

Oracle® Financial Services Compliance Agent Cloud Service User Guide



Release 25.05.01

G35567-01

May 2025

ORACLE®

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

1 Preface

Audience	1-1
Comments and Suggestions	1-1
Help	1-1
Related Resources	1-1

2 Introduction

Getting Started	2-1
Accessing OFSCA	2-1
User Roles and Privileges	2-2
Editing the User	2-5
Deactivating the User	2-5

3 Configuring the Transaction Monitoring System

Recommend Scenarios	3-1
Select Red Flags	3-2
Select from Recommended Scenarios	3-3
View the Recommended Custom Scenarios	3-4
Configure Selected Scenarios	3-5
Upload Transaction Data	3-6
Treat Outliers	3-8
Review Threshold Recommendations	3-10
Set up accounts, channels, and limits	3-10
Create agents	3-11
Editing An Agent	3-14
Review	3-15
Resetting the Transaction Monitoring System	3-15
Recommend Initial Thresholds	3-17
Select scenarios and segment codes	3-18
Upload Transaction Data	3-20
Treat Outliers	3-22
Review Threshold Recommendations	3-24

Set up accounts, channels, and limits	3-24
Create agents	3-25
Editing An Agent	3-28
Review	3-29
Resetting the Transaction Monitoring System	3-29
User Defined Thresholds	3-31
Set up jurisdiction codes, scenarios, and thresholds	3-33
Map jurisdiction codes to segments	3-35
Set up accounts, channels, and limits	3-36
Design scenarios	3-37
Create agents	3-43
Editing An Agent	3-46
Upload transaction data	3-47
Review	3-49
Resetting the Transaction Monitoring System	3-52

4 Understanding the OFSCA Dashboard

Overall System Performance	4-2
Segment Performance	4-5

5 Running and Comparing Experiments

User Defined Experiment	5-1
Selecting the Segment	5-2
Selecting an Agent	5-2
Copying or Modifying the Control Set	5-3
Managing Scenarios Threshold Set Name	5-3
Managing Account-Transaction Product Constraints (per day)	5-10
Monitoring New Offerings	5-12
Reviewing the Experiment	5-14
Segment Strength	5-14
Generating Experiment from Recommendation	5-16
Generating Experiments for Segment	5-17
View Analysis	5-19
Comparing an Experiment	5-21
Comparing Experiments to Assess Risk of New Offerings	5-24
Risk of New Offering-Account Type	5-24
Risk of New Offering-Transaction Product	5-26

6	Modifying the System	
	Adding an Account	6-2
	Adding a Transaction Product	6-4
7	Navigating the OFSCA UI	
	Managing Users	7-1
	Creating a New User	7-2
	Managing Transaction Monitoring Performance	7-2
	Creating a New Experiment	7-3
	Managing Segments	7-3
	Managing Experiments	7-4
	Managing Offerings Setup	7-5
	Viewing Scenario Setup	7-6
	Using Documents	7-6
8	Understanding the OFSCA Metrics	
	Segment Strength Score	8-1
	System Strength Score	8-1
	Segment Performance	8-2
	Scenario Performance	8-2
	Account Vulnerability	8-2
	Channel Vulnerability	8-3
9	Appendix	
	How to Calculate the Target Amount	9-1
	Sample Template	9-1
	How to Calculate the CIB Parameter for Historical Activity	9-2
	Aggregates List	9-3
	Methodology	9-11
	Simulating Aggregates	9-12
	Fitting and Sampling from a Generative Model	9-12
	Recommending Thresholds	9-12
	Risks and Limitations	9-14
	Supported Scenarios (System Recommended Thresholds)	9-15
10	Glossary	

1

Preface

Canadian STR User Guide describes how to use Compliance Regulatory Reporting Application.

Audience

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

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/>.

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.

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>.

2

Introduction

OFS Compliance Agent (OFSCA) is an AI-powered experimentation platform that measures the performance of your Transaction Monitoring System (TMS), identifies areas for improvement, optimizes the system's performance, and provides evidence to support your decision-making.

Topics:

- [Getting Started](#)
- [Accessing OFSCA](#)
- [User Roles and Privileges](#)

Getting Started

To use FCCM Cloud Service, you need to activate the Cloud Service. Once the service is activated, you can onboard application users to access the subscribed cloud services. For more information, see the [Get Started with Oracle Financial Services Crime and Compliance Management Cloud Service](#).

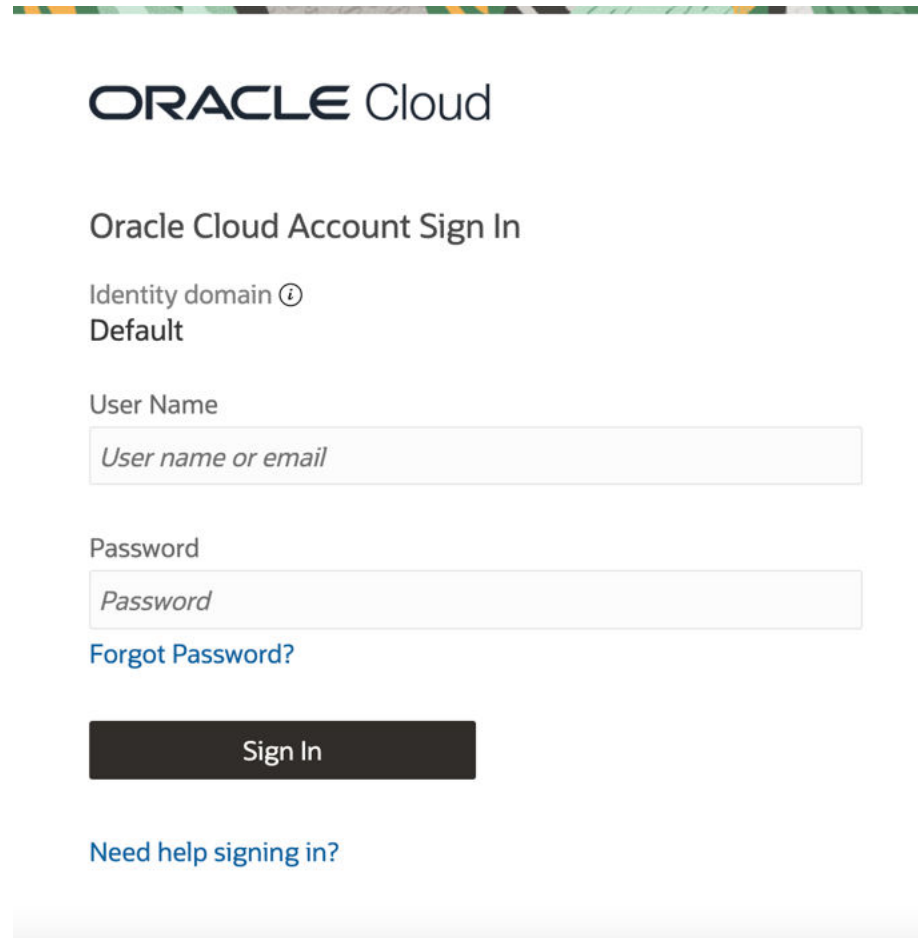
Accessing OFSCA

Once the Compliance Agent application is configured, you can access it by following these steps.

To access Compliance Agent, follow these steps:

1. Enter the application's URL in your browser to open the Login window.

Figure 2-1 Login Window

The image shows the Oracle Cloud Account Sign In window. At the top is the Oracle Cloud logo. Below it is the title "Oracle Cloud Account Sign In". There is a section for "Identity domain" with a dropdown menu showing "Default". Below that is a "User Name" field with a placeholder "User name or email". Below that is a "Password" field with a placeholder "Password". There is a link "Forgot Password?" below the password field. At the bottom is a "Sign In" button and a link "Need help signing in?".

ORACLE Cloud

Oracle Cloud Account Sign In

Identity domain ⓘ
Default

User Name
User name or email

Password
Password

[Forgot Password?](#)

Sign In

[Need help signing in?](#)

2. Enter your login credentials (User Name and Password) to sign in.
3. Click on **Sign In** to access the Compliance Agent application.

User Roles and Privileges

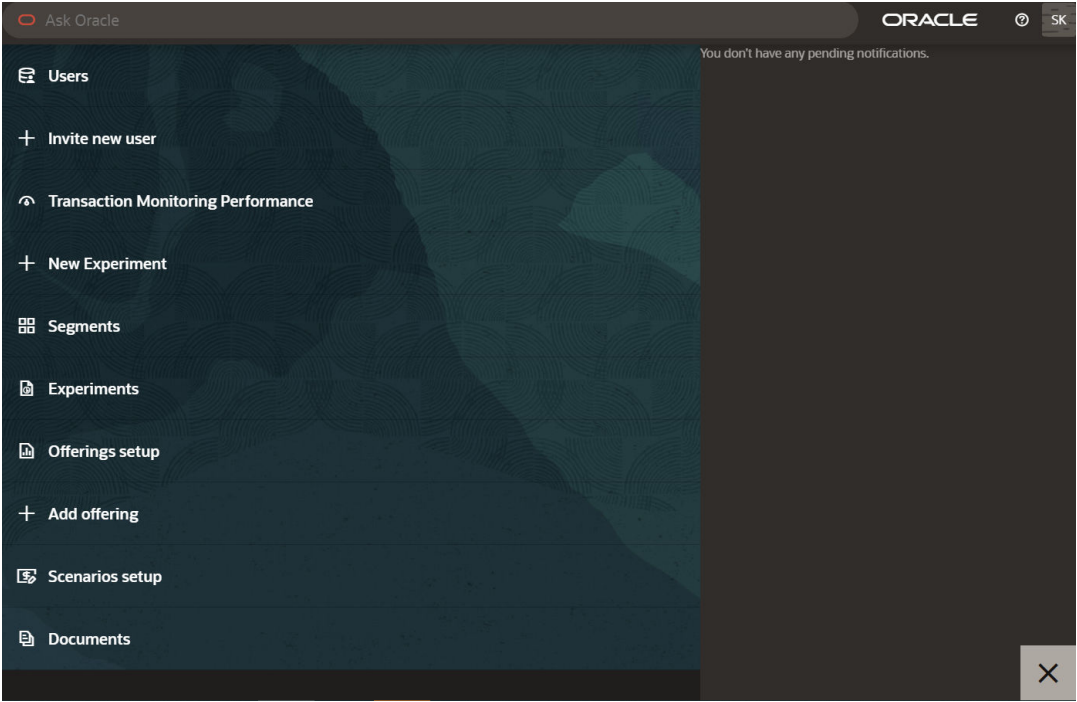
Topics:

- [Editing the User](#)
- [Deactivating the User](#)

The Compliance Agent application utilizes a role-based access control model, meaning that users are granted specific roles to access different application functionalities. To create a new user and assign a role type in the Compliance Agent application, an administrator user can follow these steps:

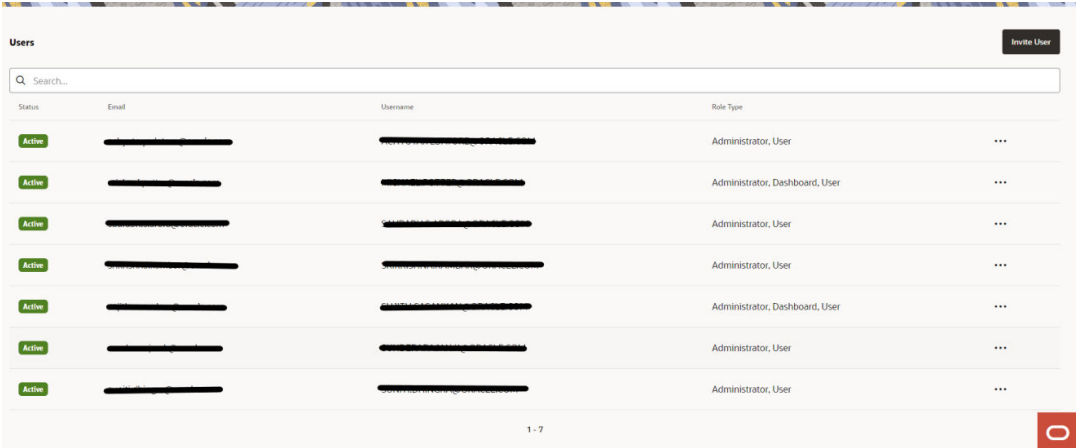
1. Click **Open Ask Oracle**  to display the Ask Oracle window. The following window is displayed.
2. Click **Users** menu to display the Users window. The following window is displayed

Figure 2-2 Application Menu



3. Click **Users** menu to display the Users window. The following window is displayed.

Figure 2-3 Users



4. Click **Invite User** to create a new user. The following window is displayed.

Figure 2-4 Invite Users

The 'Invite User' dialog box is shown with the following fields and labels:

- First Name (Required)
- Last Name (Required)
- User Name (Required)
- Email (Required)
- Role type (Required)

Buttons: Cancel, Invite

5. Enter the following details:
 - First Name: Enter the First Name of the user
 - Last Name: Enter the Last Name of the user
 - User Name: Enter the name of the user
 - Email: Enter the Email of the user
6. Select the required **Role** type from the drop-down list. The available options are Admin and User
 - a. Admin: Admin can add other users to the system and assign them rights. An admin can also access the application
 - b. User: User can access the application.

 Note:

The Invite User window is displayed only if you are logged in as Administrator.

7. Click **Invite** to create the required user for the system.

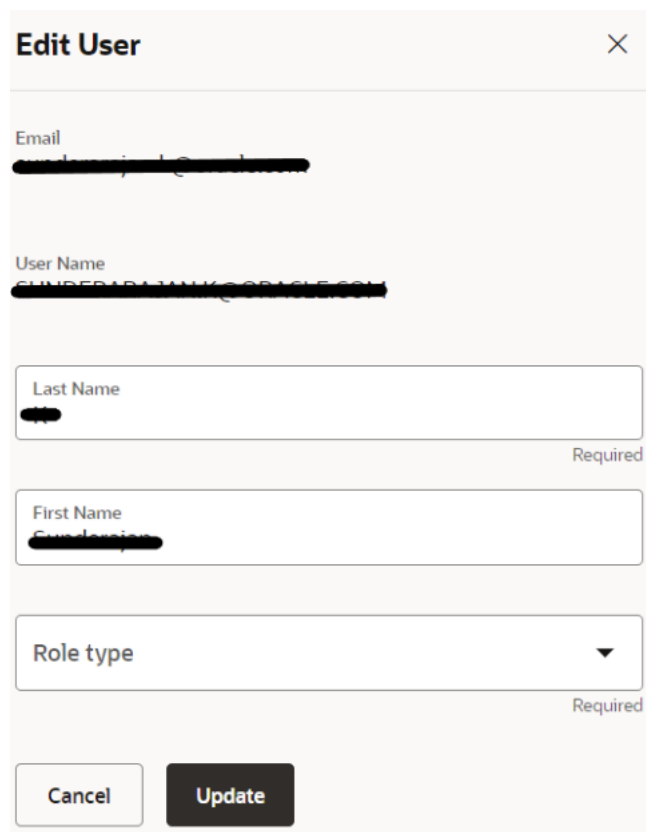
Editing the User

An administrator user can edit the user information of a selected user in the Compliance Agent application.

To edit the user information, follow these steps:

1. Click **Action**  icon of the selected user in the User window and then click Edit user. The following window is displayed.

Figure 2-5 Edit User



2. Edit the required fields.

 Note:

You cannot edit the User Name and Email fields.

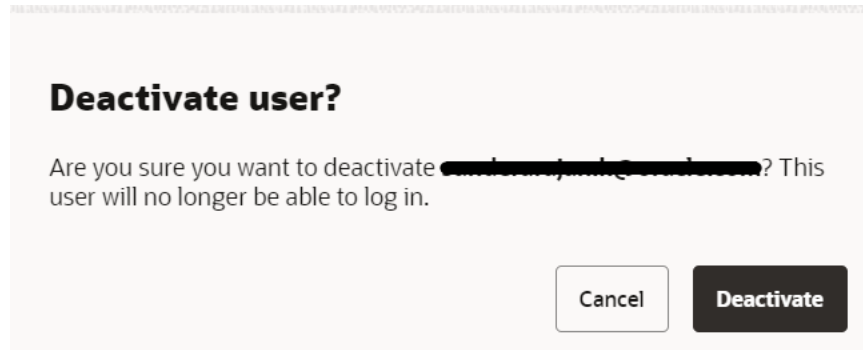
Deactivating the User

An admin user can deactivate the user information of a selected user in the Compliance Agent application.

To deactivate the selected user, follow these steps:

1. Click **Action**  icon of the selected user in the User window and then click Deactivate user. The confirmation window is displayed.

Figure 2-6 Deactivate Users



2. Click **Deactivate** to deactivate the selected user. Once deactivated, the user cannot log in to the system

3

Configuring the Transaction Monitoring System

See the following three options that you can take sequentially or independently:

1. If you select *Recommend Scenarios*, the *Recommend Initial Thresholds* module will apply to the same set of Scenarios. And the same Scenarios are used in the *Assess your Transaction Monitoring System* module.

Note:

The template for the *Recommend Initial Thresholds* module will be populated with inputs needed for the Scenarios in the *Recommended Scenarios* module.

2. If you select the *Recommend Initial Thresholds* module, you will be guided to through its flows.
3. If you select the *Assess your Transaction Monitoring System* module, you will be guided to the old flow of providing Scenarios Thresholds and Constraints in the csv.

You can configure your Transaction Monitoring System by following these three options, that you can perform sequentially or independently:

- **Recommend Scenarios:** If you want to use system recommended scenarios to assess your Transaction Monitoring System. If you select *Recommend Scenarios*, the *Recommend Initial Thresholds* module will apply to the same set of Scenarios. And the same Scenarios are used in the *Assess your Transaction Monitoring System* module.

Note:

The template for the *Recommend Initial Thresholds* module will be populated with inputs needed for the Scenarios in the *Recommended Scenarios* module.

- **Recommend Initial Thresholds:** If you want to generate initial threshold recommendations for new Oracle Behavior Detection scenarios and then assess your Transaction Monitoring System. If you select the *Recommend Initial Thresholds* module, you will be guided to through its flow.
- **User Defined Thresholds:** If you want to assess your Transaction Monitoring System with the pre-defined/user-defined thresholds. If you select the *Assess your Transaction Monitoring System* module, you will be guided to the old flow of providing Scenarios Thresholds and Constraints in the csv.

Recommend Scenarios

This section describes the system recommended Scenarios.

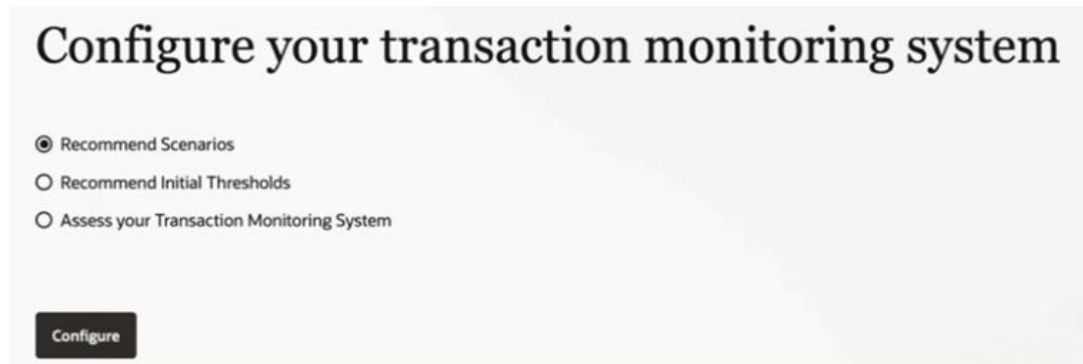
Configuring the Transaction Monitoring System involves the following processes:

1. [Select Red Flags](#)
2. [Select from Recommended Scenarios](#)
3. [Configure Selected Scenarios](#)
4. [Upload Transaction Data](#)
5. [Treat Outliers](#)
6. [Review Threshold Recommendations](#)
7. [Set up Accounts, Channels, and Limits](#)
8. [Create Agents](#)
9. [Review](#)

To configure your transaction monitoring system, follow these steps:

1. Click the OFSCA URL enter username & password, and press Enter. The **Configuration** page is displayed:

Figure 3-1 Recommend Scenarios



2. Select **Recommend Scenarios** and click **Configure**. The **Recommend Scenarios - Step 1** page is displayed.

Select Red Flags

In this step you will need to select the Red Flags for which you want to generate recommended Scenarios.

Compliance Agent can recommend scenarios that are best suited to monitor these red flags.

To select the Red Flags for Scenario recommendations, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.

Figure 3-2 Select Red Flags

Configure your transaction monitoring system

Specify the Red Flags for which you want to Recommended Scenarios

Upload a csv file with list of Red Flags

[Download Template](#)

Use this template to specify the Red Flags for which you want Scenario Recommendations.

Drag and Drop
Supported formats: CSV

[Discard](#) [Clear](#) [Continue](#)

1 | 9

- Select Red Flags
- Select from Recommended Scenarios
- Configure Selected Scenarios
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations
- Set up accounts, channels and limits

2. Add the Red Flags and save the CSV file.
3. Click **Drag and Drop**, and place the filled in template. You can see a preview of the uploaded CSV file.
4. Click **Continue** to navigate to the Select from Recommend Scenarios step.

Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Click **Clear** to start the Configure your Transaction Monitoring System from the initial steps again for configuration.

Select from Recommended Scenarios

In this step, you will specify the new scenarios you wish to deploy and generate recommendations for.

The system will evaluate the data you uploaded in the previous step, which may take some time, before displaying the recommended Scenarios.

Once the evaluation is complete, you can review the Red Flags you uploaded earlier alongside the recommended scenarios for each one. This includes viewing their corresponding scores and confidence levels.

The recommended scenarios are ranked based on their Confidence Level and Score.

Table 3-1 Sample Table

SL#	Deciding Criterion	Confidence Level
1	If the top three scenarios add up to ≥ 0.95 probability	High
2	If the top three scenarios adds in the probability range of < 0.95 and ≥ 0.75	Medium
3	If the top three scenarios add up to < 0.75 probability	Low

If the recommended scenario is not appropriate for your requirement, you can choose one or more scenarios from the Selected Scenario column.

Figure 3-3 Select from Recommended Scenarios

Red Flag	Recommended Scenario	Confidence Level	Selected Scenario	Score
Transactional activity suggests that a transaction may be	CIB: Significant Change from Previous Peak Activity	low		.34
Transactional activity suggests that a transaction may be	(ML/CU) Single or Multiple Cash Transactions: Large	low		.12

1 rows selected Total 6

Configure Custom Scenarios (Optional)

Choose Red Flag for Recommendation

The customer's business account shows large purchases of luxury
Transactional activity suggests that a transaction may be inconsis

Last saved
Thursday, May 15, 2025 11:02 Zulu

Discard Continue

2 | 10

- Select Red Flags
- Select from Recommended Scenarios**
- Configure Selected Scenarios
- View Recommended Custom Scenarios
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations

If you choose **Configure Custom Scenarios**, you will be redirected to the **View Recommended Custom Scenarios** page. However, if you do not choose **Configure Custom Scenarios**, you will be redirected to the **Configure Selected Scenarios** page.

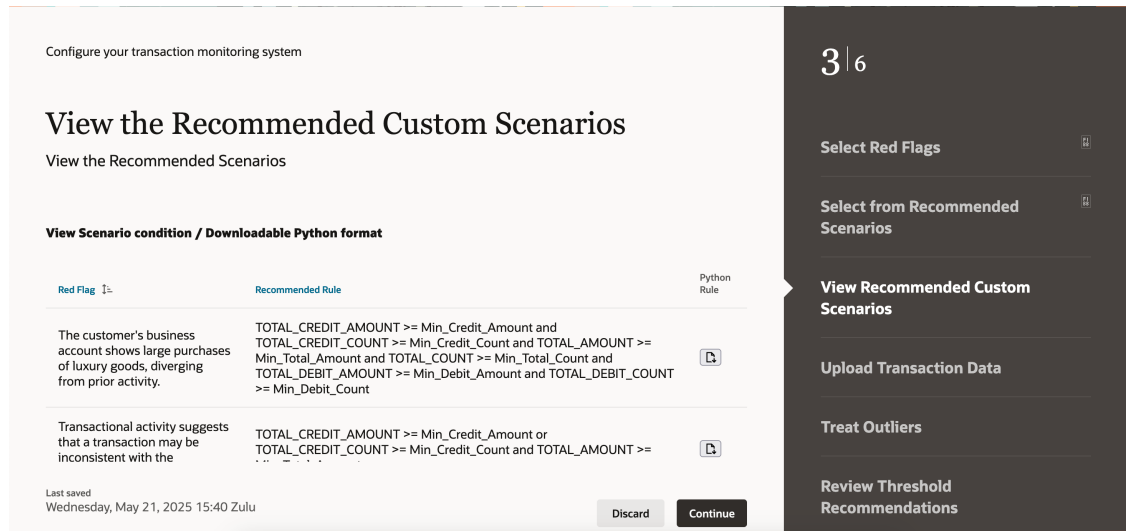
Click **Continue** to navigate to the Select Segments step.

View the Recommended Custom Scenarios

In this step you can review and download the recommended custom scenario rule in Python format.

This step presents a list of recommended custom scenarios based on the Red Flags selected in the previous step. Each scenario includes a short description of the selected Red Flag along with a corresponding recommended rule generated to detect the red flag activity. The clipboard icon corresponding to the red flag allows you to download the Python code for further implementation.

Figure 3-4 View the Recommended Custom Scenarios



Once you've reviewed the suggested rules, click **Continue** to proceed to the next step [Upload Transaction Data](#).

Configure Selected Scenarios

In this step you will specify the segments where the selected scenarios are to be deployed and configure the non-tunable parameters of the scenarios.

To proceed, upload a CSV file containing a list of new scenarios and values for non-tunable parameters as per the prescribed template.

Note that OFSCA does not provide threshold recommendations for non-tunable parameters, as these should be determined by the business needs and expertise of the institution's Anti-Money Laundering (AML) subject matter experts.

The Recommended Value will be generated at the end of the process.

To setup the Segments, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.

Figure 3-5 Configure Selected Scenarios
Note:

- Do not modify the column names of the CSV file.
- If you are not using the default risk tiers (RR/MR/HR) at your institution, each of these thresholds (for example, Min_Amt_RR, Min_Amt_MR and Min_Amt_HR) should be set to the same value.

2. Enter the segment_name for each of the rows.
3. Add the values (cells marked as **N**) for non-tunable parameters.
4. Enter the current_value for the cells where tunable_parameter is **N** and save the file.
5. Click **Drag and Drop**, and place the CSV file. You can see a preview of the uploaded CSV file.
6. Click **Continue** to navigate to the Upload Transaction Data step.

Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Click **Clear** to start the Configure your Transaction Monitoring System from the initial steps again for configuration.

Upload Transaction Data

In this step you will need to provide transaction aggregates.

Upload a csv file with aggregates for each transaction product for credits and debits.

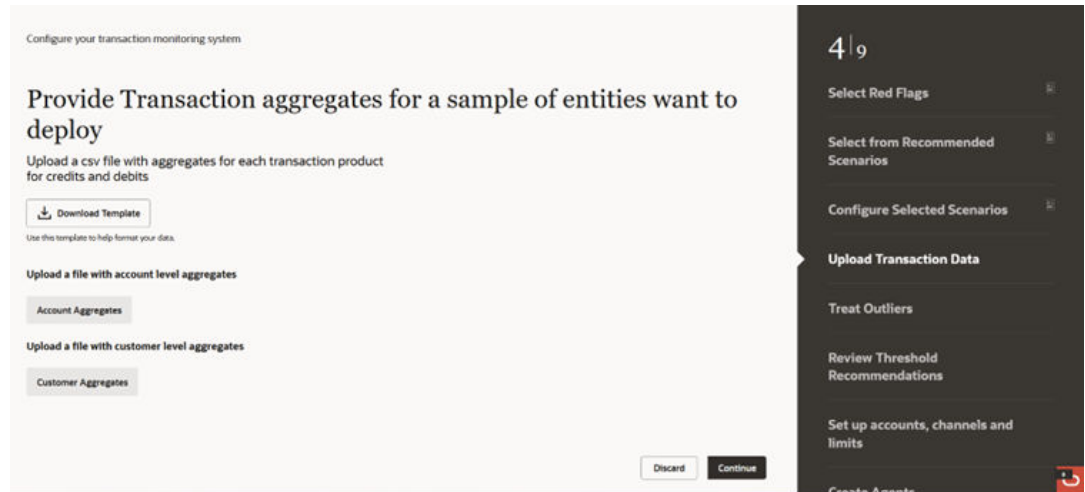
The template requires you to provide aggregates extracted from historical transaction data depending on the scenario.

See [Supported Scenarios \(System Recommended Thresholds\)](#) for more details.

To upload Transaction Aggregates, follow these steps:

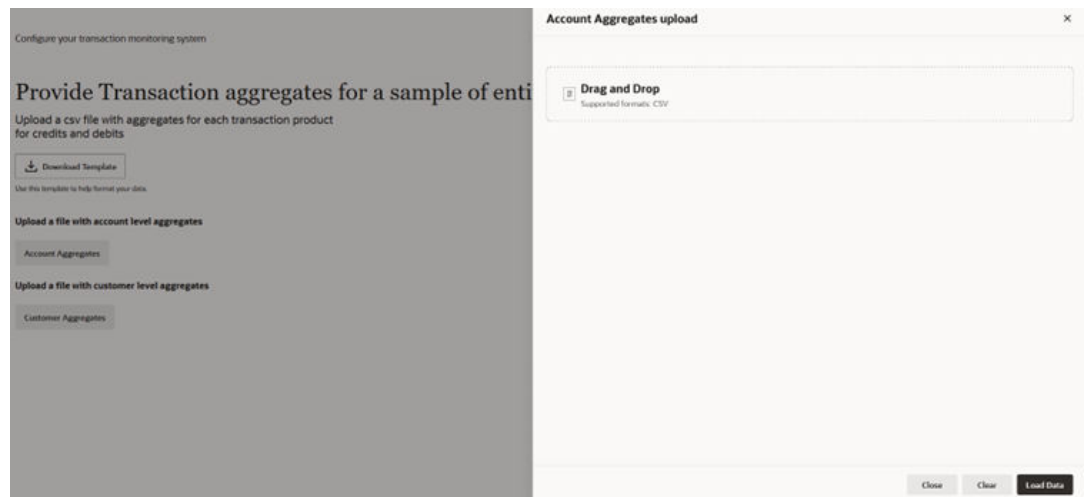
1. Click **Download Template**. The CSV file is downloaded.
2. Fill in the required information in the template.

Figure 3-6 Upload Transaction Data



3. Click **Account Aggregates** to upload the data. The Account Aggregates page opens on the right of your screen.

Figure 3-7 Upload Account Level Aggregates



4. Click **Drag and Drop** and upload the data.
5. Click **Load Data** upload the Account Level Aggregates.
Click **Close** to close the page.
Click **Clear** to clear the loaded data.

Figure 3-8 Account Level Aggregates Preview

Account Aggregates upload

Loaded File
acc_dl.csv

Segment Name	Month ID	Transaction Product	Direction	Total Amount	Total High Risk Amount
SEGMENT_NAME	MONTH_ID	TRANSACTION_PRODUCT	DIRECTION	TOTAL_AMOUNT	TOTAL_HIGH_RISK
AMEA	01/01/23	EFT	Credit	47471	3
AMEA	01/01/23	EFT	Debit	25563	3
AMEA	01/01/23	EFT-Fedwire	Credit	18130	3
AMEA	01/01/23	EFT-Fedwire	Debit	44169	6

1 - 5 >

Close

Clear

Load Data

Click **Account Aggregates** again to preview the Account Level Aggregates data.

6. Upload the **Customer Level Aggregates**. To upload, see the steps 3, 4, and 5.
7. Click **Continue** to navigate to the Treat Outliers step.

Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Treat Outliers

In this step you will need to remove outlying values from the uploaded data based on two approaches - Inter Quartile Range (IQR) and Percentile

If you select IQR, the available options for thresholds are 1.5 IQR, 2 IQR, and 3 IQR.

If you select percentile, the available options for thresholds are 1, 5, and 10.

Select tails - Left Tails Only or Right Tails Only or Both to trim data.

Table 3-2 Outlier Combination

SL#	Approach	Tails	Thresholds	Outlier Treatment Logic
1	Inter Quartile Range	Left Tail only	1.5 IQR	Remove the values which are less than $Q1 - 1.5 \text{ IQR}$.
2	Inter Quartile Range	Right Tail only	1.5 IQR	Remove the values which are greater than $Q3 + 1.5 \text{ IQR}$.
3	Inter Quartile Range	Both Tails	1.5 IQR	Remove the values which are less than $Q1 - 1.5 \text{ IQR}$ and the ones which are greater than $Q3 + 1.5 \text{ IQR}$.
4	Percentile	Left Tail only	5	Remove the values which are less than 5th percentile.
5	Percentile	Right Tail only	5	Remove the values which are greater than 95th percentile.
6	Percentile	Both Tails	5	Remove the values which are less than 5th percentile and the ones which are greater than 95th percentile.

To remove Outliers, follow these steps:

1. Select an Outlier Removal Approach – **Inter Quartile Range** or **Percentile**.
2. Select Tails - **Left Tails Only** or **Right Tails Only** or **Both**.
3. From the **Thresholds** drop-down, select a threshold.

Figure 3-9 Remove Outliers

4. Click **Continue** to view the recommended Threshold values. The system calculates the initial thresholds.

Or click **Discard** to discard the current activity.

Click **Download** to the data and review. You can also edit the data and upload again.

Review Threshold Recommendations

In this step you can review the Threshold recommendations.

Figure 3-10 Review Recommended Thresholds

Configure your transaction monitoring system

Review Recommended Thresholds

View the Recommended Threshold Values

Recommended Values Edit

Segment Name	Scenario Name	Parameter Name	Recommended Values
AMEA_HR	(ML/AC) High Risk Transactions: High Risk Geography	Min_HRG_Total_Trans_Amt	25887.09
AMEA_HR	(ML/AC) Anticipatory Profile - Expected Activity	HR_Min_Pct_Com_Pre_Dep_Amt_Inc	0
AMEA_HR	(ML/AC) High Risk Transactions: High Risk Geography	Min_HRG_Trans_Amt_Primary	88772.1
AMEA_HR	(ML/AC) High Risk Transactions: High Risk Geography	Min_Perc_HRG_Amount	47
AMEA_HR	(ML/AC) High Risk Transactions: High Risk Geography	Min_HRG_Trans_Amt_Secondary	88772.1

Last used
Friday, April 11, 2025 10:30 Zulu

Download Discard Continue

6/9

- Select Red Flags
- Select from Recommended Scenarios
- Configure Selected Scenarios
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations**
- Set up accounts, channels and limits

Click **Discard** to discard the current activity.

Click **Download** to the data and review. You can also edit the data and update the values in case there is a change needed.

Set up accounts, channels, and limits

In this section you will configure the various products (accounts and channels) offered tovarious segments within your institution.

You will also specify any limits or restrictions imposed on these products for each segment. Upload a CSV file with accounts, channels and limits in use by each segment.

The template requires filling of details – Jurisdiction, Segment Name, Account Type, Channel, and Withdrawal Limit.

To setup segments, accounts, channels, and limits, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.
2. Fill in the required information in the template.
3. Click **Drag and Drop**, and place the filled in template. You can see a preview of the uploaded CSV file.

Figure 3-11 Set up segments, accounts, channels and limits
Note:

- If a channel does not have a withdrawal limit, this can be indicated as NA instead of a number.
- You can remove the uploaded CSV file if required by using the **Clear** button.

4. Click **Continue** to navigate to the Create an agent for each segment step.

Create agents

When creating an agent, a Human Trafficking (HT) agent is automatically generated by default. However, you may need to create a new agent for a segment in the following scenarios:

- If the expected activity of the segment changes and hence the target amount has to change.
- When the distribution of accounts used by customers in the segment changes and hence distribution of accounts changes.

Figure 3-12 Create an agent for each segment

To create an agent, follow these steps:

1. Click **Create Agent** to create an agent for each segment. The **New Agent** page is displayed

Figure 3-13 New Agent

New Agent

Agent AMEA_HR

Agent Name
AMEA_HR Agent nn

Agent Description

Target Account

Amount to transfer (in 1 month)
Expected monthly activity for the suspicious customer in this segment

Maximum Required Minimum Required

Intermediate Accounts

Intermediate Account Distribution percentage 0

Intermediate Account Distribution percentage 0

Intermediate Account Distribution percentage 0

Intermediate Account Distribution percentage 0

Cancel Create Agent

2. Enter the **Agent Description**. The description can be used to note any specific products or channels the agent has access to. A good description can help you determine if this agent can be reused in future experiments.
3. Select the required option from the **Target Account** drop-down list. In this example, the available options are RBK, CBK, and RBR.
4. Enter the Maximum and Minimum amount for the segment in the respective fields.

 Note:

- The maximum and minimum should be equal to amounts that are in the unusual range for the segment.
- To calculate target amounts, see the suggested query in the [How to Calculate the Target Amount](#) section.
- Ensure that the Max Target Amount is set such that the granularity (Max Target Amount/20) is lower than any limits that have been set. E.g., if the limit for a channel is \$ 10,000 then the Max Target Amount should be lower than \$200,000.

5. Select the required Intermediate Account from the drop-down list.

 Note:

You can create a maximum of four intermediate accounts for each segment.

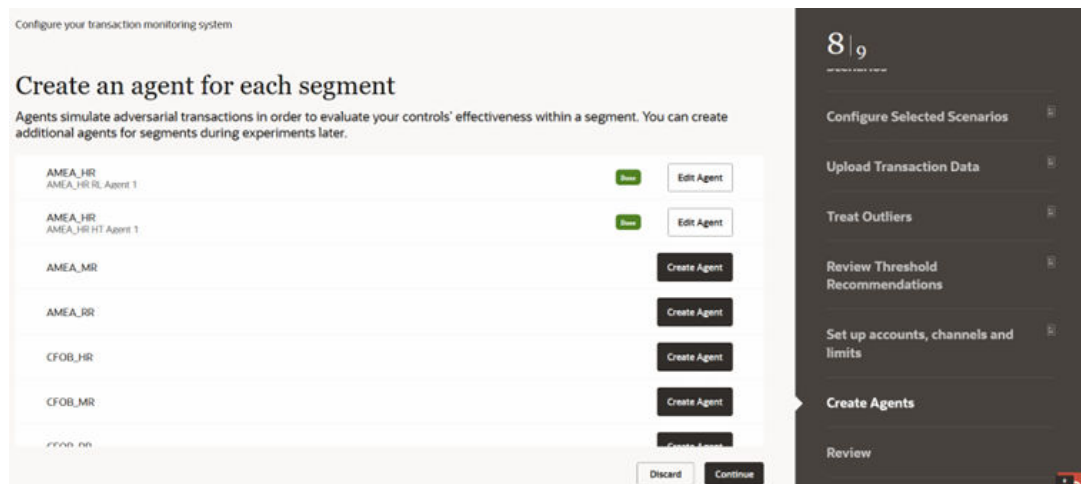
6. Select the required Distribution percentage from the drop-down list. The distribution must approximately reflect the product portfolio for the chosen segment. If a segment has more than four products, the four most widely used or four riskiest products can be considered.

 Note:

The total distribution percentage of all the intermediate accounts must be equal to 100 percentage.

7. Click **Close**  icon to close the Intermediate Account for the segment.
8. Click **Add Another** to add another Intermediate Account for the segment.
9. Click **Create Agent** to create an agent. The following page is displayed.

Figure 3-14 Agent Created



Similarly, you can create an agent for multiple segments.

10. Click **Continue** to navigate to the Review step.

Editing An Agent

This section describes how to edit the created agent for each segment if required.

To edit the created agent, follow these steps:

1. Click **Edit Agent** to edit the required fields. The following page is displayed.

Figure 3-15 Edit Agent

Edit Agent [X]

Agent AMEA_HR

Agent Name: AMEA_HR RL Agent 1

Agent Description: This is for AMEA_HR

Target Account: CBK

Amount to transfer (in 1 month)
Expected monthly activity for the suspicious customer in this segment

Maximum: 1499 (Required)

Minimum: 501 (Required)

Intermediate Accounts

Intermediate Account	Distribution percentage	
CBK	100	
Intermediate Account	0	⊗
Intermediate Account	0	⊗
Intermediate Account	0	⊗ ⊗

Cancel Save Agent

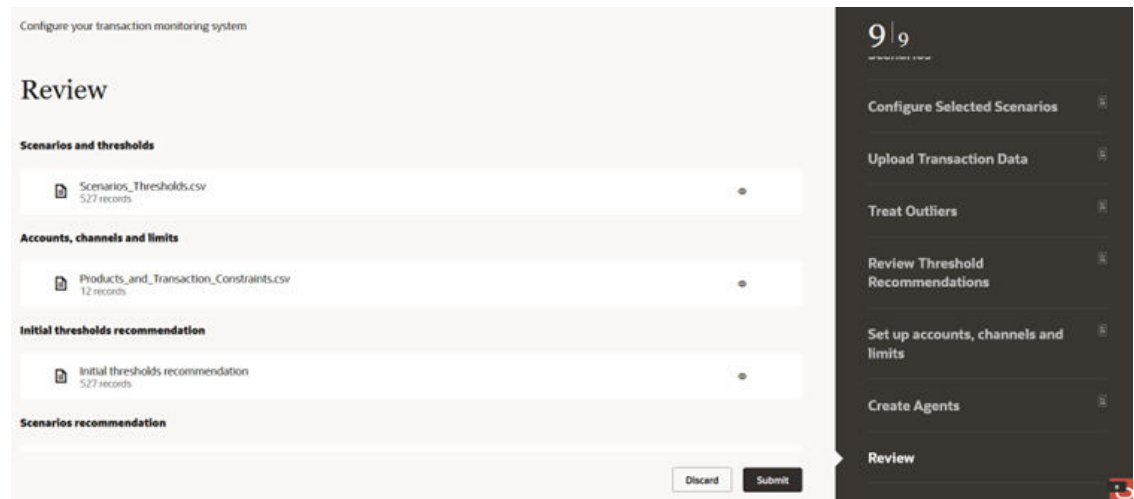
2. Click **Save Agent** to save any modifications made to the agent.

Review

In this step, you can review the uploaded data and created agents for each of the segments.

Click the **View** icon in under the **Scenarios and thresholds**, **Jurisdiction codes**, **segments**, **accounts**, **channels and limits**, and **Initial thresholds recommendation** sections to view the uploaded products and transaction constraints.

Figure 3-16 Review the System



Click **Submit** to configure your transaction monitoring system. You can now view the Transaction Monitoring Performance-related details.

You can also view details the by clicking the respective tabs for Segments and Experiments.

Resetting the Transaction Monitoring System

This section describes how to reset your transaction monitoring system configuration in OFSCA.

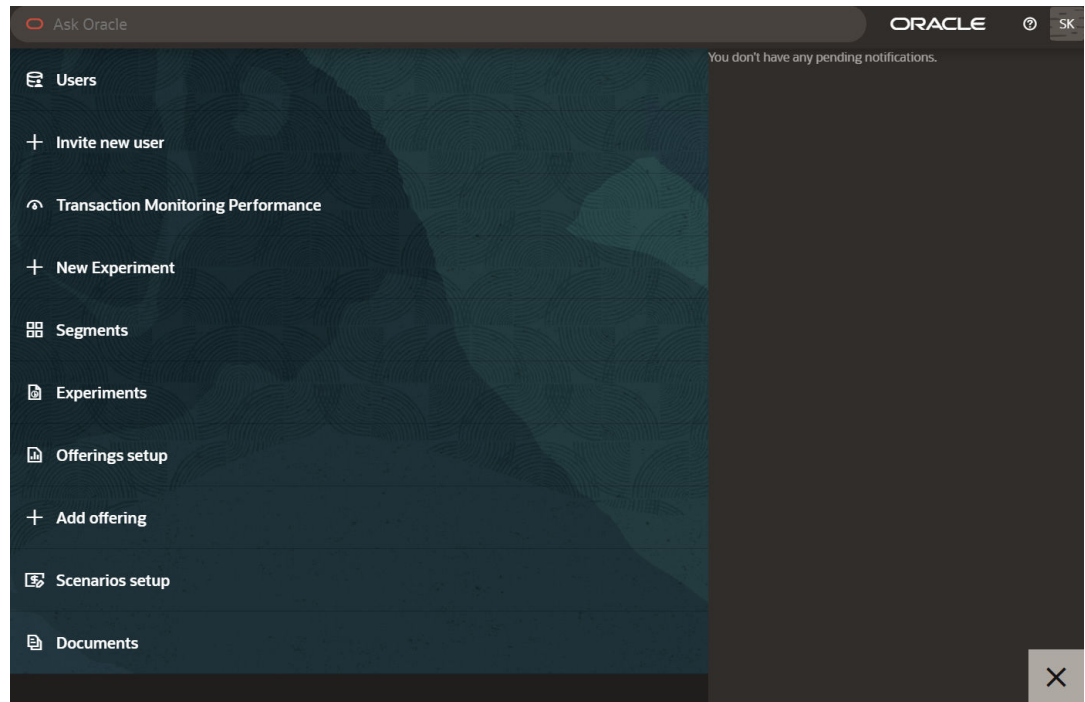
To reset the system and initial configuration, follow these steps:

1. Click



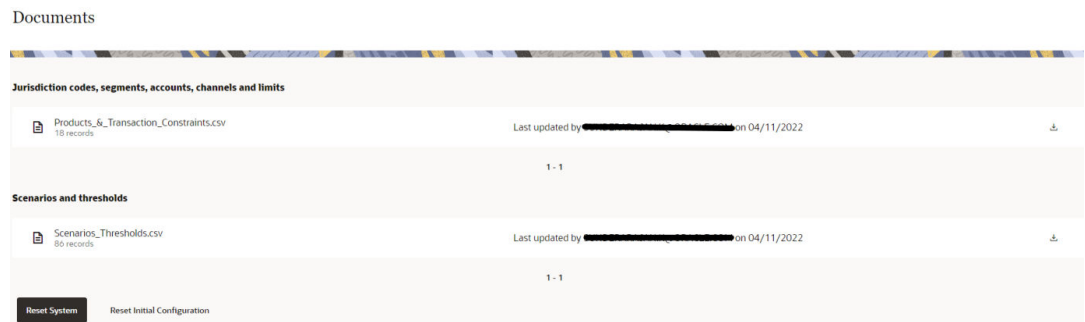
Open Ask Oracle to display the Ask Oracle window. The following window is displayed.

Figure 3-17 Application Menu



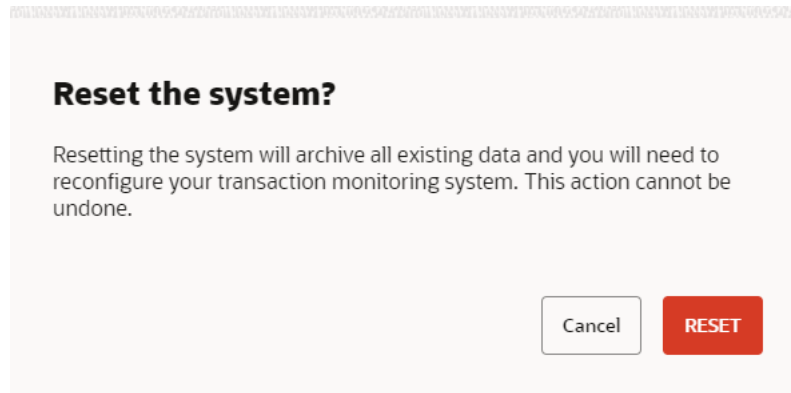
2. Click **Documents** menu to display the Documents window. The following window is displayed.

Figure 3-18 Documents Menu



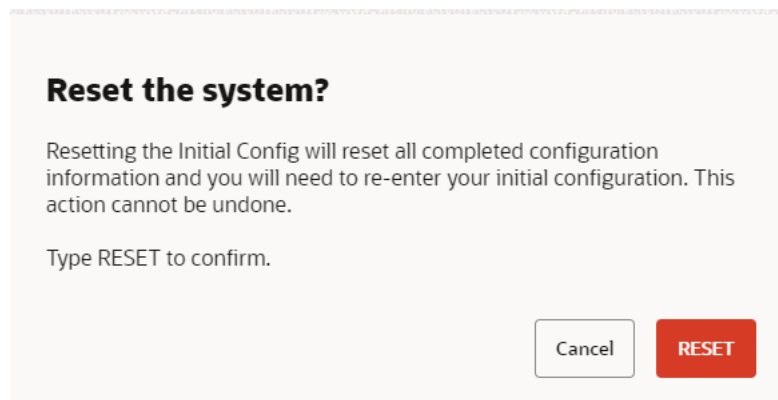
3. Click **Reset System** to reset your transaction monitoring system. The confirmation window is displayed.

Figure 3-19 Reset System



4. Click **RESET** to reset the system. It will archive all the existing data and you need to reconfigure your transaction monitoring system. Or Click **Cancel** to cancel the action.
5. Click **Reset Initial Configuration** in the Documents window to reset the initial configuration. The confirmation window is displayed.

Figure 3-20 Reset the Initial Configuration



6. Click **RESET** to reset the initial configuration. It will reset all the completed configuration information and you need to reconfigure your initial configuration. Or Click **Cancel** to cancel the action.

Recommend Initial Thresholds

You can configure the Transaction Monitoring System so that it can also help in recommending Thresholds for New Scenarios.

Configuring the Transaction Monitoring System involves the following processes:

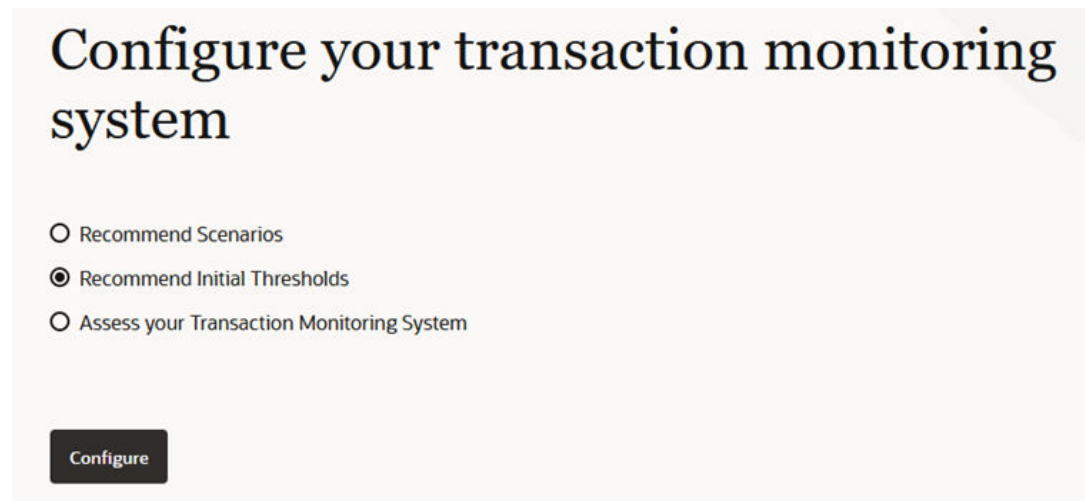
1. [Select Scenarios and Segment Codes](#)
2. [Upload Transaction Data](#)
3. [Treat Outliers](#)
4. [Review Threshold Recommendations](#)
5. [Set up Accounts, Channels, and Limits](#)
6. [Create Agents](#)

7. [Review](#)
8. [Resetting the Transaction Monitoring System](#)

To configure your transaction monitoring system, follow these steps:

1. Click the OFSCA URL enter username & password, and press Enter. The **Configuration** page is displayed:

Figure 3-21 Recommend Initial Thresholds



2. Select **Recommend Initial Thresholds** and click **Configure**. The **Select scenarios and segment codes** page is displayed.

Select scenarios and segment codes

In this step you will need to specify the new scenarios that you wish to deploy and generate recommendation for.

The inputs can now be provided for multiple segments.

Specify jurisdiction codes or segments at your institution, choose the scenarios that will be deployed against each segment.

Upload a csv file with a list of new scenarios and values for non-tunable parameters in a prescribed template. Note that OFSCA does not recommend thresholds for non-tunable parameters which should be informed by the needs of the business and expertise of an institution's AML subject matter experts.

The template requires filling of details - Segment Name, Scenario Name, Parameter Name, Current Value, Recommended Value (generated at the end of process), and Tunable Parameter.

To setup segment codes, scenarios and thresholds, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.
2. Fill in the required information in the template.

Figure 3-22 Select Scenarios and Segment Codes_Default

Configure your transaction monitoring system

Specify new scenarios you want to deploy

Upload a csv file with list of new scenarios and values for non-tunable parameters

☐ Are you using Oracle's default Risk Categories (HR,MR,RR) ?

[Download Template](#)

Use this template to specify new scenarios you want to deploy.

Drag and Drop

Supported formats: CSV

[Discard](#) [Clear](#) [Continue](#)

- 1 | 7
- Select scenarios and segment codes
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations
- Set up accounts, channels and limits
- Create Agents
- Review

Note:

- Do not modify the column names of the CSV file.
- If you are not using the default risk tiers (RR/MR/HR) at your institution, each of these thresholds (for example, Min_Amt_RR, Min_Amt_MR and Min_Amt_HR) should be set to the same value.

Figure 3-23 Select Scenarios and Segment Codes_Are you using Oracle's default Risk Categories (HR,MR,RR)?

Configure your transaction monitoring system

Specify new scenarios you want to deploy

Upload a csv file with list of new scenarios and values for non-tunable parameters

☒ Are you using Oracle's default Risk Categories (HR,MR,RR) ?

[Download Template](#)

Use this template to specify new scenarios you want to deploy.

Drag and Drop

Supported formats: CSV

[Discard](#) [Clear](#) [Continue](#)

- 1 | 7
- Select scenarios and segment codes
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations
- Set up accounts, channels and limits
- Create Agents
- Review

3. Click **Drag and Drop**, and place the filled in template. You can see a preview of the uploaded CSV file.
4. Click **Continue** to navigate to the Upload Transaction Data step.

Figure 3-24 Select Scenarios and Segment Codes_Preview

Configure your transaction monitoring system

Specify new scenarios you want to deploy

Upload a csv file with list of new scenarios and values for non-tunable parameters

Loaded File
new_scenarios_template(1).csv

Preview

	segment_name	scenario_name	parameter_name	current_value	recommended_value
1					
2	CFOB	(ML/CU) Rapid Movement of Funds - All Activity	Frequency_Period		
3	CFOB	(ML/CU) Rapid Movement of Funds - All	HR_Max_Credit_Amt_Seasoned		

Discard Clear Continue

1 | 7

- Select scenarios and segment codes
- Upload Transaction Data
- Treat Outliers
- Review Threshold Recommendations
- Set up accounts, channels and limits
- Create Agents
- Review

Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Click **Clear** to start the Configure your Transaction Monitoring System from the initial steps again for configuration.

Upload Transaction Data

In this step you will need to provide transaction aggregates.

Upload a csv file with aggregates for each transaction product for credits and debits.

The template requires you to provide aggregates extracted from historical transaction data depending on the scenario.

See [Supported Scenarios \(System Recommended Thresholds\)](#) for more details.

To upload Transaction Aggregates, follow these steps:

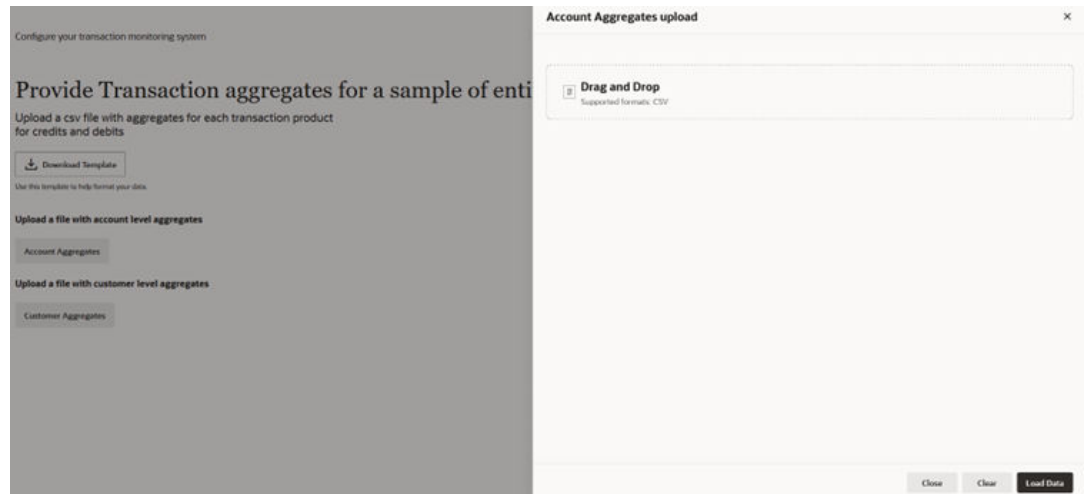
1. Click **Download Template**. The CSV file is downloaded.
2. Fill in the required information in the template.

Figure 3-25 Upload Transaction Data



3. Click **Account Aggregates** to upload the data. The Account Aggregates page opens on the right of your screen.

Figure 3-26 Upload Account Level Aggregates



4. Click **Drag and Drop** and upload the data.
5. Click **Load Data** upload the Account Level Aggregates.
Click **Close** to close the page.
Click **Clear** to clear the loaded data.

Figure 3-27 Account Level Aggregates Preview

Account Aggregates upload ×					
Loaded File acc_dl.csv					
Segment Name	Month ID	Transaction Product	Direction	Total Amount	Total High Risk Amount
SEGMENT_NAME	MONTH_ID	TRANSACTION_PRODUCT	DIRECTION	TOTAL_AMOUNT	TOTAL_HIGH_RISK
AMEA	01/01/23	EFT	Credit	47471	3
AMEA	01/01/23	EFT	Debit	25563	3
AMEA	01/01/23	EFT-Fedwire	Credit	18130	3
AMEA	01/01/23	EFT-Fedwire	Debit	44169	6
1 - 5 >					
				Close	Clear Load Data

Click **Account Aggregates** again to preview the Account Level Aggregates data.

6. Upload the **Customer Level Aggregates**. To upload, see the steps 3, 4, and 5.
7. Click **Continue** to navigate to the Treat Outliers step.

Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Treat Outliers

In this step you will need to remove outlying values from the uploaded data based on two approaches - Inter Quartile Range (IQR) and Percentile

If you select IQR, the available options for thresholds are 1.5 IQR, 2 IQR, and 3 IQR.

If you select percentile, the available options for thresholds are 1, 5, and 10.

Select tails - Left Tails Only or Right Tails Only or Both to trim data.

Table 3-3 Outlier Combination

SL#	Approach	Tails	Thresholds	Outlier Treatment Logic
1	Inter Quartile Range	Left Tail only	1.5 IQR	Remove the values which are less than $Q1 - 1.5 \text{ IQR}$.
2	Inter Quartile Range	Right Tail only	1.5 IQR	Remove the values which are greater than $Q3 + 1.5 \text{ IQR}$.
3	Inter Quartile Range	Both Tails	1.5 IQR	Remove the values which are less than $Q1 - 1.5 \text{ IQR}$ and the ones which are greater than $Q3 + 1.5 \text{ IQR}$.
4	Percentile	Left Tail only	5	Remove the values which are less than 5th percentile.
5	Percentile	Right Tail only	5	Remove the values which are greater than 95th percentile.
6	Percentile	Both Tails	5	Remove the values which are less than 5th percentile and the ones which are greater than 95th percentile.

To remove Outliers, follow these steps:

1. Select an Outlier Removal Approach – **Inter Quartile Range** or **Percentile**.
2. Select Tails - **Left Tails Only** or **Right Tails Only** or **Both**.
3. From the **Thresholds** drop-down, select a threshold.

Figure 3-28 Remove Outliers

4. Click **Continue** to view the recommended Threshold values. The system calculates the initial thresholds.

Or click **Discard** to discard the current activity.

Click **Download** to the data and review. You can also edit the data and upload again.

Review Threshold Recommendations

In this step you can review the Threshold recommendations.

Figure 3-29 View/Edit Threshold Recommendations

View/Edit Threshold Recommendations			
Threshold recommendations			
Segment name	Scenario Name	Threshold Name	Recommended Values
CFOB	(ML/CU) Rapid Moveme...	RR_Min_Debit_Ct_Seas...	5
CFOB	(ML/CU) Rapid Moveme...	RR_Max_Debit_Ct_Seas...	14
CFOB	(ML/CU) Rapid Moveme...	RR_Min_Credit_Ct_Seas...	9
CFOB	(ML/CU) Rapid Moveme...	RR_Max_Credit_Ct_Seas...	18
CFOB	(ML/CU) Rapid Moveme...	RR_Min_Credit_Amt_Se...	2641
CFOB	(ML/CU) Rapid Moveme...	RR_Min_Percentage_Se...	15
CFOB	(ML/CU) Rapid Moveme...	MR_Min_Percentage_Se...	22
CFOB	(ML/CU) Rapid Moveme...	MR_Min_Debit_Ct_Seas...	6
CFOB	(ML/CU) Rapid Moveme...	MR_Max_Debit_Ct_Seas...	15
CFOB	(ML/CU) Rapid Moveme...	MR_Min_Credit_Ct_Sea...	3

Click **Discard** to discard the current activity.

Click **Download** to the data and review. You can also edit the data and update the values in case there is a change needed.

Set up accounts, channels, and limits

In this section you will configure the various products (accounts and channels) offered to various segments within your institution.

You will also specify any limits or restrictions imposed on these products for each segment. Upload a CSV file with accounts, channels and limits in use by each segment.

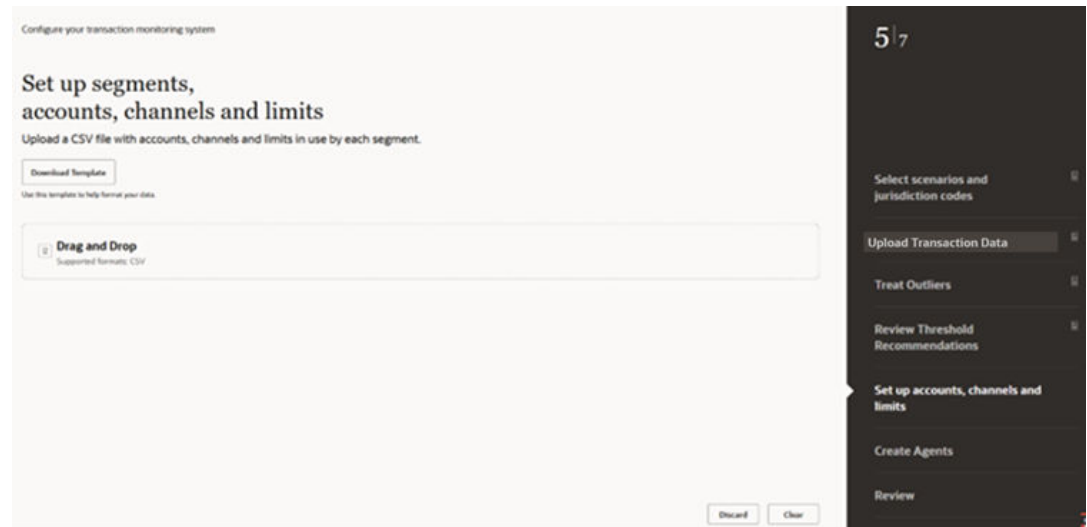
The template requires filling of details – Jurisdiction, Segment Name, Account Type, Channel, and Withdrawal Limit.

To setup segments, accounts, channels, and limits, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.
2. Fill in the required information in the template.

3. Click **Drag and Drop**, and place the filled in template. You can see a preview of the uploaded CSV file.

Figure 3-30 Set up segments, accounts, channels and limits



Note:

- If a channel does not have a withdrawal limit, this can be indicated as NA instead of a number.
- You can remove the uploaded CSV file if required by using the **Clear** button.

4. Click **Continue** to navigate to the Create an agent for each segment step.

Create agents

When creating an agent, a Human Trafficking (HT) agent is automatically generated by default. However, you may need to create a new agent for a segment in the following scenarios:

- If the expected activity of the segment changes and hence the target amount has to change.
- When the distribution of accounts used by customers in the segment changes and hence distribution of accounts changes.

Figure 3-31 Create an agent for each segment



To create an agent, follow these steps:

1. Click **Create Agent** to create an agent for each segment. The **New Agent** page is displayed

Figure 3-32 New Agent

New Agent [X]

Agent AMEA_HR

Agent Name
AMEA_HR Agent nn

Agent Description

Target Account [v]

Amount to transfer (in 1 month)
Expected monthly activity for the suspicious customer in this segment

Maximum [v] Required Minimum [v] Required

Intermediate Accounts

Intermediate Account [v]	Distribution percentage [v]	
Intermediate Account [v]	Distribution percentage [v]	
Intermediate Account [v]	Distribution percentage [v]	[X]
Intermediate Account [v]	Distribution percentage [v]	[X]
Intermediate Account [v]	Distribution percentage [v]	[X] [X]

Cancel Create Agent

2. Enter the **Agent Description**. The description can be used to note any specific products or channels the agent has access to. A good description can help you determine if this agent can be reused in future experiments.
3. Select the required option from the **Target Account** drop-down list. In this example, the available options are RBK, CBK, and RBR.
4. Enter the Maximum and Minimum amount for the segment in the respective fields.

 Note:

- The maximum and minimum should be equal to amounts that are in the unusual range for the segment.
- To calculate target amounts, see the suggested query in the [How to Calculate the Target Amount](#) section.
- Ensure that the Max Target Amount is set such that the granularity (Max Target Amount/20) is lower than any limits that have been set. E.g., if the limit for a channel is \$ 10,000 then the Max Target Amount should be lower than \$200,000.

5. Select the required Intermediate Account from the drop-down list.

 Note:

You can create a maximum of four intermediate accounts for each segment.

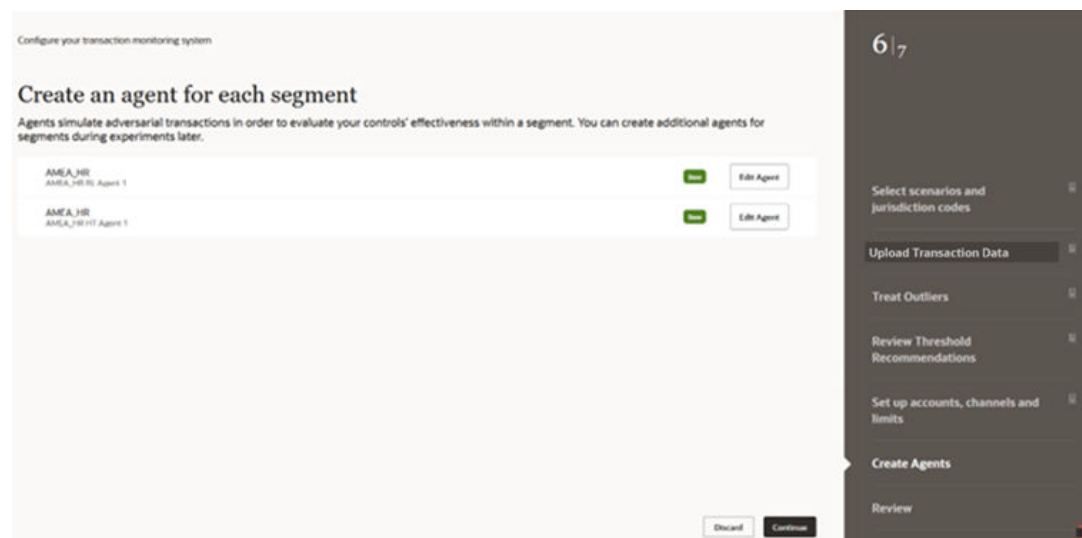
6. Select the required Distribution percentage from the drop-down list. The distribution must approximately reflect the product portfolio for the chosen segment. If a segment has more than four products, the four most widely used or four riskiest products can be considered.

 Note:

The total distribution percentage of all the intermediate accounts must be equal to 100 percentage.

7. Click **Close**  icon to close the Intermediate Account for the segment.
8. Click **Add Another** to add another Intermediate Account for the segment.
9. Click **Create Agent** to create an agent. The following page is displayed.

Figure 3-33 Agent Created



Similarly, you can create an agent for multiple segments.

10. Click **Continue** to navigate to the Review step.

Editing An Agent

This section describes how to edit the created agent for each segment if required.

To edit the created agent, follow these steps:

1. Click **Edit Agent** to edit the required fields. The following page is displayed.

Figure 3-34 Edit Agent

The screenshot shows the 'Edit Agent' form for 'Agent AMEA_HR'. The form includes the following fields and sections:

- Agent Name:** AMEA_HR RL Agent 1
- Agent Description:** This is for AMEA_HR
- Target Account:** CBK
- Amount to transfer (in 1 month):** Expected monthly activity for the suspicious customer in this segment.
 - Maximum:** 1499 (Required)
 - Minimum:** 501 (Required)
- Intermediate Accounts:**
 - Intermediate Account:** CBK, **Distribution percentage:** 100
 - Intermediate Account:** (empty), **Distribution percentage:** 0 (with a delete icon)
 - Intermediate Account:** (empty), **Distribution percentage:** 0 (with a delete icon)
 - Intermediate Account:** (empty), **Distribution percentage:** 0 (with a delete icon)
- Buttons:** Cancel, Save Agent

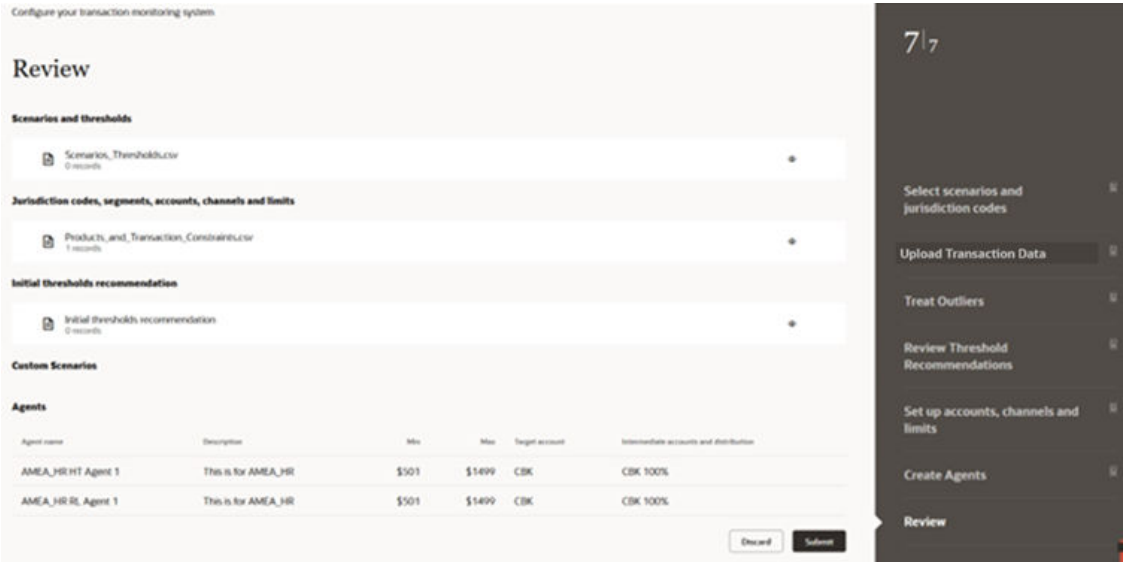
2. Click **Save Agent** to save any modifications made to the agent.

Review

In this step, you can review the uploaded data and created agents for each of the segments.

Click the **View** icon in under the **Scenarios and thresholds**, **Jurisdiction codes**, **segments**, **accounts**, **channels and limits**, and **Initial thresholds recommendation** sections to view the uploaded products and transaction constraints.

Figure 3-35 Review the System



Click **Submit** to configure your transaction monitoring system. You can now view the Transaction Monitoring Performance-related details.

You can also view details the by clicking the respective tabs for Segments and Experiments.

Resetting the Transaction Monitoring System

This section describes how to reset your transaction monitoring system configuration in OFSCA.

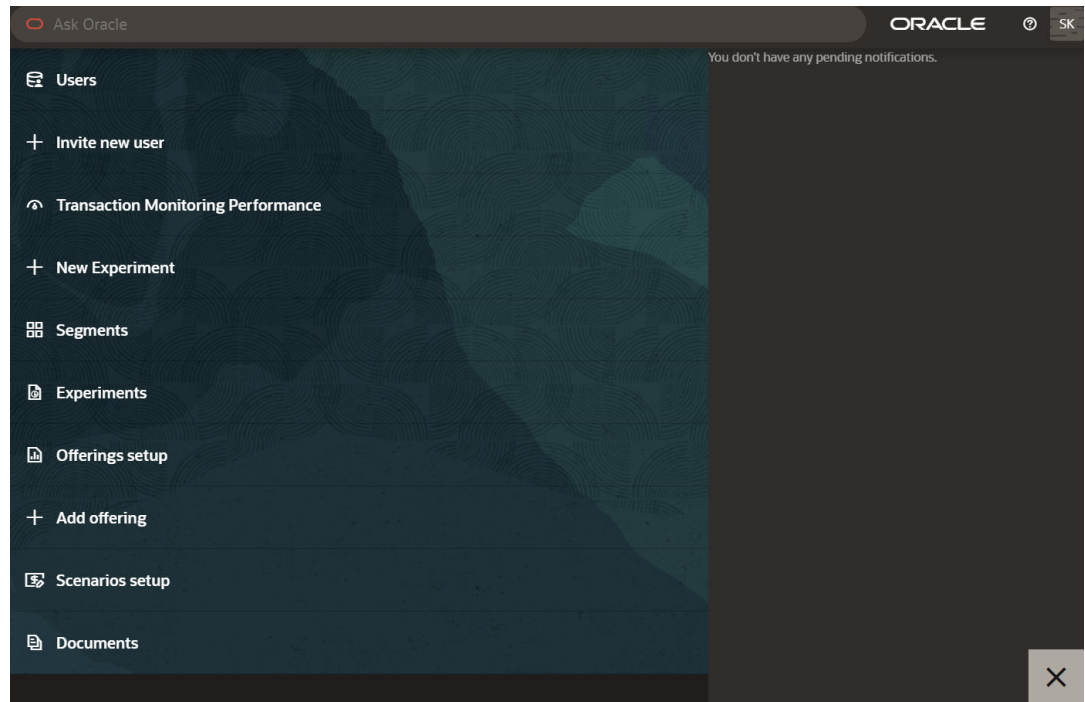
To reset the system and initial configuration, follow these steps:

1. Click



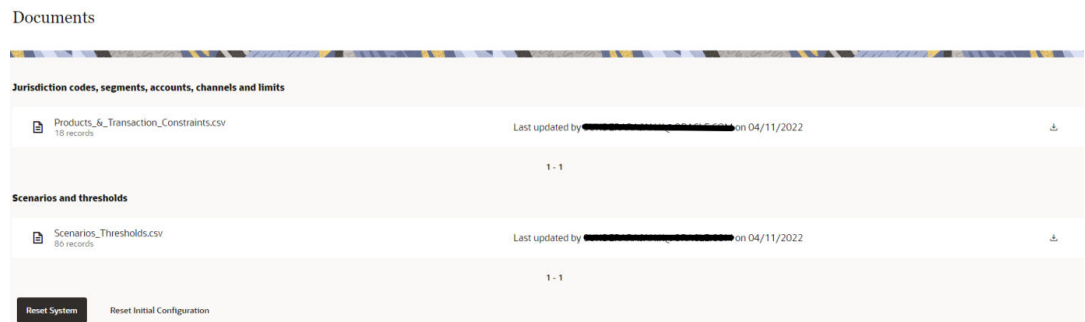
Open Ask Oracle to display the Ask Oracle window. The following window is displayed.

Figure 3-36 Application Menu

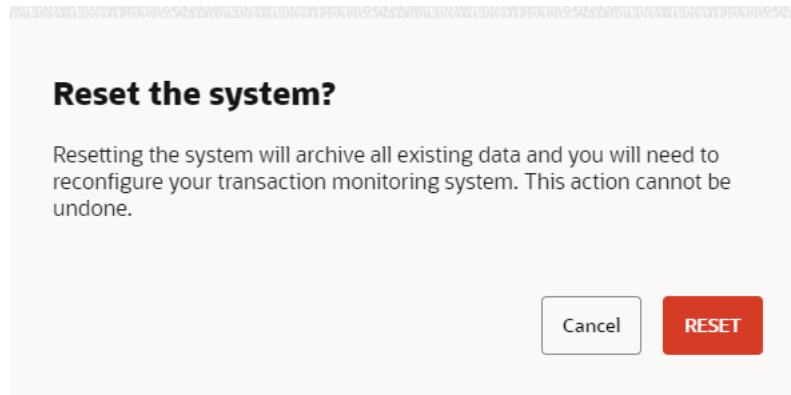


2. Click **Documents** menu to display the Documents window. The following window is displayed.

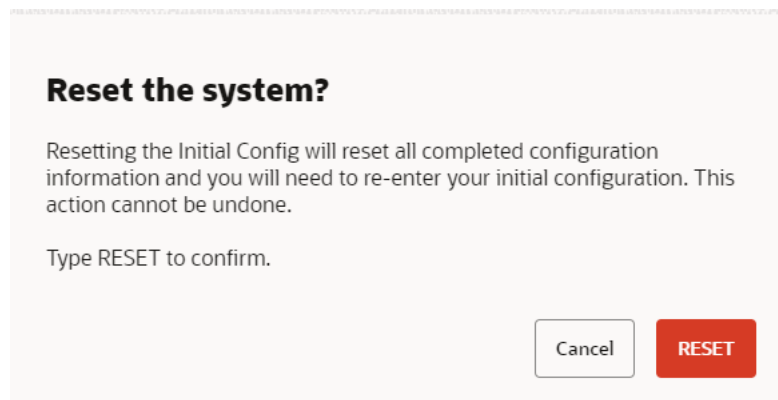
Figure 3-37 Documents Menu



3. Click **Reset System** to reset your transaction monitoring system. The confirmation window is displayed.

Figure 3-38 Reset System

4. Click **RESET** to reset the system. It will archive all the existing data and you need to reconfigure your transaction monitoring system. Or Click **Cancel** to cancel the action.
5. Click **Reset Initial Configuration** in the Documents window to reset the initial configuration. The confirmation window is displayed.

Figure 3-39 Reset the Initial Configuration

6. Click **RESET** to reset the initial configuration. It will reset all the completed configuration information and you need to reconfigure your initial configuration. Or Click **Cancel** to cancel the action.

User Defined Thresholds

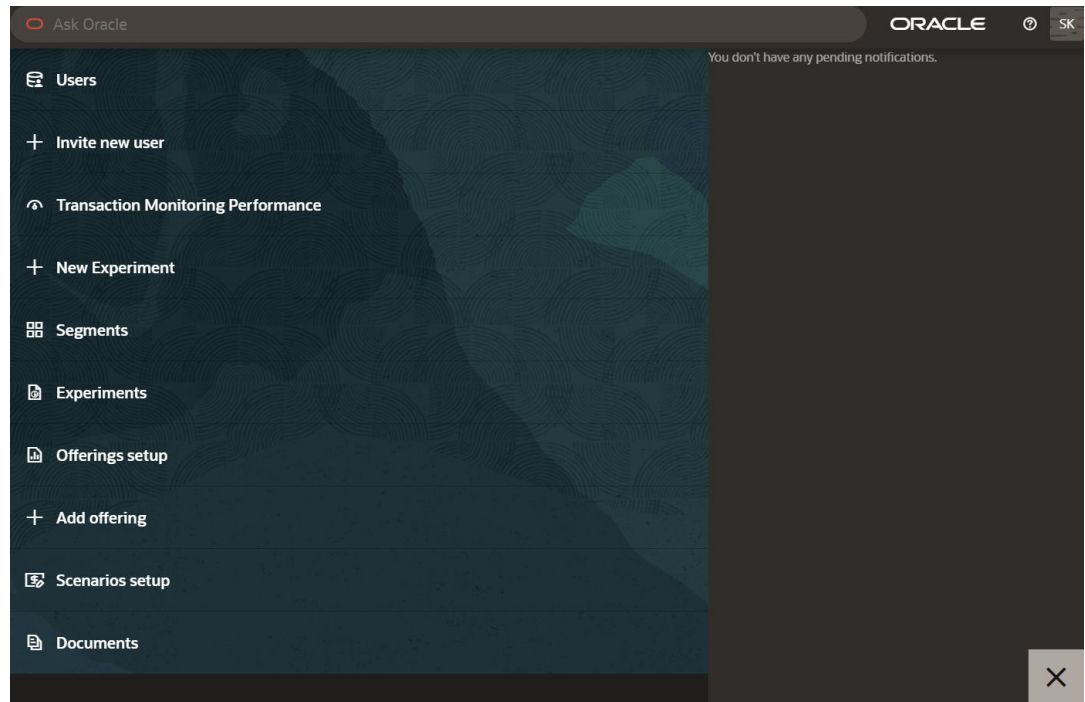
This section describes how to configure the transaction monitoring system with user defined thresholds.

To configure your transaction monitoring system, follow these steps:

1. Click **Open Ask Oracle**



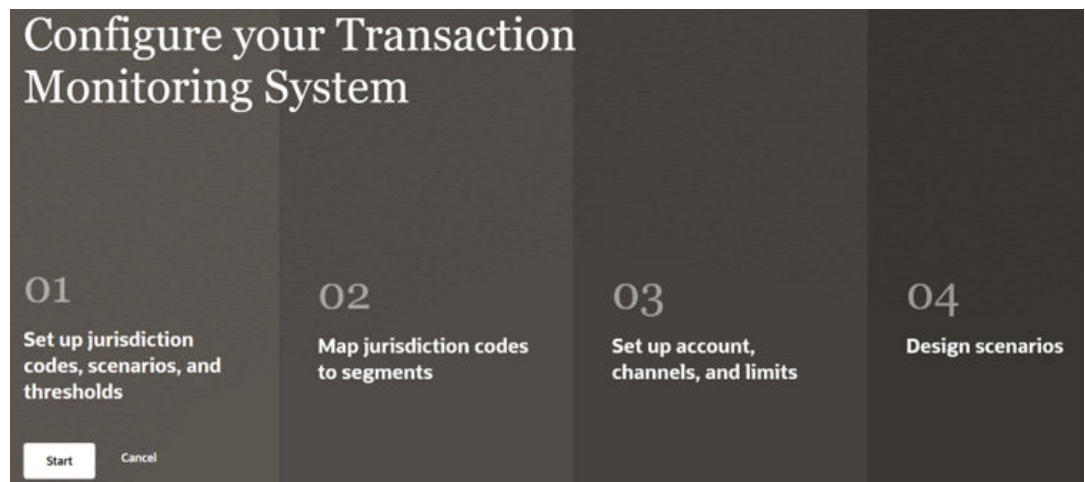
Figure 3-40 Application Menu



At least one step is required. If you have only one step, then it appears unnumbered in the output.

2. Click **Transaction Monitoring Performance** in the above menu to display the Configure your Transaction Monitoring System window. The following window is displayed.

Figure 3-41 Configure Transaction Monitoring System



3. Click **Start** to configure your transaction monitoring system.

Topics:

- [Set up jurisdiction codes, scenarios, and thresholds](#)
- [Map jurisdiction codes to segments](#)

- [Set up accounts, channels, and limits](#)
- [Design scenarios](#)
- [Create agents](#)
- **[Upload transaction data](#)**
- [Reviewing your Transaction Monitoring System](#)

Set up jurisdiction codes, scenarios, and thresholds

This section outlines the steps to duplicate your transaction monitoring system in OFSCA. You'll specify jurisdiction codes or segments at your institution, choose the scenarios that will be monitored, and set thresholds for each scenario.

The following scenarios are supported:

- RMF
- SigCash
- LRT
- CIB:PAA
- HRG:HRT
- HRG:HRE
- Deposits/Withdrawals in Same or Similar Amounts
- Anomalies in ATM, Bank Card: Excessive Withdrawals
- CIB:PPA
- CIB:HRG
- Single or Multiple Cash Transactions: Possible Currency Transaction Report
- CIB: Foreign Activity
- CIB: Product Utilization Shift
- RMF : FTN
- LDA

Figure 3-42 Set up jurisdiction codes, scenarios, and thresholds

Configure your transaction monitoring system

Set up jurisdiction codes, scenarios and thresholds

Upload a CSV file with thresholds and parameters for scenarios in use by each jurisdiction code.

[Download SQL Script](#)

Use this query to create the CSV file.

[Download Template](#)

Use this template to help format your data.

Drag and Drop
Supported formats: CSV

[Discard](#) [Clear](#) [Continue](#)

1 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data
- Review

To set up jurisdiction codes, scenarios and thresholds, follow these steps:

**Note:**

Click **Download SQL Script** to download SQL script and execute the script against data in Oracle's Financial Crime Data Model to extract the required data

1. Click **Download Template** to download the template and format the extracted data into CSV file.

**Note:**

- You must not modify jurisdiction, scenario_name, and scenario_id in the CSV file.
- If your institution uses different risk categories or labels, you should set the threshold values for the default values in the OFSCA defined labels (Min_Amt_RR, Min_Amt_MR, Min_Amt_HR) to the same value. This ensures consistency in how risk is evaluated, even though your institution doesn't use the default OFSCA provided labels.

2. To upload the CSV file with the necessary data, simply drag and drop it into the designated field or click on the icon  to open the file selector dialog box and choose the file. Once the CSV file is loaded, the following window is displayed.

Figure 3-43 Uploaded CSV File

Configure your transaction monitoring system

Set up jurisdiction codes, scenarios and thresholds

Upload a CSV file with thresholds and parameters for scenarios in use by each jurisdiction code.

Loaded File
scenarios_thresholds_template.csv

Preview

	jurisdiction	scenario_name	scenario_id	parameter_name	threshold_id	current_value_transaction
2	AMEA_JAPAC	(ML/CU) Rapid Movement of Funds All Activity	6	Frequency_Period	2817	7

Discard Clear Continue

1 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data
- Review

Note:

You can remove the uploaded CSV file if required by using the Clear button.

- Click **Continue** to navigate to the Map jurisdiction codes to segments step.
Or Click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window. Click **Start** to start the Configure your Transaction Monitoring System from the initial steps again for configuration.

Map jurisdiction codes to segments

In this section, you will map jurisdiction codes in Oracle's Transaction Monitoring Solution to segments at your institution.

Figure 3-44 Map jurisdiction codes to segments

Configure your transaction monitoring system

Map jurisdiction codes to segments

☒ Jurisdiction codes are the same as segments at my institution.

Jurisdiction	Segment
CFOB	

Total 1

Discard Continue

2 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data
- Review

To map jurisdiction codes to segments, follow these steps:

1. Enter the required name in the Segment field.
Enable the checkbox "Jurisdiction codes are the same as segments at my institution" if segments are equivalent to jurisdiction codes.
2. Click **Continue** to navigate to the Set up accounts, channels, and limits step.

Set up accounts, channels, and limits

In this section you will configure the various products (accounts and channels) offered to various segments within your institution. You will also specify any limits or restrictions imposed on these products for each segment.

Figure 3-45 Set up accounts, channels, and limits

Configure your transaction monitoring system

Set up jurisdiction codes, segments, accounts, channels and limits

Upload a CSV file with thresholds and parameters for scenarios in use by each jurisdiction code.

☒ Add default risk levels (RR, MR, HR) to segment names in the template

Download Template

Use this template to help format your data.

Drag and Drop
Supported formats: CSV

Discard Clear

3 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits**
- Design scenarios
- Create agents
- Upload transaction data
- Review

To set up an account, channels, and limits, follow these steps:

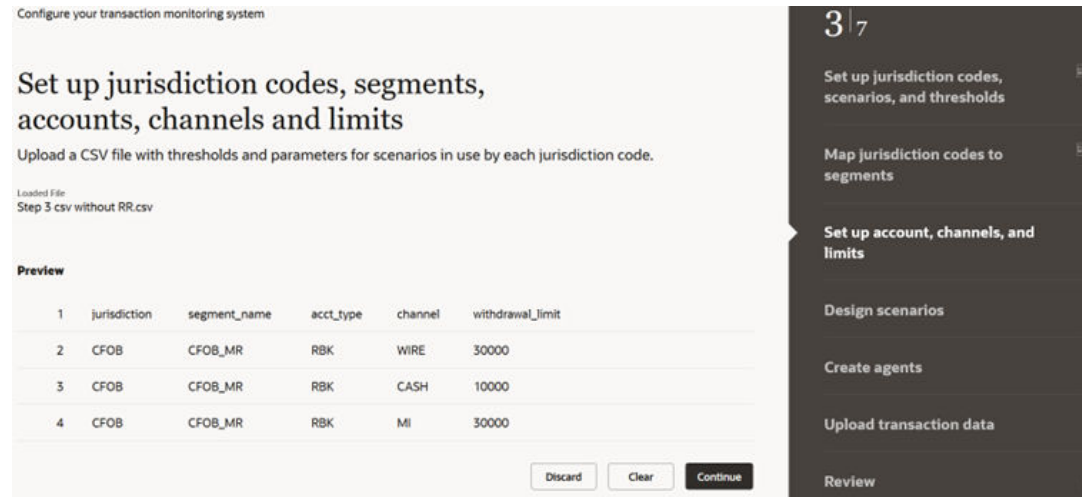
1. Enable the Add default risk levels (RR, MR, HR) to segment names in the template check box if your institution uses Oracle's default risk tiers - RR, MR, and HR and if each customer segment at your institution is mapped to one of these risk tiers.
2. Click **Download Template** to download the template and populate the template with required data

Note:

- You can update details in the Channel and Withdraw_Limit columns as per requirement.
- Specify the channel name as CASH, MI, and WIRE in the Channel column.
- Withdrawal limits refer to hard limits on how much funds can be withdrawn from an account type through a specific channel.

3. Drag and drop the CSV file into the Drag and Drop field or click  icon to open the file selector dialog box and select the required file. Once the CSV file is loaded, the following window is displayed.

Figure 3-46 Uploaded CSV file to Set up Account, Channels, and Limits



Configure your transaction monitoring system

Set up jurisdiction codes, segments, accounts, channels and limits

Upload a CSV file with thresholds and parameters for scenarios in use by each jurisdiction code.

Loaded File
Step 3 csv without RR.csv

Preview

	jurisdiction	segment_name	acct_type	channel	withdrawal_limit
1					
2	CFOB	CFOB_MR	RBK	WIRE	30000
3	CFOB	CFOB_MR	RBK	CASH	10000
4	CFOB	CFOB_MR	RBK	MI	30000

Discard Clear Continue

3 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits**
- Design scenarios
- Create agents
- Upload transaction data
- Review

 Note:

- If a channel does not have a withdrawal limit, this can be indicated as NA instead of a number.
- You can remove the uploaded CSV file if required by using the Clear button.

4. Click **Continue** to navigate to the Design scenarios step.

Design scenarios

Financial institutions often customize or modify Oracle's standard scenarios or use purpose built scenarios to meet their specific requirements. Oracle Financial Services Compliance Agent Cloud (OFSCA) provides a scenario authoring feature that lets you incorporate these customized scenarios into its simulator, enabling a comprehensive evaluation of your transaction monitoring system.

 Note:

Scenarios are assumed to follow an if-then-else logic for alerting similar to Oracle's Out of the Box scenarios.

In this section, you will design custom scenarios in Oracle's Transaction Monitoring Solution for segments at your institution.

**Note:**

You may skip creating a custom scenario in the initial configuration by using the **Skip** button.

Figure 3-47 Designing Custom Scenarios

To design a new custom scenario during initial configuration, follow these steps:

1. From the **Select segment(s) to add a custom scenario to** drop-down list, select segment(s).
The Create Scenario button is enabled.
2. Click **Download Template**. A JSON template is downloaded.
Currently, a single JSON file can be used to configure a scenario for only one risk segment. If a scenario has to be configured for three risk segments, for example, BCAP_RR, BCAP_MR, BCAP_HR, three different JSON files are required with three different scenario names. For sample files, see [Sample Template](#)
3. Enter the Scenario Name, relevant jurisdiction that the scenario monitors, Threshold name, Lookback period, Rule run frequency, and Account Types to be monitored in the JSON template.

**Note:**

You must use only those *Jurisdiction* values in the JSON template that are available in the CSV file that has been uploaded in the *Set up jurisdiction codes, scenarios, and thresholds* section.

4. Click **Create Scenario**. Drag and Drop the required JSON template. The selected JSON template details are displayed.

Figure 3-48 Create Custom Scenario

Create Custom Scenario

File Name
CS_TEMPLATE_RMF.JSON

Aggregates, Jurisdictions and Thresholds - Edit JSON

```
{
  "credit_amt" : 5000,
  "credit_ct" : 5,
  "debit_amt" : 5000,
  "debit_ct" : 5
},
"CFOB_RR" :
{
  "credit_amt" : 5000,
  "credit_ct" : 5,
  "debit_amt" : 5000,
  "debit_ct" : 5
}
}
```

862

Parse Status Scenario Name Jurisdiction Thresholds

Pass

Scenario Type
RL

Aggregates

tot_credit_amount	⌕	tot_amount	⌕
tot_debit_amount	»		⌕
tot_credit_amount_with_mita(min_i	>		⌕
tot_debit_amount_with_mita(min_i	<		⌕
tot_credit_amount_cash	<		⌕
tot_debit_amount_cash	<		⌕
tot_credit_amount_with_rita(min_ir	<		⌕
tot_credit_count	<		⌕

Custom Scenario Conditions
(credit_amt + debit_amt) <= tot_amount

41

Condition Parse Status
Pass

Cancel Remove Reset Parse

5. Select the scenario type RL or HT from the Scenario Type drop-down list. The list of aggregates for RL and HT are available in the [Aggregates List](#) section.
 - **RL** - RL stands for "Risk and Liability" experiments, which are used to evaluate the overall strength and performance of the system. Scenarios added using this option will be used to assess the system's performance and identify any potential risks or liabilities.
 - **HT** - HT stands for "Human Trafficking" experiments, which are used to evaluate the system's performance specifically against the Human Trafficking typology. Scenarios added using this option will be used to assess the system's effectiveness in detecting and addressing specific Human Trafficking risks.

Figure 3-49 Create Custom Scenario - Accept

Create Custom Scenario

Pass

Scenario Type
RL

Aggregates

tot_credit_amount
tot_debit_amount
tot_credit_amount_with_mita(min_i
tot_debit_amount_with_mita(min_i
tot_credit_amount_cash
tot_debit_amount_cash
tot_credit_amount_with_rita(min_ir
tot_credit_count

tot_amount

Custom Scenario Conditions
(credit_amt + debit_amt) <= tot_amount

41

Condition Parse Status
Pass

Cancel Remove Reset Parse Accept

6. Based on your selection, a relevant list of aggregates is displayed. Select and move the required aggregates to the right-hand side box.
7. Enter scenario conditions in the Custom Scenario Condition box using thresholds and aggregates.

Note:

When entering scenario conditions, only a single space must be used between each term in the expression. It is mandatory even when parentheses are used.

- Correct: (Total_Trxn_Amt >= RR_Min_Total_Amt) and (Total_Trxn_Ct >= RR_Min_Total_Ct)
- Incorrect: (Total_Trxn_Amt>=RR_Min_Total_Amt) and (Total_Trxn_Ct>=RR_Min_Total_Ct)

8. Click **Parse** to validate the condition. If the validation is successful, the parsing will be passed.
9. Click **Accept** to add the newly created scenario. This scenario will be listed on the Custom Scenario page.
10. If you want to modify a newly created scenario, click **Edit** and modify information based on your requirements.

Figure 3-50 Design Custom Scenarios - Edit

Configure your transaction monitoring system Create Scenario

Design Custom Scenarios

Upload a JSON file with custom scenario jurisdiction specific threshold values and aggregates

Select segment(s) to add a custom scenario to ▼

Scenario Name	File Name	Created On	
Custom_RMF_Scenario	CS_TEMPLATE_RMF.JSON	11/26/2024 10:48	Edit

Last saved
Tuesday, November 26, 2024 10:29 Zulu

Skip Step Discard Clear Continue

4 | 7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios**
- Create agents
- Upload transaction data
- Review

Note:

Once you process the scenario, you cannot edit it.

11. Click **Continue** to go to the Create agents step.
12. You can also create custom scenarios using the Oracle Ask menu.

Figure 3-51 Create Scenario Using Oracle Ask Page

Design Custom Scenarios

Upload a JSON file with custom scenario jurisdiction specific threshold values and aggregates Create Scenario

Download Template

Use this template to help format your custom scenario data

Custom Scenarios

13. On the Custom Scenario page, click **Create Scenario**. The Create Scenario dialog is displayed. Repeat Step-3 to Step-9.

Design Custom Scenarios
Upload a JSON file with custom scenario jurisdiction specific threshold values and aggregates

[Download Template](#)
Use this template to help format your custom scenario data

Custom Scenarios

Scenario Name	File Name	Created On	Created By	Row Action
custom_sig_wire	CS_SIG_CASH.JSON	06/13/2024 21:17	SRIKRISHNA.KAMBAR@ORACLE.COM	...

Row Action menu options: Edit, View, Process

14. Click ... **Option** Icon and then click **Process**. A new custom scenario is created. You can also modify the scenario using the **Edit** option.

Note:

Once you process the scenario, you cannot edit it.

The New Scenario will be available as part of a New Threshold Set with the current Production Controls, which can be used while creating experiments in that segment.

Copy and modify control set
Select a scenario threshold set and/or account-channel constraint set to modify.

Agent: CFOB_RR RL Agent 1 Target Account: RBK Max: \$55000 Min: \$5000 Intermediate Accounts: RBK 100%

Experiment Description: Experiment with custom sig_wire scenario monitoring segment CFOB_RR

Scenarios threshold set name: Custom Scenario custom_sig_wire

Experiment scenario threshold set name: Custom Scenario custom_sig_wire Threshold Set

Add Scenario

(ML/CU) Patterns of Funds Transfers Between Customers and External Entities	
(ML/CU) Rapid Movement of Funds - All Activity	
(ML/CU) Single or Multiple Cash Transactions: Large Significant Transactions	
custom_sig_wire	

Discard Continue

3/4

Select Segment

Select Agent

Copy and modify control set

Review

You can perform the following activities using the Row Action.

- **Edit** - The Edit option allows you to modify the existing information of a scenario. This option is used when you need to make changes or updates to the scenario's details.
- **View** - The View option allows you to view the scenario without making any changes. This option is useful when you want to review the scenario or gather information from it.

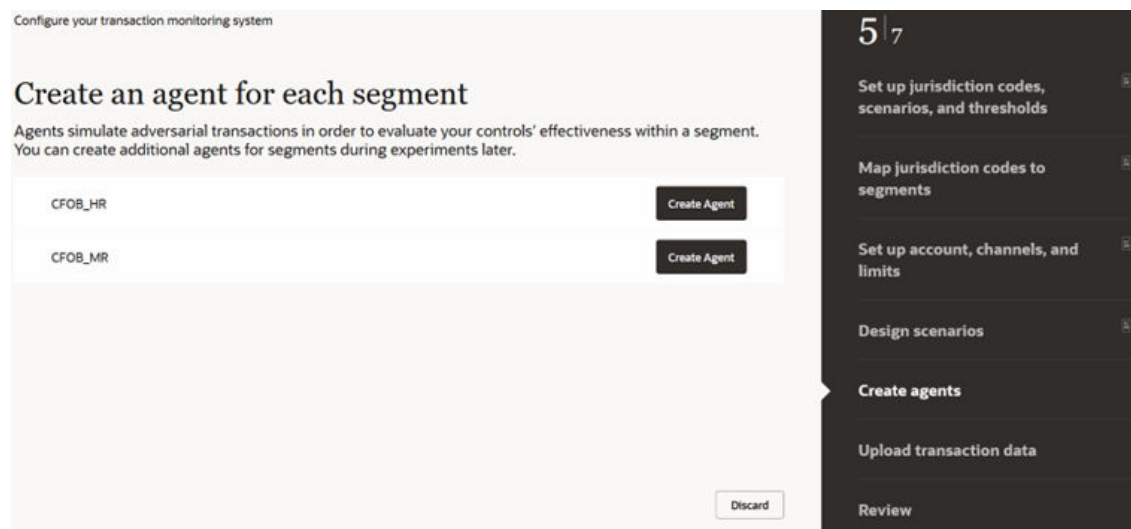
- **Process** - The Process option is used to create a custom scenario. This option enables you to define and set up a new scenario according to your specific requirements.

Create agents

When creating an agent, a Human Trafficking (HT) agent is automatically generated by default. However, you may need to create a new agent for a segment in the following scenarios:

- If the expected activity of the segment changes and hence the target amount has to change.
- When the distribution of accounts used by customers in the segment changes and hence distribution of accounts changes.

Figure 3-52 Create agents



To create an agent, follow these steps:

1. Click **Create Agent** to create an agent for each segment. The New Agent window is displayed

Figure 3-53 New Agent

Create Agent

Agent

Segments List

Agent NameAgent Description

Target Account

Amount to transfer (in 1 month)

Expected monthly activity for the average customer in this segment

MaximumMinimum

RequiredRequired

Historical Activity (per month)

Average monthly credit amountAverage monthly debit amount

Peak monthly creditPeak monthly debit

High Risk Geography monthly creditHigh Risk Geography monthly debit

Standard deviation of monthly creditStandard deviation of monthly debit

Peak Foreign Credit AmountPeak Foreign Debit Amount

Historical Daily Average Amount

2. Enter the **Agent Description**. The description can be used to note any specific products or channels the agent has access to. A good description should help you determine if this agent can be reused in future experiments.
3. Select the required option from the Target Account drop-down list. In this example, the available options are RBK, CBK, and RBR.
4. Enter the Maximum and Minimum amount for the segment in the respective fields.

 Note:

- The maximum and minimum should be equal to amounts that are in the unusual range for the segment.
- To calculate target amounts, see the suggested query in the [How to Calculate the Target Amount](#) section.
- Ensure that the Max Target Amount is set such that the granularity (Max Target Amount/20) is lower than any limits that have been set. E.g., if the limit for a channel is \$ 10,000 then the Max Target Amount should be lower than \$200,000.

5. Enter the amount in the following fields:

- Average monthly credit amount
- Peak monthly credit
- Peak monthly debit
- High Risk Geography monthly credit
- High Risk Geography monthly debit
- Standard deviation of monthly credit
- Standard deviation of monthly debit
- Average Foreign monthly credit
- Average Foreign monthly debit

 Note:

- Historical Activity (per month) field is displayed only if the CIB scenario is loaded in the system.
- To calculate CIB parameter, see the suggested query in the [#unique_58](#) section.

6. Select the required Intermediate Account from the drop-down list.

 Note:

You can create a maximum of four intermediate accounts for each segment.

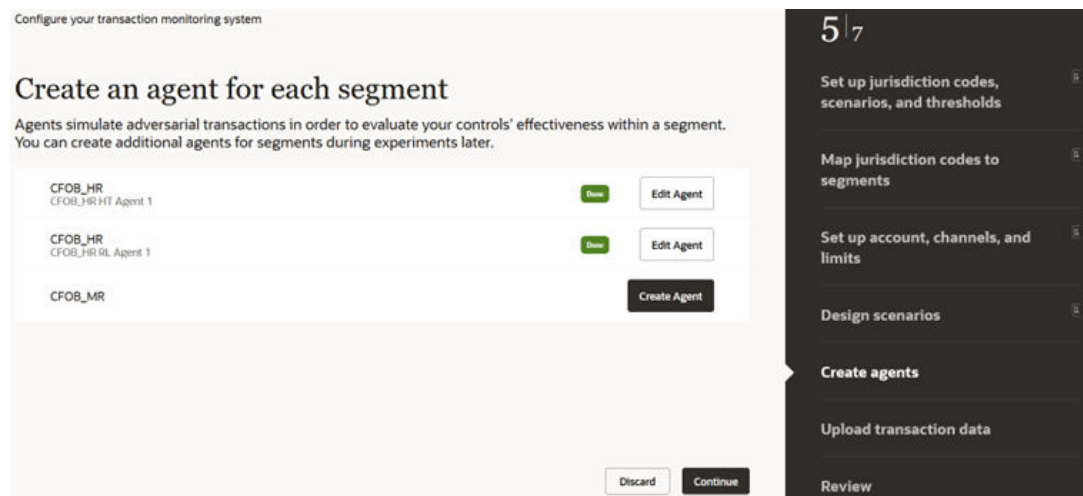
7. Select the required Distribution percentage from the drop-down list. The distribution should approximately reflect the product portfolio for the chosen segment. If a segment has more than four products, the four most widely used or four most riskiest products can be considered.

 Note:

The total distribution percentage of all the intermediate accounts should be equal to 100 percentage.

8. Click **Close**  icon to close the Intermediate Account for the segment.
9. Click **Add Another** to add another intermediate account for the segment.
10. Click **Create Agent** to create an agent. The following window is displayed.

Figure 3-54 Agent Created



Similarly, you can create an agent for the remaining segments.

11. Click **Continue** to navigate to the Upload transaction data step.

Editing An Agent

This section describes how to edit the created agent for each segment if required.

To edit the created agent, follow these steps:

1. Click **Edit Agent** to edit the required fields. The following window is displayed.

Figure 3-55 Edit Agent

New Agent [X]

Agent AMEA_HR

Agent Name: AMEA_HR Agent 2
Agent Description: test

Target Account: RBK

Amount to transfer (in 1 month)
Expected monthly activity for the average customer in this segment

Maximum: 10000 (Required)
Minimum: 501 (Required)

Historical Activity (per month)

Average monthly credit amount: 10000 (Required)
Average monthly debit amount: 100000 (Required)

Peak monthly credit: 10000 (Required)
Peak monthly debit: 10000 (Required)

High Risk Geography monthly credit: 10000 (Required)
High Risk Geography monthly debit: 10000 (Required)

Standard deviation of monthly credit: 10000 (Required)
Standard deviation of monthly debit: 10000 (Required)

Intermediate Accounts

Intermediate Account: RBK, Distribution percentage: 50
Intermediate Account: CBK, Distribution percentage: 50 [X]

[Add Another]

[Cancel] [Save Agent]

2. Click **Save Agent** to save any modifications made to the agent.

Upload transaction data

In this step, upload transaction data to calculate the impact of changing threshold values on alert volumes. This data will be used to compute and display the Alert Volume Impact on the Experiments Comparison page.

Uploaded CSV file containing aggregated data for each transaction product, including both credits and debits. The template requires you to provide aggregates extracted from historical transaction data relevant to the specific scenario.

To upload Transaction data, follow these steps:

1. Click **Download Template**. The CSV file is downloaded.

Figure 3-56 Upload transaction data

Configure your transaction monitoring system

Provide Transaction data for a sample of entities for Alert Volume Impact Computations

Upload a csv file with aggregates for each transaction product for credits and debits

[Download Template](#)

Use this template to help format your data.

Drag and Drop
Supported formats: CSV

[Discard](#) [Clear](#) [Continue](#)

- 6 | 7
- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data**
- Review

2. Fill in the required information in the template.
3. Click **Drag and Drop**, and place the filled in template. You can see a preview of the uploaded CSV file.
4. Click **Continue** to navigate to the Review step.

Figure 3-57 Upload transaction data - Preview

Configure your transaction monitoring system

Provide Transaction data for a sample of entities for Alert Volume Impact Computations

Upload a csv file with aggregates for each transaction product for credits and debits

Loaded file:
transaction_2seg_13scn.csv

Preview report

1	CFOB	01/23/0001	EFT	Credit	33819	2	28000	18	26018	8	10279	12
1	CFOB	01/23/0001	EFT	Debit	26898	3	19000	5	39202	13	28188	19
1	CFOB	01/23/0001	EFT-Fedwire	Credit	36351	6	37000	10	32617	11	41029	18

Last saved
Tuesday, November 26, 2024 11:09 Zulu

[Discard](#) [Clear](#) [Continue](#)

- 6 | 7
- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data**
- Review

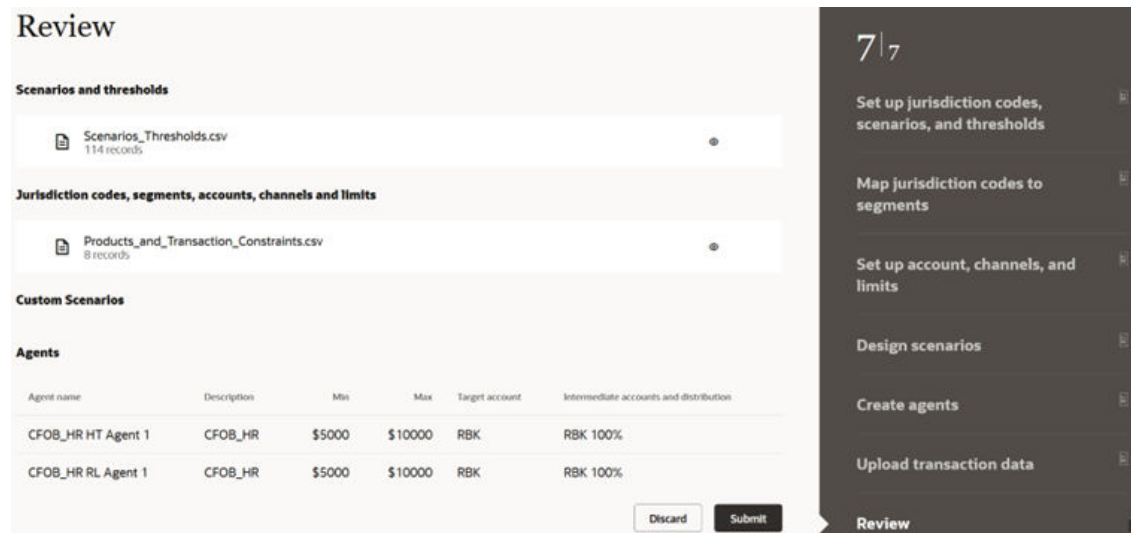
Or click **Discard** to discard the current activity and return to the Configure your Transaction Monitoring System window.

Click **Clear** to start the Configure your Transaction Monitoring System from the initial steps again for configuration.

Review

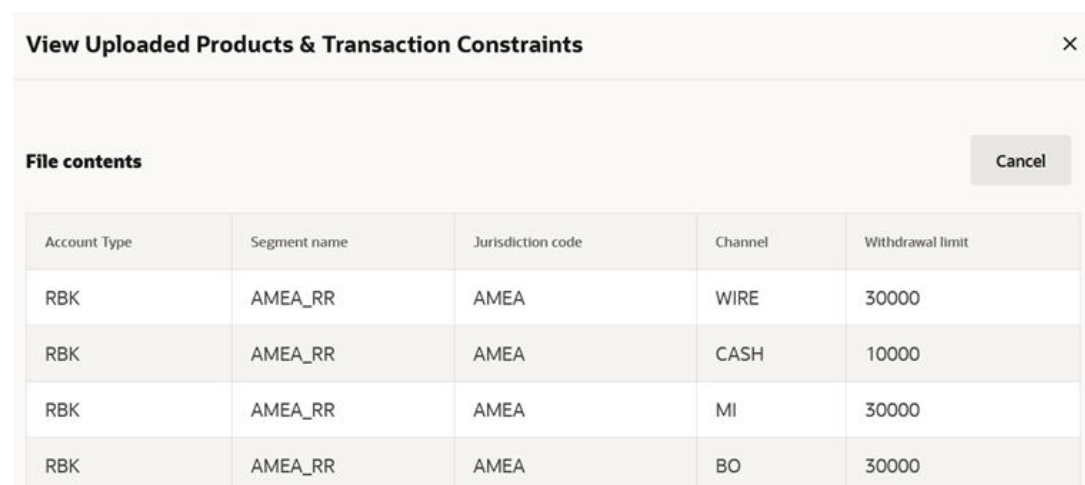
In this section, you can view the uploaded data and created agents for each of the segments.

Figure 3-58 Review



1. Click the View icon  in **Jurisdiction codes, segments, accounts, channels, and limits** to view the uploaded products and transaction constraints. The following window is displayed.

Figure 3-59 Uploaded Products and Transaction Constraints



2. Click **Cancel** to exit the window.

3. Click  the View icon in Scenarios and thresholds to view the uploaded scenario thresholds. The following window is displayed.

Figure 3-60 Uploaded Scenario Thresholds

View Uploaded Scenario Thresholds ×

File contents Cancel

Jurisdiction code	Scenario Name	Scenario ID	Parameter Name	Threshold ID	Curr Value Tx	Threshold Set ID
AMEA	(ML/CU) Large Reportable Transactions	114000078	Actvty_Risk_Cutoff_Lvl	8231	5	
AMEA	(ML/CU) Large Reportable Transactions	114000078	All_Jurisdictions_FI	8232	'Y'	
AMEA	(ML/CU) Large Reportable Transactions	114000078	All_Trans_Src_FI	8233	'Y'	
AMEA	(ML/CU) Large Reportable Transactions	114000078	Curr_Type	8234	'B'	

- Click **Cancel** to exit the window.

Figure 3-61 Review - Submit

Review

Scenarios and thresholds

Scenarios_Thresholds.csv
114 records

Jurisdiction codes, segments, accounts, channels and limits

Products_and_Transaction_Constraints.csv
8 records

Custom Scenarios

Agents

Agent name	Description	Min	Max	Target account	Intermediate accounts and distribution
CFOB_HR HT Agent 1	CFOB_HR	\$5000	\$10000	RBK	RBK 100%
CFOB_HR RL Agent 1	CFOB_HR	\$5000	\$10000	RBK	RBK 100%

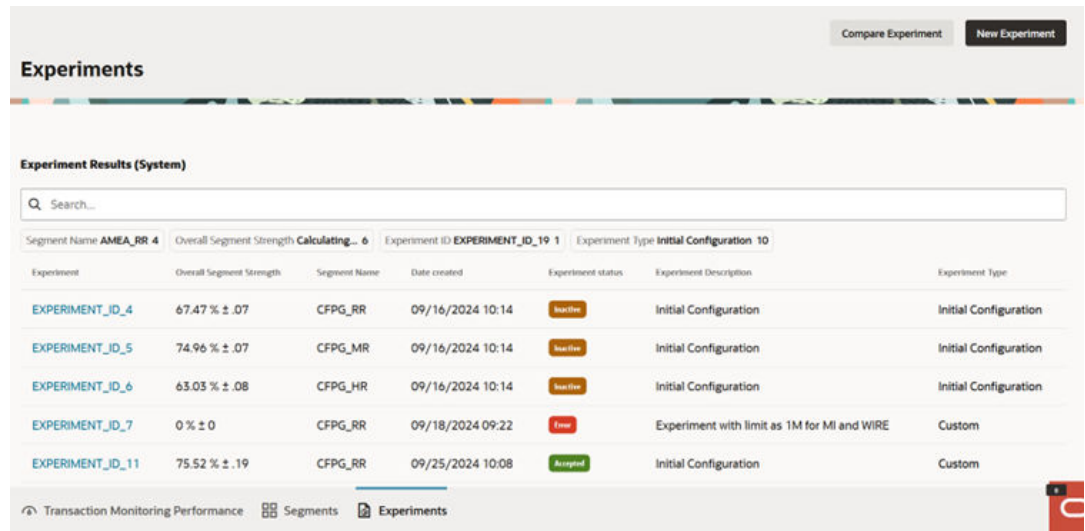
Discard Submit

7/7

- Set up jurisdiction codes, scenarios, and thresholds
- Map jurisdiction codes to segments
- Set up account, channels, and limits
- Design scenarios
- Create agents
- Upload transaction data
- Review**

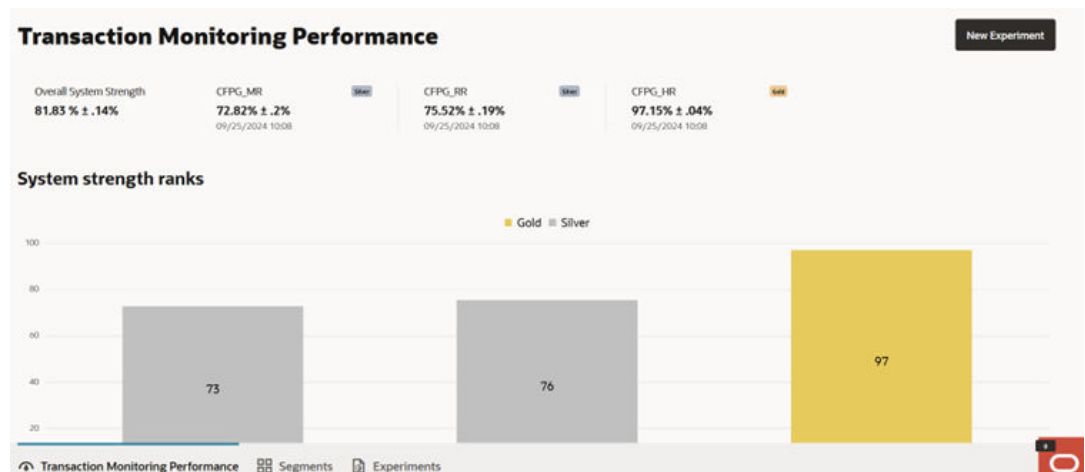
- Click **Submit** to configure your transaction monitoring system. This will trigger experiment of type "Initial Set Up" for each of the segments you have configured.
- Navigate to the Experiments tab and you can view the created experiment is in In progress status as shown below:

Figure 3-62 Experiments

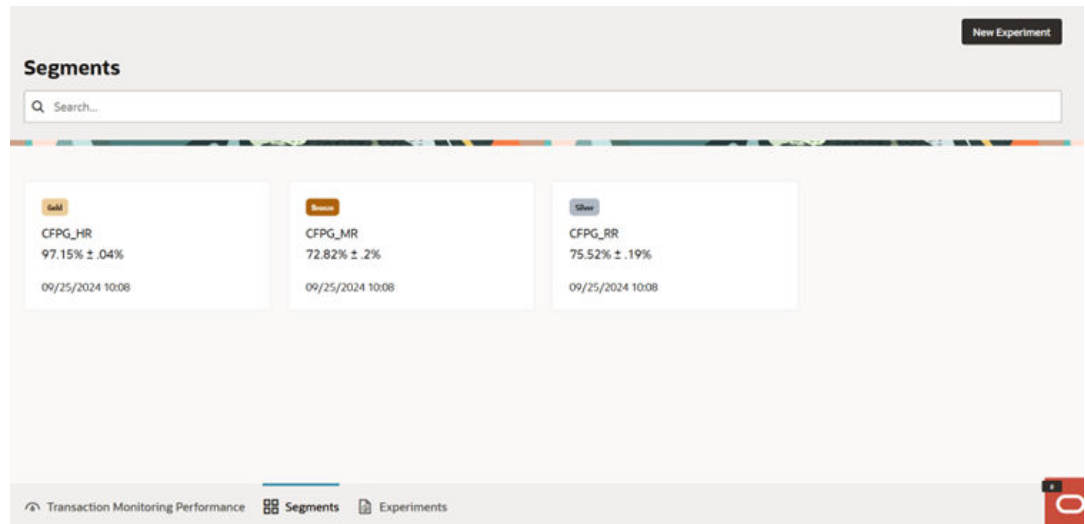


Once the experiment is completed, the status of the experiment will change from "In Progress" to "Completed". If the experiment has run successfully, the dashboard will be updated as shown below:

Figure 3-63 Transaction Monitoring Performance



Navigate to the Segments tab to view the segments.

Figure 3-64 Segments

Resetting the Transaction Monitoring System

This section describes how to reset your transaction monitoring system configuration in OFSCA.

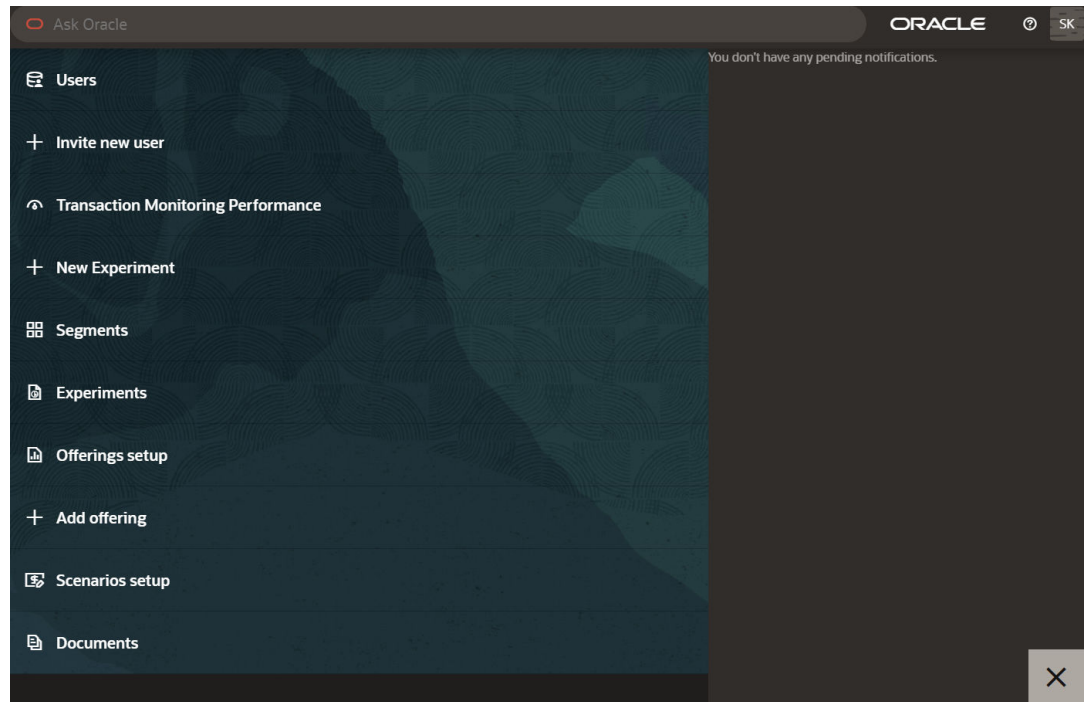
To reset the system and initial configuration, follow these steps:

1. Click



Open Ask Oracle to display the Ask Oracle window. The following window is displayed.

Figure 3-65 Application Menu



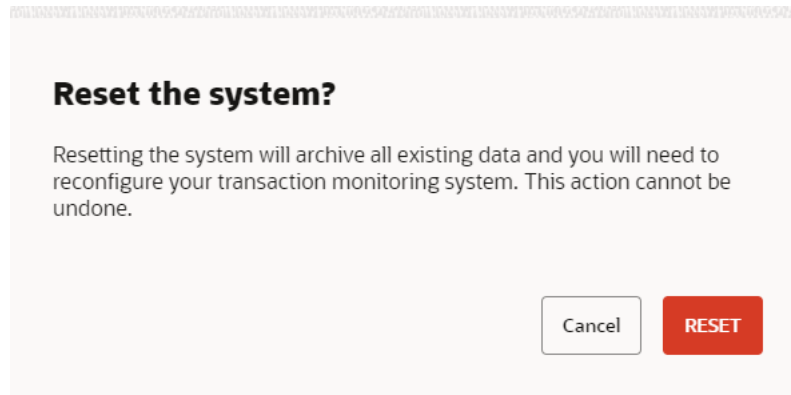
2. Click **Documents** menu to display the Documents window. The following window is displayed.

Figure 3-66 Documents Menu



3. Click **Reset System** to reset your transaction monitoring system. The confirmation window is displayed.

Figure 3-67 Reset System



4. Click **RESET** to reset the system. It will archive all the existing data and you need to reconfigure your transaction monitoring system. Or Click **Cancel** to cancel the action.

4

Understanding the OFSCA Dashboard

This section provides a comprehensive overview of the Oracle Financial Services Compliance Agent Cloud (OFSCA) performance monitoring dashboard, highlighting its key components and functionalities.

Topics:

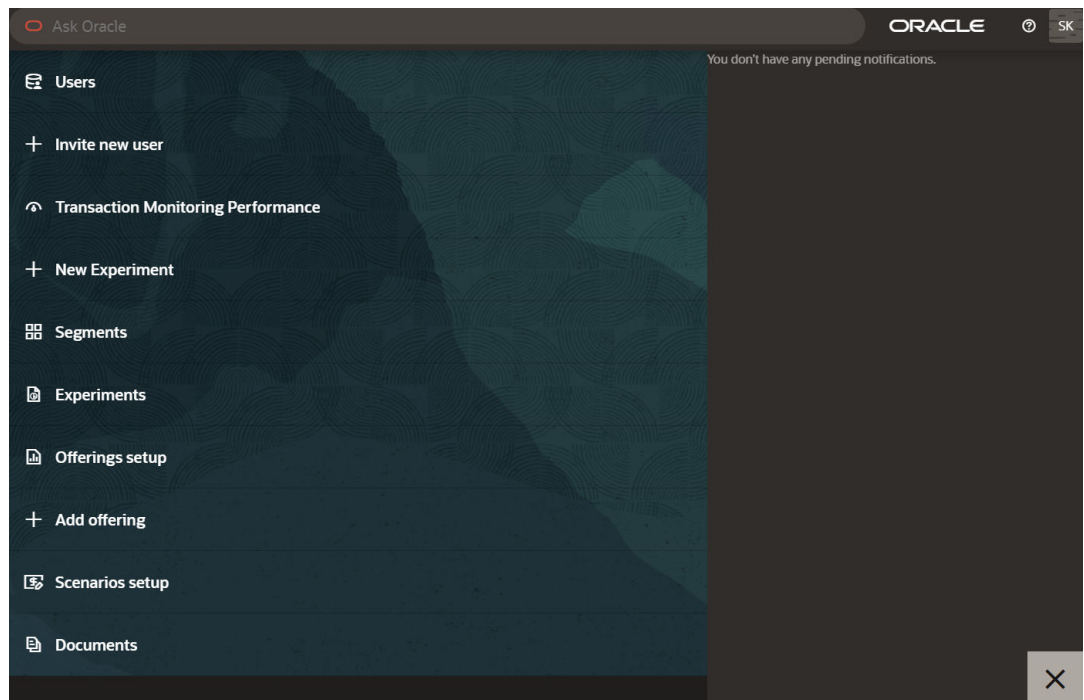
- [Overall System Performance](#)
- [Segment Performance](#)

The dashboard includes various components that provide valuable insights into system performance.

To access the Transaction Monitoring Performance dashboard, follow these steps:

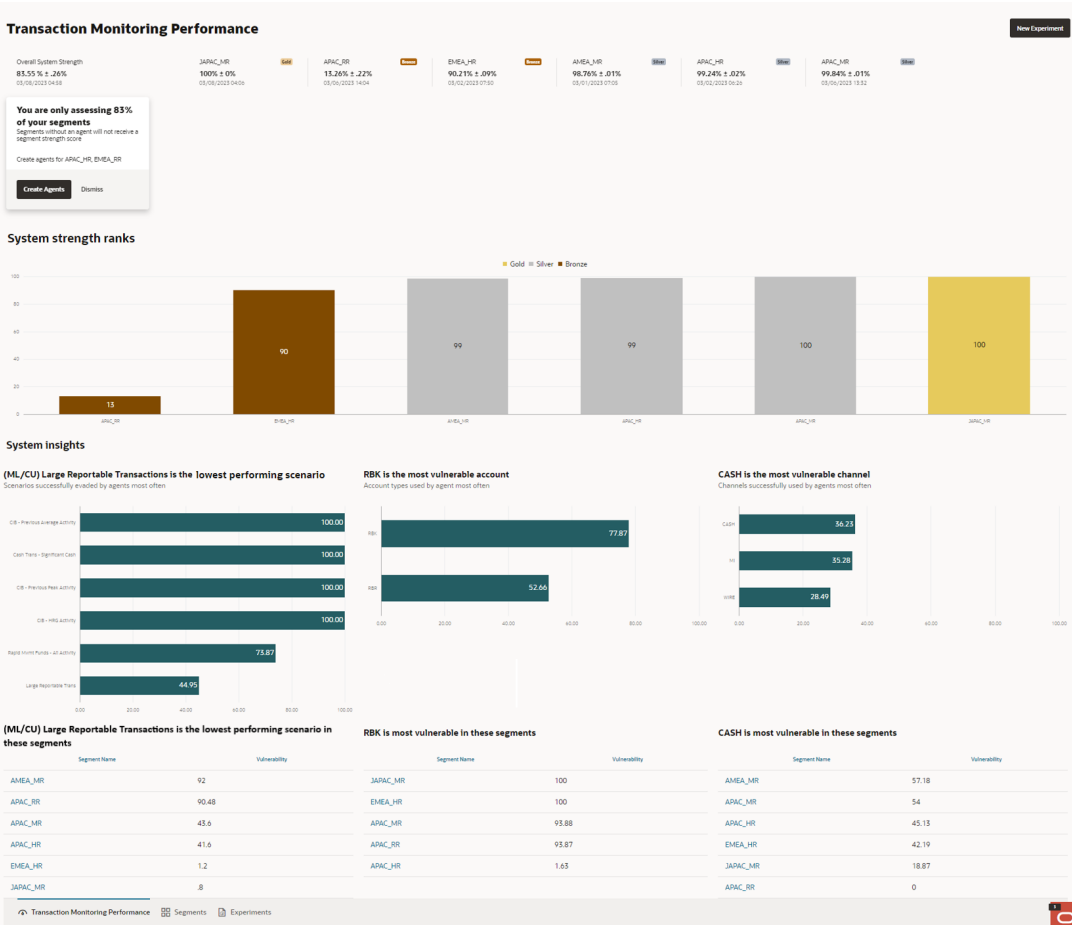
1. Click **Open Ask Oracle**  to display the Ask Oracle window. The following window is displayed.

Figure 4-1 Application Menu



2. Click **Transaction Monitoring Performance** menu to display the Transaction Monitoring Performance dashboard window. The following window is displayed.

Figure 4-2 Transaction Monitoring Performance

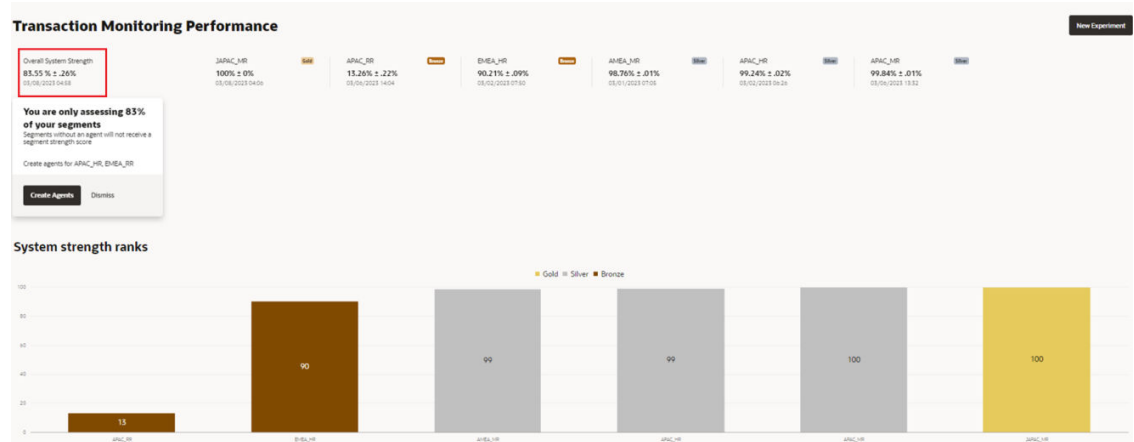


Overall System Performance

This metric, displayed on the Overall System Strength component of the Transaction Monitoring System, indicates the general strength of your institution's segments, with higher values being more desirable than lower ones.

Overall System Strength: Displays the overall strength of the Transaction Monitoring System across all your institution's segments. For this metric, a higher value is preferable to a lower value.

Figure 4-3 Overall System Strength

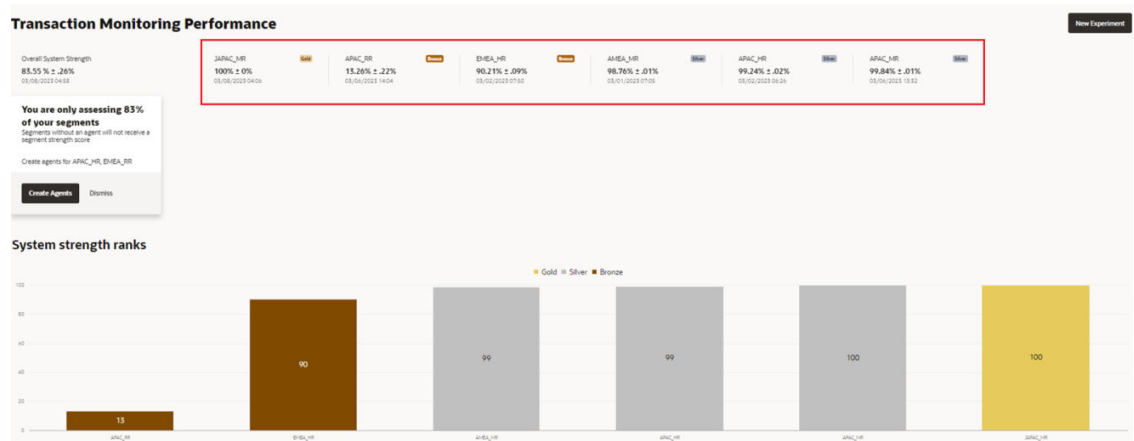


Note:

When Agents are not created for all the available Segments, you can view the **You are assessing only _ % of your segments** tile under the Transaction Monitoring Performance dashboard. Click **Create Agents** to create agents for other segments. For example, see the **Overall System Strength** image.

Individual Segment Strength: Displays the strength of each individual segment

Figure 4-4 Individual Segment Strength

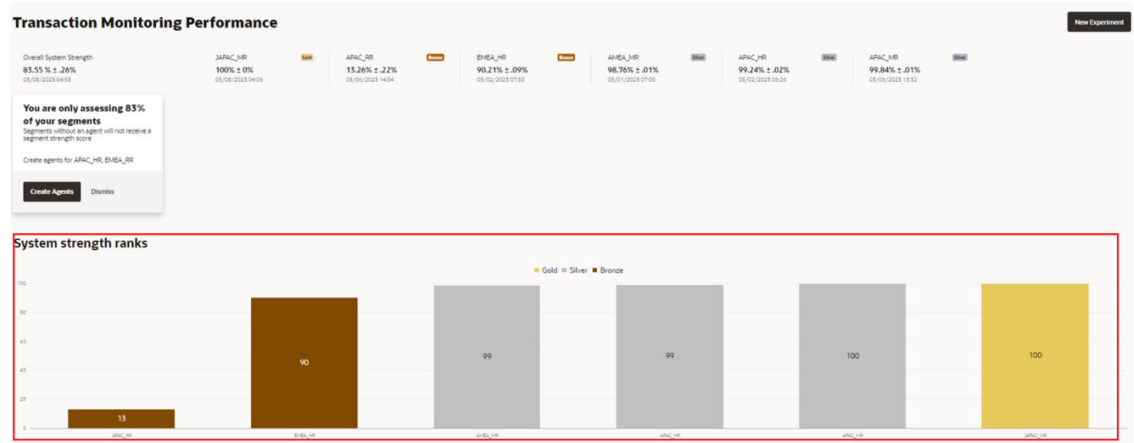


System Strength ranks: The System Strength Ranks component displays each segment's strength and confidence rankings, which can be viewed by hovering over the specific segment. Based on the performance of the TMS for a given segment, it is categorized as follows:

- **Gold:** The segments in the top third in terms of performance are in the Gold category.
- **Silver:** The segments in the middle third in terms of performance are in the Silver category.
- **Bronze:** The segments in the bottom third in terms of performance are in the Bronze category.

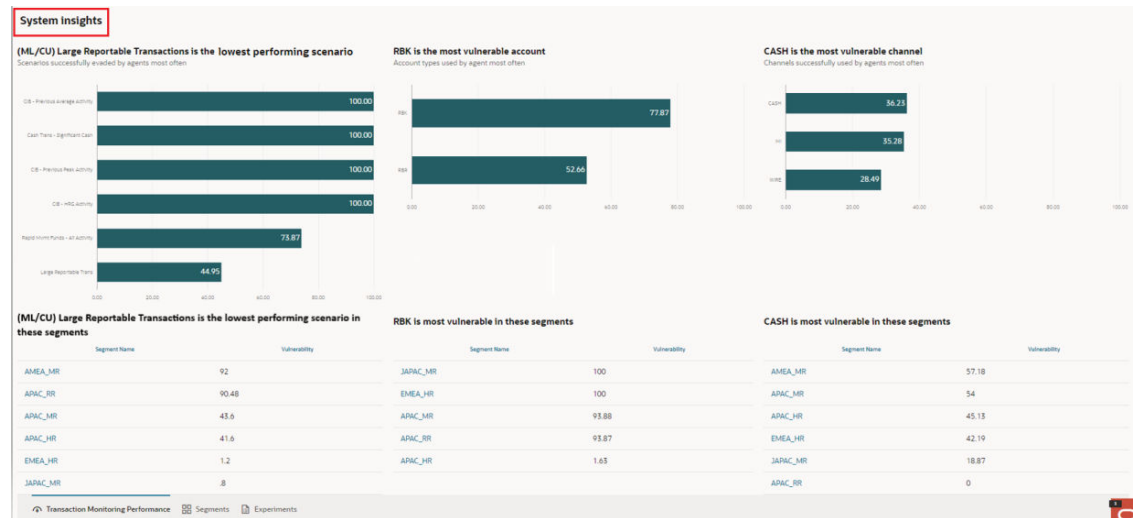
Ideally, the segments that are considered high risk by an institution should be in the gold category, while segments that are low risk can be in the bronze or silver category.

Figure 4-5 System Strength ranks



System Insights: Displays the overall system level insights.

Figure 4-6 System Insights

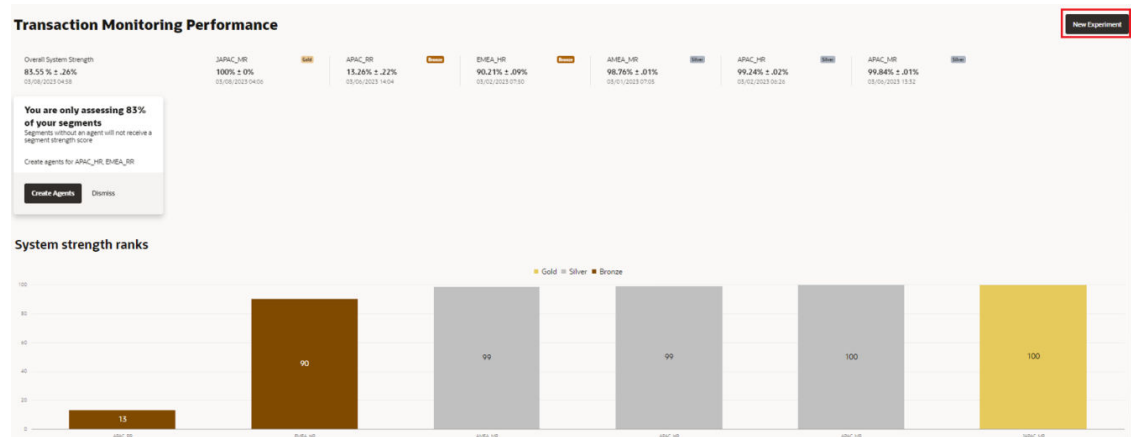


- **<(ML/AC) CIB: High Risk Geography Activity>** is the lowest performing scenario: The system highlights the scenario with the lowest performance and identifies the segments that require attention. We recommend addressing this scenario in the listed segments. Access the dashboard for the respective segment by clicking the hyperlink provided.
- **<RBR>** is the most vulnerable account: The system highlights the most susceptible account type and identifies the segments where the account type is most vulnerable. We recommend addressing any monitoring gaps related to this account type in the listed segments. Access the dashboard for these segments by clicking on the provided hyperlink.
- **<WIRE>** is the most vulnerable channel: The system highlights the most vulnerable communication channel and identifies the segments where the channel is at the highest

vulnerable. We recommend addressing any monitoring gaps related to this channel in the listed segments. Access the dashboard for this segment by clicking on the provided hyperlink.

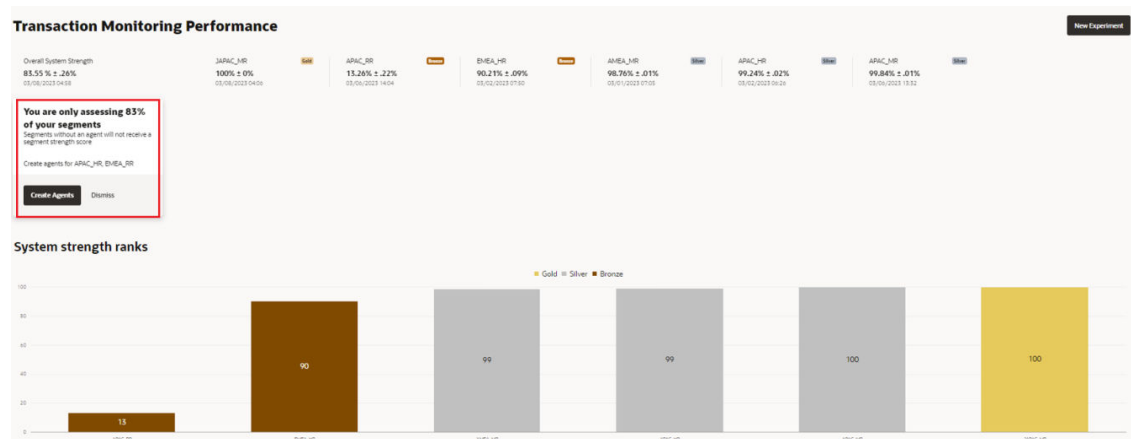
New Experiment: You can create a new user defined experiment. For more information, see the [User Defined Experiment](#) section.

Figure 4-7 New Experiment



Create Agents: You can create an agent for the segments which is not created during the initial configuration. For more information, see the [Creating an Agent](#) section.

Figure 4-8 Create Agents

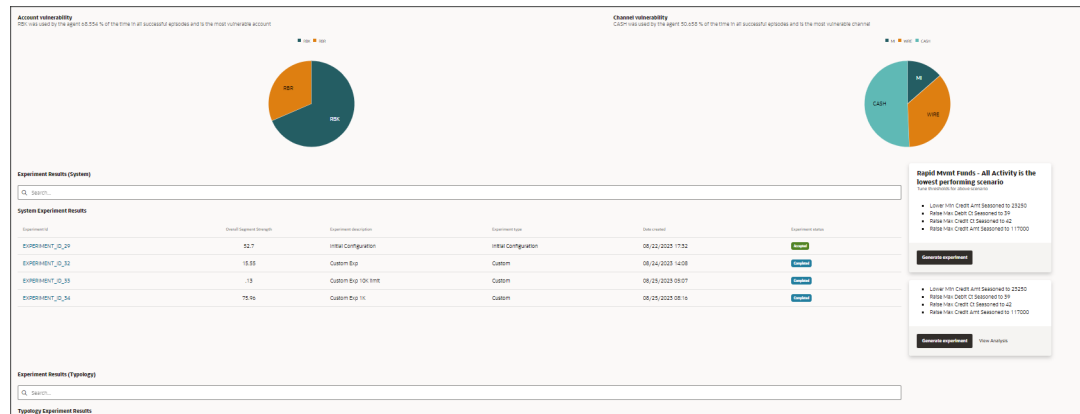


Segment Performance

You can view the individual segment dashboard as follows:

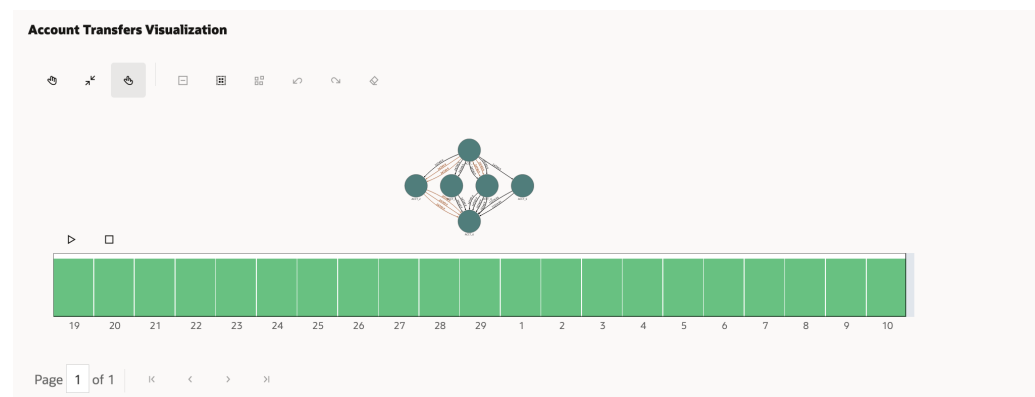
1. Click on the individual segment **<APAC_MR>** at the top of the dashboard to view the individual segment dashboard. The following window is displayed.

Figure 4-9 Segment Dashboard



- The segment dashboard contains the following:
 - Scenario Performance:** The scenario performance metric measures the level of resistance provided by scenarios against an intelligent adversarial agent. A high value of the performance metric indicates significant resistance offered by the scenario, which alerts on any attempts to move money through your institution by the agent. Based on performance, the scenarios are bucketed into three categories as follows:
 - Gold:** The scenarios in the top third in terms of performance are in the Gold category.
 - Silver:** The scenarios in the middle third in terms of performance are in the Silver category.
 - Bronze:** The scenarios in the bottom third in terms of performance are in the Bronze category. Tuning one of the low performing scenarios in the Bronze category is one way to improve performance of the segment.
 - Account Transfers Visualization:** This option allows you to visualize the episodes generated by the agent to evade an institution's TMS. This will allow institutions to understand the nature of these patterns and determine if they present a material risk to the institution.

Figure 4-10 Account Transfers Visualization



- Account Vulnerability:** The account vulnerability metric identifies the account types most susceptible to exploitation by an intelligent agent to transact money through your financial system. A high value for this metric indicates that the agent prefers this specific account type while moving money through your institution.

- **Channel Vulnerability:** The channel vulnerability metric identifies the channels most susceptible to exploitation by an intelligent agent to transact money through your financial system. A high value for this metric indicates that the channel is the preferred instrument the agent uses to move money through your institution. Tuning scenarios and implementing controls that monitor this specific channel is recommended to address any shortcomings in your transaction monitoring system.
- **System Experiment:** Experiments to assess the performance of the TMS holistically for the chosen segment.
- **Typology:** Experiment to show how well the system performs against specific typologies.

For more information about Recommendations to increase segment strength, see the [Generating Experiment from Recommendation](#) section.

3. For more information on these metrics, see the [Understanding the OFSCA Metrics](#) section.

5

Running and Comparing Experiments

You can run the experiment in the following modes:

- [User Defined Experiment](#)
- [Generating Experiment from Recommendation](#)

You can compare two experiments as explained below:

- [Comparing an Experiment](#)

User Defined Experiment

This section provides a guide on creating and executing customized experiments to validate any hypotheses you may have. Conducting these experiments allows you to simulate the effects of changes made to your transaction monitoring system. In turn, this enables you to carry out thorough what-if analysis, evaluate the impact of various decisions and make the most informed decisions accordingly.

Topics:

- [Selecting the Segment](#)
- [Selecting an Agent](#)
- [Copying or Modifying the Control Set](#)
- [Monitoring New Offerings](#)
- [Reviewing the Experiment](#)

Generating New Experiment

To generate a new experiment, follow these steps:

1. Click **New Experiment** on the dashboard to generate a new experiment. The New Experiment window is displayed.

Figure 5-1 New Experiment



2. Click **Start** to start configuring the new experiment. The Select Segment window is displayed.
 - If an experiment has been configured but has not been executed then dialog appears.
 - Click **Continue** to continue with the configured data for the experiment or click **Discard** to discard the configured data and the Select Segment window is displayed.

Selecting the Segment

To select the segment, follow these steps:

Figure 5-2 Select Segment

New Experiment

Select Segment

Discard Continue

Select Segment

Required

1 | 4 Steps

Select Segment

Select Agent

Copy or modify control set

Review

1. Select the required segment from the Select **Segment** drop-down list.
2. Click **Continue** to navigate to the Select Agent step. Or
Click **Discard** to discard the current activity and return to the New Experiment window and again click **Start** to start the **New Experiment** from the initial steps.

Selecting an Agent

You can select from one of the available agents or create a new agent.

Figure 5-3 Select Agent

Select Agent

Choose existing or create a new agent to simulate adversarial transactions

Create Agent

Select Agent	Agent Name	Agent Description	Target	Max	Min	Intermediate accounts and distribution	Actions
☐	APAC_HR Agent 1	Initial Config Agent	RBK	\$500000	\$5000	CBK 33.3%, RBK 33.3%, RBR 33.3%	...
☐	APAC_HR Agent 2		RBK	\$96000	\$2000	CBK 33.3%, RBK 33.3%, RBR 33.3%	...
☐	APAC_HR Agent 3	Initial Config Agent	RBK	\$96000	\$4000	CBK 33.3%, RBK 33.3%, RBR 33.3%	...
☐	APAC_HR Agent 4 New Account Type Offering	Agent for assessing risk of new offering CHK	RBK	\$500000	\$5000	CBK 25%, CHK 25%, RBK 25%, RBR 25%	...
☒	APAC_HR HT Agent 4	Initial Config Agent	RBK	\$96000	\$4000	CBK 33.3%, CHK 33.3%, RBR 33.3%	...

To select/create an agent, follow these steps:

1. Select the agent that is created during the initial setup on the **Select Agent** option. You can also select experiment for HT agent. Or

If you want to create a new agent then click **Create Agent**.

For information about how to create an agent, see the [Creating an Agent](#) section. Once the agent is created, then select the created agent.

2. Click **Continue** to navigate to the Copy and modify control set step.

Copying or Modifying the Control Set

This section demonstrates how to specify the controls (scenario thresholds, account transaction product constraints) that are evaluated in an experiment.

Figure 5-4 Copy / modify the Control Set

New Experiment

Copy and modify control set

Discard Continue

Select a scenario threshold set and/or account-channel constraint set to modify.

Agent	Target Account	Min	Max	Intermediate Accounts
EMEA_HR Agent	RBR	\$44000	\$2200	RBK, 50%, RBR 50%

Experiment account-channel constraint set name Required

Experiment scenario threshold set name Required

Experiment Description Required

Scenarios threshold set name Required

Account-Channel constraints (per day)

Account-channel constraint set Required

Q Search...

3/4 Steps

- Select Segment
- Select Agent
- Copy and modify control set**
- Review

Enter/select the details in the following fields:

- **Experiment account-transaction product constraint set name:** Select the drop-down list from the Account-transaction product constraint set to define the name.
- **Experiment scenario threshold set name:** Enter the Threshold Set Name. The name must be unique to a particular threshold set.
- **Experiment Description:** Enter the description of the Experiment. This field is optional, but a good description can be useful for audit purposes.

Managing Scenarios Threshold Set Name

Use this section to add scenarios, add and edit threshold values in the Copy and Modify Control Set page.

To add Scenarios threshold set name, follow these steps.

1. On the **Copy and Modify Control Set** page, go to **Scenarios threshold set name** field.
2. Select the required scenario threshold set you want to use or modify. The Add Scenario button allows you to add new scenarios to your control set.

Figure 5-5 Scenario

Scenarios

Threshold set 1

Required

Add Scenario

(ML/AC) CIB: Significant Change from Previous Average Activity	  >
(ML/AC) CIB: Significant Change from Previous Peak Activity	  >
(ML/CU) Large Reportable Transactions	  >
(ML/CU) Rapid Movement of Funds - All Activity	  >
(ML/CU) Single or Multiple Cash Transactions: Large Significant Transactions	  >

You can perform the following:

3. Click **Add scenario** to add a new scenario for the respective threshold set. The following window is displayed

Figure 5-6 Add Scenario

Scenarios Supported

Q Search...

Action

Scenario Name

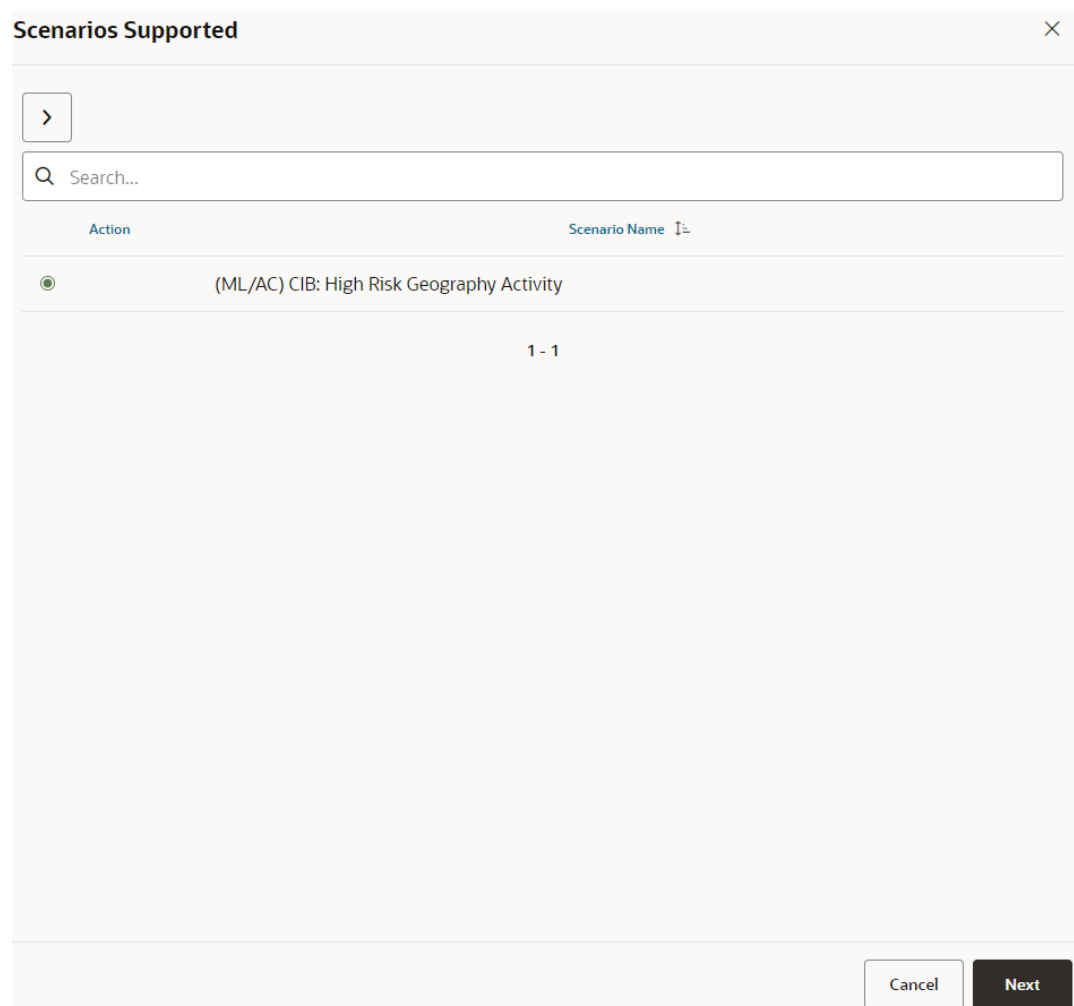
(ML/AC) CIB: High Risk Geography Activity

1 - 1

Cancel

- a. Search the required scenario in the Search box.
- b. Click on the **Action** option of the required scenario to be added to the threshold set.

Figure 5-7 Selected Scenario



The image shows a dialog box titled "Scenarios Supported" with a close button (X) in the top right corner. Inside the dialog, there is a navigation icon (a square button with a right-pointing chevron) in the top left. Below it is a search bar with a magnifying glass icon and the placeholder text "Search...". Under the search bar is a table with two columns: "Action" and "Scenario Name". The "Scenario Name" column has a sort icon (two vertical bars). There is one row in the table with a radio button in the "Action" column and the text "(ML/AC) CIB: High Risk Geography Activity" in the "Scenario Name" column. Below the table, the text "1 - 1" is centered. At the bottom right of the dialog are two buttons: "Cancel" and "Next".

Action	Scenario Name 
☒	(ML/AC) CIB: High Risk Geography Activity

1 - 1

Cancel Next

- a. Click **Navigation** icon  or click **Next** to view the threshold details. The following window is displayed

Figure 5-8 Threshold Details

Threshold details

☐	≡	Threshold Name	Threshold Value
☒	≡	Look_Back_Period	12
☐	≡	Mantas_Bus_Acct_Type_Lst	RBK,RBR,CBK
☐	≡	Max_Num_SD_MR	10
☐	≡	Min_Amt_MR	27000
☐	≡	Min_Incr_MR	200
☐	≡	Min_Num_SD_MR	2

1 rows selected Total 6

Cancel Add Scenario

- a. Double-click on the required Threshold Value field and then edit the threshold value.
 - b. Click **Add Scenario**. The scenario is added to the respective threshold set.
4. Click **Delete**  icon to delete the selected scenario.
 5. Click **Edit**  icon to edit the selected scenario. The following window is displayed.

Figure 5-9 Edit a Scenario

Threshold details ×

☐	≡	Threshold Name	Threshold Value
☒	≡	Max_Num_SD_MR	10
☐	≡	Min_Amt_MR	27000
☐	≡	Min_Incr_MR	200
☐	≡	Min_Num_SD_MR	2
☐	≡	Look_Back_Period	12
☐	≡	Mantas_Bus_Acct_Type_Lst	RBK,RBR,CBK

1 rows selectedTotal 6

CancelUpdate Scenario

- a. Double-click on the required Threshold Value field and then edit the threshold value.

Figure 5-10 Threshold Value

Threshold details ×			
☐	≡	Incl_Jurisdictions_Lst	'Inactive'
☐	≡	Include_Related_Parties_Fl	'Y'
☐	≡	Mantas_Bus_Acct_Type_Lst	RBK,RBR,CBK
☐	≡	Max_Days_Opened	90
☐	≡	Min_Individual_Trans_Amt	10000
☐	≡	Lrf_Digits	4
☐	≡	Primary_Cust_Fl	'Y'
☐	≡	Actvty_Risk_Cutoff_Lvl	5
☐	≡	All_Trans_Src_Fl	'Y'
☐	≡	Curr_Type	'B'
☐	≡	Effctv_Risk_Cutoff_Lvl	5
☐	≡	Frequency_Period	7
☐	≡	Incl_BO_Trnx_Prdct_Type_Lst	'JOURNAL'
☒	≡	Incl_Cash_Trnx_Prdct_Type_Lst	'DEBIT-CARD', 'SVC', 'CREDIT-CARD', 'CURRENCY',...
☐	≡	Incl_ML_Trnx_Prdct_Type_Lst	'CASH-EQ-CASHIER-CHECK', 'CASH-EQ-CERT-CH...

- a. Click **Update Scenario** to modify the information
6. Click **Navigation**  icon to view the scenario information as follows:

Figure 5-11 Scenario Information

(ML/AC) CIB: Significant Change from Previous Average Activity ×	
Threshold Name 	Threshold Value
Look_Back_Period	12
Mantas_Bus_Acct_Type_Lst	RBK,RBR,CBK
Max_Num_SD_MR	10
Min_Amt_MR	27000
Min_Incr_MR	200
Min_Num_SD_MR	2
1 - 6	

Managing Account-Transaction Product Constraints (per day)

Use this section to add and edit account transaction details in the Copy and Modify Control Set page.

When a new account or transaction product is added to a segment, it is necessary to Select the required option from the drop-down list. The account types will be displayed based on the selected Account-transaction product constraint set.

Figure 5-12 Account-transaction product constraint set

Account-Channel constraints (per day)

Account-channel constraint set
Control set test 5

Required

Q Search...

CBK

 >

RBK

 >

RBR

 >

You can perform the following:

1. Search the account type in the Search box.
2. Click **Edit**  icon to edit the selected account type. The following window is displayed.

Figure 5-13 Edit an Account

The dialog box titled "Channel Details" contains the following elements:

- Account Type:** RBK
- Table:** A table with two columns: "Channel" and "Withdrawal Limit". It contains one row with "WI" and "4000".
- Footer:** "1 rows selected" and "1 - 1".
- Buttons:** "Cancel" and "Update".

Channel	Withdrawal Limit
WI	4000

- a. Double-click on the **Withdrawal Limit** field and edit the required value.
- b. Click **Update** to update the modified value.
3. Click **Navigation** > icon to view the transaction product information as follows

Figure 5-14 Channel Details

The image shows a 'Channel Details' window with a close button (X) in the top right corner. Inside the window, the 'Account Type' is set to 'RBK'. Below this, there is a table with two columns: 'Channel' and 'Withdrawal Limit'. The table contains one row with 'WI' in the 'Channel' column and '4000' in the 'Withdrawal Limit' column. Below the table, the text '1 - 1' is displayed. At the bottom right of the window, there is a 'Cancel' button.

Channel	Withdrawal Limit
WI	4000

4. Click **Continue** on the Copy and modify control set window to navigate to the Review step.

Monitoring New Offerings

Use this section to modify the threshold value for the newly added offerings (Account Type and Transaction product).

For more information on how to add a new offering (Account Type or Transaction product), see [Modifying the System](#).

To monitor the newly added offerings, follow these steps:

1. On the **Copy and Modify Control Set** section, go to Scenarios Threshold Set Name drop-down list.
2. Select the required Scenarios threshold set name from the drop-down list. The scenarios are displayed based on the selected Scenarios threshold set name.

- Click the **Edit**  icon to modify the selected scenario threshold values. The Threshold Details window is displayed.

Figure 5-15 Threshold Details Window

Threshold details ×			
☐	≡	Incl_Jurisdictions_Lst	'Inactive'
☐	≡	Include_Related_Parties_Fl	'Y'
☐	≡	Mantas_Bus_Acct_Type_Lst	RBK,RBR,CBK
☐	≡	Max_Days_Opened	90
☐	≡	Min_Individual_Trans_Amt	10000
☐	≡	Lrf_Digits	4
☐	≡	Primary_Cust_Fl	'Y'
☐	≡	Actvty_Risk_Cutoff_Lvl	5
☐	≡	All_Trans_Src_Fl	'Y'
☐	≡	Curr_Type	'B'
☐	≡	Effctv_Risk_Cutoff_Lvl	5
☐	≡	Frequency_Period	7
☐	≡	Incl_BO_Trnx_Prdct_Type_Lst	'JOURNAL'
☒	≡	Incl_Cash_Trnx_Prdct_Type_Lst	'DEBIT-CARD', 'SVC', 'CREDIT-CARD', 'CURRENCY',...
☐	≡	Incl_MI_Trnx_Prdct_Type_Lst	'CASH-EQ-CASHIER-CHECK', 'CASH-EQ-CERT-CH...

- Double-click on the required Threshold Value field and then edit the threshold value.
- When a new offering (account type) is added, you can append the name of new account type to list in Mantas_Bus_Acct_Types_Lst.
- When a new transaction product is added to system, you can append the name of that transaction product to the value of one of the following thresholds.
 - Incl_Cash_Trnx_Prdct_Type_Lst - If new Product is mapped to Cash transaction product.
 - Incl_MI_Trnx_Prdct_Type_Lst - If new Product is mapped to MI transaction product.
 - Incl_Wire_Trnx_Prdct_Type_Lst - If new Product is mapped to WIRE transaction product. For example, ZELLE is mapped to WIRE (Can be comma separated in case of multiple Products).
 - Incl_BO_Trnx_Prdct_Type_Lst - If new Product is mapped to BO transaction product.
- Click **Update Scenario** to modify the information.

Reviewing the Experiment

In this section, you can verify all the parameters before running the experiment.

Figure 5-16 Review Experiment

New Experiment

Review JAPAC_MR Threshold set 100 Experiment

Discard Run Experiment

After you run the experiment, you will be able to evaluate the new strength score before committing any changes to production.

Segment
JAPAC_MR

Agent

JAPAC_MR Agent 1.0 Overall segment agent	RBR Max \$3000 Min \$2000	RBK 50%, RBR 50%
---	---------------------------------	------------------

Control Set

Scenarios
JAPAC_MR Threshold set 100 (current)

Account-Channel constraints (per day)
JAPAC_MR Control set test 100 (current)

JAPAC_MR Threshold set 100 Experiment modifications

Scenarios
7 changes

(ML/AC) CIB: Significant Change from Previous Average Activity added

(ML/AC) CIB: Significant Change from Previous Average Activity added

1. Click Run Experiment to generate the new experiment. Upon completion of the experiment, the status of the experiment can be viewed in the Experiments tab.
2. The results of the experiments will be available in the Transaction Monitoring Performance Dashboard or you can view results by clicking the View Results on the notification of the Ask Oracle window.

Segment Strength

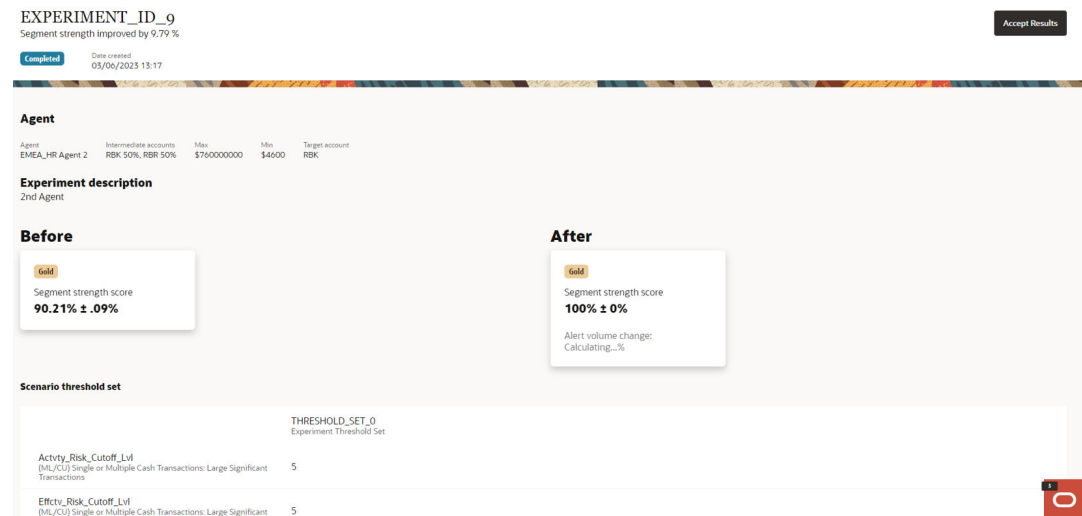
You can view the experiments for the following cases:

- **System Experiment:** This allows you to view the experiments which depicts system strength.
- **Typology:** This allows you to view the experiments which covers typology scenarios like Human Trafficking

To view result of the generated experiment for System Experiments and Typology, follow these steps:

1. Click on the required **Experiment ID** in the Experiments tab to view the System Experiments results. The following window is displayed.

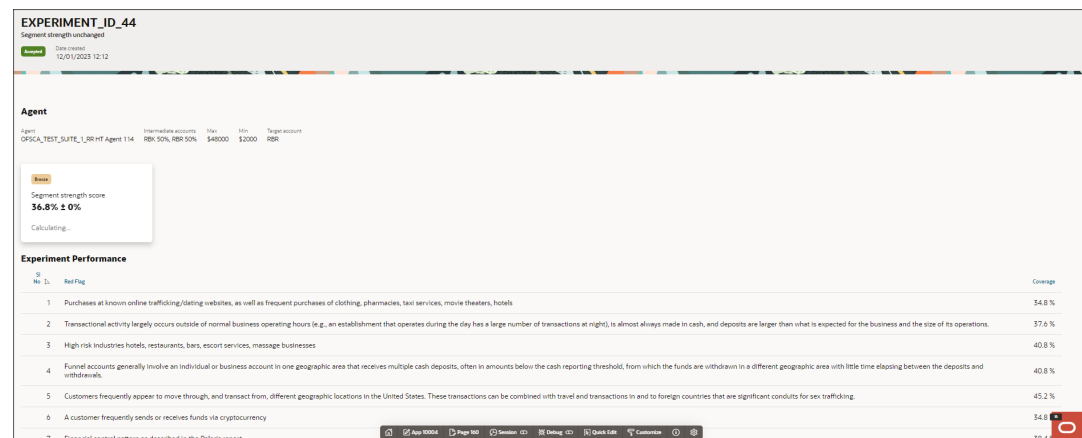
Figure 5-17 Segment Strength



Here, the expected change in performance of the system and the expected change in alert volume are displayed. An experiment is successful, if there is an increase in system strength without a disproportionate increase in alert volume.

2. Click on the required **Experiment ID** in the Experiments tab to view the typology results. The following window is displayed.

Figure 5-18 Typology Experiment



If you select a Typology Experiments, for example, Human Trafficking, a detailed report in terms of Red Flag Coverage is displayed for the same. The Metrics cover seven different patterns as below:

- a. Purchases at known online trafficking/dating websites, as well as frequent purchases of clothing, pharmacies, taxi services, movie theatres, hotels
- b. Transactional activity largely occurs outside of normal business operating hours (for example, an establishment that operates during the day has a large number of transactions at night), is almost always made in cash, and deposits are larger than what is expected for the business and the size of its operations.

- c. High risk industries includes hotels, restaurants, bars, escort services, massage businesses
- d. Funnel accounts generally involve an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.
- e. Customers frequently appear to move through and transact from different geographic locations in the United States. These transactions can be combined with travel and transactions in and to foreign countries, which are significant conduits for sex trafficking.
- f. A customer frequently sends or receives funds via cryptocurrency
- g. Financial control pattern as described in the Polaris report. The Value closer to 100 indicates higher Coverage. However, a value close to 0 indicated lesser Coverage.

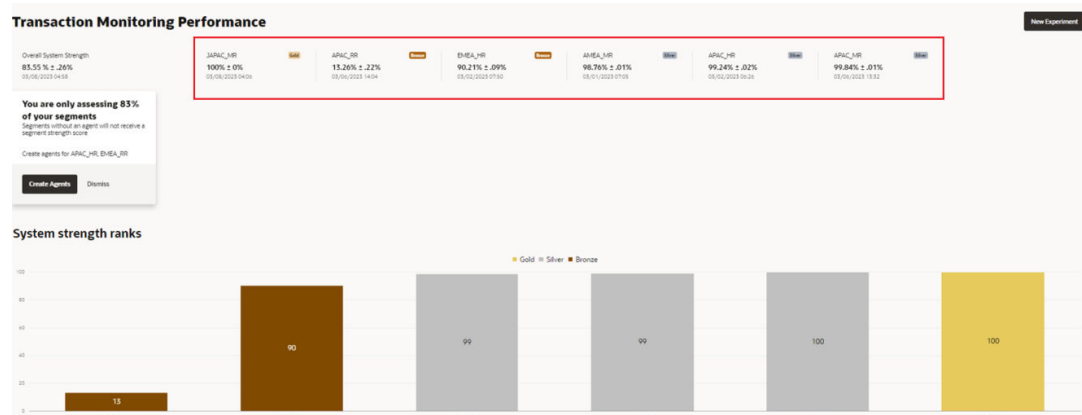
Generating Experiment from Recommendation

OFSCA offers recommendations to tackle the identified deficiencies. A deficiency can be a low scenario performance or a high account/ channel vulnerability. The recommendations aim to tune the scenario with the highest chances of addressing the selected deficiency. To generate recommended thresholds for the scenario, OFSCA evaluates the performance of simulated TMS against multiple sets of candidate thresholds within proximity of the production (currently applied) values. A set of candidates is evaluated by using a combined metric analyzing both the percentage of episodes getting alerted and the average number of distinct alerts per episodes. OFSCA recommends the set that has performed optimally as per the metric. This section describes the process for generating experiments to assess the effectiveness of these recommendations.

To generate an experiment for the particular segments, follow these steps:

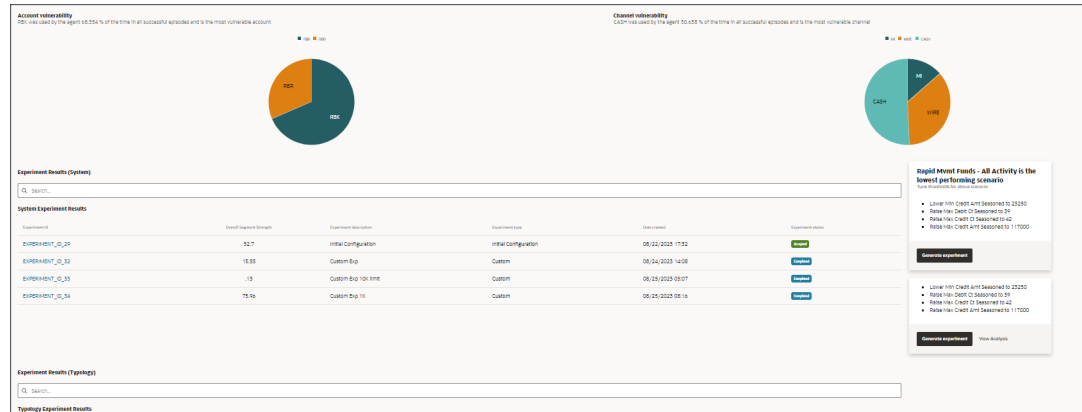
1. Click Open Ask Oracle  to display the Ask Oracle window.
2. Click **Transaction Monitoring Performance** menu to display the Transaction Monitoring Performance dashboard. The following window is displayed.

Figure 5-19 Transaction Monitoring Performance Dashboard



3. Click the required segment (for example, APAC_MR) to view the individual segment dashboard. The following window is displayed.

Figure 5-20 Segment Dashboard



This dashboard presents the insights generated for the scenario performance, account vulnerability, and transaction product vulnerability.

For each Insight, we see OFSCA-identified scenarios that can be adapted to address the identified vulnerabilities for each section. Besides, OFSCA provides specific threshold recommendations for the scenarios identified.

Generating Experiments for Segment

You can generate an experiment to evaluate this specific recommendation by clicking Generate Experiment on the segment dashboard.



Note:

If the results of the generated experiments do not meet your expectation, then consider generating a new experiment based on other recommendations displayed in the Transaction Monitoring Performance dashboard.

To generate an experiment, follow these steps:

1. Click **Generate Experiment** on the segment dashboard. The Copy or Modify Control Set window is displayed. The recommended threshold values are auto populated in the listed Scenarios.

Figure 5-21 Copy or Modify Control Set

Copy and modify control set

Select a scenario threshold set and/or account-channel constraint set to modify.

Agent	Target Account	Max	Min	Intermediate Accounts
AMEA_MR Agent 1	IBK	\$28800	\$1200	IBK 100%

MI is most vulnerable channel. Tune the scenario Large Reportable Trans because it was alerted least for the account type used most on MI channel. Raise to 15002880, Lower Min Trans Amt to 95680.

View Analysis

Experiment Description

MI is most vulnerable channel. Tune the scenario Large Reportable Trans because it was alerted least for the account type used most on MI channel. Raise to 15002880, Lower Min Trans Amt to 95680.

Scenarios threshold set name
Production Thresholds

Experiment scenario threshold set name
Production Thresholds

Search...

Add Scenario

(ML/AC) CIB: High Risk Geography Activity

(ML/AC) CIB: Significant Change from Previous Average Activity

Discard
Continue

- The dialog box appears if the unfinished experiment is running on the existing segment. In that case, click **OK** on the dialog box to continue generating the experiment.
 - The experiment description will be auto populated with the recommendation from the segment dashboard.
 - Do not change the default value in the Scenarios Threshold Set Name drop-down list.
- Enter the relevant name or description for threshold set in the Experiment Scenario Threshold Set Name field.
 - If you want to modify the recommended thresholds, Click **Edit**  icon against the existing scenarios. The Threshold Details window is displayed.
 - Modify the threshold value. Click **Update Scenario**. The Scenario List page is displayed.
 - Click **Continue** to navigate to the Review step. The following window is displayed.

Figure 5-22 Review Segment

New Experiment

Review AMEA_RR Threshold set 1 Experiment

Discard Run Experiment

After you run the experiment, you will be able to evaluate the new strength score before committing any changes to production.

Segment
AMEA_RR

Agent

AMEA_RR Agent 1.0 Overall segment agent	CBK Max \$100000 Min \$10000	RBK 75%, RBR 25%
--	------------------------------------	------------------

Control Set

Scenarios
AMEA_RR Threshold set 1 (current)

Account-Channel constraints (per day)
AMEA_RR Control set test 2 (current)

AMEA_RR Threshold set 1 Experiment modifications

Scenarios
0 changes

Account-Channel constraints (per day)
0 changes

4 | 4 Steps

Select Segment

Select Agent

Copy or modify control set

Review

- Click **Run Experiment** to run the experiment. A notification will be delivered through the Ask Oracle window when the experiment is complete and you can view the generated experiment either through the Transaction Monitoring Performance dashboard or in the Experiments tab.

View Analysis

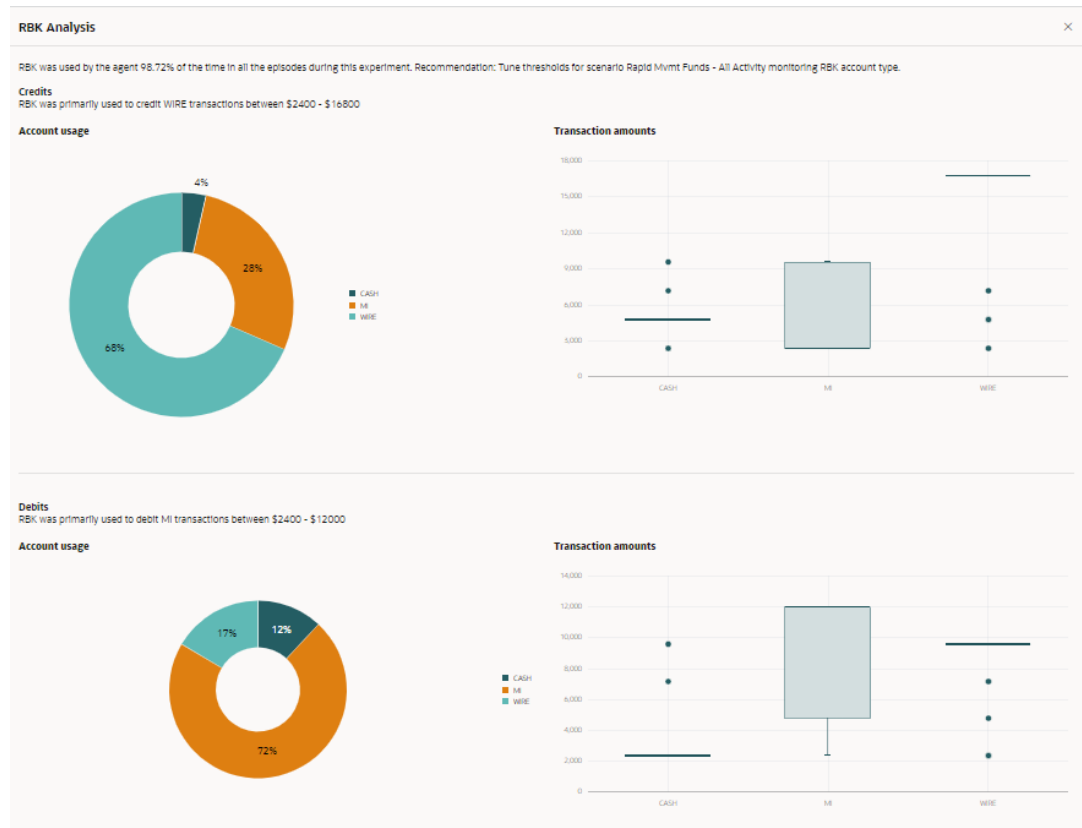
To view the identified vulnerability in detail, follow the step:

- Click View Analysis on the segment dashboard in each of the tiles provides a more detailed analysis of the identified vulnerability.

For account vulnerability, it presents an analysis of the agent's transactional activity involving the most vulnerable account type.

It presents a breakdown of activity in the account type by transaction product as well as the range of activity observed for each of these transaction products for credits and debits.

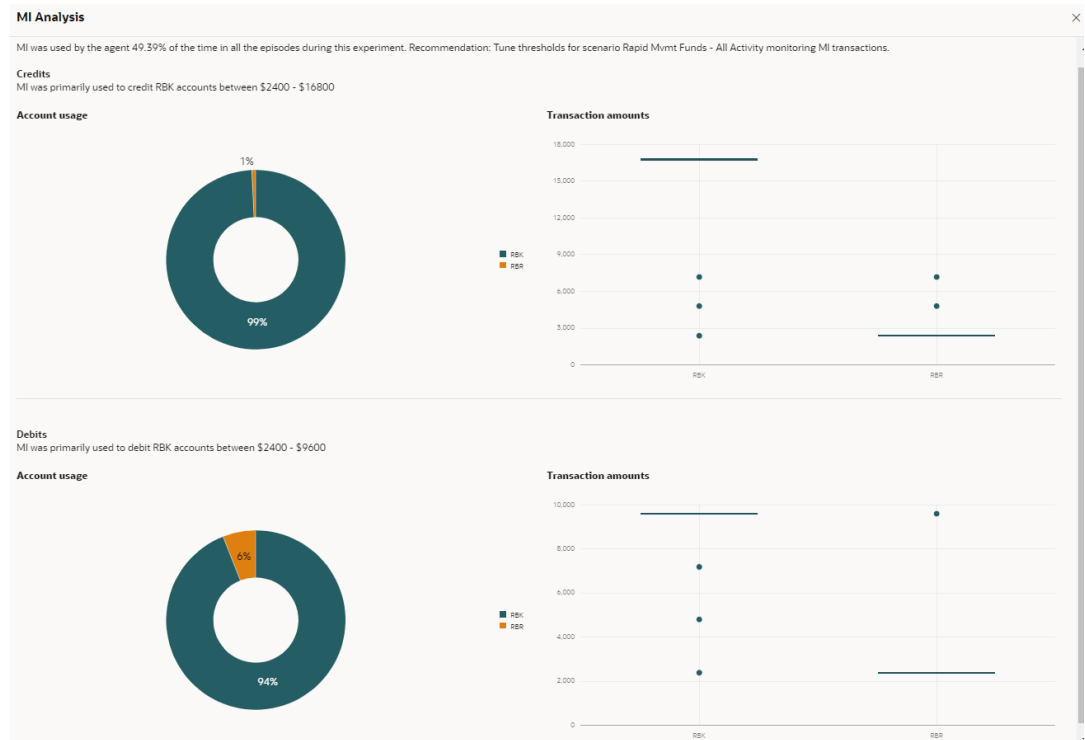
Figure 5-23 For Account Type



For transaction product vulnerability, it presents an analysis of the agent's transactional activity involving the most vulnerable transaction product type.

It presents a breakdown of activity in the transaction product type by account as well as the range of activity observed for each of these account types for credits and debits

Figure 5-24 For Channel



This can also inform hypotheses a user can test using custom experiments. For example, if the account vulnerability analysis indicates that wires are the most commonly used transaction product for a specific account, a user can try tuning thresholds of scenarios that monitor wires.

2. Hoverover to view details

Comparing an Experiment

In this section, you can compare two experiments of the same segment.

To compare the two experiments, follow these steps:

1. Click Open Ask Oracle  to display the Ask Oracle window.
2. Click **Experiments** menu to display the Experiments window. The following window is displayed.

Figure 5-25 Experiments

[illegible]

3. Click **Compare Experiment**. The following window is displayed.

Figure 5-26 Compare Experiment

Compare experiments [X]

Select 2 experiments in the same segment

Experiment 1 [v] Required

Experiment 2 [v] Required

Cancel Compare

4. Select the required experiment that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select the required experiment that you want to compare with experiment 1 from the Experiment 2 drop-down list.

 Note:

You can compare the experiments in the same segments only.

6. Click **Compare to compare** the selected experiments. The compared result is displayed. Results from the two selected experiments and the currently accepted experiment for the segment are displayed as shown in the below figure. Any differences between the agents used, and the thresholds evaluated are also displayed.

Figure 5-27 Experiment Result

Compare Experiments			
	EXPERIMENT_ID_8 Accepted	EXPERIMENT_ID_16 Custom Offering 2ELLE-40k Gift Experiment Results	EXPERIMENT_ID_17 Custom Offering 2ELLE Experiment Results
Segment strength score	50.65% ± 3.4%	44.0% ± 2.2%	40.25% ± 3.35%
Risk level	Low	Low	Low
Asset volume		120.19	1.72
Agent	DEMO005_OR Custom Agent 1	DEMO005_OR Custom Agent 1	DEMO005_OR Custom Agent 1
Experiment description	DEMO005_OR experiment	DEMO005_OR Control Set 16	Waiting for experiment TS data
Impact of Adding New Offering		7.40.35	7.10.55
Actions		Accept Results	Accept Results

You can compare the results between two experiments and accept them based on the segment strength score.

 Note:

You can not accept the result if the experiment has more than four accounts.

Comparing Experiments to Assess Risk of New Offerings

Use this section to verify the impact of adding a new offering such as account type and transaction product by comparing the experiments.

Topics:

- [Risk of New Offering-Account Type](#)
- [Risk of New Offering-Transaction Product](#)

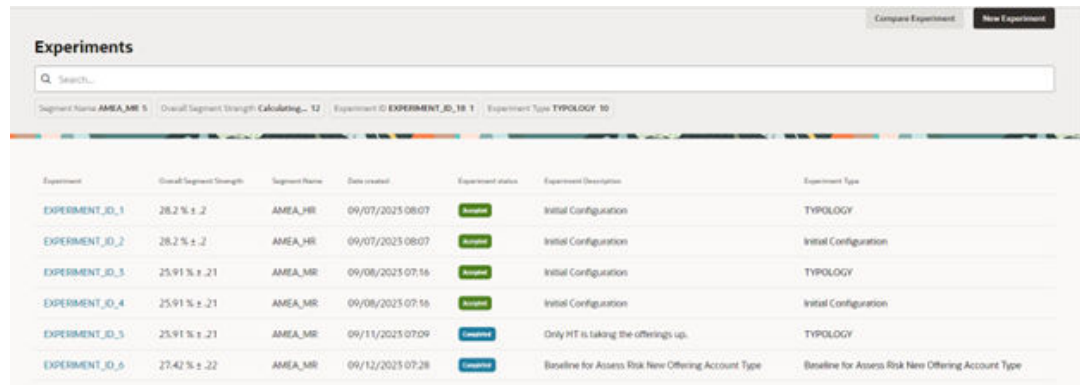
Risk of New Offering-Account Type

Use this section to verify the impact of adding a new offering as an account type by comparing the experiments.

To compare the two experiments to assess the risk of the new offering as an account type, follow these steps:

1. Click **Open Ask Oracle**  to display the Ask Oracle window.
2. Click the **Experiments** menu. The Experiments window is displayed.

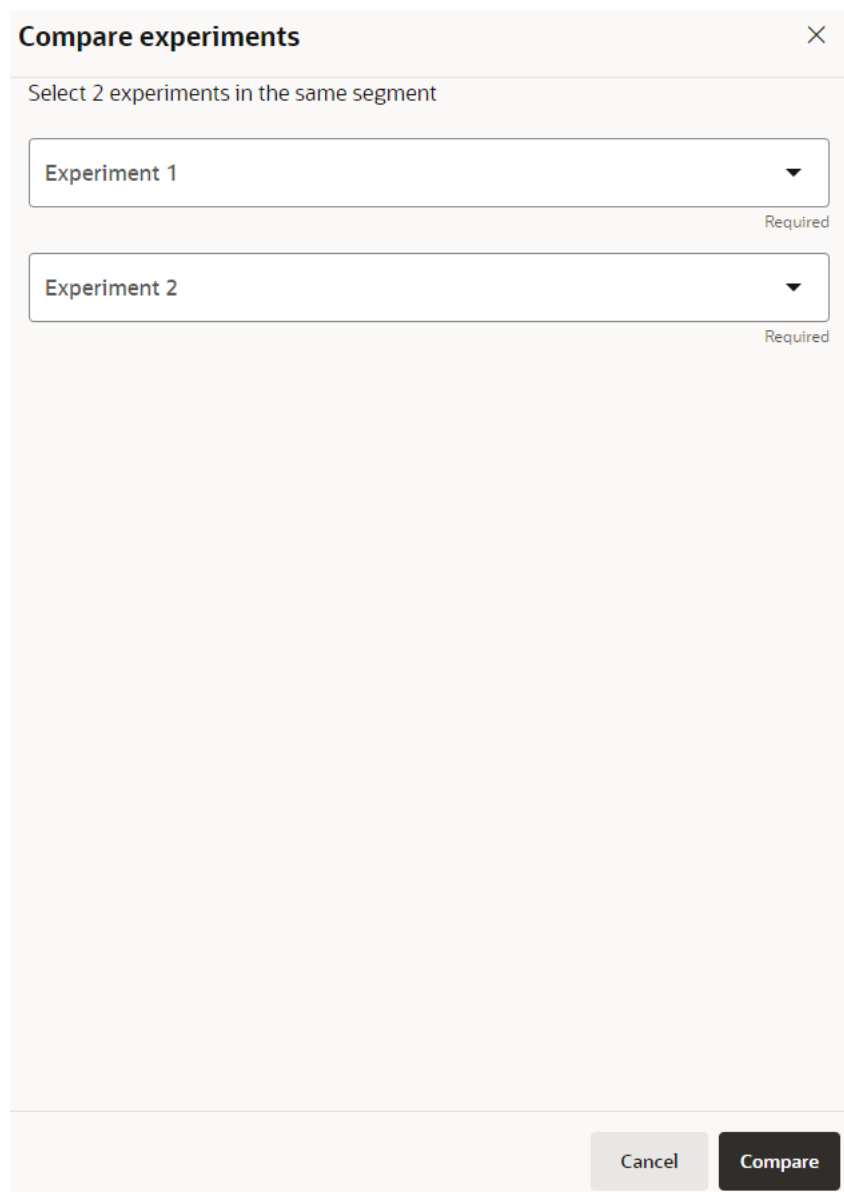
Figure 5-28 Compare Experiments



Experiment	Overall Segment Strength	Segment Name	Date created	Experiment status	Experiment Description	Experiment Type
EXPERIMENT_ID_1	28.2 % ± .2	AMEA_MRI	09/07/2025 08:07	Completed	Initial Configuration	TYPOLOGY
EXPERIMENT_ID_2	28.2 % ± .2	AMEA_MRI	09/07/2025 08:07	Completed	Initial Configuration	Initial Configuration
EXPERIMENT_ID_3	25.91 % ± .21	AMEA_MRI	09/08/2025 07:56	Completed	Initial Configuration	TYPOLOGY
EXPERIMENT_ID_4	25.91 % ± .21	AMEA_MRI	09/08/2025 07:56	Completed	Initial Configuration	Initial Configuration
EXPERIMENT_ID_5	25.91 % ± .21	AMEA_MRI	09/11/2025 07:09	Completed	Only HT is taking the offerings up.	TYPOLOGY
EXPERIMENT_ID_6	27.42 % ± .22	AMEA_MRI	09/12/2025 07:28	Completed	Baseline for Assess Risk New Offering Account Type	Baseline for Assess Risk New Offering Account Type

- Click Compare Experiment. The following window is displayed.

Figure 5-29 Compare Experiment



Compare experiments

Select 2 experiments in the same segment

Experiment 1

Required

Experiment 2

Required

Cancel
Compare

4. Select the experiment which has a newly added offering as an account type that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select another experiment that has a newly added offering as the account type with different set of constraints that you want to compare with Experiment 1 from the Experiment 2 drop-down list.

 Note:

You can compare the experiments in the same segments only.

6. Click **Compare** to compare the selected experiments. The compared result is displayed. Results from the two selected experiments and the currently accepted experiment for the segment are displayed as shown in the below figure. Any differences between the agents used, and the thresholds evaluated are also displayed.

Figure 5-30 Experiment Result

Compare Experiments			
	EXPERIMENT_ID_9 Accepted	EXPERIMENT_ID_16 Custom Offering ZELLE-486 Limit Experiment Results	EXPERIMENT_ID_17 Custom Offering ZELLE Experiment Results
Segment strength score	50.05% ± 3.4%	4.48% ± 2%	40.25% ± 3.58%
Test time	0:00:00	0:00:00	0:00:00
Alert volume		140.78	1.72
Agent	DEVCORE_RR Custom Agent 1	DEVCORE_RR Custom Agent 1	DEVCORE_RR Custom Agent 1
Experiment description	DEVCORE_RR experiment	DEVCORE_RR Control Set 16	Warning 502 experiment TS alert
Impact of Adding New Offering		7.45.35	7.10.35
Actions		Accept Results	Accept Results

You can compare the results between the experiments to determine the incremental risk resulting from using different sets of controls to monitor the new account type. If the system strength has dropped relative to the accepted experiment, this indicates that the new account type is not monitored as effectively as existing accounts. This is acceptable if an institution knows the account is being offered to low risk customers.

If the system strength has not changed or increased relative to the accepted experiment, this indicates that the new account type is being more effectively monitored than existing account types. For accounts that are being offered to higher risk customers, institutions should look to devise controls that result in an increase in system strength.

7. Click **Accept Results** to accept the experiment for the particular segment.

 Note:

You can add up to 5 account types in an Experiment but only Experiments with up to 4 account types can be accepted

Risk of New Offering-Transaction Product

Use this section to verify the impact of adding a new offering as a transaction product by comparing the experiments.

To compare the two experiments to assess the risk of the new offering as a Transaction Product, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click the **Experiments** menu. The Experiments window is displayed.

Figure 5-31 Experiments

The screenshot shows the 'Experiments' window with a search bar and a table of experiment data. The table has columns for Experiment, Overall Segment Strength, Segment Name, Date created, Experiment status, Experiment Description, and Experiment Type.

Experiment	Overall Segment Strength	Segment Name	Date created	Experiment status	Experiment Description	Experiment Type
EXPERIMENT_ID_1	28.2 % ± .2	AMEA_HR	09/07/2025 08:07	Complete	Initial Configuration	TPOLOGY
EXPERIMENT_ID_2	28.2 % ± .2	AMEA_HR	09/07/2025 08:07	Complete	Initial Configuration	Initial Configuration
EXPERIMENT_ID_3	25.91 % ± .21	AMEA_MR	09/08/2025 07:56	Complete	Initial Configuration	TPOLOGY
EXPERIMENT_ID_4	25.91 % ± .21	AMEA_MR	09/08/2025 07:56	Complete	Initial Configuration	Initial Configuration
EXPERIMENT_ID_5	25.91 % ± .21	AMEA_MR	09/11/2025 07:09	Complete	Only HT is taking the offerings up.	TPOLOGY
EXPERIMENT_ID_6	27.42 % ± .22	AMEA_MR	09/12/2025 07:28	Complete	Baseline for Assess Risk New Offering Account Type	Baseline for Assess Risk New Offering Account Type

3. Click **Compare Experiment**. The following window is displayed.

Figure 5-32 Compare Experiment

Compare experiments

Select 2 experiments in the same segment

Experiment 1

Required

Experiment 2

Required

Cancel Compare

4. Select the experiment which has a newly added offering as a Transaction Product that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select another experiment that has a newly added offering as the Transaction Product with different set of constraints that you want to compare with Experiment 1 from the Experiment 2 drop-down list.

 Note:

You can compare the experiments in the same segments only. You can add up to 5 account types in an Experiment.

6. Click **Compare** to compare the selected experiments. The compared result is displayed.

Results from the two selected experiments and the currently accepted experiment for the segment are displayed as shown in the below figure. Any differences between the agents used, and the thresholds evaluated are also displayed.

Figure 5-33 Experiment Result

Compare Experiments			
	EXPERIMENT_00_8 Accepted	EXPERIMENT_00_16 Custom Offering ZELLE: 4th Test Experiment Results	EXPERIMENT_00_17 Custom Offering ZELLE Experiment Results
Segment strength score	50.83% ± 3.54%	4.48% ± 2.2%	40.25% ± 3.36%
Risk level	Low	Low	Low
Alert volume		120.19	1.72
Agent	DEVIC005_00 Custom Agent 1	DEVIC005_00 Custom Agent 1	DEVIC005_00 Custom Agent 1
Experiment description	DEVIC005_00 experiment	DEVIC005_00 Control Set 16	Testing 001 experiment TS area
Impact of adding new offering		7.40.33	7.10.33
Actions		Accept Results	Accept Results

You can compare the results between the experiments to determine the incremental risk resulting from using different sets of controls to monitor the new account type. If the system strength has dropped relative to the accepted experiment, this indicates that the new account type is not monitored as effectively as existing accounts. This is acceptable if an institution knows the account is being offered to low risk customers.

If the system strength has not changed or increased relative to the accepted experiment, this indicates that the new account type is being more effectively monitored than existing account types. For accounts that are being offered to higher risk customers, institutions should look to devise controls that result in an increase in system strength.

7. Click **Accept Results** to accept the experiment for the particular segment.

6

Modifying the System

If you have recently added add-ons to your product portfolio, you may need to adjust your system accordingly. This section provides a step-by-step guide to integrating new account types and Transaction Products into your existing system.

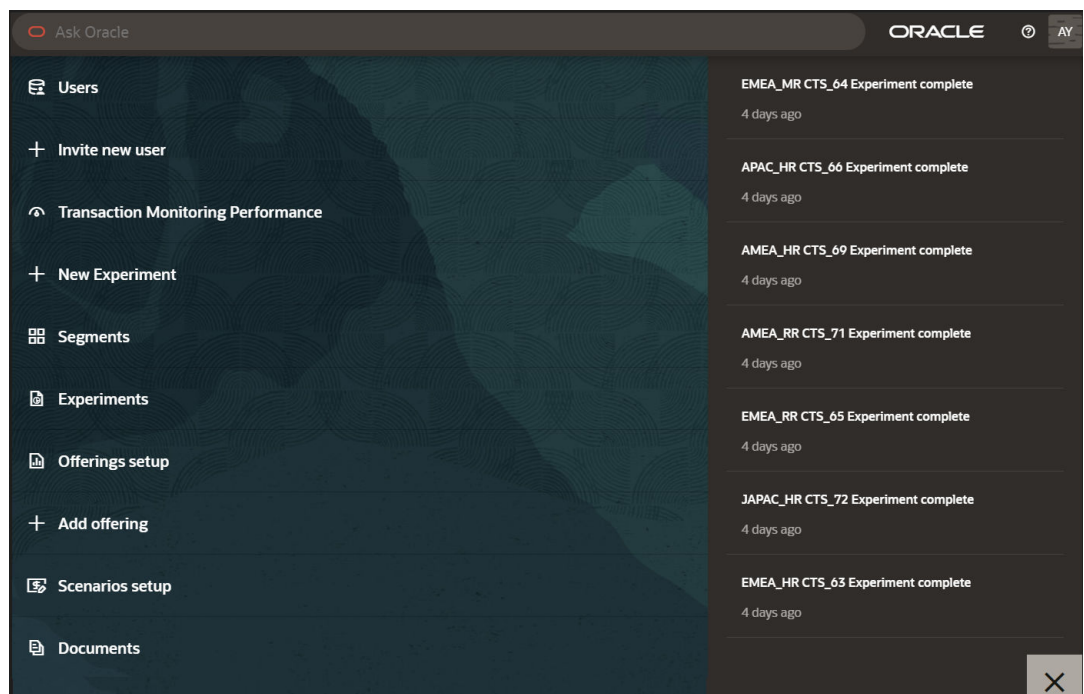
Topics:

- [Adding an Account](#)
- [Adding a Transaction Product](#)

To view the Offerings Setup, follow these steps:

1. Click  Open Ask Oracle to display the Ask Oracle window. The Application page is displayed.

Figure 6-1 Ask Oracle Menu



2. Click **Offerings** setup menu to display the Offerings Setup window. The Offering Setup window is displayed.

Figure 6-2 Offerings Setup

Offerings Setup Add Offering

Search...

AMEA 12 | OFSCA_TEST_SUITE_1_RR 12 | RBR 45 | CASH 35

Jurisdiction code	Segment	Account	Channel	Withdrawal Limit(per day)
AMEA	AMEA_HR	CBK	CASH	10000
OFSCA_TEST_SUITE_1	OFSCA_TEST_SUITE_1_RR	RBR	MI	10000
AMEA	AMEA_HR	RBK	CASH	2500
AMEA	AMEA_HR	RBR	MI	3000
AMEA	AMEA_MR	CBK	MI	3500
AMEA	AMEA_MR	RBK	WI	2000
AMEA	AMEA_MR	RBR	CASH	2600
AMEA	AMEA_RR	RBK	MI	4500
AMEA	AMEA_RR	RBR	MI	5000
JAPAC	JAPAC_HR	CBK	WI	4500
JAPAC	JAPAC_HR	RBK	WI	1200
JAPAC	JAPAC_HR	RBR	CASH	3500

Offerings setup Scenarios setup Documents

You can view the list of offerings currently configured in OFSCA and also you can perform the following:

- Click **Add Offering** to create a new account or Transaction Product in the system. You can also add offerings directly from Application menu by clicking Add Offering.
 - To add an account, see the [Adding an Account](#) section.
 - To add a channel, see the [Adding a Transaction Product](#) section.

You can search for the required details in the Search field. The available options are Jurisdiction, Segment, Account, and Channel.

Adding an Account

Use this section to add a new or an existing account to the segment.

To add an account to the segment, follow these steps:

- On the Ask Oracle menu or Offering Setup page, click **Add Offering**. The Add Offering window is displayed

Figure 6-3 Add Offering for Account

Add Offering

Offering Type

☐ Account

☐ Transaction product

Offering Account

New or existing?

☐ Add new account to segment(s)

☒ Add existing account to additional segment(s)

Account name

Associate jurisdiction codes, segments, and channels

Jurisdiction code	Segment	Channel

1 rows selected Total 1

Add Another

Account-Transaction product constraints (per day)

Cancel Add Offering

2. Select **Account** from the Offering Type option.
3. To add a new account to the segment, select **Add** new account to segment(s). Enter the name of the new account in the Account Name field
4. To add an existing account to a segment, select Add existing account to additional segment(s). Select the existing account name from the drop-down list in the Account Name field.

Note:

You can add up to four accounts to a segment.

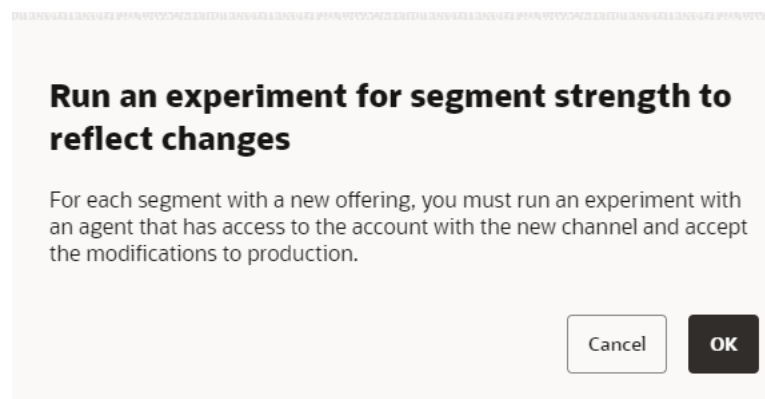
5. In the Associate jurisdiction codes, segments, and channels group, double-click on the **Jurisdiction** code and select the required jurisdiction code from the drop-down list. The account will only be available in these selected jurisdictions.
6. Click on the **Segment** and select the required segment from the drop-down list. The account will be available only to agents belonging to selected segments.

 Note:

The drop-down list displays the result based on the selected jurisdiction code.

7. Click on the **Channel** and select this icon to display the Search field. Search the required channel in the field. Only selected channels can be used to transfer funds in and out of this account type.
8. Click **Add Another** to add this account to a different jurisdiction codes, segments, and channels to the account.
9. Click **Add Offering**. A dialog box appears:

Figure 6-4 Confirmation Dialog Box



10. Click **OK** to add an account in the particular segment. The newly added account will be available to new agents in the chosen segment. A new agent will be automatically created for this segment and It will have access to new offering.
11. A new experiment must be run to get an updated segment strength score with the newly added "account type". To run the experiment, the newly created agent must be chosen. You can also modify the Account-Channel constraints associated with this account or configure a scenario to monitor this new account before you run the experiment. For more information, see [Copying or Modifying the Control Set](#)

Adding a Transaction Product

Use this section to add a new or an existing Transaction Product to the segment.

To add a Transaction Product, follow these steps:

1. On the Ask Oracle menu or Offering Setup page, click Add Offering to create a new channel. The Add Offering window is displayed

Figure 6-5 Add Offering for Transaction Product

The screenshot shows the 'Add Offering' dialog box with the following sections:

- Offering Type:** Radio buttons for 'Account' and 'Transaction product' (selected).
- Offering Transaction product:** Radio buttons for 'Add new transaction product to segment(s)' and 'Add existing transaction product to additional segment(s)' (selected).
- Transaction product name:** A dropdown menu.
- Associate jurisdiction codes, segments, and accounts:** A table with columns 'Jurisdiction code', 'Segment', and 'Account'. It shows 1 row selected and a total of 1.
- Buttons:** 'Add Another', 'Cancel', and 'Add Offering'.

Jurisdiction code	Segment	Account

1 rows selected Total 1

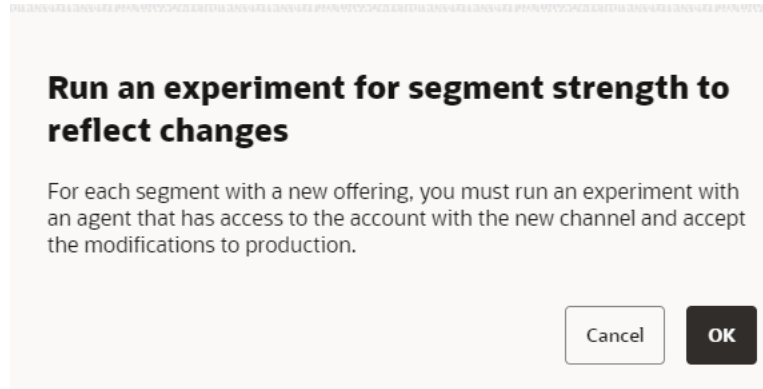
2. Select **Channel** from the Offering Type option.
3. To add a new Transaction Product to the segment, select **Add** new Transaction Product to segment(s). Enter the name of the new Transaction Product in the Transaction Product Name field.
4. To add an existing Transaction Product to a segment, select **Add existing Transaction Product** to additional segment(s). Select the existing Transaction Product name from the drop-down list in the Transaction Product Name field.
5. In the Associate jurisdiction codes, segments, and accounts group, double-click on the **Jurisdiction code** and select the required jurisdiction code from the drop-down list. The new Transaction Product will be available in the selected jurisdictions.
6. Click on the **Segment** and select the required segment from the drop-down list. The new Transaction Product will only be available to agents belonging to the selected segments

 Note:

The drop-down list displays the result based on the selected jurisdiction code.

7. Click on the Account and select this  icon to display the Search field. Search the required account in the field. The new channel can be used to transfer funds only from the selected account types.
8. Click **Add Another** to add this transaction product to a different jurisdiction codes, segments, and accounts to the channel.
9. Click **Add Offering**. A new Transaction Product is added to the segment.

Figure 6-6 Confirmation Dialog Box



10. Click **OK** to add a Transaction Product in the particular segment.
11. A new experiment must be run to get an updated segment strength score with the newly added "Transaction Product".

7

Navigating the OFSCA UI

This section describes how to navigate the key components of the OFSCA application.

Topics:

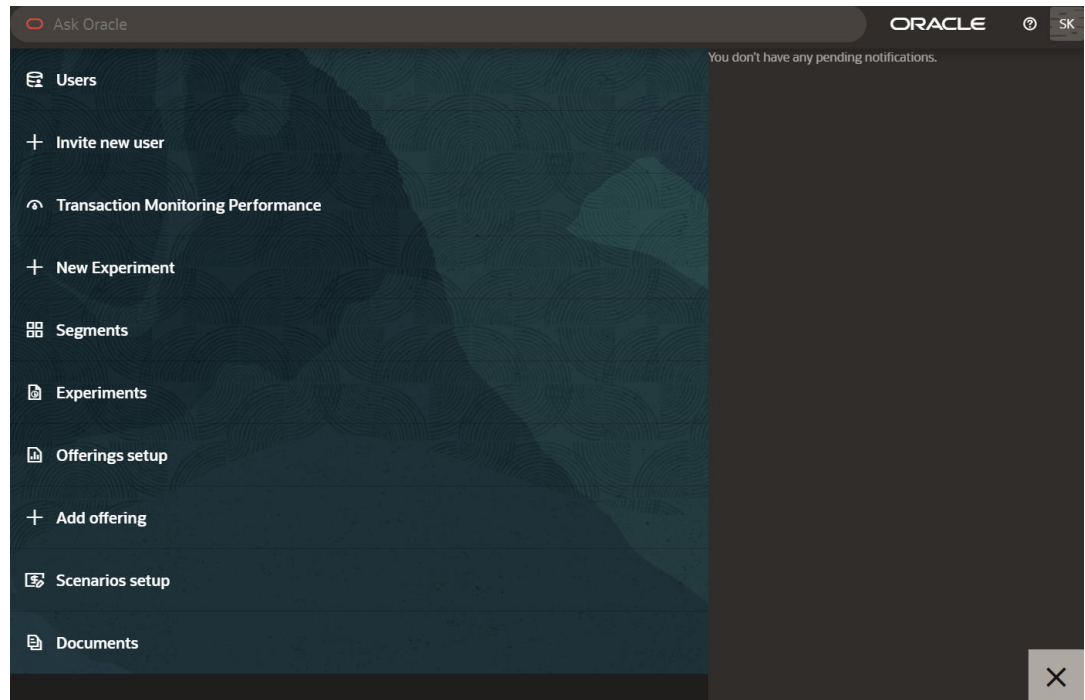
- [Creating a New User](#)
- [Managing Transaction Monitoring Performance](#)
- [Creating a New Experiment](#)
- [Managing Segments](#)
- [Managing Experiments](#)
- [Managing Offerings Setup](#)
- [Viewing Scenario Setup](#)
- [Using Documents](#)

Managing Users

To view the list of users in the application, follow these steps:

1. Click **Open Ask Oracle**  to display the Ask Oracle window. The following window is displayed.

Figure 7-1 Application Menu



2. Click **Users** menu to display the Users window. For more information, see the [User Roles and Privileges](#) section.

Creating a New User

To create a new user, follow these steps:

1. Click **Open Ask Oracle**  to display the Ask Oracle window.
2. Click **Invite User** menu to create a new user. For more information, see the [Invite User section](#).

Note:

Only Admin users can create a new user.

Managing Transaction Monitoring Performance

To view the transaction monitoring performance dashboard, follow these steps:

1. Click **Open Ask Oracle**  to display the Ask Oracle window.
2. Click **Transaction Monitoring Performance** menu to display the Configure your Transaction Monitoring System window. For more information, see the [Configuring the Transaction Monitoring System](#) section.



Note:

Once the system is configured, you can see the [Configuring the Transaction Monitoring System](#) dashboard instead of Configuring your Transaction Monitoring System window

Creating a New Experiment

To create a new experiment, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **New Experiment** menu to display the New Experiment window. For more information, see the [New Experiment](#) section.

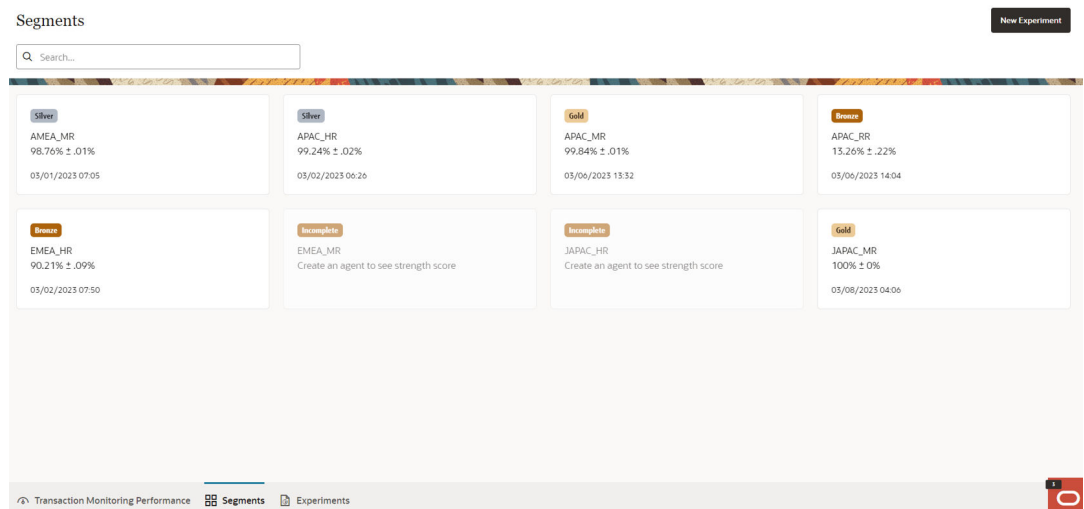
Managing Segments

To get an overview of the performance of all segments at your institution, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **Segments** menu to display the Segments window. The following window is displayed.

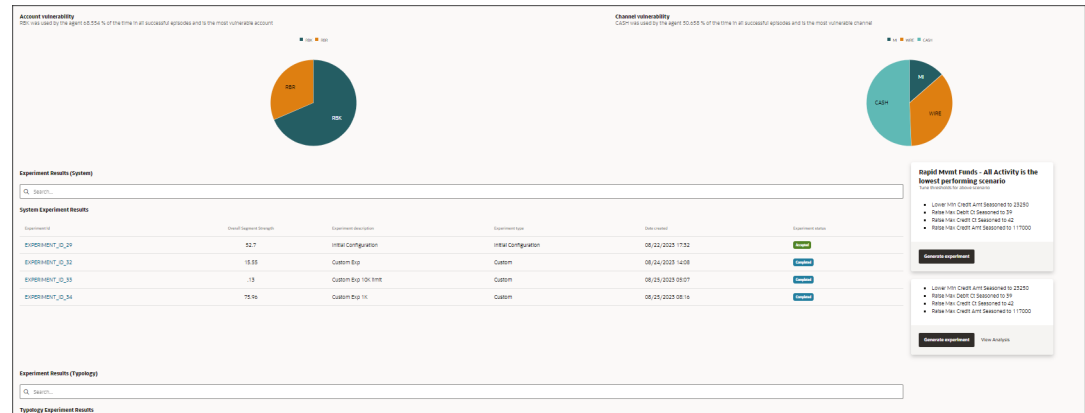
Figure 7-2 Segments



3. Click on the Search bar and select the required filter options from the drop-down list. The available filter options are Segment, Segment strength score, and Date created.
Or Click on the required filter button below the Search bar and select the required filter options from the drop-down list.

- Click on the individual segment <APAC_MR>. It will navigate to the segment's dashboard as follows:

Figure 7-3 Segment Dashboard



For more information about the segment dashboard, see the [Generating Experiment from Recommendation](#) section.

Managing Experiments

To view the experiments, follow these steps:

- Click  **Open Ask Oracle** to display the Ask Oracle window.
- Click **Experiments** menu to display the Experiments window. The following window is displayed.

Figure 7-4 Experiments

Experiments						
Experiment Results (System)						
Experiment	Overall Segment Strength	Experiment description	Experiment type	Date created	Experiment status	Experiment description
EXPERIMENT_01_01	12.7	Initial Configuration	Initial Configuration	08/24/2023 17:52	Active	Initial Configuration
EXPERIMENT_01_02	15.85	Custom Exp	Custom	08/24/2023 14:08	Active	Custom Exp
EXPERIMENT_01_03	19	Custom Exp 10k time	Custom	08/24/2023 09:07	Active	Custom Exp 10k time
EXPERIMENT_01_04	75.94	Custom Exp 1M	Custom	08/25/2023 08:16	Active	Custom Exp 1M
EXPERIMENT_01_05	9.2	OPSCA TEST_BULK_LDR	Custom	11/29/2023 04:28	Active	Custom Experiment from Bulk without CDB
EXPERIMENT_01_06	5.4	OPSCA TEST_BULK_LDR	Custom	11/29/2023 07:14	Active	Custom Exp from Bulk_LDR on monitored
EXPERIMENT_01_07	19.02	OPSCA TEST_BULK_LDR	Custom	11/29/2023 09:40	Active	300k LPT
EXPERIMENT_01_08	4.67	OPSCA TEST_BULK_LDR	Custom	11/29/2023 11:24	Active	25k on monitored
EXPERIMENT_01_09	100	OPSCA TEST_BULK_LDR	Custom	12/01/2023 04:09	Active	Exp with only 8 scenarios
EXPERIMENT_01_10	9.2	OPSCA TEST_BULK_LDR	Custom	12/01/2023 11:54	Active	300k LPT 3 scenarios with 25k on monitored
EXPERIMENT_01_11	4.9	OPSCA TEST_BULK_LDR	Custom	01/10/2024 10:40	Active	3 scenarios 25k on monitored
Experiment Results (Typology)						
Experiment	Overall Segment Strength	Experiment description	Experiment type	Date created	Experiment status	Experiment description
EXPERIMENT_01_01	14.4	APAC_MR	Typology	10/12/2023 09:54	Active	HT agent
EXPERIMENT_01_02	9.2	APAC_MR	Typology	11/28/2023 11:01	Active	HT agent
EXPERIMENT_01_03	34.9	OPSCA TEST_BULK_LDR	Typology	12/01/2023 10:12	Active	HT agent BulkTest
EXPERIMENT_01_04	33.2	OPSCA TEST_BULK_LDR	Typology	12/01/2023 14:26	Active	HT agent - Changing threshold with

The following table describes fields and buttons in the experiments window.

Table 7-1 Experiment

Fields	Description
New Experiment	Click New Experiment to generate a new experiment for the segment. To create a new experiment, see the User Defined Experiment section.
Compare Experiment	Click Compare Experiment to compare the two selected experiment in the same segment. For more information, see the Comparing an Experiment section.
Search	The field to search for Experiment. Enter a specific segment name for which you want to search, and press Enter on the keyboard to display the results. The search is available for all the fields.
Experiment	Experiment name of the created segment.
Overall Segment Strength	Displays the segment strength.
Segment Name	Displays the segment strength.
Segment Name	Name of the segment.
Date Created	The date on which the Experiment is created.
Experiment Status	Displays the status of the Experiment. The statuses are: • In progress: The experiment is in running state. • Completed: The running experiment is completed. • Accepted: Currently, the user has accepted experiment and the controls evaluated in this experiment are in production. • Inactive: Initially, it was accepted by the user. To improve segment strength, the user conducted another new experiment for the segment, which has been accepted. So, the previous experiment status of the segment will be changed to inactive. • Error: It is due to a convergence problem. To resolve this issue, contact the support team.
Experiment Description	The description of the Experiment.
Experiment Type	Displays the type of the Experiment. The types are: • Initial setup: The experiment is generated through the initial configuration of the system. • Custom: New experiment is generated through the experiment workflow. • Recommendation: The experiment is generated through recommendation method.

Managing Offerings Setup

To create an account/channel in the system, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **Offerings** setup menu to display the Offerings Setup window. For more information, see the [Modifying the System](#) section.

Viewing Scenario Setup

To view the scenario setup for the system, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **Scenarios** setup menu to display the Scenario Setup window. The following window is displayed.

Figure 7-5 Scenario Setup

Scenario Setup

Search...

(ML/CU) Large Reportable Transactions 835 | OFSCA_TEST_SUITE_4 392 | THRESHOLD_SET_0 1,111 | Look_Back_Period 233

Scenario name	Jurisdiction code	Segment	Threshold set ID	Parameter name	Value
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_1	Min_HRG_Pctg_Amt_HR	50
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_1	Min_HRG_Pctg_Incr_HR	500
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_2	Look_Back_Period	12
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_2	Mantas_Bus_Acct_Types_Lst	RBK,RBR,CBK
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_2	Min_HRG_Amt_HR	60000
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_2	Min_HRG_Pctg_Amt_HR	50
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_HR	THRESHOLD_SET_2	Min_HRG_Pctg_Incr_HR	200
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_MR	THRESHOLD_SET_1	Min_HRG_Pctg_Incr_MR	100
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_MR	THRESHOLD_SET_1	Look_Back_Period	12
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_MR	THRESHOLD_SET_1	Mantas_Bus_Acct_Types_Lst	RBK,RBR,CBK
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_MR	THRESHOLD_SET_1	Min_HRG_Amt_MR	60000
(ML/AC) CIB: High Risk Geography Activity	AMEA	AMEA_MR	THRESHOLD_SET_1	Min_HRG_Pctg_Amt_MR	50

Offerings setup Scenarios setup Documents

You can view the list of scenarios that are associated with the Jurisdiction code, Segment, Threshold set ID, Parameter name, and Value.

Using Documents

To reset the system and initial configuration, follow these steps:



1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **Documents** menu to display the Documents window.
3. Click **Download**  icon to download the files you have uploaded.

8

Understanding the OFSCA Metrics

This section describes information about the OFSCA metrics.

Topic:

- [Segment Strength Score](#)
- [System Strength Score](#)
- [Segment Performance](#)
- [Scenario Performance](#)
- [Account Vulnerability](#)
- [Channel Vulnerability](#)

Segment Strength Score

OFSCA's segment strength score is a metric that measures the transaction monitoring controls' effectiveness in monitoring a customer segment. The score is determined based on the following steps. This metric is calculated by the following:

1. The '% transferred' is estimated, which reflects the percentage of the target amount that an agent can transfer from the source account to the target account before the first alert is triggered.
2. The final metric value is calculated as $100 - \text{'% transferred'}$.

The metric is computed over multiple episodes sampled from the trained agent. 95% confidence intervals for this metric are also computed from these episodes. The closer the value is to 100%, the better the transaction monitoring system performs for a given customer segment, as the agent's ability to transfer a high% of the target amount is limited. Conversely, a value closer to 0 indicates the system is not performing optimally for this segment, as the agent can transfer a high% of the target amount before the first alert is triggered.

Limitations

This metric is reliable only if the experiment is a success (that is, the agent has been trained successfully), signifying the agent's successful training. However, this metric should not ascertain any decisive conclusions if the agent fails to converge. In such cases, OFSCA generates an error message indicating the unsuccessful experiment.

System Strength Score

The system strength score gives a consolidated view of the performance of the entire transaction monitoring system. This metric is computed by taking a simple average of the segment strength scores of all of the institution's customer segments. The variance for each segment strength score is also aggregated to produce a confidence interval for this metric.

Limitations

As this metric is an average, it might obscure the poor performance of one or more segments. Even if the system strength score is high, monitoring the individual segment strength scores is important.

Segment Performance

The Segment Performance metric captures the efficacy of the System in detecting various Typologies, for example, Human Trafficking. A high value of the performance metric indicates that the scenarios deployed to combat Typologies (Human Trafficking) offer significant resistance to the agent by alerting it as it attempts to move money through your institution. OFSCA calculates the segment performance for Red Flag Coverage by the following:

- Simulating patterns depicting Human Trafficking cases.
- Estimating the percentage of episodes where the HT Agent scenarios alerted.

If the scenarios did not alert in the majority of the simulated episodes, it means that the System is unable to resist the agent and has low efficacy. A value close to 100 means the System offers high Coverage in detecting the Human Trafficking pattern.

A value close to 0 means the System has very low efficacy. Tuning the existing HT Agent scenarios or deploying more can improve the performance of the TMS for the segment in question.

Scenario Performance

Enter a short description hereThe scenario performance metric captures which scenarios offer the most resistance to an intelligent adversarial agent. A high value of the performance metric indicates that the scenario offers significant resistance to the agent by alerting on it as it attempted to move money through your institution.

OFSCA calculates the performance of a scenario by the following:

1. Sampling episodes from the trained agent's policy.
2. Estimating the percentage of episodes where the scenario alerted.

If a scenario did not alert in the majority of the simulated episodes, it means that the scenario is unable to resist the agent and has low efficacy.

A value close to 100 means this scenario has high efficacy and offers very high resistance to the agent. A value close to 0 means the scenario has very low efficacy.

Tuning a low performing scenario can lead to an improvement in the performance of the TMS for the segment in question. 95% confidence intervals are also computed for this metric.

Account Vulnerability

The account vulnerability metric captures which account types are most liable to being abused by an intelligent agent to move money through your financial system. A high value for this metric indicates that this account type was the agent's preferred account when moving money through your Institution.

OFSCA calculates the vulnerability of an account by the following:

1. Sampling episodes from the trained agent's policy.

2. Estimating the funds that flowed through each account type. For example, if \$100 was credited into an account and debited from the account, the funds that flowed through that account were \$100. If only \$50 was debited, only \$50 flowed through that account.
3. Normalizing this across all account types.

An account type with a high value for this metric is preferred by the agent over an account type with a lower value of this metric. Enhancing controls that monitor a vulnerable account type can improve the performance of the TMS for the segment in question.

Limitations

1. Currently, any funds that flow through an account are attributed to that account even if those funds did not reach the destination account. This could lead to the vulnerability of an account type being inflated in a given episode. However, since the metric is computed by averaging across multiple episodes, this should not have a bearing on the final metric.
2. If two or more account types (e.g., BRK and RBK) are highly vulnerable, then the agent will break ties randomly and will assign a high vulnerability score to one of these account types while assigning a lower vulnerability score to others. If the overall segment score does not improve significantly even after remediating the account type with the highest vulnerability score (e.g., BRK), this could be because other account types continue to be vulnerable. Once an experiment to address the most vulnerable account type (BRK) has been run and accepted, the segment dashboard will update to now indicate that the second account type (RBK) is most vulnerable. You might have to run an experiment to address monitoring gaps for this second account type (RBK) before overall segment score improves.

Channel Vulnerability

The channel vulnerability metric captures which channels are most liable to being abused by an intelligent agent to move money through your financial system. A high value for this metric indicates that this channel was the agent's preferred instrument for transferring money through your institution.

OFSCA calculates the vulnerability of the channel by the following:

1. Sampling episodes from the trained agent's policy.
2. Estimating the funds that were transacted using each channel. For example, if A transferred \$100 to B using wires and B transferred \$50 to C using MI. Funds attributed to wire = 100 and funds attributed to MI = \$50.
3. Normalize this across all channel types.

A channel with a high value for this metric is preferred by the agent over a channel with a lower value for this metric. Enhancing controls that monitor a vulnerable channel can improve the performance of the TMS for the segment in question.

Limitations

1. Currently, any funds that are transferred using a channel are attributed to that channel for computing the vulnerability metric, even if those funds did not reach the destination account. This could lead to the vulnerability of a channel type being inflated in a given episode. However, since the metric is computed by averaging across multiple episodes, this should not have a bearing on the final metric.
2. If two or more channels (e.g., Wire and MI) are highly vulnerable, then the agent will break ties randomly and will assign a high vulnerability score to one of these channels while assigning a lower vulnerability score to others. If the overall segment score does not improve significantly even after remediating the channel with the highest vulnerability score

(e.g., Wire), this could be because other channels continue to be vulnerable. Once an experiment to address the most vulnerable channel has been run and accepted, the segment dashboard will update to now indicate that the second channel (MI) is most vulnerable. You might have to run an experiment to address monitoring gaps for this second channel (MI) before overall segment score improves.

Appendix

Topics:

- [How to Calculate the Target Amount](#)
- [How to Calculate the CIB Parameter for Historical Activity](#)
- [Methodology](#)
- [Simulating Aggregates](#)
- [Recommending Thresholds](#)
- [Risks and Limitations](#)

How to Calculate the Target Amount

The following query is a suggested way of arriving at these target amounts:

```
select t.JRSDCN_CD,(t.AVG_AMT + 2*t.SD) as min_amt,(t.AVG_AMT + 5* t.SD) as max_amt
from /*Consider mean of deposit and withdrawal amounts rather than just one or the other. */
(select JRSDCN_CD, AVG((TOT_DEPST_AM+TOT_WDRWL_AMT)/2) as avg_amt,
STDDEV((TOT_DEPST_AM+TOT_WDRWL_AMT)/2) as sd from CUST a inner join
CUST_SMRY_MNTH b on a.CUST_INTRL_ID = b.CUST_INTRL_ID /*Choose an appropriate
time frame */ where MNTH_SMRY_START_DT between '01-MAY-15' and '01-SEP-15' /* This
assumes JURSDCN_CD = Segment. if not adjust appropriately */ group by JRSDCN_CD) t;
```

Sample Template

This appendix provides sample templates.



Note:

If the JSON is not properly formatted, it will result in an error within the application. To avoid this issue, you must download the template from the user interface (UI) for each upload. The provided examples must only be used as a reference.

Template for each risk category (RR, MR, HR)

Sample Template-1

```
{
  "scenario_name":
  "custom_rmf_4", "jurisdiction_thresholds":
  { "BCAP": {
    "RR_Min_Credit_Amt":0.01,
    "RR_Max_Credit_Amt":100000000, "RR_Min_Credit_Ct":1,
    "RR_Max_Credit_Ct":100000, "RR_Min_Debit_Ct":1,
```

```

        "RR_Max_Debit_Ct":100000, "RR_Min_Perc": 0.8,
        "lookback_period": 14,
        "rule_run_frequency": 7,
        "accts_monitored": "RBK, RBR"
    }
}

```

Sample Template-2

```

{
    "scenario_name":
    "custom_rmf_5", "jurisdiction_thresholds":
    { "BCAP": {
        "MR_Min_Credit_Amt":0.01,
        "MR_Max_Credit_Amt":100000000, "MR_Min_Credit_Ct":1,
        "MR_Max_Credit_Ct":100000, "MR_Min_Debit_Ct":1,
        "MR_Max_Debit_Ct":100000, "MR_Min_Perc": 0.8,
        "lookback_period": 14,
        "rule_run_frequency": 7,
        "accts_monitored": "RBK, RBR"
    }
}

```

Sample Template-3

```

{
    "scenario_name":
    "custom_rmf_6", "jurisdiction_thresholds":
    { "BCAP": {
        "HR_Min_Credit_Amt":0.01,
        "HR_Max_Credit_Amt":100000000, "HR_Min_Credit_Ct":1,
        "HR_Max_Credit_Ct":100000, "HR_Min_Debit_Ct":1,
        "HR_Max_Debit_Ct":100000, "HR_Min_Perc": 0.8,
        "lookback_period": 14,
        "rule_run_frequency": 7,
        "accts_monitored": "RBK, RBR"
    }
}

```

How to Calculate the CIB Parameter for Historical Activity

The following query is a suggested way for calculating CIB parameters from the data:

```

select
    c.JRSDCN_CD,
    AVG(t.AVG_CREDIT_AMT) as AVG_CREDIT_AMT,
    AVG(t.AVG_DEBIT_AMT) as AVG_DEBIT_AMT,
    AVG(t.SD_CREDIT) as SD_CREDIT,

```

```

    AVG(t.SD_DEBIT) as SD_DEBIT,
    AVG(t.MAX_CREDIT_AMT) as MAX_CREDIT_AMT,
    AVG(t.MAX_DEBIT_AMT) as MAX_DEBIT_AMT,
    AVG(t.AVG_FRGN_IN_AMT) as AVG_FRGN_MONTHLY_CDT,
    AVG(t.AVG_FRGN_OUT_AMT) as AVG_FRGN_MONTHLY_DBT,
    AVG(HIST_DAILY_AVG_AMT) as HIST_DAILY_AVG_AMT
from
acct a INNER JOIN cust_acct ca
  on a.ACCT_INTRL_ID = ca.ACCT_INTRL_ID
INNER JOIN cust c on
  ca.CUST_INTRL_ID = c.CUST_INTRL_ID
INNER JOIN (select
    asm.ACCT_INTRL_ID,
    AVG(asm.TOT_DEPST_AM) as AVG_CREDIT_AMT,
    AVG(asm.TOT_WDRWL_AM) as AVG_DEBIT_AMT,
    STDDEV(asm.TOT_DEPST_AM) as SD_CREDIT,
    STDDEV(asm.TOT_WDRWL_AM) as SD_DEBIT,
    MAX(asm.TOT_DEPST_AM) as MAX_CREDIT_AMT,
    MAX(asm.TOT_WDRWL_AM) as MAX_DEBIT_AMT,
    AVG(NVL(asm.FRGN_WIRE_TRXN_IN_AM,0) +
NVL(asm.FRGN_CHK_TRXN_IN_AM,0) + NVL(asm.FRGN_CHK_TRXN_IN_FUNC_AM,0) +
NVL(asm.FRGN_WIRE_TRXN_IN_FUNC_AM,0)) as AVG_FRGN_IN_AMT,
    AVG(NVL(asm.FRGN_WIRE_TRXN_OUT_AM,0) +
NVL(asm.FRGN_CHK_TRXN_OUT_AM,0) + NVL(asm.FRGN_CHK_TRXN_OUT_FUNC_AM,0) +
NVL(asm.FRGN_WIRE_TRXN_OUT_FUNC_AM,0)) as AVG_FRGN_OUT_AMT,
    case when sum(case when aasd.ATM_TRXN_OUT_AM > 0 then 1 else 0
end) > 0 then sum(aasd.ATM_TRXN_OUT_AM) / sum(case when aasd.ATM_TRXN_OUT_AM
> 0 then 1 else 0 end)
    else 0 end as HIST_DAILY_AVG_AMT
  from
    acct_smry_mnth asm
  inner join ACCT_ATM_SMRY_DAILY aasd
    on asm.acct_intrl_id = AASD.acct_intrl_id
  where asm.MNTH_SMRY_START_DT >= add_months(trunc(sysdate,
'month'), -12) -- Recent 12 months data
    and asm.MNTH_SMRY_START_DT < trunc(sysdate,'month')
  GROUP BY asm.ACCT_INTRL_ID) t on
  a.ACCT_INTRL_ID = t.ACCT_INTRL_ID GROUP BY c.JRSDCN_CD;

```

Aggregates List

The section provides the list of aggregates available for RL and HT.

The following table provides the list of aggregates available for RL and HT.

Table 9-1 List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_CASH_DEBIT_AMT	Total Cash Debit Amount for HT Transactions	HT
TOT_CASH_CREDIT_AMT	Total Cash Credit Amount for HT Transactions	HT
TOT_CASH_DEBIT_CT	Total Cash Debit Count for HT Transactions	HT
TOT_CASH_CREDIT_CT	Total Cash Credit Count for HT Transactions	HT
TOT_WIRE_DEBIT_AMT	Total Wire Debit Amount for HT Transactions	HT
TOT_WIRE_CREDIT_CT	Total Wire Credit Count for HT Transactions	HT
TOT_CRYPTO_DEBIT_AMT	Total Crypto Debit Amount for HT Transactions	HT
TOT_CRYPTO_CREDIT_CT	Total Crypto Credit Count for HT Transactions	HT
TOT_CASH_DEBIT_AMT_DAY	Total Cash Debit Amount for HT Transactions during the daytime	HT
TOT_CASH_CREDIT_AMT_DAY	Total Cash Credit Amount for HT Transactions during the daytime	HT
TOT_CASH_DEBIT_CT_DAY	Total Cash Debit Count for HT Transactions during the daytime	HT
TOT_CASH_CREDIT_CT_DAY	Total Cash Credit Count for HT Transactions during the daytime	HT
TOT_CASH_DEBIT_AMT_NIGHT	Total Cash Debit Amount for HT Transactions during the nighttime	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_CASH_CREDIT_AMT_NIGHT	Total Cash Credit Amount for HT Transactions during the nighttime	HT
TOT_CASH_DEBIT_CT_NIGHT	Total Cash Debit Count for HT Transactions during the nighttime	HT
TOT_CASH_CREDIT_CT_NIGHT	Total Cash Credit Count for HT Transactions during the nighttime	HT
TOT_WIRE_DEBIT_AMT_DAY	Total Wire Debit Amount for HT Transactions during the daytime	HT
TOT_WIRE_CREDIT_AMT_DAY	Total Wire Credit Amount for HT Transactions during the daytime	HT
TOT_WIRE_DEBIT_CT_DAY	Total Wire Debit Count for HT Transactions during the daytime	HT
TOT_WIRE_CREDIT_CT_DAY	Total Wire Credit Count for HT Transactions during the daytime	HT
TOT_WIRE_DEBIT_AMT_NIGHT	Total Wire Debit Amount for HT Transactions during the nighttime	HT
TOT_WIRE_CREDIT_AMT_NIGHT	Total Wire Credit Amount for HT Transactions during the nighttime	HT
TOT_WIRE_DEBIT_CT_NIGHT	Total Wire Debit Count for HT Transactions during the nighttime	HT
TOT_WIRE_CREDIT_CT_NIGHT	Total Wire Credit Count for HT Transactions during the nighttime	HT
TOT_CRYPTO_DEBIT_AMT_DAY	Total Crypto Debit Amount for HT Transactions during the daytime	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_CRYPTOCREDIT_AMT_DAY	Total Crypto Credit Amount for HT Transactions during the daytime	HT
TOT_CRYPTODEBIT_CT_DAY	Total Crypto Debit Count for HT Transactions during the daytime	HT
TOT_CRYPTOCREDIT_CT_DAY	Total Crypto Credit Count for HT Transactions during the daytime	HT
TOT_CRYPTODEBIT_AMT_NIGHT	Total Crypto Debit Amount for HT Transactions during the nighttime	HT
TOT_CRYPTOCREDIT_AMT_NIGHT	Total Crypto Credit Amount for HT Transactions during the nighttime	HT
TOT_CRYPTODEBIT_CT_NIGHT	Total Crypto Debit Count for HT Transactions during the nighttime	HT
TOT_CRYPTOCREDIT_CT_NIGHT	Total Crypto Credit Count for HT Transactions during the nighttime	HT
TOT_HOTELS_DEBIT_AMT	Total Hotels Debit Amount for HT Transactions	HT
TOT_HOTELS_CREDIT_AMT	Total Hotels Credit Amount for HT Transactions	HT
TOT_HOTELS_DEBIT_CT	Total Hotels Debit Count for HT Transactions	HT
TOT_HOTELS_CREDIT_CT	Total Hotels Credit Count for HT Transactions	HT
TOT_DATING_SERVICES_DEBIT_AMT	Total Dating Services Debit Amount for HT Transactions	HT
TOT_DATING_SERVICES_CREDIT_AMT	Total Dating Services Credit Amount for HT Transactions	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_DATING_SERVICES_DEBIT_CT	Total Dating Services Debit Count for HT Transactions	HT
TOT_DATING_SERVICES_CREDIT_CT	Total Dating Services Credit Count for HT Transactions	HT
TOT_DRUG_STORES_DEBIT_AMT	Total Drug Stores Debit Amount for HT Transactions	HT
TOT_DRUG_STORES_CREDIT_AMT	Total Drug Stores Credit Amount for HT Transactions	HT
TOT_DRUG_STORES_DEBIT_CT	Total Drug Stores Debit Count for HT Transactions	HT
TOT_DRUG_STORES_CREDIT_CT	Total Drug Stores Credit Count for HT Transactions	HT
TOT_TAXIS_DEBIT_AMT	Total Taxis Debit Amount for HT Transactions	HT
TOT_TAXIS_CREDIT_AMT	Total Taxis Credit Amount for HT Transactions	HT
TOT_TAXIS_DEBIT_CT	Total Taxis Debit Count for HT Transactions	HT
TOT_TAXIS_CREDIT_CT	Total Taxis Credit Count for HT Transactions	HT
TOT_BARS_DEBIT_AMT	Total Bars Debit Amount for HT Transactions	HT
TOT_BARS_CREDIT_AMT	Total Bars Credit Amount for HT Transactions	HT
TOT_BARS_DEBIT_CT	Total Bars Debit Count for HT Transactions	HT
TOT_BARS_CREDIT_CT	Total Bars Credit Count for HT Transactions	HT
TOT_RENTAL_CARS_DEBIT_AMT	Total Rental Cars Debit Amount for HT Transactions	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_RENTAL_CARS_CREDIT_AMT	Total Rental Cars Credit Amount for HT Transactions	HT
TOT_RENTAL_CARS_DEBIT_CT	Total Rental Cars Debit Count for HT Transactions	HT
TOT_RENTAL_CARS_CREDIT_CT	Total Rental Cars Credit Count for HT Transactions	HT
TOT_MOVIE_THEATERS_DEBIT_AMT	Total Movie Theaters Debit Amount for HT Transactions	HT
TOT_MOVIE_THEATERS_CREDIT_AMT	Total Movie Theaters Credit Amount for HT Transactions	HT
TOT_MOVIE_THEATERS_DEBIT_CT	Total Movie Theaters Debit Count for HT Transactions	HT
TOT_MOVIE_THEATERS_CREDIT_CT	Total Movie Theaters Credit Count for HT Transactions	HT
TOT_WOMEN_ACCESSORY_STORES_DEBIT_AMT	Total Women Accessory Stores Debit Amount for HT Transactions	HT
TOT_WOMEN_ACCESSORY_STORES_CREDIT_AMT	Total Women Accessory Stores Credit Amount for HT Transactions	HT
TOT_WOMEN_ACCESSORY_STORES_DEBIT_CT	Total Women Accessory Stores Debit Count for HT Transactions	HT
TOT_WOMEN_ACCESSORY_STORES_CREDIT_CT	Total Women Accessory Stores Credit Count for HT Transactions	HT
TOT_JEWELRY_DEBIT_AMT	Total Jewelry Stores Debit Amount for HT Transactions	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_JEWELRY_CREDIT_AMT	Total Jewelry Stores Credit Amount for HT Transactions	HT
TOT_JEWELRY_DEBIT_CT	Total Jewelry Stores Debit Count for HT Transactions	HT
TOT_JEWELRY_CREDIT_CT	Total Jewelry Stores Credit Count for HT Transactions	HT
TOT_WOMEN_WEAR_STORES_DEBIT_AMT	Total Women Wear Stores Debit Amount for HT Transactions	HT
TOT_WOMEN_WEAR_STORES_CREDIT_AMT	Total Women Wear Stores Credit Amount for HT Transactions	HT
TOT_WOMEN_WEAR_STORES_DEBIT_CT	Total Women Wear Stores Debit Count for HT Transactions	HT
TOT_WOMEN_WEAR_STORES_CREDIT_CT	Total Women Wear Stores Credit Count for HT Transactions	HT
TOT_OTHER_DEBIT_AMT	Total Other Debit Amount for HT Transactions	HT
TOT_OTHER_CREDIT_AMT	Total Other Credit Amount for HT Transactions	HT
TOT_OTHER_DEBIT_CT	Total Other Debit Count for HT Transactions	HT
TOT_OTHER_CREDIT_CT	Total Other Credit Count for HT Transactions	HT
TOT_WIRE_CREDIT_AMT	Total Wire Credit Amount for HT Transactions.	HT
TOT_WIRE_DEBIT_CT	Total Wire Debit Count for HT Transactions.	HT
TOT_CRYPTOCREDIT_AMT	Total Crypto Credit Amount for HT Transactions	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
TOT_CRYPTO_DEBIT_CT	Total Crypto Debit Count for HT Transactions	HT
tot_credit_amount	Total credit amount	RL
tot_debit_amount	Total debit amount	RL
tot_amount	Total credit amount + Total debit amount	RL
tot_credit_amount_with_mita(min_ind_val_tshld)	Total credit amount with minimum individual transaction value as a parameter. min_ind_val_tshld should be present in the thresholds field of JSON value. If min_ind_val_tshld is not provided, it will default to zero.	RL
tot_debit_amount_with_mita(min_ind_val_tshld)	Total credit amount with minimum individual transaction value as a parameter. min_ind_val_tshld should be present in the thresholds field of JSON value. If min_ind_val_tshld is not provided, it will default to zero.	RL
tot_credit_amount_cash	Total credit amount in cash	RL
tot_debit_count_cash_with_rita(min_ind_val_tshld=,max_ind_val_tshld=)	Total debit count with a range of minimum and maximum individual transaction amounts. For CASH channel only	RL

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
tot_credit_amount_with_rita(min_ind_val_tshld,max_ind_val_tshld)	Total credit amount with range between min_ind_val_tshld and max_ind_val_tshld. Both min_ind_val_tshld and max_ind_val_tshld should be present in thresholds field of JSON value.	RL
tot_credit_count	Total credit count	RL
tot_debit_count	Total debit count	RL
tot_credit_amount_cash_with_rita(min_ind_val_tshld=,max_ind_val_tshld=)	Total credit amount with a range of minimum and maximum individual transaction amounts. For CASH channel only	RL
tot_credit_count_cash_with_rita(min_ind_val_tshld=,max_ind_val_tshld=)	Total credit count with a range of minimum and maximum individual transaction amounts. For CASH channel only	RL
tot_debit_amount_cash_with_rita(min_ind_val_tshld=,max_ind_val_tshld=)	Total debit amount with a range of minimum and maximum individual transaction amounts. For CASH channel only	RL
tot_debit_amount_cash	Total debit amount in cash	RL

Methodology

OFS Compliance Agent can recommend thresholds for AML scenarios based on summary transaction statistics of a sample of focal entities (accounts/customers/external entities).

This involves the following two steps:

1. Using summary statistics from a sample of customers to simulate transaction aggregates that are representative of the aggregate transactional behavior of the entire population of customers.

2. Using these simulated transaction aggregates to recommend thresholds for specific scenarios and parameters.

Simulating Aggregates

One of the key considerations in designing this approach is to keep data requirements low.

A segment of customers at a mid-sized financial institution could have millions of customers. Although we can derive accurate threshold estimates if this entire dataset were available, this may impose prohibitive costs in terms of storage, compute and speed.

To get realistic estimates of transaction aggregates from a sample of customers, we implement the following algorithm.

1. Obtain monthly transaction aggregates from a sample of focal entities (1 % of customer segment or 25,000 whichever is bigger). If the scenario being tuned is customer focused, account focused or external entity focused, the aggregates should be at a customer level, account level or external entity level respectively. Only transaction aggregates relevant to the scenario being tuned are used.
2. Use an outlier detection technique (IQR or percentile based) to trim outliers that may skew estimates.
3. Linearly scale the aggregates to get the aggregates for the appropriate lookback.
4. Fit a generative model to this data.
5. Sample new observations from this model that approximately captures the real behavior of the segment.

Fitting and Sampling from a Generative Model

This section describes fitting and sampling from a generative model

A multi-variate normal distribution is used to model the transaction aggregates. This model was chosen for the following reasons.

To get realistic estimates of transaction aggregates from a sample of customers, we implement the following algorithm.

1. The model we choose has to be flexible enough to model the dependencies between various transaction aggregates. For example, Amounts and Counts tend to be correlated; similarly, Credits and Debits could be correlated. For this reason, a multi-variate model was chosen.
2. Assuming the customers in a segment behave homogeneously, we can assume their transactions are drawn from the same distribution. Given the transaction aggregates are just sum of these transactions, the transaction aggregates can be assumed to be approximately normal.

Even so, the marginal distributions of certain aggregates may not be normal. For this reason, the marginal are transformed using Box Cox transforms to ensure they are normal.

Once the model is fit, and samples are drawn from this model, an inverse box cox transformation is applied to reverse transform the samples to the original scale.

Recommending Thresholds

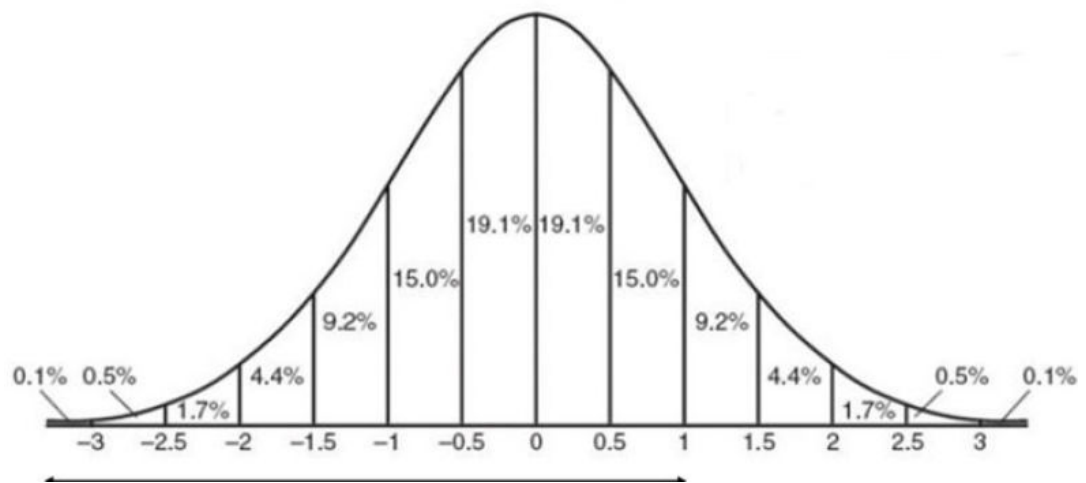
This section describes the recommended thresholds.

Once a population of transaction aggregates have been generated, we can recommend thresholds.

To recommend these thresholds, we rely on some industry standard heuristics.

1. **Calculate Percentiles:** After removing the outliers, the cleansed data is analyzed to determine the thresholds within each segment as defined by the scenario logic. Suspicious activity is usually associated with higher values and is therefore expected to be found within the right tail of the distribution. The values corresponding to the right tail are identified by computing the percentiles of the data values within the distribution. For this purpose, 85th percentile is recommended as the base percentile below which the data is assumed to be within acceptable limits and not suspicious. The choice of 85th percentile is based on the distribution statistics of a normal distribution, where 85% of the data lies within Mean + 1 standard deviation. The base percentile can be customized to suit the user's preferences.

Figure 9-1 Calculate Percentile



2. **Compute Jumps:** Jumps can be defined as relative differences (deviations) between two consecutive data points that are sorted in ascending order. A conservative method of setting thresholds is to select values just prior to significant increases in values observed in the data. This is because larger jumps indicate a departure in behavior from entities at lower percentiles, which warrants enhanced scrutiny. By utilizing jumps, recommended thresholds can be conservatively and dynamically established based on observed variations in the actual data distribution, rather than adopting a more static "one size fits all" approach (see *Option 3 (Using Percentiles)*). Jumps and corresponding peaks can be computed as follows for each scenario, segment (excluding risk levels), calibratable parameter:
 - For Amount or Continuous parameters: Calculate percentile boundary values at 0.1 incremental within a band. For Example: Jump and Slope at 95th percentile (p95.0) is calculated as:
 - $\text{Jump (p95.0)} = (\text{p95.1} - \text{p95.0}) / \text{p95.0}$
 - $\text{Slope (p95.0)} = \text{J95.1} - \text{J95.0}$
 - Peak = positive slope followed by negative slope
 - For Count or Discrete parameters: Calculate cumulative frequency distribution for count value as X, and total frequency across all count values as Y. OFS Compliance Studio ML4AML Use Case Guide | 321
 - $\text{Jump (Cur)} = (\text{Xnext}/\text{Y} - \text{Xcur}/\text{Y}) / \text{Xcur}/\text{Y}$
 - $\text{Slope (Cur)} = \text{Jnext} - \text{Jcur}$
 - Peak = positive slope followed by negative slope

3. **Identify Thresholds: Option 1 (Using Jump and multiple bands)** - Assuming the base percentile to be 85th (default) percentile (p85), the data may need to be stratified by risk depending on the scenario. This stratification is done based on the overall risk level that can take any of the following three values: High Risk (HR), Medium Risk (MR) and Regular Risk (RR). A risk boundary represents a conservative yet acceptable range of threshold values for a given segment. The percentile risk boundaries (configurable by the user) for the three risk levels can be defined as:

- HR: p85 – p90
- MR: p90 – p95
- RR: p95 – p99.9

Determining threshold values within a given risk boundary (band) provides an opportunity to identify anomalies within each risk level and helps set thresholds in way to provide more conservative (lower thresholds) coverage for HR activity relative to MR activity and RR activity. The threshold values corresponding to the risk levels can be identified by the highest peaks within the respective percentile bands.

Option 2 (Using Jump and single band) - This approach can be used as an alternative to Option-1 by considering only one single percentile band and identifying 3 highest peaks within the chosen boundary values. Assuming the base to be 85th percentile, identify 3 highest peaks, P1, P2, P3 between p85-p99.9 and assign them as thresholds for HR, MR, and RR risk levels respectively.

 Note:

If 3 peaks cannot be found or population size is low (for ex: <1000), options are provided to determine threshold using various options (share a peak, borrow a threshold from neighbor segment, or default percentile).

Option 3 (Using Percentiles) - Assuming the base percentile to be 85th percentile, the thresholds can be directly set at 85th, 90th and 95th percentiles (configurable by the user) for HR, MR, and RR risk levels respectively. In this case no other calculations would be necessary other than the percentiles.

Risks and Limitations

This section describes the Risks and Limitations

There are no industry standard practices for tuning methodology. The methodology outlined in this document aims at providing a generic framework while allowing customizations as per FI's risk tolerance.

The methodology used here cannot be used to produce recommendations for two kinds of thresholds.

1. **Max Thresholds** : The methodology is designed to recommend thresholds only for Min thresholds. Any thresholds that impose an upper bound on some activity, e.g., Max_Credit_Amt in the RMF scenario, cannot be tuned using this methodology.
2. **Secondary Thresholds**: This methodology can recommend only one threshold for a given parameter. For example, in the HRG Funds Transfer scenario, three thresholds are used to evaluate the Total Amount of HRG Transactions parameter.
 - a. Min HRG Total Trans Amt
 - b. Min HRG Total Trans Amt (Primary)

c. Min HRG Total Trans Amt (Secondary)

This methodology can recommend only one threshold for this parameter. The recommended threshold should be used only to recommend the threshold that is satisfied by all events generated by the scenario. In the example of the HRG Funds Transfer scenario, this threshold is Min HRG Total Trans Amt.

Supported Scenarios (System Recommended Thresholds)

The section provides the list of supported scenarios.

The following table provides the list of supported scenarios.

Table 9-2 List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
Rapid Movement of Funds – All Activity (RMF)	Money launderers typically move funds between accounts to help integrate the funds and give the appearance of legitimacy. One possible indication of money laundering activity is the rapid movement of funds into and out of an account. The scenario detects both new accounts/customers and more seasoned accounts/customers that move transactions of all types in and out of an account or accounts within a specified Lookback Period. The scenario can take into account the amount or velocity of funds through the account relative to the account balance or net worth.	TOTAL_AMOUNT and TOTAL_COUNT
Single or Multiple Cash Transactions: Large Significant Transactions (SigCash)	Money launderers may deposit or withdraw significant amounts of cash, either in a single transaction, or in multiple transactions over a period. Such deposits may not appear to be consistent with the type of account or the declared business or activity that the customer is involved with. This scenario detects instances of large cash deposits or withdrawals (over USD 10,000 or comparable cash reporting threshold for different jurisdictions) and detects smaller, multiple deposits or withdrawals over a specified Lookback Period (typically two weeks or 30 days) that aggregate to a significant amount. The scenario enables detection of structuring activity across branches or locations. Thresholds can be modified to enable application of scenarios to various reporting threshold requirements.	TOTAL_AMOUNT and TOTAL_COUNT

Table 9-2 (Cont.) List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
Large Reportable Transactions (LRT)	Certain countries require that financial institutions report customer transactions that exceed a specified threshold. These requirements typically pertain to new customer relationships and transactions associated with account opening. They may also pertain to existing customer relationships. Clients may also have internal policies that require the reporting or review of transactions exceeding certain amounts. This scenario detects deposits of any type (across products and asset types), made at account opening or within a certain period after account opening, that exceed a specified threshold. The definition of new account is configurable. The scenario also detects deposits or withdrawals of any type (across products and asset types) in existing accounts that exceed a certain threshold. The scenario detects such transactions involving a single account or multiple accounts that are linked to the customer or household through the client's house holding process. The scenario provides separate thresholds for each type of relationship (new or existing) that are tunable to support client and country specific regulatory requirements.	TOTAL_AMOUNT
CIB: Significant Change from Previous Average Activity (CIB:PAA)	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, etc. on a daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts, customers, and correspondent banks that may be considered to be at risk by monitoring electronic funds transfers, check, monetary instrument, cash and journal activity and detecting significant changes from the average of previous monthly transaction activity.	TOTAL_AMOUNT
CIB: Significant Change from Previous Peak Activity (CIB:PPA)	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, and so forth on a daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario is targeted to accounts, customers, and correspondent banks that have a volatile historical behavior. The scenario monitors electronic funds transfers, check, monetary instrument, cash, and journal transactions; and detects significant changes from the previous monthly peak transaction activity.	TOTAL_AMOUNT

Table 9-2 (Cont.) List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
CIB: High Risk Geography Activity (CIB:HRG)	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, and so forth on a daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring for electronic funds transfers, check, and monetary instrument activity involving high risk geographies and detecting significant changes from the previous monthly high-risk geography transaction activity.	TOTAL_AMOUNT and HRG_AMOUNT
High Risk Transactions: Focal High Risk Entity (HRG:HRE)	Financial institutions must apply enhanced scrutiny to transactions involving high-risk entities, as such activity that may subject the institution to a greater risk of money laundering or fraud. Any account, customer, correspondent bank, or external entity found on a watch list is considered to be a high-risk entity. This scenario monitors transactions to and from high-risk entities during a specified Lookback Period.	TOTAL_HIGH_RISK_AMOUNT and TOTAL_HIGH_RISK_COUNT
High Risk Transactions: High Risk Geography (HRG:HRT)	Financial institutions are expected to apply enhanced scrutiny to transactions both to and from areas considered high risk. Because of the large volume and speed of transactions, electronic funds transactions are considered particularly vulnerable to money laundering. This scenario identifies accounts, customer, or entities that may be at risk based on the incidence of electronic funds transfers, cash, checks, or monetary instrument transactions involving specified high-risk geographic areas.	HRG_AMOUNT, HRG_COUNT, TOTAL_AMOUNT, VHRG_AMOUNT, and VHRG_COUNT
Deposits/Withdrawals in Same or Similar Amounts	Most deposits and withdrawals of funds into and out of an account are done for specific purposes and, therefore occur in varying amounts. The occurrence of repetitive patterns, or a high percentage, of deposits or withdrawals in the same amount or similar amount, may be unusual activity for the account or customer. This type of activity may indicate attempts to structure funds into the institution or remit funds in a structured manner to fund illicit activities. This scenario detects patterns of deposits and/or withdrawals made in the same or similar amounts that aggregate above specified thresholds. The specification of similar amounts is configurable.	OCCURRENCE_COUNT

Table 9-2 (Cont.) List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
Anomalies in ATM, Bank Card: Excessive Withdrawals	Bank/Debit cards can be easily used at Automated Teller Machine (ATM) to transfer assets to other individuals or locations due to the anonymity they afford the users. Deposits can be made into accounts in any number of ways and then be removed as currency from almost any location. A sudden increase in the number or amount of ATM deposits and withdrawals may indicate an attempt to launder funds; an increase in ATM withdrawals, or change in the location of ATMs used may also indicate account takeover. Sudden increases in the activity at a certain location may indicate fraudsters' use of skimmed or compromised Bank/Debit cards. This scenario monitors a sudden increase in the amount of Bank/Debit cards withdrawals at ATMs that may indicate money laundering, terrorist financing, or an account takeover.	TWO_DAY_AVG_AMOUNT and HIST_MONTH_AVG
Transactions in Round Amounts	Most electronic funds transfers (EFT) or monetary instruments are done for a specific purpose and, therefore, in a precise amount. The occurrence of a high percentage of transactions in round amounts may be indicative of attempts to launder funds or perpetrate fraud. This scenario detects patterns of EFT or monetary instruments in round amounts that in the aggregate satisfy specified thresholds.	TOTAL_ROUND_AMOUNT, TOTAL_ROUND_COUNT, TOTAL_AMOUNT, and TOTAL_COUNT
CIB: Foreign	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, and so forth on a daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring for foreign electronic funds transfers and check transactions and detecting significant changes from the previous monthly foreign transaction activity.	TOTAL_AMOUNT and TOTAL_FOREIGN_AMOUNT
CIB: Product Utilization Shift	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, and so forth on a daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring for changes in the types of products that are utilized by the account, (product utilization shift) among electronic funds transfers, check, monetary instrument, cash, and journal transactions.	TOTAL_AMOUNT

Table 9-2 (Cont.) List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
Rapid Movement of Funds: Funds Transfers (RMF:FTN)	This scenario targets one of the typical behaviors of the placement stage of money laundering, where illegally obtained money from various sources is collected at one place and then disbursed for the purpose of layering. The scenario monitors the activity where funds are funneled into the accounts of one beneficiary from many originators or funds are transferred out by one originator to many beneficiaries.	TOTAL_AMOUNT and TOTAL_COUNT
Large Depreciation of Account Value (LDA)	A large and sudden debit, or series of debits, from an account causing a significant depreciation in the account's net worth could signal account takeover or other type of fraudulent activity. This scenario identifies accounts that experience a significant value depreciation within a specified period. The scenario also distinguishes between new and seasoned accounts based on the account open date.	TOTAL_AMOUNT
Single or Multiple Cash Transactions: Possible Currency Transaction Report	Money launderers seeking to place or move funds in the banking system may structure their deposits or withdrawals of cash and cash equivalent monetary instruments to avoid the filing of a CTR. For example, the launderer may make deposits of cash at various branches that aggregate over the CTR threshold, but go unreported because the deposit at each branch did not trigger a reporting action. This scenario detects instances of a single deposit or withdrawal over the CTR threshold, or multiple deposits or withdrawals over the current and previous day that aggregate over the threshold.	TOTAL_AMOUNT
Anomalies in ATM Bank Card - Foreign Transactions	Bank/Debit cards can be easily utilized at ATMs to transfer assets to other individuals or locations due to the anonymity afforded to ATM users. Deposits can be made into accounts in any number of ways and then be removed as currency from almost any location. A sudden increase in the number or amount of ATM deposits and withdrawals may indicate an attempt to launder funds; an increase in ATM withdrawals, or change in the location of ATMs used may also indicate account takeover. Sudden increases in the activity at a certain location may indicate fraudsters' use of skimmed or compromised Bank/Debit cards. This scenario monitors foreign ATM withdrawal activity that could be indicative of money laundering or terrorist financing.	TOTAL_FOREIGN_COUNT, TOTAL_AMOUNT, and TOTAL_FOREIGN_AMOUNT
Anticipatory Profile – Expected Activity	Financial institutions are under increased regulatory pressure to improve their collection and verification of customer information, particularly at account opening. The information collected to support these efforts provides a rich source of data that can be used to support enhanced profiling capabilities. Anticipatory profiling is designed to leverage key parameters that describe anticipated or expected account activity. This scenario monitors transactions involving client accounts relative to the expected activity involving the account and generates an alert when activity deviates significantly from expected activity.	TOTAL_AMOUNT, TOTAL_COUNT, and TOTAL_EXPECTED_AMOUNT

Table 9-2 (Cont.) List of Supported Scenarios

Scenario Name	Scenario Description	Aggregates+
Escalation in Inactive Accounts	Money launderers may open accounts, deposit illicit funds, conduct a small number of transactions to test the system, and then leave the account alone for a period to avoid raising suspicions. They then remove a significant portion of the balance of the account, often leaving the remaining balance behind to avoid detection. This scenario generates an alert for accounts that are inactive for a predefined period and then have a sudden escalation in activity. It identifies accounts that may be considered to be at risk based on the number, amount, or a large portion of recent transactions in contrast to its previous dormant status. The client's risk exposure is greater for outgoing funds relative to incoming funds. The system then monitors significant withdrawal activity at more stringent thresholds than deposit activity.	TOTAL_AMOUNT and TOTAL_COUNT
Structuring - Avoidance of Reporting Thresholds	Money launderers seeking to place or move funds in the banking system may structure their cash monetary instrument, or wire transactions to avoid reporting requirements, such as the filing of a currency transaction report (CTR) or other report required in a given country. The institution may wish to monitor more closely any accounts, customers, households, or external entities engaging in such activity. Oracle detects instances of cash, monetary instrument, or wire transaction(s) in amounts just below applicable reporting thresholds during a specified Lookback Period. The scenario supports the use of multiple threshold sets to accommodate reporting requirements that may differ by country or jurisdiction, as well as to support multiple thresholds within a country or jurisdiction (that is, support of CTR and cash log thresholds can occur simultaneously).	TOTAL_ATTEMPT_COUNT
Anticipatory Profile - Income	Financial institutions are under increased regulatory pressure to improve their collection and verification of customer information, particularly at account opening. The information collected to support these efforts provides a rich source of data that can be used to support enhanced profiling capabilities. Anticipatory profiling is designed to leverage key parameters that describe anticipated or expected account activity. This scenario monitors all transactions involving the focal customer and generates an alert when the amount of credits into the focal customer's accounts exceeds a percentage of the monthly income (income as stated by the customer or verified by the client).	TOTAL_AMOUNT, MONTHLY_INCOME, and TRANSACTIONS_RELATED

+Based on transactions data to compute threshold for the given scenario.

Glossary

This section describes a glossary of terms used across the OFSCA application.

Account

A bank account where funds can be deposited or withdrawn.

Agent

A virtual money launderer powered by artificial intelligence can perceive the account balances and transaction monitoring rules in a simulated environment and move funds from a source account to a destination account within a simulated environment.

Channels

A transaction channel can be used to transfer funds in and out of an account, e.g., Wire. Controls Set A specific configuration of the transaction monitoring system, i.e., controls and limits.

Episode

An episode is an instantiation of the policy learned by the agent to move funds from the source to the target account. It is a sequence of actions the agent takes to accomplish its goal.

Experiment

The training of an Agent in a simulated environment. The financial transactions made by a trained agent are subsequently used to measure the performance of a transaction monitoring system and surface insights.

Granularity

The agent can transfer funds only in whole number multiples of granularity. The granularity is calculated as $1/20 \times \text{Target Amount}$. If the Target Amount is \$100,000, the agent can transact only in whole number multiples of \$5,000 ($1/20 \times \$100,000$).

Jurisdiction Code

The Jurisdiction associated with a customer is specified in Oracle's FCDM data model.

Limits

Any limit or restriction on the amount of funds or the number of transactions that can be made from an account or using a channel.

Offerings

The financial products (Accounts and Channels) offered by an institution to its customers.

Scenario

A rule used to monitor the behavior of interest. Each scenario pertains to one focus type and underlying pattern and thresholds.

Segment

The Customer segment is associated with a customer. Each customer should belong to just one segment. The controls (thresholds and limits) a customer is subject to depend on the segment the customer belongs to.

Source Account

The account which is the source of funds. This is typically considered to be external to the institution.

Target Account

The account which is the intended destination of funds. The agent seeks to move the funds from the source account to this target or destination account.

Threshold

A numeric value specifies a range of activities deemed to be of interest. Each scenario typically has multiple thresholds.

Transaction Monitoring System (TMS)

Transaction Monitoring System is the collection of controls (including scenarios and other limits) that have been put in place to deter and detect suspicious activity and to comply with AML regulations.