Oracle® Financial Services Compliance Agent Cloud Service

User Guide

Release 24.08.01
G13806-04
August 2024

Oracle Financial Services Compliance Agent Cloud Service User Guide, Release 24.08.01

G13806-04

Contents

1
Preface

FCCM Cloud Service Compliance Agent User Guide describes how to use Compliance Agent Application.

1.1 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.

1.2 Comments and Suggestions

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

1.3 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.

1.4 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:

2.1 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.

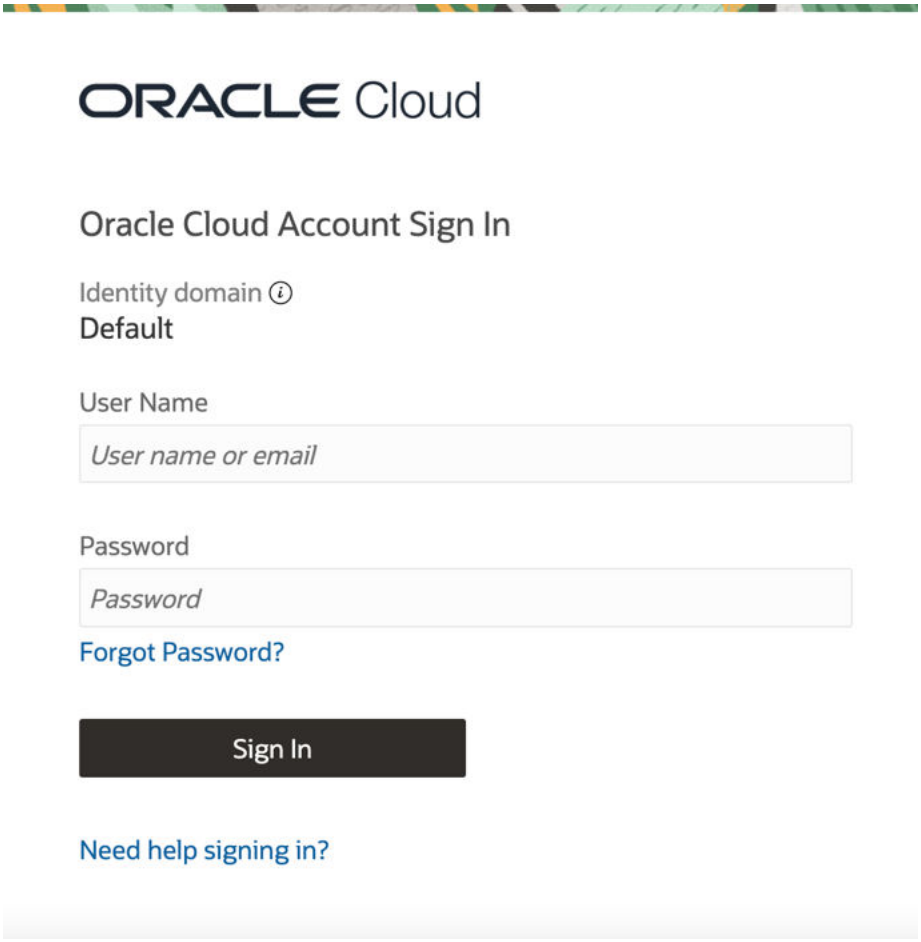
2.2 Accessing OFSCA

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



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

2.3 User Roles and Privileges

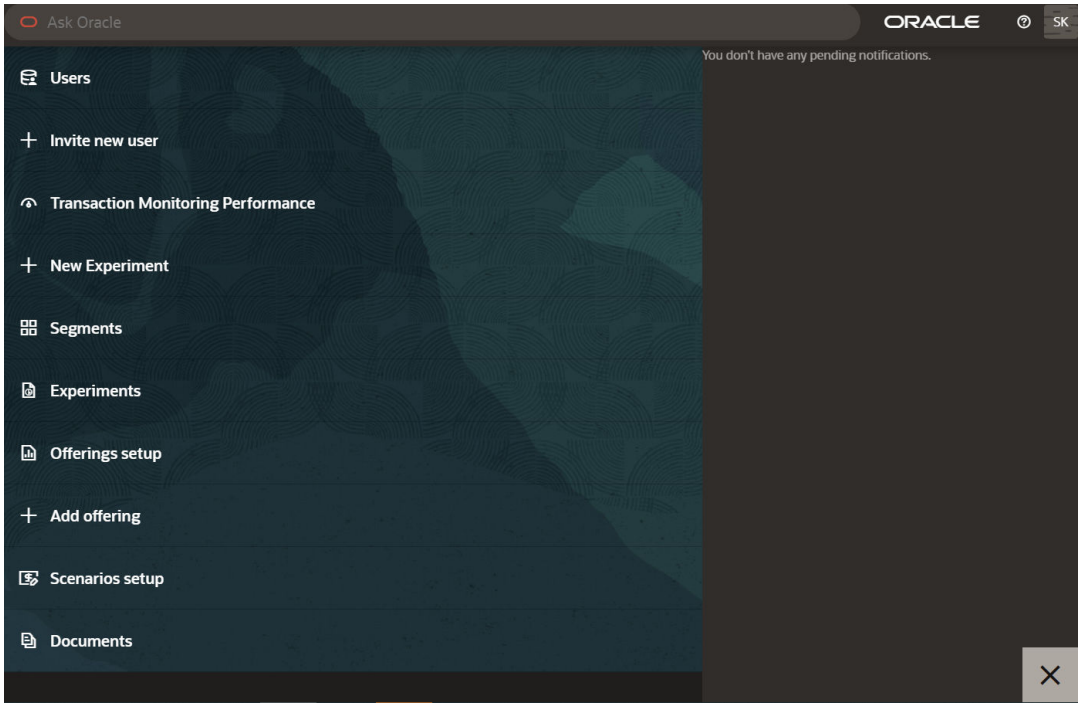
Topics:

- 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:

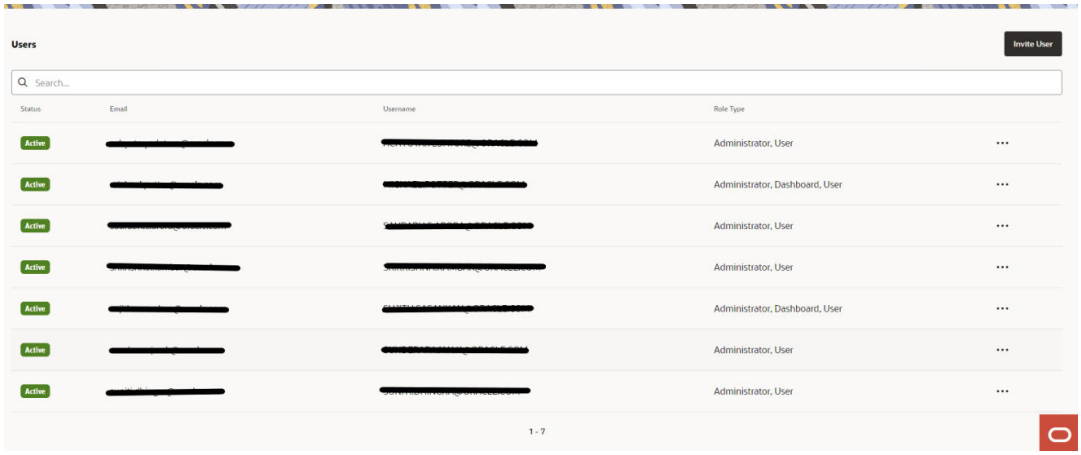
1. Click **Open Ask Oracle**  to display the Ask Oracle window. The following window is displayed.
2. Click **Users** menu to display the Users window. The following window is displayed

Figure 2-2 Application Menu



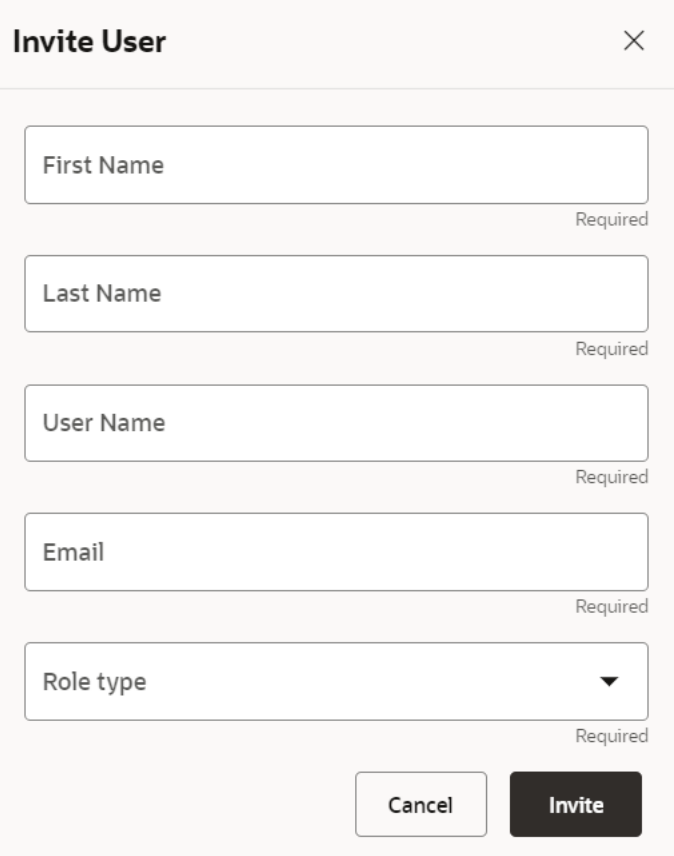
3. Click **Users** menu to display the Users window. The following window is displayed.

Figure 2-3 Users



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

Figure 2-4 Invite Users



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.

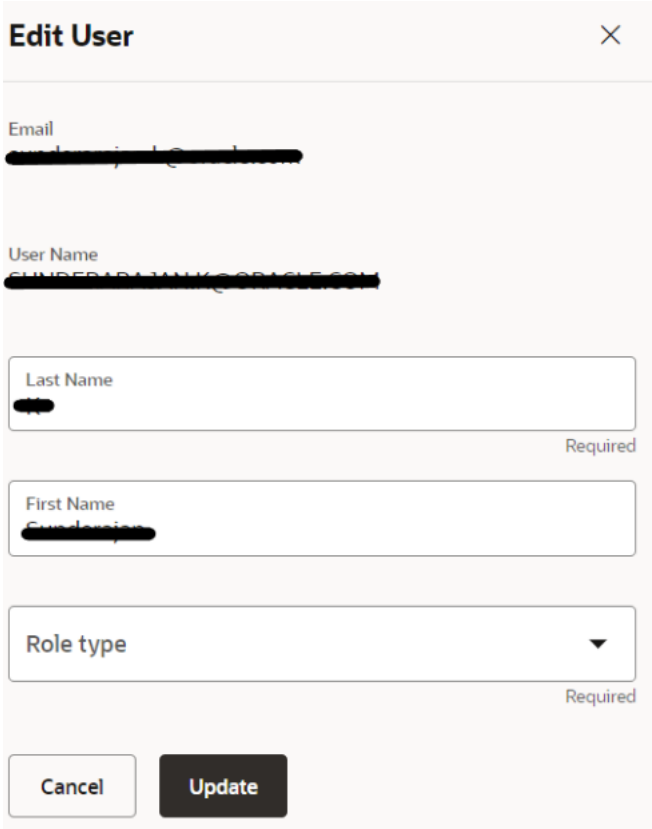
2.3.1 Editing the User

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.

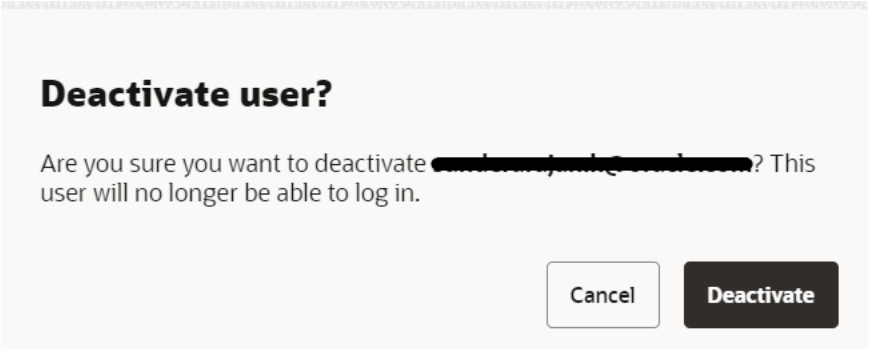
2.3.2 Deactivating the User

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

You can configure your Transaction Monitoring System with:

- **System Recommended Thresholds**: If you want to generate initial threshold recommendations for new Oracle Behavior Detection scenarios and then assess your Transaction Monitoring System.
- **User Defined Thresholds**: If you want to assess your Transaction Monitoring System with the pre-defined/user-defined thresholds.

3.1 System Recommended Thresholds

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

If you are migrating from a different vendor to Oracle's Transaction Monitoring System, Compliance Agent can recommend preliminary thresholds for scenarios you want to deploy.

This involves the following steps:

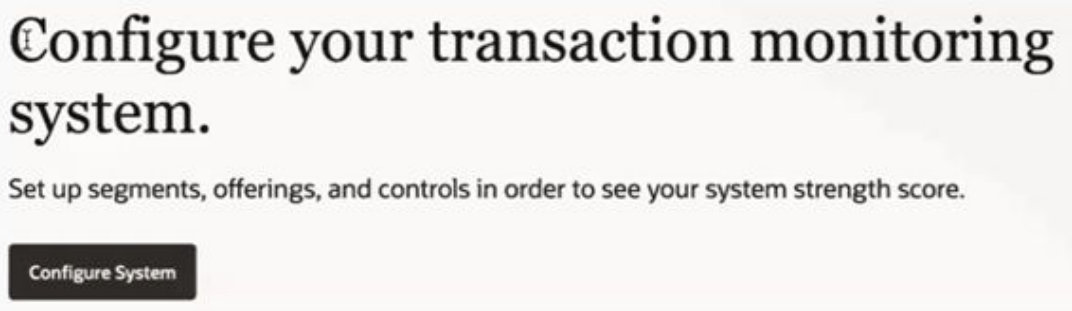
1. Select Scenarios and Segment Codes
2. Upload Transaction Aggregates
3. Treat Outlier
4. Review Threshold Recommendations
5. Set up Accounts, Channels, and Limits
6. Create Agents
7. Review
8. Resetting the Transaction Monitoring System

For more information on Methodology and Simulating Aggregates, see Appendix.

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 as shown below:

Figure 3-1 Configuration

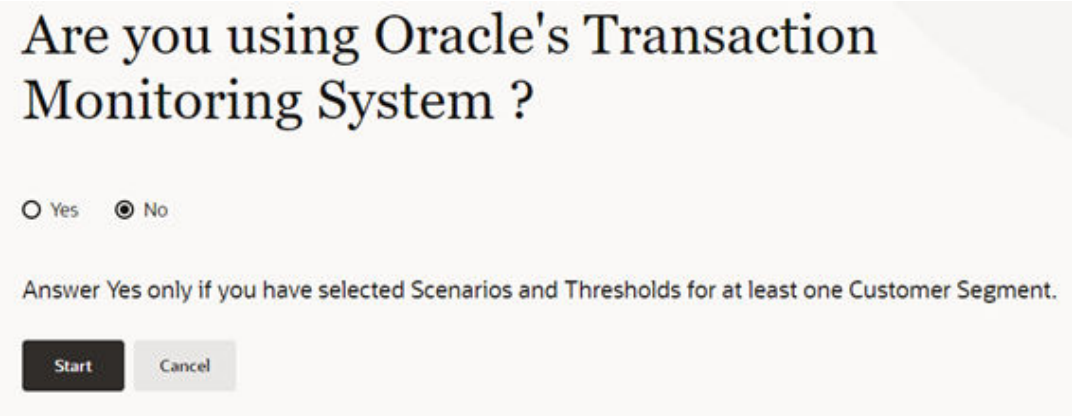


2. Click **Configure System**. The **Existing Oracle Customer** page is displayed.
3. Select **No** and click **Start**.

   Selecting **No** guides you through the configuration workflow for users who are not presently using Oracle's Transaction Monitoring System.

   Select **Yes**, if you are an existing customer and have selected Scenarios and Thresholds for at least one Customer Segment.

Figure 3-2 Are you using Oracle's Transaction Monitoring System?



4. On the **Initial Configuration – Overview** page, click **Start** to configure your transaction monitoring system

Figure 3-3 Initial Configuration – Overview

3.1.1 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.

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.

> **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.

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 Aggregates 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.

3.1.2 Upload Transaction Aggregates

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 – e.g. for the RMF scenario, the expected data includes Customer Internal ID, Month ID, Total Credit Amount, Total Debit Amount, Total Credit Count, and Total Debit Count.

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.
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 Treat Outliers 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.

3.1.3 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 3-1 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 IQR.
2	Inter Quartile Range	Right Tail only	1.5 IQR	Remove the values which are greater than Q3 + 1.5 IQR.
3	Inter Quartile Range	Both Tails	1.5 IQR	Remove the values which are less than Q1 - 1.5 IQR and the ones which are greater than Q3 + 1.5 IQR.
4	Percentile	Left Tail only	5	Remove the values which are less than 5th percentile.

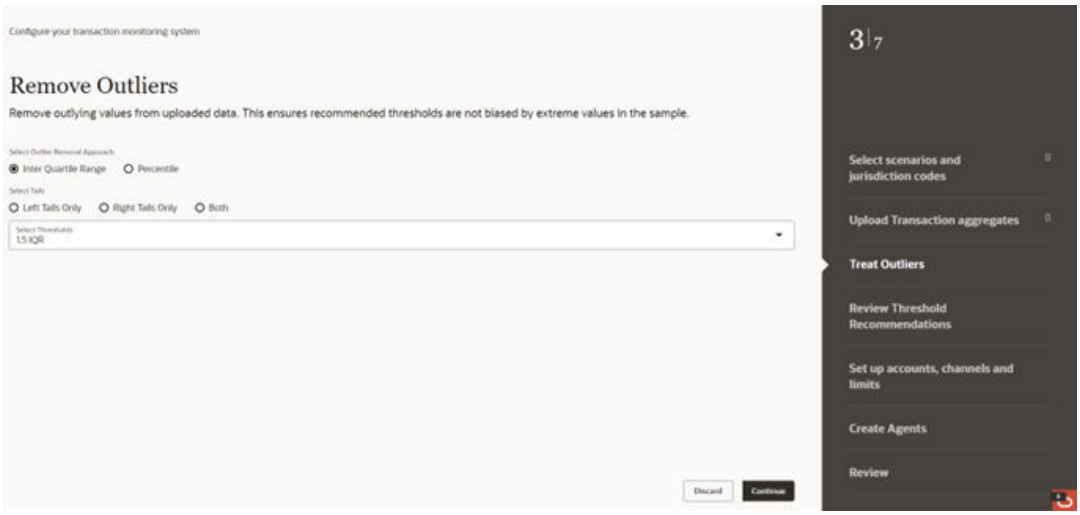
Table 3-1 (Cont.) Outlier Combination

SL#	Approach	Tails	Thresholds	Outlier Treatment Logic
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 3-4 Remove Outliers



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

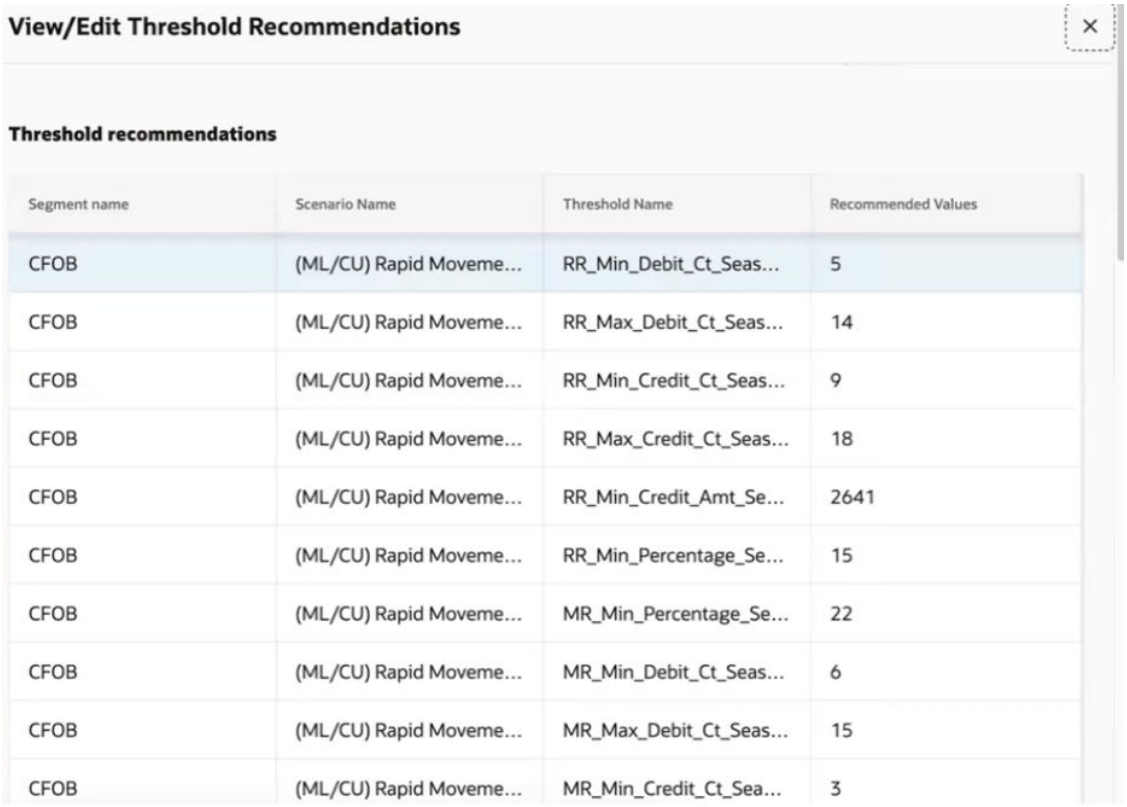
   Or click **Discard** to discard the current activity.

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

3.1.4 Review Threshold Recommendations

In this step you can review the Threshold recommendations.

Figure 3-5 View/Edit Threshold Recommendations



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.

3.1.5 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 3-6 Set up segments, accounts, channels and limits

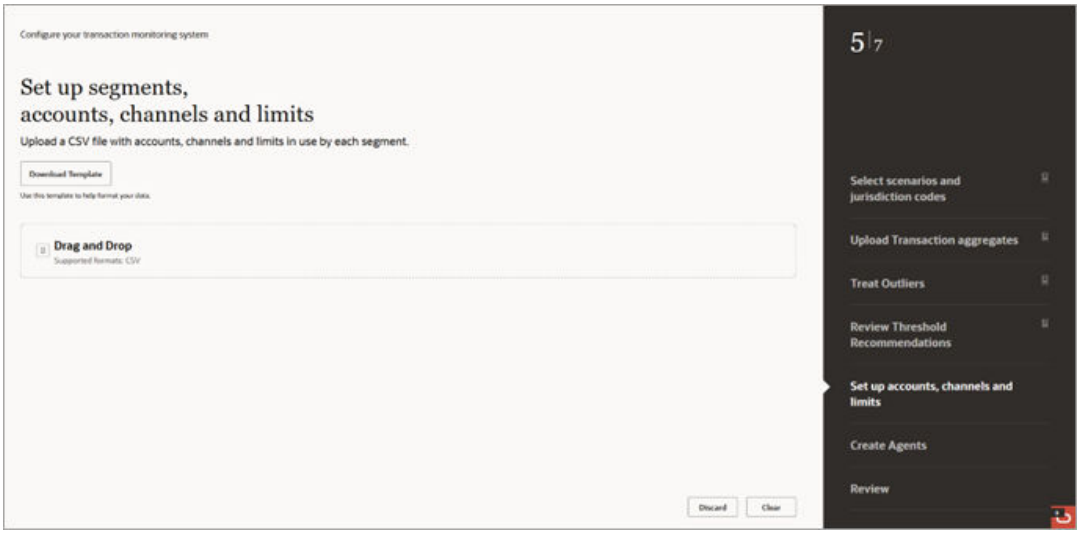
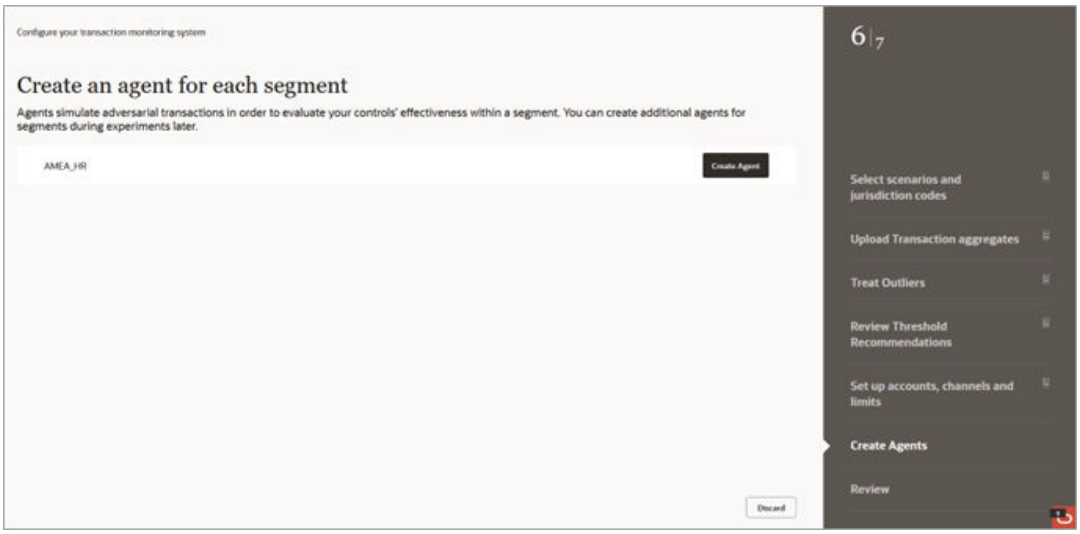


Figure 3-7 Preview of Uploaded CSV file to Set up Account, Channels, and Limits



> **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 Createan agent for each segment step.

3.1.6 Creating an Agent

This section describes how to create an agent for each segment. Whenever a new agent is created, by default, a Human Trafficking (HT) agent is created. You can create a new agent for the following situations:

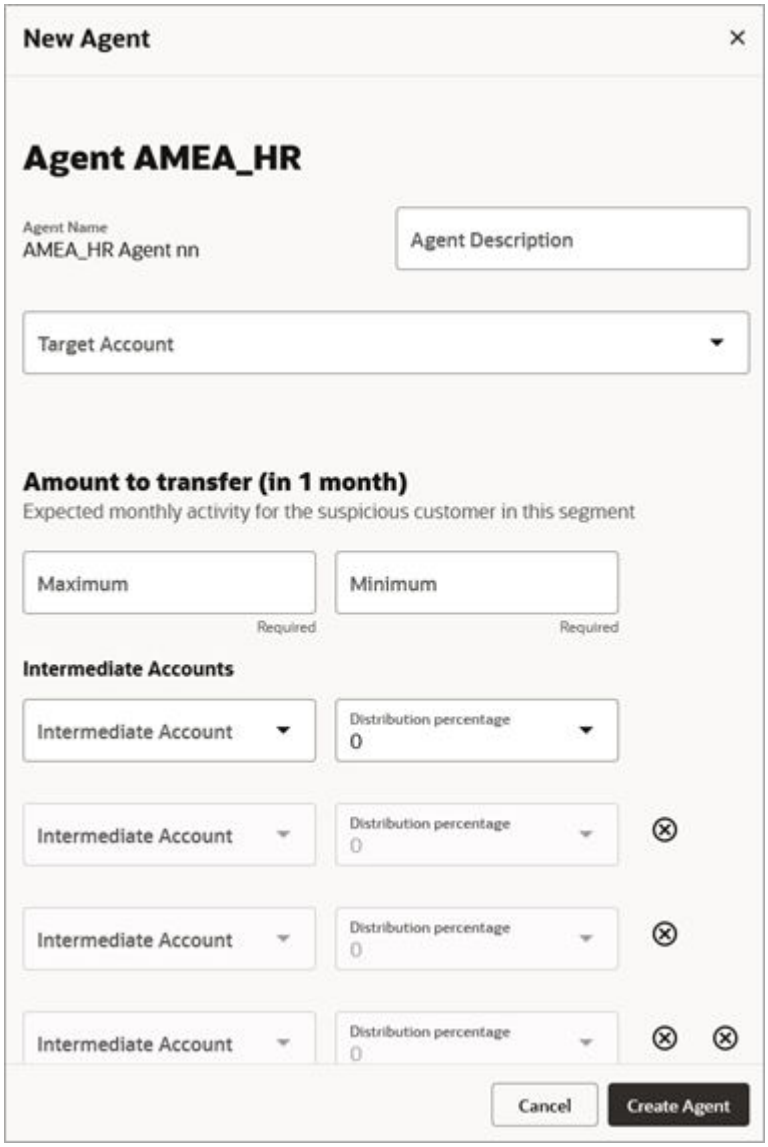
- If the expected activity of the segment changes and hence the target amount has to change.
- When the distribution of accounts used by customers in the segment changes and hence distribution of accounts changes.

Figure 3-8 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 3-9 New 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.

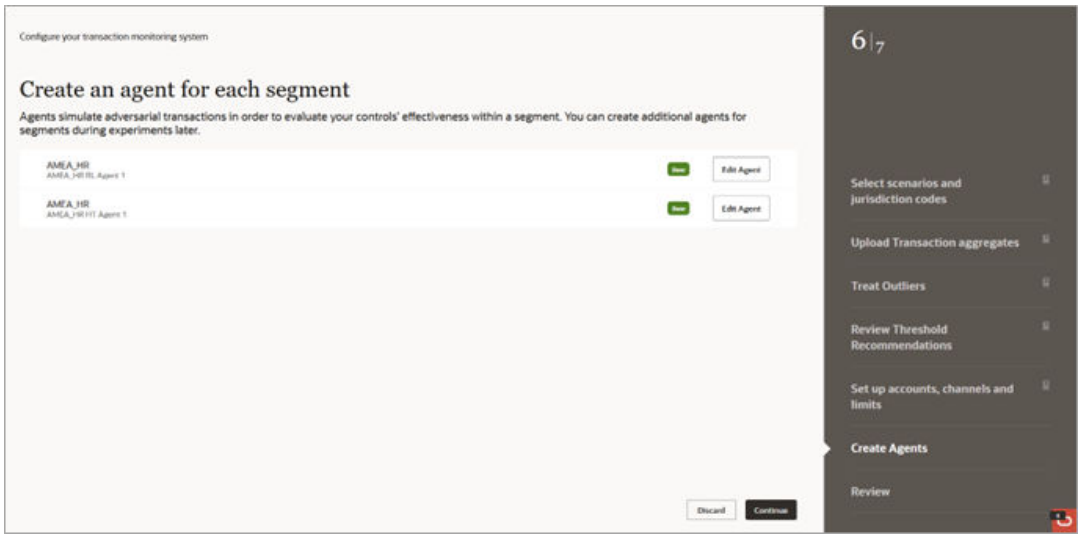
> **Note:**
>
> You can create a maximum of four intermediate accounts for each segment.

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 3-10 Agent Created



Similarly, you can create an agent for multiple segments.

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

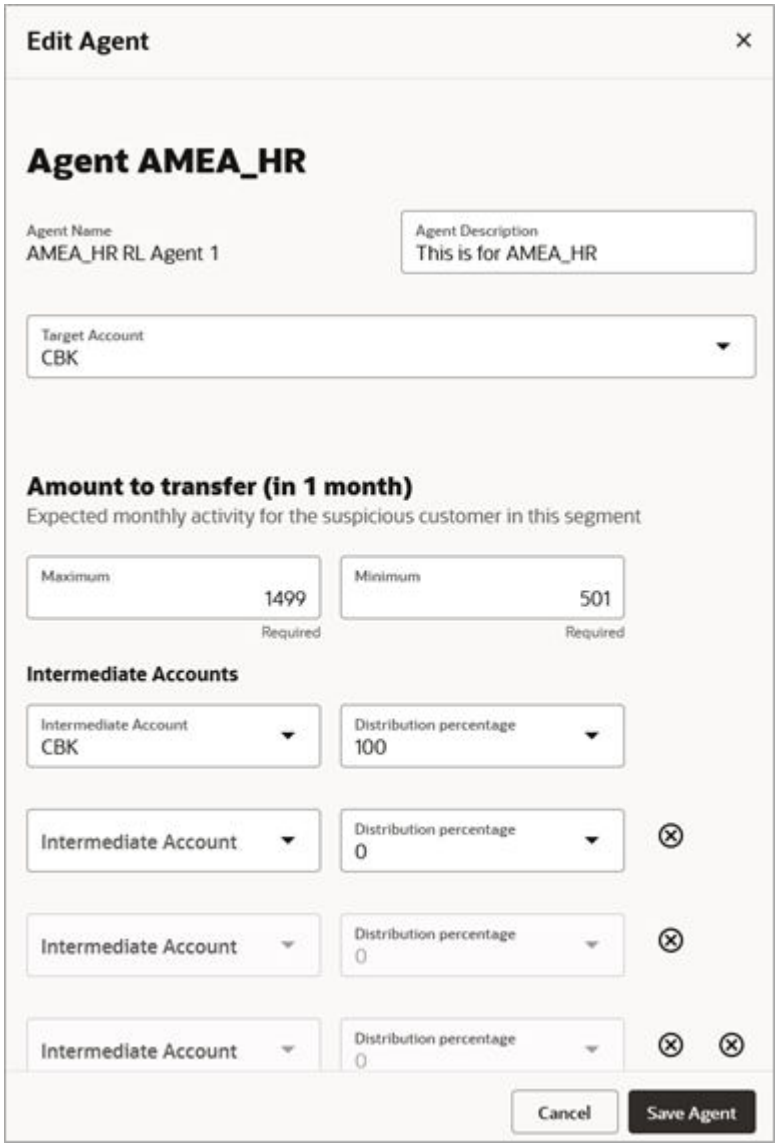
3.1.6.1 Editing An Agent

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 3-11 Edit Agent



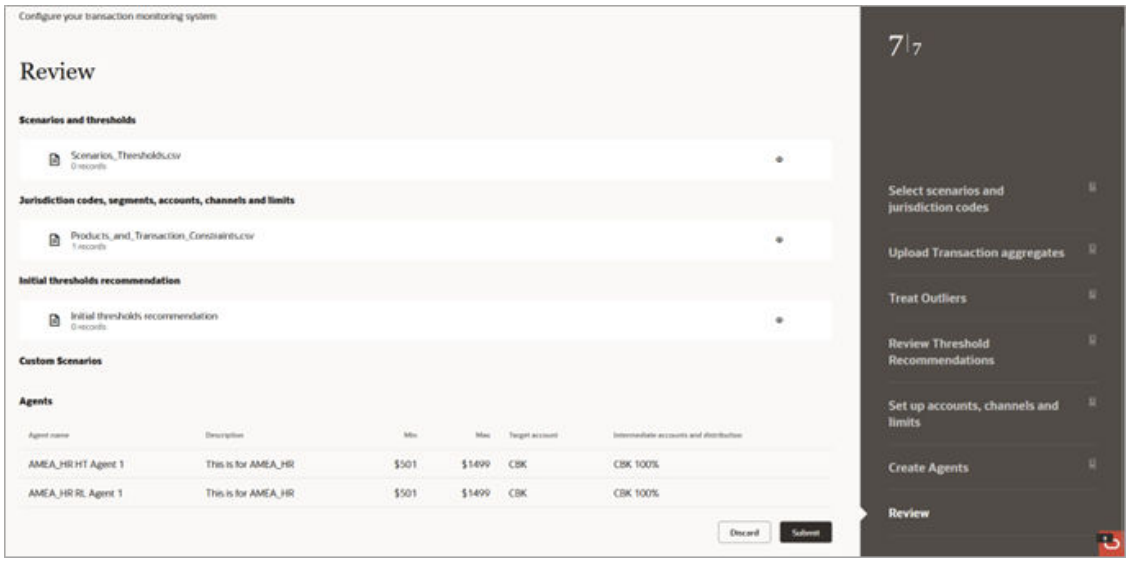
2. Click **Save Agent** to save any modifications made to the agent.

3.1.7 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 3-12 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.

3.1.8 Resetting the Transaction Monitoring System

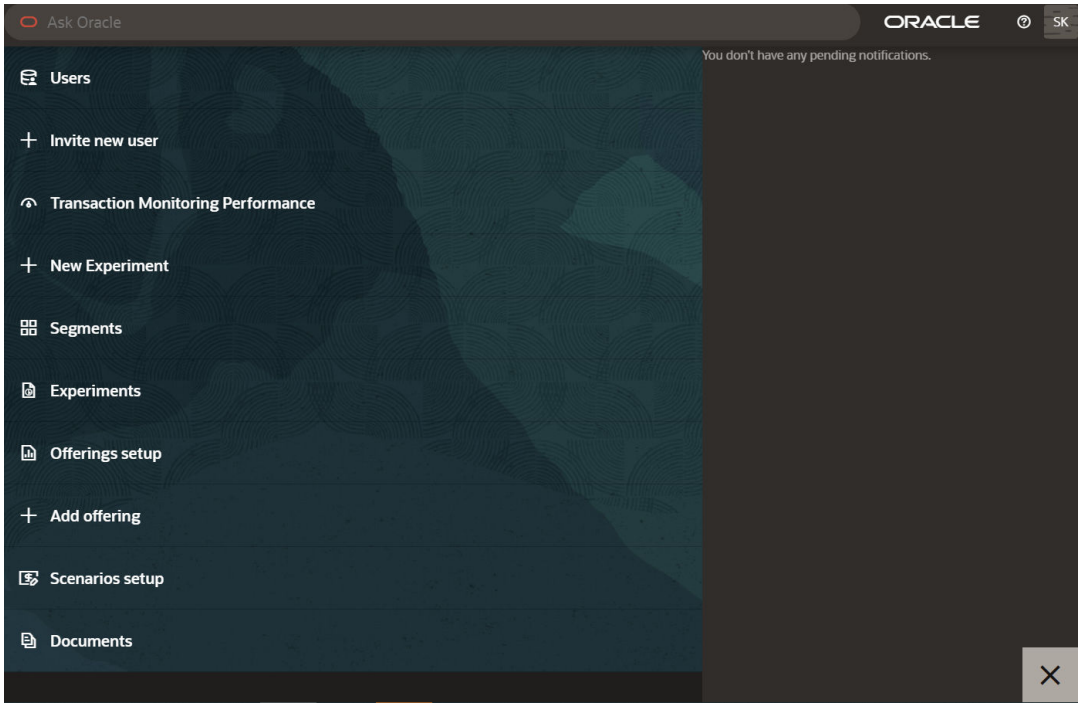
This section describes how to reset your transaction monitoring system configuration in OFSCA.

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 3-13 Application Menu

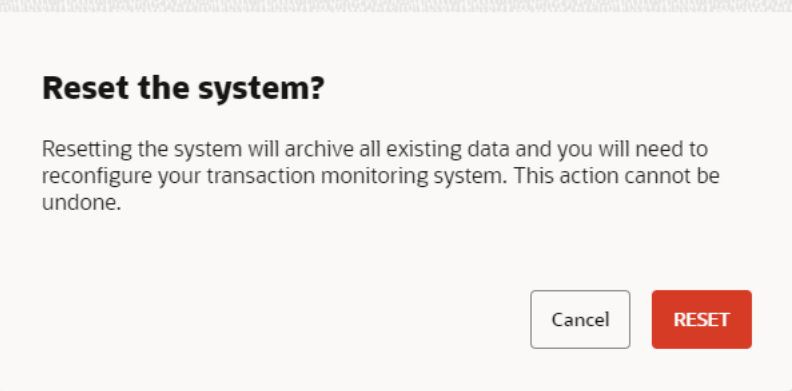


2. Click **Documents** menu to display the Documents window. The following window is displayed.

Figure 3-14 Documents Menu

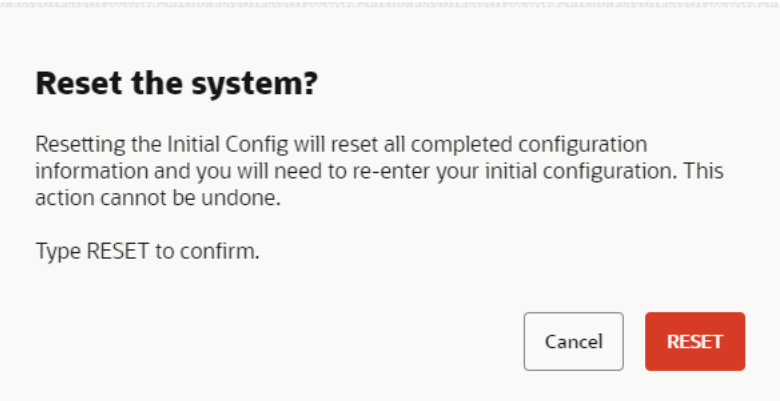
3. Click **Reset System** to reset your transaction monitoring system. The confirmation window is displayed.

Figure 3-15 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 3-16 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.

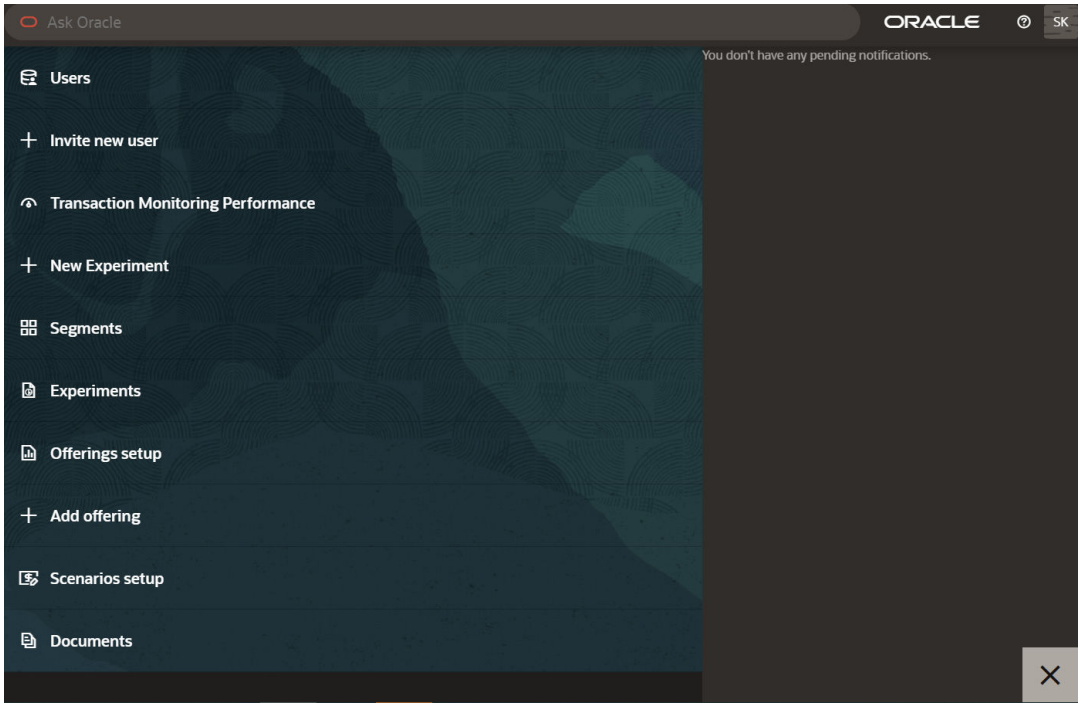
3.2 User Defined Thresholds

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 3-17 Application Menu



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

Figure 3-18 Configure Transaction Monitoring System

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

Topics:

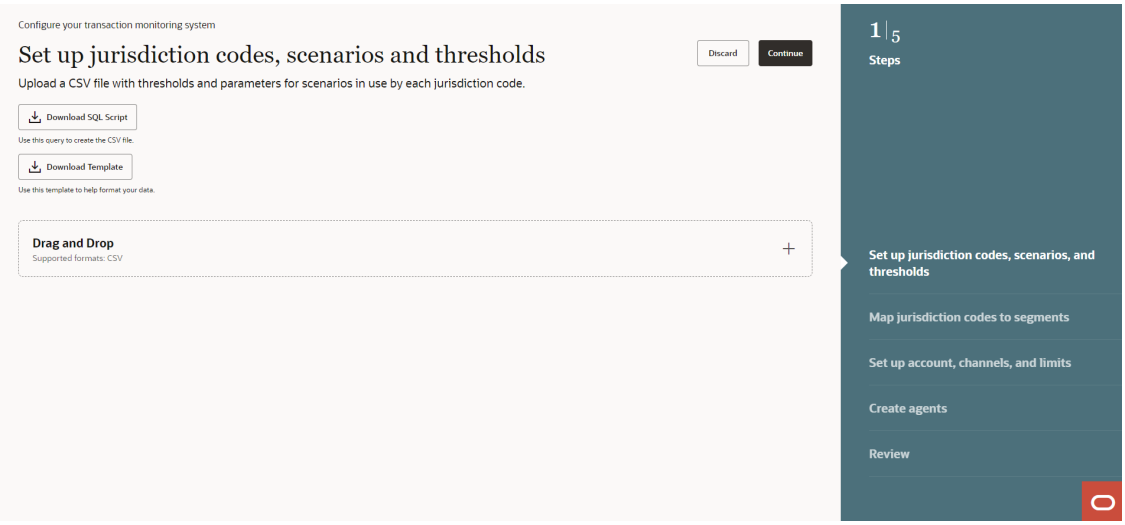
- Setting up Jurisdiction Codes, Scenarios and Thresholds
- Mapping Jurisdiction Codes to Segments
- Setting up Jurisdiction Codes, Segments, Accounts, Channels, and Limits
- Creating an Agent

- Reviewing your Transaction Monitoring System

3.2.1 Setting 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.

Figure 3-19 Set up Jurisdiction Codes, Scenarios, and thresholds



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

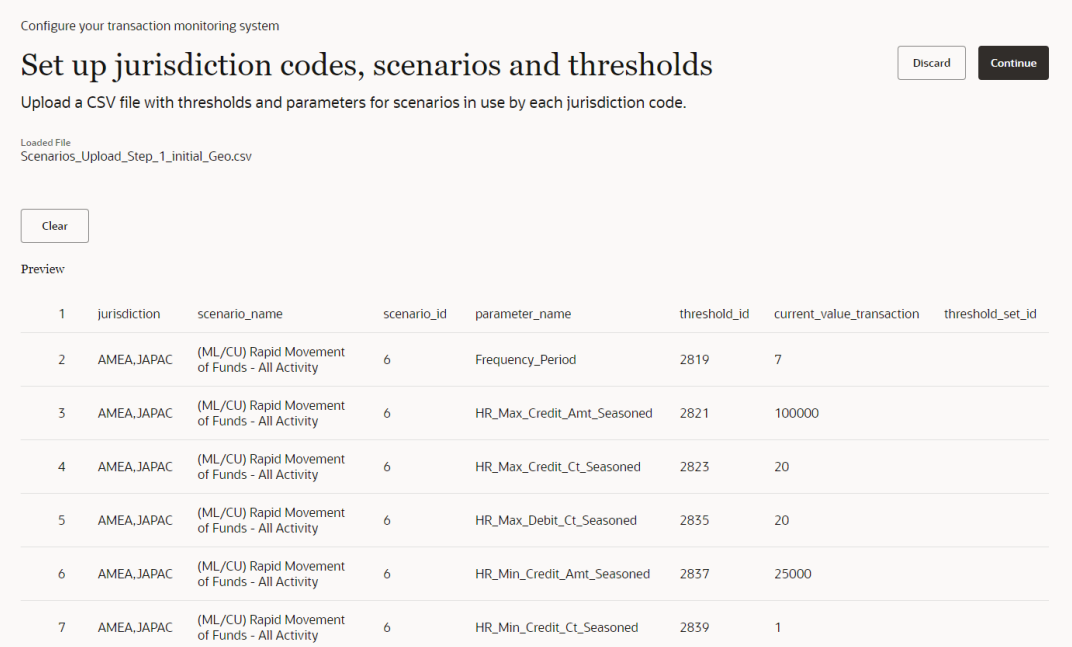
> **Note:**
>
> Click **Download SQL** Script to download SQL script and execute the script against data in Oracle's Financial Crime Data Model to extract the required data

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

   > **Note:**
   >
   > - You should not modify jurisdiction, scenario_name, and scenario_id in 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. 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 3-20 Uploaded CSV File



1	jurisdiction	scenario_name	scenario_id	parameter_name	threshold_id	current_value_transaction	threshold_set_id
2	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	Frequency_Period	2819	7	
3	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	HR_Max_Credit_Amt_Seasoned	2821	100000	
4	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	HR_Max_Credit_Ct_Seasoned	2823	20	
5	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	HR_Max_Debit_Ct_Seasoned	2835	20	
6	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	HR_Min_Credit_Amt_Seasoned	2837	25000	
7	AMEA,JAPAC	(ML/CU) Rapid Movement of Funds - All Activity	6	HR_Min_Credit_Ct_Seasoned	2839	1	

> **Note:**
>
> You can remove the uploaded CSV file if required by using the Clear button.

3. 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

3.2.2 Designing Custom Scenarios

Some FI's customize or modify Oracle's Out of the Box scenarios or use purpose built scenarios for their specific needs. OFSCA's customs scenario authoring functionality allows you to include such scenarios in OFSCA's simulator allowing you to get an accurate assessment of your entire 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.

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

1. Click **Download Template**. A JSON template is downloaded.

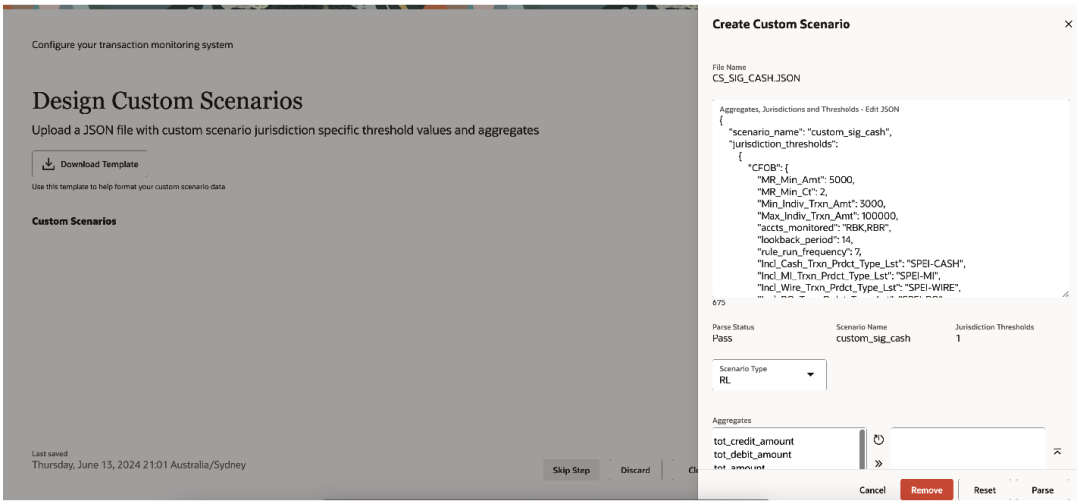
   Currently, a single JSON file can be used to configure a scenario for only one risk segment. If a scenario has to be configured for three risk segments, for example, BCAP_RR, BCAP_MR, BCAP_HR, three different JSON files are required with three different scenario names. For sample files, see **Sample Template**

2. 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 Setting up Jurisdiction Codes, Scenarios, and Thresholds section.

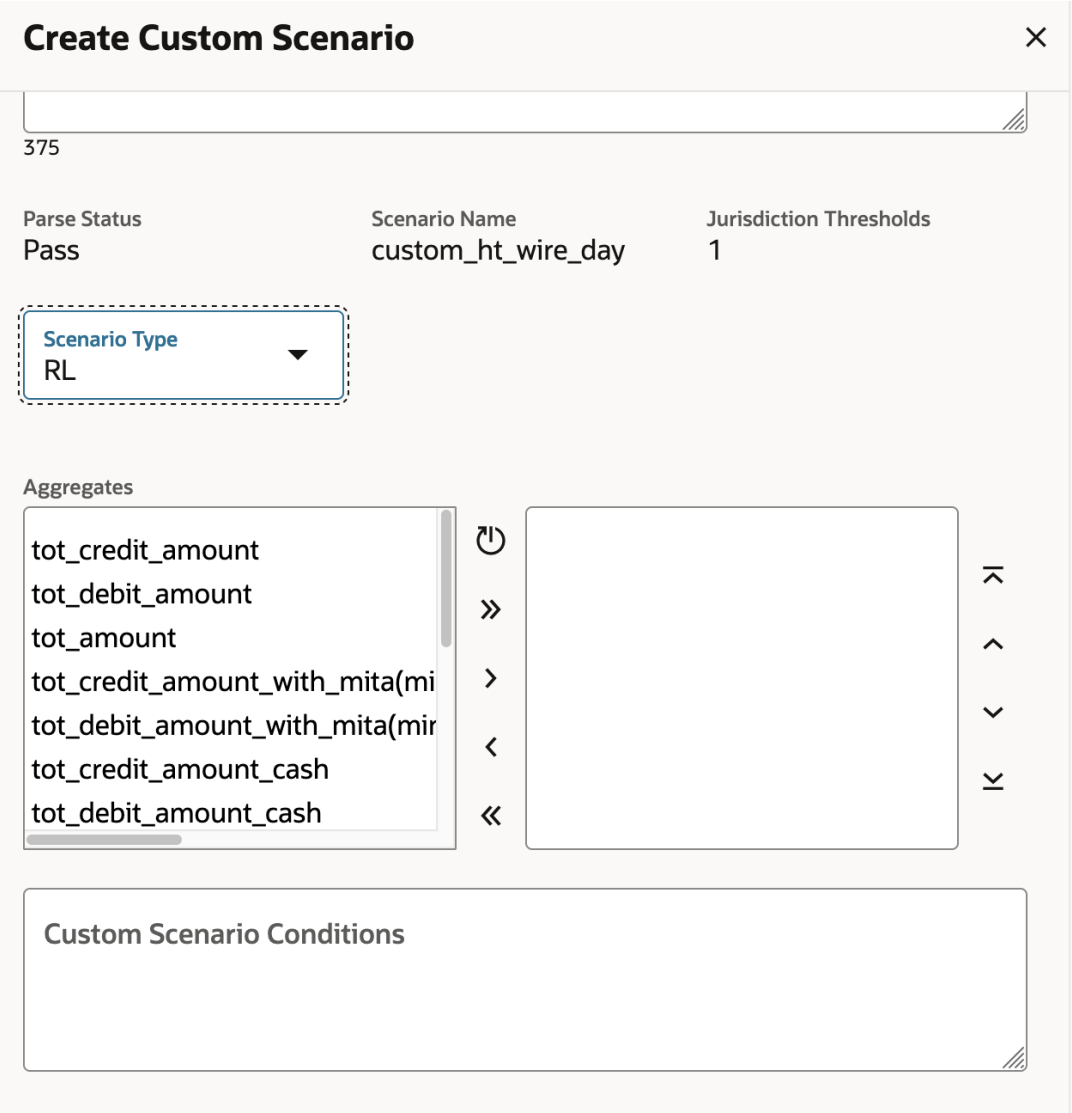
3. Click **Create Scenario**. Drag and Drop the required JSON template. The selected JSON template details are displayed.

Figure 3-21 Create Custom Scenario



4. 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.



5. Based on your selection, a relevant list of aggregates is displayed. Select and move the required aggregates to the right-hand side box.
6. 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)

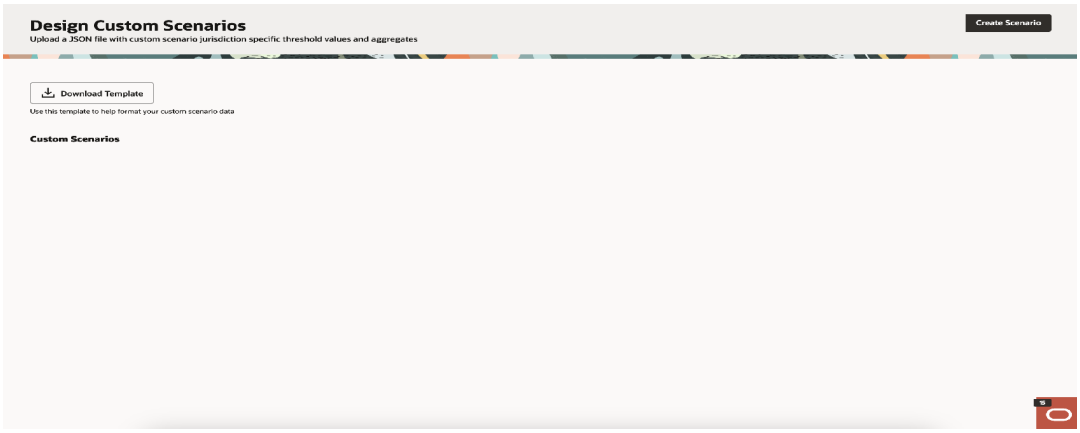
7. Click **Parse** to validate the condition. If the validation is successful, the parsing will be passed.

8. Click **Accept** to add the newly created scenario. This scenario will be listed on the Custom Scenario page.
9. If you want to modify a newly created scenario, click **Edit** and modify information based on your requirements.

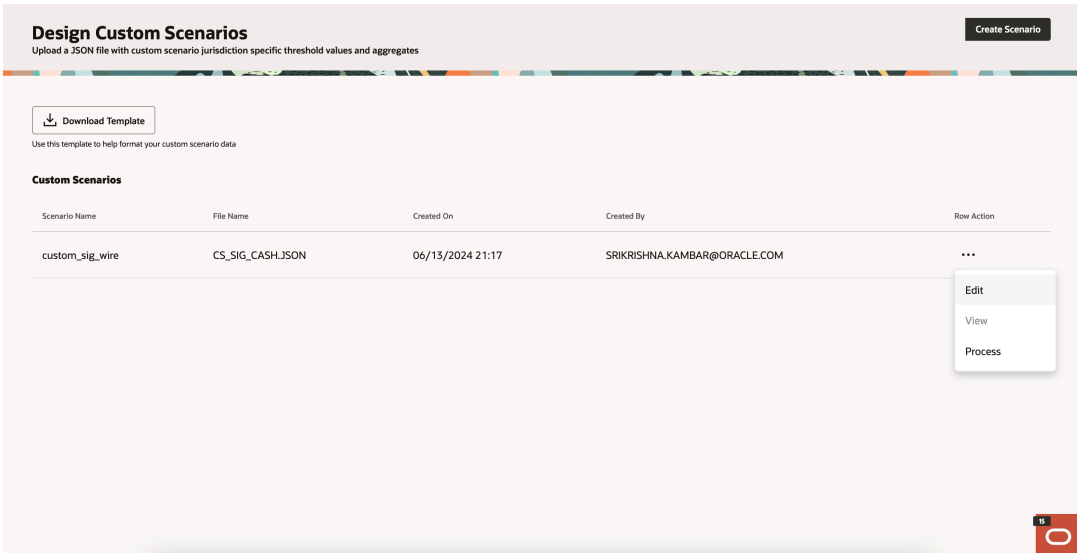
> **Note:**
>
> Once you process the scenario, you cannot edit it.

10. You can also create custom scenarios using the Oracle Ask menu.

Figure 3-22 Create Scenario Using Oracle Ask Page



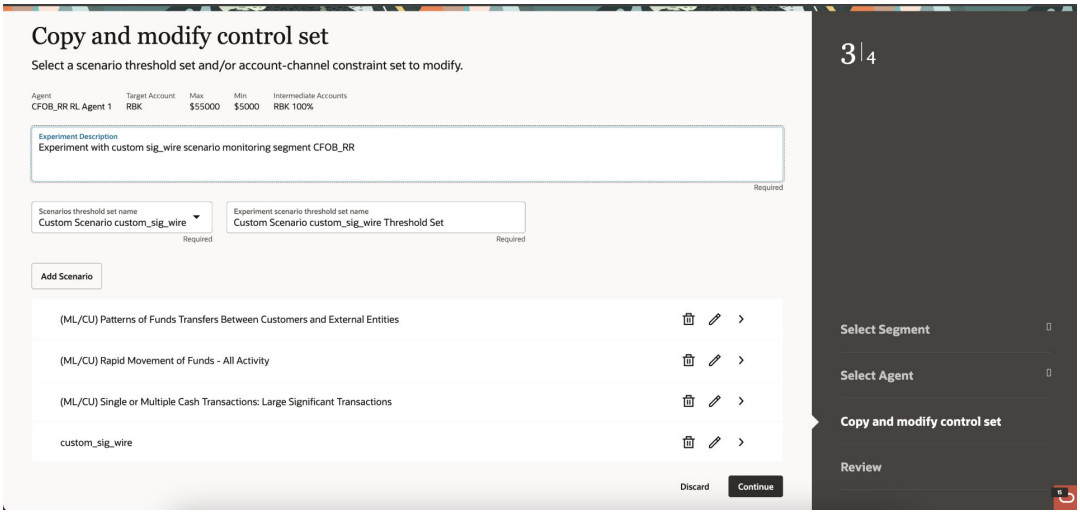
11. On the Custom Scenario page, click **Create Scenario**. The Create Scenario dialog is displayed. Repeat Step-3 to Step-9.



12. 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.



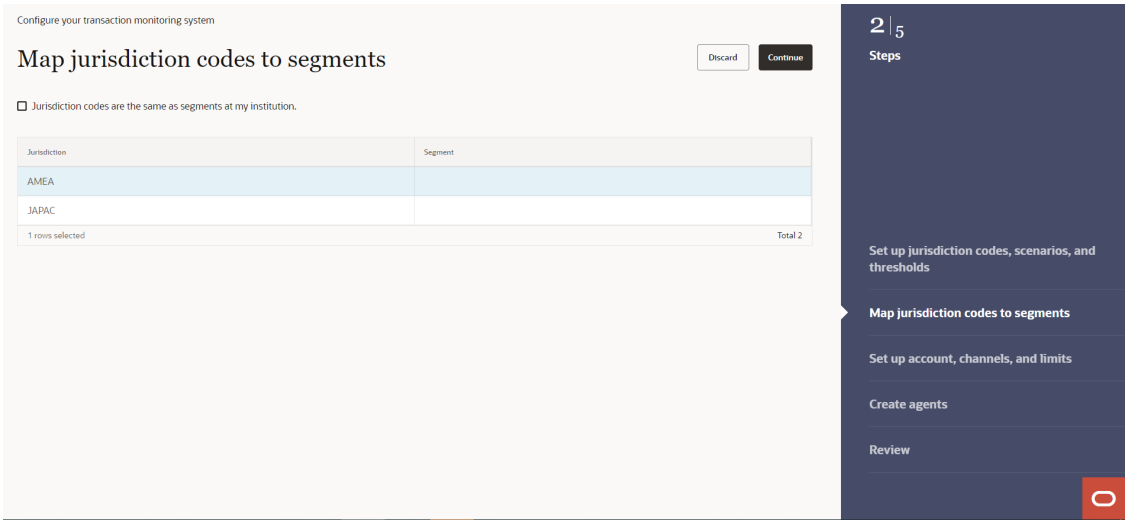
You can perform the following activities using the Row Action.

- **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.

3.2.3 Mapping Jurisdiction Codes to Segments

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

Figure 3-23 Map Jurisdiction Codes to Segments



To map jurisdiction codes to segments, follow these steps:

1. Enter the required name in the Segment field.

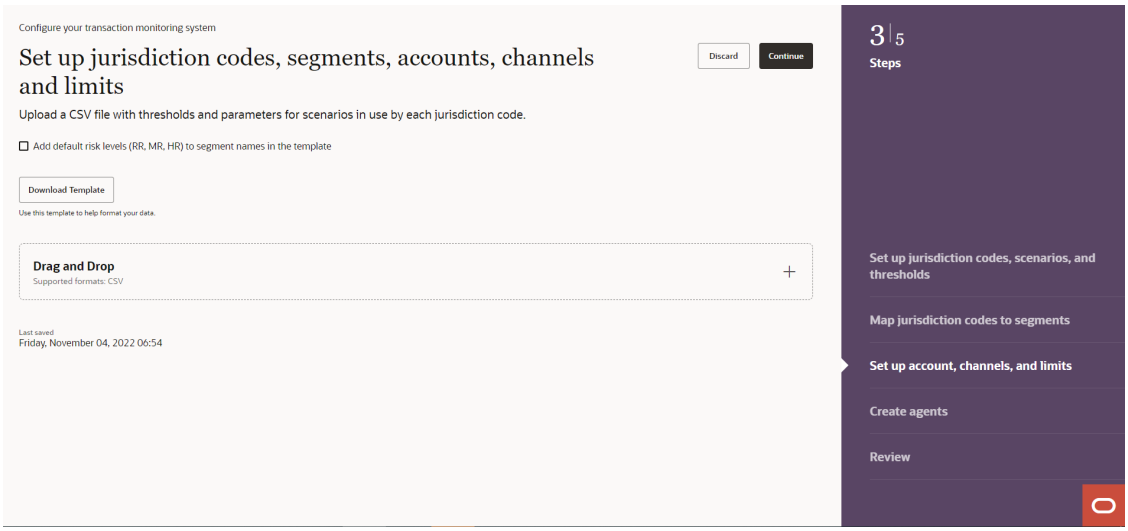
   Or Enable the checkbox jurisdiction codes are the same as segments at my institution if segments are equivalent to jurisdiction codes

2. Click **Continue** to navigate to the Setup jurisdiction codes, segments, accounts, channels and limits step.

3.2.4 Setting up Jurisdiction Codes, Segments, 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 3-24 Set up Account, Channels, and Limits



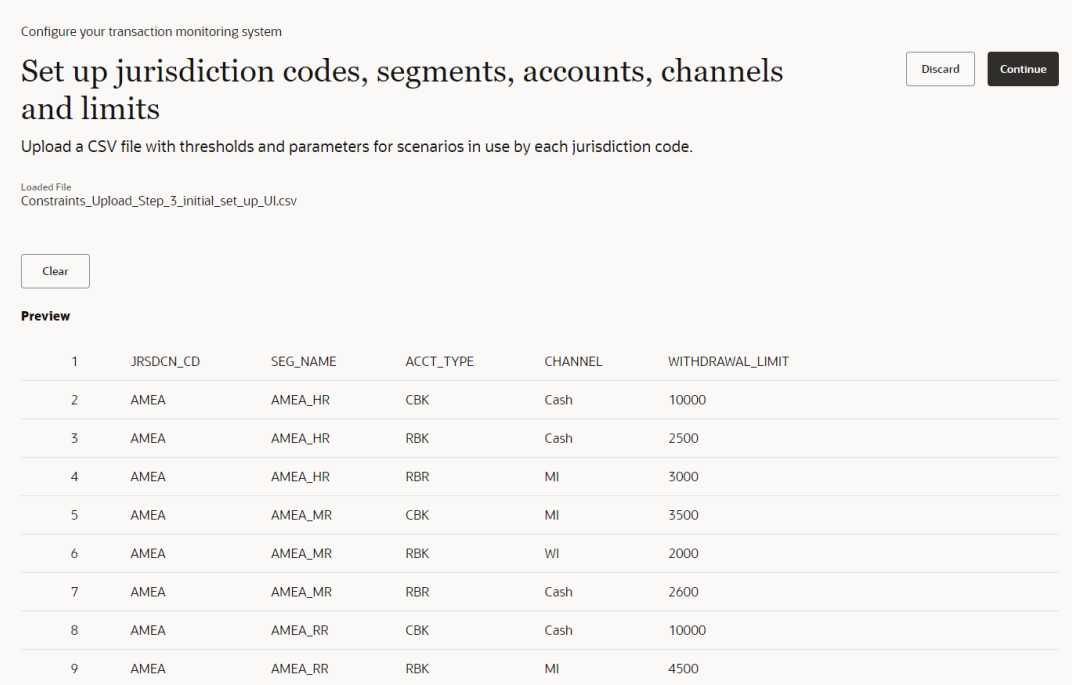
To set up an account, channels, and limits, follow these steps:

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 3-25 Uploaded CSV file to Set up Account, 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.

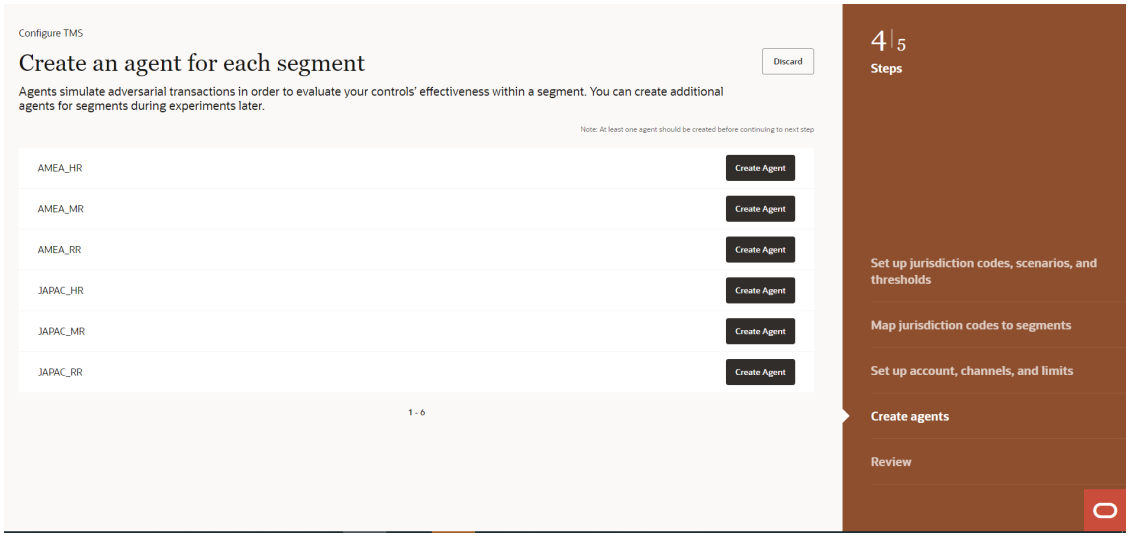
4. Click **Continue** to navigate to the Create an agent for each segment step.

3.2.5 Creating an Agent

This section describes how to create an agent for each segment. Whenever a new agent is created, by default, a Human Trafficking (HT) agent is created. You can create a new agent for the following situations:

- 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.

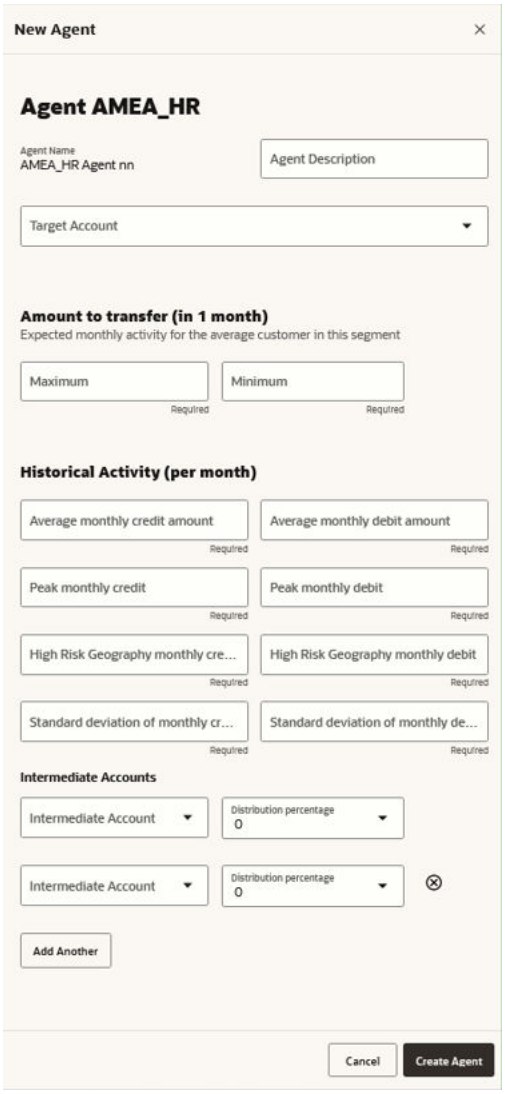
Figure 3-26 Create an Agent



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 3-27 New 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 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

> **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 How to Calculate the CIB Parameter section.

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

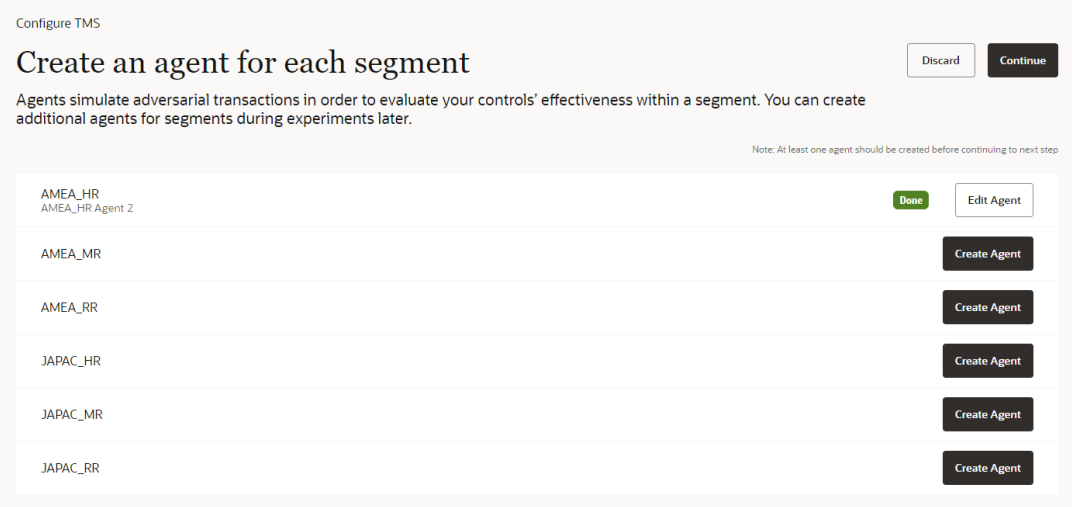
> **Note:**
>
> You can create a maximum of four intermediate accounts for each segment.

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 3-28 Agent Created



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

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

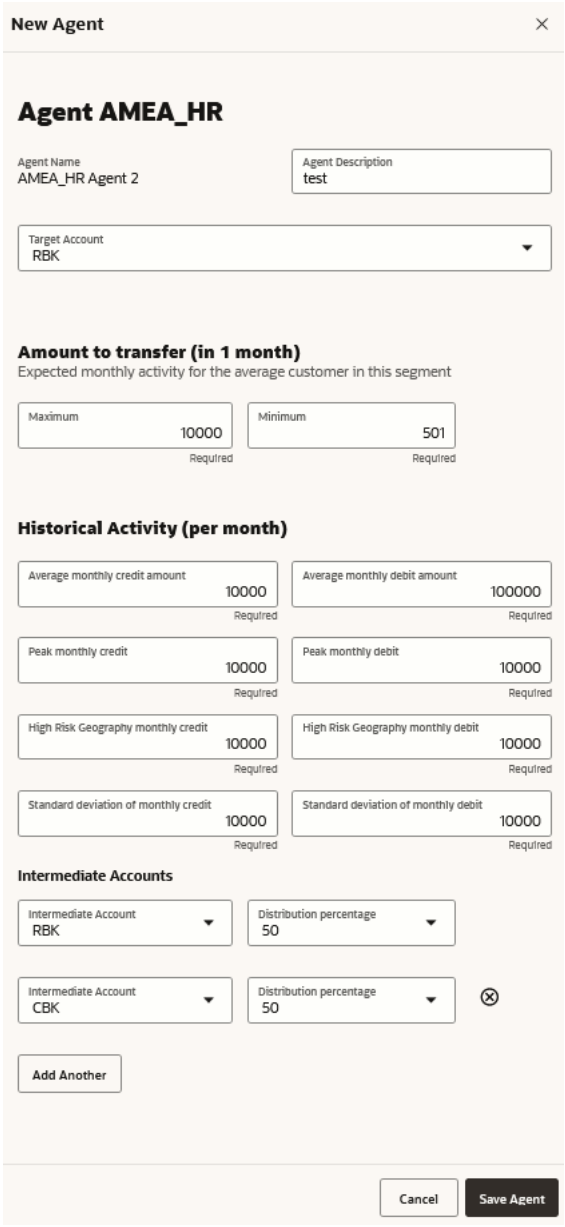
3.2.5.1 Editing An Agent

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 3-29 Edit Agent

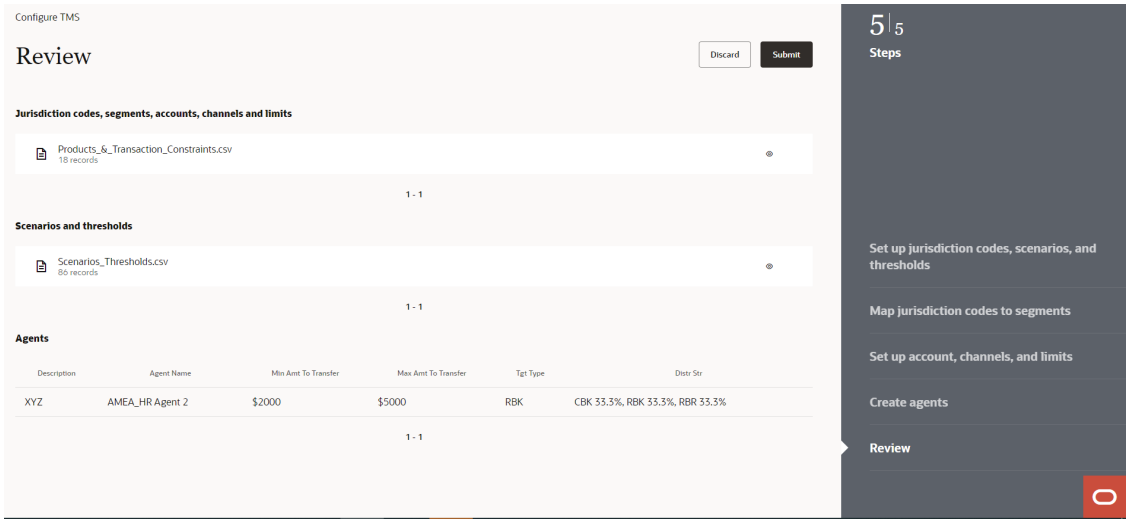


2. Click **Save Agent** to save any modifications made to the agent.

3.2.6 Reviewing Transaction Monitoring System

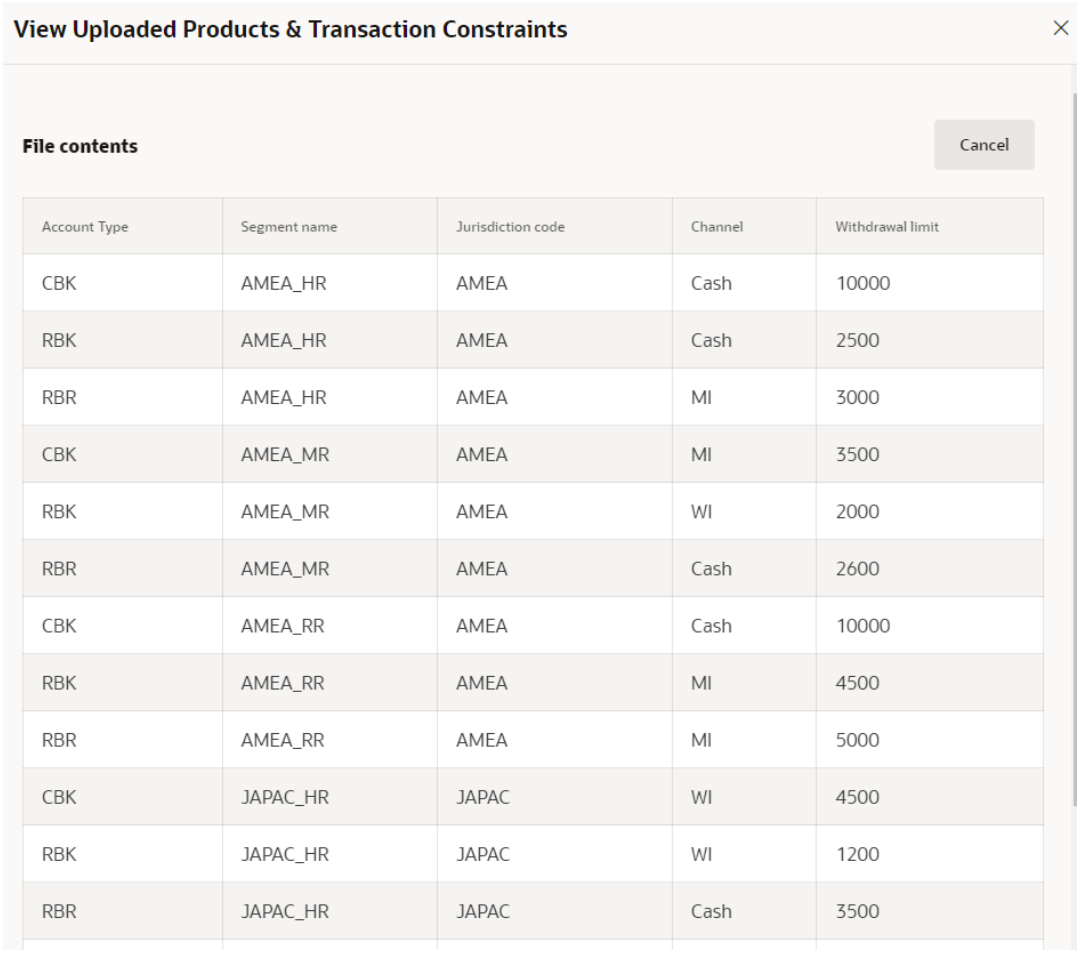
In this section, you can view the uploaded data and created agents for each of the segments.

Figure 3-30 Review the System



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

Figure 3-31 Uploaded Products and Transaction Constraints

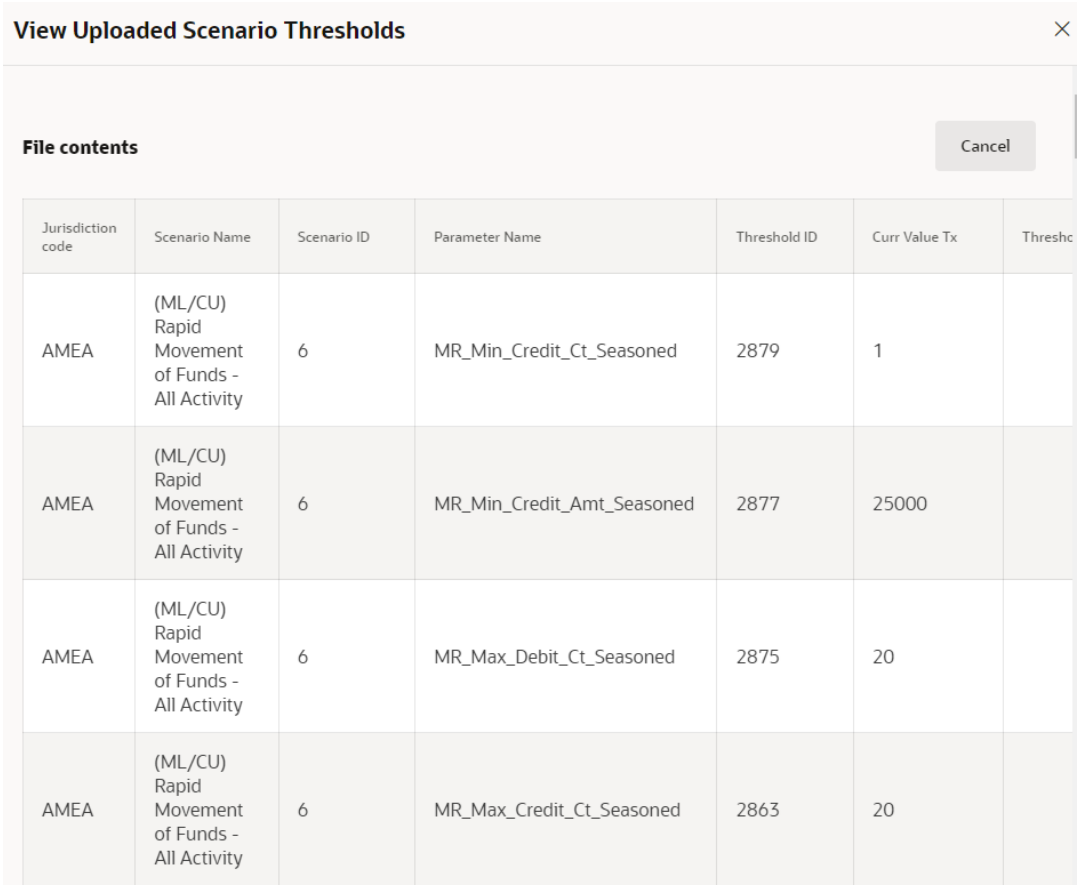


Account Type	Segment name	Jurisdiction code	Channel	Withdrawal limit
CBK	AMEA_HR	AMEA	Cash	10000
RBK	AMEA_HR	AMEA	Cash	2500
RBR	AMEA_HR	AMEA	MI	3000
CBK	AMEA_MR	AMEA	MI	3500
RBK	AMEA_MR	AMEA	WI	2000
RBR	AMEA_MR	AMEA	Cash	2600
CBK	AMEA_RR	AMEA	Cash	10000
RBK	AMEA_RR	AMEA	MI	4500
RBR	AMEA_RR	AMEA	MI	5000
CBK	JAPAC_HR	JAPAC	WI	4500
RBK	JAPAC_HR	JAPAC	WI	1200
RBR	JAPAC_HR	JAPAC	Cash	3500

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

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

Figure 3-32 Uploaded Scenario Thresholds



View Uploaded Scenario Thresholds

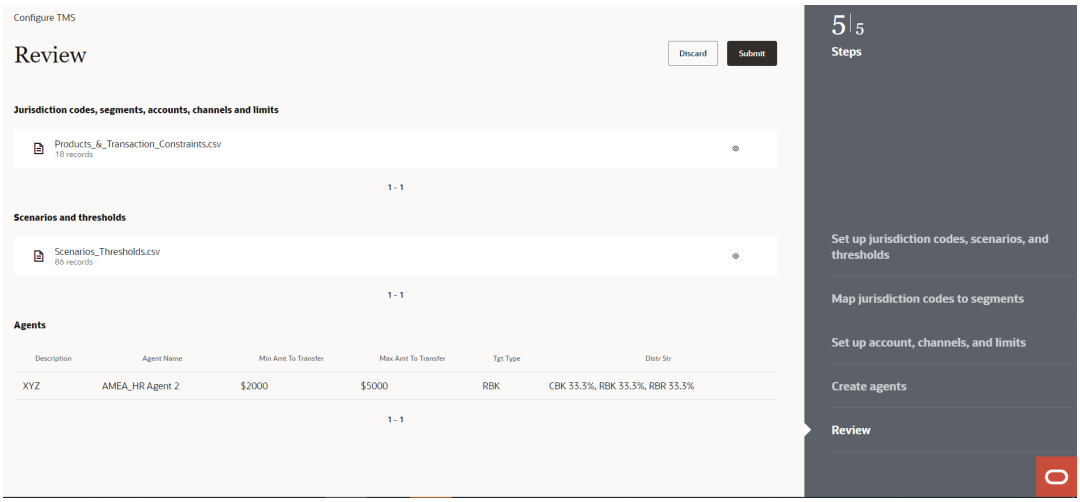
File contents

Cancel

Jurisdiction code	Scenario Name	Scenario ID	Parameter Name	Threshold ID	Curr Value Tx	Threshc
AMEA	(ML/CU) Rapid Movement of Funds - All Activity	6	MR_Min_Credit_Ct_Seasoned	2879	1	
AMEA	(ML/CU) Rapid Movement of Funds - All Activity	6	MR_Min_Credit_Amt_Seasoned	2877	25000	
AMEA	(ML/CU) Rapid Movement of Funds - All Activity	6	MR_Max_Debit_Ct_Seasoned	2875	20	
AMEA	(ML/CU) Rapid Movement of Funds - All Activity	6	MR_Max_Credit_Ct_Seasoned	2863	20	

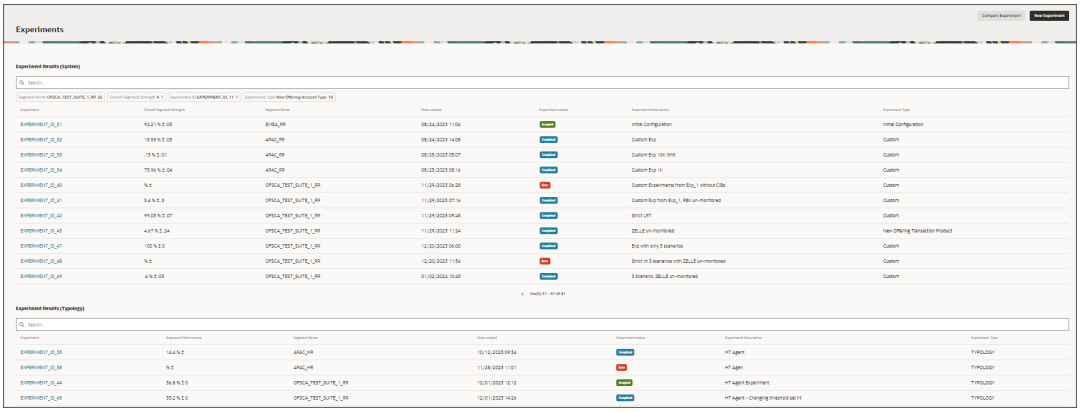
4. Click **Cancel** to exit the window.

Figure 3-33 Review the System



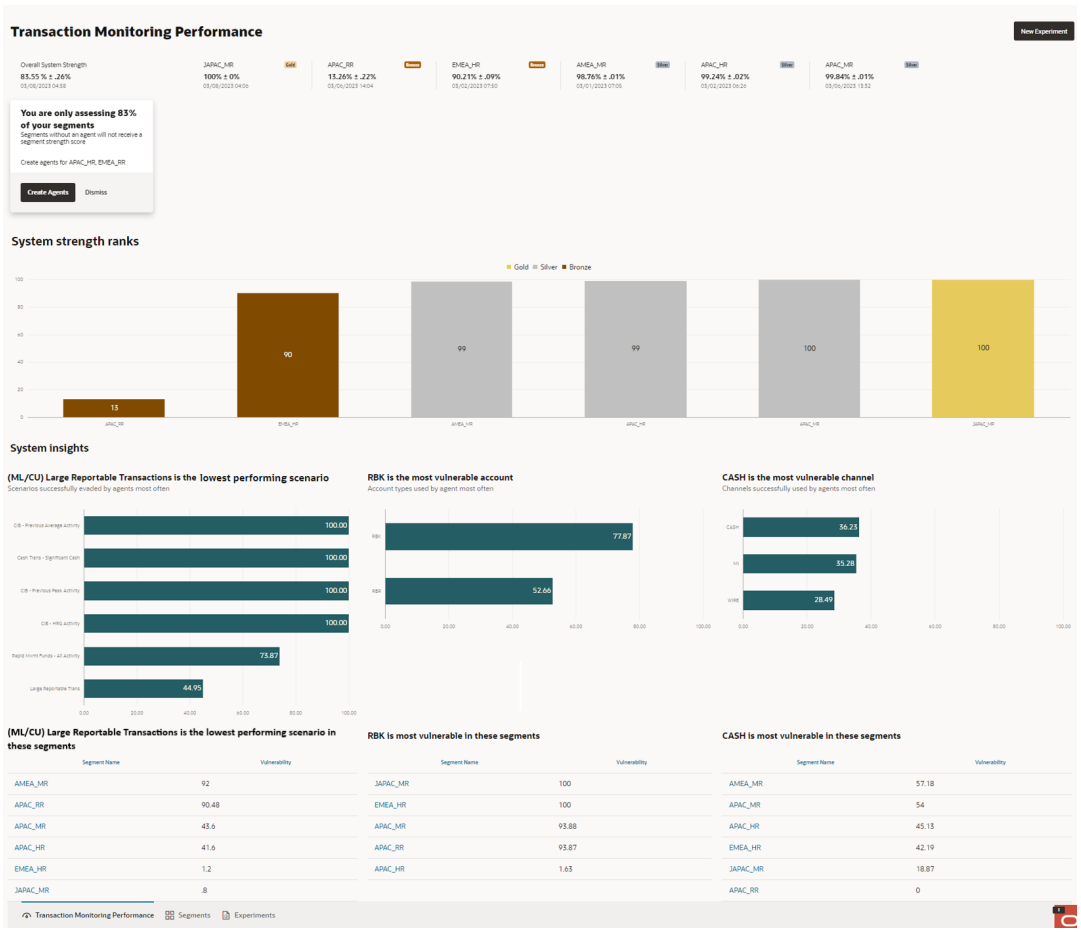
5. Click Submit to configure your transaction monitoring system. This will trigger experiment of type "Initial Set Up" for each of the segments you have configured.
6. Navigate to Experiments tab and you can view the created experiment is in In progress status as shown below:

Figure 3-34 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 3-35 Transaction Monitoring Performance



3.2.7 Resetting the Transaction Monitoring System

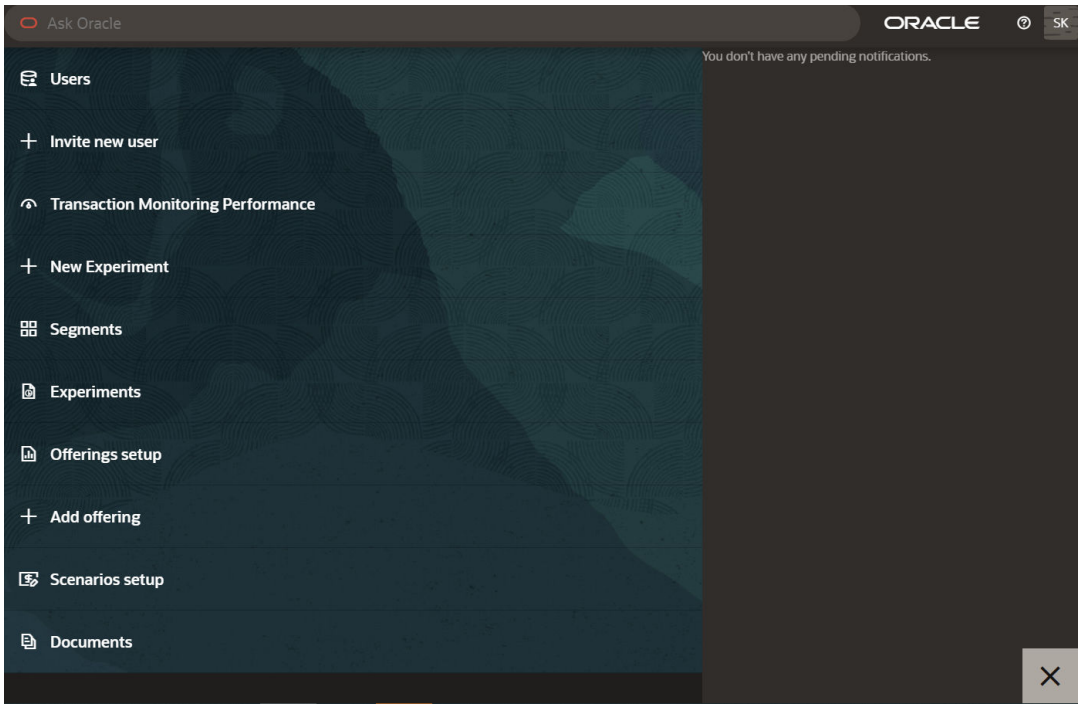
This section describes how to reset your transaction monitoring system configuration in OFSCA.

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

1. Click

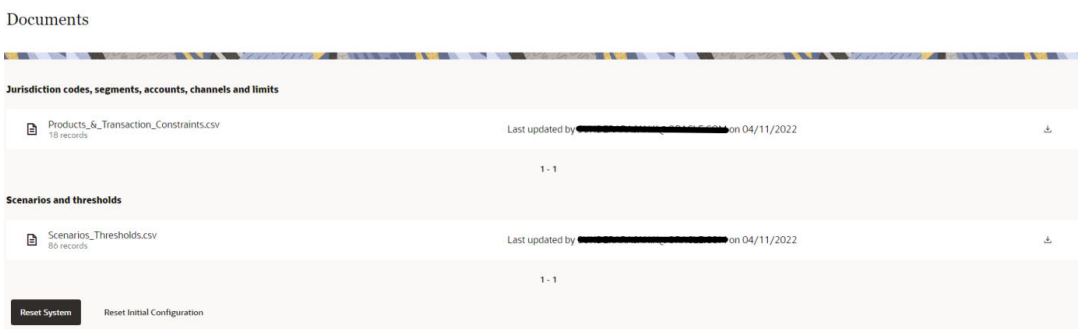
Open Ask Oracle to display the Ask Oracle window. The following window is displayed.

Figure 3-36 Application Menu



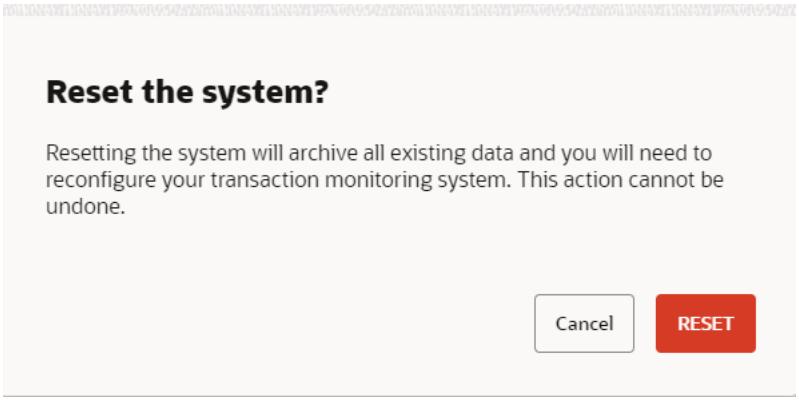
2. Click **Documents** menu to display the Documents window. The following window is displayed.

Figure 3-37 Documents Menu



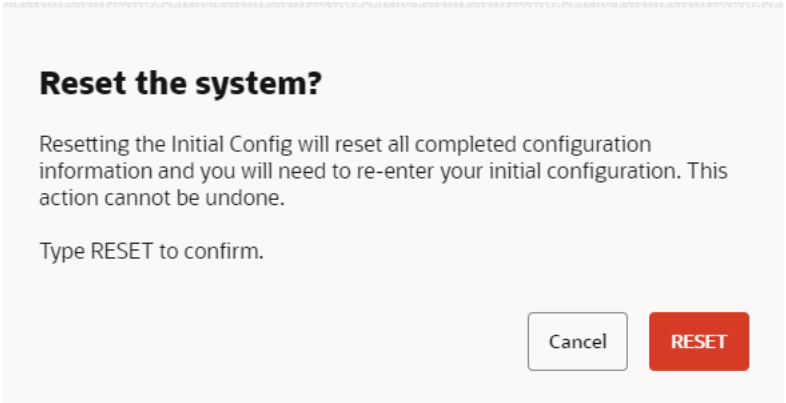
3. Click **Reset System** to reset your transaction monitoring system. The confirmation window is displayed.

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.

4

Understanding the OFSCA Dashboard

This section provides an overview of the OFSCA performance monitoring dashboard, including its components and functionalities.

Topics:

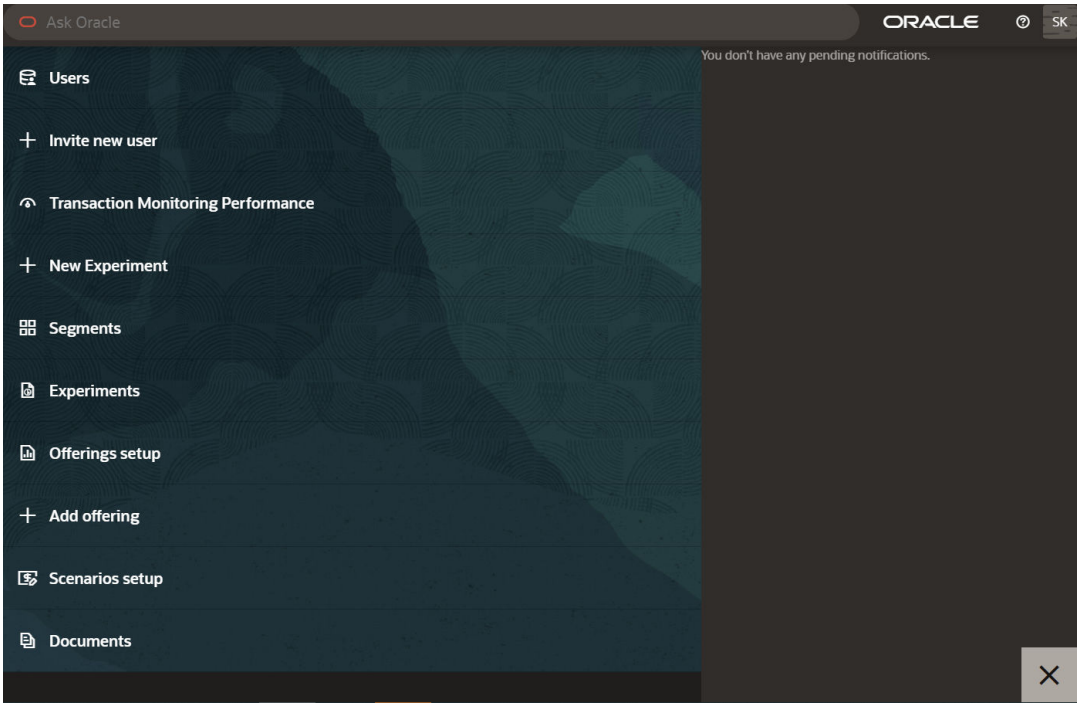
- Overall System Performance
- Segment Performance

This section describes the components available in the OFSCA performance monitoring dashboard

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

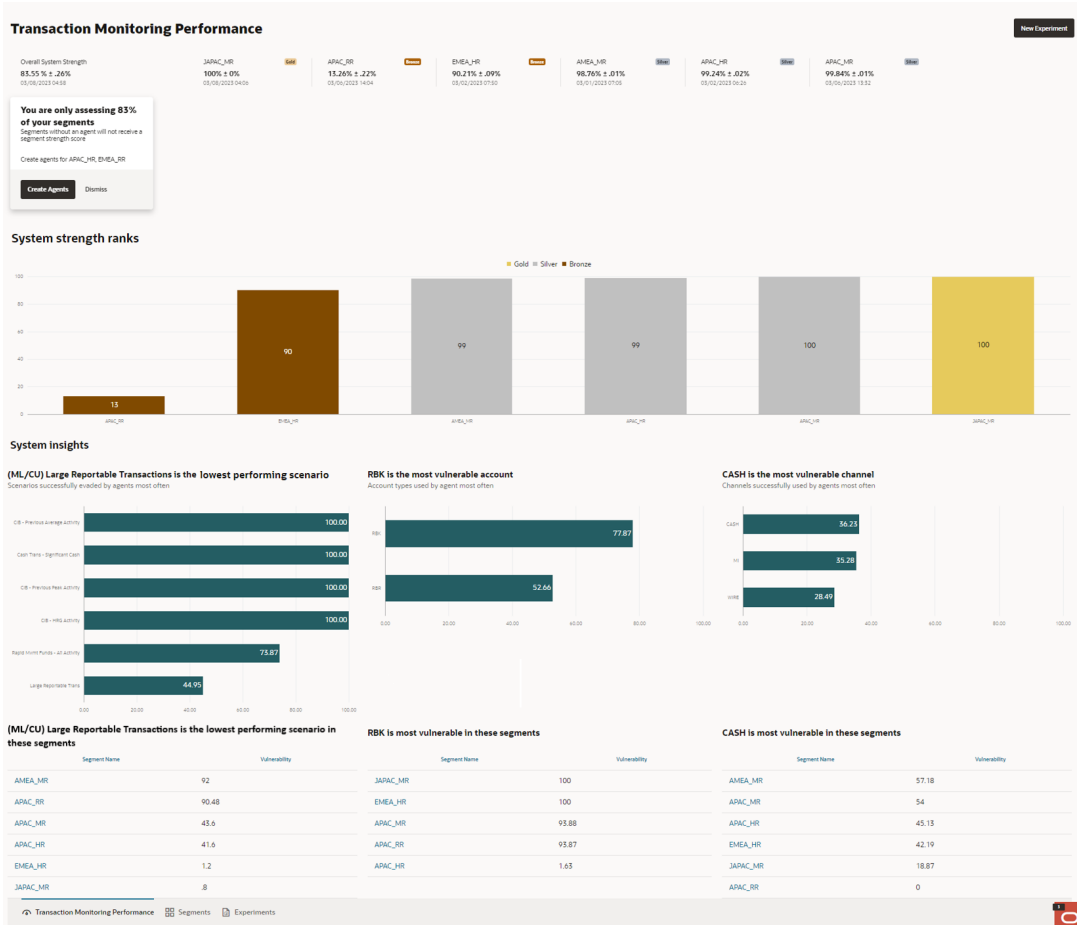
1. **Click Open Ask Oracle**  to display the Ask Oracle window. The following window is displayed.

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

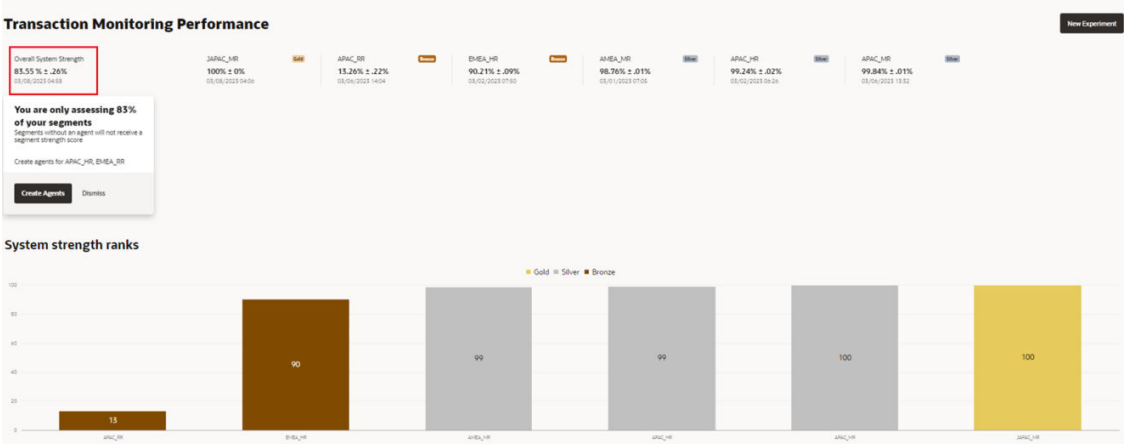


4.1 Overall System Performance

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.

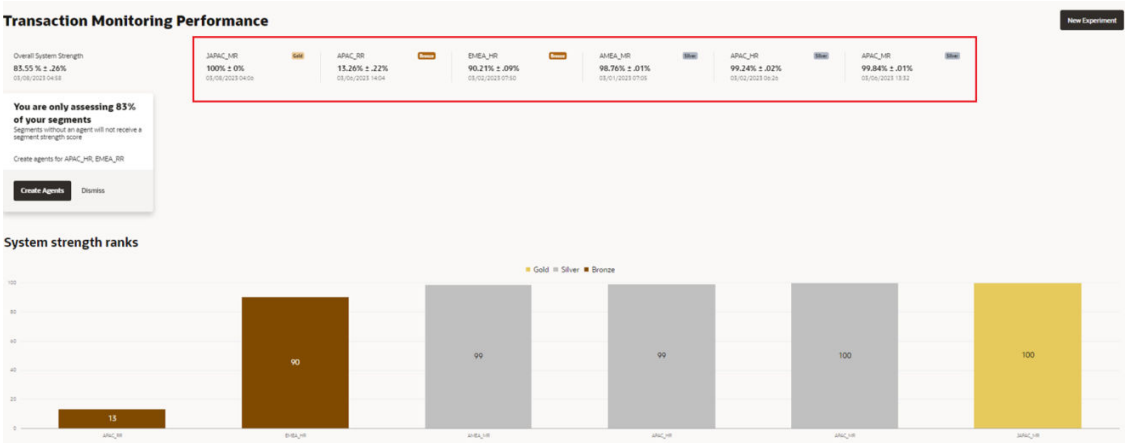
Overall System Strength: Displays the overall strength of the Transaction Monitoring System across all your institution's segments. For this metric, a higher value is preferable to a lower value.

Figure 4-3 Overall System Strength



Individual Segment Strength: Displays the strength of each individual segment

Figure 4-4 Individual Segment Strength

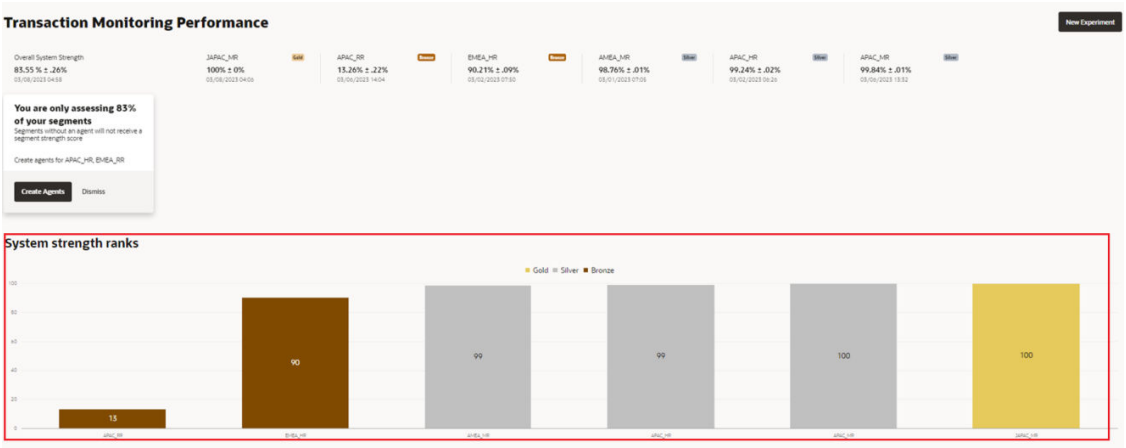


System Strength ranks: The System Strength Ranks component displays each segment's strength and confidence rankings, which can be viewed by hovering over the specific segment. Based on the performance of the TMS for a given segment, it is categorized as follows:

- **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.

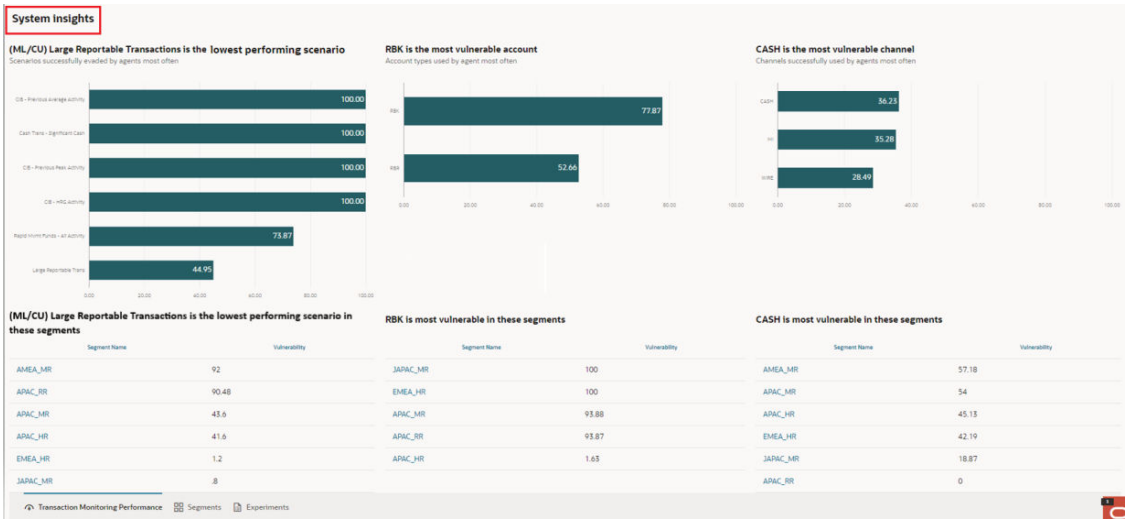
Ideally, the segments that are considered high risk by an institution should be in the gold category, while segments that are low risk can be in the bronze or silver category.

Figure 4-5 System Strength ranks



System Insights: Displays the overall system level insights.

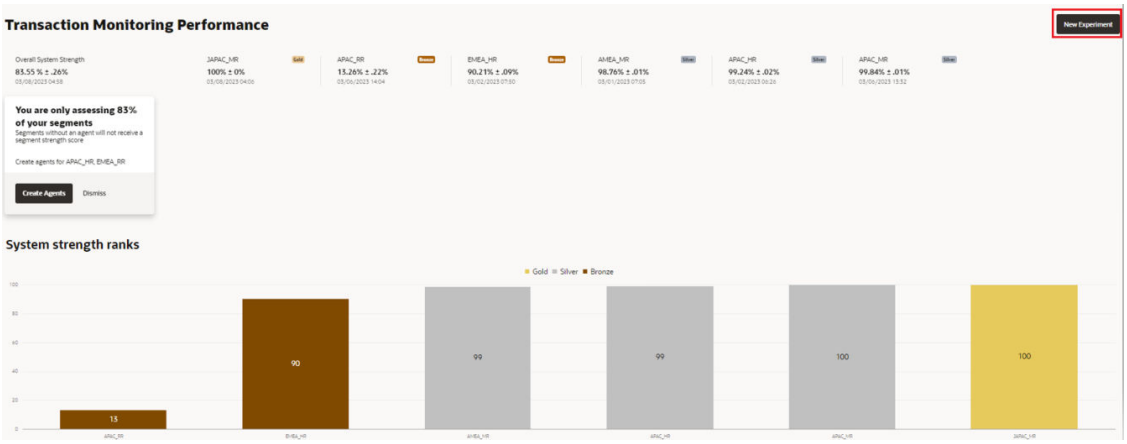
Figure 4-6 System Insights



- **<(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.

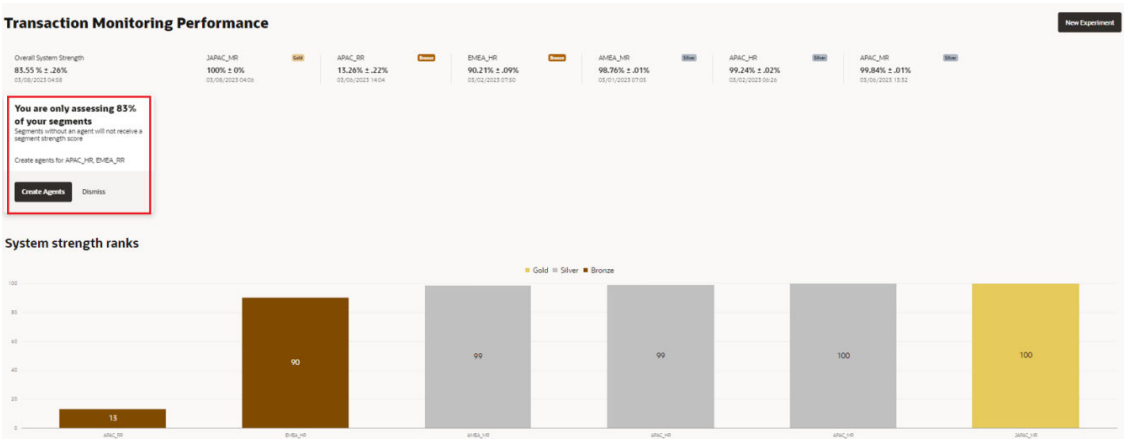
New Experiment: You can create a new user defined experiment. For more information, see the User Defined Experiment section.

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

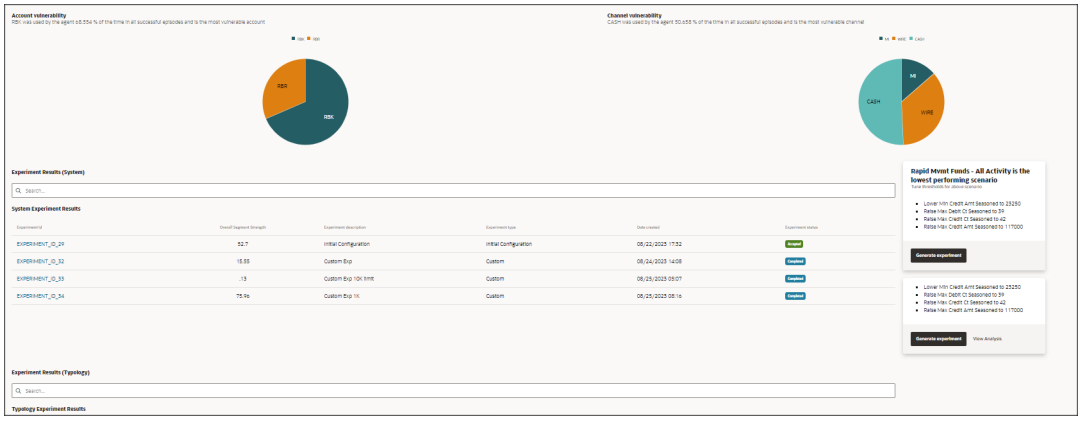


4.2 Segment Performance

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.

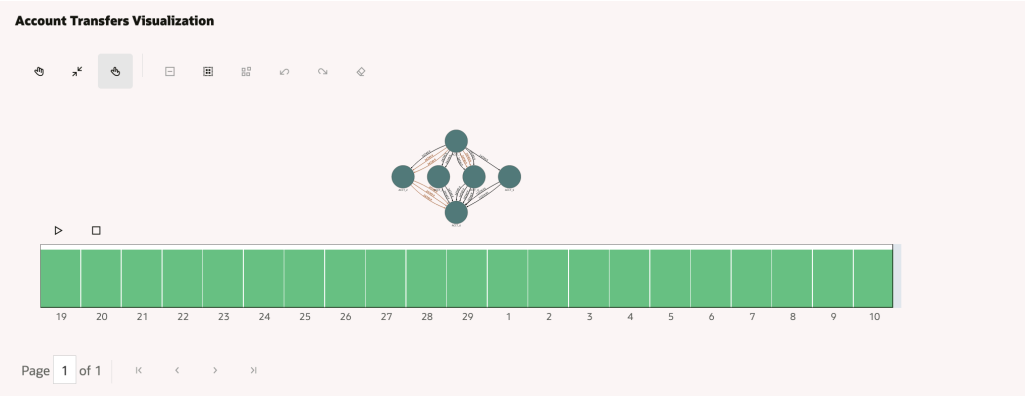
Figure 4-9 Segment Dashboard



2. 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

5.1 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.

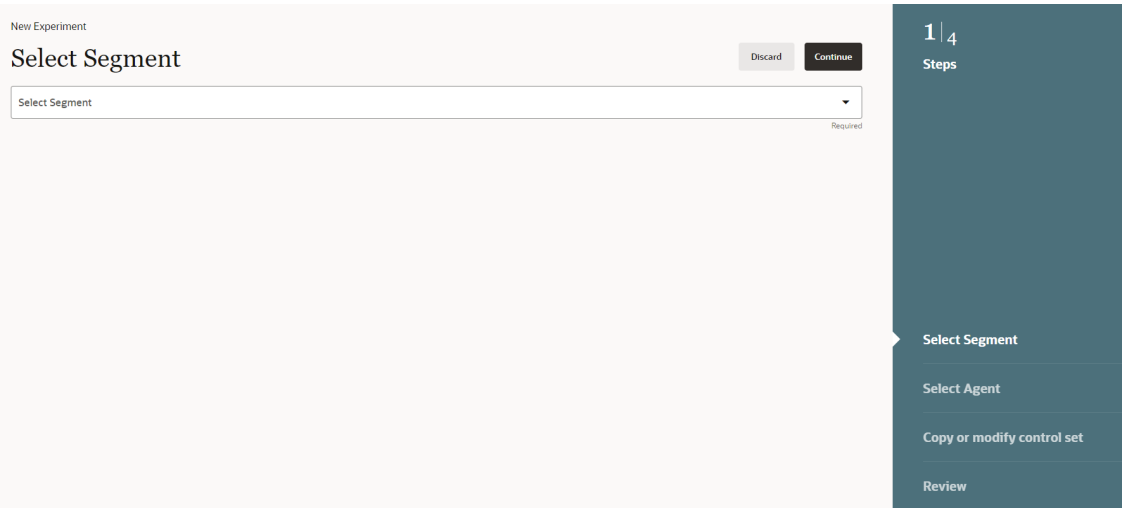
Figure 5-1 New Experiment

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.

5.1.1 Selecting the Segment

To select the segment, follow these steps:

Figure 5-2 Select Segment



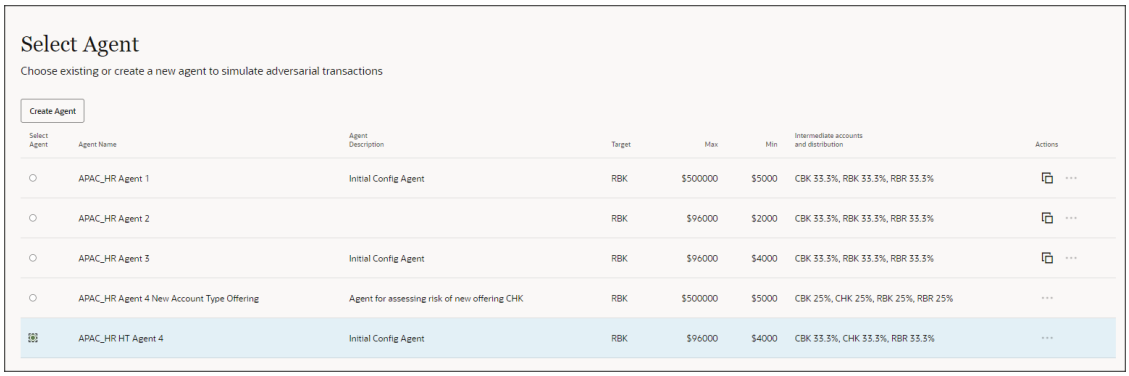
1. Select the required segment from the Select **Segment** drop-down list.
2. Click **Continue** to navigate to the Select Agent step. Or

   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.

5.1.2 Selecting an Agent

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

Figure 5-3 Select Agent



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**.

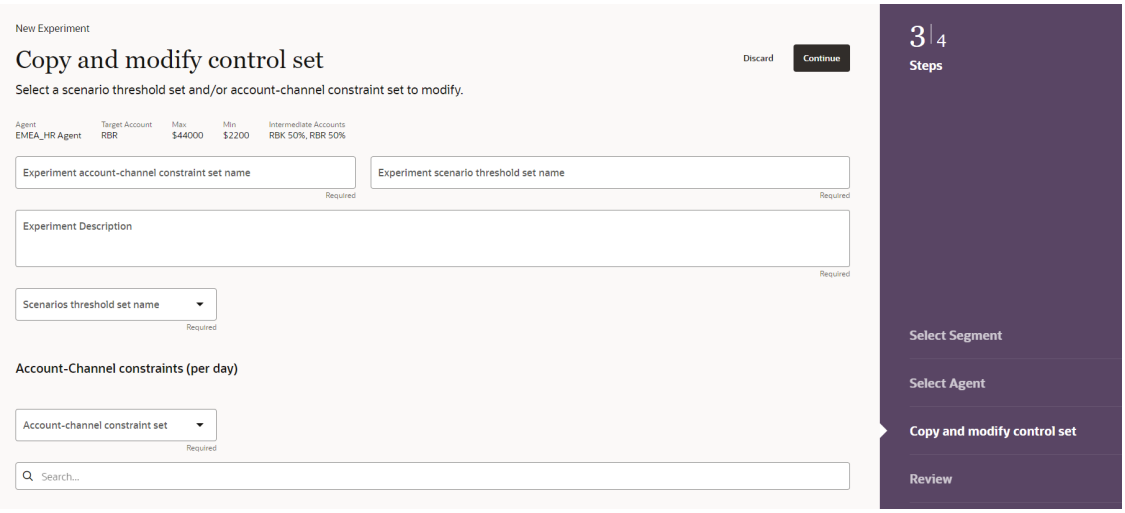
   For information about how to create an agent, see the Creating an Agent section. Once the agent is created, then select the created agent.

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

5.1.3 Copying or Modifying the Control Set

This section demonstrates how to specify the controls (scenario thresholds, account transaction product constraints) you want to evaluate in an experiment.

Figure 5-4 Copy / modify the Control Set



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.

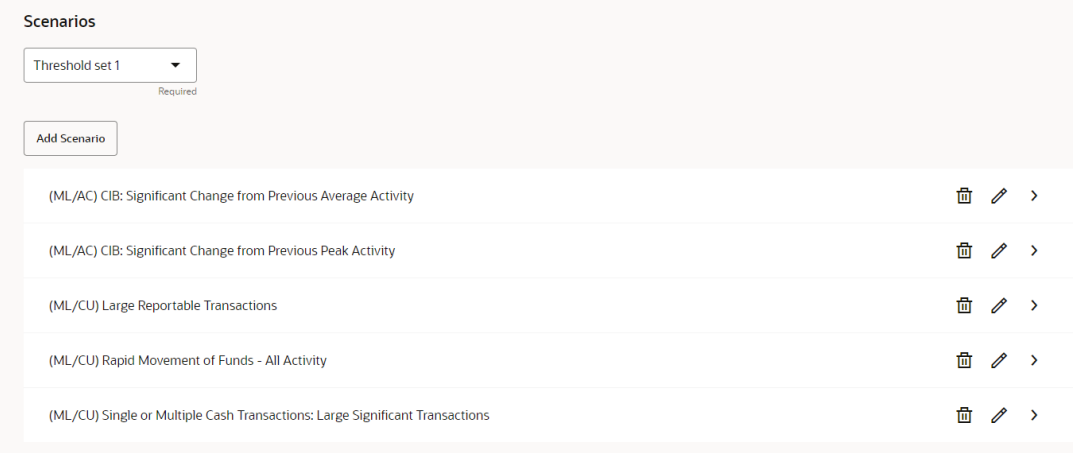
5.1.3.1 Managing Scenarios Threshold Set Name

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.

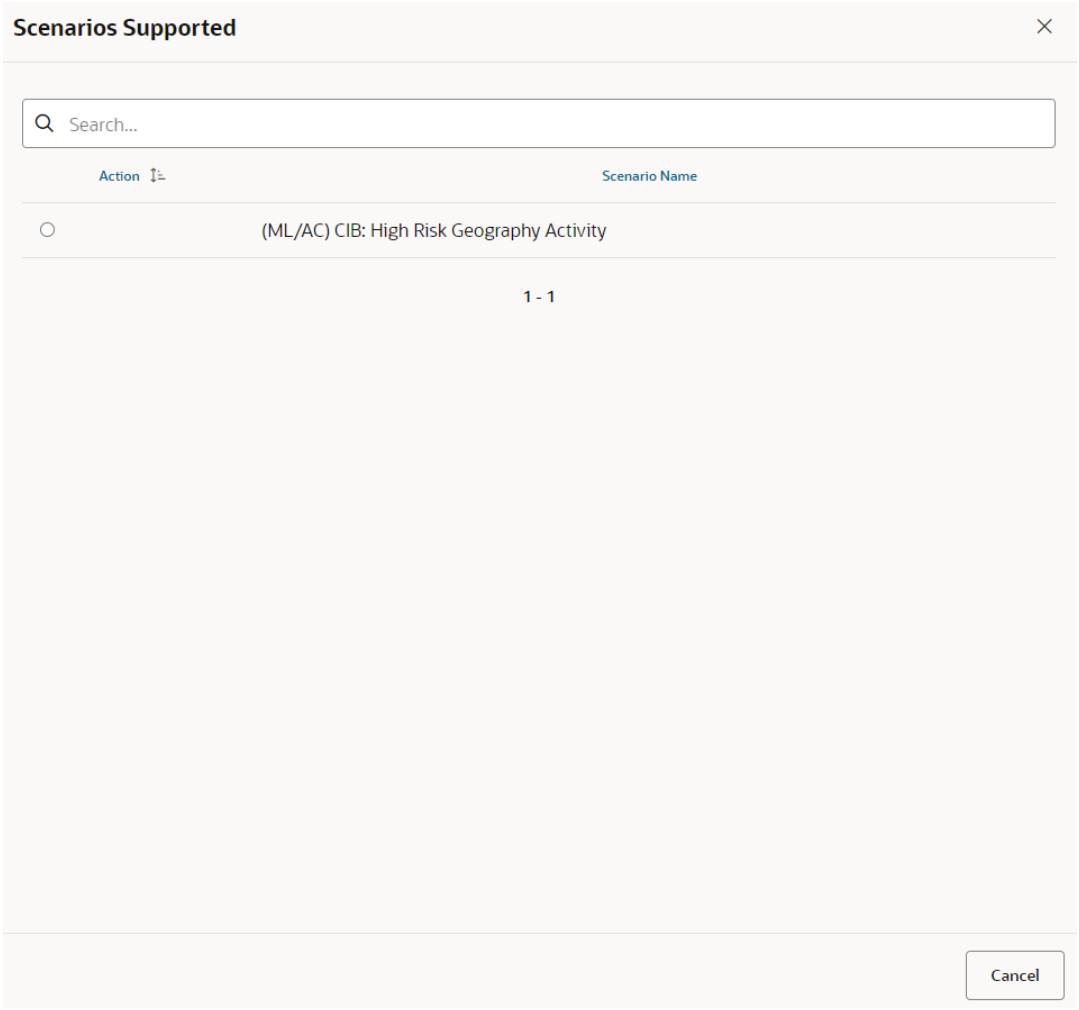
Figure 5-5 Scenario



You can perform the following:

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

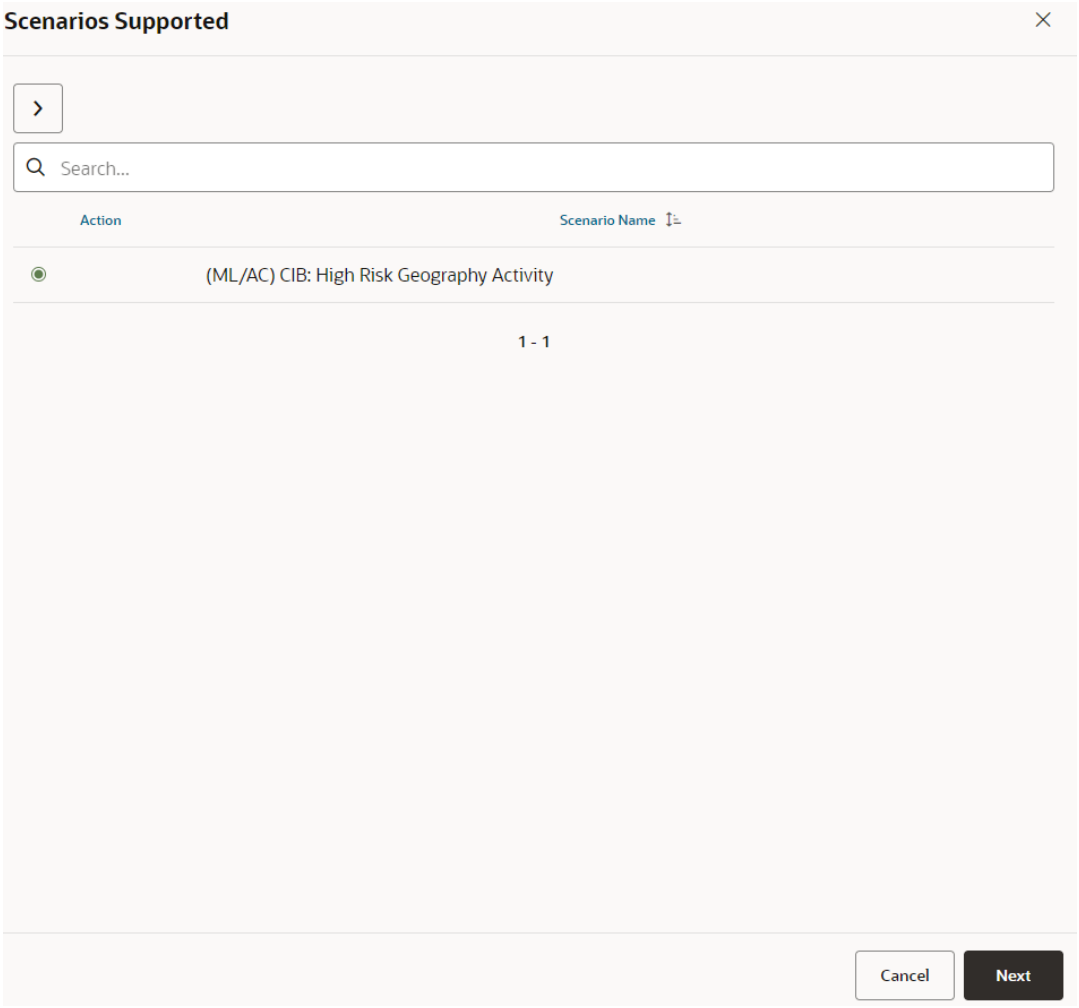
Figure 5-6 Add Scenario



a. Search the required scenario in the Search box.

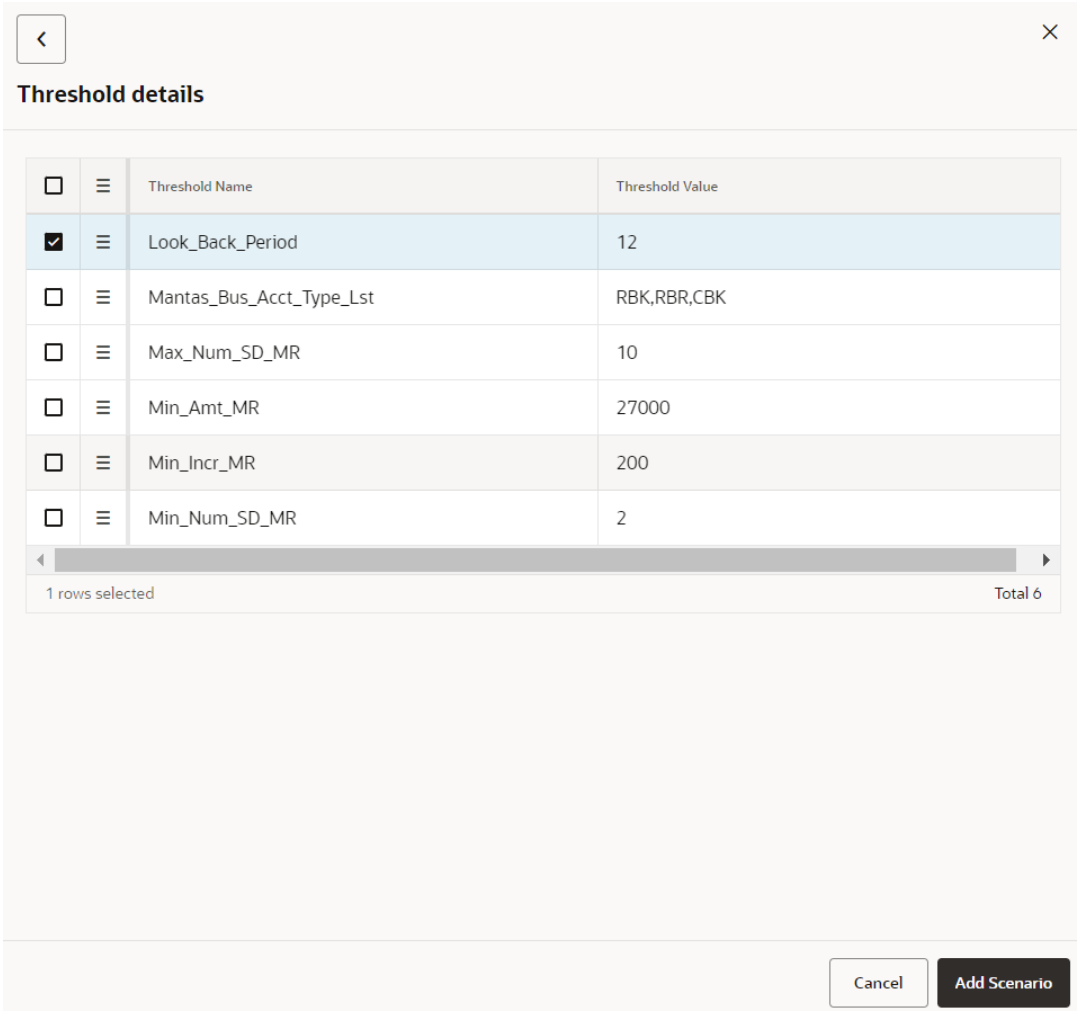
b. Click on the **Action** option of the required scenario to be added to the threshold set.

Figure 5-7 Selected Scenario



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

Figure 5-8 Threshold Details



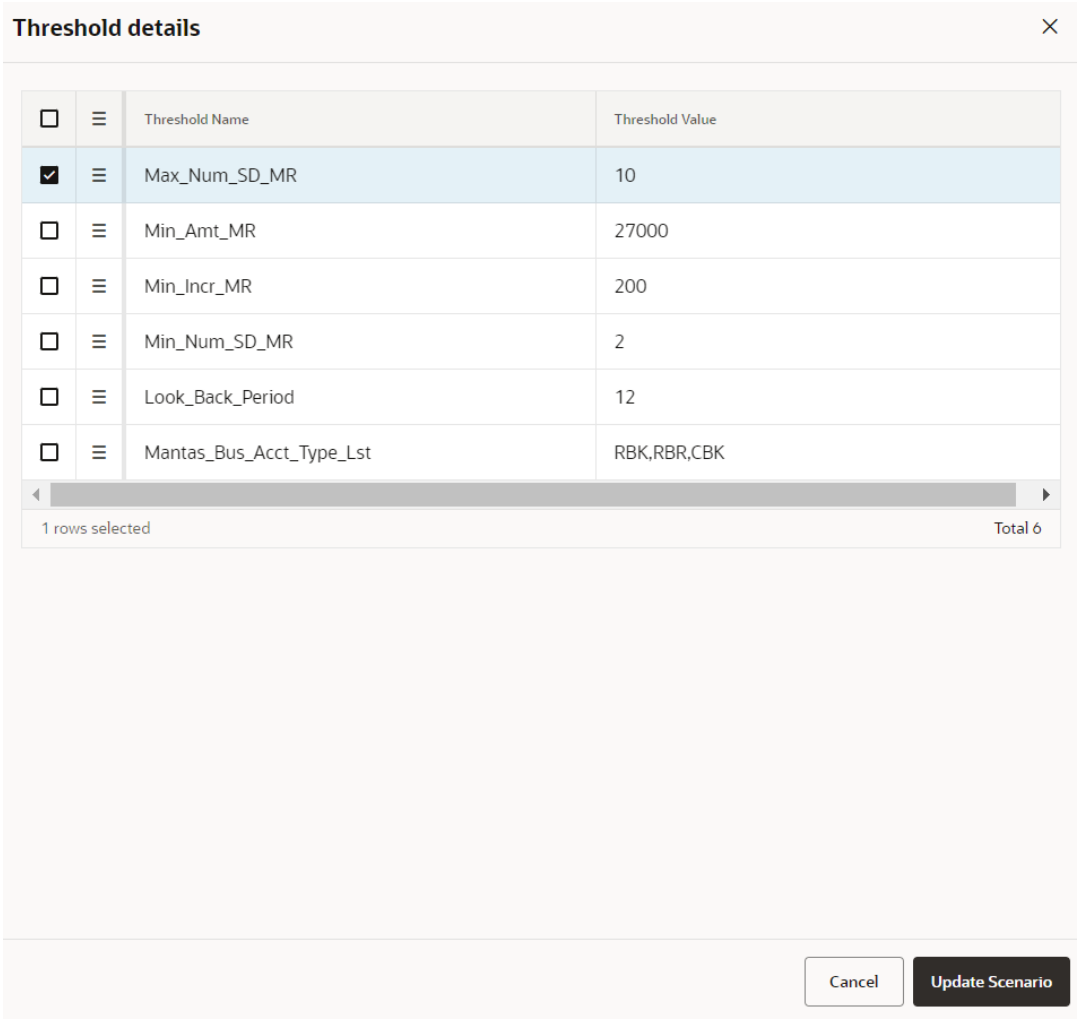
a. Double-click on the required Threshold Value field and then edit the threshold value.

b. Click **Add Scenario**. The scenario is added to the respective threshold set.

4. Click **Delete** icon to delete the selected scenario.

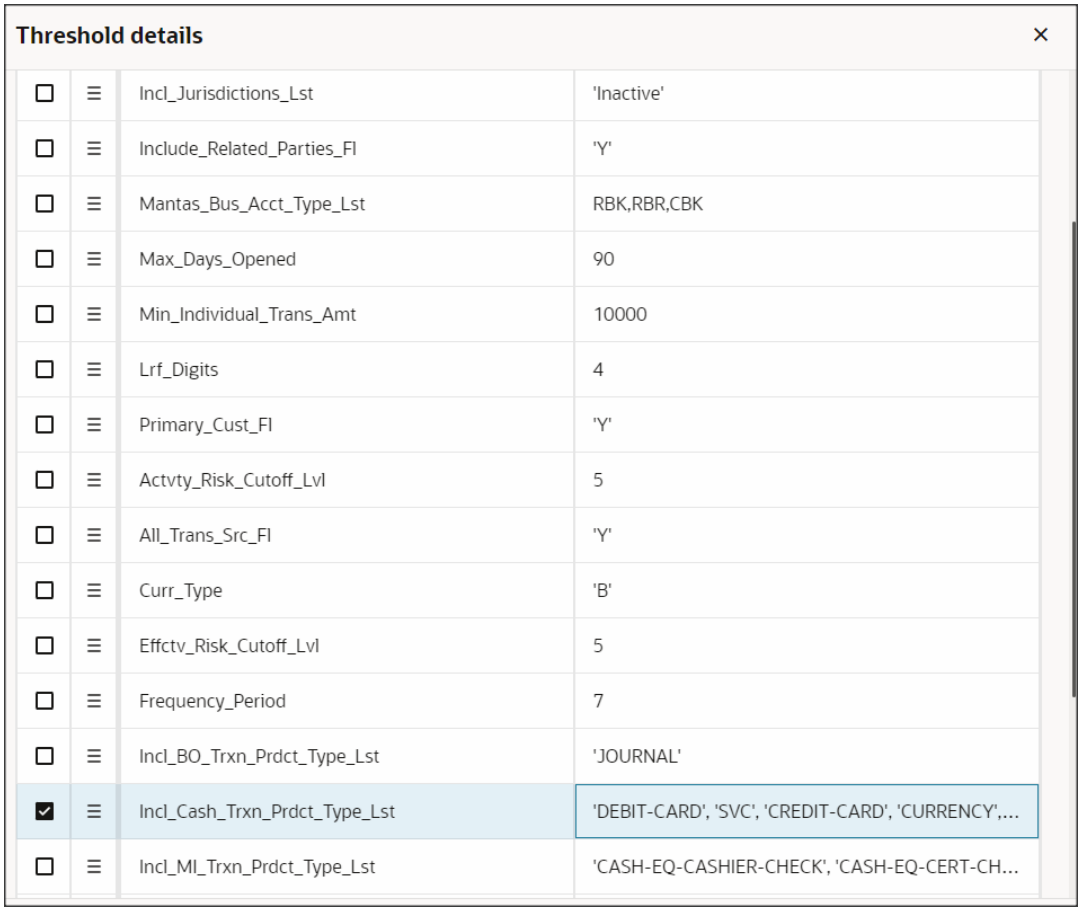
5. Click **Edit** icon to edit the selected scenario. The following window is displayed.

Figure 5-9 Edit a Scenario



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

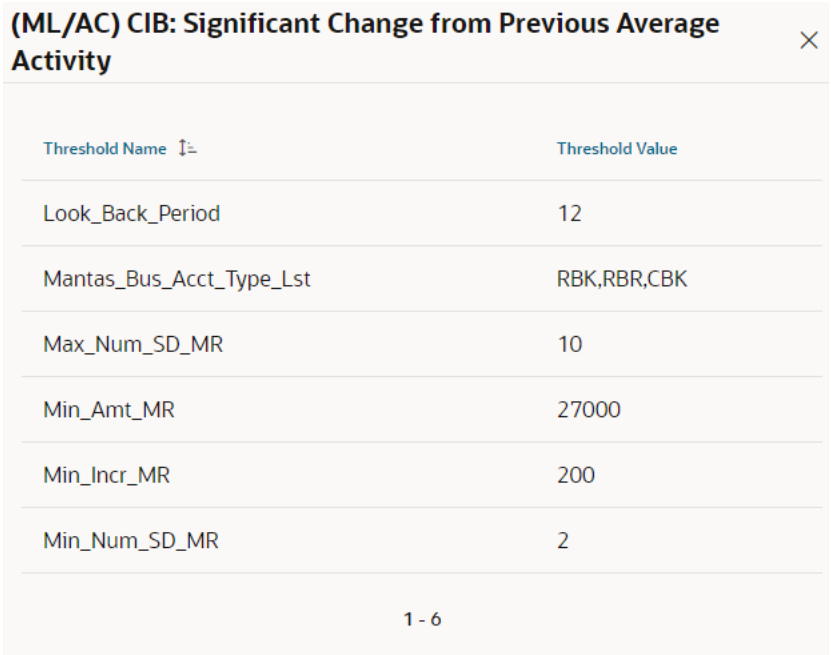
Figure 5-10 Threshold Value



a. Click **Update Scenario** to modify the information

6. Click **Navigation** › icon to view the scenario information as follows:

Figure 5-11 Scenario Information

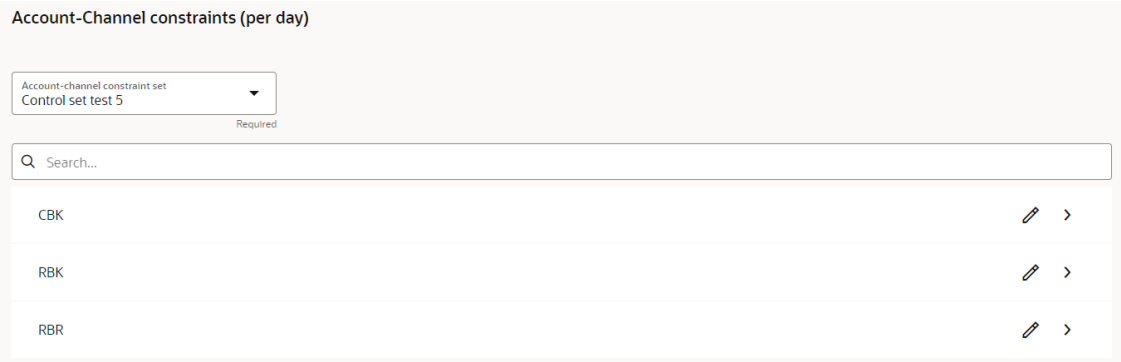


5.1.3.2 Managing Account-Transaction Product Constraints (per day)

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.

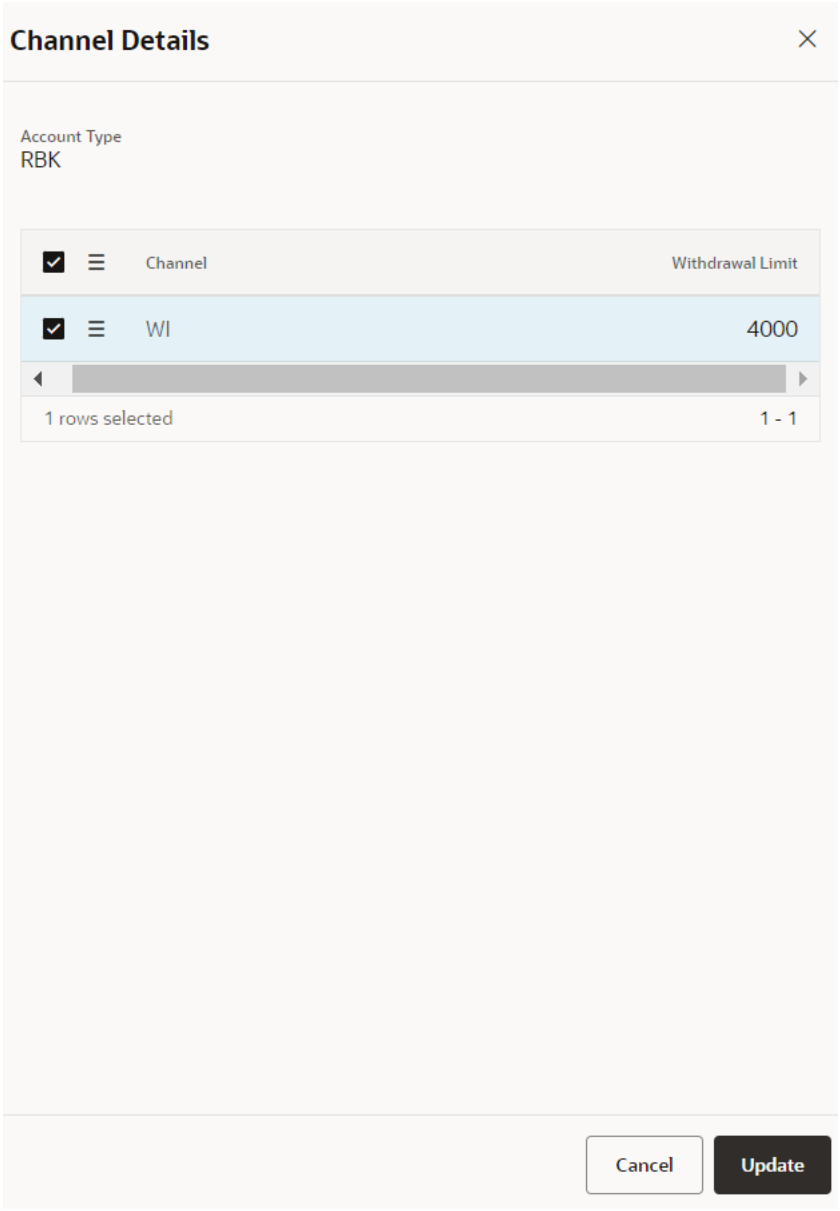
Figure 5-12 Account-transaction product constraint set



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

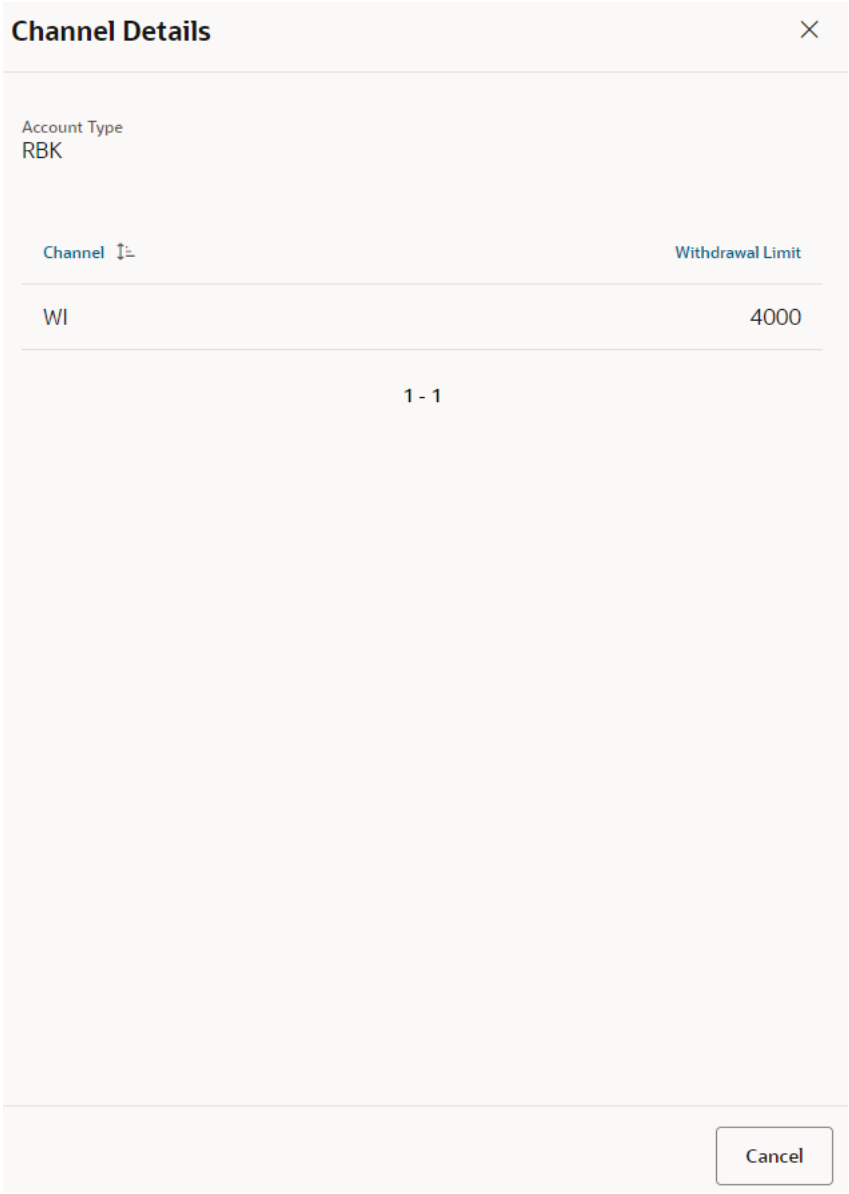


a. Double-click on the **Withdrawal Limit** field and edit the required value.

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



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

5.1.4 Monitoring New Offerings

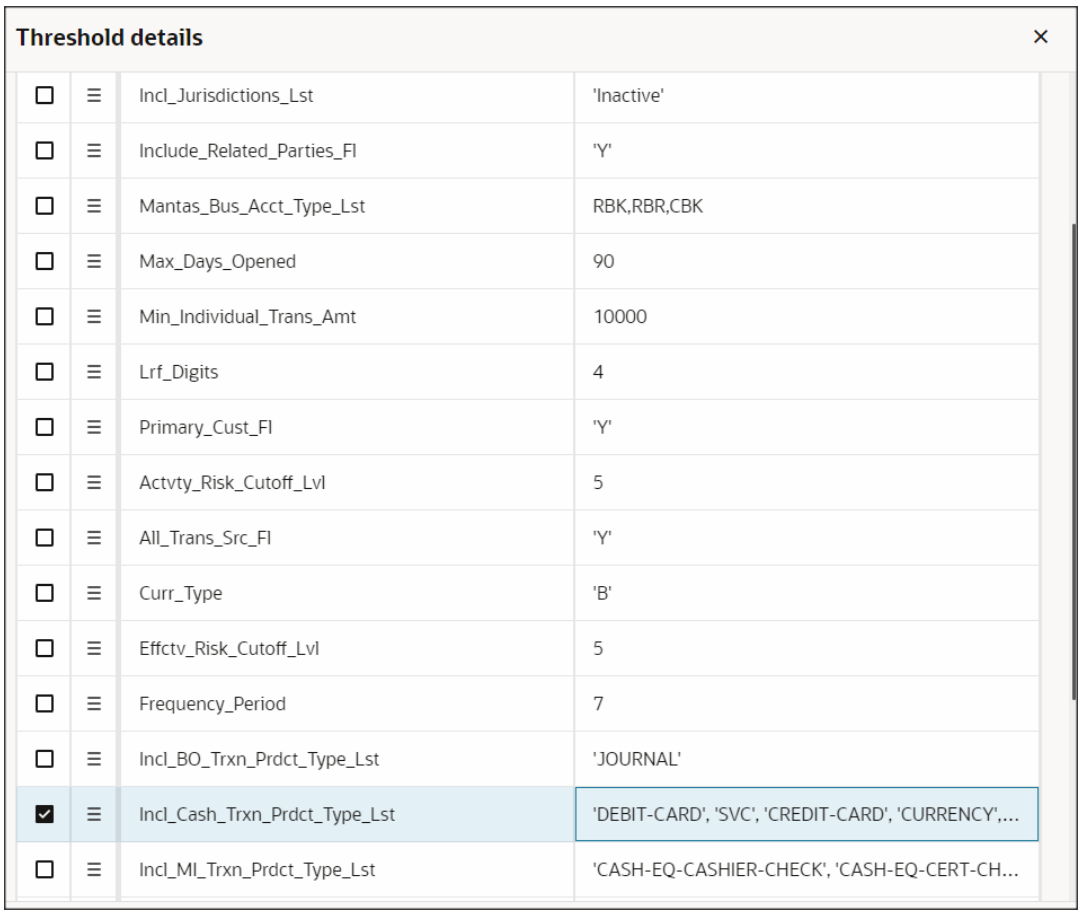
Use this section to modify the threshold value for the newly added offerings (Account Type and transaction product). For more information on how to add a new offering (Account Type or transaction product), see Modifying the System.

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.

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

Figure 5-15 Threshold Details Window

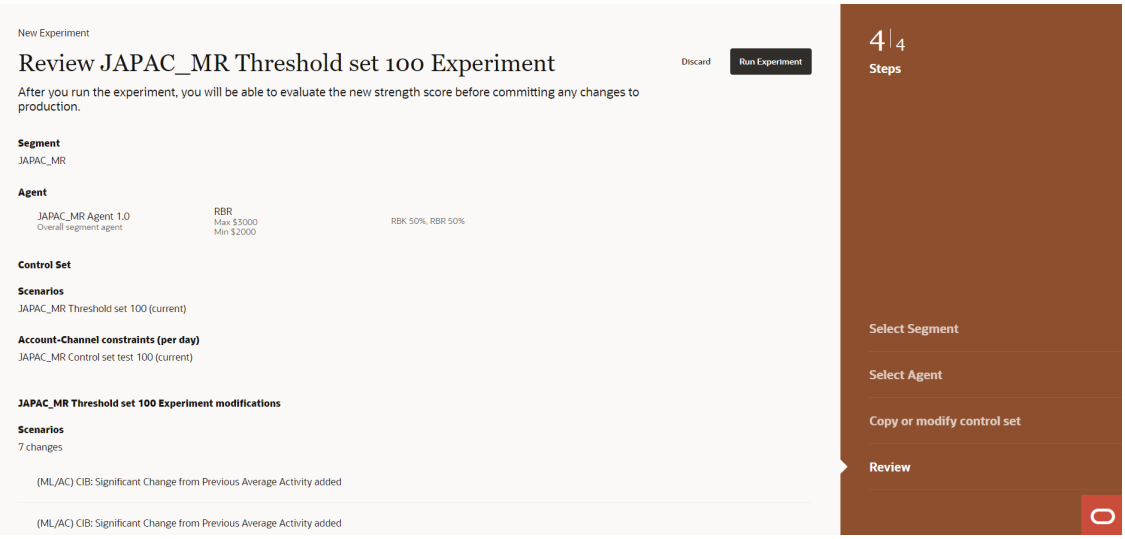


4. Double-click on the required Threshold Value field and then edit the threshold value.
5. When a new offering (account type) is added, you can append the name of new account type to list in Mantas_Bus_Acct_Types_Lst.
6. When a new transaction product is added to system, you can append the name of that transaction product to the value of one of the following thresholds.
   - Incl_Cash_Trxn_Prdct_Type_Lst - If new Product is mapped to Cash transaction product.
   - Incl_MI_Trxn_Prdct_Type_Lst - If new Product is mapped to MI transaction product.
   - Incl_Wire_Trxn_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_Trxn_Prdct_Type_Lst - If new Product is mapped to BO transaction product.
7. Click **Update Scenario** to modify the information.

5.1.5 Reviewing the Experiment

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

Figure 5-16 Review Experiment



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.

5.1.5.1 Segment Strength

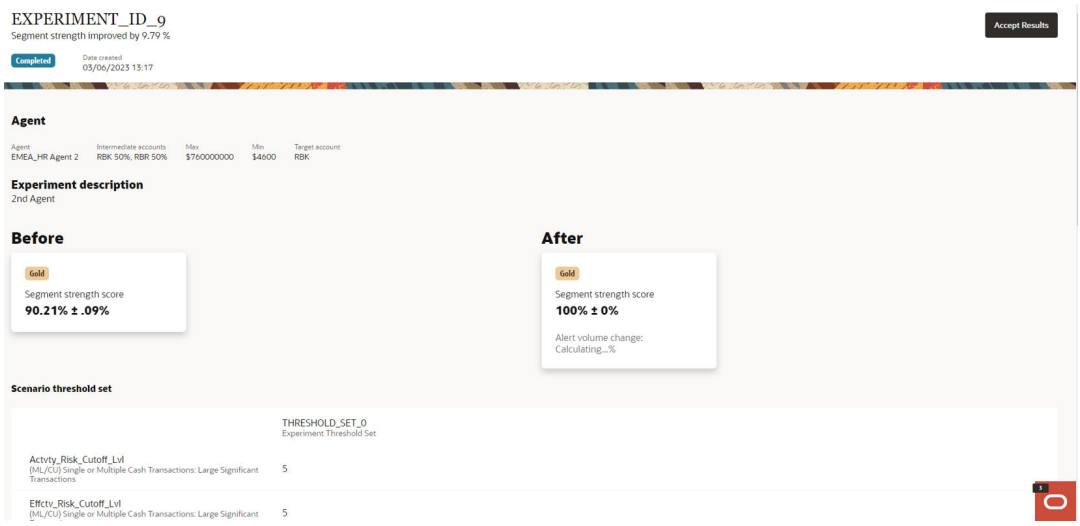
You can view the experiments for the following cases:

- **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.

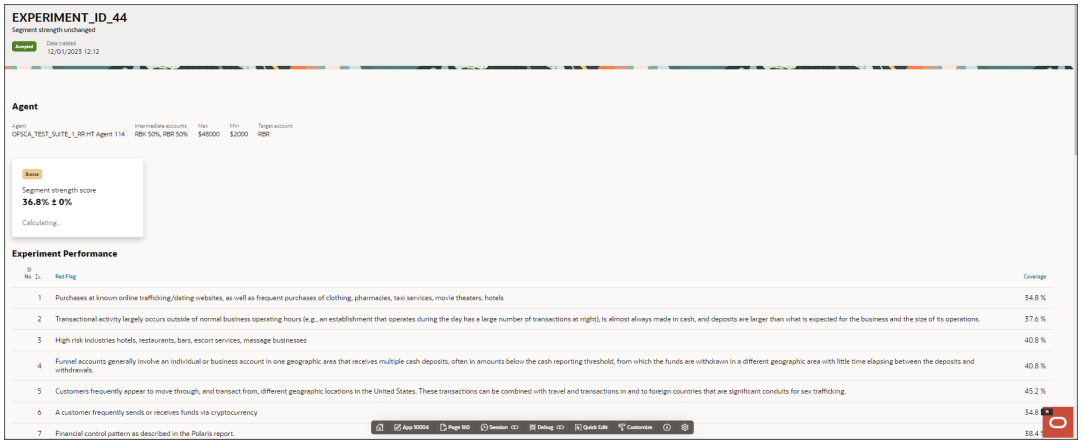
Figure 5-17 Segment Strength



(Optional) 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.

5.2 Generating Experiment from Recommendation

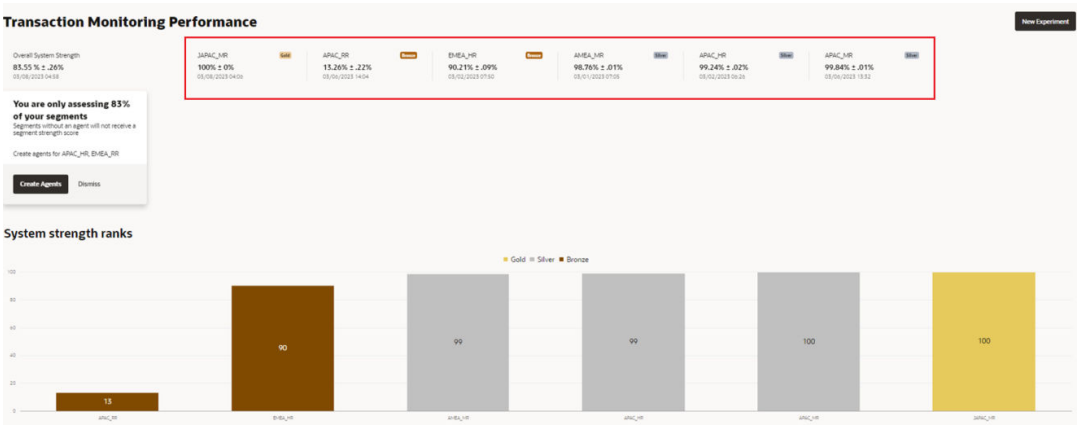
OFSCA offers recommendations to tackle the identified deficiencies. A deficiency can be a low scenario performance or a high account/ channel vulnerability. The recommendations aim to tune the scenario with the highest chances of addressing the selected deficiency. To generate recommended thresholds 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.

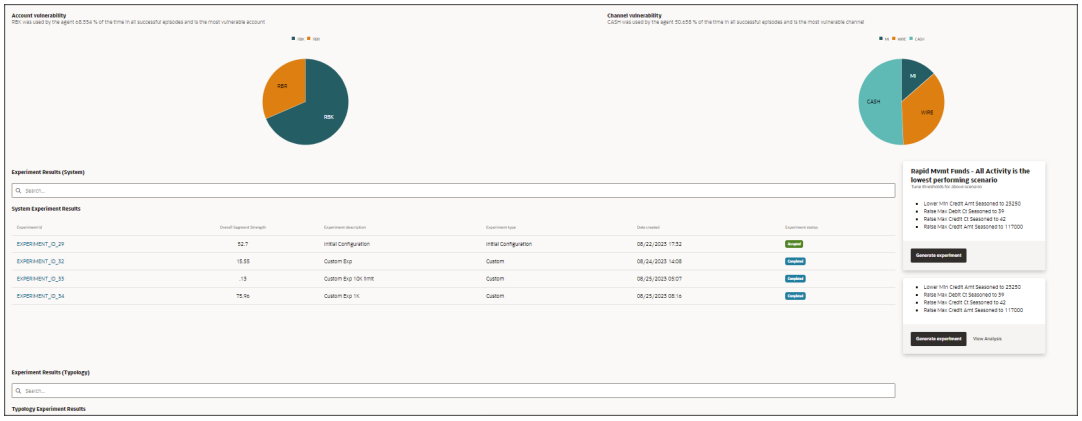
2. Click **Transaction Monitoring Performance** menu to display the Transaction Monitoring Performance dashboard. The following window is displayed.

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.

5.2.1 Generating Experiments for Segment

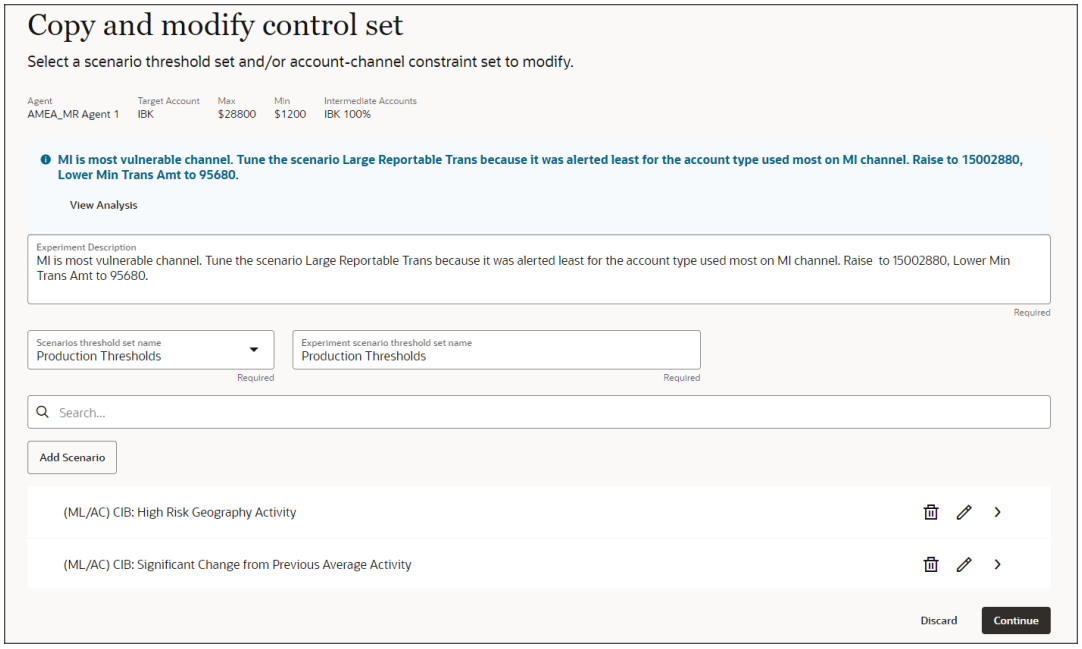
You can generate an experiment to evaluate this specific recommendation by clicking Generate Experiment on the segment dashboard.

> **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.

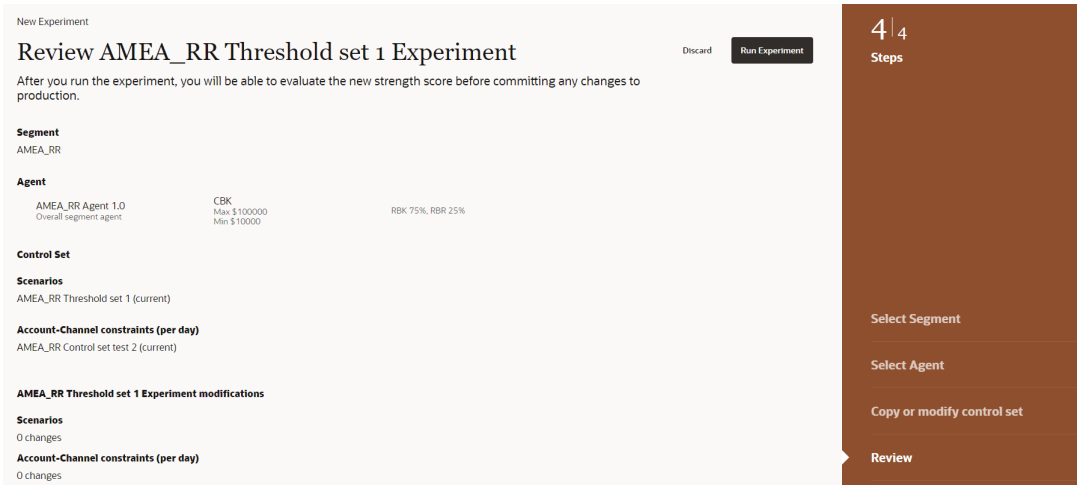
Figure 5-21 Copy or Modify Control Set



- 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.

2. Enter the relevant name or description for threshold set in the Experiment Scenario Threshold Set Name field.
3. If you want to modify the recommended thresholds, Click **Edit** icon against the existing scenarios. The Threshold Details window is displayed.
4. Modify the threshold value. Click **Update Scenario**. The Scenario List page is displayed.
5. Click **Continue** to navigate to the Review step. The following window is displayed.

Figure 5-22 Review Segment



6. 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.

5.2.2 View Analysis

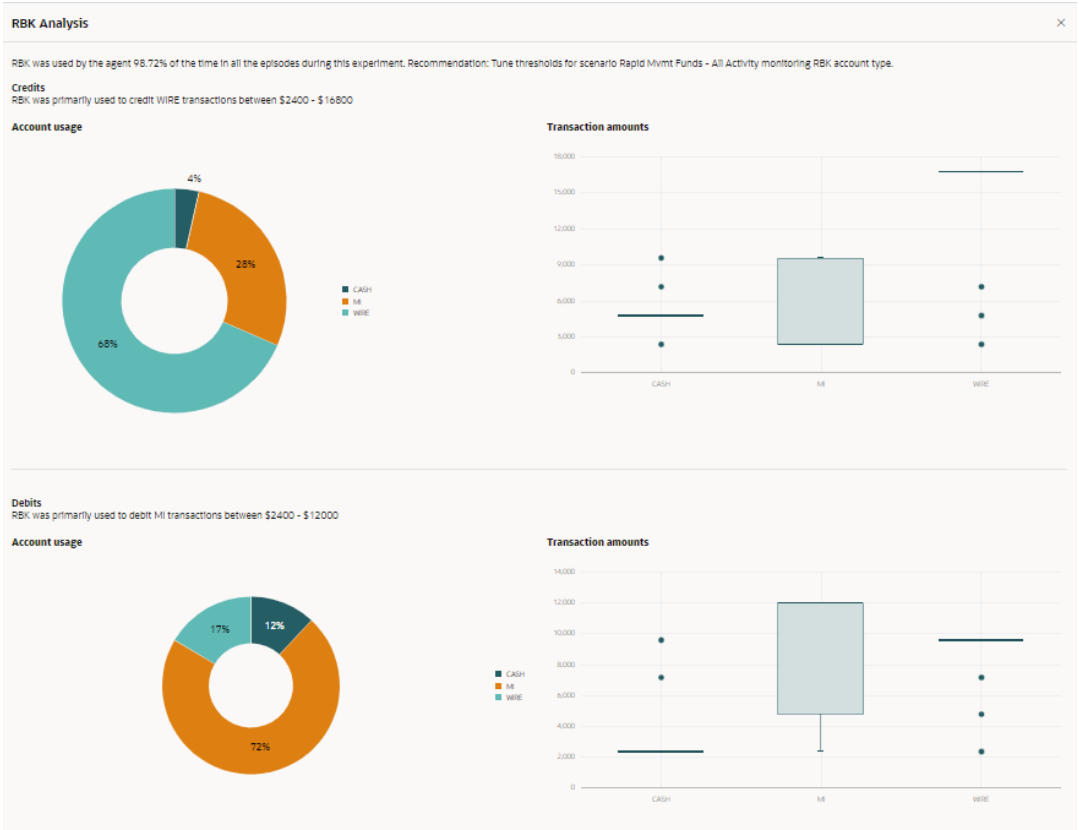
To view the identified vulnerability in detail, follow the step:

1. 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.

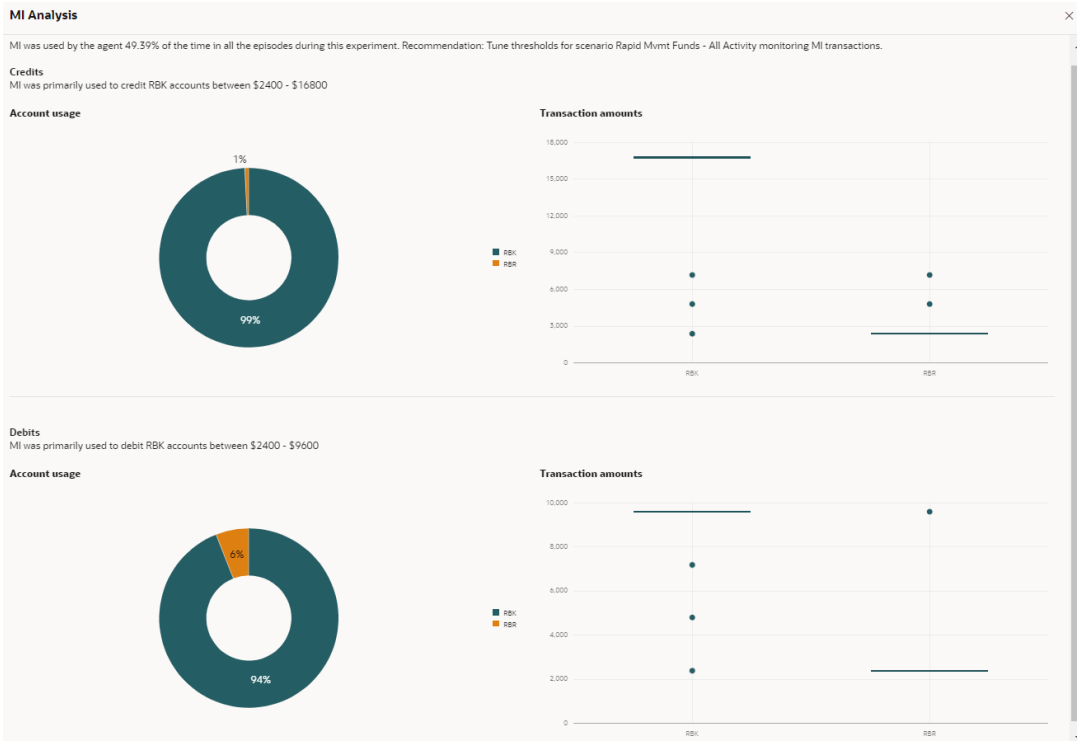
Figure 5-23 For Account Type



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

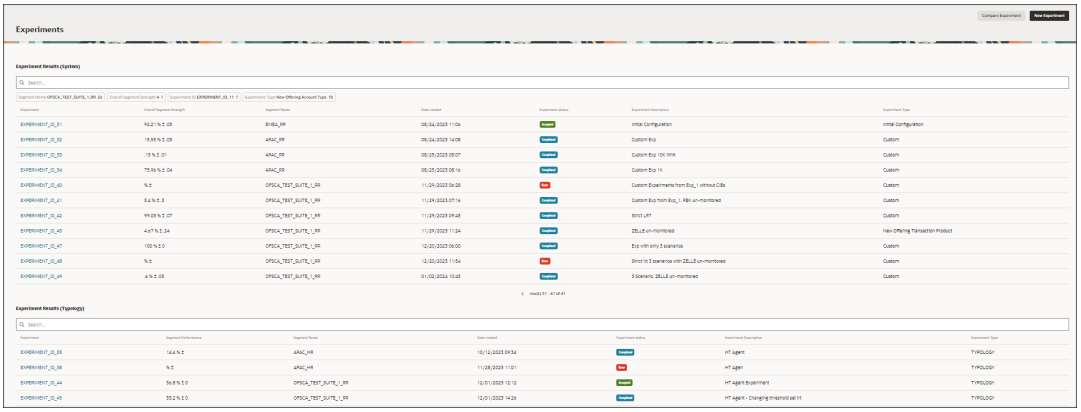
5.3 Comparing an Experiment

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

To compare the two experiments, follow these steps:

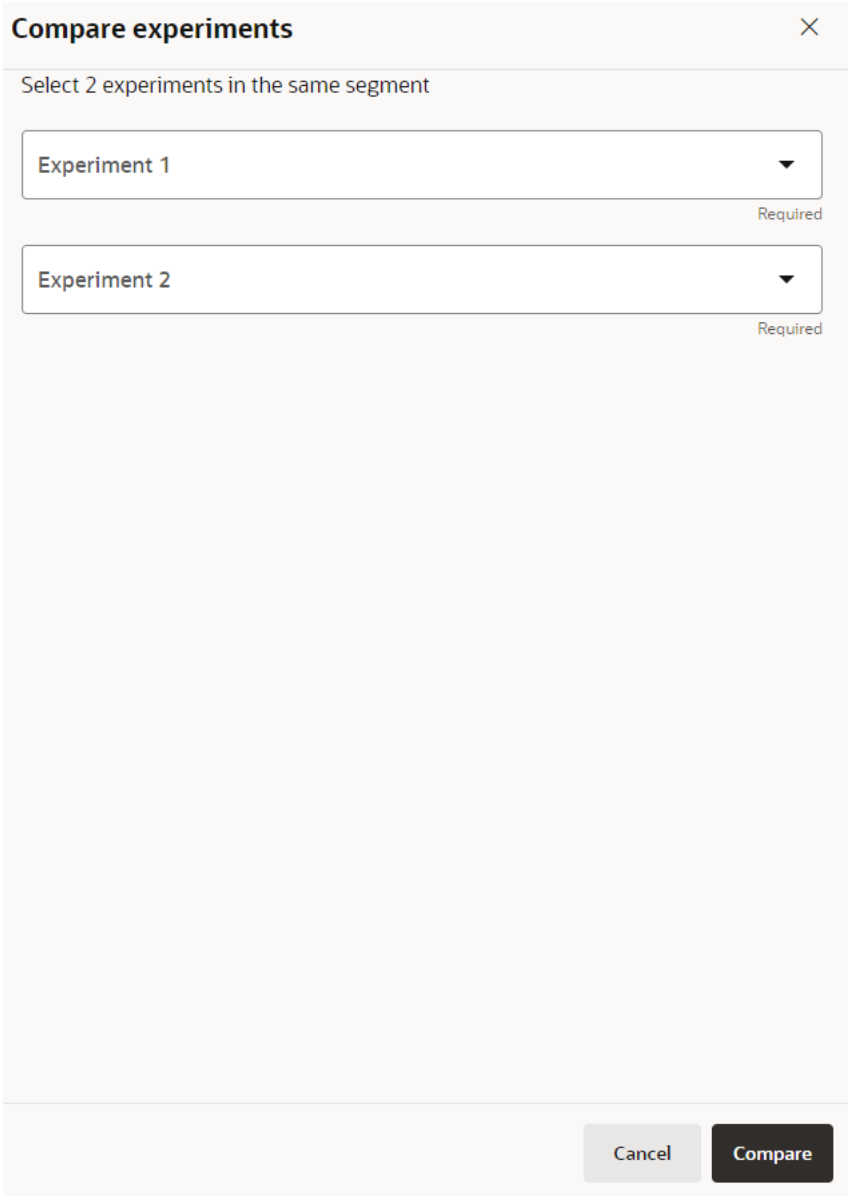
1. Click Open Ask Oracle  to display the Ask Oracle window.
2. Click **Experiments** menu to display the Experiments window. The following window is displayed.

Figure 5-25 Experiments



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

Figure 5-26 Compare Experiment



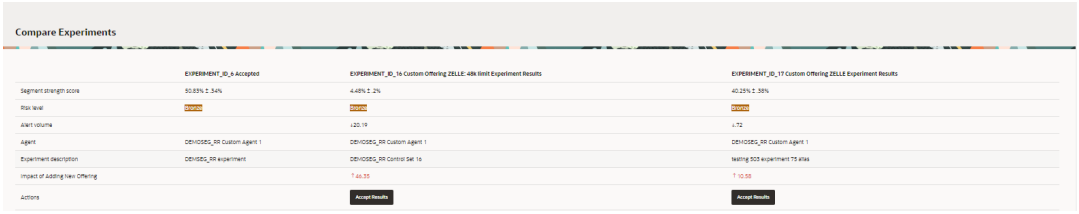
4. Select the required experiment that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select the required experiment that you want to compare with experiment 1 from the Experiment 2 drop-down list.

> **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



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.

5.4 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

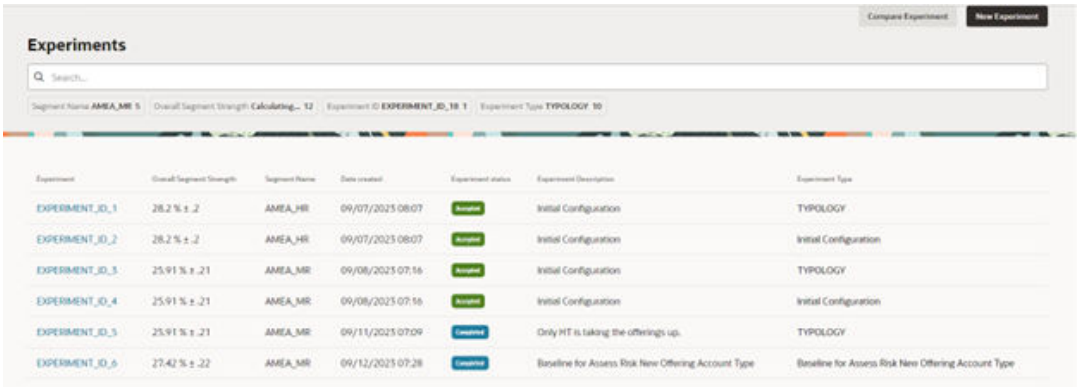
5.4.1 Risk of New Offering-Account Type

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:

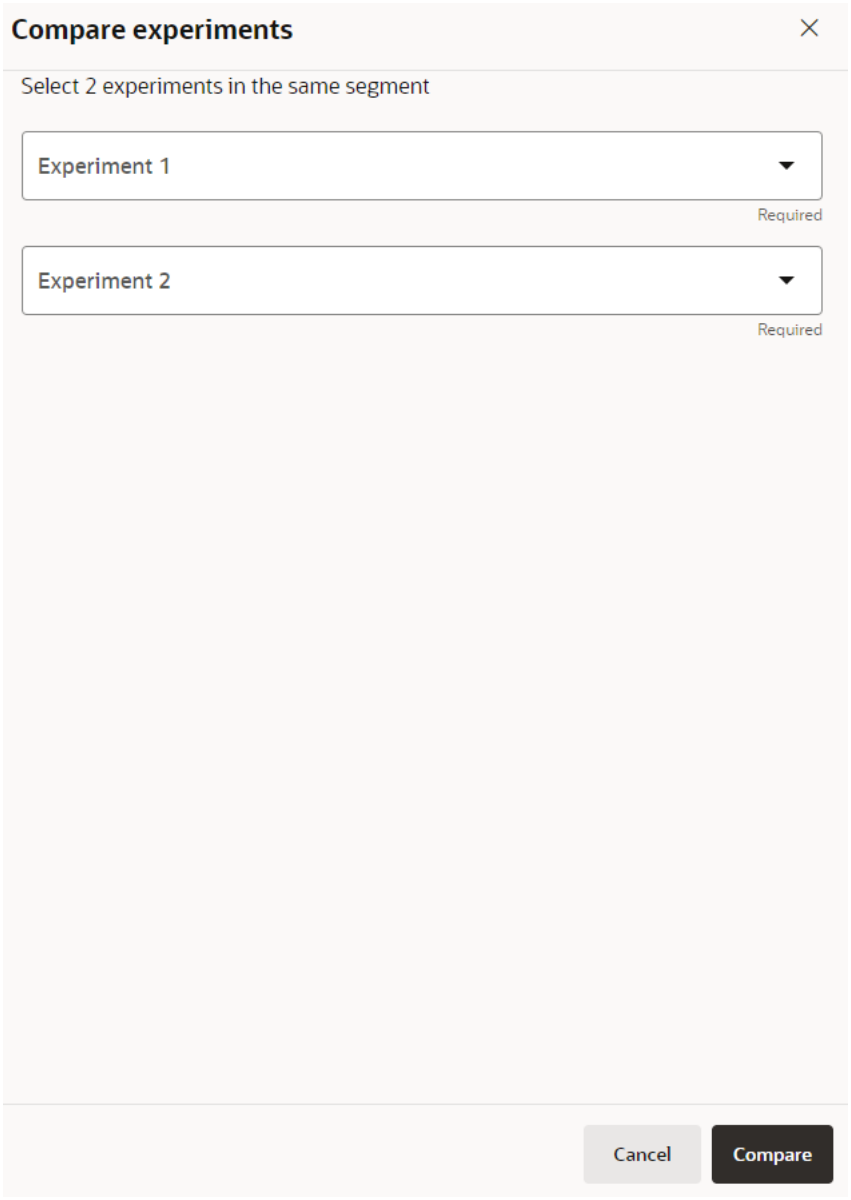
1. Click **Open Ask Oracle**  to display the Ask Oracle window.
2. Click the **Experiments** menu. The Experiments window is displayed.

Figure 5-28 Compare Experiments



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

Figure 5-29 Compare Experiment



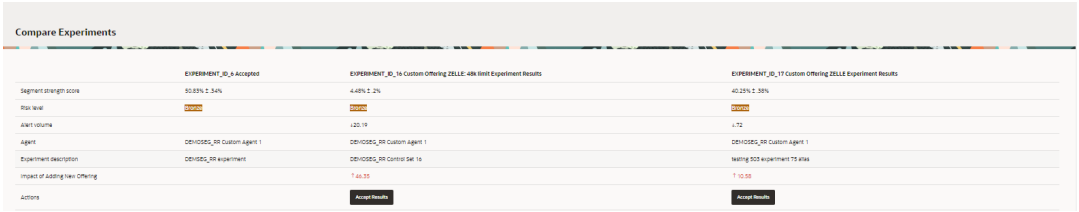
4. Select the experiment which has a newly added offering as an account type that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select another experiment that has a newly added offering as the account type with different set of constraints that you want to compare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



   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

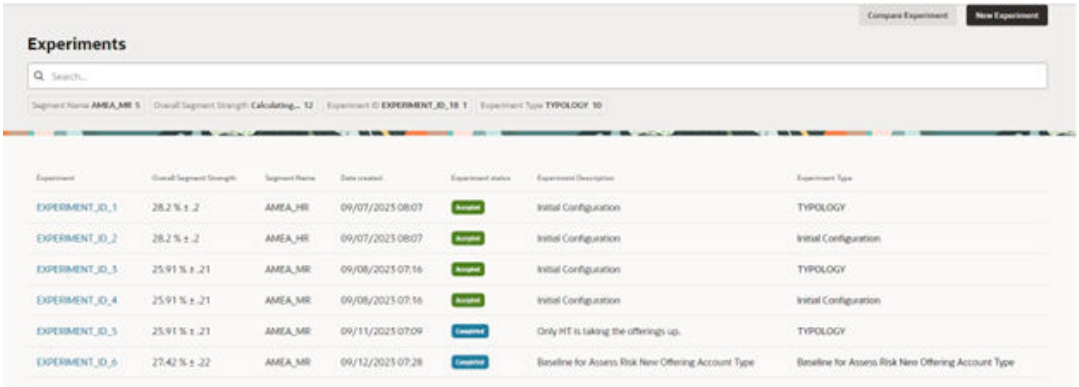
5.4.2 Risk of New Offering-Transaction Product

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:

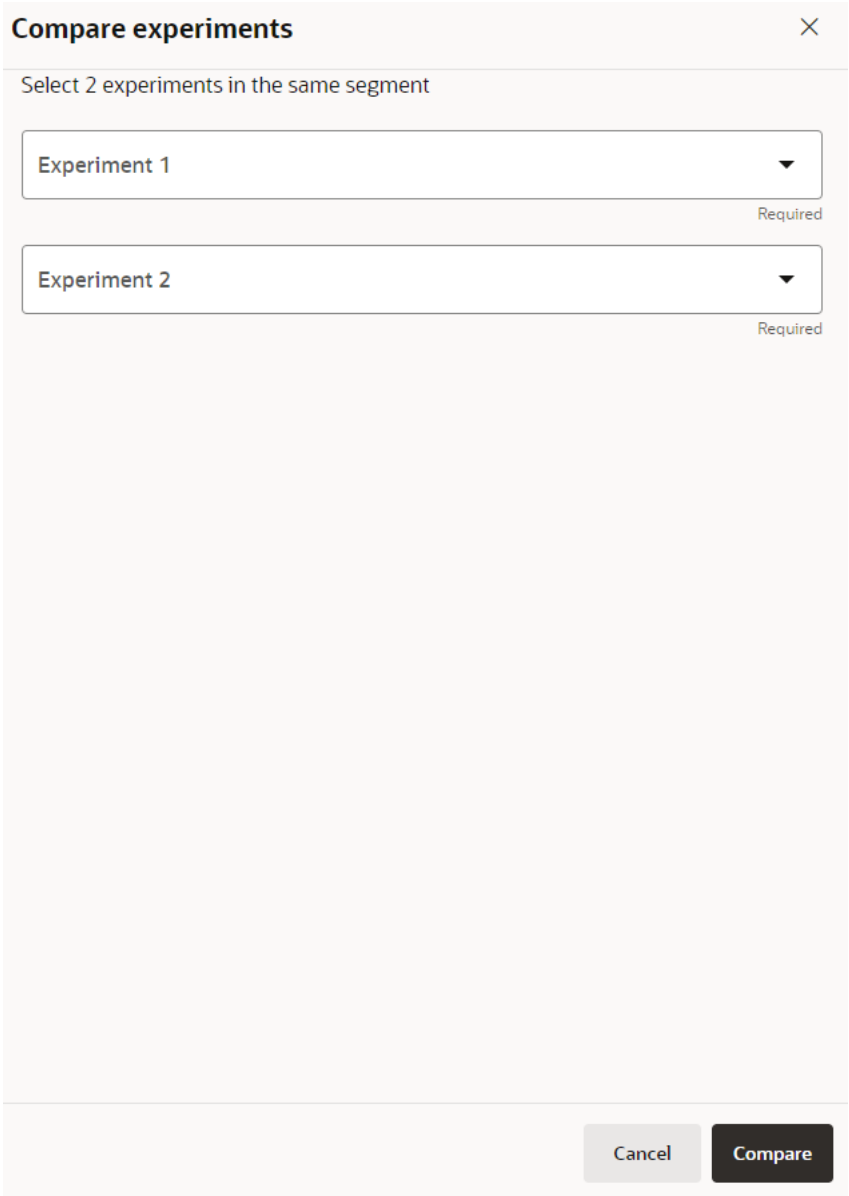
1. Click **Open Ask Oracle**  to display the Ask Oracle window.
2. Click the **Experiments** menu. The Experiments window is displayed.

Figure 5-31 Experiments



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

Figure 5-32 Compare Experiment



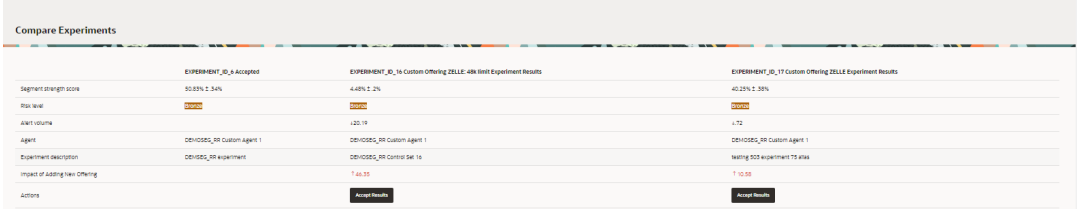
4. Select the experiment which has a newly added offering as a Transaction Product that you want to compare with another experiment from the Experiment 1 drop-down list.
5. Select another experiment that has a newly added offering as the Transaction Product with different set of constraints that you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



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.

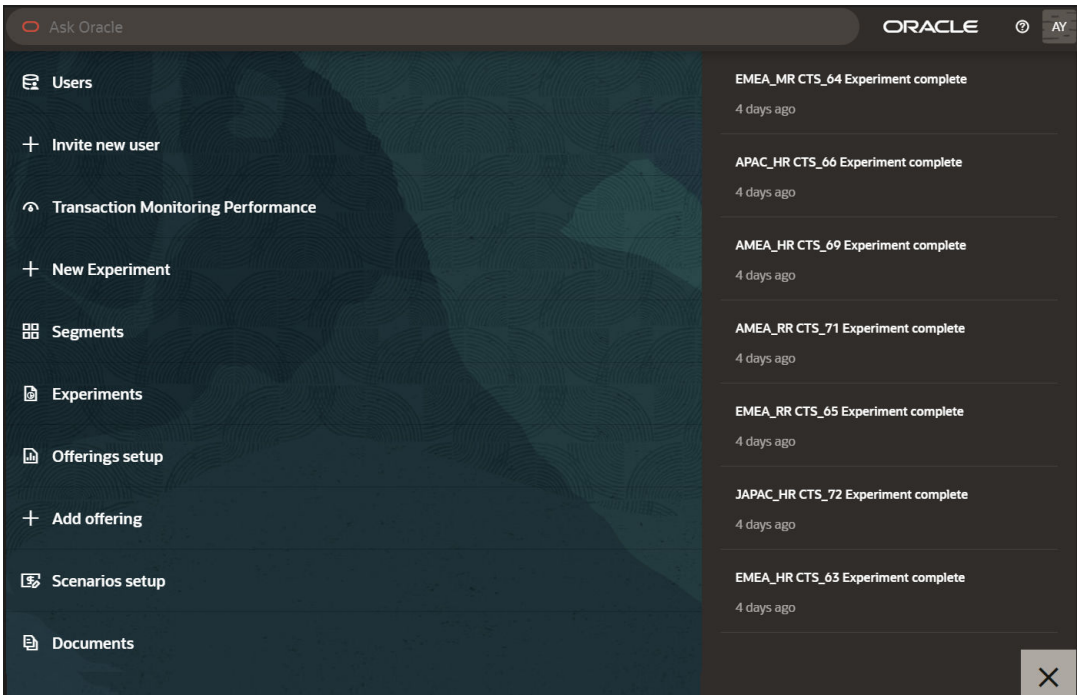
Topics:

- Adding an Account
- Adding a Transaction Product

To view the Offerings Setup, follow these steps:

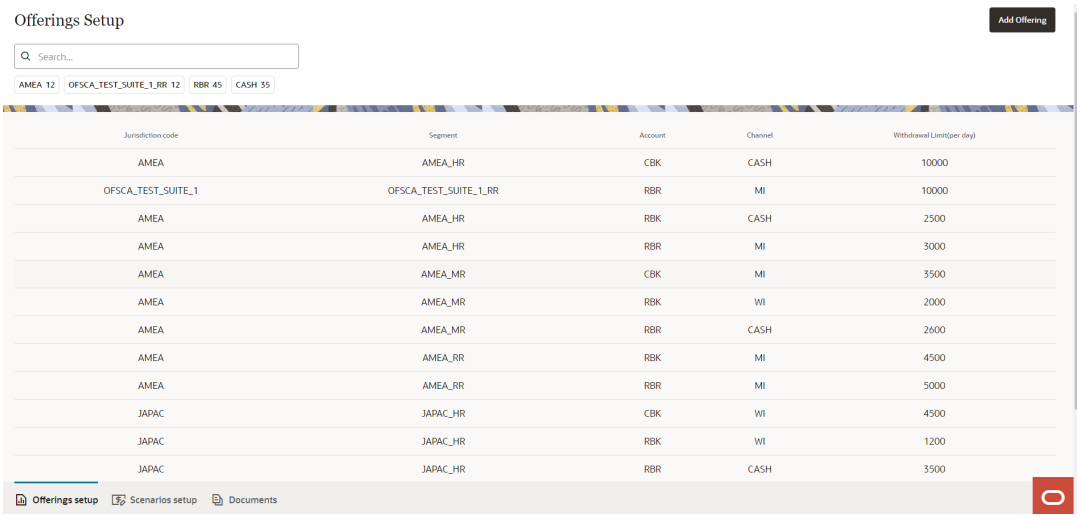
1. Click  Open Ask Oracle to display the Ask Oracle window. The Application page is displayed.

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



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

3. 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.

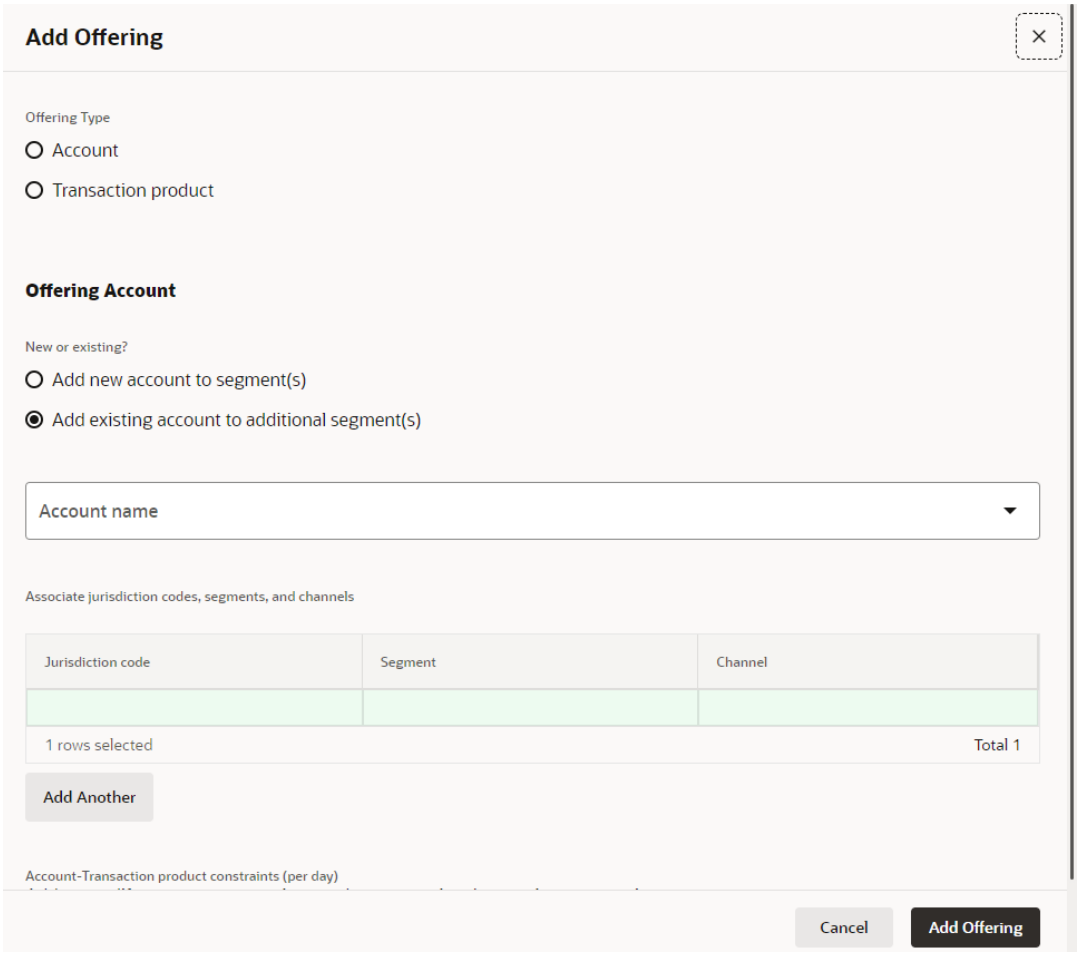
6.1 Adding an Account

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

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

1. 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



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.

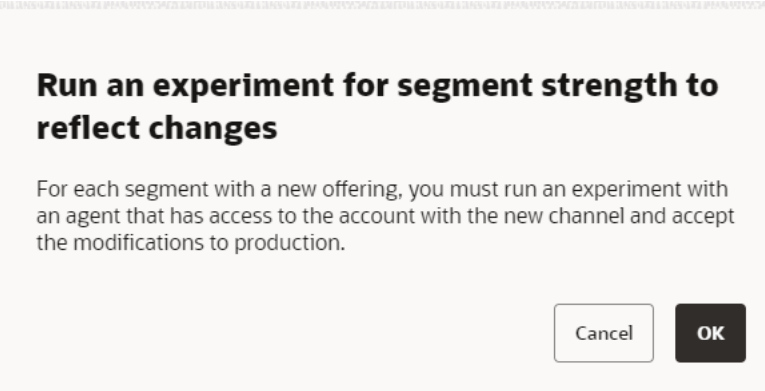
> **Note:**
>
> You can add up to four accounts to a segment.

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

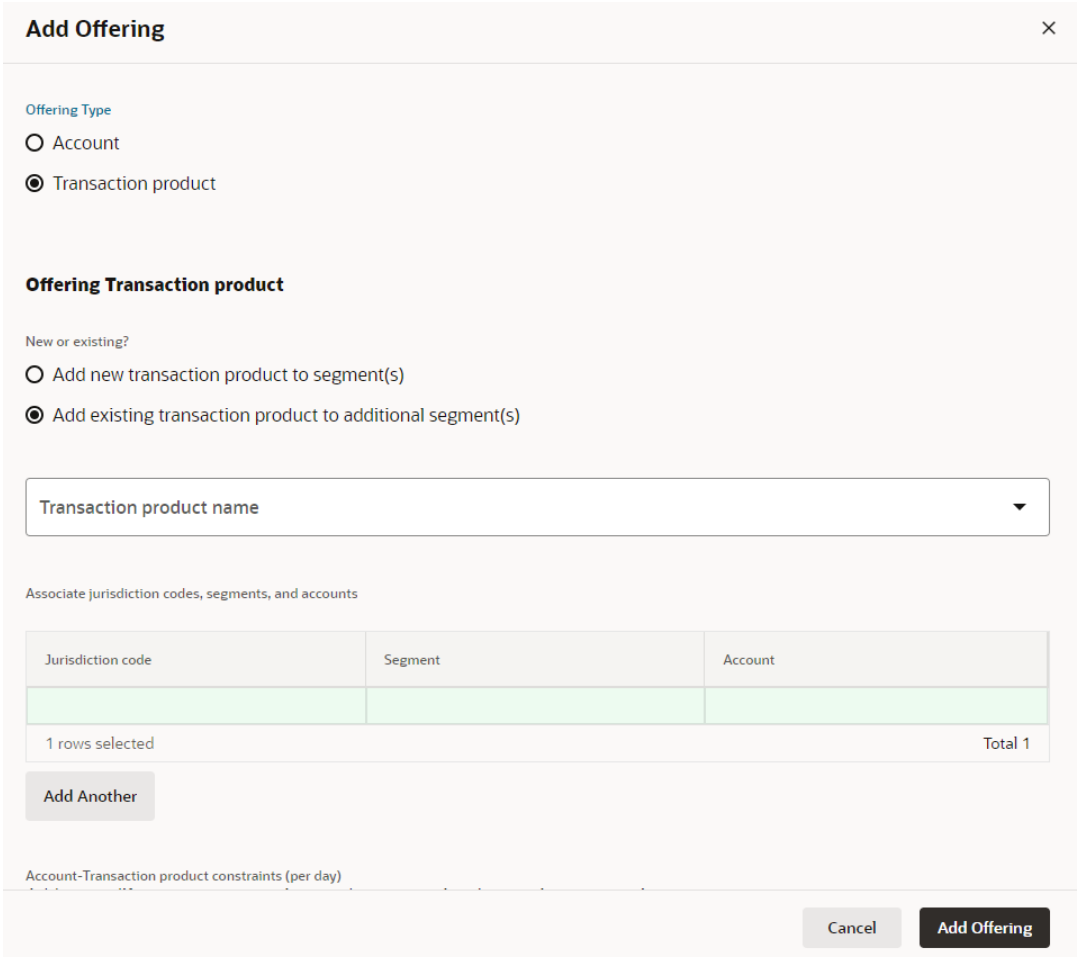
6.2 Adding a Transaction Product

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

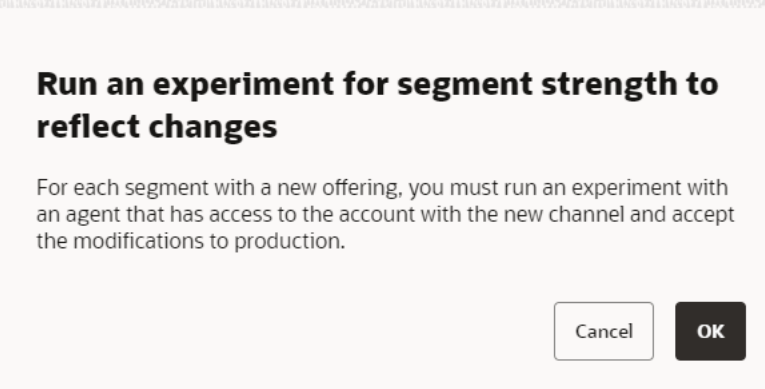


2. Select **Channel** from the Offering Type option.
3. To add a new Transaction Product to the segment, select **Add** new Transaction Product to segment(s). Enter the name of the new Transaction Product in the Transaction Product Name field.
4. To add an existing Transaction Product to a segment, select **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.

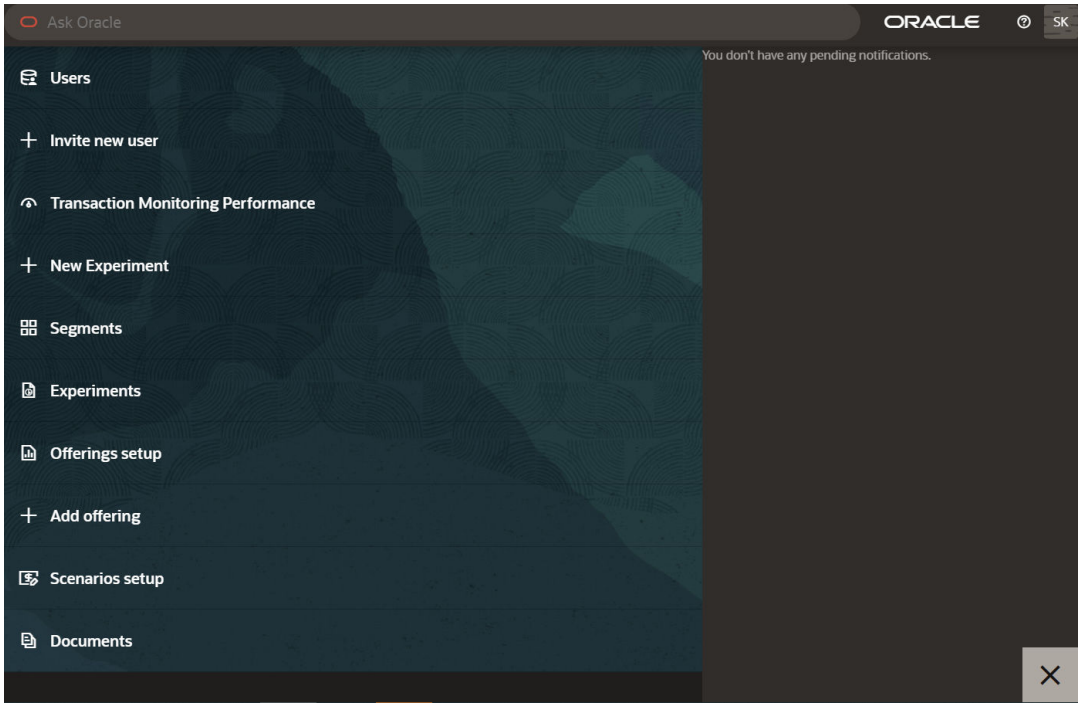
Topics:

7.1 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.

7.2 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.

7.3 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

7.4 Creating a New Experiment

To create a new experiment, follow these steps:

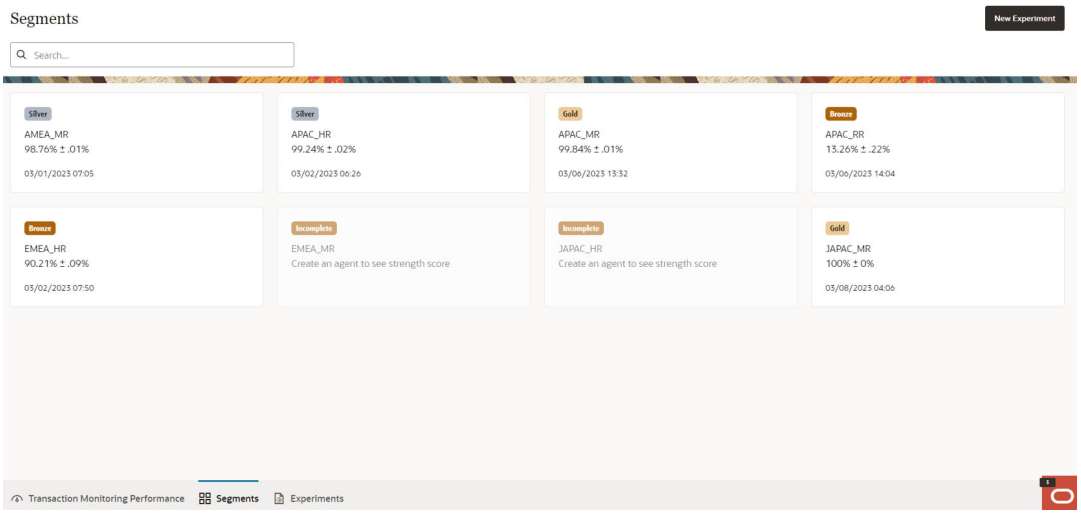
1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **New Experiment** menu to display the New Experiment window. For more information, see the New Experiment section.

7.5 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

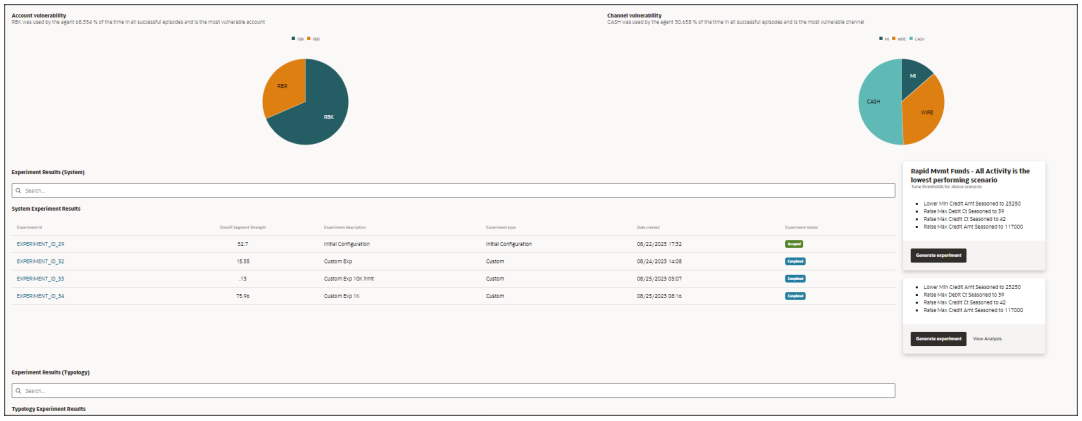


3. Click on the Search bar and select the required filter options from the drop-down list. The available filter options are Segment, Segment strength score, and Date created.

   Or Click on the required filter button below the Search bar and select the required filter options from the drop-down list.

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

Figure 7-3 Segment Dashboard



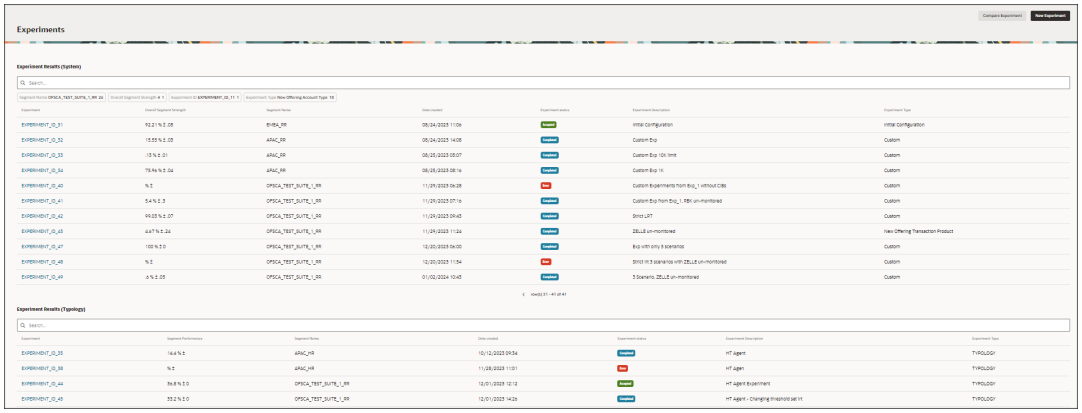
For more information about the segment dashboard, see the Generating Experiment from Recommendation section.

7.6 Managing Experiments

To view the 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 7-4 Experiments



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.

7.7 Managing Offerings Setup

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

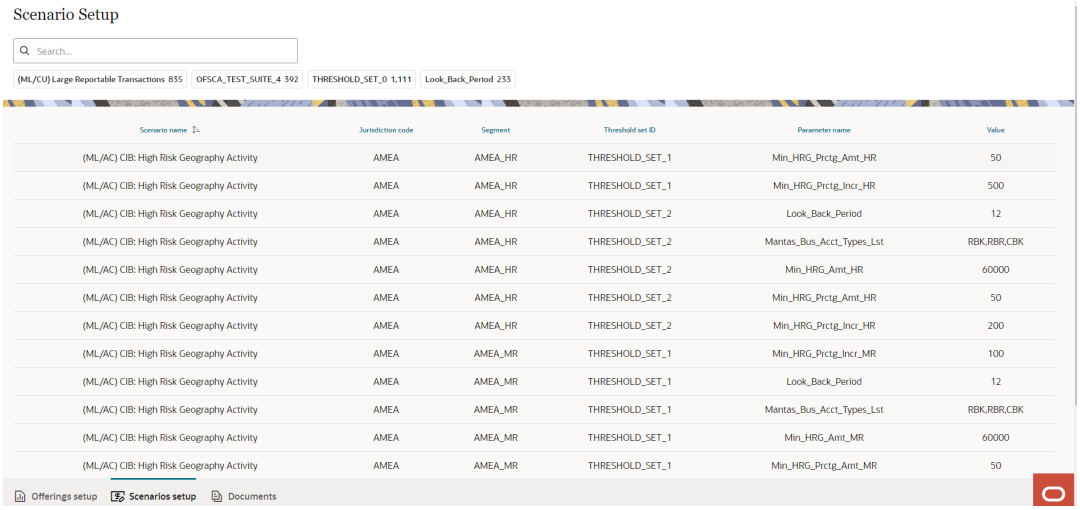
1. Click **Open Ask Oracle** to display the Ask Oracle window.
2. Click **Offerings** setup menu to display the Offerings Setup window. For more information, see the Modifying the System section.

7.8 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



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

7.9 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:

8.1 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 - '% 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.

8.2 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.

8.3 Segment Performance

The Segment Performance in 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.

8.4 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 vale 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.

8.5 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 are 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.

8.6 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 are 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.

9 Appendix

Topics:

9.1 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;

9.2 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"
      }
    }
  }
```

9.3 How to Calculate the CIB Parameter

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

/*CIB Parameters*/ 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 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 ACCT_INTRL_ID,              AVG(TOT_DEPST_AM) as
AVG_CREDIT_AMT,              AVG(TOT_WDRWL_AM) as AVG_DEBIT_AMT,
            STDDEV(TOT_DEPST_AM) as SD_CREDIT,
            STDDEV(TOT_WDRWL_AM) as SD_DEBIT,              MAX(TOT_DEPST_AM) as
MAX_CREDIT_AMT,              MAX(TOT_WDRWL_AM) as MAX_DEBIT_AMT              from
acct_smry_mnth              --where MNTH_SMRY_START_DT between '01-MAY-15' and '01-
SEP-15'              where MNTH_SMRY_START_DT >= add_months(trunc(sysdate, 'month'), -
12)    -- Recent 12 months data              and MNTH_SMRY_START_DT < trunc(sysdate,
'month')                        GROUP BY ACCT_INTRL_ID) t        on a.ACCT_INTRL_ID =
t.ACCT_INTRL_ID        GROUP BY c.JRSDCN_CD.
```

9.4 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
AGGREGATE_NAME	AGGREGATE_DESC	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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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
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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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
TOT_CRYPTO_CREDIT_AMT_DAY	Total Crypto Credit Amount for HT Transactions during the daytime	HT
TOT_CRYPTO_DEBIT_CT_DAY	Total Crypto Debit Count for HT Transactions during the daytime	HT
TOT_CRYPTO_CREDIT_CT_DAY	Total Crypto Credit Count for HT Transactions during the daytime	HT
TOT_CRYPTO_DEBIT_AMT_NIGHT	Total Crypto Debit Amount for HT Transactions during the nighttime	HT
TOT_CRYPTO_CREDIT_AMT_NIGHT	Total Crypto Credit Amount for HT Transactions during the nighttime	HT
TOT_CRYPTO_DEBIT_CT_NIGHT	Total Crypto Debit Count for HT Transactions during the nighttime	HT
TOT_CRYPTO_CREDIT_CT_NIGHT	Total Crypto Credit Count for HT Transactions during the nighttime	HT

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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
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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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
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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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_JEWLERY_DEBIT_AMT	Total Jewelry Stores Debit Amount for HT Transactions	HT
TOT_JEWLERY_CREDIT_AMT	Total Jewelry Stores Credit Amount for HT Transactions	HT
TOT_JEWLERY_DEBIT_CT	Total Jewelry Stores Debit Count for HT Transactions	HT
TOT_JEWLERY_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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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_CRYPTO_CREDIT_AMT	Total Crypto Credit Amount for HT Transactions	HT
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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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
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

Table 9-1 (Cont.) List of Aggregate

Aggregate Name	Aggregate Description	Scenario Type
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

9.5 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.

9.6 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.

9.6.1 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.

9.7 Recommending Thresholds

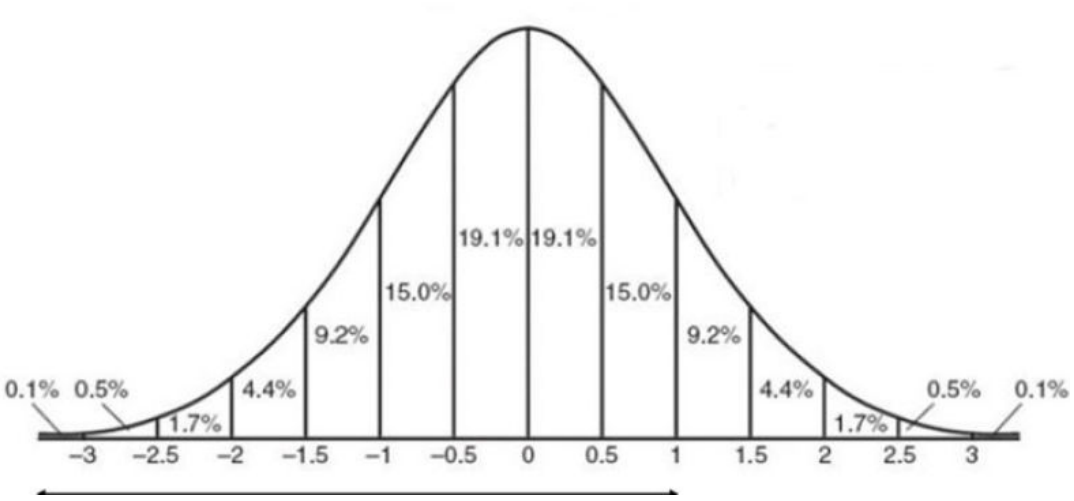
This section describes the recommended thresholds.

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:
     - Jump (p95.0) = (p95.1 – p95.0) / p95.0
     - Slope (p95.0) = J95.1 – 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 Jump (Cur) = (Xnext/Y – Xcur/Y) / Xcur/Y Slope (Cur) = Jnext – 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.

9.8 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.

10

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 x Target Amount. If the Target Amount is $100,000, the agent can transact only in whole number multiples of $5,000 (1/20 x $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.