

Oracle® Sanctions Application Pack

Readme



Release 8.1.2.11.0

G50092-01

February 2026

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE®

Oracle Sanctions Application Pack Readme, Release 8.1.2.11.0

G50092-01

Copyright © 2000, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Oracle Financial Services Sanctions Application Pack Release v8.1.2.11.0

2 About This Release

2.1	What's New	1
2.2	Bugs Fixed	2
2.3	Known Issues	2

1

Oracle Financial Services Sanctions Application Pack Release v8.1.2.11.0

Learn about the Oracle Financial Services (OFS) Sanctions Application Pack v8.1.2.0.0 Minor Release.

Oracle Financial Services (OFS) Sanctions Application Pack is a separately licensed product.

Description

Oracle Financial Services (OFS) Sanctions Application Pack v8.1.2.0.0 Minor Release #10 8.1.2.11.0 (ID 38384230).

This Oracle Financial Services (OFS) Sanctions Application Pack release is cumulative of all enhancements and bug fixes since the v8.1.2.0.0 release.

Prerequisites

Refer to the following prerequisites:

- Before applying Oracle Financial Services (OFS) Sanctions Application Pack v8.1.2.11.0, it is required to install Oracle Financial Services (OFS) Sanctions Application Pack v8.1.2.0.0. For detailed instructions on installing this Sanctions Application Pack Release, see [Installation Guide](#).

How to Apply This Patch

For detailed instructions on installing the OFS Sanctions Application Pack 8.1.2.11.0 release, see the [Oracle Financial Services \(OFS\) Sanctions Application Pack Installation Guide](#).

2

About This Release

Learn about the Oracle Financial Services (OFS) Sanctions Application Pack v8.1.2.0.0 Minor Release.

This section describes the new features, bugs addressed, and known issues in this release.

- [What's New](#)
- [Bugs Fixed](#)
- [Known Issues](#)

2.1 What's New

New, changed, and deprecated features of OFS Sanctions Application Pack are described, with pointers to additional information.

The following list describes new features and enhancements for OFS Sanctions Application Pack Release 8.1.2.11.0:

Customer Screening

- **Audit trail for batch screening** : Introduced the capability to track and extract an audit trail from the backend for batch screening activities. This enhancement allows users to review customer data that was screened, alongside the corresponding matched watchlist data.
This feature provides verifiable evidence that screening was executed at the correct time, against the appropriate watchlists, and using proper configurations such as matching thresholds, algorithms, and rule sets. It also ensures complete transparency by capturing relevant match details from the watchlist, supporting compliance and audit requirements.
- **Queue criteria enhancements**: Queue management now supports filtering alerts and including them in queues based on Dow Jones watchlist attributes. You can configure queue criteria using Dow Jones watchlist attributes such as watchlist name, country, list provider name, list category, and list reference name.
This enhancement enables queues to display alerts according to specific watchlist attributes, allowing administrators to assign alerts more efficiently to user groups with the appropriate expertise for investigation.
- **Display PEP Role End Date**: For each PEP alert, all relevant PEP roles will be shown, along with their respective start and end dates.
This provides detailed information such as role and associated dates enables clear identification of whether an individual is a current PEP, a former PEP, or associated with a time-limited public function. Standardizing these specific PEP attributes helps reduce subjective interpretation and enhances consistency in decision-making.

Transaction Filtering

- **ISO 20022 Goods and Ports Support**: Goods and ports screening for ISO messages is now supported via a dedicated web service with XPath mapping.
Ensures all ISO 20022 messages are thoroughly screened for restricted goods and ports, reducing the risk of costly compliance violations. Identifies and flags potential sanctions-related issues early in the transaction

- **ISO Message Screening:** Screening web service mappings for ISO message categories have been enhanced to support jurisdiction and business domain–specific configurations. This provides more granular control over which screening service is invoked for a given ISO message, based on regional and line-of-business requirements. Users can now configure and assign tags to each screening web service mapping for ISO message categories. Tags can be defined based on Jurisdiction and Business domain.

2.2 Bugs Fixed

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

The following bugs have been addressed in Oracle Financial Services (OFS) Sanctions Application Pack Release 8.1.2.10.0.

Table 2-1 Resolved Issues

Product	Bug ID	Description
Customer Screening	38369405	Resolved an issue where Customer Screening requests that failed input validation were still being forwarded to EDQ. Invalid requests are now blocked prior to EDQ invocation and the appropriate validation error is returned, reducing unnecessary EDQ calls and ensuring only valid transactions are submitted for screening.
Customer Screening	38472042	Resolved an intermittent issue in Customer Screening where zipper alerts did not consistently reflect status changes after user actions. Zipper alerts now reliably transition to the correct status, ensuring accurate queue visibility and downstream processing.
Customer Screening	37894920	Resolved an issue where real-time screening file uploads could take excessively long (e.g., over 4 hours for 49 records). Screening performance has been improved so small uploads are processed within expected timeframes.
Customer Screening	38451506	Resolved an issue where users experienced errors during the loading of watchlists in Oracle Enterprise Data Quality (EDQ).
Customer Screening	38148053	Added audit trail capability to the Customer Screening batch process. This enhancement enables tracking of batch activities, providing visibility and traceability for audit and compliance requirements.
Customer Screening	38660107	Resolved an issue where the alert filter within the Queue Management screen was not functioning as expected for Customer Screening (CS). The alert filter now correctly filters and displays the relevant alerts.
Customer Screening	38266392	Enhanced the system to ensure that structured fields present in XML files from WC are now correctly imported and available within Oracle Enterprise Data Quality (EDQ), improving data integration and usability.

2.3 Known Issues

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

The following is the list of Known Issues is Customer Screening and Transaction Filtering included in the release 8.1.2.11.0.

Table 2-2 Known Issue List

Product	Bug No	Severity	Description
Transaction Filtering	36973164	3	8.1.2.8.0: Feedback is not generated for AutoAction SLA alerts related to ISO messages.
Transaction Filtering	36973157	3	8.1.2.8.0: Cutoff/SLA functionality does not work as expected for ISO message types.
Transaction Filtering	36925848	3	8.1.2.8.0: The V_ERROR_MSG field is incomplete in the RTI_EXECUTION_ERROR table.