

Oracle® Financial Crime and Compliance Management Cloud Services

Getting Started with Transaction Monitoring



24.2.1
F94159-02
February 2024

ORACLE®

Oracle Financial Crime and Compliance Management Cloud Services Getting Started with Transaction Monitoring, 24.2.1

F94159-02

Copyright © 2024, Oracle and/or its affiliates.

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

Contents

Preface

Audience	iv
Help	iv
Comments and Suggestions	iv
Related Resources	iv

1 About Transaction Monitoring

Quick Tour	1-2
Transaction Monitoring Workflow	1-4
Process Flow for Administrator	1-5

Preface


This preface introduces information sources that can help you use the application.

The following sections provide information that can help you use the application.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Investigation Hub Cloud Service or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

Help

Use Help Icon  to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access the <https://docs.oracle.com/en/> to find guides and videos.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: <https://support.oracle.com/portal/>.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud: <http://cloud.oracle.com>
- Community: Use <https://community.oracle.com/customerconnect/> to get information from experts at Oracle, the partner community, and other users.
- Training: Take courses on Oracle Cloud from <https://education.oracle.com/oracle-cloud-learning-subscriptions>.

1

About Transaction Monitoring

Oracle Financial Services Crime and Compliance Management Transaction Monitoring Cloud Service (FCCM TM Cloud Service) enables financial institutions to efficiently detect and investigate suspected money laundering activity to comply with current and future regulations and guidelines. It provides automated and consistent surveillance of accounts, customers, and third parties in transactions across all business lines. The application enables organizations to monitor customer transactions, using customer historical information and account profiles to provide a holistic view of transactions and activities. The scenarios are optimized for smaller financial institutions to detect, investigate, and report suspected money laundering and terrorist financing activities with simple configuration and operational control.

Key Features

The key features of the application include the following:

- Risk-based monitoring and investigations of suspicious activities that specifically target smaller financial institutions.
- In-built scenario library to detect the most common anti-money laundering scenarios.
- Ready to run data pipelines to prepare and optimize data for behavior detection, which includes an extensive library of data quality rule checks.
- Ability to create and tailor data and scenario pipelines to meet customer requirements.
- Ability to configure thresholds to provide optimum configuration.
- Ability to tune scenario parameters to provide optimum configuration.
- Robust in-built case management streamlines analysis and resolution in a single unified platform.
- Ability to generate operational reports of cases enhances data visualization and analyses. The ability to run reports is role-based, and users can generate reports and view them in tabular and graphical formats.
- Process Modeling Framework which facilitates built-in tooling for orchestration of human and automatic workflow interfaces. This enables Administrators to model business processes and create configurable workflows.

User Roles and Privileges

You can perform activities associated with your user group throughout the functional areas in the application. For more information about which actions can be performed by your user role, see User Roles and Privileges.

Security within the Application

Security layers control how you interact with the application. Users may only access cases that are mapped to their user group. For more information about mapping users to user groups, see [Application Security](#).

Table 1-1 Security Details within the Application

Security Layer Type	Controls	Description
Roles	Access to Features and Functions	This security layer identifies features and functions the user can access within the application. For example, Case Analysts can access and take action on cases.
Business Domains	Access to Case and Business Information	You can restrict access along operational business lines and practices, such as Retail Banking. Users can only see cases that are assigned to at least one of the business domains their user group is mapped to. For more information about Business Domains, see Configuring Business Domains .
Jurisdictions	Access to Case Information	You can restrict access using geographic locations or legal boundaries. Users can only see cases that belong to the jurisdiction their user group is mapped to. For more information about Jurisdictions, see Configuring Jurisdictions .

Quick Tour

The following table provides a bird's eye view of the tasks and the order to execute these tasks using the application. Click the links to read details of each task. You can use the links on this page to help you immediately begin using FCCM TM Cloud Service.

Table 1-2 Quick Tour

Order	Task	Who Does This?	Action
1	Subscribe	Tenant Admin	Subscribe to the application. You will receive a Welcome e-mail with the URL and temporary password.
2	Provision Users.	Sys Admin	Configure the Security Management System (SMS) to create users, assign roles, and implement user authorization and authentication. For more information, see Getting Started.

Table 1-2 (Cont.) Quick Tour

Order	Task	Who Does This?	Action
3	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.
4	Import and Create Pipelines	Data Admin	<ul style="list-style-type: none">• Import the ready-to-use pipelines. You can also create a copy of the imported pipelines and save it as a new pipeline.• Create new pipelines and configure them to meet your needs.
5	Configure Case Management	Sys Admin	<ul style="list-style-type: none">• Create This topic tells how to configure business domains. Business Domains, Jurisdictions, Case Actions, and .• Map Security Attributes, such as Case Actions to Status, and Case Scoring.• Metering
6	Set and Test Scenarios and Thresholds	Sys Admin	Create threshold sets to define tunable values for selected pipelines. <ul style="list-style-type: none">• To create threshold sets, see Managing Threshold Sets.• To test threshold sets, see Threshold Simulator.

Table 1-2 (Cont.) Quick Tour

Order	Task	Who Does This?	Action
7	Create and Execute Jobs and Batches	Sys Admin	Create jobs to define a collection of instructions for executing pipelines against threshold sets. Then create batches to run jobs at required intervals to identify and generate events. For more information, see Managing Batches and Scheduler Service .
8	Investigate Cases	Analysts and Investigators	Investigate and monitor money laundering activities that are generated as events. <ol style="list-style-type: none"> 1. Determine Which Cases to Work 2. Review Details of the Case 3. Document Your Decision 4. Take Action
9	Manage Investigation and Reporting	Supervisors	<ul style="list-style-type: none"> • Assign new cases and manage your team's backlog of cases. • Review cases and reports to verify that they are complete. • File SAR and create MIS reports.

Transaction Monitoring Workflow

Use the following workflow for FCCM TM Cloud Service.

Data Ingestion and Processing

Data ingestion loads the sample staging data, business domain, and jurisdiction data into the application for further processing. The application processes and prepares the data using various operations and data quality check rules such as filter, validate, derive, aggregate, join, and so on. During ingestion, the data is moved from the Common Staging Tables to the Business Tables to run scenarios.

Scenarios

Behaviors of interest, that is, potentially problematic behaviors with respect to possible money-laundering activities, are created as scenarios. The Transaction Monitoring scenarios are optimized for smaller financial institutions to detect suspected money laundering and terrorist financing activities with simple configuration and operational control. The required threshold parameters are defined in these scenarios. The data obtained from data ingestion are run using the scenarios to identify events or alerts.

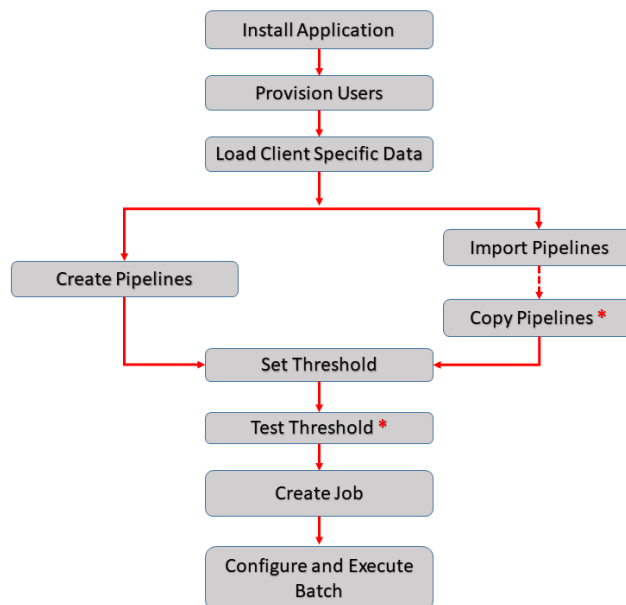
Investigate Cases

Transaction Monitoring enables analysts to identify and report suspected money laundering activities and investigate the events that are identified as cases.

Process Flow for Administrator

The system administrator configures the application.

Figure 1-1 Process Flow for Administrator



An asterisk * Indicates this step is optional. You can choose to copy pipelines and save it as a new copy based on your requirements.