Oracle ® Watchlist Screening

Oracle Watchlist Screening Data Interfaces Guide

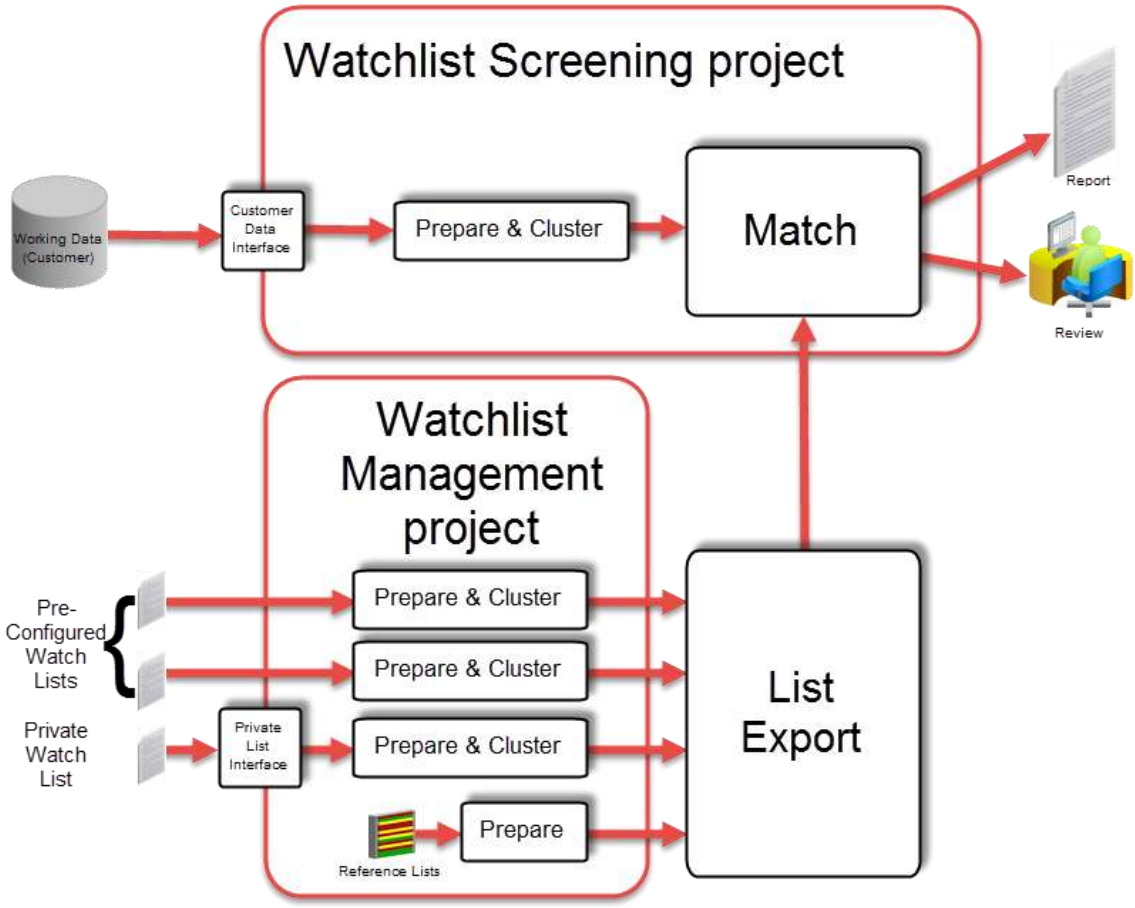
Version 12.2.1

September 2016

Table of Contents

Chapter 1: Introduction

This document describes the Oracle Watchlist Screening Data Interfaces. This is the set of interfaces used to pass customer data and private watch list data into Oracle Watchlist Screening:



The Customer Data Interface (CDI) describes a standard format for customer data. Customer data must conform to the CDI in order to be screened by Oracle Watchlist Screening.

The Private List Interface (PLI) describes a standard format in which private watch list data must be passed to Oracle Watchlist Screening.

This document describes:

- The Oracle Watchlist Screening Batch Screening Customer Data Interface.
- The real-time Web service interfaces for customer data.
- Private Watch List File Formats.

Note: Oracle Watchlist Screening is pre-configured to import and process a number of commercially available and government-provided watch lists. No additional configuration is necessary to import data from these watch lists, and so they are not covered in this guide.

Chapter 2: The Customer Data Interface (CDI)

Customer data enters Oracle Watchlist Screening in one of two ways:

- Via batch interfaces.
- Via a real-time interface (a Web Service).

This section discusses Oracle Watchlist Screening's batch and real-time customer interfaces.

2.1 Batch Screening Customer Data Interface (CDI)

The Customer Data Interface for the Oracle Watchlist Screening batch screening processes consists of a pair of **.csv** (comma-separated value) files with a pre-defined structure and a set of validation rules. The **.csv** files specify the field names for the data set, but this format cannot perform any data validation. As a result, the validation rules form an essential part of the data interface contract, checking for appropriate data types, ensuring that mandatory fields are populated and performing some semantic checks on the data provided (for example, dates of birth should not be in the future).

This chapter discusses the structure of the interface files in section 2.1.1 "Batch Screening CDI file formats", and describes the validation rules in section 2.1.1 "Customer data validation".

2.1.1 Batch Screening CDI file formats

Data for batch screening is supplied in two customer data files, **customerindividuals.csv** and **customerentities.csv**. On installation, these files are populated with sample customer data, which should be replaced with your own data, once it has been transformed into the required format.

Note:

- It is recommended that you keep a copy of the sample customer data files, as they can be used to tune matching rules and verify correct functioning of your installation on a known data set.
- The files must be saved in UTF-8 format.

This section lists the CDI fields used when performing batch screening. The CDI for individual screening is detailed in section "Individual screening input attributes", and the CDI for entity screening in section "Entity screening input attributes". In both cases, attributes fall into one of three classes:

- **Mandatory attributes** are absolutely required for the batch screening process. They are tagged in the CDI tables with the ***[Mandatory attribute]*** tag.
- **Recommended attributes** are used in matching, typically either to eliminate false positive matches which would occur if the mandatory fields alone were used, or to reinforce the likelihood of a possible match. They are tagged in the CDI tables with the ***[Recommended attribute]*** tag.

- **Optional attributes** are not used in the Oracle Watchlist Screening match processes. Information provided in these fields may be of use in processes downstream of the match process.

Individual screening input attributes

This section lists the CDI fields used when screening individuals via the batch process. Fifty customizable input attributes are available for the individual screening process. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your screening process. The following table lists the individual CDI fields in order, the data format expected for each field, and notes on their use in screening.

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is included in the CDI for consistency with the internal list data interface. The LDI uses it to identify the source list of the watch list record (for example, WC-PEP, WC-SAN, HMT-IB). It is included in the alert key.
ListRecordType	String	This field is included in the CDI for consistency with the internal list data interface. In the LDI, it is used when filtering alerts, to determine whether the record is a sanctions, PEP or enhanced due diligence record.
ListRecordOrigin	String	This field is included in the CDI for consistency with the internal list data interface. The LDI uses it to record the provenance of a record when it is part of a consolidated list.
CustId	String	***[Mandatory attribute]*** This attribute is *not* used as part of the matching process, but is used to create the case key. Therefore, it should be populated with a unique customer identifier.
CustSubId	String	This field is included in the CDI for consistency with the internal list data interface. In the LDI, it is used to assign a unique identifier to a record when multiple aliases were originally contained within a single list record.
PassportNumber	String	This is an optional field that may be used to capture customer passport numbers where known for use in the review process. Note that customer passport numbers are not matched against list passport numbers using the default screening rules due to the scarcity of this data on the watch lists.
NationalId	String	This is an optional field that may be used to capture customer National IDs where known for use in the review process. Note that National IDs are not matched against list National IDs using the default screening rules due to the scarcity of this data on the watch lists.
Title	String	This field should contain the titles of customers (such as Mr/Mrs/Dr/Herr/Monsieur). It is used to derive gender values where this information is not already stated, and is used during the review process. Note that it is important that titles are not included in the name fields if possible.

Field Name	Expected Data Format	Notes
FullName	String	***[Mandatory attribute]*** The individual matching process is based primarily on the name supplied for the individual. **Either** a full name, a pair of given and family names, or an original script name **must** be submitted to the screening process for screening to proceed.
GivenNames	String	
FamilyName	String	
NameType	String	This is an optional field used in the review process only. It is included on the interface for consistency with the lists, where multiple names of the same person may exist, and where the Name Type therefore denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). Where customer records have been split out during preparation (before using Watchlist Screening), you may wish to use the Name Type in a similar way. For example, if two customer records were derived from a single Customer ID with multiple names (such as Mrs Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.
NameQuality	String	This field is included in the CDI for consistency with the internal list data interface, and is assigned a value of **Low**, **Medium** or **High** to indicate the quality of the individual name. **High** is used for Primary names and specified Good/High quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	***[Mandatory attribute]*** The individual matching process is based primarily on the name supplied for the individual. **Either** a full name, a pair of given and family names, or an original script name **must** be submitted to the screening process for screening to proceed. If you populate the OriginalScriptName, then you will also need to enable two facets of Match processor configuration that are disabled by default: the **Original Script Name** Cluster and some or all of the Match Rules that include **Original script name** in their name. To adapt Match Processor configuration, you will need to open the Watchlist Screening project within the Director user interface, and make the changes to every process used by your Oracle Watchlist Screening installation. There are separate processes for different types of screening. Examples include **Individual Batch PEP Screening**, **Individual Real-time Screening** and **Individual Batch EDD Screening**. Each of these processes will include a match processor with a name that is the same as the process name (for example, in the **Individual Batch SAN Screening** process, the Match processor will also be called **Individual Batch SAN Screening**)
Gender	String	The value supplied should be either 'M' or 'F'. The gender is not used directly in the matching process, but optionally, the value of the Gender field can be

Field Name	Expected Data Format	Notes
		used by the elimination rules to eliminate poor matches.
DateOfBirth	String, representing a date, in the format 'YYYYMMDD'; day, month and year are required.	***[Recommended attribute]*** Birth date information can be used in matching to identify particularly strong matches, or to eliminate matches that are too weak.
YearOfBirth	String, in the format 'YYYY'.	
Occupation	String	This is an optional field that may be used to eliminate records with "safe" occupations, in the review process and in risk scoring. Note that customer occupations are not matched against list occupations using the default screening rules.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	***[Recommended attribute]*** City data is used to strengthen potential match information.
State	String	
PostalCode	String	
AddressCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** The customer's country of residence can be used in optional country prohibition screening.
CountryOfBirthCode	String; ISO 2-character country code.	***[Recommended attribute]***
NationalityCountryCodes	String; comma-separated list of ISO 2-character country codes.	***[Recommended attribute]*** The customer's nationality can be used in optional country prohibition screening.

Field Name	Expected Data Format	Notes
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	This field is included on the interface for consistency with the list interface. It is not expected to be used for customer records.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally instead of using the Watchlist Screening rules. It is normally populated using Watchlist Screening's risk scoring process. **NOTE**: it is possible to elminate records if their risk score is below a certain threshold.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.

Field Name	Expected Data Format	Notes
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
customString1 to customString40	String	Fifty custom fields are provided in the customer data interface for individuals. Forty of these are intended to hold string data, five hold dates and five numeric data. **NOTE:** The interface file is a comma-separated value (**.csv**) file, and so all fields intrinsically contain strings. The data quality analysis process will, however, raise a low severity error if date or number fields are found to contain inappropriate data.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	
customNumber1 to customNumber5	Number	

Entity screening input attributes

This section lists the CDI fields used when screening entities via the batch process. Fifty customizable input attributes are available for the entity screening process. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your screening process. The following table lists the entity CDI fields in order, the data format expected for each field, and notes on their use in screening:

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is included in the CDI for consistency with the internal list data interface. The LDI uses it to identify the source list of the watch list record (for example, WC-PEP, WC-SAN, HMT-IB). It is included in the alert key.
ListRecordType	String	This field is included in the CDI for consistency with the internal list data interface. In the LDI, it is used when filtering alerts, to determine whether the record is a sanctions, PEP or enhanced due diligence record.
ListRecordOrigin	String	This field is included in the CDI for consistency with the internal list data interface. The LDI uses it to record the provenance of a record when it is part of a consolidated list.
CustId	String	***[Mandatory attribute]*** This attribute is **not** used as part of the matching process, but is used to create the case key. Therefore, it should be populated with a unique customer identifier.
CustSubId	String	This field is included in the CDI for consistency with the internal list data interface. In the LDI, it is used to assign a unique identifier to a record when multiple aliases were originally contained within a single list record.
RegistrationNumber	String	This is an optional field that may be used to capture entity registration numbers where known for use in

Field Name	Expected Data Format	Notes
		the review process. Note that entity registration numbers are not matched against list entity registration numbers using the default screening rules due to the scarcity of this data in the watch lists.
EntityName	String	***[Mandatory attribute]*** The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name **must** be submitted to the screening process for screening to proceed.
NameType	String	This is an optional field used in the review process only. It is included on the interface for consistency with the lists, where multiple names of the same entity may exist, and where the Name Type therefore denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). Where customer records have been split out during preparation (before using Watchlist Screening), you may wish to use the Name Type in a similar way. For example, if two customer records were derived from a single Customer ID with multiple names you may wish to denote one as the primary name and one as an alias.
NameQuality	String	This field is included in the CDI for consistency with the internal list data interface, and is assigned a value of **Low**, **Medium** or **High** to indicate the quality of the entity name. **High** is used for Primary names and specified Good/High quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	***[Mandatory attribute]*** The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name **must** be submitted to the screening process for screening to proceed. If you populate the OriginalScriptName, then you will also need to enable two facets of Match processor configuration that are disabled by default: the **Original Script Name** Cluster and some or all of the Match Rules that include **Original script name** in their name. To adapt Match Processor configuration, you will need to open the Watchlist Screening project within the Director user interface, and make the changes to every process used by your Oracle Watchlist Screening installation. There are separate processes for different types of screening. Examples include **Entity Batch PEP Screening**, **Entity Real-time Screening** and **Entity Batch EDD Screening**. Each of these processes will include a match processor with a name that is the same as the process name (for example, in the **Entity Batch SAN Screening** process, the Match processor will also be called **Entity Batch SAN Screening**).
AliasIsAcronym	String	If this field is set to Y, this flags an alias as an acronym as opposed to a full entity name. Leaving the field blank or setting it to any other value has no effect (i.e.

Field Name	Expected Data Format	Notes
		an alias is assumed to be a full entity name). **NOTE**: This flag is used during matching.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	***[Recommended attribute]*** City data is used to strengthen potential match information.
State	String	
PostalCode	String	
AddressCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** Address country data is used to strengthen potential match information.
RegistrationCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** The entity's registration country can be used in optional country prohibition screening.
OperatingCountryCodes	String; ISO 2-character country code.	***[Recommended attribute]*** Any of the entity's operating countries can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to and Internet or intranet resource for the record.	This field is included on the interface for consistency with the list interface. It is not expected to be used for customer records.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally instead of using the Watchlist Screening rules. It is normally populated using Watchlist Screening's risk scoring process. **NOTE**: it is possible to elminate records if their risk score is below a certain threshold.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
customString1 to customString40	String	Fifty custom fields are provided in the customer data interface for entities. Forty of these are intended to hold string data, five hold dates and five numeric data. **NOTE:** The interface file is a comma-separated value (**.csv**) file, and so all fields intrinsically contain strings. The data quality analysis process will, however, raise a low severity error if date or number fields are found to contain inappropriate data.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	
customNumber1 to customNumber5	Number	

2.1.1 Customer data validation

Two processes are provided in the Oracle Watchlist Screening project to analyze customer data quality–one for individual data and one for entity data. A customer data quality analysis job, **Analyze Customer Data Quality**, is also provided, which runs the customer data snapshots, then calls the data quality analysis processes. The results from the data quality analysis are written to a staged data file, which can be viewed using the Server Console UI.

Data quality analysis is a superset of the validation performed by the main customer data preparation process. In addition, it covers multiple other issues of varying severity. Four severity levels are defined in the business rule data which drives the data quality analysis. The most severe issues, designated severity 1, are the issues which are also detected by the screening processes, and would cause a record to be rejected.

Severities 2 and 3 represent data quality issues of decreasing severity which may have an adverse impact on the effectiveness of screening. Severity 4 issues do not have any impact on the standard screening functionality, but may indicate data which require correction.

Severity 1 – Prevents screening

Severity 1 errors prevent screening from being carried out. They result from missing or extremely low quality data in the case key and/or mandatory screening fields. For example:

- `CustId` is null.
- The `FullName`, `FamilyName` and `OriginalScriptName` fields are null.
- The `FullName`, `FamilyName` and `OriginalScriptName` fields contain no usable data. That is, no data remains after name normalization has been performed.
- The `EntityName` and `OriginalScriptName` fields are null.
- The `EntityName` and `OriginalScriptName` fields contain no usable data. That is, no data remains after name normalization has been performed.

Severity 2 – Invalid data, limiting screening effectiveness

Severity 2 errors may limit the effectiveness of screening. They result from suspect or invalid data in the ancillary screening fields, for example:

- Low quality individual name data in `FullName`, `GivenNames` or `FamilyName`. This category includes the following error conditions:
  - One of the name fields consists of initials only.
  - One or more of `FullName`, `GivenNames` or `FamilyName` contains no usable data after name normalization has been performed. (Note however that the condition where both `FullName` and `FamilyName` contain no usable data is a severity 1 error).
  - One of the name fields contains unexpected characters, such as numerals, most punctuation marks and currency symbols. (Note that the symbols -, &, ’, /, +, ” and the comma are special cases which are covered in the multiple names check below).

    - One of the name fields contains a possible title.
    - One of the name fields contains possible multiple names, indicated by tokens such as: +, &, And, Or, Now, Nee and so on.
    - One of the name fields contains a suspected entity name, indicated by tokens such as: Ltd., Trading, Co. and so on.
    - One of the name fields contains suspect data, as identified by tokens such as Deceased, Test, Dummy and so on.
    - The `Full Name` field contains only a single name token.
    - The `Full Name` field contains non-Latin characters that would be more accurately screened in the `OriginalScriptName` field.
- Low quality entity name data in `EntityName`. This category includes the following error conditions:
    - Short name, defined as a name containing fewer than five alpha characters.
    - Name contains unexpected characters, such as numerals, most punctuation marks and currency symbols. (Note that the symbols -, &, ', /, +, " and the comma are special cases which are covered in the multiple names check below).
    - Name contains possible multiple names, indicated by tokens such as: trading as, t/a, DBA, doing business as and so on.
    - Name contains suspect data, as identified by tokens such as Deceased, Test, Dummy, non-Latin characters and so on.
- Invalid ISO country code supplied;
- `DateOfBirth` is not a valid date in YYYYMMDD format where supplied;
- `DateOfBirth` is in the future;
- `YearOfBirth` is not a valid year in YYYY format where supplied;
- `YearOfBirth` is in the future;
- `YearOfBirth` does not match `DateOfBirth` where both are supplied;
- `Gender` not 'M' or 'F' where supplied.

Severity 3 – Missing data, limiting screening effectiveness

Severity 3 errors may limit the effectiveness of screening. They result from missing data in the ancillary screening fields. For example:

- `FamilyName` supplied without `GivenNames`;
- No country codes supplied;
- `City` not supplied;
- Neither `DateOfBirth` nor `YearOfBirth` supplied;
- `Gender` not supplied.

Severity 4 – No impact on screening

Severity 4 errors have no impact on screening, but may indicate data issues that impact on the downstream use or interpretation of results. For example:

- `RiskScore` is not an integer between 0 and 100 inclusive (where supplied);
- `DataConfidenceScore` is not an integer between 0 and 100 inclusive (where supplied);
- One or both of `AddedDate` or `LastUpdatedDate` are not valid dates in YYYYMMDD format (where supplied);
- One or more of `CustomDate1 – CustomDate5` are not valid dates in YYYYMMDD format (where supplied);
- One or more of `CustomNumber1 – CustomNumber5` are non-numeric (where supplied).

2.2 Web service interfaces for Customer Data

The Customer Data Interface for real-time screening is encapsulated by a pair of Web services, named IndividualScreen and EntityScreen. The Oracle Watchlist Screening user application is an interface to the real-time Web services; however, it is also possible to integrate directly with the web services, if necessary.

This section describes the inputs accepted by the real-time screening Web services.

NOTE: Both Web services output a list of relationships from the matching processor. In Case Management, relationships are grouped into alerts, which are then further grouped into cases. An alert contains all the relationships formed between a single input record and a single watch list record, including any aliases of that record. A case contains all the alerts created for a single input record.

The output data includes an alert ID field and a case key field. Alerts are derived by grouping the relationship data on the case key and alert ID. Where data varies between relationships in an alert, the alert data is taken from the relationship with the highest match score.

To derive case data, group the relationships by case key.

2.2.1 The IndividualScreen Web service interface

This section describes the input fields of the individual screening Web service. The input fields can be split into two groups,

- Standard fields; and
- Customizable fields.

The Oracle Watchlist Screening user application can be configured to display any combination of these fields in any order in the individual data entry tab (see the Oracle Watchlist Screening Implementation Guide for further details). In addition, the label displayed in the user interface for each of these fields can be overridden on a per-locale basis. The default user interface

configuration, including order, default field label and visibility, is detailed in the Oracle Watchlist Screening Implementation Guide.

Standard individual input fields

The list of standard input fields for performing individual screening is as follows:

Field Name	Data Type	Used in Matching?
ListSubKey	String	N
ListRecordType	String	N
ListRecordOrigin	String	N
CustId	String	N
CustSubId	String	N
PassportNumber	String	N
NationalId	String	N
Title	String	N
FullName	String	Y
GivenNames	String	Y
FamilyName	String	Y
NameType	String	N
NameQuality	String	N
PrimaryName	String	N
OriginalScriptName	String	Y
Gender	String	Y[1]
DateOfBirth	Date	Y
YearOfBirth	String	Y[2]
Occupation	String	Y[3]
Address1	String	N
Address2	String	N
Address3	String	N
Address4	String	N
City	String	Y
State	String	N
PostalCode	String	N
AddressCountryCode	String	Y
ResidencyCountryCode	String	Y
CountryOfBirthCode	String	Y
NationalityCountryCodes	String	Y
ProfileHyperlink	String	N
RiskScore	Number	Y[4]
DataConfidenceScore	Number	N
DataConfidenceComment	String	N

[1] The value of the Gender field can be used by the elimination rules to eliminate poor matches.

[2]The value of the YearOfBirth (and DateOfBirth) fields can be used by the elimination rules to eliminate records where the DoB differs by more than a configured threshold.

[3]The value of the Occupation field can be used by the elimination rules to eliminate safe occupations.

[4]The value of the RiskScore field can be used by the elimination rules to eliminate safe customer records.

Customizable individual input fields

Fifty customizable input attributes are available for the individual screening process. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your screening process.

The list of customizable input fields for individual screening is as follows:

Field Name	Data Type	Used in Matching?
customString1 to customString40	String	N
customDate1 to customDate5	Date, specified in the XML DateTime format (see below).	N
customNumber1 to customNumber5	Number	N

The XML DateTime format

Dates in this format have the form yyyy-MM-dd'T'HH:mm:ss.S'Z', where:

- yyyy indicates the year
- MM indicates the month
- dd indicates the day
- the constant 'T' indicates the start of the required time section
- HH indicates the hour
- mm indicates the minute
- ss.S indicates the seconds and fractional seconds
- Z indicates that the time is specified in UTC.

All elements must be present; for example:

1969-05-31T00:00:00.0Z

2.2.2 The EntityScreen Web service interface

This section describes the input fields of the entity screening Web service. The input fields can be split into two groups,

- Standard fields, and
- Customizable fields.

The Oracle Watchlist Screening user application can be configured to display any combination of these fields in any order in the entity data entry tab (see the Oracle Watchlist Screening Implementation Guide for further details). In addition, the label displayed in the user interface for each of these fields can be overridden on a per-locale basis. The default user interface configuration, including order, default field label and visibility, is detailed in the Oracle Watchlist Screening Implementation Guide.

Standard entity input fields

The list of standard input fields for performing entity screening is as follows:

Field Name	Data Type	Used in Matching?
ListSubKey	String	N
ListRecordType	String	N
ListRecordOrigin	String	N
CustId	String	N
CustSubId	String	N
RegistrationNumber	String	N
EntityName	String	Y
NameType	String	N
NameQuality	String	N
PrimaryName	String	N
OriginalScriptName	String	Y
AliasIsAcronym	String	Y
Address1	String	N
Address2	String	N
Address3	String	N
Address4	String	N
City	String	Y
State	String	N
PostalCode	String	N
AddressCountryCode	String	Y
RegistrationCountryCode	String	Y
OperatingCountryCodes	String	Y
ProfileHyperlink	String	N
RiskScore	Number	N[5]
DataConfidenceScore	Number	N
DataConfidenceComment	String	N

Customizable entity input fields

Fifty customizable input attributes are available for the entity screening process. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your screening process.

The list of customizable input fields for entity screening is as follows:

Field Name	Data Type	Used in Matching?
customString1 to customString40	String	N
customDate1 to customDate5	Values for these fields should be specified in the XML DateTime format (see below).	N
customNumber1 to customNumber5	Number	N

[5]The value of the RiskScore field can be used by the elimination rules to eliminate safe customer records.

The XML DateTime format

Dates in this format have the form yyyy-MM-dd'T'HH:mm:ss.S'Z', where:

- yyyy indicates the year
- MM indicates the month
- dd indicates the day
- the constant ‘T’ indicates the start of the required time section
- HH indicates the hour
- mm indicates the minute
- ss.S indicates the seconds and fractional seconds
- Z indicates that the time is specified in UTC.

All fields must be present. For example:

1969-05-31T00:00:00.0Z

Chapter 3: The Private List Interface (PLI)

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 or against external watch lists that Oracle Watchlist Screening is not pre-configured to work with. The Private List Interface (PLI) is used to import data from private watch lists or other sources into Oracle Watchlist screening. It consists of a pair of **.csv** (comma-separated value) files with a pre-defined structure and a set of validation rules.

This chapter discusses the structure of the interface files.

3.1 Private List Interface (PLI) file formats

Private Watch List data must be supplied in two data files, **privateindividuals.csv** and **privateentities.csv**. On installation, these files are populated with sample private watch list data, which should be replaced with your own data, once it has been transformed into the required format. For information about the location of these two files, see section 3.1.2 of the Oracle Watchlist Screening Implementation Guide.

Note:

- It is recommended that you keep a copy of the sample private watch list files, as they can be used to verify correct functioning of your installation on a known data set.
- The files must be saved in UTF-8 format.

This section lists PLI fields. The PLI for individuals is detailed in section 3.1.1 "Individual private watch list input attributes", and the PLI for entity screening in section 3.1.2 "Entity private watch list input attributes". In both cases, attributes fall into one of three classes:

- **Mandatory attributes** are absolutely required for screening. They are tagged in the PLI tables with the ***[Mandatory attribute]*** tag.
- **Recommended attributes** are used in matching, typically either to eliminate false positive matches which would occur if the mandatory fields alone were used, or to reinforce the likelihood of a possible match. They are tagged in the PLI tables with the ***[Recommended attribute]*** tag.
- **Optional attributes** are not used in the Oracle Watchlist Screening match processes. Information provided in these fields may be of use in processes downstream of the match process.

3.1.1 Individual private watch list input attributes

This section lists the PLI fields used for individuals. In addition to a number of prescribed fields, fifty customizable input attributes are available for individual private watch lists. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list. The following table lists the individual PLI fields in order, the data format expected for each field, and notes on their use in screening.

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List and so on). It is included in the alert key.
ListRecordType	String	***[Mandatory attribute]***This field is used when filtering alerts, to determine whether the record is a sanctions, PEP or enhanced due diligence record. It must contain a value of **SAN**, **EDD**, or **PEP** or a combination of these values. If you want to include a combination of values, the values should be comma-separated, and enclosed by double quotation marks. For example: **"SAN, EDD, PEP"**
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	***[Mandatory attribute]*** This attribute is *not* used as part of the matching process, but is used to create the case key. Therefore, it should be populated with a unique identifier.
PassportNumber	String	This is an optional field that may be used to capture customer passport numbers where known for use in the review process. Note that passport numbers are not used in the default screening rules.
NationalId	String	This is an optional field that may be used to capture customer National IDs where known for use in the review process. Note that National IDs are not used in the default screening rules.
Title	String	This field should contain the titles of customers (such as Mr/Mrs/Dr/Herr/Monsieur). It is used to derive gender values where the gender is not already stated, and is used during the review process. Note that it is important that titles are not included in the name fields if possible.
FullName	String	***[Mandatory attribute]*** The individual matching process is based primarily on the name supplied for the individual. **Either** a full name, a pair of given and family names, or an original script name **must** be submitted to the screening process for screening to proceed.
GivenNames	String	
FamilyName	String	
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same person. The Name Type therefore denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two private list records were derived from a single source with multiple names (such as Mrs Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.
NameQuality	String	This field may be assigned a value of **Low**, **Medium** or **High** to indicate the quality of the individual name. **High** is used for Primary names and specified Good/High quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.

Field Name	Expected Data Format	Notes
OriginalScriptName	String	***[Mandatory attribute]*** The individual matching process is based primarily on the name supplied for the individual. **Either** a full name, a pair of given and family names, or an original script name **must** be submitted to the screening process for screening to proceed. If you populate the OriginalScriptName, then you will also need to enable two facets of Match processor configuration that are disabled by default: the **Original Script Name** Cluster and some or all of the Match Rules that include **Original script name** in their name. To adapt Match Processor configuration, you will need to open the Watchlist Screening project within the Director user interface, and make the changes to every process used by your Oracle Watchlist Screening installation. There are separate processes for different types of screening. Examples include **Individual Batch PEP Screening**, **Individual Real-time Screening** and **Individual Batch EDD Screening**. Each of these processes will include a match processor with a name that is the same as the process name (for example, in the **Individual Batch SAN Screening** process, the Match processor will also be called **Individual Batch SAN Screening**).
Gender	String	The value supplied should be either 'M' or 'F'. The gender is not used directly in the matching process, but optionally, the value of the Gender field can be used by the elimination rules to eliminate poor matches.
Occupation	String	This is an optional field that may be used to eliminate records with "safe" occupations, in the review process and in risk scoring. Note that customer occupations are not matched against list occupations using the default screening rules.
DateOfBirth	String, representing a date, in the format 'YYYYMMDD'; day, month and year are required.	***[Recommended attribute]*** Birth date information can be used in matching to identify particularly strong matches, or to eliminate matches that are too weak.
YearOfBirth	String, in the format 'YYYY'.	
Deceased Flag	String	If populated, this optional field should contain either **Y** or **N**.
DeceasedDate	String, representing a date, in the format 'YYYYMMDD'.	If populated, this optional field should contain either the current date or a date in the past.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	***[Recommended attribute]*** City data is used to strengthen potential match information.
State	String	

Field Name	Expected Data Format	Notes
PostalCode	String	
AddressCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** The country of residence can be used in optional country prohibition screening.
CountryOfBirthCode	String; ISO 2-character country code.	***[Recommended attribute]***
NationalityCountryCodes	String; comma-separated list of ISO 2-character country codes.	***[Recommended attribute]*** The nationality can be used in optional country prohibition screening.

Field Name	Expected Data Format	Notes
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	**This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the individual.**
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally instead of using the Watchlist Screening rules. It is normally populated using Watchlist Screening's risk scoring process. **NOTE**: it is possible to eliminate records if their risk score is below a certain threshold.
RiskScorePEP	Number, between 0 and 100	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.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field should contain either **Y** or **N**.
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field should contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether the individual is part of an international organization or government, and at what level). It can be used to filter watch list records, and is primarily used by the World-Check watch list, but

Field Name	Expected Data Format	Notes
		could be used by a private watch list if required. See section 3.2 of the Oracle Watchlist Screening Implementation guide for more information about filtering.
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for individuals. Forty of these are intended to hold string data, five hold dates and five numeric data. **NOTE:** The interface file is a comma-separated value (**.csv**) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are output if they do not.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	
customNumber1 to customNumber5	Number	

3.1.2 Entity private watch list input attributes

This section lists the private PLI fields used for entities. In addition to a number of prescribed fields, fifty customizable input attributes are available for entity private lists. Forty of these are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list. The following table lists the entity PLI fields in order, the data format expected for each field, and notes on their use in screening:

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List and so on). It is included in the alert key.
ListRecordType	String	***[Mandatory attribute]***This field is used when filtering alerts, to determine whether the record is a sanctions, PEP or enhanced due diligence record. It must contain a value of **SAN**, **EDD**, or **PEP** or a combination of these values. If you want to include a combination of values, the values should be comma-separated, and enclosed by double quotation marks. For example: **"SAN, EDD, PEP"**
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	***[Mandatory attribute]*** This attribute is **not** used as part of the matching process, but is used to create the case key. Therefore, it should be populated with a unique customer identifier.
RegistrationNumber	String	This is an optional field that may be used to capture entity registration numbers where known for use in the review process. Note that entity registration numbers are not used for matching in the default screening rules.
EntityName	String	***[Mandatory attribute]*** The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name **must** be submitted to the screening process for screening to proceed.

Field Name	Expected Data Format	Notes
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same entity. The Name Type therefore denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two private list records were derived from a single source with multiple names, you may wish to denote one as the primary name and one as an alias.
NameQuality	String	This field may be assigned a value of **Low**, **Medium** or **High** to indicate the quality of the individual name. **High** is used for Primary names and specified Good/High quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	***[Mandatory attribute]*** The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name **must** be submitted to the screening process for screening to proceed. If you populate the OriginalScriptName, then you will also need to enable two facets of Match processor configuration that are disabled by default: the **Original Script Name** Cluster and some or all of the Match Rules that include **Original script name** in their name. To adapt Match Processor configuration, you will need to open the Watchlist Screening project within the Director user interface, and make the changes to every process used by your Oracle Watchlist Screening installation. There are separate processes for different types of screening. Examples include **Entity Batch PEP Screening**, **Entity Real-time Screening** and **Entity Batch EDD Screening**. Each of these processes will include a match processor with a name that is the same as the process name (for example, in the **Entity Batch SAN Screening** process, the Match processor will also be called **Entity Batch SAN Screening**).
AliasIsAcronym	String	If this field is set to **Y**, this flags an alias as an acronym as opposed to a full entity name. Leaving the field blank or setting it to any other value has no effect (i.e. an alias is assumed to be a full entity name). **NOTE**: This flag is used during matching.
VesselIndicator	String	This field should be set to **Y** if the entity is a vessel (a ship). It should be left empty or set to **N** if the entity is not a vessel.
VesselInfo	String	If the entity is a vessel, you can populate this field with information about it: for example, its call sign, type, tonnage, owner, flag and so on.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	***[Recommended attribute]*** City data is used to strengthen potential match information.
State	String	

Field Name	Expected Data Format	Notes
PostalCode	String	
AddressCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** Address country data is used to strengthen potential match information.
RegistrationCountryCode	String; ISO 2-character country code.	***[Recommended attribute]*** The entity's registration country can be used in optional country prohibition screening.
OperatingCountryCodes	String; ISO 2-character country code.	***[Recommended attribute]*** Any of the entity's operating countries can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to and Internet or intranet resource for the record.	This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the entity.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally instead of using the Watchlist Screening rules. It is normally populated using Watchlist Screening's risk scoring process. **NOTE**: it is possible to elminate records if their risk score is below a certain threshold.
RiskScorePEP	Number, between 0 and 100	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.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field should contain either **Y** or **N**.
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field should contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether it relates to an international organization or government, and at what level). It can be used to filter watch list records, and is primarily used by the World-Check watch list, but could be used by a private watch list if required. See section 3.2 of the Oracle Watchlist Screening Implementation guide for more information about filtering.
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for entities. Forty of these are intended to

Field Name	Expected Data Format	Notes
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	hold string data, five hold dates and five numeric data. **NOTE:** The interface file is a comma-separated value (**.csv**) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are output if they do not.
customNumber1 to customNumber5	Number	