Oracle® Financial Crime and Compliance Management Cloud Services

Getting Started with Transaction Monitoring

25.11.01
G48403-01
November 2025

Oracle Financial Crime and Compliance Management Cloud Services Getting Started with Transaction Monitoring, 25.11.01

G48403-01

Copyright © 1994, 2025, 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

About This Content

Audience i
Help ii
Documentation Accessibility ii
Diversity and Inclusion ii
Related Resources ii
Conventions ii
Comments and Suggestions iii

1 About Transaction Monitoring

1.1 Quick Tour 2
1.2 Transaction Monitoring Workflow 4
1.3 Process Flow for Administrator 4

Copyright © 1994, 2025, Oracle and/or its affiliates.

About This Content

Use the Application Security Administration to help Administrators classify users and the data that they are permitted to access.

Audience

This guide is intended for administrator users who are tasked with creating and classifying users.

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 customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Resources

See these Oracle resources:

- FCCM Cloud Services Documentation

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.

Audience

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

Copyright © 1994, 2025, Oracle and/or its affiliates.

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.

Copyright © 1994, 2025, Oracle and/or its affiliates.

Convention	Meaning
`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/.

Copyright © 1994, 2025, Oracle and/or its affiliates.

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 Provision Users..

Copyright © 1994, 2025, Oracle and/or its affiliates.

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 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 Jurisdictions.

1.1 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.
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.

Copyright © 1994, 2025, Oracle and/or its affiliates.

Table 1-2 (Cont.) Quick Tour

Order	Task	Who Does This?	Action
4	Import and Create Pipelines	Data Admin	• 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	• Create 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. • To create threshold sets, see Managing Threshold Sets. • To test threshold sets, see Threshold Simulator.
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. 1. Determine Which Cases to Work 2. Review Details of the Case 3. Document Your Decision 4. Take Action

Copyright © 1994, 2025, Oracle and/or its affiliates.

Table 1-2 (Cont.) Quick Tour

Order	Task	Who Does This?	Action
9	Manage Investigation and Reporting	Supervisors	• 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.

1.2 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

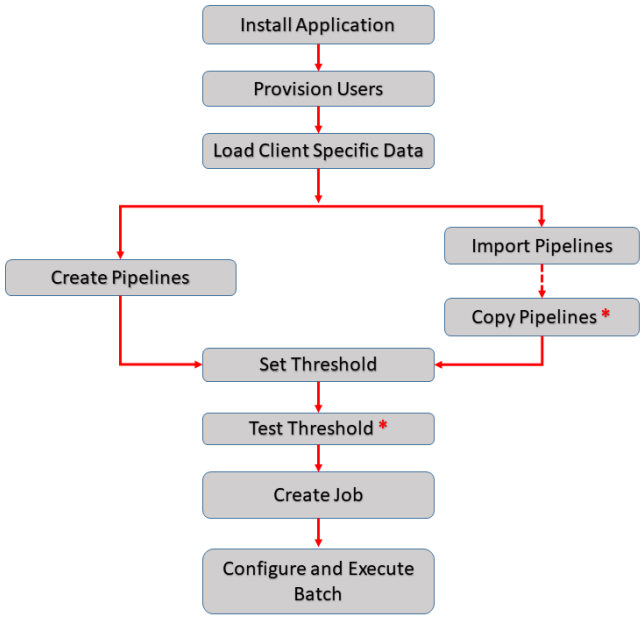
Transaction Monitoring enables analysts to identify and report suspected money laundering activities and investigate the events that are identified as cases.

1.3 Process Flow for Administrator

The system administrator configures the application.

Copyright © 1994, 2025, Oracle and/or its affiliates.

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.

Copyright © 1994, 2025, Oracle and/or its affiliates.