Oracle FCCM Cloud Service Transaction Filtering

Performing Administrative Tasks

Release 24.05.01
F98388-01
May 2024

Oracle FCCM Cloud Service Transaction Filtering Performing Administrative Tasks, Release 24.05.01

F98388-01

Contents

Preface

1 About Oracle Financial Services Transaction Filtering

Preface

Performing Administrative Tasks introduces information sources that can help you use the Oracle Financial Services Transaction Filtering Cloud Service (OFS TF CS) application.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle Transaction Filtering Cloud services 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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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/.

1

About Oracle Financial Services Transaction Filtering

Introduction to Oracle Financial Services Transaction Filtering.

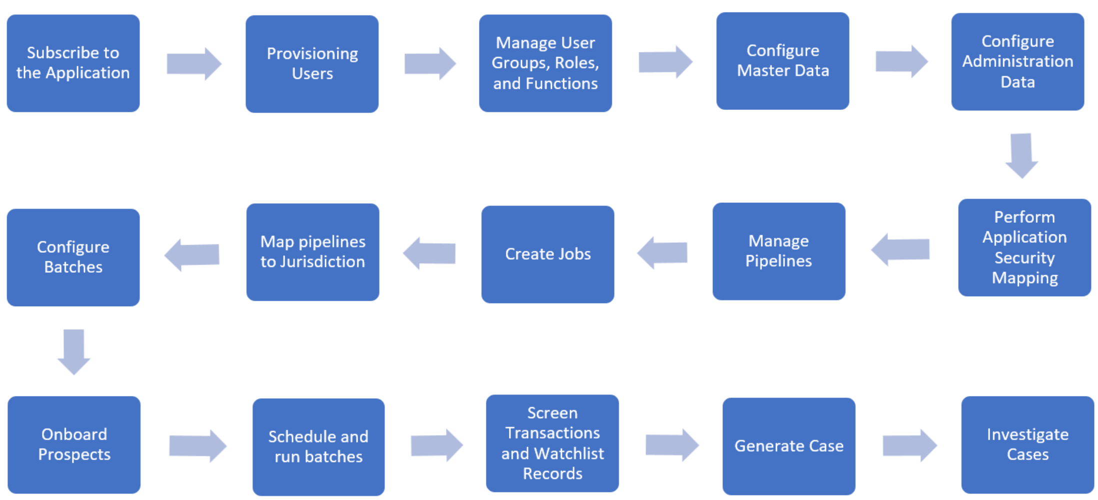
Oracle Financial Services Transaction Filtering is a Sanctions screening system that identifies Individuals, entities, cities, countries, goods, ports, BICs, and Stop keywords that may either be suspicious, restricted, or sanctioned with relation to a financial transaction that is processed through the Transaction Filtering application. The application enables you to integrate with any clearing or payment system, accept messages from the source system, and scans them against different watch lists maintained within the application to identify any suspicious data present within the message. The Transaction Filtering application can scan messages which are in the SWIFT, ISO20022, or Fedwire category.

1.1 Process Flow for Administrator

Tranasaction Filtering 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 move data between environments.

Figure 1-1 Process Flow for Administrator



1.2 Quick Tour of Transaction Filtering

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

Click the links to read details of each task.

Table 1-1 Quick Tour of Transaction Filtering

Order	Tasks	Details and Documentation Reference
1	Subscribe to the Application	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	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 Setup your Cloud Account.
3	Manage User Groups, Roles, and Functions	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	Configure Master Data	Define the master data values. For more information, see Master Data.
5	Configure Transaction Filtering Administration Data	Define the TF Administration data values. For more information message types, categories and configurations, see Transaction Filtering Administration.
6	Perform Application Security Mapping	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	Import the ready-to-use pipelines to the Transaction Filtering 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	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	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	Define batches specific to Transaction Filtering in the Scheduler Service window. For more information, see Managing Batches section of Pipeline Designer and Scheduler Service.
11	Onboard Prospects	TF supports both synchronous and asynchronous real-time API. For more information on the transaction messages, see Transaction Filtering API Guide.
12	Schedule and run batches	Schedule and run the TF-specific batches in the Scheduler window to load data. For more information, see Managing Batches section of see Pipeline Designer and Scheduler Service.

Table 1-1 (Cont.) Quick Tour of Transaction Filtering

Order	Tasks	Details and Documentation Reference
13	Screen Transactions and Watch list Records	Screen records against watch list data. For more information, see Matching Rules Widget. For editing the watchlist data, see Watchlist Management.
14	Generate Case	Cases are generated based on the matching rules and associated thresholds. For information on matching rule, see Matching Guide.
15	Investigate Cases	Investigate and monitor cases. For more information, see Investigating Cases.

1.3 Transaction Filtering Workflow

The figure illustrates the Transaction Filtering workflow.

Figure 1-2 Flow Diagram for Synchronous API

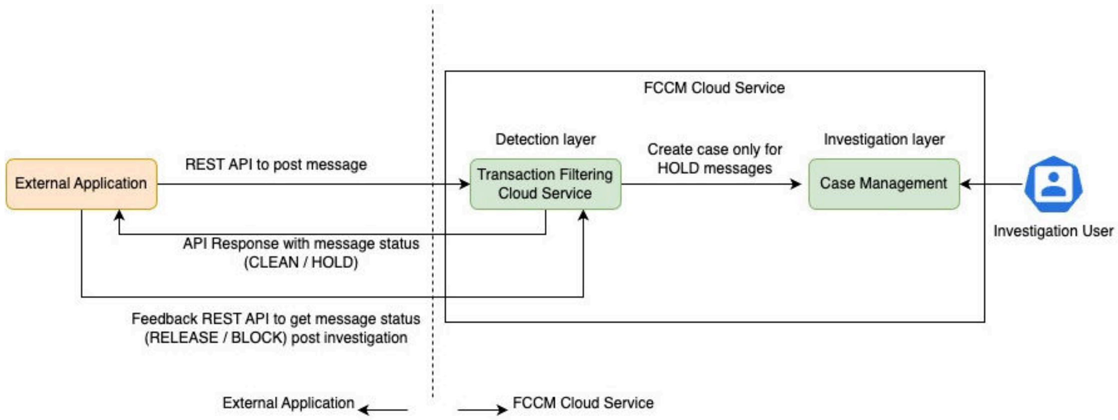
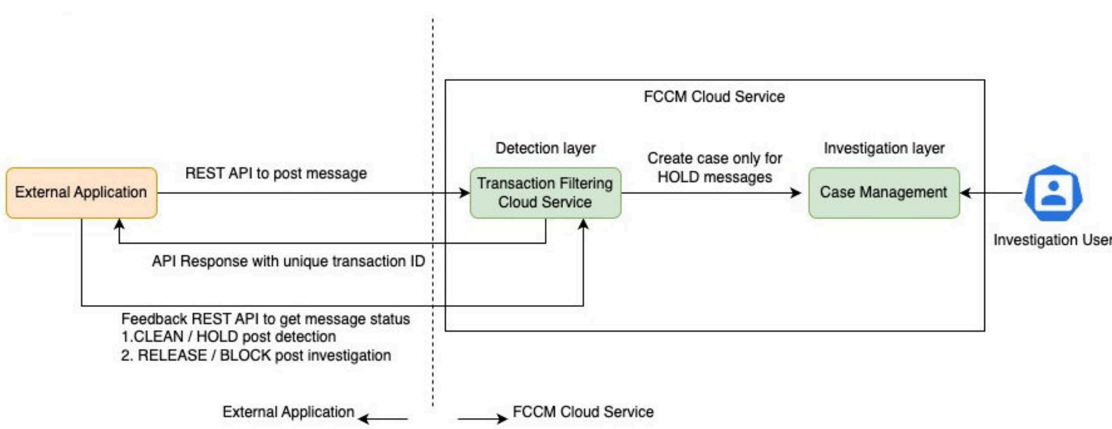


Figure 1-3 Flow Diagram for Asynchronous API



1.4 Load Transaction Data to OpenSearch

Infromation about loading transaction 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 to Identifier watchlist and load it to OS for matching, run the **IdentifierWatchlistLoad** batch in the Scheduler Service.
- To load the data to Country Watchlist and load it to OS for matching, run the **CountryWatchlistLoadbatch** in the Scheduler Service.
- To load the data to City Watchlist and load it to OS for matching, run the **CityWatchlistLoadbatch** in the Scheduler Service.
- To load the data to Goods Watchlist and load it to OS for matching, run the **GoodsWatchlistLoad** batch in the Scheduler Service.
- To load the data to Port Watchlist and load it to OS for matching, run the **PortWatchlistLoad** batch in the Scheduler Service.

1.5 Manage Pipelines

Information about managing the TF pipelines.

Matching configuration is set using the **Matching Rules** widget. Each widget defines a match configuration for a source (transaction) 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. A case 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 (Jaro Winkler, Levenshtein). Each attribute level match has a threshold, below which the score is not considered, and a weightage.

There are two ready-to-use pipelines that are used for SWIFT And Fedwire screening and ISO20022 screening.

1.6 Generate Alert

Information about generating an 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 transaction 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.

1.7 Generate a Case

Information about generating a case.

When one or more matches are recorded between a watch list and a transaction record record, a case is generated. If a new alert is generated, a new case is also generated in Enterprise Case Management (ECM).

1.8 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.