OEDQ must have a unique name. The names used for the projects will be required when configuring the Oracle Watchlist Screening User Application, so where multiple copies of the project are installed, it is recommended that the names used for the projects are clearly descriptive.

2.4 Enabling the Oracle Watchlist Screening User Application Components

The Oracle Watchlist Screening User Application is an optional component of Oracle Watchlist Screening which allows users to perform real-time screening of entities and individuals, and to review and manage potential matches. This section describes the steps required to install and configure the Oracle Watchlist Screening User Application.

Before the Oracle Watchlist Screening User Application is used for the first time, the Watchlist Management job must have been run in order to prepare the watch list data for screening and to prepare the picklist Reference Data. Failing to do so will result in an error being generated.

NOTE: If you attempt to access the Oracle Watchlist Screening User Application without first associating at least one of your user groups with the Oracle Watchlist Screening User Application (see Configuring the security settings), you will not be able to launch the Oracle Watchlist Screening User Application.

2.4.1 Associating the Application with Screening Projects

The Oracle Watchlist Screening User Application acts as an interface to a pair of Web services, used for screening individuals and entities respectively. The Web services are defined as part of the Watchlist Screening project, installed in section 2.3 "Importing the Oracle Watchlist Screening Projects". If you have renamed your screening project, or have installed multiple copies of the screening project, you will need to edit your **sentryblueprint.properties** file to configure the list of valid projects that may be used by the Oracle Watchlist Screening User Application.

NOTE: Irrespective of the configuration in **sentryblueprint.properties**, users will still only be able to connect to projects as allowed by their groups and permissions. In addition, the Oracle Watchlist Screening User Application cannot connect to a project which does not contain the real-time screening Web services, `IndividualScreen` and `EntityScreen`. In summary, a project will only be available to a logged in user of the Oracle Watchlist Screening User Application if:

- the user has permission to access the project; and

- the project is listed in the sentryblueprint.properties file; and
- the project contains the IndividualScreen and EntityScreen web services.

Each project that the Oracle Watchlist Screening User Application should be able to access needs the following entries in the **sentryblueprint.properties** file:

- An arbitrary project identifier, which is included in the comma-separated list specified by the `projectIdentifiers` property. (Note that project identifiers should *not* contain spaces);
- A property of the form `<identifier>.director.project`, which links the identifier to the name of the project in OEDQ;
- A property of the form `<identifier>.ui.screening.layout`, which specifies the layout of the user interface to be used when connecting to that project (see section 5.1 "The Oracle Watchlist Screening User Application Customization files").

For example, the default configuration in the **sentryblueprint.properties** file following the first installation of Oracle Watchlist Screening is as follows:

```
projectIdentifiers = OWS
ui.screening.layouts = default-screening-layout
OWS.director.project = Watchlist Screening
OWS.ui.screening.layout = default-screening-layout
ui.default-screening-layout.properties = sentryblueprint-default-screening-layout
```

Comparing this snippet with the description above, we can see that:

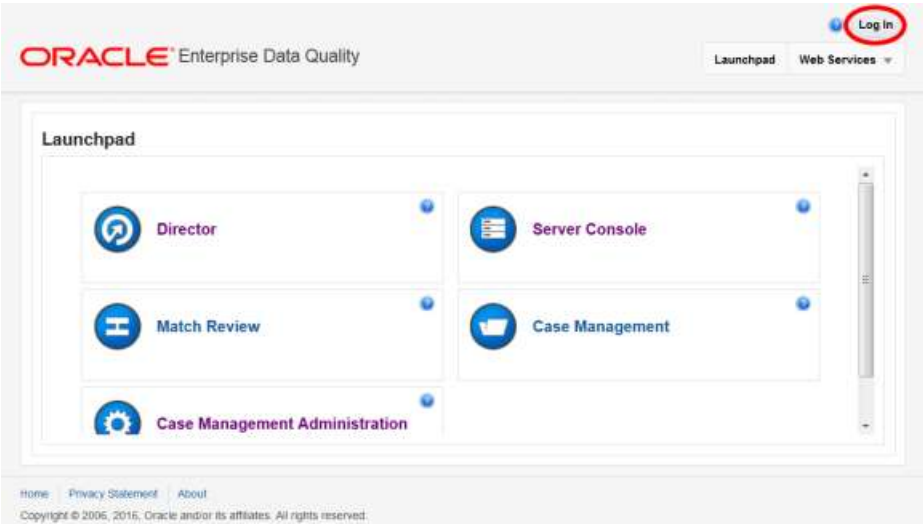
- There is a single project identifier, `OWS`, in use;
- The `OWS` identifier refers to the `Watchlist Screening` project;
- The user interface configuration to be used when connecting to this project is defined by the `ui.default-screening-layout` property.

To add one or more projects or to further customize the screening layouts, refer to the comments in the **sentryblueprint.properties** file.

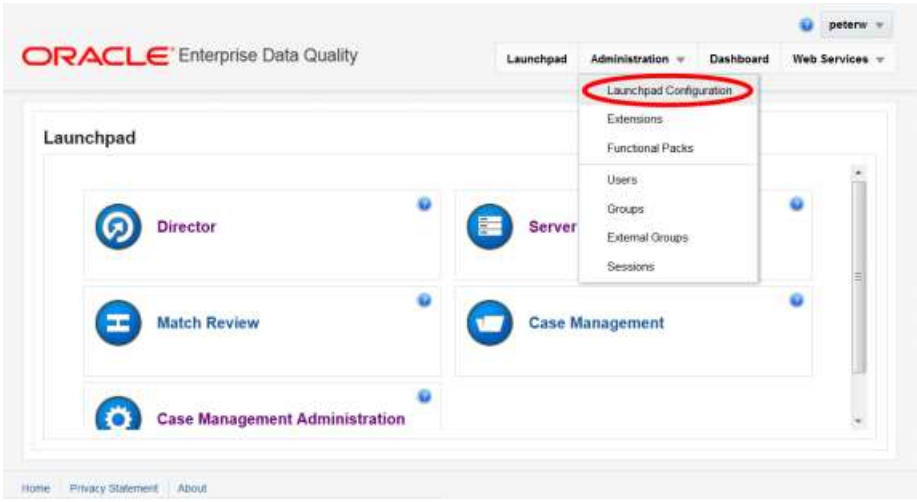
2.4.2 Publish Applications to the Launchpad

Before the Oracle Watchlist Screening User Application, or any other applications, can be launched, you must publish them to the OEDQ Launchpad.

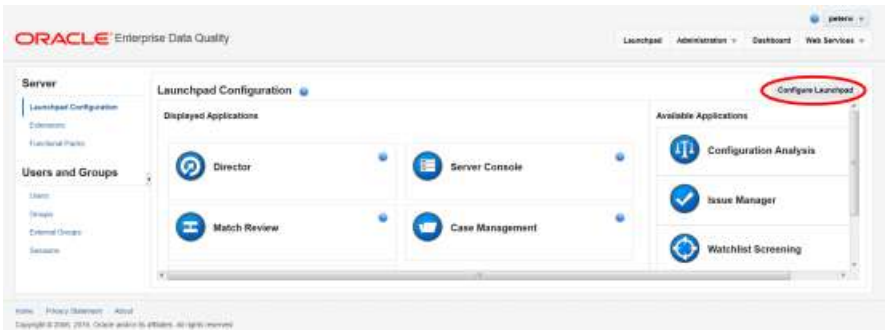
1. To do this, open the Launchpad in your browser and click **Log In**:



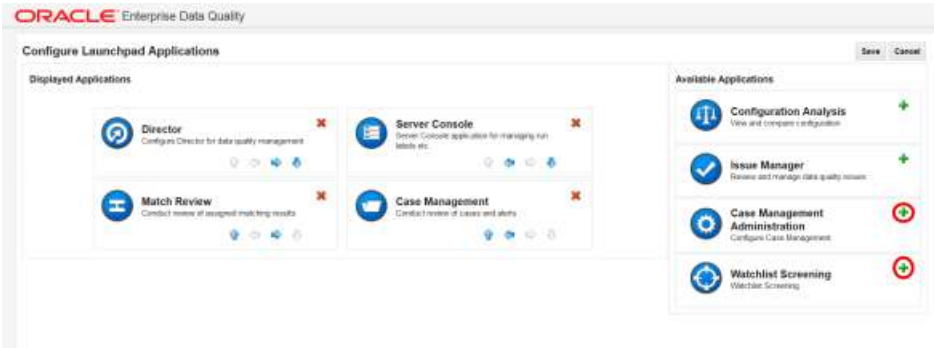
2. Login with your credentials, and next, select Launchpad Configuration from the Administration drop down:



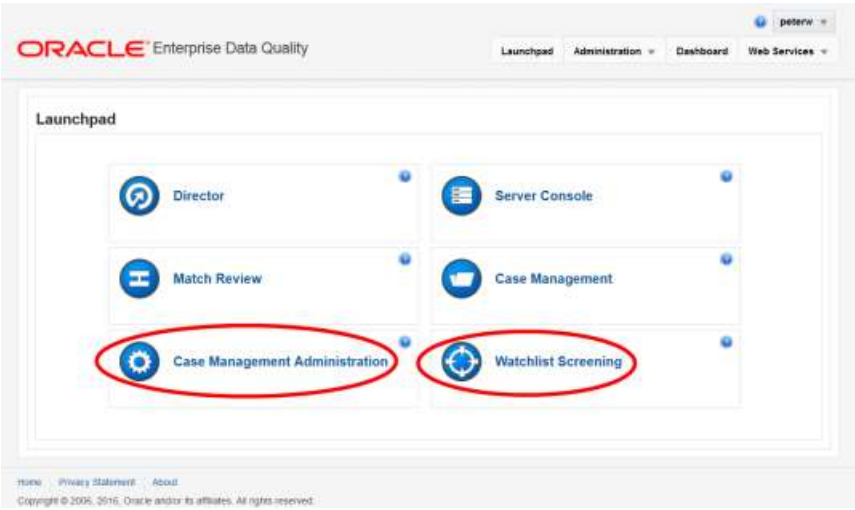
3. Click **Configure Launchpad**.



4. In the list of Available Applications, click ✚ beside **Watchlist Screening** and then click ✚ beside **Case Management Administration** to move them to the list of Displayed Applications.



5. Click **Save**, and then click **Launchpad** to Return to the Launchpad. The Watchlist Screening and Case Management Administration applications will be available:



2.4.3 Create the User Groups

Application security in OEDQ is controlled by a system of users and groups. Users are assigned to groups. Permissions are granted to groups, so a user's permissions will be the set of all permissions granted to their groups.

Applications are also assigned to groups. A user can only launch an application if they belong to at least one group with which that application is associated.

An Oracle Watchlist Screening deployment requires five user groups, which you must create. All users of Oracle Watchlist Screening must be assigned to at least one of these groups.

Each group that you create represents a different role in your Oracle Watchlist Screening deployment. The permissions that you must give to each group are detailed in the following table.

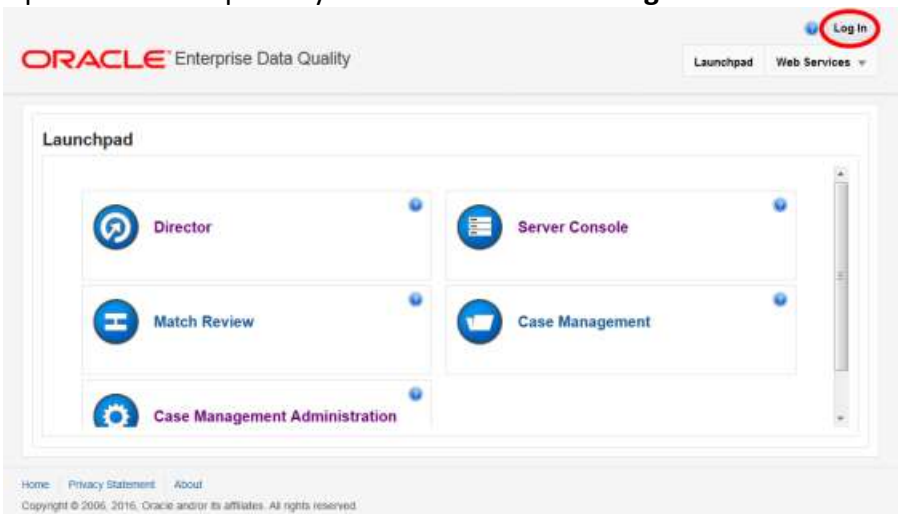
Group name	Description	Application Access	Functional Permissions
Sentry Approver	Users in this group have the same screening permissions as users in the Sentry Screener group, plus case reviewer permissions. Users can change the state of cases and assign them to other users, and can also create filters to search for cases and browse unassigned cases.	Watchlist Screening	C.M. Dynamic: Sentry Approver C.M.Static: Change Assignment C.M.Static: Change State C.M.Static: Edit Case C.M.Static: Edit User Filters C.M. Static: View Cases C.M. Static: View Cases Assigned To Others C.M.Static: View Unassigned Cases Dashboard: View Dashboard Sentry: Perform Case And Alert Management Sentry: Perform Real-Time Screening Sentry: View Real-Time Screening Receipt Sentry: View Real-Time Screening Results System: Connect to Messaging System
Sentry Data Entry	Users in this group only have sufficient permissions to log on and enter data for screening. They will be alerted if a potential match is found, but will not be able to see the details of the potential matching records. This group is not granted permissions to access Case Management functionality, and the case management tab is not visible to users in this group.	Watchlist Screening	Sentry: Perform Real-Time Screening System: Connect to Messaging System

Group name	Description	Application Access	Functional Permissions
Sentry Manager	The Sentry Manager group has all the permissions associated with the Sentry Reviewer group, plus a more managerial set of Case Management permissions.	Watchlist Screening Case Management Administration	C.M. Dynamic: Sentry Approver C.M. Dynamic: Sentry Reviewer C.M.Static: Apply Bulk Updates C.M.Static: Change Assignment C.M.Static: Change Invalid States C.M.Static: Change State C.M.Static: Delete Attachments C.M.Static: Delete Comments C.M.Static: Edit Case C.M.Static: Edit Global Filters C.M.Static: Edit State Expiry Time C.M.Static: Edit User Filters C.M.Static: Restrict Attachments C.M.Static: Restrict Cases C.M.Static: Restrict Comments C.M. Static: View Cases C.M.Static: View Cases Assigned To Others C.M.Static: View Unassigned Cases Dashboard: View Dashboard Sentry: Perform Case And Alert Management Sentry: Perform Real-Time Screening Sentry: View Real-Time Screening Receipt Sentry: View Real-Time Screening Results System: Connect to Messaging System
Sentry Reviewer	Users in this group have the same screening permissions as users in the Sentry Screener group, plus case reviewer permissions. Users can change the state of cases and assign them to other users, and can also create filters to search for cases and browse unassigned cases.	Watchlist Screening	C.M. Dynamic: Sentry Reviewer C.M.Static: Change Assignment C.M.Static: Change State C.M.Static: Edit Case C.M.Static: Edit User Filters C.M. Static: View Cases C.M. Static: View Cases Assigned To Others C.M.Static: View Unassigned Cases Dashboard: View Dashboard Sentry: Perform Case And Alert Management Sentry: Perform Real-Time Screening Sentry: View Real-Time Screening Receipt Sentry: View Real-Time Screening Results System: Connect to Messaging System

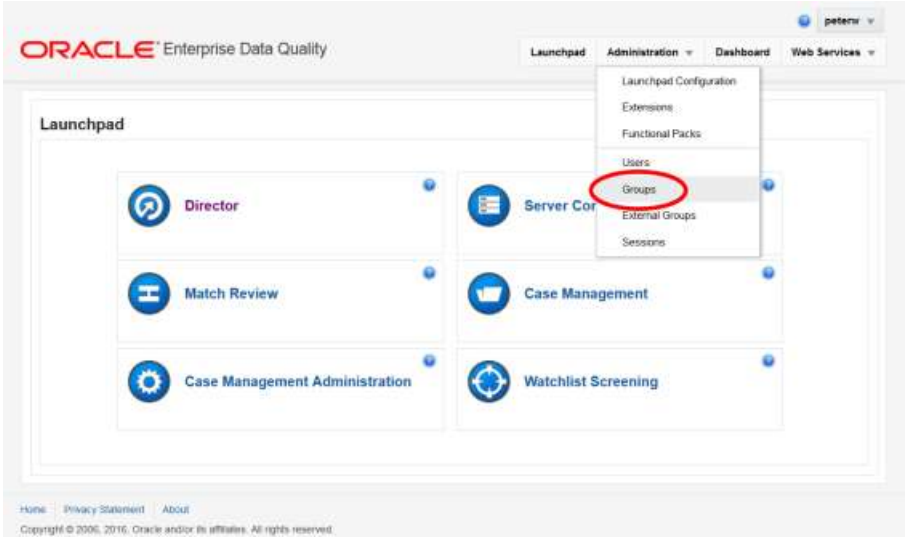
Group name	Description	Application Access	Functional Permissions
Sentry Screener	Users in this group can enter data for screening and view the details of potential matches. Users in this group can also access the OEDQ Dashboard. This group is not granted permissions to access Case Management functionality, and the case management tab is not visible to users in this group.	Watchlist Screening	Dashboard: View Dashboard Sentry: Perform Real-Time Screening Sentry: View Real-Time Screening Receipt Sentry: View Real-Time Screening Results System: Connect to Messaging System

Referring to the table above, create the user groups as follows:

1. Open the Launchpad in your browser and click **Login**:



2. Login with your credentials, and select **Groups** from the Administration drop down:

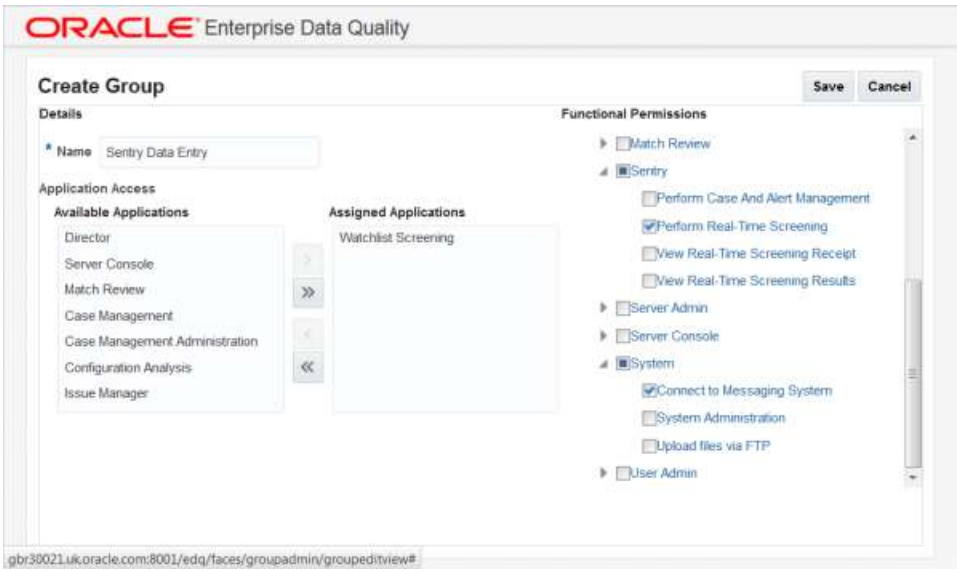


3. Click  to proceed to the Create Group screen.
4. In the Create Group screen:
    a. Enter the Group's Name.

b. Select the required applications in the list of Available Applications, and click  to move then to the list of Assigned Applications.

c. Select the required Functional Permissions.

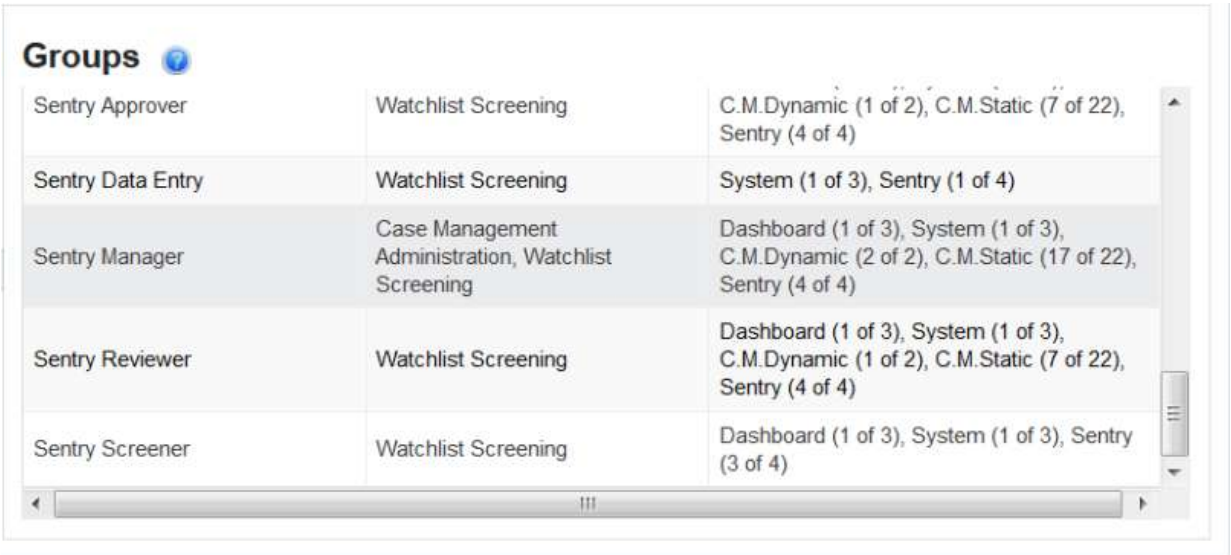
d. Click **Save**.



The screenshot above shows the configuration of the Sentry Data Entry user group.

5. Repeat steps 3 and 4 until you have created all five of the required user groups.

When you have finished, you should have added the following five groups (the group name is in the left-hand column, its application access is shown in the middle column, and its functional permissions are shown in the right-hand column):

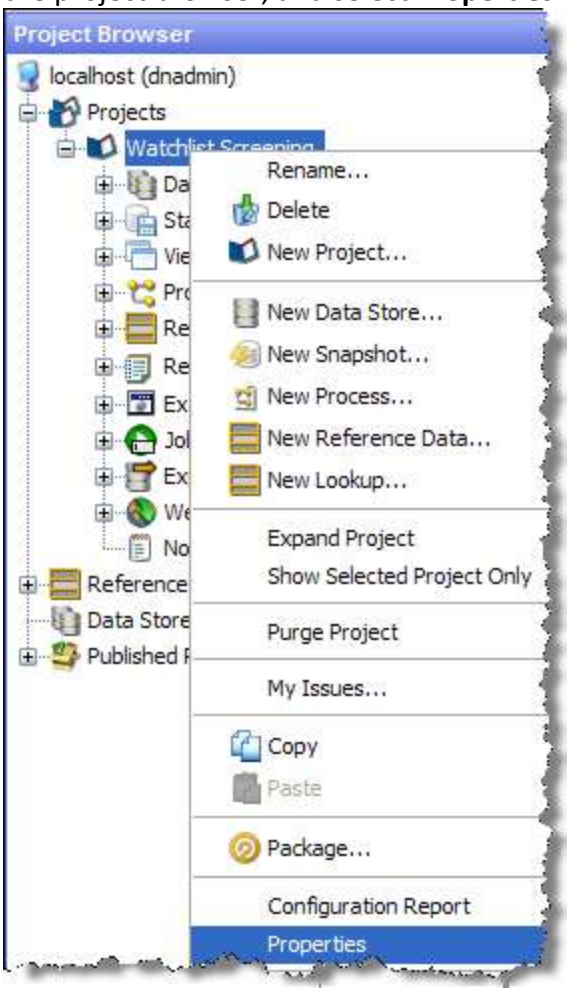


If the permissions associated with these groups are not appropriate for your deployment, you can set them up differently or create new ones. For more information on configuring users, permissions and roles, please refer to the online help.

2.4.4 Granting User Groups Access to the Project

The Oracle Watchlist Screening user groups have already been granted permissions to use the Oracle Watchlist Screening user application, but they also need to be granted access to the Watchlist Screening project. Such access is not included in the .dxi file, so must be manually granted at this point.

1. Open OEDQ Director. Right click on your imported Watchlist Screening project in the project browser, and select **Properties**.



2. In the **Properties** dialog, select the **Security** tab:

Any groups that already have the Add Project permission will be displayed here, and will have automatic access to all OEDQ projects. It is recommended that most users not be granted the Add Project permission. Instead, they can be granted specific access to the required projects by adding their user groups to this list.

3. Click **Configure**.
4. In the **Groups** dialog select all the Watchlist Screening groups (by default, those starting with the word **Sentry**) in the left-hand list and click the right arrow:

5. The groups will be moved into the right-hand list. Click **OK**.
6. All the Watchlist Screening groups now have access to the project:

7. Click **Close** to leave the **Properties** dialog.

2.4.5 Approaches to User Management

There are three approaches to managing users:

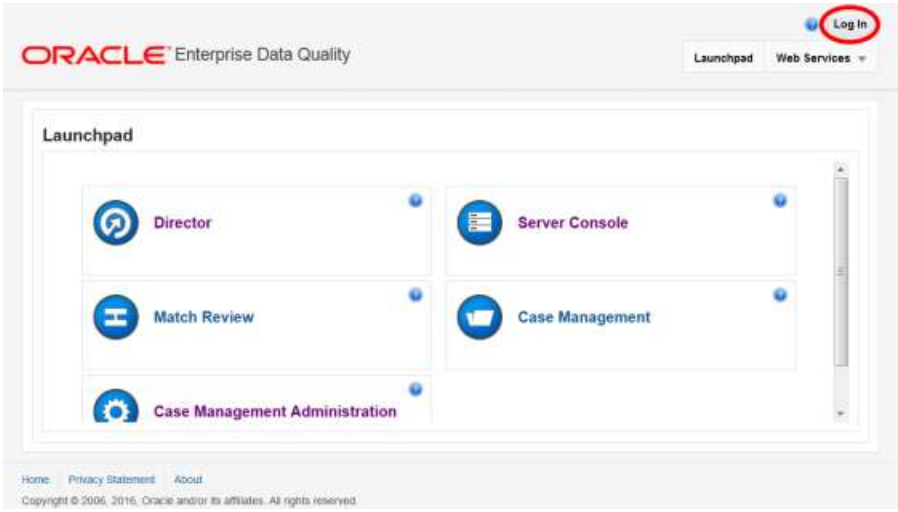
1. Manage internally - users are created and associated with user groups within Oracle Watchlist Screening.
2. Manage externally - users are created and associated with user groups in an external system (for example, WebLogic or an LDAP server). The external system's user groups are then mapped to Oracle Watchlist Screening user groups.
3. Manage internally and externally - both of the approaches above are applied in parallel.

2.4.5.1 Managing Users Internally

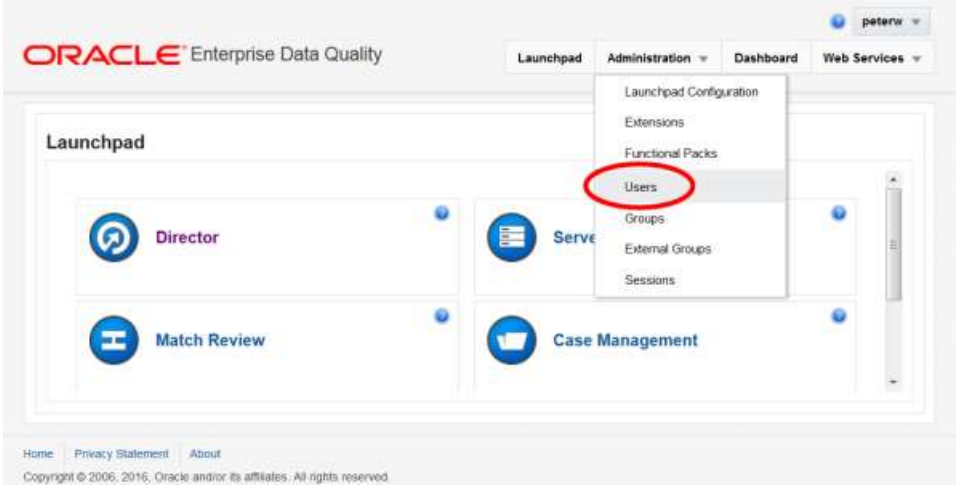
Follow the instructions in this section if you want to manage users internally within Oracle Watchlist Screening.

To create a user and associate it with a user group(s), proceed as follows:

1. Open the Launchpad in your browser and click **Login**:

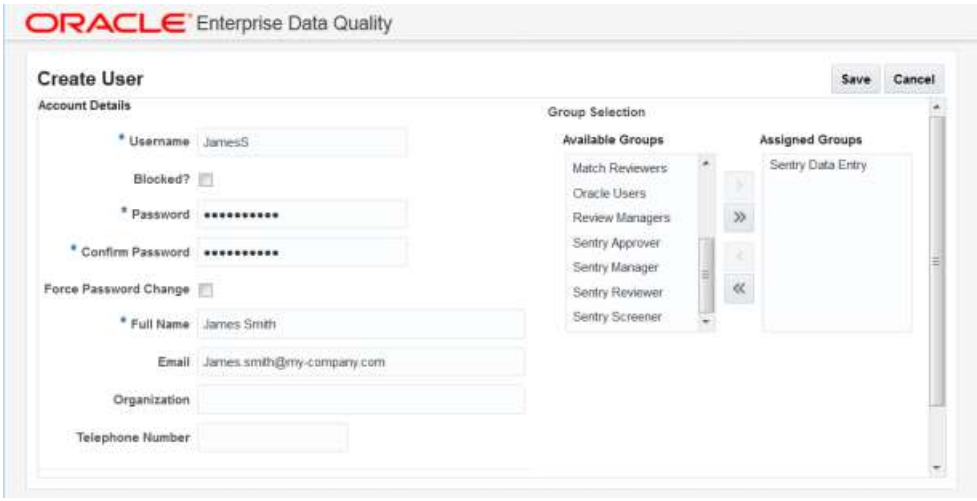


2. Login with your credentials, and select **Users** from the **Administration** drop down:



3. Click  to proceed to the Create User screen.
4. In the Account Details section, complete all of the mandatory fields and any of the optional fields as required.
5. In the Group Selection section, select one or more of the Sentry user groups in the list of Available Groups, and click  to move it to the list of Assigned Groups.

6. Click **Save**.



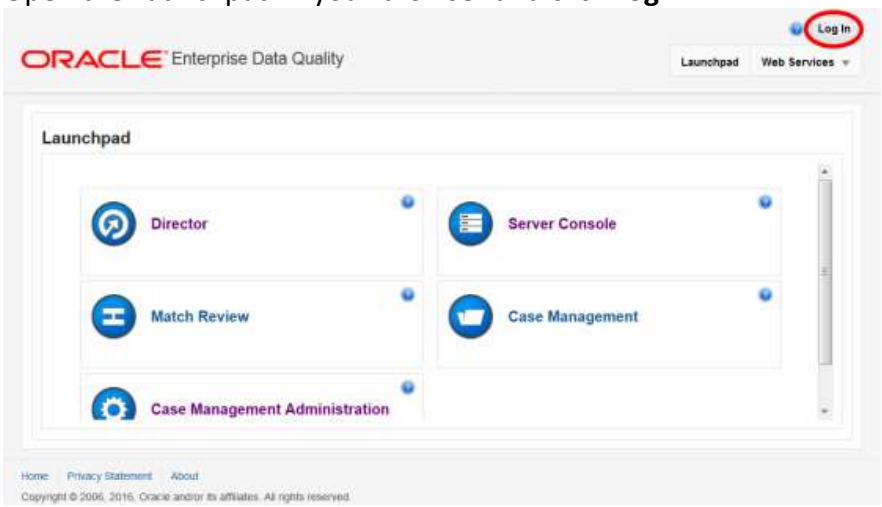
2.4.5.2 Managing Users Externally

Follow the instructions in this section if you want to manage users externally outside of Oracle Watchlist Screening. In such deployments, users are created in an external application (for example, in WebLogic), and are placed into external user groups (for example, WebLogic user groups). These external user groups are then mapped to Oracle Watchlist Screening user groups. You will usually require one external user group for each Oracle Watchlist Screening user group. For example, you might create an external user group called **WebLogic Sentry Approver** and map this to the Oracle Watchlist Screening **Sentry Approver** user group. The Oracle Watchlist Screening user group that an external user group is mapped to determines the users' available applications, functional permissions and project permissions.

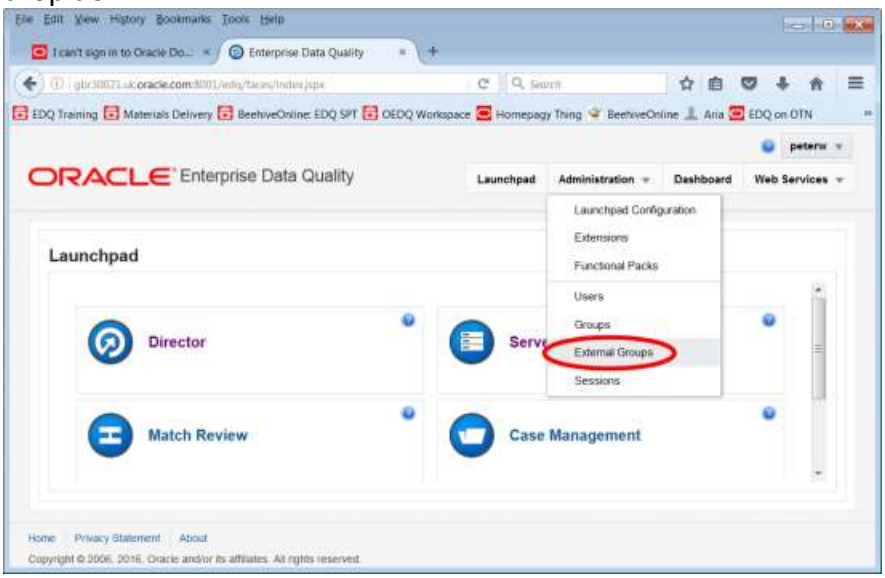
The instructions below describe how to map an external user group to an Oracle Watchlist Screening user group. The creation of external users and external user groups is beyond the scope of this document - refer to your external system's documentation for help about this.

To map an external user group to an Oracle Watchlist Screening user group, proceed as follows:

1. Open the Launchpad in your browser and click **Login**:



2. Login with your credentials, and select **External Groups** from the **Administration** drop down:



3. Select an External Group, and click **Edit**.
4. Select an Oracle Watchlist Screening user group in the list of Available Groups, and click  to move it to the group of Assigned Groups.
5. Click **Save**.
6. Repeat steps 3 and 4 to map each of your external user groups to an Oracle Watchlist Screening user group.

2.5 Importing Case Management Filters and Reports

This section describes the steps required to import pre-built Case Management filters and reports within Oracle Watchlist Screening.

The next steps require the use of the Oracle Watchlist Screening user interface, which you should be able to access from the OEDQ Launchpad. If it is not visible, follow the steps described in 2.4.2 : Publish Applications to the Launchpad.

1. Navigate to the Watchlist Screening user interface's **Case Management** tab.
2. Click the **Browser** sub-tab.
3. Right-Click the word **Global** and select **Import Filter**. The Import dialogue box is displayed.
4. Click  . Navigate to the **casesources** folder in the Oracle Watchlist Screening distribution, and select **sentry-cm-filters.dfl**.
5. Click **OK**. The Import Filters dialogue box is displayed. All of the filters should already be selected.
6. Click **OK** to import the filters and reports.

The filters and reports are imported as Global filters. This means that anybody with access to the Oracle Watchlist Screening user interface will be able to make use of them. See the Appendix about Filters and Reports Included With the Distribution for a list of the filters and reports.

2.6 Adjusting Server Startup Arguments (WebLogic Only)

If your instance of Oracle Watchlist Screening uses the WebLogic application server, and you are screening against the World-Check watch list, then, in order to download the World-Check reference data successfully, you must add the following to the 'Server Start' arguments of your EDQ managed server:

```
-DUseSunHttpHandler=true
```

This is only required if you are using the WebLogic application server **and** screening against the World-Check watch list.

Chapter 3: General Configuration

The sections in this chapter describe the following general configuration areas for Oracle Watchlist Screening:

- Configuring Watch List Management and Screening;
- Configuring Case Management;
- Scheduling the Screening Job;
- Filtering Watch List Data;
- Risk Scoring;
- Country Prohibition Screening; and
- Validating The Installation.

3.1 Configuring Watch List Management and Screening

The Oracle Watchlist Screening distribution contains two Run Profiles for configuring watch list management and screening: **watchlist-management.properties** and **watchlist-screening.properties**.

Run Profiles are optional templates that specify a number of 'override' configuration settings for externalized options when a Job is run. They offer a convenient way of saving and reusing a number of configuration overrides, rather than specifying each override as a separate argument.

Run Profiles may be used when running jobs either from the Command Line Interface, using the 'runopsjob' command, or in the Server Console UI.

For further information about Run Profiles and using the Command Line Interface, see the OEDQ online help.

The **watchlist-management.properties** Run Profile controls:

- which watch lists are downloaded, and the configuration of the download process;
- whether filtering is applied to the watch lists; and
- whether Data Quality Analysis is applied to the watch lists.

Additionally, the **watchlist-screening.properties** Run Profile controls:

- Real-Time and Batch Screening set up;
- Screening reference ID prefixes and suffixes;
- Watch list routing; and
- configuration of match rules.

Note: The properties controlling match rules are not included in the **watchlist-screening.properties** Run Profile by default. See Configuring Match Rules for further information.

3.1.1 Preparing Watch List Data

Oracle Watchlist Screening is pre-configured to handle reference data from the following sources:

- HM Treasury
- OFAC
- EU consolidated list
- UN consolidated list
- World-Check
- Dow Jones Watchlist
- Dow Jones Anti-Corruption List
- Accuity

Additionally, you can optionally supply reference data from your own private watch list using the Private List Interface (PLI).

Values in the **watchlist-management.properties** Run Profile control which lists are used and how they are downloaded, staged, and filtered (or not).

Note:

- Watch lists can be downloaded automatically (by setting the appropriate values in the Run Profile) or manually (by navigating to the list provider's web site, downloading the list and saving it to the matching sub-folder in the Landing Area).
- The staging value **must** be set to **Y** the first time a watch list is downloaded. Thereafter, leave it set to Y to refresh the staged data every time a download is performed, or **N** to preserve the pre-existing staged data.
- All downloaded watch lists **must** be set to filtered or unfiltered.
- The Accuity, Dow Jones, Dow Jones Anti-Corruption and World-Check lists are all provided as paid services. To use one of these watch lists it is necessary to apply to the individual list providers for an account. Please refer to the relevant provider websites for further information.
- The option to download private watch lists is not supplied, as it is assumed that this data will be available in house.

For specific configuration information on each of these watch lists, see Appendix B: Watch List Information.

Example - Preparing the Accuity list

This example describes how to edit the **watchlist-management.properties** Run Profile to allow the download and configuration of the Accuity list. The steps in the example can be applied, with little modification, to other data lists.

Download and Staging

To automatically download the Accuity list, set the following values to Y:

```
phase.ACY\ -\ Download.enabled
phase.ACY\ -\ Stage\ reference\ lists.enabled
```

Note: To manually download the Accuity list, leave these values set to N. Navigate to the URL provided in the Accuity Reference Data section, download the list and save it to the config/landingarea/Accuity subfolder.

Filtering

To prepare the Accuity list with filtering, set the following value to Y:

```
phase.ACY\ -\ Prepare\ without\ filtering.enabled
```

To prepare the Accuity list without filtering, set the following values to Y:

```
phase.ACY\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled
phase.ACY\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled
```

For details of how to configure watchlist filtering, See "Filtering Watch List Data".

Data Quality Analysis

To enable Data Quality analysis for the Accuity list, set the following values to Y:

```
phase.DQ\ -\ Stage\ ACY\ reference\ lists.enabled
phase.DQ\ -\ ACY\ reference\ data\ quality\ analysis.enabled
stageddata.DQ\ ACY\ -\ Invalid\ Standard\ Country\ in\ Accuity\
Nationality\ to\ Standard\ Country.visible
stageddata.DQ\ ACY\ -\ Missing\ Source\ in\ Accuity\ Source\ Risk\
Scores\ Reference\ Data.visible
stageddata.DQ\ ACY\ -\ Obsolete\ Source\ in\ Accuity\ Source\ Risk\
Scores\ Reference\ Data.visible
```

Enable phases for download and staging

To enable automated download of the Accuity list, the OEDQ server must be connected to the internet.

Enter the username and password combination for the Accuity login in the values ending:

```
ftp://username:password@ftp.financialgo.net/PIDGWL.ZIP
```

If the OEDQ server is connected to the internet via a proxy, set the following properties:

- proxy_host
- proxy_port
- proxy_username
- proxy_password

3.1.2 Private Watch List Set Up

Oracle Watchlist Screening is pre-configured to work with a number of commercially-available and government-provided watch lists. However, you can also screen against your own private watch lists. On installation, screening is configured to run against a sample private watch list with minimal additional configuration, allowing the installation to be validated quickly. The

sample private watch list is provided in two files - **privateindividuals.csv** and **privateentities.csv**- in the **config/landingarea/Private** folder.

> **The OEDQ Config Folder**:
> Your OEDQ instance's **config** folder might not be named 'config'. The choice of the config folder's name is made when OEDQ is installed - in some cases a name is automatically allocated. OEDQ release 11g and later has both a 'base' and a 'local' config folder. The base config folder is often called '**oedqhome**', and the local config folder is often called '**oedqlocalhome**'. In some cases, dots or underscores may be inserted into these names (for example: 'oedq_local_home'). Whenever you see a file path in this document that begins with **config**, this always refers to your OEDQ instance's local config folder.

The first step in screening against your own private watch list is to replace the data in the supplied files with your own data. To do this:

1. Transform your private watch list data into the format specified by the Private List Interface (see the Data Interfaces Guide for further information).
2. Replace the data in the **privateindividuals.csv** and **privateentities.csv** files with your transformed private watch list data.

> **Note**: The files must be saved in UTF-8 format.
>
> **Note**: To screen against multiple private watch lists, consolidate them into the the two files: **privateindividuals.csv** and **privateentities.csv**. These two files can also be used to hold data from external watch lists that Oracle Watchlist Screening is not pre-configured to work with.

The second and final step is to enable the staging and preparation of the private watch list in the `watchlist-management.properties` Run Profile. To stage your private watch list set the following value to **Y**:

```
phase.PRIV\ -\ Stage\ reference\ lists.enabled
```

Once you have done this, set the following value to **Y** to prepare the private watch list without filtering:

```
phase.PRIV\ -\ Prepare\ without\ filtering.enabled
```

Or set both of the following values to **Y** to prepare the private watch list with filtering:

```
phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled
phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled
```

3.1.3 Showing Watch List Staged Data/Snapshots in the Server Console UI

Certain types of staged data and snapshots are hidden in the Server Console UI by default. These are:

- Watch list snapshots
- Intermediate filtered watch list staged data
- Centralized Reference Data staged data/snapshots

To display this data, set the corresponding visibility property value(s) in the relevant Run Profile(s) to **Y**.

For example, to make all Accuity watch list snapshots generated during Watchlist Management visible, set the following properties in the `watchlist-management.properties` Run Profile:

- `stageddata.ACY\ Sources.visible = Y`
- `stageddata.ACY_All.visible = Y`
- `stageddata.ACY_Sources.visible = Y`

3.1.4 Configuring Match Rules

Match rules - and also match clusters - can be configured and controlled by adding a property to the `watchlist-screening.properties` Run Profile.

For example, to disable the **Exact name only** rule for Batch and Real-Time Sanctions screening, add the following property to the Run Profile:

```
phase.*.process.*.[I010O]\ Exact\ name\ only.san_rule_enabled = false
```

Note: Capitalization must be respected and characters must be escaped as required.

The * character denotes a wildcard, and therefore specifies that the above rule applies to all phases and all processes. If disabling the rule for Batch screening only, the property would read:

```
phase.Batch\ screening.process.*.[I010O]\ Exact\ name\
only.san_rule_enabled = false
```

Note: For further details on tuning Match rules, please refer to the Oracle Watchlist Screening Matching Guide.

3.1.5 Real-Time and Batch Screening Set Up

By default, Real-Time and Batch screening is enabled for SAN, PEP and EDD records.

This is controlled by the Real-Time and Batch screening properties in the `watchlist-screening.properties` Run Profile. Using these properties, it is possible to enable or disable Real-Time or Batch screening for all records or by record type.

For example, to only run Real-Time screening for PEP and EDD individual and entity records, change the value of the following properties as indicated:

- `phase.Start\ Batch\ Screening.enabled = N`
- `phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.san_enabled = N`
- `phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.san_enabled = N`

Ensure all other Real-Time screening properties are set to **Y**.

3.1.6 Outputting Relationships Data to Files

Screening identifies possible relationships (or possible matches if you like) between individuals and entities in your customer data and the individuals and entities on watch lists. These relationships form the basis of the alerts and cases that you can review in the Oracle Watchlist Screening user interface. When you run screening in batch, as well as outputting these relationships to the Oracle Watchlist Screening user interface, you can also output them

to .csv files. This can be useful if, for example, you want to use Oracle Watchlist Screening to identify the relationships, but you want to review them using another system.

To enable the output of relationships data to files, set the following values to **Y** in the Batch Screening Setup section of the `watchlist-screening.properties` Run Profile:

```
phase.*.process.*.output_relationships
phase.Export\ Batch\ Relationships.enabled
```

When you run screening with these run profile parameters enabled, two files are created:

- relns-ent-batch.csv (which holds relationship data for entities).
- relns-ind-batch.csv (which holds relationship data for individuals).

The two files are placed in the **config/landingarea/sentryrelns** folder.

3.2 Filtering Watch List Data

3.2.1 Enabling Watch List Filtering

Watch list data is filtered either during List Management, Screening, or both.

To enable filtering for a specific watch list, set the **Prepare Filtering** phase(s) in the appropriate Run Profile to **Y**, and the **Prepare Without Filtering** phase(s) to **N**.

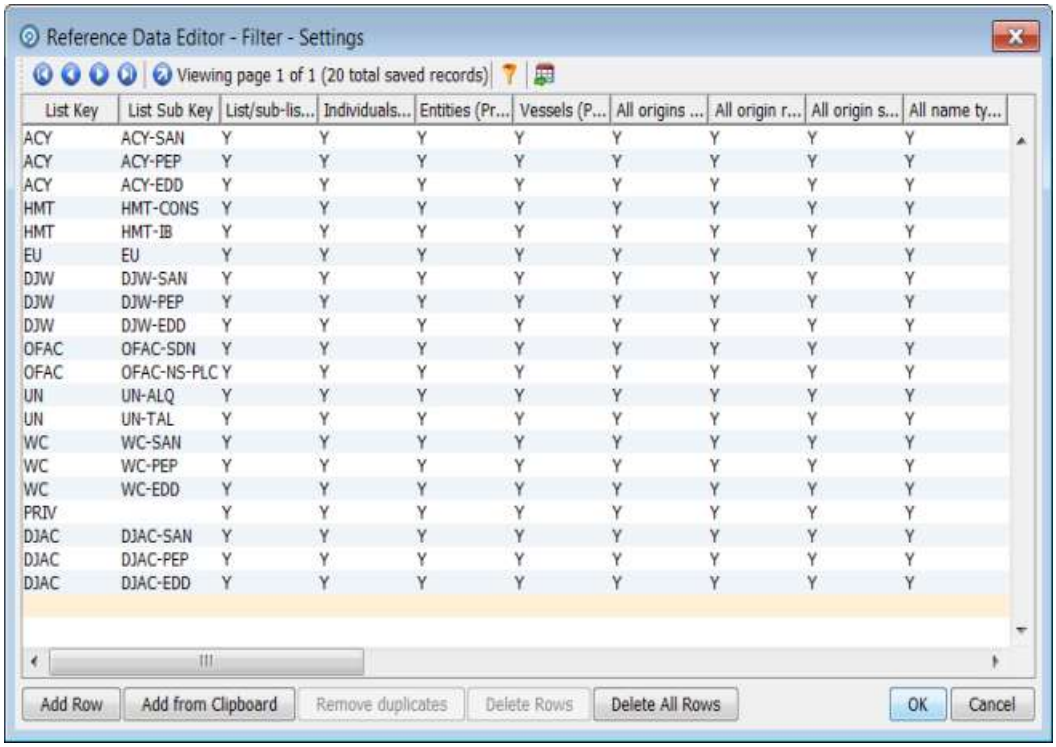
3.2.2 Configuring Watch List Filtering

Watchlist filtering is controlled by configuring reference data in the Watchlist projects.

Note:

- The reference data sets in Watchlist Management and Watchlist Screening projects are identical. This is to support installations requiring filtering at different stages. For example, a company may wish to perform initial filtering as watch list data is prepared, and then run several screening projects on specific parts of that data (by country, origin, etc.)
- Once data is filtered out, it is not possible to filter it back in. E.g. if all entities are filtered out in Watchlist Management, even if the Watchlist Screening project is configured to include entities, they will not show up in results data.

The top level of filtering is controlled by editing the **Filter - Settings** reference data:



All the reference data filters are set to **Y** by default, except **Linked Profiles** which is set to **N**. Unless these settings are changed, no actual filtering is performed on watch list data.

In the **Filter - Settings** reference data, a value of **Y** indicates that all records should be included - in other words, no filter should be applied.

Broadly speaking, watch list filtering falls into four categories:

- By list and list sub key.
- By list record origin characteristics.
- By list profile record characteristics.
- By linked profiles.

Primary and Secondary Filtering, and Linked Records

- Primary filtering - These filters are used to return all profiles that match the criteria specified.
- Linked Profiles - If this value is set to Y, then all profiles linked to those captured by Primary filters are also captured; an example of use is a filter configured to capture all Sanctions and their related PEPs.
- Secondary filtering - These filters are applied to further filter any linked profiles that are returned.

Note: Only the World-Check and DJW watch lists can provide Linked Profiles.

Setting Multiple Values for Primary and Secondary Filters

The following filter options require further configuration in additional reference data:

- Origins
- Origin Regions
- Origin Statuses
- Primary and Secondary Name Qualities
- Primary and Secondary Name Types
- Primary and Secondary PEP Classifications

To filter using one or more of these options, set the relevant value in the **Filter - Settings** reference data to **N**, and then make further changes to the corresponding reference data.

The affect of setting a value in the **Filter - Settings** reference data to **N** is that only records that match values set in the corresponding reference data will be included. For example, if you set the value of **All name qualities (Primary)?** to **N** in **Filter - Settings**, then, in the **Filter - Primary Name Qualities** reference data you could determine which name qualities should be included for each watch list. For instance, if you include a row for High quality names in the EU watch list, but you do not include rows for medium and low quality names for this watch list, then only records with high quality names will be included for this watch list.

Some of these reference data sets will be prepopulated with rows, to be edited or removed as required. These rows contain data (generally, but not always) supplied by each watch list provider, and are all contained within the Watchlist Management project.

E.g. to view all possible keywords for World-Check data, open the **WC Keyword** reference data in the Watchlist Management project. See the following example for further details.

3.2.3 Example - Filtering World Check Data

This example describes configuring filtering on the World-Check Sanctions list in the Watchlist Management project, and setting further filters in the Watchlist Screening project. Specifically:

- enabling filtering in the Run Profiles;
- configuring the Primary filters in the Watchlist Management project to return only active records for sanctioned individuals (not entities) originating from the EU list;
- enabling the filtering of Linked Profiles in the Watchlist Management project; and
- configuring the Secondary filters in the Watchlist Screening project to further filter out all Linked Profiles of deceased individuals.

Setting filtering options in the Run Profiles

In the **watchlist-management.properties** Run Profile, set the World-Check filtering phases as follows:

- phase.WC\ -\ Prepare\ without\ filtering.enabled = N
- phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y
- phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y

In the **watchlist-screening.properties** Run Profile, set the World-Check filtering phases as follows:

- phase.WC\ -\ Load\ without\ filtering.enabled = N
- phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = Y
- phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y

Setting Primary Filters and Linked Profiles in the Watchlist Management project

1. In Director, open the Watchlist Management project and expand the Reference Data node.
2. Locate the **Filter - Settings** reference data, and double-click to open it.
3. Ensure the **List/sub-list (Primary?)** value in the **WC-SAN** row is set to **Y**.
4. Set the **Entities (Primary)?** value in the **WC-SAN** row to **N**.
5. Set the **Inactive (Primary)?** value in the **WC-SAN** row to **N**.
6. Set the **All Origins (Primary)?** value in the **WC-SAN** row to **N**.
7. Ensure all other values in the **WC-SAN** row are set to **Y**.
8. Click **OK** to close the reference data and save changes.
9. Locate the **Filter - Origins** reference data and double-click to open it.
10. Add a new row with the following values:
    a. List Key - WC
    b. List Sub Key - WC-SAN
    c. Origin - EU
11. Change the **Linked Profiles?** value in the **WC-SAN** row to **Y**.
12. Click **OK** to close the **Filter Settings** reference data and save changes.

Setting Secondary Filters in the Watchlist Screening project

1. Open the Watchlist Screening project, and expand the reference data link.
2. Locate the **Filter - Settings** reference data file, and double-click to open it.
3. Set the **Deceased (Secondary)?** value in the **WC-SAN** row to **N**.
4. Click **OK** to close the reference data and save changes.

3.2.4 Screening All Data Using Sanctions Rules

By default, watch list records are routed to the different screening processes depending on their record type (i.e. SAN, PEP or EDD). This allows different rules, and hence different levels of rigor, to be applied to the list data according to risk appetite.

However, if you want to use the same screening logic for all list records, and do not want the overhead of maintaining separate rulesets, the system can be configured to reroute all list records to the SAN screening processes. To do this, set the **phase.*.process.*.Screen\ all\ as\ SAN?** value in the **watchlist-screening.properties** Run Profile to **Y**.

3.3 Configuring Case Management

Oracle Watchlist Screening uses the OEDQ Case Management application to investigate and manage cases and alerts generated by the matching processes.

The following sections describe the default case source and workflows provided with the Oracle Watchlist Screening User Application, but all of these can be edited to suit your requirements. For full instructions on editing workflows and case sources, please refer to the OEDQ online help.

3.3.1 Case and Alert Workflows

Three workflows are provided with the Oracle Watchlist Screening User Application: one for cases and two for alerts.

Workflows describe the states that an alert (or case) may pass through during its lifecycle, and how it can transition from one state to another. If the provided workflows do not suit your requirements, they can be edited in the Case Management Administration application.

> **Note**: An alert is a potential match between the input data and a watch list. A case is a collection of all the alerts for a given input record. Screening a single customer record may result in several alerts, all of which will be grouped into a single case.

For more information on cases, alerts and workflows, please refer to the OEDQ online help.

The Case Workflow

The case workflow in **sentry-case-workflow.dxic** is very simple, consisting of a single state: **Generated**.

The Alert Workflows

The two alert workflows are **sentry-alert-workflow.dxic** (the default option) and **sentry-alert-basic.workflow.dxic**.

The states within each workflow are prefixed according to their use. The prefixes are:

- SAN for use with sanctions alerts;
- PEP for use with PEP alerts; and
- EDD for enhanced due diligence alerts.

For diagrams of these workflows See "Watchlist Workflow Diagrams".

sentry-alert-workflow.dxic

This is a complex workflow designed for two user types – Reviewer and Approver.

Reviewers can:

- escalate an Open alert as a possible True Match;
- send an alert for Further Information; or
- eliminate an alert as a False Positive.

Approvers take over when an alert is identified as a possible True Match. From here, they can:

- identify the alert as a True Match (this is known as “completing” an issue);

- send the alert for Further Information; or
- reopen the alert (i.e. submit it for rework by a Reviewer).

When completed as a True Match, SAN alerts are taken through a True Match Exit process.

PEP and EDD alerts can either be confirmed as True Matches, or flagged as High, Medium or Low Risk and assessed accordingly. If so flagged, they are sent for an automatic Risk Review after a preset period of time.

NOTE: In this workflow no state is a "dead end". In other words, False Positives and True Matches can be re-opened for investigation at any time.

sentry-alert-workflow-basic.dxic

This workflow is much simpler. Each alert can exist in one of four states:

- Open
- Pending
- False Positive
- True Match

There is no provision for different user types and an alert in any one state can be changed to any other state.

3.3.2 Customizing the Case Management Display Settings

The layout of the **Alert Details** area (hereafter, the **Details** area) on the **Case Management** tab can be customized. Any changes made to the layout are system-wide (that is, different users cannot have different layouts configured) per case source. For these reasons the ability to make these changes are restricted to users in a group that has been assigned the **C.M.Static: Edit Supplementary Data** permission.

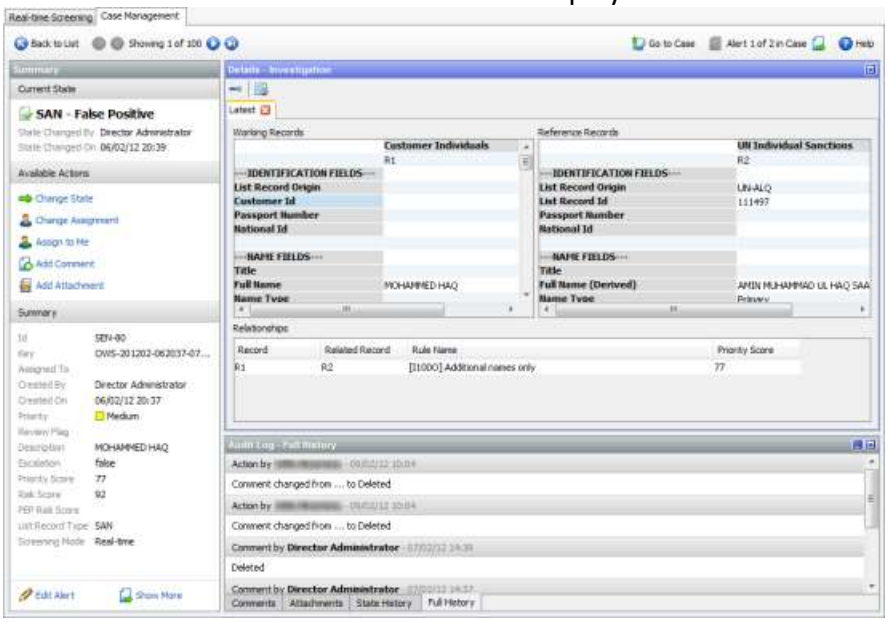
Note: These settings can also be managed in the Case Management application.

To display the **Details** area:

1. Click the **Case Management** tab in Watchlist Screening.
2. Select the **Filter** tab on the bottom of the Browser area.
3. Select **Alerts** in the **Type** field, and click ▶. All currently active alerts are displayed in the **Results** area. If no alerts have been generated, the Results area will remain blank.

   Note: If no alerts have yet been generated, the **Results** area will remain blank. Run a screening operation, and then return to this procedure.

4. Double-click an alert. The **Details** area is displayed:



Layout Options

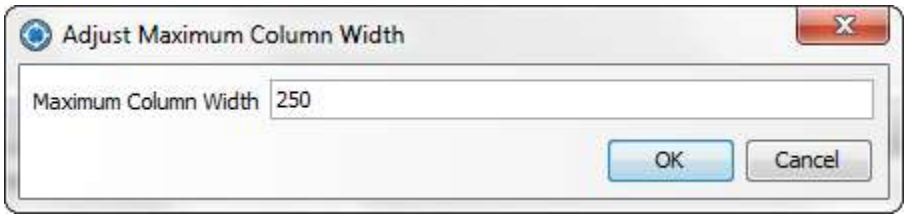
Horizontal and Vertical views

By default, the Working and Reference Records areas are displayed vertically (i.e. side-by-side) as in the screenshot above.

To switch the Working and Reference Records columns from a vertical (the default) to a Horizontal layout, click in the top-left corner of the **Details** area, and then click the arrow next to it. To switch back, click the arrow again. The arrow changes orientation depending on the view currently selected.

Resize columns

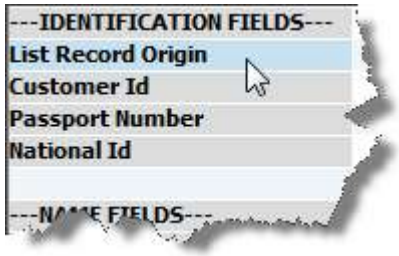
To resize the Working and Reference Records columns, click and then click . The **Adjust Maximum Column Width** dialog is displayed:



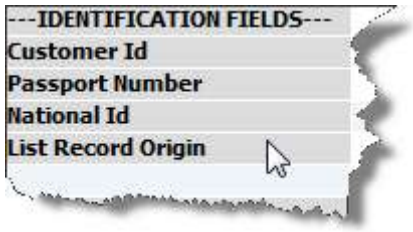
Edit the column width as required, and click OK to save changes, or Cancel to abandon.

Click and drag attributes

To move an attribute up or down through a Record column, click to select it:



and drag to the position required:



Edit Attributes

Attributes can be renamed or hidden (or revealed) as required. Additionally, it is possible to insert header or separator rows to make sure the Working Record attributes align with the corresponding Reference Record attributes.

Renaming an attribute

1. Right-click on the attribute and select **Rename**.
2. Edit the name in the **Rename** dialog.
3. Click **OK** to save changes or **Cancel** to abandon.

Hiding or revealing an attribute

To hide an attribute or attributes, right-click on the attribute and select **Hide**. The attribute will disappear.

To reveal an attribute:

1. Right-click on any attribute and select **Show Attributes > Select**.
2. In the dialog displayed, locate the required attribute(s) and check the selection box(es).
3. Click **OK** to save changes or **Cancel** to abandon.

Revealing all attributes

Right-click on an attribute and select **Show Attributes > All**.

3.3.3 Customizing the Data Access Permissions

As well as the application and functional permissions already discussed, Case Management allows you to create data access permissions. These permissions can be associated with case sources, transitions and states, and act as additional, configuration-specific checks on the data that can be accessed by various users.

A user can only view data with permission settings compatible with his or her own permissions. A user can only apply transitions to cases or alerts if they have the appropriate

permissions to do so. Whole sets of data can be hidden from groups of users by assigning the corresponding state, for example, a permission setting that is not granted to those users.

Use the Permissions Administration section of Case Management Administration to create the permissions you require. Use the Workflow Editor to assign them to the appropriate states and transitions in your workflow, and use OEDQ to associate them with the appropriate case source or sources.

For further details on configuring and assigning permissions, please refer to the OEDQ online help.

3.3.4 Customizing the Flag Keys

A case source includes the definition of the flag key for that case source. A flag key is a set of fields in the data which are considered significant when evaluating a match, but which do not contribute to the case or alert keys. For a more complete description of case, alert and flag keys, please refer the OEDQ online help.

If data in a field included in a flag key changes, the Review Flag in Case Management is set. This is because it may be useful to re-evaluate any previous decisions made on the alert. It is then possible to find any alerts with a Review Flag, or to customize the alert workflow such that a further action is triggered, such as a change of workflow state.

> **NOTE**: The review flag is also set if the number of records in an alert changes; for example, if a new alias name of a list record is added that matches the customer record.

An example of a potential flag key field is date of birth; some potential matches may be eliminated on the grounds that the date of birth is too different between the customer and watch list records. Therefore, if the date of birth information on either list changes, it is likely that any potential matches which depend on it should be re-reviewed. An example of a field which should not be included in the flag key is account balance. This contains a value which is likely to change rapidly but which does not have any impact on the match decisions.

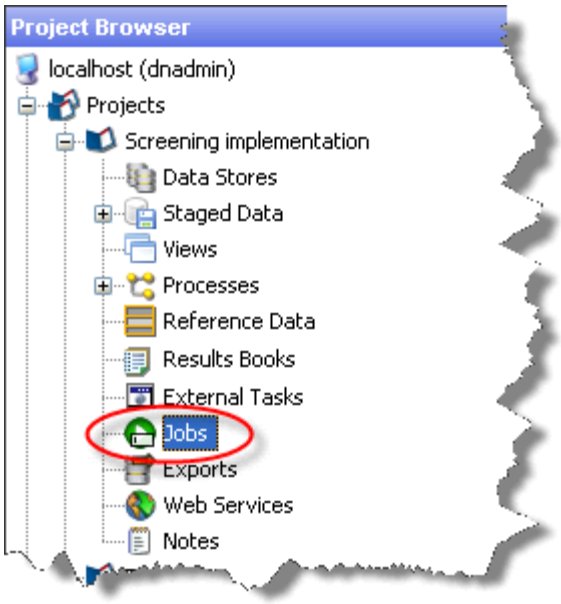
Oracle Watchlist Screening is supplied with a default flag key configuration as part of the default case source. You may wish to check that the flag key configuration for the default case source is appropriate for your screening requirements.

For further details on configuring flag keys and alert workflows, please refer to the OEDQ online help.

3.4 Scheduling the Screening Job

Jobs are collections of processes, organized into phases, which may be executed manually or configured to run periodically using a scheduler.

The jobs belonging to a project are managed via, and stored in, the project's Jobs node in the project browser:



3.4.1 Selecting your Main Oracle Watchlist Screening Job

Oracle Watchlist Screening provides one MAIN job and four ancillary jobs.

When run, the MAIN job will:

- snapshot all list reference data;
- prepare the customer data if batch processing is in use, and
- run the screening processes configured in that job.

When configuring your Oracle Watchlist Screening installation, you must schedule the MAIN job to run on a regular basis.

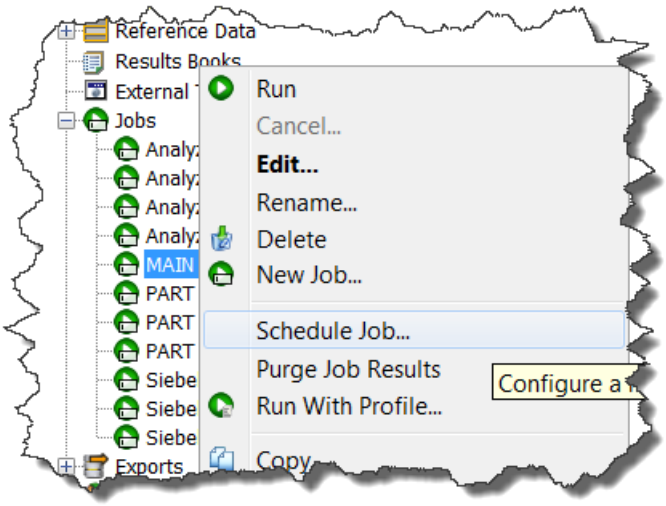
> You can configure Oracle Watchlist Screening to only snapshot, prepare and screen the watch list data that your installation requires by amending properties in the `watchlist-management.properties` and `watchlist-screening.properties` Run Profiles. See Configuring Watch List Management and Screening for more information about the Run Profiles.

In general, the ancillary jobs are called by the MAIN job, or by other ancillary jobs. These are present within Oracle Watchlist Screening to enable configuration re-use and are not usually invoked directly.

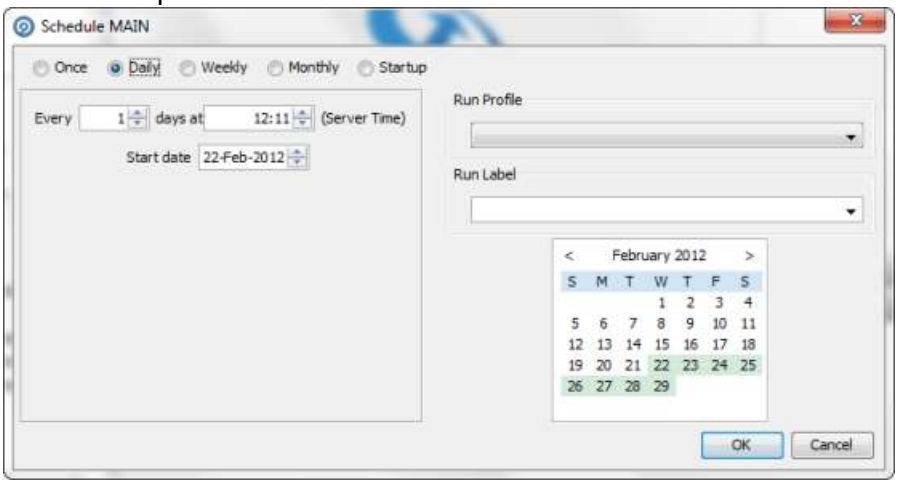
3.4.2 Scheduling a Job

To schedule your selected MAIN job to occur at regular times:

1. Right-click on the job's entry under the job node and select 'Schedule Job…'



2. Configure a schedule for the job by selecting the frequency, start date, and a Run Profile if required. Click **OK** to create the schedule:



NOTE: External scheduling tools can be used to run the Oracle Watchlist Screening processes if required. Jobs can be started by calling OEDQ from a command line interface. See the OEDQ user guide for more information.

3.4.3 Configuring Batch Screening Schedules for Different Matching Types

Some implementations may require different schedules for each kind of screening. For example, suppose an organization requires that Sanctions screening is performed daily, but a weekly schedule is sufficient for PEP and EDD screening. The two MAIN jobs which carry out batch screening each contain three separate batch screening phases. The batch phases cover sanctions, PEP and EDD screening, respectively.

To configure batch screening schedules:

1. Create one copy of the **watchlist-screening** Run Profile for each schedule. Oracle recommends that each copy be given a meaningful name for ease of use.
2. Edit each copy to turn on or off SAN/PEP/EDD screening as required.
3. Use Server Console UI or an external tool to schedule jobs to use the appropriate Run Profile.

3.5 Risk Scoring

Oracle Watchlist Screening includes a mechanism for estimating the relative risk of doing business with a given entity or individual. A risk score is calculated for each individual or entity on each watch list, based on various attributes such as country of residence, operating country, associated regime and so on. For a full description of the risk scores and weightings supplied as defaults with Oracle Watchlist Screening, please refer to Appendix D: Risk scoring reference data.

The risk element score values and weightings supplied with Oracle Watchlist Screening are general defaults only. They should be evaluated and tuned by a risk and compliance expert with knowledge of your business requirements and the relevant legislation.

3.5.1 Adjusting the Risk Scoring Mechanism

Oracle Watchlist Screening calculates a risk score and a PEP risk score for every alert created by the screening processes. The risk score is a relative measure, out of a maximum of 100, of the risk posed by the identified individual or entity. The PEP risk score identifies the relative riskiness of the individual or entity when considered as a PEP, and as such does not apply to sanctions. This may be quite different to the non-PEP risk score. Therefore, the same algorithms are used to derive the risk score and PEP risk score, but the underlying scores and weightings on which the calculations are based are different.

> **NOTE:** The remainder of this section will use the phrase 'risk scores' exclusively. However, the methods and algorithms described apply equally to PEP risk scores.

The overall risk score of a potential match is calculated as a weighted average of the risk scores calculated for the watch list and customer data records which are involved in the match. In turn, both the watch list risk score and customer data risk score are calculated as a weighted average of the risk scores of contributing risk elements. A risk element is a data field, such as country of operation or occupation, which can be assigned a risk score based on its value.

The risk scoring calculation can be customized by adjusting:

- the scores associated with the values of the risk elements; or
- the relative weightings of the risk elements; or
- the relative weight of the watch list risk score and the customer data risk score.

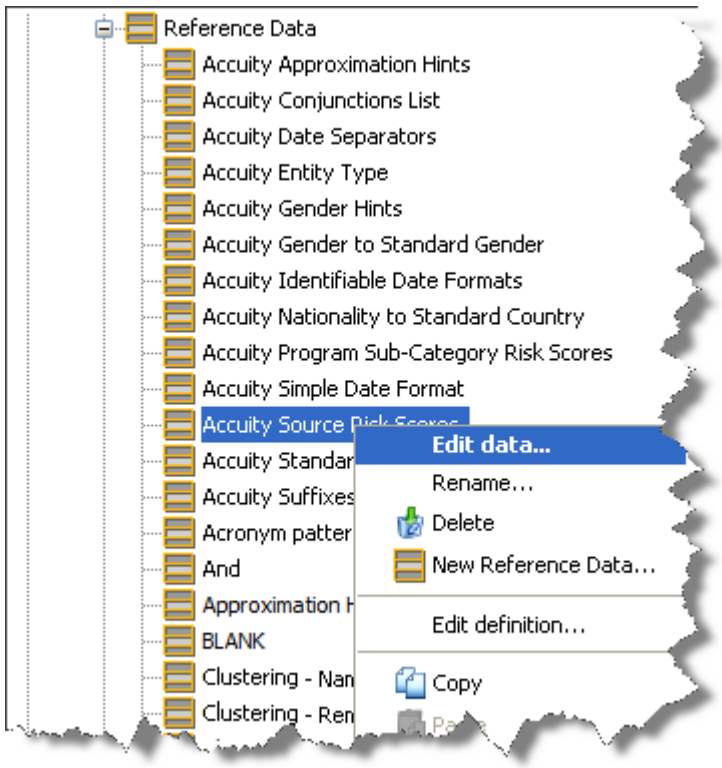
The reference data tables which must be adjusted to fine-tune the risk scoring mechanism depend on which watch lists you are using in your screening processes.

Alternatively, Oracle Watchlist Screening may be integrated with a third party source of watchlist risk scores which can be used to completely replace the in-process risk score calculation.

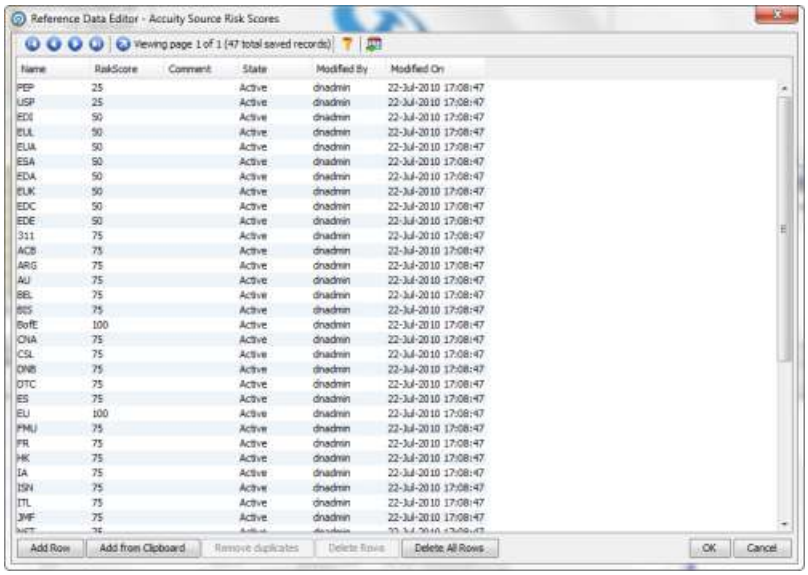
Adjusting the Risk Element Scores

Risk element scores are adjusted by editing reference data directly. The elements that are considered when calculating a risk score for a record depend on the fields that are present in the watch list (or customer) record.

To edit the risk element values, open the Watchlist Management project, double click on the reference data item in the Project Browser, or right-click on the reference data item and select **Edit data…**:



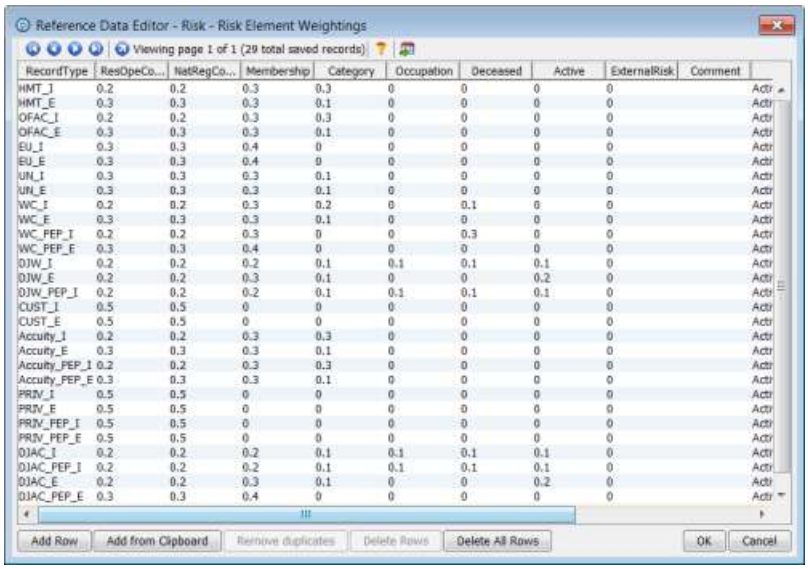
The risk score can then be edited directly in the **Reference Data Editor**:



NOTE: If you edit the risk scores you must re-run the Download, Prepare, Filter and Export All Lists job (in the Watchlist Management project), and then run the MAIN job (in the Watchlist Screening project). Until this is done, the new risk scores will not be reflected in the generated matches.

Adjusting the Risk Element Weightings

Risk element weightings are controlled in a set of reference data named Risk Element Weightings. This reference data set specifies, for each type of record, which fields in that record contribute to the risk score calculation, and to what degree:



Record types are specified as a combination of the originating watch list and a suffix specifying whether the record represents and individual (_I), or an entity (_E). Working records have a record type of CUST_I or CUST_E, respectively.

The **ResOpeCountries** column specifies the weighting for the **Residential Country** field for individuals, or the **Operating Country** field for entities. The **NatRegCountries** column specifies the weighting for the **Nationality Country** field for individuals, or the **Registrations Country** field for entities.

This reference data, which is in the Watchlist Management project, can be edited as described above. The higher the weighting number, the more the corresponding element will contribute to the final score. The weighting scores for each row type should add up to 1.

The overall risk score calculation for a record containing n elements is therefore as follows:

$$\text{Risk Score} = E1w1 + E2w2 + \ldots + Enwn$$

Where the risk element score for element x is represented by E_x, the weighting for element x is represented by w_x, and

$$(w1 + w2 + \ldots + wn = 1).$$

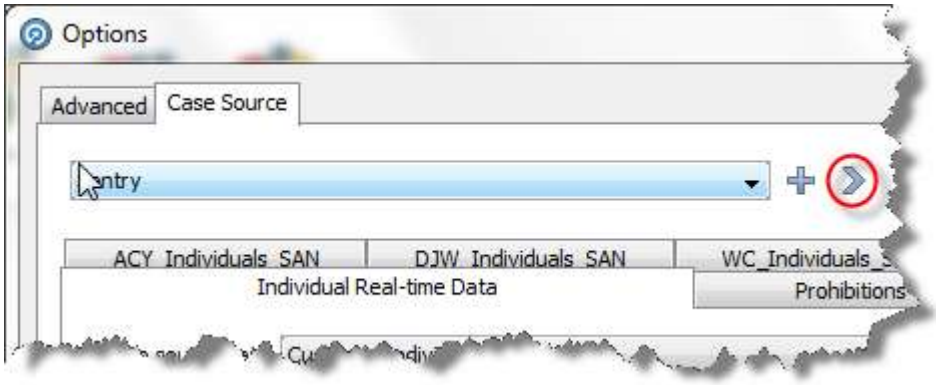
Note that if no data is present for a given element, it is not assumed to have a risk score of zero, but instead will not be included in the risk score calculation.

Adjusting the Watch List and Customer Data Risk Score Weightings for the Combined Risk Score Calculation

The final risk score is calculated as a parameter, which is passed into the alert workflow. The parameter is named matchRiskScore. (The parameter which receives the PEP risk score is named matchRiskScorePEP).

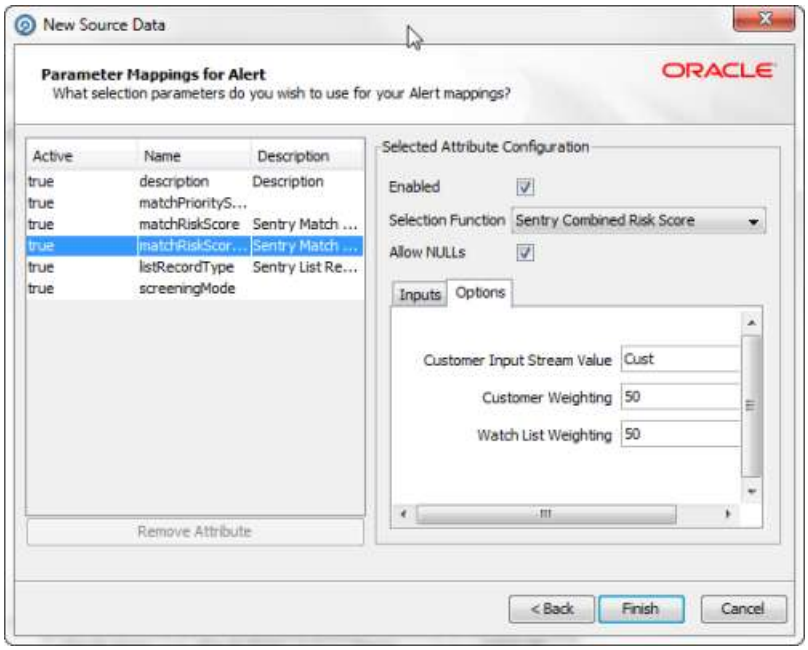
By default, the customer and watch list risk scores contribute equally to the overall risk score.

To edit the watch list and customer data risk score weightings, open the relevant screening process in OEDQ and double-click on the main match processor. Select **Advanced Option** and then the **Case Source** tab. Open the **Case Source Configuration** screen by clicking on the right arrow next to the case source name:



Click **Next** until the **Parameter Mappings for Alert** screen appears.

A special selection function, Sentry Combined Risk Score, is used to calculate the risk score. The options on the risk score can be used to specify the relative contribution, out of 100, of the customer and the watch list risk scores to the overall value. Select the risk score parameter whose configuration you wish to change, then the **Options** sub-tab in the attribute configuration pane:



The Customer Weighting and Watch List Weighting specify the relative contributions of the customer data and the watch list data to the final risk score, respectively, as a score out of 100.

> **NOTE:** You must edit the weightings for the main match processor in every screening process in use in your implementation.

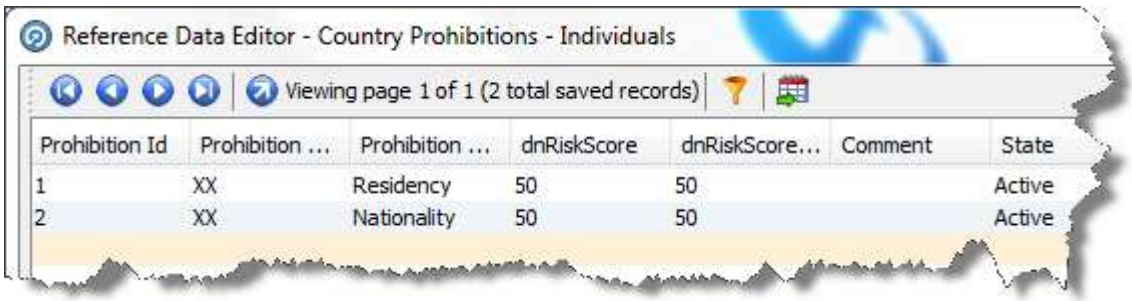
3.6 Country Prohibition Screening

Country prohibition screening involves matching customer data against a list of prohibited countries. The implementation of this additional screening is optional, and is only performed for SAN screening.

3.6.1 Configuring Prohibition Screening

To configure country prohibition screening:

- In the Watchlist Management project, edit the Country Prohibitions - Individuals reference data to configure the required prohibitions for individuals. Each row specifies a Prohibition Id (a unique identifier for the row), the Prohibition Country Code (an ISO-3166-1 two character country code), a risk score value and the Prohibition Type ("Nationality" or "Residency").
- In the Watchlist Management project, edit the Country Prohibitions - Entities reference data to configure the required prohibitions for entities. Valid prohibition types for entities are [country of] Registration and [country of] Operation.



- **NOTE:** If you edit the country prohibitions reference data, you must re-run the Download, Prepare, Filter and Export All Lists job (in the Watchlist Management project), and then run the MAIN job (in the Watchlist Screening project). Until this is done, the amended datawill not be reflected in the generated matches.

3.6.2 Extending Prohibition Screening

Oracle Watchlist Screening, as delivered, allows for prohibition screening against Nationality and Residency for Individuals and [country of] Operation and [country of] Registration for Entities. Additional prohibition types can be added as follows:

- Create new entries in the prohibition reference data with a new Prohibition Type name, for example "Employment Country".
- [Batch screening only] Extend the customer data preparation process to create a new attribute, for example **dnEmploymentCountryCode**.
- Edit the appropriate screening process(es), to create the necessary match rules and clusters for the new attribute.

3.7 Validating The Installation

Oracle Watchlist Screening is provided with a set of sample customer data conforming to the Customer Data Interface (see Appendix E: Sample Customer Data for more details). Once the

Oracle Watchlist Screening components have been installed and configured, you can use the sample customer data to verify that the installation and configuration has been successful.

3.7.1 Testing Reference Data Quality

To test reference data quality - that is the quality of the data from the watch lists - run the 'Analyze Reference Data Quality' job (in the Watchlist Management project). You should run this job from the Server Console user interface (or using the Command Line interface) against the **watchlist-management.properties** run profile, or an edited copy of it. In the **watchlist-management.properties** run profile, you will find a section for each watch list, and within each watch list's section, you will find a group of parameters that control data quality analysis for that watch list. In order to run data quality analysis for a watch list, the values for these parameters should be set to **Y**. Here is an example for the Accuity watch list:

```
# Enable the following lines to run DQ for ACY
phase.DQ\ -\ Stage\ ACY\ reference\ lists.enabled = Y
phase.DQ\ -\ ACY\ reference\ data\ quality\ analysis.enabled = Y
stageddata.DQ\ ACY\ -\ Invalid\ Standard\ Country\ in\ Accuity\
Nationality\ to\ Standard\ Country.visible = Y
stageddata.DQ\ ACY\ -\ Missing\ Source\ in\ Accuity\ Source\ Risk\
Scores\ Reference\ Data.visible = Y
stageddata.DQ\ ACY\ -\ Obsolete\ Source\ in\ Accuity\ Source\ Risk\
Scores\ Reference\ Data.visible = Y
```

Note that, until you edit the **watchlist-management.properties** run profile, all of these parameters will be set to **N**.

The results of the 'Analyze Reference Data Quality' job are written as staged data. You can view them in the Server Console user interface.

3.7.2 Testing Customer Data Quality

To test customer data quality, run the 'Analyze Customer Data Quality' job (in the Watchlist Screening project). You should run this job from the Server Console user interface without a run profile.

The results of the 'Analyze Customer Data Quality' job are written as staged data. You can view them in the Server Console user interface.

3.7.3 Testing Batch Screening

To test batch screening against the sample customer data:

1. Ensure the **Download, Prepare, Filter and Export All Data** job in the **Watchlist Management** project has been run.
2. Run the **Main** job in the **Watchlist Screening** project with a Run Profile configured for batch screening only.

NOTE: Running screening against the sample customer data will result in the creation of Cases and Alerts that should be manually deleted before the implementation is used to screen 'live' data.

Chapter 4: Preparing Customer Data for Screening

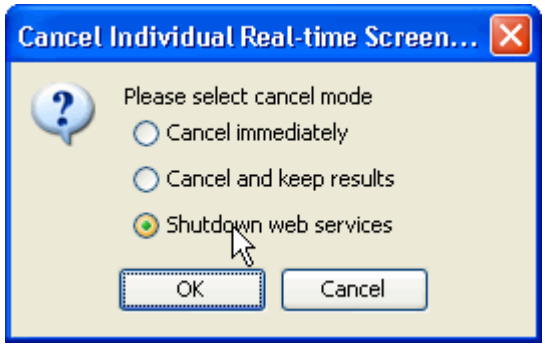
4.1 Real-Time Screening

Real-time screening can be deployed in conjunction with a back-office batch screening approach, allowing the business to screen individuals and entities at the point of data acquisition and on an ongoing basis.

For real-time screening, users enter data to be screened either in the Watchlist Screening UI or in a system integrated with Watchlist Screening web services.

NOTE:

- Real-time screening can only be peformed when the real-time screening job is running.
- If you need to cancel either of the real-time screening processes for any reason other than as part of a scheduled job, it is important that you select the **Shutdown web services** option in the **Cancel** dialog:



4.2 Batch Screening

Batch screening processes are configured to run against the sample data supplied with Oracle Watchlist Screening with minimal additional configuration, allowing the installation to be validated quickly. The sample data used is provided in two files - **customerindividuals.csv** and **customerentities.csv** - in the **config/landingarea/Customer** folder.

The OEDQ Config Folder:
Your OEDQ instance's **config** folder might not be named 'config'. The choice of the config folder's name is made when OEDQ is installed - in some cases a name is automatically allocated. OEDQ release 11g and later has both a 'base' and a 'local' config folder. The base config folder is often called '**oedqhome**', and the local config folder is often called '**oedqlocalhome**'. In some cases, dots or underscores may be inserted into these names (for example: 'oedq_local_home'). Whenever you see a file path in this document that begins with **config**, this always refers to your OEDQ instance's local config folder.

To run batch screening against your own customer data, you need to replace the data in the supplied files with your own. To do this:

1. Transform your customer data into the format specified by the Customer Data Interface (see the Oracle Watchlist Screening Data Interfaces Guide for further information).
2. Replace the data in the **customerindividuals.csv** and **customerentities.csv** files with your transformed customer data.
3. Use the **Analyze Customer Data Quality** job (See "Analyzing Customer Data Quality" below) to evaluate the fitness of your customer data for screening.
4. Amend or improve any customer data rows which display significant data quality issues.

Note: The **customerindividuals.csv** and **customerentities.csv** files must be saved in UTF-8 format.

4.2.1 Analyzing Customer Data Quality

Oracle Watchlist Screening is supplied with a process which checks the data in the customer data files for compliance with the Customer Data Interface (CDI). This process can be run independently of the screening process, and identifies potential issues with the customer data quality which may affect the efficiency of screening.

Running the Data Quality Analysis

To analyze your working customer data:

1. Ensure that your working data has been copied into the **customerindividuals.csv** and **customerentities.csv** files in the **landingarea/Customer** directory.
2. Run the **Analyze Customer Data Quality** job.

The job checks your customer data for any quality issues that may have a negative impact on the screening process. The results of the quality analysis are written as staged data and can be viewed using the Server Console UI.

Data Quality Errors

The error codes and the associated messages that can be raised by the customer data quality analysis are listed in the CDI Error Codes reference data. Each error message is assigned an error severity, from 1 to 4, which corresponds to the likely impact the issue will have on screening efficiency. The error severities are as follows:

Severity code	Description
1	Severe data error which prevents screening.
2	Invalid data which will limit the effectiveness of screening.
3	Missing data which will limit the effectiveness of screening.
4	Invalid data which has no effect on screening. Errors in this category will not affect the output of the match processor, but may cause issues when manually evaluating any potential matches that are raised.

Please refer to the Oracle Watchlist Screening Customer Data Interface Guide for a more complete description of the data quality checks and potential validation errors.

Any rows in your customer data which cause a severity 1 error message to be raised will also be rejected by the screening process. These rows lack data in the core attributes used by the screening process, and so cannot be processed meaningfully.

The screening processes will output rows which cannot be screened into the CUST_Individuals_Invalid staged data or the CUST_Entities_Invalid staged data, as appropriate. The error codes associated with each row will also be written to the database.

Chapter 5: Customizing the Oracle Watchlist Screening User Application

The user interface for the Oracle Watchlist Screening User Application is highly customizable. Many aspects of its appearance and functionality can be altered to fit the needs of your organization. In particular:

- The default Oracle logo and color scheme can be replaced with your company branding (see section 5.2 "Configuring Branding in the Oracle Watchlist Screening User Application");
- The labels and messages displayed to the user during normal operation can all be localized into different languages and customized to your requirements (see section 5.3 "Customizing Application Labels and Messages");
- The data entry interface is highly customizable, and different layouts can be specified on a per-Project basis (see section 5.4.2 "Customizing the Real-Time Screening Input Fields");
- The data items present in the output interface can also be customized on a per-Project basis (see section 5.4.3 "Customizing the Real-Time Screening Output Fields").

5.1 The Oracle Watchlist Screening User Application Customization files

Three types of **.properties** file are used to customize the appearance and behavior of the Oracle Watchlist Screening User Application:

- The **sentryblueprint.properties** file. This file defines the colors and images to be used for branding in the Oracle Watchlist Screening User Application. It also defines the mappings between project identifiers and project names (see section 2.4.1 "Associating the Application with Screening Projects"), and links each project to a user interface layout. A given installation of OEDQ should contain only one version of this file.
- The **layout.properties** files. These files define the user interface layouts used by the Oracle Watchlist Screening User Application. Oracle Watchlist Screening is supplied with one version of this file (**sentryblueprint-default-screening-layout.properties**).
- Each of these files defines a single user interface layout. You can create additional versions of this file as required, and associate them with your screening project or projects in **sentryblueprint.properties**.
- The **sentrymessages.properties** file (which is used by default) and two localized files: **sentrymessages-en.properties** and **sentrymessages-de.properties**. The **sentrymessages-** *localecode***.properties** files. The latter files provide localized versions of the user interface labels and messages.

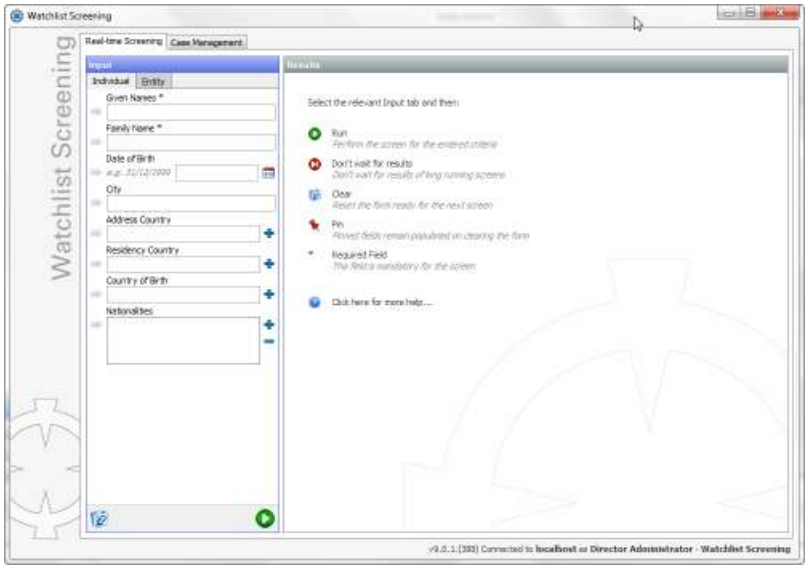
You should create a copy of this file, with appropriate label and field translations, for each locale you wish to support in your version of the Oracle Watchlist Screening User Application. Each copy should be named **sentrymessages-** *localecode***.properties**, with *localecode* being replaced with the locale you wish to support in each case. The file

appropriate to the locale in which the application is running will be selected automatically.

5.2 Configuring Branding in the Oracle Watchlist Screening User Application

The appearance of the Oracle Watchlist Screening User Application can be customized to reflect your company branding. You can customize the background color of the application and select banner images to use, either at the top of the application window or at the left of the window.

By default, the Oracle Watchlist Screening User Application uses a silver background with Oracle Watchlist Screening branding at the left hand side of the application window:



You can also customize many of the labels and messages used by the application. Custom messages and labels are locale-sensitive, so can be overridden based on the locale currently in use by the client computer.

5.2.1 Customizing the Background Color

The background color is specified as a property, `outerbranding.background`, in the **sentryblueprint.properties** file. To change the background color, remove the hash (#) sign from the start of the line containing the `outerbranding.background` property, and specify your desired color. The color is specified as a hexadecimal RGB value.

5.2.2 Customizing the Application Banner

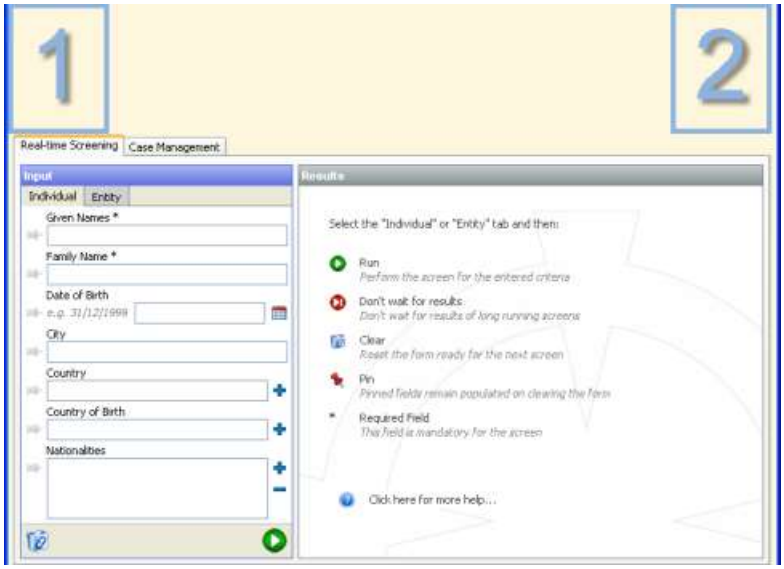
The user interface makes provision for a left-hand banner and a top banner. Images can be pinned to the top or the bottom of the left hand banner, or to the right or the left of the top banner. Pinning an image to an edge means that the image will always remain next to the pinned edge, even if the window is resized. In the default branding layout, the Oracle logo is pinned to the top of the left banner, and the crosshairs logo is pinned to the bottom.

You can specify your own images for use in the banners, and the placement of those images. The left hand banner will adjust its width to accommodate your widest image, and the top banner will adjust its height.

WARNING: Any custom branding images will be deleted when OEDQ is upgraded. Before performing an upgrade, you should ensure that you have backup copies of any custom branding images used by your installation. You will also need to reinstate the branding images to their original location after the upgrade is complete.

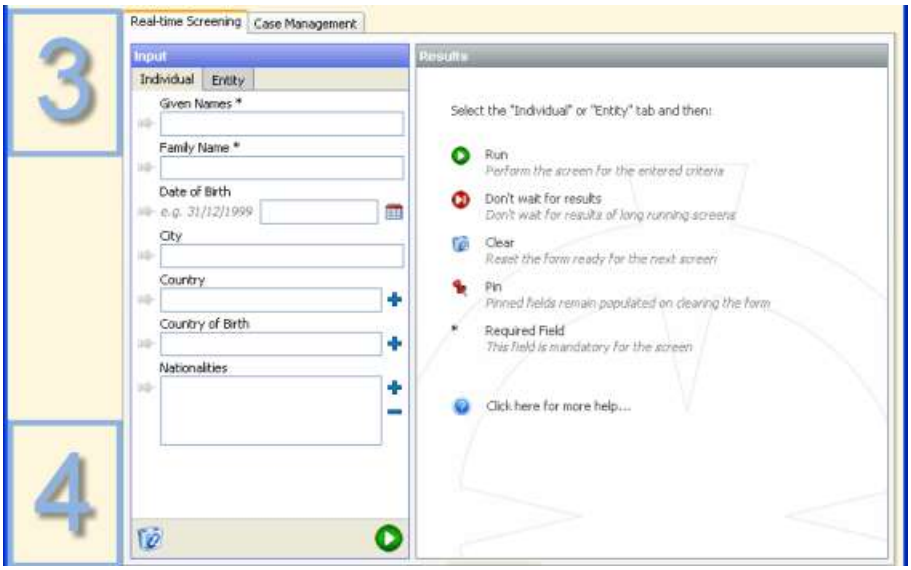
Example – Top Banner

The next figure shows an example of the top banner branding in use. The blue bounded square containing the numeral '1' is pinned to the left of the top banner. The blue bounded square containing the numeral '2' is pinned to the right:



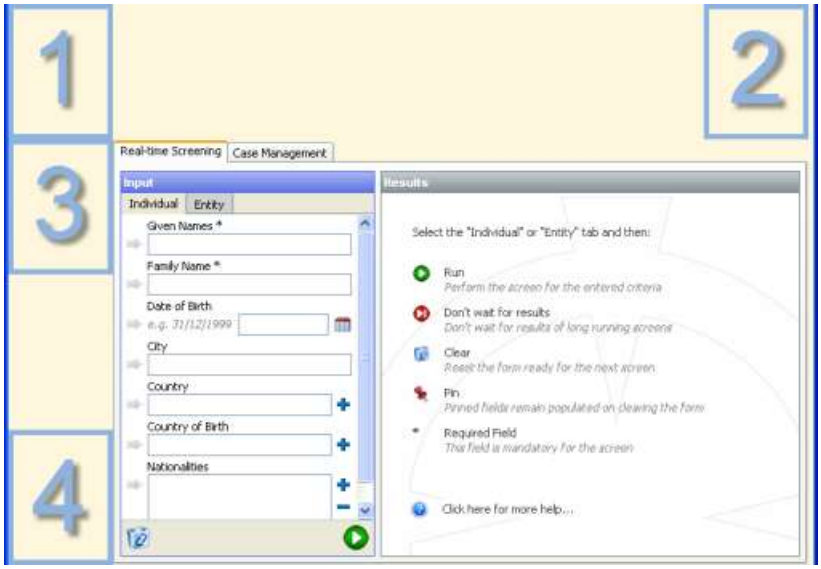
Example – Left Banner

The next figure shows a further example of the left-hand banner branding in use. The blue bounded square containing the numeral '3' is pinned to the top of the banner. The blue bounded square containing the numeral '4' is pinned to the bottom:



Example – Both Banners

Finally, the following figure shows the layout created when both the top and left-hand banners are in use. The top banner sits above both the main area of the screen and the left hand banner, so the image pinned to the left of the top banner sits directly above the image pinned to the top of the left banner:



Specifying Custom Banner Settings

To configure the Oracle Watchlist Screening User Application to use custom branding images:

- Place the images you wish to use in an appropriate location in the Web server directory. For example, if you are using Tomcat, you may create a **sentry** folder in the **images** folder of your OEDQ deployment. That is:

  ~/tomcat/6.0/webapps/dndirector/Images/sentry

- Uncommend and edit the appropriate branding image properties in the **sentryblueprint.properties** file.

The property names used to control the branding images are as follows:

- `leftbranding.imagetop` specifies an image to be pinned to the top of the left banner.
- `leftbranding.imagebottom` specifies an image to be pinned to the bottom of the left banner.
- `topbranding.imageleft` specifies an image to be pinned to the left of the top banner.
- `topbranding.imageright` specifies an image to be pinned to the right of the top banner.

To specify a branding image for a particular location, ensure that the property pertaining to that location is not commented out (that is, the line containing that property does not start with a hash (#) sign). Set the value of the property to the name of the image file you wish to use at that location.

Filenames are specified relative to the root directory of the application in the Web server. If you have placed your branding images in a folder called **sentry** within the **images** folder of your OEDQ deployment, your properties file may look like this:

```
topbranding.imageleft    = */resources/Images/sentry/1.png
topbranding.imageright   = */resources/Images/sentry/2.png
leftbranding.imagetop    = */resources/Images/sentry/3.png
     leftbranding.imagebottom =
         */resources/Images/sentry/4.png
```

If no branding images are required, not even the default ones, remove the hash (#) sign from the start of the `leftbranding` property lines, and leave the filenames, after the equals signs, blank.

> **NOTE:** If you do not wish to use the top banner, you can simply comment out the `topbranding` properties (that is, prefix the line containing the property definition with a hash (#) sign). If you do not wish to use the left banner, you must supply blank filenames for the `leftbranding` properties, or the application will use the default ones.

5.3 Customizing Application Labels and Messages

You can customize the labels on the data entry fields and many of the messages shown when the application is in use. The messages are defined in locale-specific sentrymessages files. The files will be found in the **properties/blueprints** directory under the **config** directory, and are named **sentrymessages_***localecode***.properties**, where *localecode* is the designation of the locale in use. Two sentrymessages files are provided in the standard Oracle Watchlist Screening distribution: **sentrymessages_en.properties**, which is used for English-speaking locales, and **sentrymessages_de.properties**, which is used for German-speaking locales.

If no locale-specific properties file is found for the current locale, the messages in the default file, **sentrymessages.properties**, will be used instead.

Properties are provided to allow you to customize:

- The application title;
- The date format;
- The tab labels; and
- The results messages.

Results messages are provided to alert the user that:

- No matches have been found;
- A single match has been found, and a case created if appropriate;
- Several matches have been found, and a case created if appropriate.

If Case Management is in use and one or more possible matches are found, the message will contain a link to the generated case. If Case Management has been disabled, no case is created and no link is provided. In addition, different versions of the message can be defined for display to data entry users, who cannot view match results, and to power users, who can.

NOTE: Case Management might be disabled on the server or servers that provide the screening web services to the Watchlist Screening User Application, as it is possible to "refer" all matches generated on the screening server(s) to a separate server hosting Case Management in a High Availability environment.

The properties and their uses are as follows:

- `ui.application.title` specifies the name of the application, as displayed in the title bar. This is defined as a plain text string.
- `ui.dateformat` specifies the standard date format to be used by the application.
- `screening.individualsearch.tab.label` specifies the label to be used for the individual screening tab.
- `screening.entitysearch.tab.label` specifies the label to be used for the entity screening tab.
- `screening.status.possibleMatchesSingle.label` specifies the text to be shown to a power user when a single possible match has been identified and Case Management is in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.dataentry.possibleMatchesSingle.label` specifies the text to be shown to a data-entry user when a single possible match has been identified and Case Management is in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.possibleMatchesMulti.label` specifies the text to be shown to a power user when multiple possible matches have been identified and Case Management is in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.dataentry.possibleMatchesMulti.label` specifies the text to be shown to a data-entry user when multiple possible matches have been identified and Case Management is in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.possibleMatchesSingle.label.nocase` specifies the text to be shown to a power user when a single possible match has been identified and Case Management is *not* in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.dataentry.possibleMatchesSingle.label.nocase` specifies the text to be shown to a data-entry user when a single possible match has been identified and Case Management is *not* in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.possibleMatchesMulti.label.nocase` specifies the text to be shown to a power user when multiple possible matches have been identified and Case Management is *not* in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.dataentry.possibleMatchesMulti.label.nocase` specifies the text to be shown to a data-entry user when multiple possible

matches have been identified and Case Management is *not* in use. This label can be defined using a piece of html code, allowing formatting to be specified.

- `screening.status.noMatch.label` specifies the text to be shown to a power user when no matches have been identified and Case Management is in use. This label can be defined using a piece of html code, allowing formatting to be specified.
- `screening.status.dataentry.noMatch.label` specifies the text to be shown to a data-entry user when no matches have been identified. This label can be defined using a piece of html code, allowing formatting to be specified.

5.4 Customizing Interface Layouts

The input fields used to submit data from the Oracle Watchlist Screening User Application to the real-time screening processes, and the output attributes displayed by the User Application after a real-time screen has been run, can all be customized.

User interface layouts are defined in layout configuration files in the **.properties** format. The **sentryblueprint.properties** file specifies which layout configuration file should be used for each project.

Layout configuration files can be specific to a single project, or can be shared between many projects. Each file must specify both input and output field configuration.

A single layout configuration file, **sentryblueprint-default-screening-layout.properties**, is supplied with Oracle Watchlist Screening. It is recommended that you retain an unmodified copy of this file, to facilitate easy reversion to the default configuration if required.

5.4.1 Configuring a New Interface Layout

The following steps describe the actions required to create a new interface layout and associate it with one (or more) of your Oracle Watchlist Screening projects:

- Save a copy of **sentryblueprint-default-screening-layout.properties** with an appropriate name (for the purposes of illustration, we will be using the name **sentryblueprint-edited-screening-layout.properties**).
- Edit the input and output field configuration as described in the following sections, as required. Input field configuration is described in section 5.4.2 "Customizing the Real-Time Screening Input Fields", and output field configuration in section 5.4.3 "Customizing the Real-Time Screening Output Fields".
- Add a layout identifier to be used with your new layout to the list in **sentryblueprint.properties**. This is an arbitrary value, but should be easy to associate with the layout file, for example:

  ```
  ui.screening.layouts =
  defaultScreeningLayout,editedScreeningLayout
  ```

- Add a row into **sentryblueprint.properties** to associate the new layout identifier with its layout configuration file. In our example case, this will appear as follows :

  ```
  ui.editedScreeningLayout.properties = sentryblueprint-edited-
  screening-layout
  ```

Note that the left hand side of the assignment takes the form `ui.<layoutIdentifier>.properties`, and the value assigned to it is the file name of the layout configuration file, minus the **.properties** extension.

- Edit the project details contained in **sentryblueprint.properties** to associate the new layout with the required projects. The statements which perform this function take the form:

  `<projectIdentifier>.ui.screening.layout = <layoutIdentifier>`

For example, to associate a project with the identifier **France** with our new layout configuration, we would use the following assignment:

```
France.ui.screening.layout = editedScreeningLayout
```

5.4.2 Customizing the Real-Time Screening Input Fields

The following aspects of the data entry interface can be configured:

- Which data entry tabs are available to the users;
- Which controls are present on the tabs, and the order in which they appear;
- The labels used for each control;
- Whether data entry is optional or mandatory for each control presented.

Additionally, the method of data entry can be specified for the custom String input fields. You can select:

- single line free text;
- multi-line free text;
- single-select picklists;
- multi-select picklists;
- radio buttons; or
- check boxes.

This allows you to mandate that any values supplied for these fields are drawn from a discrete set of values fitting the requirements of your organization.

The Customer Data Interface provides two pre-defined sets of input attributes for real-time screening: one for individuals and one for entities. In addition, fifty customizable input fields (forty string fields, five number fields and five date fields) are provided for each set of input attributes.

The next two sections detail the configuration options available for all the input fields, and an example of their use. The additional options available for the customizable string fields are addressed in Configuring Custom String Input Fields.

For a full description of the pre-defined input attributes, please see the Customer Data Interface Guide, which is provided as part of the Oracle Watchlist Screening distribution.

Controlling the Data Entry Tabs

The Oracle Watchlist Screening User Application provides two tabs within its data entry interface: one for entering individual data, and one for entering entity data. Either or both of the tabs can be removed from the user interface if required, and custom, localized labels can be defined for the tabs (see section 5.3 "Customizing Application Labels and Messages").

To hide the individual data entry tab, include the following line in the layout configuration file:

```
screening.individual.tab.required = N
```

To hide the Entity data entry tab, include the following line in the layout configuration file:

```
screening.entity.tab.required = N
```

Both these lines are included in the default layout configuration file, but are inactivated by placing a hash mark (#) at the beginning of the line. If you have created your layout configuration file by copying the default file, you can activate either one of these lines by simply removing the hash mark.

The Input Field Configuration Format

Each input field for each attribute is controlled by a set of properties in the **layout.properties** file.

The property names for individual screening are constructed as follows:

```
screening.individual.inputfield.<fieldName>.<propertyName>
```

The property names for entity screening are constructed as follows:

```
screening.entity.inputfield.<fieldName>.<propertyName>
```

NOTE: You *must* specify a value for all three input field properties (`label`, `order` and `required`) if you wish it to be displayed. Input fields are only shown for attributes that have properties defined.

If you do not wish to display an input field for an attribute, simply comment out the properties for that attribute by prefixing the line with a hash mark (#).

The value supplied for the field name specifies which input field is being configured. The value specified for property name specifies which property is being set. Three properties are available for each input field:

Property name	Description
`label`	This property, which is optional, specifies a localized label to be used for the input field. Labels are specified as a reference to a property in an **sentrymessages** file (see Tip, below). **Note**: This property only affects the label that is displayed for the input field. The data columns passed back out via Case Management will be labeled with the field names defined in the case source. Follow the instructions in section 3.3 "Configuring Case Management" to ensure that the case source labels match the input labels.
`required`	This property specifies whether or not a value must be supplied for that attribute. It can take values of 'Y' (a value is required), or 'N' (specifying a value is optional). Required attributes are tagged with an asterisk (*) in the user interface, and if you attempt to run a screen without supplying a value for a required attribute an error message will be

Property name	Description
	 shown, for example:
`order`	This property determines the position of the input field on the screen relative to the other fields. Field order is specified as an integer, and fields which are assigned lower numbers appear first in the layout. The numbers used to specify the order do not have to be contiguous (that is, there can be gaps in the sequence).

TIP: References to another property are specified by a percentage sign (%) followed by the property name. For example, the following property definition specifies that the label for the first custom string input field used for individual screening is defined by the `screening.individual.inputfield.customString1` property in the appropriate **sentrymessages** file:

```
screening.individual.inputfield.customString1.label
=%screening.individual.inputfield.customString1
```

Default label values are provided in the **sentrymessages** file for the custom input fields; the default values for the standard fields are implicit. However, you can override the labels for any of the input fields by adding, or editing, the `label` properties in the **sentrymessages** files.

Example: Input Field Configuration

Consider the following snippet of the **sentryblueprint-default-screening-layout.properties** file:

```
screening.individual.inputfield.fullName.order = 30
screening.individual.inputfield.fullName.required = Y
screening.individual.inputfield.fullName.label = %screening.individual.inputfield.fullName
#screening.individual.inputfield.familyName.order = 50
#screening.individual.inputfield.familyName.required = Y
screening.individual.inputfield.dateOfBirth.order = 60
screening.individual.inputfield.dateOfBirth.required = N
screening.individual.inputfield.city.order = 120
screening.individual.inputfield.city.required = N
#screening.individual.inputfield.postalCode.order = 14
#screening.individual.inputfield.postalCode.required = N
screening.individual.inputfield.addressCountryCode.order = 140
screening.individual.inputfield.addressCountryCode.required = N
screening.individual.inputfield.countryOfBirthCode.order = 150
screening.individual.inputfield.countryOfBirthCode.required = N
screening.individual.inputfield.nationalityCountryCodes.order = 160
screening.individual.inputfield.nationalityCountryCodes.required = N
```

If this defines all the input attribute fields for the application, and the property `screening.individual.inputfield.fullName` has been defined as 'Applicant name' in the **sentrymessages** file, the application will look like this:

Comparing the code against the user interface, we can notice that:

- The order attributes do not start at 1 and are not contiguous. However, there are no gaps in the user interface display. The order numbers specified in the properties file shipped with Oracle Watchlist Screening are intentionally spaced widely apart, to allow for easier insertion and re-ordering of fields.
- The first field, which represents the `fullName` input attribute, is labeled 'Applicant name', as determined by the label property and the corresponding **sentrymessages** file. The other fields do not have custom label properties, and so are displayed with their default labels.
- The label on the first field includes an asterisk (*), showing that the user must supply data in this field.
- Although properties for the `familyName` and `postalCode` fields appear to be present in the definition, fields are not shown in the interface. This is because the properties have been commented out, and so are ignored by the application.

Configuring Custom String Input Fields

The entity screening and individual screening input interfaces both include forty custom string input fields. In addition to the control offered by the properties described in The Input Field Configuration Format, the data entry method of the custom string fields can be selected from the following options:

- **Single line of text** is the format used for the standard string entry fields. A single line text box is presented to the user, allowing input of free text values.

- **Multi-line text** is used to facilitate the input of longer sections of free text (up to 2,000 characters in length). A single line text box plus a button is presented to the user. The text box will display the first section of any text value set in the control. The button is used to open a popup window, which is used to edit the text value.

Note: Both single and multi-line text input fields support values up to 2,000 characters in length. It is usually most convenient for the user to have single-line controls where short values are expected, and multi-line controls where longer sections of text are expected.

- **Radio buttons** can be used to allow the user to select one value from a pre-defined set. The pre-defined values are stored in a picklist Reference Data set; See "Customizing the Real-Time Screening Input Fields" for further information. The maximum number of items that can be presented using a radio button control is 20.
- **Check boxes** are also used to allow the user to select from a list of pre-defined items. They differ from radio buttons in that check boxes allow multiple items to be selected. The maximum number of items that can be presented using a check box control is 20.
- **Single selection picklists** also allow the user to select a single value from a pre-defined list of items. If your list of items is relatively short, the decision to use a picklist or a radio control is largely a matter of preference. For longer lists, containing more than 20 items, a picklist must be used.
- **Multiple selection picklists** allow the user to select several items from a pre-defined list of items. If your list of items is relatively short, the decision to use a picklist or a set of checkboxes is largely a matter of preference. For longer lists, containing more than 20 items, a picklist must be used.

Property name	Description
`picklistID`	This property specifies the name of a JMP file that must exist in the **landingarea/sentryrefdata** subfolder on the server. Note that you should not specify the .jmp extension (e.g. you can enter a value of **countries**, but not **countries.jmp**).
`delimiter`	This property specifies the character to be used as a delimiter between values submitted from multi-select controls. If it is not specified in the properties file, a default delimiter of a single space will be used. This property is only significant when an entry method is used which allows multiple selections to be made (that is, `check_boxes` or `multi_select`).
`entrymethod`	This property controls the basic appearance and behavior of the entry field. The following options are available: **check_boxes** Display a group of check boxes for the available items. Multiple selections are possible. The items are defined in the picklist Reference Data set specified by the `picklistID` property for the field. **multi_line_text** Display a text box with a multi-line popup dialog, allowing the entry of free text values up to 2,000 characters in length. **multi_select** Display a picklist control containing the available items. Multiple selections are possible. The items are defined in the picklist

Property name	Description	
		Reference Data set specified by the `picklistID` property for the field.
	radio_buttons	Display a group of radio buttons for the available items. Only single selections are possible. The items are defined in the picklist Reference Data set specified by the `picklistID` property for the field.
	pick_list	Display a picklist control containing the available items. Only single selections are possible. The items are defined in the picklist Reference Data set specified by the `picklistID` property for the field.
	single_line_text	Display a single line text box allowing the entry of free text values. Values can be up to 2,000 characters in length, but this control is better suited to inputting shorter values. The multi-line text box should be used if longer values are expected for a given field.

Configuring Picklist Data

Using picklists, radio buttons and check boxes allows you to standardize the data input to the application by providing a set number of valid items that can be selected for input.

The items provided for all these data entry methods are configured using Reference Data sets in the Watchlist Management project. There are three such sets available by default:

- Labels - PICKLIST - Countries
- Labels - PICKLIST - Genders
- Labels - PICKLIST - Templates

The Countries and Genders picklists can be used as they are, or customized as required. The Templates picklist is an example of a custom picklist. These Reference Data sets can be edited or copied and renamed to create new custom picklists.

NOTE: The **Download, Prepare, Filter and Export All lists** job must be run to export these Reference Data sets as .JMP files to the **landingarea/sentryrefdata** folder, so that they will be displayed in the Watchlist Screening UI. The job must be re-run to update the .JMP files if the picklists are edited or a new picklist is created.

To create a new Reference Data picklist:

1. Copy one of the Picklist Reference Data sets.
2. Assign the set a name in the format "Labels - PICKLIST - *<List Name>*

To edit a picklist:

1. Locate the Reference Data set in the Reference Data subfolder of the Watchlist Management project.
2. Double-click the Reference Data set. The **Reference Data Editor** dialog is displayed.
3. Populate the **Code** and **Label** columns. The **Code** column will contain the value which is actually passed into the screening processes for the specified field (for example, USD). The **Label** column will contain the value which is to be displayed to the user (for example, US Dollars).

TIP: Labels can be specified as a reference to a localized value in a **messages.properties** file. To do this, the value in the **Label** column should have the following form:

%*<listname>*.*<codevalue>*.label

where *<listname>* is the name of the values list, and *<codevalue>* is the corresponding data value to be passed into the screening process.

Then, place a line defining the value of *<listname>*.*<codevalue>*.label in each of the **messages.properties** files in use. For example, the following line defines the label to show for the code USD, in the list called Currency:

Currency.USD.label = US Dollars

Picklist values are displayed in alphabetical order in the Watchlist Screening UI by default. To set a different order, use the following procedure:

1. Open the picklist and assign numeric values in the Order column against each item. The values should be assigned in ascending order, i.e. the value to appear first in the picklist should have the lowest value, and so on.
2. Add the following line to the **layout.properties** file (or files) which will reference this value: screening.sort.pickList.<list name>= N

Example: Input Field Configuration with Picklists

Consider the following snippet of a layout configuration file:

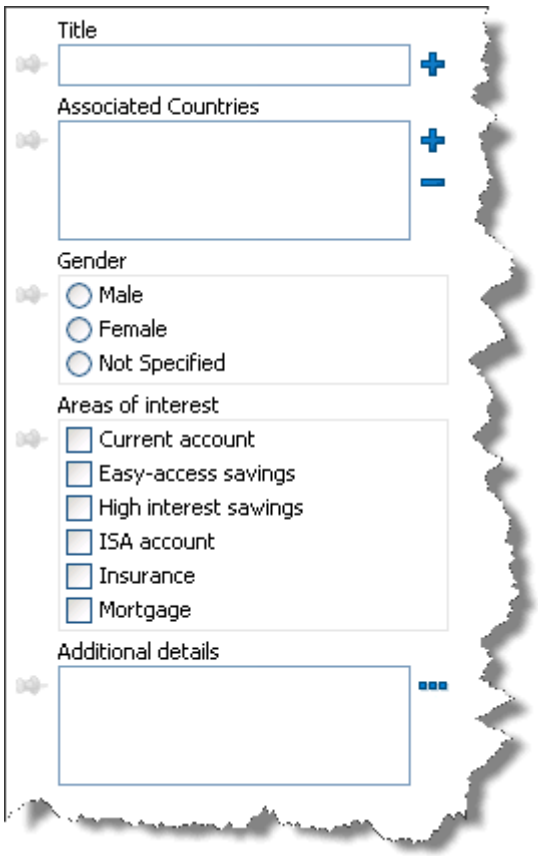
```
# Custom Input Fields - Individuals screening.individual.inputfield.customString1.label =
%screening.individual.inputfield.customString1
screening.individual.inputfield.customString1.order = 300
screening.individual.inputfield.customString1.required = N
screening.individual.inputfield.customString1.picklistID = Genders
screening.individual.inputfield.customString1.entrymethod = pick_list
screening.individual.inputfield.customString1.delimiter =
screening.individual.inputfield.customString2.label =
%screening.individual.inputfield.customString2
screening.individual.inputfield.customString2.order = 310
screening.individual.inputfield.customString2.required = N
screening.individual.inputfield.customString2.picklistID = Template
screening.individual.inputfield.customString2.entrymethod = multi_select
screening.individual.inputfield.customString2.delimiter = ;
screening.individual.inputfield.customString3.label =
%screening.individual.inputfield.customString3
screening.individual.inputfield.customString3.order = 320
screening.individual.inputfield.customString3.required = N
screening.individual.inputfield.customString3.picklistID = Template
screening.individual.inputfield.customString3.entrymethod = radio_buttons
screening.individual.inputfield.customString3.delimiter =
screening.individual.inputfield.customString4.label =
%screening.individual.inputfield.customString4
```

screening.individual.inputfield.customString4.order = 330
screening.individual.inputfield.customString4.required = N
screening.individual.inputfield.customString4.picklistID = Template
screening.individual.inputfield.customString4.entrymethod = check_boxes
screening.individual.inputfield.customString4.delimiter =
screening.individual.inputfield.customString5.label =
%screening.individual.inputfield.customString5
screening.individual.inputfield.customString5.order = 340
screening.individual.inputfield.customString5.required = N
screening.individual.inputfield.customString5.picklistID =
screening.individual.inputfield.customString5.entrymethod = multi_line_text
screening.individual.inputfield.customString5.delimiter =

And the corresponding label definitions from a **sentrymessages** file:

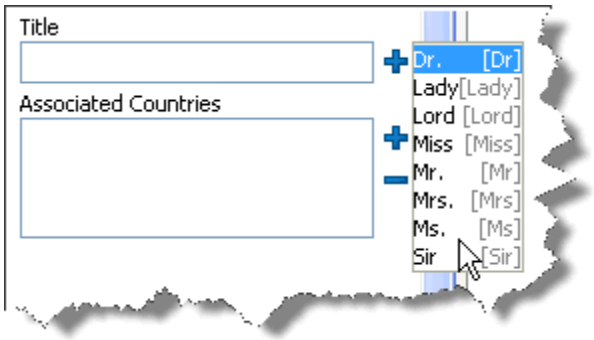
 # Real-time screening individual input field labels - Custom fields
screening.individual.inputfield.customString1 = Title
screening.individual.inputfield.customString2 = Associated Countries
screening.individual.inputfield.customString3 = Gender
screening.individual.inputfield.customString4 = Areas of interest
screening.individual.inputfield.customString5 = Additional details

These configuration options will result in an application layout similar to the following:

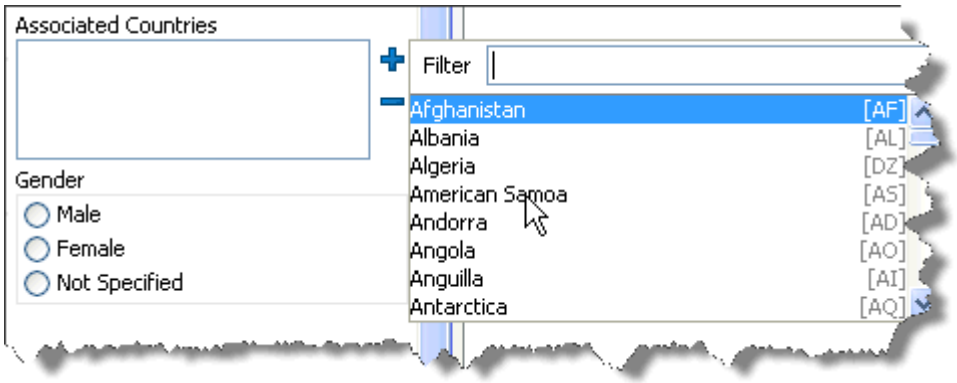


Comparing the code against the user interface, we can notice that:

- The first field, corresponding to `CustomString1`, is labeled 'Title'. As indicated by the plus button next to it, it is a picklist. Clicking on the picklist displays a filterable list of the available items:



- The second field, corresponding to CustomString2, is labeled 'Associated Countries'. As indicated by its size and the plus and minus buttons next to it, it is a multiple selection picklist. Clicking on the picklist displays a filterable list of the available items:



- The third field, corresponding to CustomString3, is labeled 'Gender', and is displayed as a set of three radio buttons, representing the available items. Only one of the radio buttons can be selected at any one time.
- The fourth field, corresponding to CustomString4, is labeled 'Areas of interest', and is displayed as a set of check boxes, representing the available items. It is possible for none, one or many of the radio buttons to be selected at any one time.
- The fifth field, corresponding to CustomString5, is labeled 'Additional details'. As indicated by its size and the ellipsis button, it is a multiple-line text entry field. Clicking on the ellipsis button causes a text entry dialog to be displayed.

5.4.3 Customizing the Real-Time Screening Output Fields

The Oracle Watchlist Screening User Application allows you to define which attributes, output from the real-time screening processes, are displayed for each potential match in the user interface, and in which order. You can also specify whether or not a (localized) field label is displayed for any given item of information, and specify a separator to be used between items in the match details, where appropriate. All settings that apply to data from the watch lists can be set globally, and overridden for individual lists, as required.

Each potential match is displayed with a set of summary information and a list of more detailed pieces of information:

The output fields are controlled by adjusting the settings in the Oracle Watchlist Screening layout properties file.

The Output Field Configuration Format

Each output field is controlled by a set of properties in the Oracle Watchlist Screening layout properties file. The property names for individual screening are constructed as follows:

```
screening.individual.outputfield.[listName].<fieldName>.<propertyName>
```

The property names for entity screening are constructed as follows:

```
screening.entity.outputfield.[listName].<fieldName>.<propertyName>
```

The value supplied for the `fieldName` specifies which output field is being configured. The value specified for `propertyName` specifies which property is being set.

Supplying a value for `listName` is optional, and allows override settings to be specified on a per-list basis. Properties which do not include a `listName` value are applied to all results from lists which do not have override settings defined.

> **NOTE:** Override settings for a list are only used if the list name is also included in the applicable `overriddenlists` property. Two of these properties exist: `screening.individual.outputfield.overriddenlists` applies to individual real-time screening, and `screening.entity.outputfield.overriddenlists` applies to entity real-time screening. Each specifies the set of lists which have active display override settings.

Each output field is represented by a set of properties, which control the way in which the information from that output field is presented:

Property Name	Description
`order`	The `order` property determines the position of the output field relative to the other fields. Field order is specified as an integer, and fields which are assigned lower numbers appear first in the layout. The numbers used to specify the order do not have to be contiguous (that is, there can be gaps in the sequence). The order of fields in the summary is independent of the fields in the details, although the numbers in the `order` field should all be unique.
`suffix`	This property specifies a localized label which should be displayed immediately after the field value. If no suffix is specified, then a semi-colon

Property Name	Description
	will be used by default. Note: the suffix is not used for detail fields when the list view layout is selected.
insummary	This property controls the contents of the summary record, and should be set to Y or N. If it is set to Y, then the information from the output field will be included in the summary, instead of in the details list. If no value is specified for this property, it is assumed to be 'N'.
showlabel	The order property specifies whether or not the output field label should be displayed, and should be set to Y or N. If it is set to Y, then the value of the output field will be prefixed with the field label. If no value is specified for this property, it is assumed to be 'N'.
alwaysdisplaylabel	This property specifies whether the output field label should be displayed even if the field contains no data for this record. It should be set to Y or N. If it is set to Y, then the label of the output field will be displayed even if the value of the output field is empty. If no value is specified for this property, it is assumed to be 'N'. This property is only considered if showlabel is set to 'Y'.
label	This property specifies a localized label to be used for the output field. Labels are specified as a reference to a property in an sentrymessages file. References to another property are specified by a percentage sign (%) followed by the property name. For example, the following property definition specifies that the full name output field used for individual screening should be labeled with the string property defined by the screening.individual.outputfield.listFullName property in the appropriate sentrymessages file: screening.individual.outputfield.listFullName.label= %screening.individual.outputfield.listFullName Default label values are provided for the output fields, and can be overridden by using the sentrymessages files.

Configuring the Summary Information

The match summary information is made up of selected output fields with optional, configurable, separators. The data from each output field will automatically be separated from the previous field with a space, in addition to any suffix supplied. To include an output field in the summary:

- Set the insummary property for the field to 'Y'.
- Consider setting the showlabel property for the field to 'N'. Fields included in the summary are generally self-explanatory, and including the labels can confuse rather than clarify the display.
- Set a value for the order property that will place the field in an appropriate place relative to the other records in the summary.
- Set a value for the suffix property which will provide an appropriate separator between this output field and the next one in the summary order.

Configuring the Match Details Information

The match details information is made up of selected output fields with optional, configurable, separators. The data from each output field will automatically be separated from the previous field with a space, in addition to any suffix supplied. To include an output field in the match details:

1. Set the insummary property for the field to 'N', or delete it.
2. Set a value for the order property that will place the field in an appropriate place relative to the other records in the details.
3. Set a value for the suffix property which will provide an appropriate separator between this output field and the next one. Suffixes are only used when the wrap view is selected in the user interface.
4. Set values for any other properties as required for the field.

Excluding an Output Field from the Display

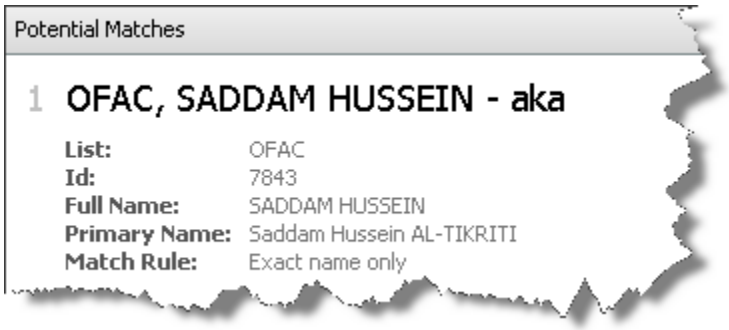
To exclude a field from the display, comment out all of its properties in the Oracle Watchlist Screening layout properties file. That is, place a hash (#) mark at the beginning of each line that defines a property for that output field.

Example: Output Field Configuration

Consider the following snippet of the Oracle Watchlist Screening layout properties file:

```
screening.individual.outputfield.listFeedId.insummary = Y
screening.individual.outputfield.listFeedId.order = 1
screening.individual.outputfield.listFeedId.suffix = %comma
screening.individual.outputfield.listGivenNames.insummary = Y
screening.individual.outputfield.listGivenNames.order = 2
screening.individual.outputfield.listGivenNames.suffix = %empty
screening.individual.outputfield.listFamilyName.insummary = Y
screening.individual.outputfield.listFamilyName.order = 3
screening.individual.outputfield.listFamilyName.suffix =
%spacehyphen
screening.individual.outputfield.listNameType.insummary = Y
screening.individual.outputfield.listNameType.order = 4
screening.individual.outputfield.listNameType.suffix = %empty
screening.individual.outputfield.listFeedName.showlabel = Y
screening.individual.outputfield.listFeedName.order = 5
screening.individual.outputfield.listId.showlabel = Y
screening.individual.outputfield.listId.order = 6
screening.individual.outputfield.listFullName.showlabel = Y
screening.individual.outputfield.listFullName.order = 7
screening.individual.outputfield.listPrimaryName.showlabel = Y
screening.individual.outputfield.listPrimaryName.order = 8
screening.individual.outputfield.listDOB.showlabel = Y
screening.individual.outputfield.listDOB.order = 9
screening.individual.outputfield.matchRule.showlabel = Y
screening.individual.outputfield.matchRule.order = 14
#screening.individual.outputfield.matchScore.showlabel = Y
#screening.individual.outputfield.matchScore.insummary = N
#screening.individual.outputfield.matchScore.order = 15
```

Using this configuration, a possible match returned by the application may look like this (with list view active):



Comparing the property definitions against the user interface, we can notice that:

- The summary uses a comma as the suffix for the list ID, and a space plus a hyphen as a suffix for the list name and the family name.
- The name of the individual is included in the summary by displaying the given name plus a space suffix, followed by the family name.
- Although a date of birth field is specified for inclusion in the details, it does not appear in the output, because there is no data to populate it and `alwaysdisplaylabel` is not set.
- Although properties for the match score field appear to be present in the display definition, the field is not shown in the interface. This is because the properties have been commented out, and so are ignored by the application.

5.5 Customizing the Screening Receipt

When a Real-Time screening search is performed, whether or not a match is returned:

- a Screening Reference ID - a unique identifier of the screening instance - is created; and
- a Screening Receipt - a PDF document containing information about the screening - can be generated.

The exact format and content of the Screening Reference ID and Receipt is controlled using the options detailed in the following sections.

5.5.1 Screening Reference ID

The Screening Reference ID is supplied in the following format: **PRE-YYYYMM-DDHHMM-UCHASH-SUF**

- PRE - Prefix specified in the `watchlist-screening.properties` Run Profile.
- YYYYMM - The server-derived year and month.
- DDHHMM - The server-derived day and time (in hours and minutes).
- UCHASH - A six-character alphanumeric upper-case hash of the Real-Time request content and User ID.
- SUF - Suffix specified in the `watchlist-screening.properties` Run Profile.

The prefix and suffix are optional, and therefore may not always be displayed.

Setting the Prefix and Suffix

The Screening Reference ID prefix and suffix are controlled with the settings in the **Screening Reference** section of the `watchlist-screening.properties` Run Profile.

By default, these values are set as follows:

- `phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.screening_reference_prefix = OWS`
- `phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.screening_reference_suffix = IND`
- `phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.screening_reference_prefix = OWS`
- `phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.screening_reference_suffix = ENT`

To change a suffix or prefix, simply replace the corresponding default three-letter value. Alternatively, delete the default value and leave blank to remove the prefix or suffix.

5.5.2 Screening Receipt

The Screening Receipt provides (electronic or printed) documentary proof that the correct details were screened. This may be useful in a number of scenarios, such as providing paperwork for a customer onboarding process.

The Screening Receipt is only visible to those user groups assigned the **Sentry: View Real-Time Screening Receipt** permission.

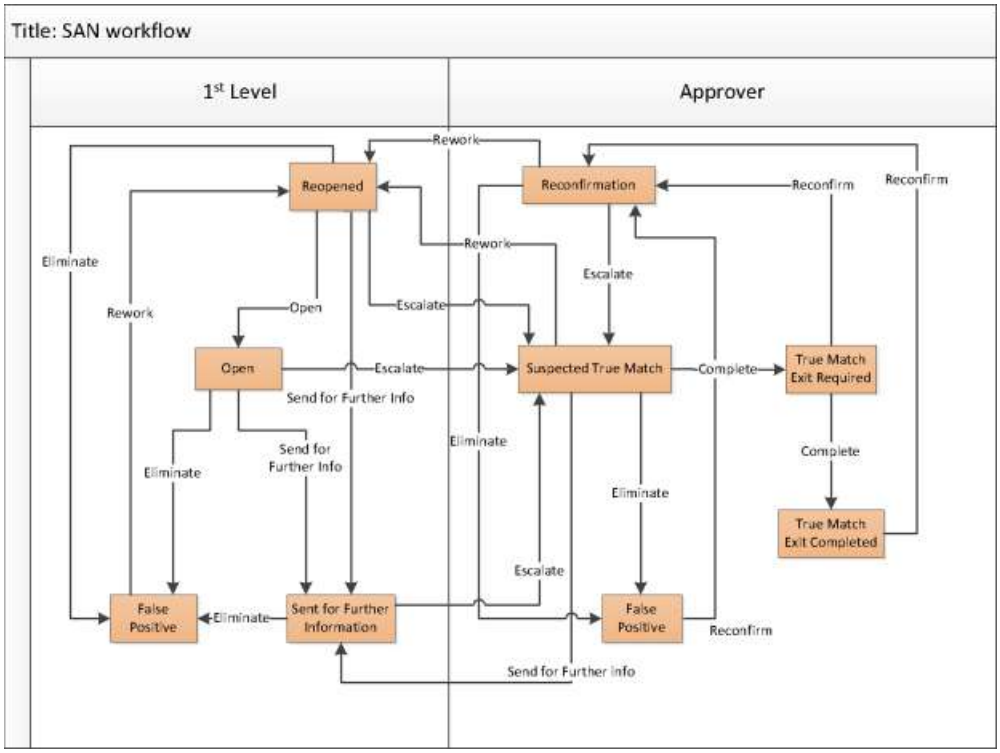
The `sentryblueprint-default-screening-layout.properties` file allows the administrator to:

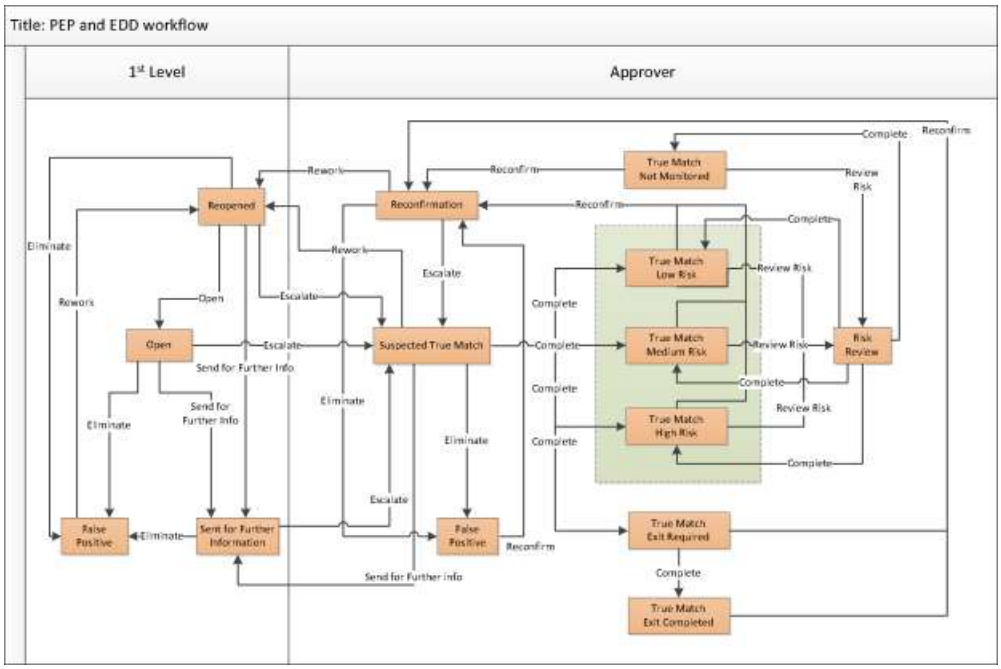
- globally turn on or off the **Show Receipt** and **Save Receipt** buttons on the **Results** pane of the Oracle Watchlist Screening UI;
- control the page size, format and standard content of the Screening Receipt PDF; and
- include or exclude information on a field-by-field basis.

See the comments in the `sentryblueprint-default-screening-layout.properties` file for further information.

Appendix A: Watchlist Workflow Diagrams

The **sentry-alert-workflow.dxic** workflow handles alerts as follows:





Appendix B: Pre-Configured Watch List Information

This appendix contains details of each of the pre-configured watch lists that can be used by Oracle Watchlist Screening:

- HM Treasury
- OFAC
- EU consolidated list
- UN consolidated list
- World-Check
- Dow Jones Watchlist
- Down Jones Anti-Corruption List
- Accuity

B.1 HM Treasury Reference Data

The HM Treasury publishes a sanctions list that can be used for screening in Oracle Watchlist Screening. The sanctions list provides "…a consolidated list of targets listed by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes" .

The HM Treasury website provides more details about the list at:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

Oracle Watchlist Screening uses the list in a semi-colon delimited form. It can be downloaded from:

http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.csv.

B.2 OFAC Reference Data

The US Treasury website states that: "The US Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction." More details on the OFAC list can be found on the US Treasury website, at:

http://www.treasury.gov/ofac/

Oracle Watchlist Screening supports two lists that are produced by OFAC:

- The OFAC Specially Designated Nationals (SDN) list, which is available for download in three separate parts from the following links:

  https://www.treasury.gov/ofac/downloads/sdn.csv

  https://www.treasury.gov/ofac/downloads/add.csv

  https://www.treasury.gov/ofac/downloads/alt.csv

- The OFAC Consolidated Sanctions List, which can be downloaded in three separate parts from the following links:

  https://www.treasury.gov/ofac/downloads/consolidated/cons_prim.csv

  https://www.treasury.gov/ofac/downloads/consolidated/cons_add.csv

  https://www.treasury.gov/ofac/downloads/consolidated/cons_alt.csv

B.3 EU Reference Data

The European Union applies sanctions or restrictive measures in pursuit of the specific objectives of the Common Foreign and Security Policy (CFSP) as set out in Article 11 of the Treaty on European Union.

The European Commission offers a consolidated list containing the names and identification details of all persons, groups and entities targeted by these financial restrictions. See the European Commission website for more details:

http://eeas.europa.eu/cfsp/sanctions/index_en.htm

The consolidated list can be downloaded from the following link:

http://ec.europa.eu/external_relations/cfsp/sanctions/list/version4/global/global.xml

B.4 UN Reference Data

The United Nations consolidated list includes all individuals and entities subject to sanctions measures imposed by the Security Council.

Details are here: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

Download link is:
https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/consolidated.xml

B.5 World-Check Reference Data

World-Check provides a subscription based service, offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the HM Treasury, OFAC, and other world lists. Three levels of subscription are provided: Standard, Premium and Premium+. Some features of the World-Check lists are only available to users with a higher subscription level.

To download the World-Check Premium+ feed, set values in the **WC Setup** section of the `watchlist-management.properties` Run Profile as follows:

```
phase.WC\ -\ Download.enabled = Y
phase.WC\ -\ Download\ native\ aliases.enabled = Y
phase.WC\ -\ Stage\ reference\ lists.enabled = Y
phase.*.snapshot.*.use_native_aliases = 1
```

To download the Standard or Premium feeds, set values in the **WC Setup** section of the `watchlist-management.properties` Run Profile as follows:

```
phase.WC\ -\ Download.enabled = Y
phase.WC\ -\ Download\ native\ aliases.enabled = N
phase.WC\ -\ Stage\ reference\ lists.enabled = Y
phase.*.snapshot.*.use_native_aliases = 0
```

See the World-Check website for more details:
https://risk.thomsonreuters.com/en/products/third-party-risk/world-check-know-your-customer.html

Note: If your instance of Oracle Watchlist Screening uses the WebLogic application server, and you are screening against the World-Check watch list, then, in order to download the World-Check reference data successfully, you must add the following to the 'Server Start' arguments of your EDQ managed server:

```
-DUseSunHttpHandler=true
```

This is only required if you are using the WebLogic application server **and** screening against the World-Check watch list.

B.6 Dow Jones Watchlist Reference Data

Dow Jones provide a subscription based service offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the various sanctions lists. See the Dow Jones website for more details:

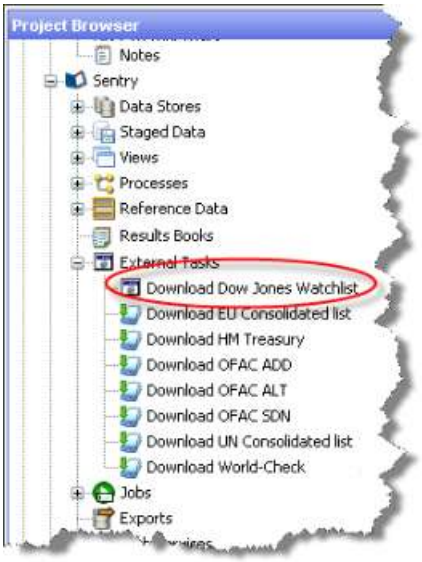
http://www.dowjones.com/products/risk-compliance/

The Dow Jones Watchlist automated download task uses one of two script files that are provided with Oracle Watchlist Screening to provide further configuration of the download process. These script files are:

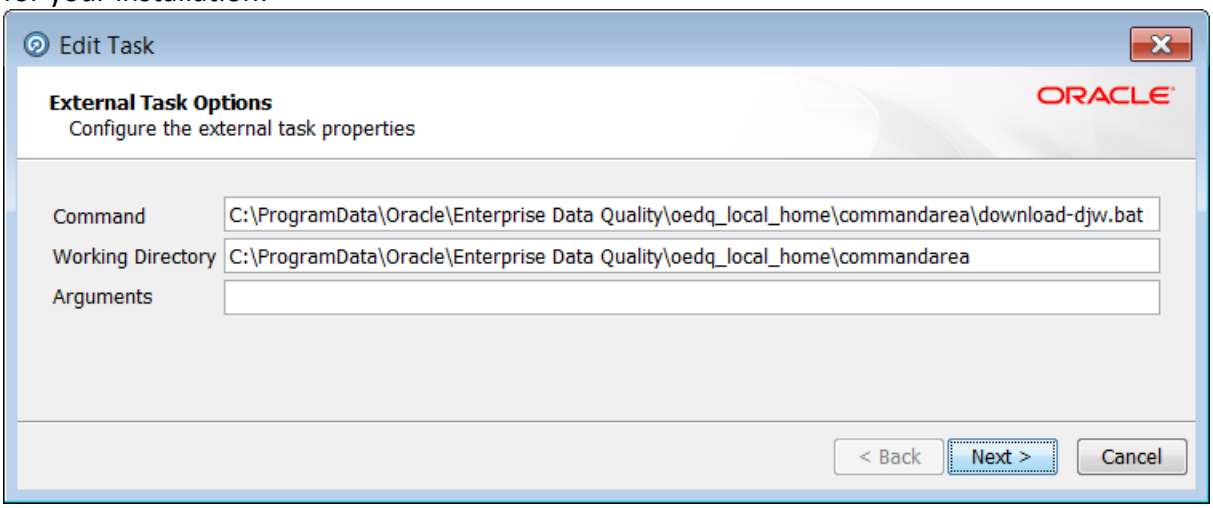
- **download-djw.sh** (for use on Unix platforms)
- **download-djw.bat** (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area. The script files must be modified to provide the appropriate download URL and any required proxy server details for your Internet connection, as detailed in the following procedure:

1. Open the **External Tasks** node for your List Management project in the project browser, and double click on the **Download Dow Jones Watchlist** task.



2. Configure the external task to call the batch or shell file, as appropriate, that is in use for your installation:



3. Configure your PATH system variable to include the path to your Java installation. The external file invokes Java directly, so the PATH must be configured appropriately.
4. Finally, edit your batch or script file to include your Dow Jones authentication information and any proxy server configuration details that are applicable.

B.7 Dow Jones Anti-Corruption List Reference Data

Dow Jones provide a subscription based service containing data to help you assess, investigate and monitor third-party risk with regard to anti-corruption compliance regulation. See the Dow Jones website for more details:

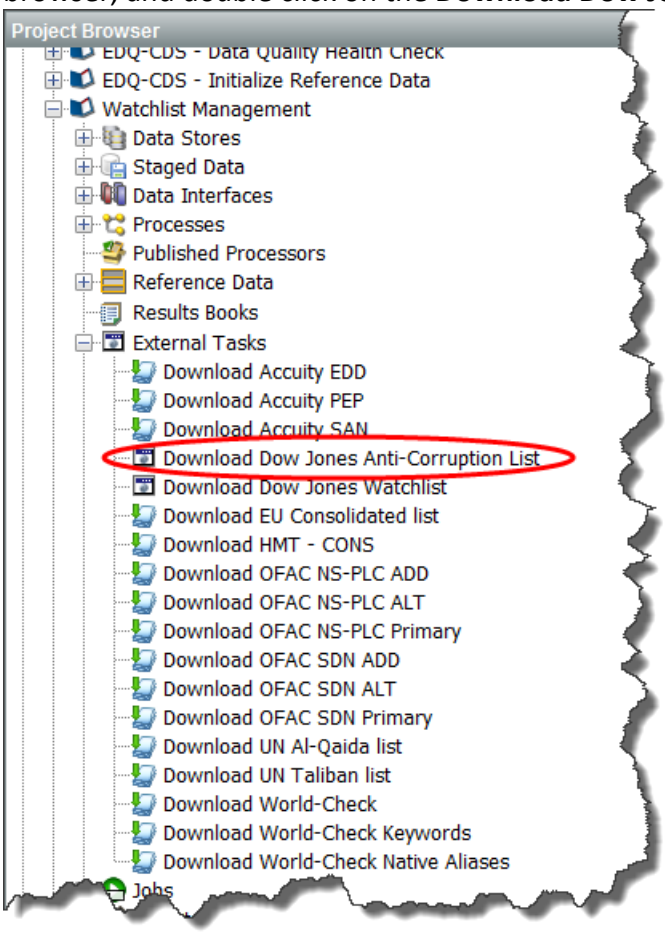
http://www.dowjones.com/products/risk-compliance/

The Dow Jones Anti-Corruption List automated download task uses one of two script files that are provided with Oracle Watchlist Screening to provide further configuration of the download process. These script files are:

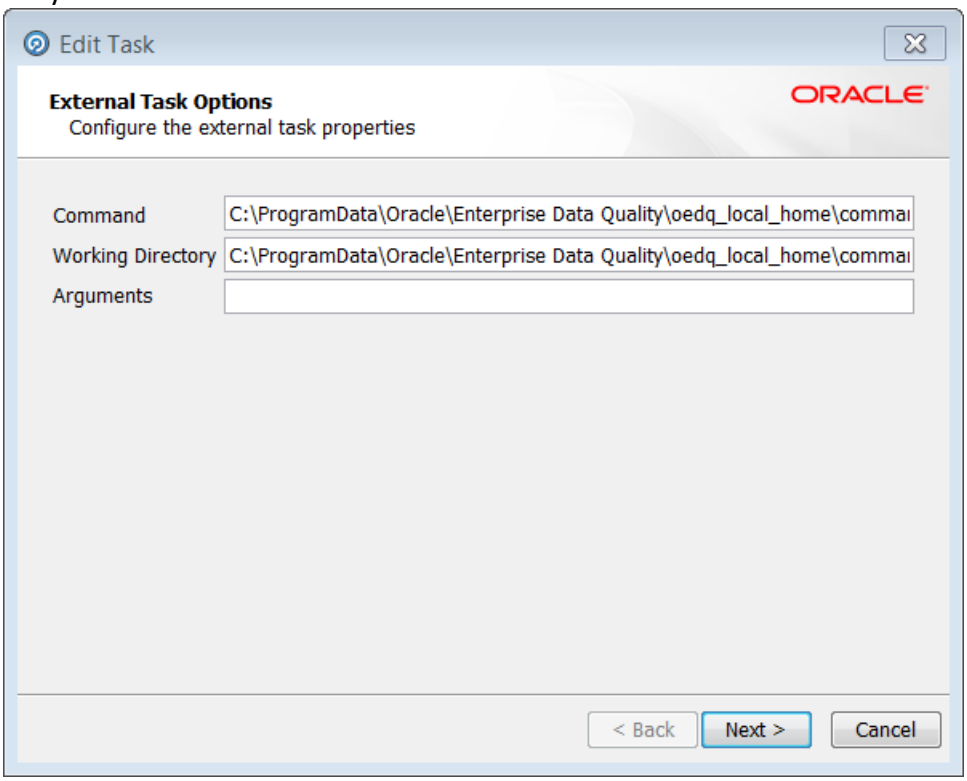
- **download-djac.sh** (for use on Unix platforms)
- **download-djac.bat** (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area. The script files must be modified to provide the appropriate download URL and any required proxy server details for your Internet connection, as detailed in the following procedure:

1. Open the **External Tasks** node for your Watchlist Management project in the project browser, and double click on the **Download Dow Jones Anti-Corruption List** task.



2. Configure the external task to call the batch or shell file, as appropriate, that is in use for your installation:



3. Configure your PATH system variable to include the path to your Java installation. The external file invokes Java directly, so the PATH must be configured appropriately.
4. Finally, edit your batch or script file to include your Dow Jones Anti-Corruption List authentication information and any proxy server configuration details that are applicable.

B.8 Accuity Reference Data

The Accuity Global Watchlist is a subscription based service. The Accuity website states:

> Accuity's proprietary collection of watch list screening databases is an aggregation of specially designated individuals and entities compiled from dozens of regulatory and enhanced due diligence lists from around the world. Global WatchList provides the ideal framework for your customer screening and interdiction filtering processes.

Accuity provide their aggregated data as a set of three lists, as follows:

- The Regulatory Due Diligence (RDD) Lists, covering sanctioned entities and individuals. Optionally, the Accuity Group File can be used in conjunction with this list (see section UNRESOLVED CROSS REFERENCE "Using the Accuity Group File");
- Enhanced Due Diligence (EDD) Lists, covering entities and individuals who are not part of the regulatory sanctions lists, but whose activity it may be desirable to monitor;

- The Politically Exposed Persons (PEPs) Due Diligence Database, covering PEPs.

Any or all of the lists can be downloaded and used separately or in conjunction with each other.

Please refer to the Accuity website for further details:

http://www.accuity.com/compliance/

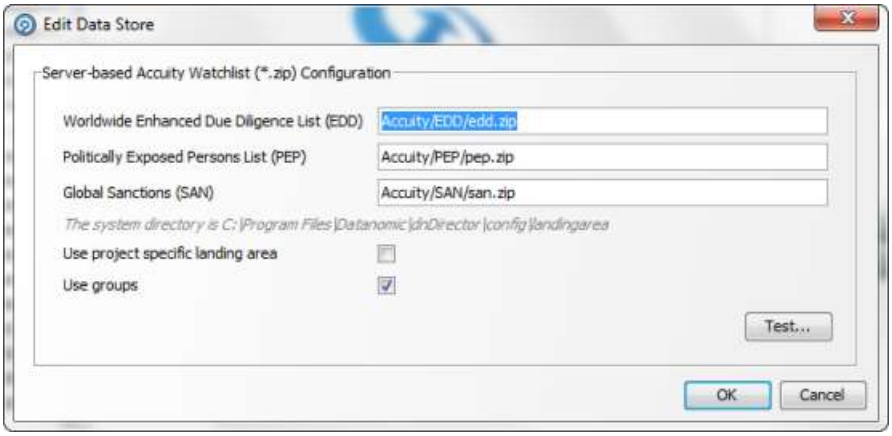
Using the Accuity Group File

The Accuity Global Watchlist is created by aggregating many other lists. As such, any given individual or entity may be represented in the list by multiple entries.

The group file, **GROUP.XML**, provides a way to work with a data set of this type in Oracle Watchlist Screening. Records which all represent the same individual or entity are collected into groups, and each group is assigned a unique group ID. The group ID is used, with a prefix indicating the fact that this is a group ID, in place of the original record identifier in Case Management. Records which are not included in a group use their original Accuity record ID, with a different prefix to indicate that they are single records.

> **Note**: The group file only applies to sanctions screening. That is, only entities and individuals on the Regulatory Due Diligence (RDD) Lists are included in the group file.

The group file allows case generation to be centered around real-world individuals, rather than separate watch list records. Groups are used by default. To change this, open the Accuity Data Store in the Watchlist Management project, and deselect the **Use groups** option:



If you choose to use the group file but it is not present in your downloaded data, an error will be generated.

New Alerts Resulting from Use of the Group File

Using the group file causes the original list ID for an entry to be replaced with the appropriate group ID. The list ID is used in the alert key, so changes to the list ID will result in new alerts being raised for existing, known relationships. There are two main scenarios in which this may occur:

- Individuals or entities are moved into, out of or between groups by Accuity, new alerts will be generated for existing relationships.

Note: Use of the group file may result in new alerts being raised for existing relationships if the group file structure is changed by Accuity. There is at present no way to circumvent this issue

- The **Use Groups** setting is changed after cases and alerts have already been generated.

WARNING: The setting for the **Use Groups** option should be selected during the implementation phase of the project. Once screening has started, it should not be changed unless absolutely necessary. Changing this setting is likely to result in existing alerts being re-raised with a new alert ID.

Appendix C: Screening Non-Latin Character Sets

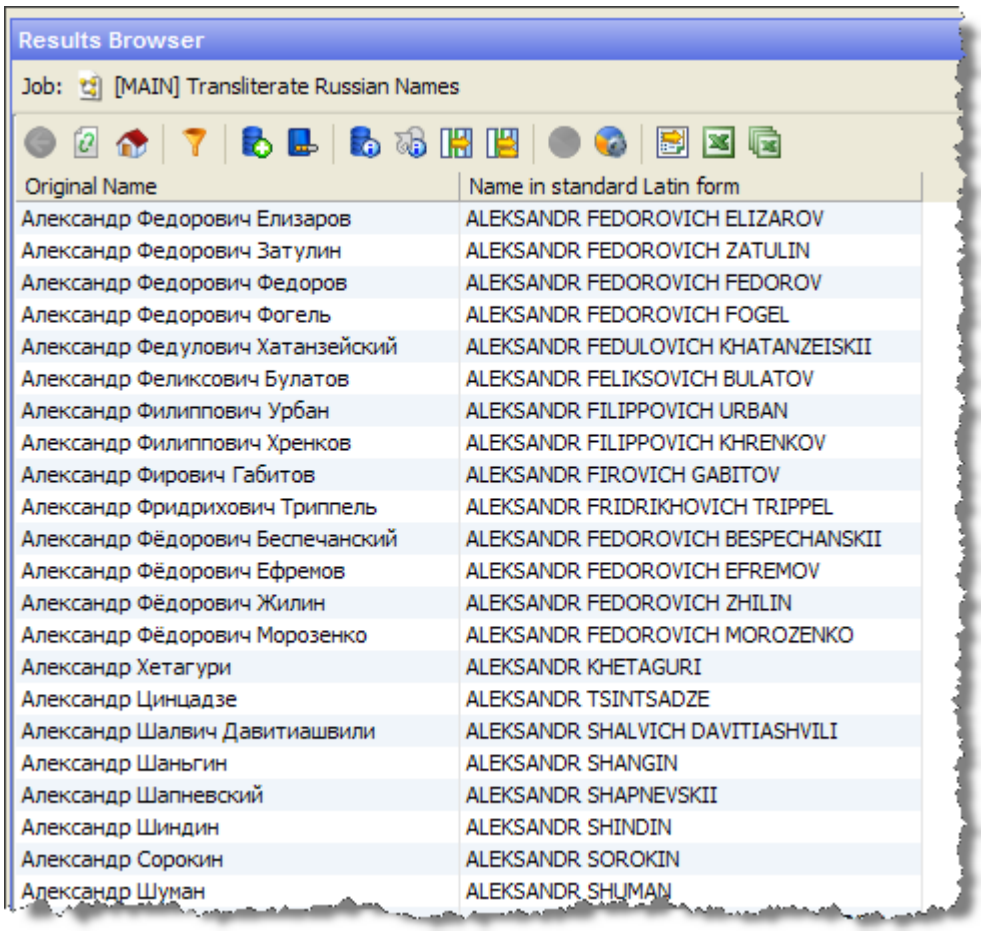
The reference data sources supported by Oracle Watchlist Screening are all provided in the Latin character set, and some in original scripts as well (See "Screening Non-Latin Character Sets"). The screening processes can be used with non-Latin data if required. In addition, Oracle can provide linguistic name matching and culture derivation by integration with IBM's Global Name Recognition product.

Non-Latin working data can be screened against the existing supported Latin reference data sources by performing transliteration of the working data from the non-Latin character set to the Latin character set.

Non-Latin working data can be screened against non-Latin reference data without any changes to the product although certain fuzzy text matching algorithms may not be as effective in the non-Latin character set. Text will be processed on a left-to-right basis.

> **NOTE:** It may be necessary to install additional language packs in order to display non-Latin data.

The screenshot below shows the transliteration of Cyrillic to the Latin character set:



Original Name	Name in standard Latin form
Александр Федорович Елизаров	ALEKSANDR FEDOROVICH ELIZAROV
Александр Федорович Затулин	ALEKSANDR FEDOROVICH ZATULIN
Александр Федорович Федоров	ALEKSANDR FEDOROVICH FEDOROV
Александр Федорович Фогель	ALEKSANDR FEDOROVICH FOGEL
Александр Федулович Хатанзейский	ALEKSANDR FEDULOVICH KHATANZEISKII
Александр Феликсович Булатов	ALEKSANDR FELIKSOVICH BULATOV
Александр Филиппович Урбан	ALEKSANDR FILIPPOVICH URBAN
Александр Филиппович Хренков	ALEKSANDR FILIPPOVICH KHRENKOV
Александр Фирович Габитов	ALEKSANDR FIROVICH GABITOV
Александр Фридрихович Триппель	ALEKSANDR FRIDRIKHOVICH TRIPPEL
Александр Фёдорович Беспечанский	ALEKSANDR FEDOROVICH BESPECHANSKII
Александр Фёдорович Ефремов	ALEKSANDR FEDOROVICH EFREMOV
Александр Фёдорович Жилин	ALEKSANDR FEDOROVICH ZHILIN
Александр Фёдорович Морозенко	ALEKSANDR FEDOROVICH MOROZENKO
Александр Хетагури	ALEKSANDR KHETAGURI
Александр Цинцадзе	ALEKSANDR TSINTSADZE
Александр Шалвич Давитиашвили	ALEKSANDR SHALVICH DAVITIASHVILI
Александр Шаньгин	ALEKSANDR SHANGIN
Александр Шапневский	ALEKSANDR SHAPNEVSKII
Александр Шиндин	ALEKSANDR SHINDIN
Александр Сорокин	ALEKSANDR SOROKIN
Александр Шуман	ALEKSANDR SHUMAN

Original Script Matching

To match original script data against reference data:

- Prepare customer data such that non-Latin names are populated in the Original Script Name fields of the Customer Data interface; and
- Enable Original Script Name match rules and clusters.

For further details on preparing customer data and enable match rules, see the Customer Data Interface and Matching Guides.

Appendix D: Risk scoring reference data

This appendix lists the reference data tables supplied with Oracle Watchlist Screening which contain data used to calculate risk scores and PEP risk scores. You can find these reference data tables in the Watchlist Management project.

D.1 General

The following reference data table contains risk score values used by multiple screening processes:

- Risk - ISO 3166-1 Country to Risk Score (used by the lookup Risk - ISO 3166-1-alpha-2 code to Risk Score) is used to derive a risk score from a country code.

D.2 Country Prohibitions

The following reference data tables contain risk score values used in country prohibition screening processes:

- Country Prohibitions - Entities
- Country Prohibitions - Individuals

D.3 Dow Jones Watchlist

The following reference data tables contain risk score values used when calculating risk scores for the Dow Jones Watchlist records:

- DJW Occupation Category
- DJW List Provider Risk Scores
- DJW SI Category Description
- DJW SI Category

D.4 Dow Jones Anti-Corruption List

The following reference data tables contain risk score values used when calculating risk scores for the Dow Jones Watchlist records:

- DJAC Occupation Category
- DJAC List Provider Risk Scores
- DJAC SI Category Description

D.5 EU Reference Data

There are no reference data tables containing risk score values used only for calculating risk scores for the EU reference data records.

D.6 HM Treasury Reference Data

The following reference data table contains risk score values used when calculating risk scores for the HM Treasury Reference Data records:

- HMT Regime

D.7 OFAC Reference Data

The following reference data table contains risk score values used when calculating risk scores for the OFAC Reference Data records:

- OFAC SDN Program

D.8 UN Reference Data

The following reference data table contains risk score values used when calculating risk scores for the UN Reference Data records:

- UN List Type

D.9 World-Check Reference Data

The following reference data tables contain risk score values used when calculating risk scores for the World-Check Watchlist records:

- WC Category
- WC Keyword (used by the lookup WC Keyword - Risk Score Lookup)

D.10 Accuity Reference Data

The following reference data tables contain risk score values used when calculating risk scores for the Accuity Reference Data records:

- Accuity Program Sub-Category Risk Scores
- Accuity Source Risk Scores

D.11 Risk Element Weightings

The following reference data table contains the weightings used when calculating a record risk score from the various contributing elements:

- Risk - Risk Element Weightings

Appendix E: Sample Customer Data

Oracle Watchlist Screening is supplied with a set of sample customer data, allowing you to run batch screening as soon as you have installed Oracle Watchlist Screening. The Oracle Watchlist Screening sample customer data is supplied in two files which conform to the Customer Data Interface format. One file, **customerindividuals.csv**, contains individual data; the other, **customerentities.csv**, contains entity data.

The sample data files are supplied in the **config/landingarea/Customer** folder of the Oracle Watchlist Screening distribution, and should be copied into the corresponding subdirectory of the landing area in your Oracle Watchlist Screening installation.

The OEDQ Config Folder:
Your OEDQ instance's **config** folder might not be named 'config'. The choice of the config folder's name is made when OEDQ is installed - in some cases a name is automatically allocated. OEDQ release 11g and later has both a 'base' and a 'local' config folder. The base config folder is often called '**oedqhome**', and the local config folder is often called '**oedqlocalhome**'. In some cases, dots or underscores may be inserted into these names (for example: 'oedq_local_home'). Whenever you see a file path in this document that begins with **config**, this always refers to your OEDQ instance's local config folder.

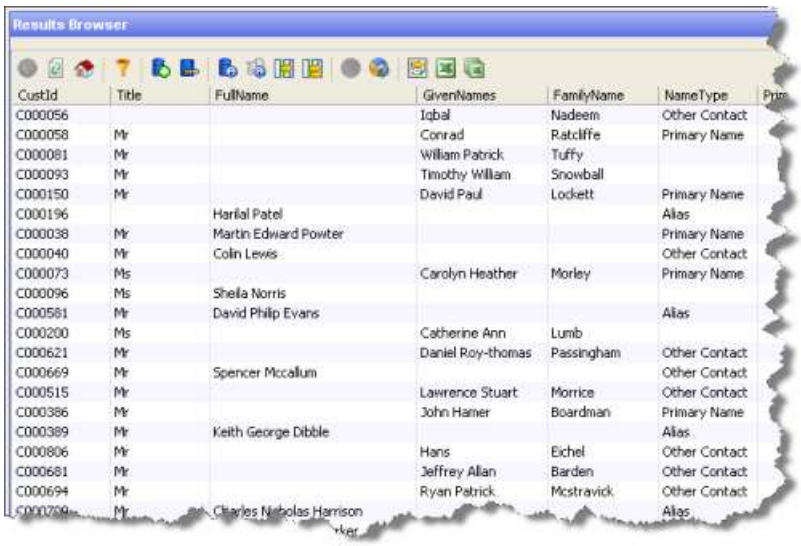
E.1 Characteristics

The Oracle Watchlist Screening sample customer data has been generated from a combination of watch list data and Companies House data, and has the following characteristics:

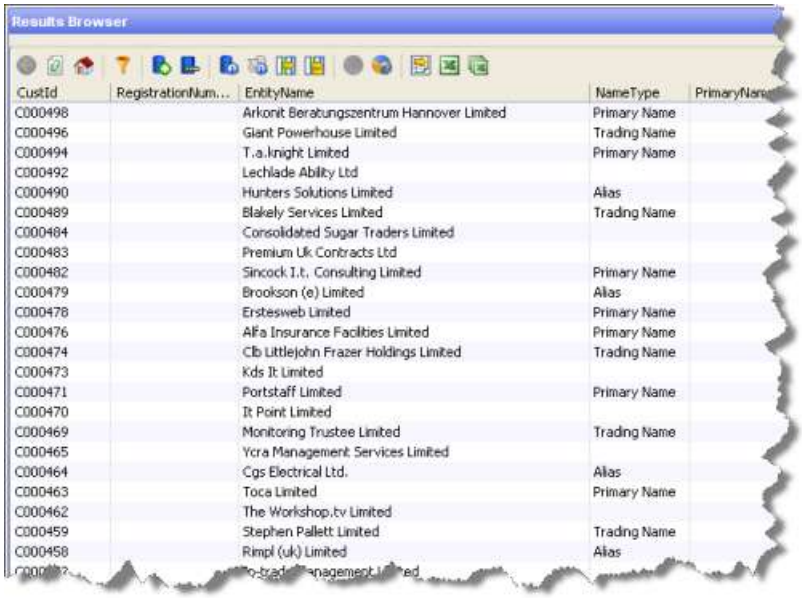
- Each of the sample data files contains 1000 records;
- The sample data has been designed to have a low percentage hit rate in the batch screening process;
- The major combinations of supplied and absent attribute values are covered by the sample data in each file;
- The sample data intentionally contains some 'low quality' entries. These can be used to test and demonstrate the data quality analysis processes.

E.2 Samples

The following screenshot illustrates a small section of the individual sample data, as seen in OEDQ:



The following screenshot illustrates a small section of the entity sample data, as seen in OEDQ:



Appendix F: Real-Time Screening Attributes

F.1 Input Attributes

The web service input interfaces for individuals and entities correspond almost exactly with the batch screening Customer Data Interface as documented in Section 2.1 of the Oracle Watchlist Screening Data Interfaces guide.

NOTE: The sole exceptions are the following input fields, which are not present on the web service interfaces as they do not apply to real-time screening:

- AddedDate
- LastUpdatedDate

See section 5.4.2 "Customizing the Real-Time Screening Input Fields" for further details on configuring the user interface.

F.2 Output Attributes

This section lists the output attributes which are available for the real-time screening processes. The user interface can be configured to display these attributes in the summary or details section of the potential match list.

See section 5.4.3 "Customizing the Real-Time Screening Output Fields" for more detail on configuring the user interface.

F.3 Individual Screening Output Attributes

The following output fields are available from the individual screening process:

Field Label	Field Name	Default Usage	Notes
Feed Id	listFeedId	Summary	An abbreviated form of the name of the list containing the potentially matching record.
Given Names	listGivenNames	Summary	
Family Name	listFamilyName	Summary	
Name Type	listNameType	Summary	
List	listFeedName	Details	The full name of the list containing the potentially matching record.
Id	listId	Details	The ID number of the potentially matching record in the list.
Full Name	listFullName	Details	
Primary Name	listPrimaryName	Details	
Date of Birth	listDOB	Details	
City	listCity	Details	
Country	listCountry	Details	
Country of	listCountryOfBirth	Details	

Field Label	Field Name	Default Usage	Notes
Birth			
Nationality	listNationality	Details	
Match Rule	matchRule	Details	The OEDQ match rule which has been used link the input data to the list record.
Match Score	matchScore	Not used	A number indicating the strength of the correlation between the input data and the match list record. The match score is expressed as an integer between 1 and 100, with higher numbers indicating a stronger match.
Risk Score	riskScore	Not used	A number indicating the relative 'riskiness' of the individual. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
Risk Score PEP	riskScorePEP	Not used	A number indicating the relative 'riskiness' of the individual, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
Case Key	caseKey	Not used	
Alert Id	alertId	Not used	
Source List	sourceList	Not used	The name of the sub-list containing the matching record. Some watch lists are composed of several sub lists; for example, the HM Treasury list includes the HMT Consolidated List (HMT-CONS) and the HMT Investment Ban List (HMT-IB).

F.4 Entity Screening Output Attributes

The following output fields are available from the entity screening process:

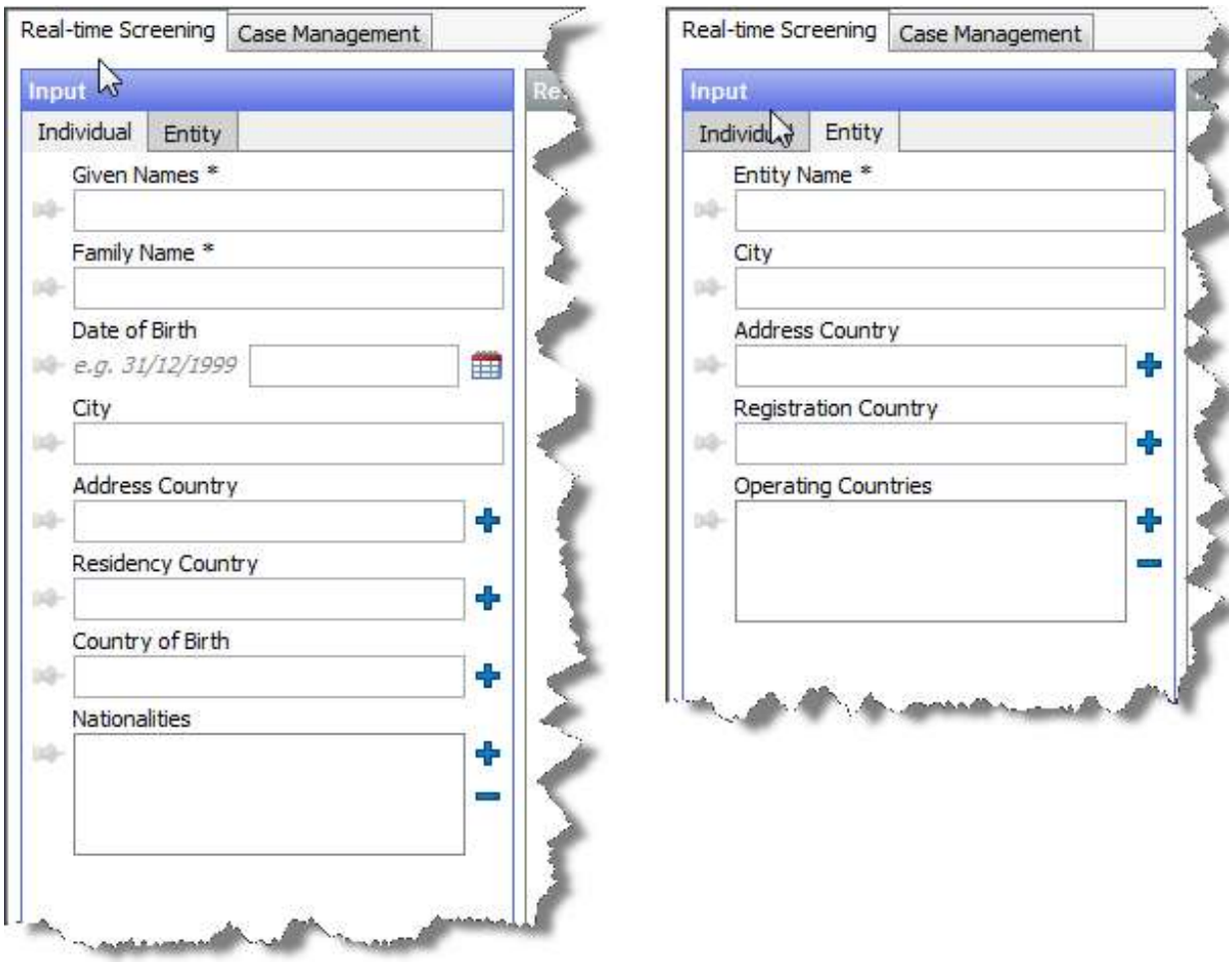
Field Label	Field Name	Default Usage	Notes
Feed Id	listFeedId	Summary	An abbreviated form of the name of the list containing the potentially matching record.
Entity Name	listEntityName	Summary	
Name Type	listNameType	Summary	
List	listFeedName	Details	The full name of the list containing the potentially matching record.
Id	listId	Details	The ID number of the potentially matching record in the list.
Primary Name	listPrimaryName	Details	
City	listCity	Details	
Country	listCountry	Details	
Operating Countries	listOperatingCountries	Details	
Registration Countries	listRegistrationCountries	Details	
Match Rule	matchRule	Details	The OEDQ match rule which has been used link the input data to the list record.
Match Score	matchScore	Not used	A number indicating the strength of the correlation between the input data and the match list record. The match score is expressed as an integer between 1 and 100, with higher numbers indicating a stronger match.

Field Label	Field Name	Default Usage	Notes
Risk Score	riskScore	Not used	A number indicating the relative 'riskiness' of the entity. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
Risk Score PEP	riskScorePEP	Not used	A number indicating the relative 'riskiness' of the entity, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
Case Key	caseKey	Not used	
Alert Id	alertId	Not used	
Source List	sourceList	Not used	The name of the sub-list containing the matching record. Some watch lists are composed of several sub lists; for example, the HM Treasury list includes the HMT Consolidated List (HMT-CONS) and the HMT Investment Ban List (HMT-IB).

Appendix G: The Default Oracle Watchlist Screening User Interface Configuration

As described in Chapter 5: Customizing the Oracle Watchlist Screening User Application, the user interface for the Oracle Watchlist Screening User Application is highly configurable.

The default fields for real-time screening are as follows:



These defaults and all the other available fields are held in the **sentryblueprint-default-screening-layout.properties** file in a standard Oracle Watchlist Screening installation.

To change the fields used, open this file (or the customized **layout.properties** file if one has been configured) and edit the attributes in the **INPUT FIELDS - INDIVIDUALS** and **INPUT FIELDS - ENTITIES** sections as required.

Custom Screening Input Attributes

There are fifty customizable input attributes for individual real-time screening, and fifty for entity real-time screening.

These attributes are provided with generic, default field labels which should be overridden by editing their definitions in the appropriate messages file. Unlike the standard input fields, it is expected that the labels for these fields, when used, will always need to be overridden.

Therefore, entries for these labels are provided in even the default **sentrymessages-en.properties** file.

Field Name	Field Label (default)	Default Usage
customString1 to customString40	Custom string #1 to Custom string #40	Not Used
customDate1 to customDate5	Custom date #1 to Custom date #5	Not Used
customNumber1 to customNumber5	Custom number #1 to Custom number #5	Not Used

Appendix H: Filters and Reports Included With the Distribution

The Oracle Watchlist Screening distribution includes a number of pre-built filters and reports. For information about how to import these filters and reports, see Importing Case Management Filters and Reports. What follows is a list of the pre-built filters and reports with a brief description of each:

Name	Filter or Report	Description
Alert age/state analysis	Report	Displays the current state of alerts on one axis and their creation date on the other. You can see the number of alerts created on each day broken down by current state.
Alert age/state analysis (EDD)	Report	As above, but for Enhanced Due Diligence (EDD) alerts only.
Alert age/state analysis (PEP)	Report	As above, but for Politically Exposed Person (PEP) alerts only.
Alert age/state analysis (SAN)	Report	As above, but for Sanctions (SAN) alerts only.
Alert priority	Report	Displays Risk Score on one axis and Priority Score on the other. Both Risk Score and Priority Score are broken into bands (for example: **50 ~ 60**, **60 ~ 70**, **70 ~ 80** and so on). You can see the number of alerts that fall into each combination of bands. For example, you can see that *n* alerts fall into the **90 - 100** band for both Risk Score and Priority Score.
Alert priority (EDD)	Report	As above, but for Enhanced Due Diligence (EDD) alerts only.
Alert priority (PEP)	Report	As above, but for Politically Exposed Person (PEP) alerts only.
Alert priority (SAN)	Report	As above, but for Sanctions (SAN) alerts only.
Alert work status	Report	Displays the Current State on one axis and the List Record Type (Usually **SAN**, **PEP** or **EDD**) on the other. So for example you can see that there are *n* SAN alerts that are currently Suspected True Matches.
Alert work status (EDD)	Report	As above, but for Enhanced Due Diligence (EDD) alerts only.
Alert work status (PEP)	Report	As above, but for Politically Exposed Person (PEP) alerts only.
Alert work status (SAN)	Report	As above, but for Sanctions (SAN) alerts only.
My alerts	Filter	Displays all alerts assigned to the current user.
My cases	Filter	Displays all cases assigned to the current user.
Open alerts	Report	Displays the number of alerts that have one of the following states: Open, Reopened, True Match Exit Required, Sent for Further Info, Suspected True Match, Reassessment. (Alerts are grouped by the user to whom they are assigned.)
Open alerts (EDD)	Report	As above, but for Enhanced Due Diligence (EDD) alerts only.
Open alerts (PEP)	Report	As above, but for Politically Exposed Person (PEP) alerts only.
Open alerts (SAN)	Report	As above, but for Sanctions (SAN) alerts only.
Unassigned alerts	Filter	Displays all unassigned alerts.
Unassigned cases	Filter	Displays all unassigned cases.