

Oracle Financial Services

Anti Money Laundering Event Scoring User Guide

Release 8.0.5.0.0

Part Number: E92945-01



DOCUMENT CONTROL

Version Number	Revision Date	Changes Done
1.0	Created August 2017	Created the document.
Created by: Brijesh	Reviewed by: Swetha/Akhilesh/Renjith	Approved by: Shandar

TABLE OF CONTENTS

1	GETTING STARTED	4
1.1	About this Guide	4
1.2	Audience	4
2	OFS ANTI MONEY LAUNDERING EVENT SCORING	5
2.1	Understanding the OFS Anti Money Laundering Event Scoring Workflow	5
2.2	Understanding User Roles in OFS Anti Money Laundering Event Scoring	5
2.3	Accessing OFS Anti Money Laundering Event Scoring	5
2.4	Creating and Editing Execution Runs	6
2.4.1	Editing an Execution Run	10
2.5	Viewing and Analyzing Results.....	10
2.6	Managing Data Groups	13
2.7	Approving Techniques for Data Groups	14
2.8	Scoring Alerts	15

1 Getting Started

Oracle Financial Services (OFS) Anti Money Laundering Event Scoring (AMLES) application scores alerts that are generated from Anti Money Laundering (AML). The number of alerts generated from AML systems do not produce accurate results to be classified as valid alerts. However, this application optimizes the filtering of valid alerts and provides highly accurate results to prioritize alerts for investigation.

1.1 About this Guide

This document provides information to users to perform functions on the OFS Anti Money Laundering Event Scoring application.

1.2 Audience

This document is for users (creators and approvers) of the OFS AMLES.

2 OFS Anti Money Laundering Event Scoring

Use the application user-interface to create techniques that work to filter alerts generated from AML systems. You can score the alerts by passing the alerts data through the application and using the techniques created. The subsections in this chapter provide details.

2.1 Understanding the OFS Anti Money Laundering Event Scoring Workflow

The application workflow is discussed here to present to you a summary of procedures and operations that would help better your understanding of the use of the application before you see sections that deal with topics in detail. The following list is a summary of steps:

1. Log in to the OFSAA Application. See [Accessing OFS Anti Money Laundering Event Scoring](#).
2. Create Execution Runs. See [Creating and Editing Execution Runs](#).
3. View Results and Run Details in Data Groups. See [Viewing and Analyzing Results](#).
4. Request for deployment of the technique for a Data Group and request for approval by a user with approver privileges. See [Managing Data Groups](#) and [Approving Techniques for Data Groups](#).
5. Score New Alerts. See [Scoring Alerts](#).

2.2 Understanding User Roles in OFS Anti Money Laundering Event Scoring

OFS Anti Money Laundering Event Scoring application uses four-eyes functionality to provide two levels of maker and checker to create and approve execution runs. The two levels of users are defined as creators and approvers. For example, if your user profile is mapped to a Creator role, you can create an execution run and request for deployment, which has to be approved by a user with Approver role.

2.3 Accessing OFS Anti Money Laundering Event Scoring

To access the application, your user profile has to be mapped to the required roles. See [Understanding User Roles in OFS Anti Money Laundering Event Scoring](#) for more information. The following is the procedure to access the *OFS Anti Money Laundering Event Scoring* window:

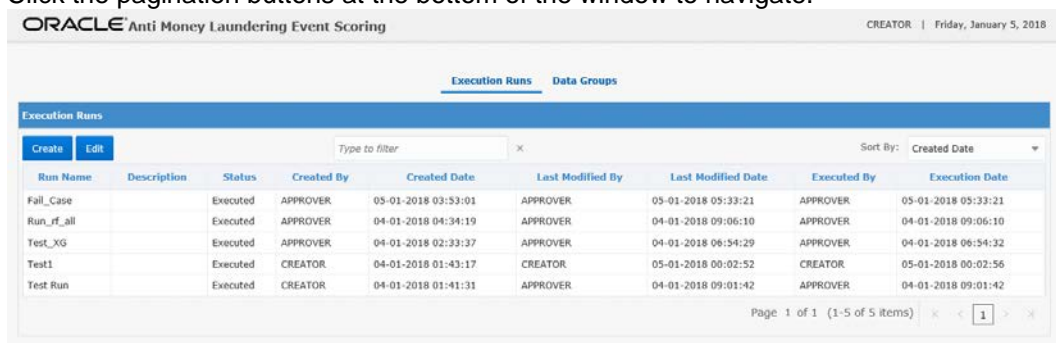
1. Log in to the OFSAA Application with your user credentials to view the *Applications* window.



2. Click **Anti Money Laundering Event Scoring** from the *Applications* window. Alternatively, you can click the left menu link. The *Anti Money Laundering Event Scoring* window appears.



3. On the *Execution Run* window, a list of Execution Runs that are in saved draft or created state are displayed. Enter characters in **Type to filter** to perform a search for data groups and click the **Sort By** drop-down list to select and sort based on various options in the list. Click the pagination buttons at the bottom of the window to navigate.



Based on the roles assigned to your user profile, you can create, edit and approve execution runs. See further sections for details.


2.4 Creating and Editing Execution Runs

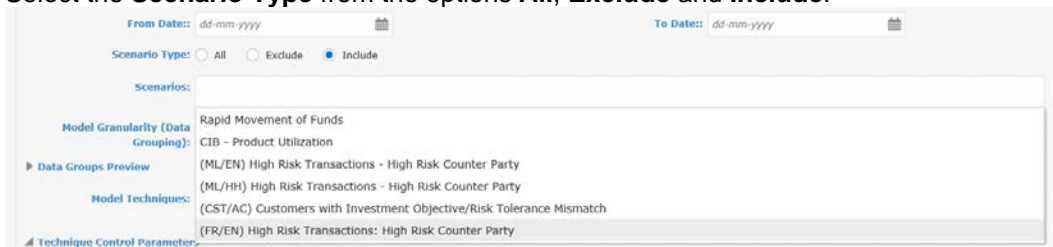
Create and execute runs to explore historical data and find the best suited technique for a data group.

The following is the procedure to create Execution Runs:

1. Click **Create** from the *Execution Run* window to view the *Execution Run Details* window.
Note: Click **Back** to go to the previous window and click **Reset** to clear all entries in the fields.
2. Enter the details in the fields on the *Execution Run Details* window.



3. Enter **Run Name** and **Run Description**.
4. Click **Date-Time Editors**  for **From Date** and **To Date** to select the **Historical Data Date Range**.
5. Select the **Scenario Type** from the options **All**, **Exclude** and **Include**.

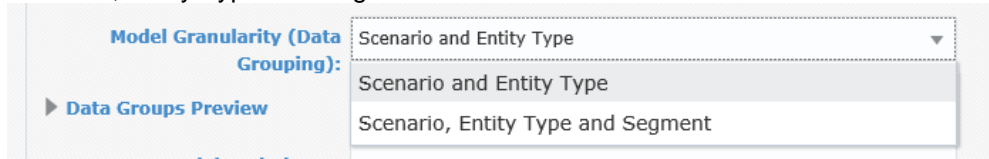


- a. **ALL** - Select to include all scenarios in the run.
- b. **Exclude** - Select to exclude certain scenarios from the run. On selecting this radio button, the **Scenarios** field appears. Click the field to display a drop-down list of Scenarios. Select the Scenarios that you want to exclude from the run. To remove a Scenario from the exclude list, click **X** on the selected Scenario.

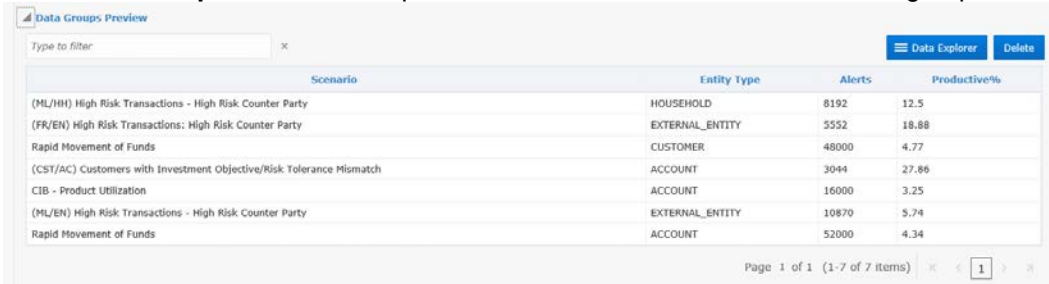
NOTE: The Scenarios are configurable in the DIM. For more details, see [Performing Administration Tasks to Prepare the Service](#).

- c. **Include** - Select to include certain scenarios in the run. On selecting this radio button, the **Scenarios** field appears. Click the field to display a drop-down list of Scenarios. Select the Scenarios that you want to include in the run. To remove a Scenario from the include list, click **X** on the selected Scenario.
6. Click the **Model Granularity (Data Grouping)** drop-down list to select the relevant groups for the run from the following options:
 - a. Scenario and Entity Type

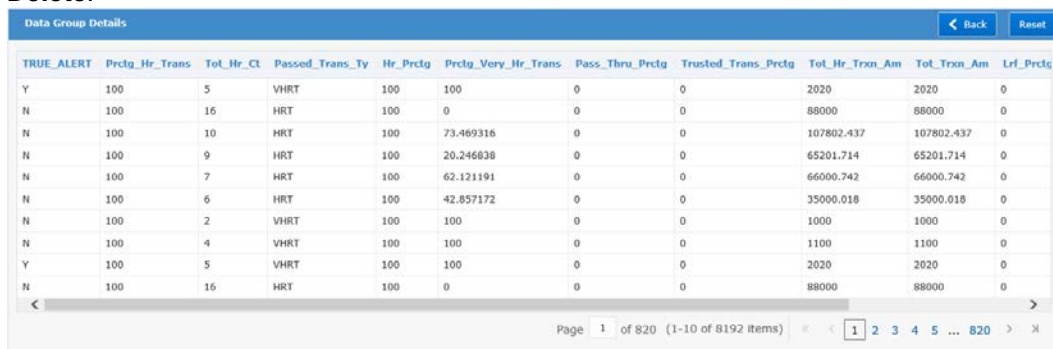
b. Scenario, Entity Type and Segment



7. Click **Data Groups Preview** to expand and view the list of the selected data groups.



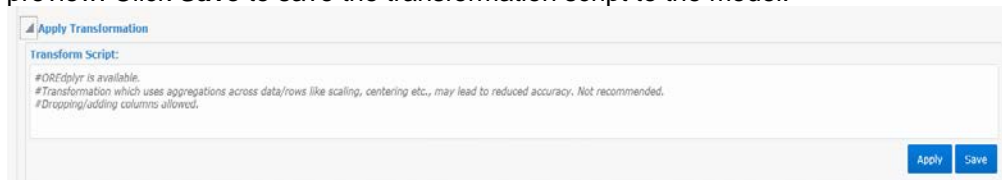
8. On the *Data Groups Preview* section, you can view columns for data groups (**Scenario**, **Entity Type**, and **Segment** (if selected)), **Alerts** and **Productive%**. Enter characters in the **Type to filter** field to perform a search. Select a row and click **Data Explorer** to view details in the *Data Group Details* window. To delete a data group, select the row and click **Delete**.



Note: On the *Data Group Details* window, click **Back** to go to the previous window and click **Reset** to clear all entries in the fields.

The following is the procedure to view and plot the data from the *Data Group Details* window:

a. Click **Apply Transformation** to expand and view the **Transform Script** field. You can write a custom R Script in Transform Script to transform the data before building the model. This field is optional. Click **Apply** to apply the transform script and preview. Click **Save** to save the transformation script to the model.



b. Click and select **Bivariate Plot**, **Univariate Box Plot**, **Correlation Heat Map**, **Univariate Density Plot**, **Empirical Logit Plot**, **Information Value Matrix** or **Weight of Evidence Matrix** from **EDA** (Exploratory Data Analysis) to plot a visual

representation of the data and click **Plot**.



c. View the details of the plot in tabular form in the section following the EDA fields.



EDA:

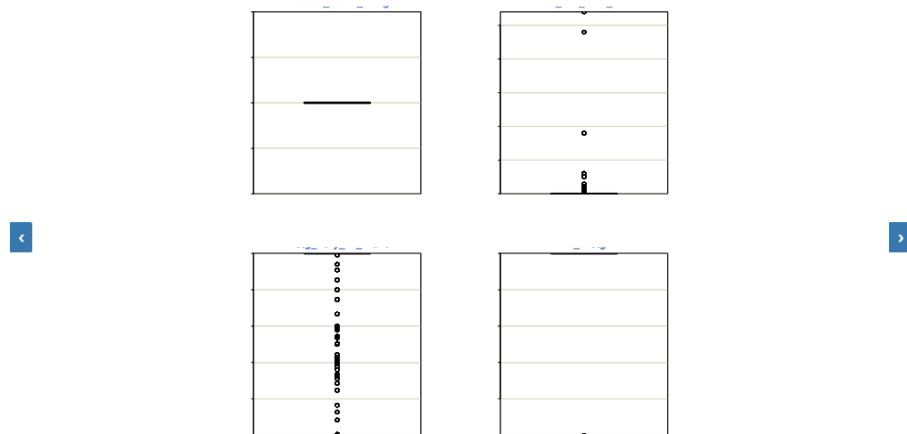
Bivariate Plot Univariate Box Plot Correlation Heat Map Univariate Density Plot Empirical Logit Plot Information Value Matrix Weight of Evidence Matrix

Plot

	Q1	Mean	Q3	Variable	Min	Max	Skewness	Median	Kurtosis
0	0		0	Trusted_Trans_Prctg	0	0	NaN	0	NaN
500	29610.9146		1000	Tot_Vhr_Trxn_Am	0	5400000	18.3216	500	368.9651
100	85.7631		100	Prctg_Very_Hr_Trans	0	100	-2.033	100	2.346
100	99.9914		100	Hr_Prctg	75.0006	100	-53.799	100	2892.6675
0	0.6497		0	Effectv_Risk_Lvl	-2	10	3.3694	0	9.4635
1	1.4306		1	Tot_VHr_Ct	0	40	0.6054	1	110.4209
4095	4232.884		5350	External_Entity	386	5586	-1.485	4402	1.5128
500	360621.7565		10000	Tot_Hr_Trxn_Am	100	300010000	30.9614	500	958.07
0	2.9335		0	Pass_Thru_Prctg	0	100	5.5864	0	29.2778
0	14.078		0	Lvl_Prctg	0	100	2.0655	0	2.3253

Page 1 of 1 (1-10 of 10 items) < 1 >

d. Scroll down further to view the details in graphical format. Use the  and  buttons to navigate through the various pages of the graph.



e. Click **Back** to go to the previous window.

9. Click the **Model Techniques** field to view a drop-down list. Select from the list that you want to run for the historical data that is filtered for the conditions entered in the previous field. To remove a Model Technique from the field, click **X**.



10. Click **Technique Control Parameters** expand and view details for tabs **Common**, **WOE Logistic Regression** and **XG Boost**. Enter data in the fields to suit your requirement to configure the number of alerts and the percentage considered for optimization. It helps improve the accuracy of the alerts. Click the headers to view the details for the respective tabs.

- a. **Common** – Select Yes or No for **Enable Null check on columns**. Enter the **Missing Value percentage Allowed** from 0 to 100. Select Yes or No for **Enable Zero Variance Check on columns**. Enter the integer value for **Minimum minority observations in CV Folds**. Enter **Minimum Validation Data Percentage** from 0 to 100. Enter the integer value for **Max cross validation runs per model** and **Max cross validation folds per repeat**.
- b. **WOE Logistic Regression** – Click and select the options from the drop-down for **Binning Type**. Enter the integer value for **Number of Bins for Quantile** and **Number of Bins for Interval**. Select All or Bad for **Enable collinearity check**.
- c. **XG Boost** – Click and select the options from the drop-down for **Booster**. Enter the numerical values for **Learning rate(eta)**, **Minimum Split Loss(gamma)**, **Maximum depth of a Tree**, **Minimum Child Weight**, **Column Sample**, **Sub Sample**, **Lambda**, **Alpha**, **Max Number of Iterations** and **Early Stop**.

NOTE: You can access the tabs based on the selections from the Model Techniques field.

11. Click **Save** to save the entries on the creation window. Click **Update** to update changes. Click **Run** to execute the scripts. After the scripts are run, you can click **Results** to view the results of the run in the Data Groups window. For more information on Results, see [Viewing the Results and Analysis](#).

2.4.1 Editing an Execution Run

To edit an Execution Run, select and click **Edit** on the *Execution Runs* window to view the details in the Execution Run Details window. Edit the fields that can be edited. **Run Name** field is read-only and you cannot edit it. For field descriptions, see [Creating and Editing Execution Runs](#) section.

The screenshot displays the 'Execution Run Details' window in the Oracle Anti Money Laundering Event Scoring application. The window title is 'ORACLE Anti Money Laundering Event Scoring' and the user is 'CREATOR' on 'Friday, January 5, 2018'. The window contains several input fields and controls: 'Run Name' is 'Test_XG'; 'Run Description' is empty; 'From Date' is '14-12-2009' and 'To Date' is '04-01-2018'; 'Scenario Type' has radio buttons for 'All' (selected), 'Exclude', and 'Include'; 'Model Granularity (Data Grouping)' is set to 'Scenario and Entity Type'; there is a 'Data Groups Preview' button; and 'Model Techniques' is 'XG Boost'.

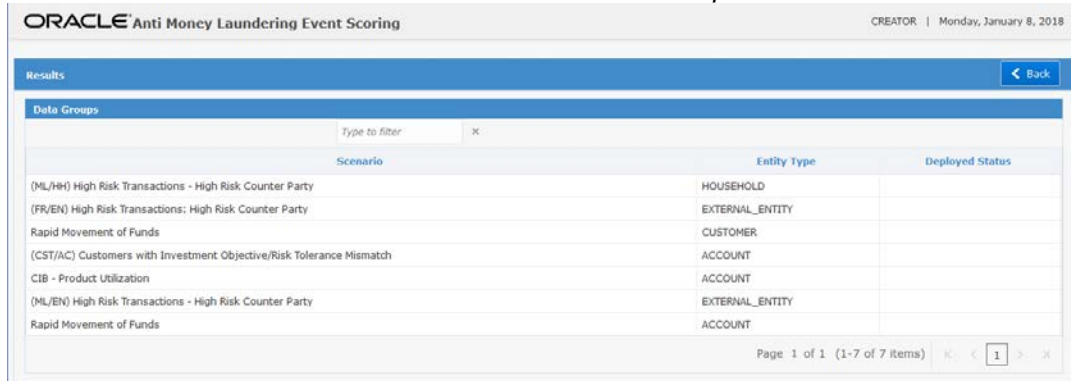
2.5 Viewing and Analyzing Results

Results provide representation of the run and is used to analyze the scores. You can analyze the results and submit the run for approval.

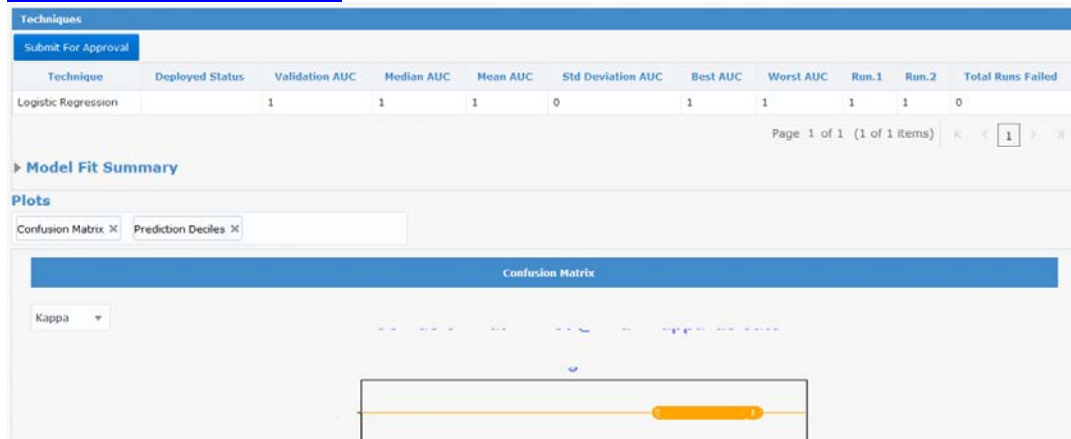
The following is the procedure to view and analyze the results:

1. Run the scripts on the *Execution Run Details* window. For more information, see [Creating and Editing Execution Runs](#).

- Click **Results** to view the results of the run in the *Data Groups* window.



- Select a Scenario row on the *Data Groups* window and the *Techniques* pane appears at the bottom. The *Techniques* pane displays Techniques that were selected on the *Execution Run Details* window. The *Techniques* pane also displays **Model Fit Summary** and **Plots** appear. Click **Submit For Approval** to deploy the Techniques for approval by a user with Approver privileges. For more information on approval, see [Approving Techniques for Data Groups](#).



NOTE: Submit for Approval button is displayed if you are a user assigned the Creator role.



- Click **Model Fit Summary** to expand and view details for the selected Model.



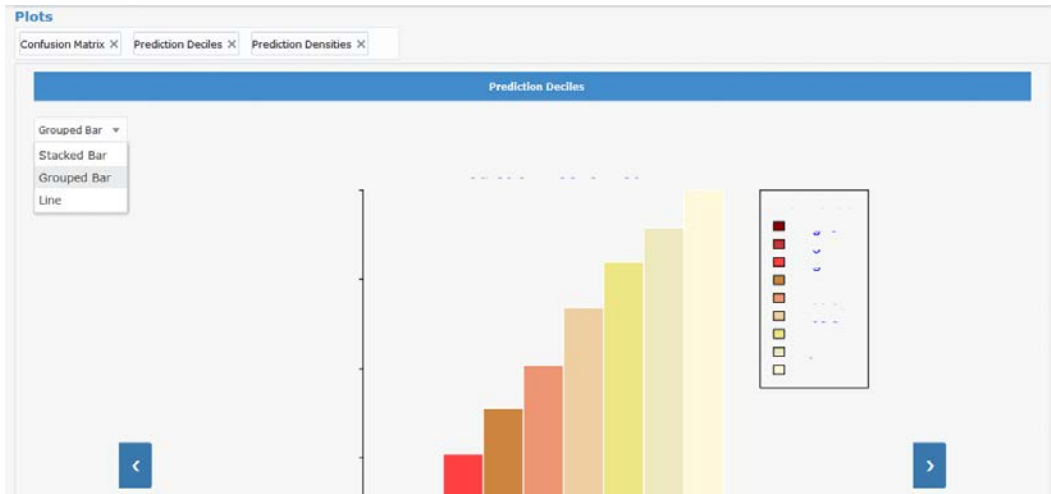
- Plots** displays a graphical view of the results of the Techniques used in the Model. You can review and analyze the results of the Techniques here. For example, Confusion Matrix can be used to compare alerts with analysis of historical

data to determine the fit or match. The framework provides Confusion Matrix for various cut-offs such as Kappa, KS, F Value, BKVN, and High3 till Low1.



- Click  to view the previous technique and  to view the next Plot. Select the available studies from the drop-down list on Plots and apply on the charts.





7. Click the **Plots** field to display the drop-down list and select a Plot to add. To remove a Plot, click **X** on the Plots displayed in the field.
8. Click **Back** to go to the previous window.

2.6 Managing Data Groups

Data Groups provides information for the status that a Run is in the workflow. For more information on workflow, see [Understanding the OFS Anti Money Laundering Event Scoring Workflow](#). You can view Runs that are approved, or you can approve Runs if you have Approver Privileges. For more information on how to approve a Run, see [Approving Techniques for Data Groups](#).

The following is the procedure to use the Data Groups user-interface:

1. Click **Data Groups** to view the *Data Groups* window. On the *Data Groups* window, the Runs are grouped in **Approved**, **Pending Approval**, **Rejected** and **Inactive** tabs. The data groups are grouped based on their current status and you can click on the respective tabs to view the data groups.

Scenario	Entity Type	Technique	Run Name ~ Version	Status
(FR/EN) High Risk Transactions: High Risk Counter Party	EXTERNAL_ENTITY	Logistic Regression	Test1 ~ 1	Approved
(CST/AC) Customers with Investment Objective/Risk Tolerance Mismatch	ACCOUNT	Logistic Regression	Test_version ~ 15	Approved

The following is the description for the statuses:

- a. **Approved** – Data Groups deployed by approvers and used in the application to predict new alerts.
- b. **Pending for Approval** – Data Groups submitted for approval by creators.

- c. **Rejected** – Data Groups rejected by approvers. Creators can rerun after applying recommended changes.
 - d. **Inactive** – Data Groups which have techniques that were replaced by newer and more effective techniques.
2. Select a Data Group and click **Results** to view the execution run results. For more information on Results, see [Viewing and Analyzing Results](#). Select a Data Group and click **View Run Details** to see details of the run. For more information on Runs, see [Creating and Editing Execution Runs](#).
 3. Click **Approved** to view a list of approved runs, select a row and click **Results** to view the Technique that is deployed for the Run in the *Deployed Status* column.

Technique	Deployed Status	Validation AUC	Median AUC	Mean AUC	Std Deviation AUC	Best AUC	Worst AUC	Run.1	Run.2	Total Runs Failed
Logistic Regression	Deployed	0.5621	0.5222	0.5222	0.0193	0.5358	0.5086	0.5086	0.5358	0

Page 1 of 1 (1 of 1 items)

2.7 Approving Techniques for Data Groups

NOTE: You must have Approver role privileges assigned to your profile to approve Techniques for Data Groups.

Users create Execution Runs and submit for approval to users with Approval privileges.

See the following sections for related topics:

- [Understanding the OFS Anti Money Laundering Event Scoring Workflow](#)
- [Understanding User Roles in OFS Anti Money Laundering Event Scoring](#)
- [Managing Data Groups](#)
- [Viewing and Analyzing Results](#)

The following is the procedure to approve a Run:

1. Log in to OFSAA application. See [Accessing OFS Anti Money Laundering Event Scoring](#) for more information.
2. Click **Data Groups** to view the *Data Groups* window. On the *Data Groups* window, the Runs are grouped in **Approved**, **Pending Approval**, **Rejected** and **Inactive** tabs. The Runs are grouped based on the current status and you can click on the respective tabs to view.

ORACLE Anti Money Laundering Event Scoring APPROVER | Monday, January 8, 2018

You have 1 Pending Approvals

Execution Runs Data Groups

Data Groups

Approved **Pending Approval** Rejected Inactive

Results View Run Details

Type to filter X

Scenario	Entity Type	Technique	Run Name ~ Version	Status
(ML/EN) High Risk Transactions - High Risk Counter Party	EXTERNAL_ENTITY	Logistic Regression	Test1 ~ 4	Pending Approval

Page 1 of 1 (1 of 1 items)

1. Click **Pending Approval** to view the Runs that are in Pending Approval status. Select a Run/Data Group and click **Results** to view the execution run results. For more information on Results, see [Viewing and Analyzing Results](#). Select a Run/Data Group and click **View Run Details** to see details of the run. For more information on Runs, see [Creating and Editing Execution Runs](#).

Technique	Deployed Status	Validation AUC	Median AUC	Mean AUC	Std Deviation AUC	Best AUC	Worst AUC	Run.1	Run.2	Total Runs Failed
Logistic Regression	Pending Approval	0.7229	0.7202	0.7202	0.0022	0.7217	0.7186	0.7217	0.7186	0

2. On the Result window, click **Approve** to approve and deploy a technique. Click **Reject** to reject by providing appropriate comments. The rejected Technique will be available to the creator to modify and resubmit. Click **Deploy** to deploy an approved technique.

2.8 Scoring Alerts

Score alerts by using alerts data generated from your AML and pass it through the OFS Anti Money Laundering Event Scoring application to receive a JSON response in readable format. You can then check the data and analyze for further processing.

The following is the procedure to extract alerts scored data from the service:

1. Create an input data file from the real-time alerts that are generated from your AML system.
2. Call OFS Anti Money Laundering Event Scoring by passing the data file. The service returns a Request ID that you can use as the Reference ID for further tracking.
3. Use the Request ID in the service to return the status of the execution: successful or failed.
4. After successful execution, use the Request ID in the service to call a JSON response that has alerts scored data.

SEND US YOUR COMMENTS

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact Oracle Support Services.

NOTE: Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.



OFSAAI

Oracle Financial Services Anti Money Laundering Event Scoring User Guide

Oracle Corporation

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065

U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

www.oracle.com/us/industries/financial-services/

Copyright © 2018 Oracle Financial Services Software Limited. All rights reserved.

No part of this work may be reproduced, stored in a retrieval system, adopted or transmitted in any form or by any means, electronic, mechanical, photographic, graphic, optic recording or otherwise, translated in any language or computer language, without the prior written permission of Oracle Financial Services Software Limited.

Due care has been taken to make this Oracle Financial Services Anti Money Laundering Event Scoring User Guide and accompanying software package as accurate as possible. However, Oracle Financial Services Software Limited makes no representation or warranties with respect to the contents hereof and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this Oracle Financial Services Anti Money Laundering Event Scoring User Guide and the accompanying Software System. Furthermore, Oracle Financial Services Software Limited reserves the right to alter, modify or otherwise change in any manner the content hereof, without obligation of Oracle Financial Services Software Limited to notify any person of such revision or changes.

All company and product names are trademarks of the respective companies with which they are associated.