OFS Customer Screening Cloud Service

Performing Administrative Tasks

Release 26.02.01
G50095-01
February 2026

ORACLE

OFS Customer Screening Cloud Service Performing Administrative Tasks, Release 26.02.01

G50095-01

Contents

1

About Oracle Financial Services Customer Screening

Introduction to Oracle Financial Services Customer Screening:

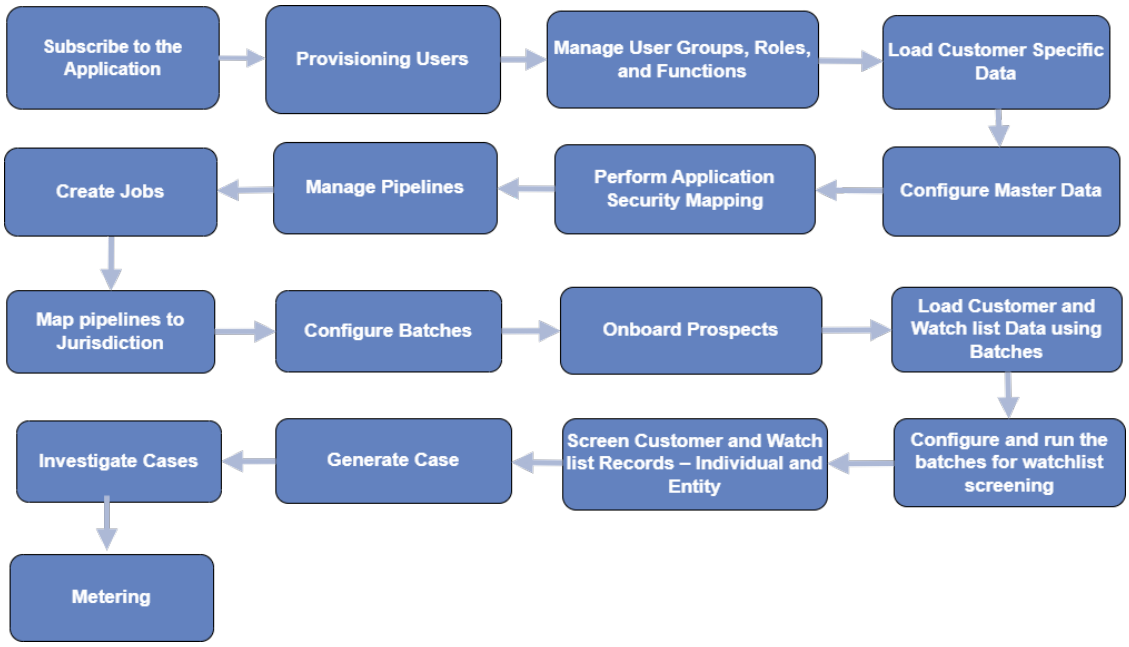
Oracle Financial Services Customer Screening (OFS CS) enables organizations to effectively and efficiently screen their customers so that they can successfully meet anti- bribery, anti-corruption, export control, and other legal regulations as well as to meet anti- money laundering and counter-terrorist 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



Click the below 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 into the application for further processing. For more information, refer to the following links: • Load Data - Customers Provisioned After 24.08.01 • Load Data - Customers Provisioned Before 24.08.01
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.
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.

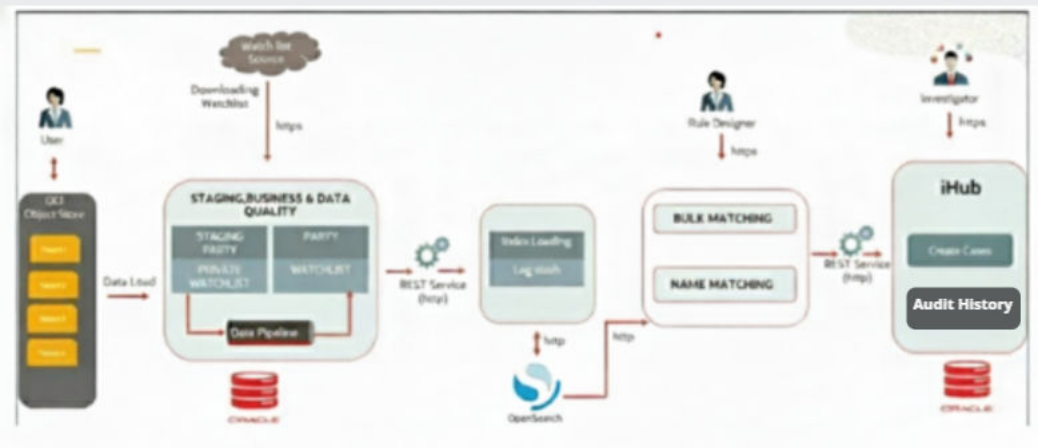
Table 1-1 (Cont.) Quick Tour of Customer Screening

Order	Tasks	Who Does This?	Details and Documentation Reference
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.

1.2 Customer Screening Workflow

The figure illustrates the Customer Screening workflow.

Figure 1-2 Customer Screening Workflow



Customer screening workflow orchestrates the sanctions screening of customers against internal and external watchlists, ensuring.

This workflow ensures:

- Automated, scalable screening across multiple tenants/clients.
- Consistent data quality and processing through rigorous controls.
- Strict role separation and robust security to prevent data leakage.
- Thorough investigative and compliance traceability. .

Here's a step-by-step explanation:

Data Ingestion

- The data ingestion process helps to collect and compartmentalize data for each tenant/client to uphold strict data separation and confidentiality.
- *Data Sources*:
  - Customer Lists: Core customer/client records subject to scrutiny.
  - Party Lists: Linked individuals/organizations of interest (e.g., beneficial owners, related vendors).
  - Transactions: Counterparties in a transaction.
- *Watchlists:*
  - External: Sanctions and PEP lists (e.g., OFAC, EU, UN, government sources) are securely downloaded via HTTPS. FinCEN names are uploaded by users in the application upon downloading the FinCEN list from a secure web-based interface.
  - Internal: Proprietary/private lists managed by the organization that can be managed through UI and API.
- *Ingestion Mechanism:*
  - Users securely upload CSV data to the Oracle Cloud Infrastructure (OCI) Object Store, partitioned by tenant to ensure data privacy and access control.

Staging, Business & Data Quality Process

This process allows users to prepare data for reliable screening while enforcing quality and business rules.

- *Data Pipeline*:
  - Cleansing: Standardizes names, dates, and removes inconsistencies (e.g., whitespace, encoding errors).
  - Validation: Ensures data is complete, accurate, and meets business rule requirements (e.g., mandatory fields, data types).
  - Enrichment (optional): Additional context or identifiers can be appended.
- *Categories Maintained:*
  - Party/Customer Data: Structured information about individuals or organizations.
  - External entity data: Structured information about Transaction counterparties
  - Watchlists: External and internal, consolidated for screening.

Index Loading & Search Preparation

- *Data Cleaning & Validation*: Verifies only high-quality, valid, and standardized data moves forward
- *Index Loader & REST Service*:
  - Cleaned data is relayed via REST APIs to an intermediate 'Index Loader.'
  - This decouples upstream processing from the search engine, allowing for asynchronous and extensible data flows.
- *Logstash Integratio*n: Leverages Logstash for advanced data transformations, enriching, and loading into OpenSearch.Pipeline: HTTP Input → Filter/Transform → Output/ OpenSearch Index
- *OpenSearch Index*:
  - Enables rapid searching, dynamic filtering, and analytics.
  - Designed for scalability, privacy, and auditability.

Screening & Matching Engine

- *Modes of Screening*:
  - Bulk (Batch) Matching: For scheduled/periodic, high-volume processing.
  - Real-time (Single) Matching: For “instant” checks—via API and UI—for onboarding or transactional triggers.
- *Matching Rule Management*:
  - Role-based secured environment for configuring matching parameters (algorithms, thresholds, fuzzy logic).
  - Change management and auditing for configuration changes.
- *Screening Execution*:
  - Matching engine queries OpenSearch for candidate matches on legal/known names, aliases, and other relevant identifiers.
  - Results surfaced through both REST API and user interface.

Alerting, Case Management, and Investigation

- *Alert Routing*: Positive/Partial matches (potential alerts) are automatically sent through REST API to the case management system (e.g., iHub).
- *Case Creation*: Cases triggered for individuals, entities, vessels, and external entities on:
  - Sanction matches
  - PEPs
  - Inclusion on adverse media/proprietary lists
  - Other exclusion/warning triggers
  - Prohibited country lists
  - FinCEN names.
- *Investigation*:
  - Investigators securely access the case management environment with strict logging and access controls.
  - Full audit trails maintained for all actions: assignment, escalation, investigation, and closure.

  - Cases can be worked, documented, and escalated as needed according to defined procedures.

Security, Access Control & Audit

- *Tenant Isolation*: Logical separation of data for each client/unit to guarantee confidentiality.
- *Secure Transmission/Storage*: HTTPS for all data flows; encryption at rest and in transit for sensitive data.
- *Role-based Access*: Least-privilege principle is applied across ingestion, configuration, investigation, and administration.
- *Audit Logs*: Detailed logs of key activities (ingestion, rule changes, investigations) for compliance and forensic review.

Audit

Comprehensive audit history maintained for:

- Cases created in the Investigation hub, for real-time and batch screening
- Private watchlist management
- Batch execution and screening
- Real-time screening

1.3 Generation of Canned Reports

The following information is about generating 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.

1.4 Generate a Case

The following information is 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.

1.5 Generate Alerts or Re-alerts

The following information is 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.

1.6 Manage Pipelines

This section details how to manage the CS pipelines.

Pre-configured, ready-to-use pipelines are available for batch and real-time screening for individuals and entities. Whereas 314A and external entity screening can be performed with batch screening. Data matches use Sanction, PEP, EDD, and PRB lists for individual, entity, and external entity screening, while 314A Screening uses FinCEN data matched against customer or external entity data. These out-of-the-box pipelines cannot be configured directly; they must first be copied, after which match attributes, rules, thresholds, and weightages can be modified.

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.

1.7 Load Customer Data to OpenSearch

The following information is 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.