Oracle® Financial Services

Behavior Detection Application Pack Release Notes

Release 8.1.2.9.0
G27456-02
February 2025

Oracle Financial Services Behavior Detection Application Pack Release Notes, Release 8.1.2.9.0

G27456-02

Contents

1

About This Content

This preface provides supporting information for the Oracle Financial Services Behavior Detection Application Pack Release Notes.

Purpose

This document contains release information for the following products:

- Oracle Financial Services Anti Money Laundering
- Oracle Financial Services Trade Based Anti Money Laundering
- Oracle Financial Services Common Reporting Standards
- Oracle Financial Services Currency Transaction Reporting
- Oracle Financial Services Enterprise Fraud Management
- Oracle Financial Services Know Your Customer
- Oracle Financial Services Crime and Compliance Management Analytics

Audience

This document is intended for users of the Oracle Financial Services Behavior Detection Application Pack, specifically those interested in a broad overview of the new features in this release. Additionally, this document is provided for those who want to know specifically which issues or change requests from the previous release have been resolved, which scenarios have been impacted by any changes, and which issues remain.

Documentation Accessibility

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

Access to Oracle Support

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

Related Resources

This section identifies additional documents related to OFS BD Application Pack. You can access the following documents from the OHC library:

- OFS Behavior Detection Application Pack Installation Guide
- OFS Behavior Detection Application Pack User Guide
- Administration Tools User Guide
- Anti-Money Laundering Technical Scenario Description
- Behavior Detection Administration Guide
- Behavior Detection Configuration Guide

- Behavior Detection Data Interface Specification
- Behavior Detection User Guide
- Common Reporting Standard Administration and Configuration Guide
- Common Reporting Standard User Guide
- Currency Transaction Reporting Administration and Configuration Guide
- Currency Transaction Reporting Technical Scenario Description
- Currency Transaction Reporting User Guide
- Financial Crimes Data Model Reference Guide Volume 1: Business Data
- Financial Crimes Data Model Reference Guide Volume 2: Oracle Financial Services Data
- Fraud Technical Scenario Description
- Glossary of Financial Crimes and Compliance Management Products
- Know Your Customer Administration Guide
- Know Your Customer Data Model Reference Guide
- Know Your Customer Risk Assessment Guide
- Know Your Customer Service Guide
- TBAML Administration Guide
- TBAML Data Model Guide
- TBAML Technical Scenario Description
- Scenario Manager User Guide
- Security Guide
- Services Guide
- Oracle Financial Services Analytical Applications Technology Matrix

Conventions

The following text conventions are used in this document.

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

2

About Oracle Behavior Detection

Learn more about Oracle Financial Services Behavior Detection (BD).

In terms of regulatory reporting, financial institutions feel increasingly boxed in. The number, frequency, and complexity of reports continue to spiral, especially for global financial institutions. At the same time, regulators strongly encourage firms to spend more time on analysis and review, such as the US Federal Reserve's guidance that financial institutions spend 80% of the time allocated for regulatory reporting on analytics/reviews and 20% on data compilation. Financial institutions also continue to struggle with data aggregation and quality, and, in many cases, the last stages of reporting are often a largely manual process.

While facing growing regulatory costs and complexity, financial services organizations struggle to realize the positive impact of more rigorous reporting requirements. As a result, they are compiling significantly more data for reporting purposes. Still, they do not have adequate time and resources to fully analyze and gain new insight from this data – translating to a missed opportunity.

The Oracle Financial Services Behavior Detection Applications Pack includes the following applications:

- Financial Services Analytical Applications Infrastructure: This application streamlines analysis using a set of tools for data management and security administration and creates a single, consistent, enterprise-wide source of all relevant customer and financial data.
- Financial Services Behavior Detection: The multiple applications within the Financial Services Behavior Detection platform enable financial institutions to meet their regulatory reporting requirements as part of an integrated financial crime and compliance management approach. It helps reduce compliance costs and manage potential exposures.
  Oracle Financial Services Behavior Detection (BD) provides automated, comprehensive, and consistent surveillance of all accounts, customers, correspondents, and third parties in transactions, trades, and orders across all business lines. The application allows organizations such as banks, brokerage firms, and insurance companies to monitor customer transactions daily, using customer historical information and account profiles to provide a holistic view of all transactions, trades, orders, and other activities. It also allows organizations to comply with national and international regulatory mandates using an enhanced level of internal controls and governance. Behavior Detection is a common platform that supports the following OFSAA products:
  - Anti-Money Laundering Enterprise Edition (AML EE) monitors transactions to identify possible money-laundering activities. These scenarios consider whether the geographical location or entities involved warrant enhanced scrutiny; monitor activity between accounts, customers, correspondents, and other entities to reveal relationships that could indicate efforts to launder funds; address sudden, significant changes in transaction activity that could indicate money laundering or fraud; and detect other types of activities that are considered potentially suspicious or indicative of money laundering.
  - Oracle Financial Services Trade-Based Anti Money Laundering (TBAML) monitors transactions to identify possible trade-based money laundering activities. The product enables comprehensive monitoring of various trade finance contracts during the life of a contract and the trade finance customers and involved parties and facilitates

detection of suspicious activity and proactive investigation and reporting of trade-based money laundering (TBML) activities.

- Know Your Customer (KYC) assesses the risk associated with a customer by considering different customer attributes and enables financial institutions to perform Due Diligence, Enhanced Due Diligence, and continuous monitoring of customers. Cases generated in Know Your Customer can be managed within Enterprise Case Management to track investigations until they have been resolved or reported to the appropriate regulatory authorities.
- Enterprise Fraud Management (EFM) detects behaviors and patterns that evolve over time and may indicate sophisticated, complex fraud activity. These scenarios monitor check and deposit/withdrawal activity, electronic payments, such as funds transfer and payments completed through clearing house (ACH) mechanisms, and ATM and Bank Card to identify patterns of activities that could indicate fraud, counterfeiting or kiting schemes, identity theft or account takeover schemes. Fraud scenarios also monitor employee transactions to identify situations in which employees, acting as insiders, take advantage of access to proprietary customer and account information to defraud the financial institution's customers.
- Currency Transaction Reporting (CTR) analyzes transaction data from the organization and identifies any suspicious activities within the institution that may lead to fraud or money laundering and must be reported to the regulatory authorities. Currency Transaction Reports (CTRs) are created either at the branches or through the end-of-day files, where the CTR application aggregates multiple transactions performed at the branch, ATMs, and Vaults. Oracle Financial Services Currency Transaction Reporting helps the organization file the CTR online with the US Financial Crimes Enforcement Network (FinCEN) using a discreet form or uploaded in a batch form in a specific text file format. CTR alerts are automatically processed and converted into CTR reports or Monetary Instrument Log reports which can be worked through the CTR user interface.

> **Note:**
>
> Oracle Financial Services Currency Transaction Reporting product only applies to North American regulations, specifically US regulatory requirements.

3

Oracle Financial Services Behavior Detection

Learn about the new features, bugs addressed, and known issues in this release of OFS Behavior Detection.

- New Features
- Bugs Fixed
- Known Issues and Limitations

> **Note:**
>
> **ATTENTION:**
> If you are upgrading from a prior release to 8.1.1 or later, please note that the dispositioning of alerts through Alert Management (AM) is no longer supported. AM can be used only to verify the output of Behavior Detection scenarios and is no longer used for alert review. By using AM for dispositioning alerts, customers will be out of compliance with their support contract. The Event Correlation module in Enterprise Case Management (ECM) should be used to correlate events from the FCCM Behavior Detection engine or those ingested from external applications. Customers are required to use ECM for reviewing and investigating alerts. A restricted use license of ECM is provided with the BDF license, which replicates the functionality available in AM to the best that is currently available within ECM. Implementations should use the available batch processes to automatically move Alerts from BDF into ECM, where correlation rules will promote them to a case. From the case, all levels of investigation can occur. If this updated process is not clear to your implementation team, you should contact Oracle Partner Network or Oracle Consulting to be trained. As of June 8th, 2021, the following Financial Crimes and Compliance Applications are no longer offered by Oracle Financial Services. These products are not supported on release 8.1.1.1 and later versions:
>
> - Oracle Financial Services Trading Compliance
> - Oracle Financial Services Trading Compliance Enterprise Edition
> - Oracle Financial Services Broker Compliance
> - Oracle Financial Services Broker Compliance Enterprise Edition
> - Oracle Financial Services Trade Blotter

What's New in Behavior Detection 8.1.2.9.0

New, changed, and deprecated features of Oracle Behavior Detection are described, with pointers to additional information.

Topics:

The following sections list the new features included in this release:

- Anti Money Laundering

Anti Money Laundering

The following table describes AML-related new features and enhancements for OFS Behavior Detection Release 8.1.2.9.0:

Feature	Description
Account Feature Mapping	Account Feature table specifies the features for an account that are not explicitly identified in the Account table. It is used to capture the various services associated to an account. The information in this table is used to help with KYC scoring. In this release, ACCT_FEATURE table is now being populated from related staging table STG_ACCT_FEATURE_MAP.
Postal Code Changes management	Postal codes are sometimes changed by the authorities for a given address. In this case, we now make sure a change in postal code, while the rest of the address stays the same, is considered as an "update" of the address, and not a "new" address.
Customer Feature	We released a similar table at Customer level, with associated mappings, in order to capture the various services associated to a customer who does not have an account association.
Merchant Category Code	It is now possible to capture the Merchant Category Code (MCC) in Cash transactions. This can be used in various transaction monitoring scenarios, especially to monitor credit cards transactions involving riskier merchants.
Audit of new Threshold Set Creation via Administration Tool	When a new threshold set is created using Admin tools (threshold editor), it will now also be auditable in KDD_TSHLD_HIST table and be visible in Scenario Manager. Earlier a new threshold set created from Admin tools was not visible in Scenario Manager.
CIB: Significant Change in Trade/ Transaction Activity (Customer Focus) Highlights	This scenario has now a parameter *Display Transactions* that allows client to configure whether to display detailed transactions and trades of current months.

Know Your Customer

The following table describes KYC-related new features and enhancements for OFS Behavior Detection Release 8.1.2.9.0:

Feature	Description
Enhancements to the Accelerated Re-review (ARR) highlights display in the KYC Risk Assessment UI	The ARR highlights are modified to better display the Rule name, Old and New value details.
KYC Risk Assessment UI Enhancement	The grid names *Party Address* and *Party Identification Documents* have been renamed as *Related Party Address* and *Related Party Identification Documents*, respectively, for better understanding.
Enhancements to the KYC Simulation Aggregate Report	Only the latest risk assessment record for a customer (imported from the production environment) is considered for comparison with simulation results.
Enhancements to display Customer Email and Identification Document Verification (IDV) Details	Customer Email and IDV details are now displayed as part of the ECM UI for the KYC OB case type.

Other Noteworthy Changes

> **Note:**
>
> As of now, Behavior Detection 8.1.2.9.0 supports HTTPS 1.1 and does not support HTTPS 2.0.

Scenario Wizard is decommissioned with the 8.1.2.6.0 release. In the Scenario Wizard folder of the 8129 Installer Package, the associated configuration files are deleted. Due to deletion constraints, the Scenario Wizard folder can still be seen at path <$FIC_HOME/ficweb>. This will be removed in next major installer release.

If you are upgrading from 8.1.2.5.0 or an older version, Scenario Wizard will still remain in the deployed area. Since Scenario Wizard is no longer supported from 8.1.2.6.0, you must delete the Scenario Wizard war and jar files by following these steps:

1. Navigate to: #deployed_area/SMLiteWeb and delete SMLiteWeb.war
2. Navigate to: #deployed_area/SMLiteWeb/WEB-INF/lib and delete all the jar files
3. Navigate to: #deployed_area/SMLiteWeb/lib and delete all the jar files

Bugs Fixed in This Release

This section describes the issues which were resolved in this release.

The following bugs have been addressed in OFS Behavior Detection Release 8.1.2.9.0.

Table 3-1 Resolved Issues

Component	Bug ID	Description
BD	37025880	BD8129:Behavior Detection Version 8.1.2. ML Release # 9 (8.1.2.9.0).
BD	37565131	Mapping to Populate CUST.ULTMT_INSTL_CUST_INTRL_ID field of CUST Table is Missing In CUSTOMER.STG_PARTY_MASTER.SQL
BD	37032098	8.1.2.9 Terrorist Financing Scenario 114000123: Mismatch Between the Primary Dataset (114018197) Vs the Wire Dataset (114018175).
BD	37067982	Terrorist Financing Scenario 114000123: Mismatch Between Highlights and Matched Transactions.
BD	37167993	8.1.2.9 Networks of Accounts Performance Issue with Primary Rule.

Table 3-1 (Cont.) Resolved Issues

Component	Bug ID	Description
BD	37215980	8.1.2.9 Anomalies in ATM, Bank Card: Structured Cash Deposits is not Generating Alerts When LOC_CT is 0.
BD	37283098	8.1.2.9 Scenario Hub and Spoke SCNRO_ID - 118860005 Code CDT_TRXNS Amount Should Check the Incoming Parameter.
BD	37364853	Scenario Hub and Spoke SCNRO_ID - 118860005 the Scenario Code CDT_TRXNS Amount Should Check the Incoming Transaction Amount.
RTF	37354690	Alert Details Export Issue.

Known Issues

Learn about the issues you may encounter and how to work around them.

There are no known issues/limitations in OFS Behavior Detection Release 8.1.2.9.0.

4

Oracle Financial Services Analytical Applications Infrastructure

Learn about Oracle Financial Services Analytical Applications Infrastructure.

For more information on new features, resolved issues, or the known issues/limitations of Oracle Financial Services Analytical Applications Infrastructure, see the Oracle Financial Services Analytical Applications (OFSAA) documentation.

5

Hardware and Software Tech Stack Details

The Technology Stack Matrices for Oracle Financial Services Analytical Applications contains information on supported operating systems and pre-requisites required to use each application.

The hardware and software combinations required for OFS BD 8.1.2.9.0 are available in the OHC Tech Stack.

6
Licensing Information

Learn more about third-party software tools used in this release.

For details on any third-party software tools used, see the OFSAA Licensing Information User Manual Release 8.1.2.0.0, available in the OFSAA Generic Documentation Library.