Oracle Financial Crime and Compliance Management Customer Screening Cloud Service

Performing Administrative Tasks

Release 24.08.01
G17331-01
August 2024

Oracle Financial Crime and Compliance Management Customer Screening Cloud Service Performing Administrative Tasks, Release 24.08.01

G17331-01

Copyright © 2000, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 About Oracle Financial Services Customer Screening

1.1 Process Flow for Administrator 1-1
1.2 Quick Tour of Customer Screening 1-2
1.3 Customer Screening Workflow 1-3
1.4 Generation of Canned Reports 1-4
1.5 Generate a Case 1-4
1.6 Generate Alerts or Re-alerts 1-4
1.7 Manage Pipelines 1-5
1.8 Load Customer Data to OpenSearch 1-5

1

About Oracle Financial Services Customer Screening

Introduction to Oracle Financial Services Customer Screening.

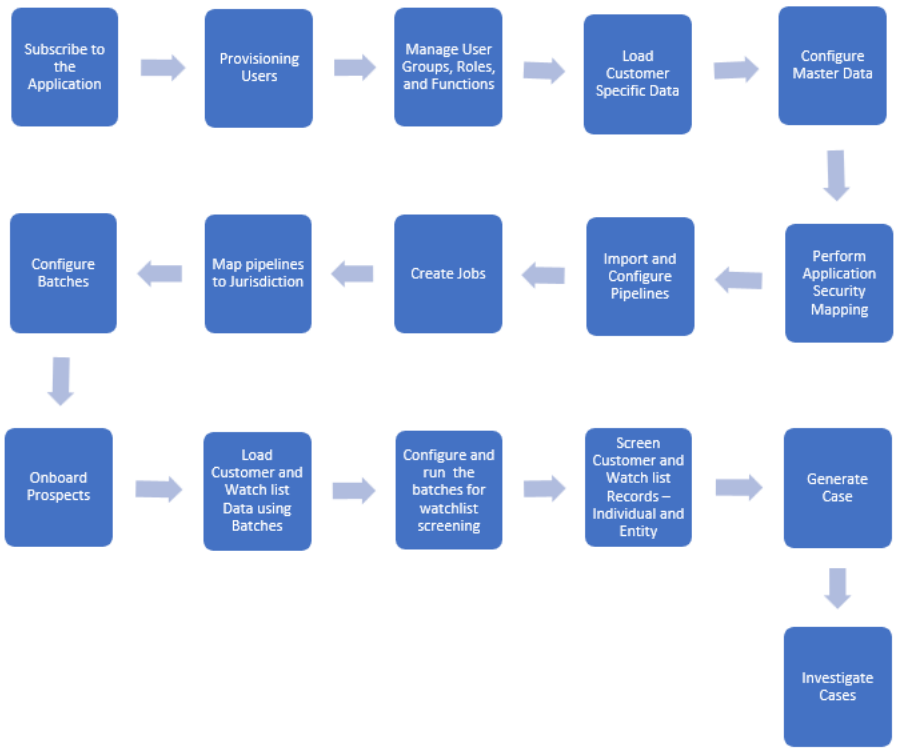
Oracle Financial Services Customer Screening (OFS CS) enables organizations to effectively and efficiently screen their customers so that they can successfully meet anti- bribery, anti-corruption, export control, and other legal regulations as well as to meet anti- money laundering and counter-terrorist financing legislations. Screening customers enables organizations to keep track of and avoid the risk of being exposed to suspicious or sanctioned individuals and organizations.

1.1 Process Flow for Administrator

Customer Screening workflow.

The System Administrator can perform the required tasks and configurations in the following order. Optionally, you can also configure and execute pipelines on a new environment, and import or copy pipelines if you are moving data between environments.

Figure 1-1 Process Flow for Administrator



1.2 Quick Tour of Customer Screening

Overview of the tasks and the order to execute the tasks using the CS Application.

Click the links to read details of each task.

Table 1-1 Quick Tour of Customer Screening

Order	Tasks	Who Does This?	Details and Documentation Reference
1	Subscribe to the Application	Tenant Admin	Subscribe to the application. For more information on the subscription process, see Getting Started with Oracle Financial Services Crime and Compliance Management Cloud Service.
2	Provision Users	System Admin	Configure Security Management System (SMS) to create users, roles, and implement user authorization and authentication. For more information on provisioning users, see Setup your Cloud Account.
3	Manage User Groups, Roles, and Functions	System Admin	Create user groups, create roles, map users to user groups, map user groups to roles, and map roles to functions. For more information on the steps involved, see Identity Management.
4	Load Customer Specific Data	Data Admin	Load customer-specific data such as sample staging data, business domain, and jurisdiction data to the application for further processing. For more information, see Data Loading.
5	Configure Master Data	CS Admin	Define the master data values. For more information, see Master Data.
6	Perform Application Security Mapping	System Admin	Create security attributes that allow or restrict access to users. For more information, see Oracle Financial Services Crime and Compliance Management Cloud Service Application Security.
7	Manage Pipelines	CS Admin	Import the ready-to-use pipelines to the CS application, create a copy of the imported pipelines and save it as a new pipeline. For more information, see Importing Pipelines and Copying Pipelines. Create new pipelines and configure the same as per your requirements. To create pipelines, see Creating Pipelines.
8	Create Jobs	CS Admin	Create jobs to define a collection of instructions for executing pipelines against threshold sets. For more information on how to create jobs, see Using Jobs.
9	Map Pipeline to Jurisdiction	CS Admin	Map a ready-to-use pipeline or add a new pipeline and map it to one or more jurisdictions. For more information, see Map Pipeline to a Jurisdiction.

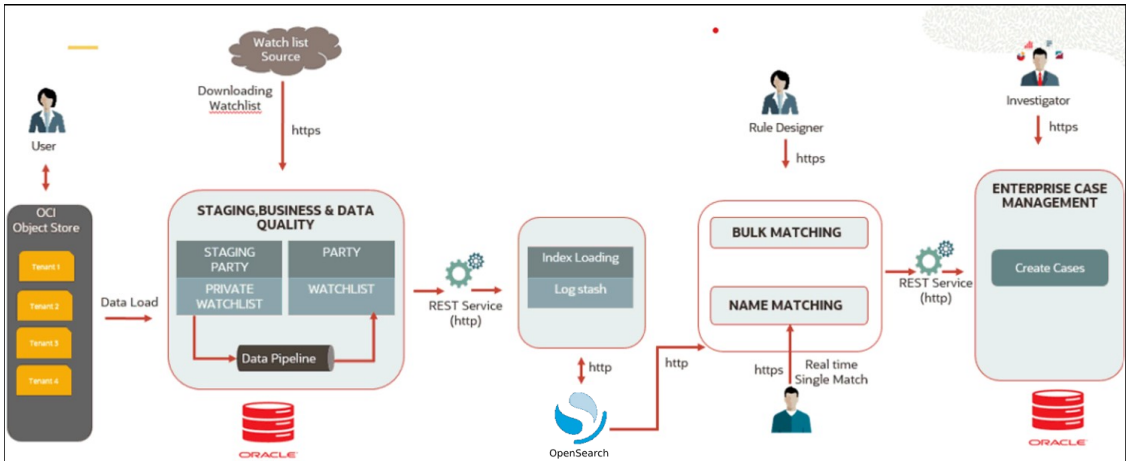
Table 1-1 (Cont.) Quick Tour of Customer Screening

Order	Tasks	Who Does This?	Details and Documentation Reference
10	Configure Batches	CS Admin	Define batches specific to CS in the Scheduler Service window. For more information, see Managing Batches section of Pipeline Designer and Scheduler Service.
11	Onboard Prospects	CS Admin	Execute the Real-time API. For more information see Rest API for Customer Screening Cloud Service.
12	Load Customer and Watch list Data using Batches	CS Admin	Run the **FullLoadCustomer** and **FullLoadCustomerdelta** batch in the Schedule window to load data. For more information, see Master Data.
13	Configure and run the batches for watchlist screening	CS Admin	Configure and run the batches specific to watchlist screening in the Schedule window to load watchlist data. For more information, see Managing Batches section of Pipeline Designer and Scheduler Service.
14	Screen Customer and Watch list Records – Individual and Entity	CS Admin	Screen records against watchlist data. For editing the watchlist data, see Watchlist Management. Alerts are generated based on the matching rules and associated thresholds For more information, see Matching Guide.
15	Generate Alert	CS Admin	Select the attribute which generates a re-alert based on the change in the attribute value. For more information, see Alert Decision widget.
16	Investigate Cases	Analysts and Investigators	Investigate and monitor cases. For more information, see Investigating Cases.
17	Metering	CS Admin	View the total number of Customer Screening scans performed. For more information, see Metering.

1.3 Customer Screening Workflow

The figure illustrates the Customer Screening workflow.

Figure 1-2 Customer Screening Workflow



1.4 Generation of Canned Reports

Information about generation of the Canned Reports.

Canned Reports captures the following information which will show up after the Batch execution for every run:

- Customers in Staging table
- Customers pushed from staging table into Transaction filtering tables
- Alerts/events generated
- Customers with non-hits
- Cases created

For more information on accessing the Canned Reports, see View Reports for Download.

1.5 Generate a Case

Information about generating a case.

When one or more matches are recorded between a watch list and a customer record, a case is generated. The user can take a decision and decide if the alert is a false positive or a true match. If a new alert is generated, a new case is also generated in Enterprise Case Management (ECM).

To generate the case in ECM, run the **ScreeningToCaseMgmt** batch in the Scheduler Service.

1.6 Generate Alerts or Re-alerts

Information about generating an alert or a re-alert.

After all the attribute level scores are calculated a weightage average score for the rule is calculated and check against the ruleset threshold to determine if an alert is to be created. The alert is created only if the customer data or watchlist data is new or significantly changed from the previous time it was screened. The **Alert Decision**widget is where attributes can be

configured to determine if a change in the data or an increase in the score will create a new alert. Alerts are generated for each match that exceeds the rule threshold.

If there is a change in the record value (first name, last name, date of birth) or score, the alert is regenerated. The attributes which resulted in the re-alert is highlighted with a red box on the Event Details page for the re-alert. For more information on event details, see the Case Investigation User guide.

You can specify the attributes which generate a re-alert based on the value change or score change in the Alert Decision window. For more information on Alert Decision window, see Using Pipeline Designer guide.

1.7 Manage Pipelines

Information about managing the CS pipelines.

There are four ready-to-use pipelines: two pipelines are used for individual batch and real- time data and two pipelines are used for entity batch and real-time data. Within the pipelines are different matching configurations for SAN, PEP, EDD, and PRB records which can be tuned depending on your risk appetite.

Matching configuration is set using the **Matching Rules** widget. Each widget defines a match configuration for a source (customer) and target (watch list). The source and target can be filtered. This is how we set the different matching configurations for entities and individuals. It can also be used for setting different configurations for jurisdictions and domains.

Each ruleset can contain multiple rules and the score given to an alert is the maximum of the individual rule scores. An alert is generated only if the score is above the ruleset threshold. Within a rule configuration, source and target attributes are defined along with the match type (exact match, fuzzy match, or date match) and scoring method (Reverse Jaro Winkler, Jaro Winkler, Levenshtein). Each attribute level match has a threshold, below which the score is not considered, and a weightage. If the Must condition is set, then a match will not be created unless the score for that attribute is above the threshold.

To match the customer records with watch list data, run the **IndividualScreening** batch for an individual or **Entity Screening** batch for an entity in the Scheduler Service.

1.8 Load Customer Data to OpenSearch

Infromation about loading customer data into OpenSearch.

Use a predefined template to create an OS index. The template has information on the data and analyzer types used in the JSON. It also describes the fields used in the JSON. OS gives results in real-time. The matching service uses OS to generate matches.

- To load the data and load it to OS for matching, Run the **CustomerFullLoad** batch in the Scheduler Service. For information on how to load data from the object store to staging and from staging to the business tables if the Anti-Money Laundering (AML) application is not deployed, see Using FCCM Data Loading Service.
- To load data for the object store to staging and staging to business tables if Anti- Money Laundering AML is not deployed, see Uploading Data Files.
- To load Customer Delta Data and load it to ES/OS for matching, Run the CustomerDeltaLoad batch in the Scheduler Service.