

Oracle® Retail Invoice Matching

Release Notes

Release 14.1.3.1

E92815-02

May 2018

This document highlights a fix available on My Oracle Support to address Data Privacy.

Note: This application's base code is not changing for this numbered version unless the fix referenced below is applied.

This hotfix addresses the following defect:

Bug 27356996- Security Enhancements for Personal Data.

The fix is located at the following Patch number on My Oracle Support:

- 21863001

Data Privacy Overview

This enhancement enables customers to accept and respond to end-user requests for data access, correction, and deletion for individual end-user data records they store in the Oracle Retail Invoice Matching application.

The retailer is responsible for fulfilling this requirement. However, to do so, the retailer requires the capability to request this data from the Oracle application as needed.

As a Data Privacy enhancement, Oracle has created a Platform Data Privacy command line tool to provide retailers with services for requesting access to personal information for review and forget/update the user's personal information if requested.

Some of the examples of the personal information can be:

- First Name
- Last Name
- Address
- Email address
- Fax Number
- Contact numbers, and so on.

The following features are handled in the Platform Data Privacy command line tool:

- End User Access/Right to Access (RTA): Enables retailers to accept and respond to end-user requests for data access, correction, and deletion for individual end-user data records they store in the Oracle service.
- Right to be Forgotten (RTF): Based on the end-user's right to request to forget and/or update their personal information, this feature enables the retailer to delete and/or update (mask) the end-user personal data during the services period. Some of the data critical for the business or is part of a legal requirement might not be deleted.
- Validate Forgotten: Based on the end-user's right to request to forget and/or update their personal information, this feature enables the retailer to validate end-user requests.
- Data Portability: End-users have the right to receive the personal data concerning their own information stored in retail applications. The feature will be handled as part of the Platform Data Privacy command line tool's Right to Access functionality.

Note: With regard to Purging functionality, output files created by the Platform Data Privacy command line tool may be purged.

Note: With regard to Logging functionality, server logs created by the Platform Data Privacy command line tool may be purged.

Installation

The services that are a part of the Platform Data Privacy command line tool are executable through a command line using the Platform Data Privacy API.

Setting up the Java Development Kit (JDK)

Java 1.8 is a prerequisite to install and test the command line tool. This chapter contains instructions on how to properly set up the right version of the Java Development Kit (JDK).

Download and Install Java 8

Windows

Download the latest 64-bit version of the Java SE Development Kit 8.

Install in a location on your local machine. Ensure that the installation folder name does not contain any whitespaces (For example: Program Files).

Define Environment Variables for JDK

To effectively use the JDK on your workstation you will need to define environment variables on your system.

Modify the PATH Variable

Modify your system's existing PATH variable to include the executable program location on your JDK installation. These executables are located under:

```
%JAVA_HOME%\bin.  
PATH=%JAVA_HOME%\bin;%PATH%
```

Testing your JDK Installation

Windows

1. Start a new command line window by selecting Start>Run>Open> and then type cmd.exe.
2. Go to the root directory by typing: cd c:\ <enter>
3. Run the Java compiler and query its version by typing: javac -version
The command should return with the Java version information. Make sure it matches the JDK version you just installed.

The command should return with the Java version information. Make sure it matches with the JDK version you just installed.

Example:

```
D:\gdpr>java -version
java version "1.8.0_66"
Java(TM) SE Runtime Environment (build 1.8.0_66-b18)
Java HotSpot(TM) 64-Bit Server VM (build 25.66-b18, mixed mode)

D:\gdpr>javac -version
javac 1.8.0_66
```

UNIX

1. Start a new UNIX session (For example: A Putty Session)
2. Go-To the HOME directory

```
export JAVA_HOME=<Absolute path where JAVA is installed>
export PATH=$JAVA_HOME/bin:$PATH
```

The command should return with the Java version information. Make sure it matches the JDK version you just installed.

Example:

```
/vol.rtk/java/oracle_linux/jdk1.8.0_112.64bit>java -version
java version "1.8.0_112"
Java(TM) SE Runtime Environment (build 1.8.0_112-b15)
Java HotSpot(TM) 64-Bit Server VM (build 25.112-b15, mixed mode)
/vol.rtk/java/oracle_linux/jdk1.8.0_112.64bit>
```

Configuring the Configuration Files

For the Platform Data Privacy command line tool to work, there are several configuration files that need to be configured.

- DATAPRIV-Global.xml: Contains DB connection details as well as details of the customer-id-format. This needs to be modified to enter database information.
- ContextOverride.properties: Contains details of the connection string to be used when using Oracle Wallet. This needs to be modified to enter the correct database information.
- DATAPRIV-Get.xml: Contains the SQL query or function to perform the Right to Access and Validate Forgotten. Changes are already completed and there are no changes necessary by the User.
- DATAPRIV-Forget.xml: Contains the SQL query or function to perform the Right to Forget. Changes are already completed and there are no changes necessary by the User.

1. Create a folder called DataPrivacy.
2. Unzip ReIM_Data_Priv.zip
3. In the ContextOverride.properties, update the datasource string to the environment where this needs to be tested -

For Example: for 14.1.1

```
datasource-url=jdbc:oracle:thin:@hostname:port/service name
```

Common instructions for both RTA & RTF for UNIX Environment:

Export the following environment variable:

1. export DATAPRIV_DIR=<Full Path of 'DataPrivacy' directory created in the above step>
2. Run the following command on <DataPrivacy_directory>

```
chmod 777 -R < DataPrivacy_directory>
```

Common Instruction for Windows Environment:

Set the following environment variable:

set DATAPRIV_DIR=<Full Path of 'DataPrivacy' directory created in above step>.

Creating and Configuring Oracle Wallet

Oracle Wallet is used to store database credentials instead of encoding these details in the configuration file (ContextOverride.properties).

1. Create an empty wallet file in a DataPrivacy/Wallet directory by running the following command in a CMD prompt in Windows and in a Unix Session in the Unix Box in the DataPrivacy directory.

```
java -classpath %DATAPRIV_DIR%/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl
%DATAPRIV_DIR%/Wallet -create
```

OR

```
java -classpath $DATAPRIV_DIR/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl
$DATAPRIV_DIR/Wallet -create
```

You will be prompted for a password. This password will manage the contents of the wallet files.

Note: Remember this password as it will be needed in succeeding commands against the wallet files.

2. Add the database credentials into the wallet by running the following command in the cmd prompt or the UNIX session in the DataPrivacy folder. This will prompt the user to enter the password created in step 1.

```
java -classpath %DATAPRIV_DIR%/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl
%DATAPRIV_DIR%/Wallet -createCredential <hostname:port/service name>
<username> <password>
```

OR

```
java -classpath $DATAPRIV_DIR/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl
$DATAPRIV_DIR/Wallet -createCredential <hostname:port/service name> <username>
<password>
<hostname:port/service name> <username> <password>
```

is the DB connect string.

This should be the same as the one defined in the ContextOverride.properties

- <username> is the DB user to connect to the Database
- <password> is the password to connect to the Database

3. Verify the database credentials in the wallet by running the following command in the CMD prompt or in a Unix Session.

```
java -classpath %DATAPRIV_DIR%/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl
%DATAPRIV_DIR%/Wallet -listCredential
```

OR

```
java -classpath $DATAPRIV_DIR/DATAPRIV_JAR/RetailAppsDataPrivServices-7.0.1-  
RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl  
$DATAPRIV_DIR/Wallet -listCredential
```

```
D:\gdpr>java -classpath ./RetailAppsDataPrivServices-7.0.1-RetailAppsDataPrivTool.jar oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -listCredential  
Oracle Secret Store Tool : Version 12.2.1.2.0  
Copyright (c) 2004, 2016, Oracle and/or its affiliates. All rights reserved.  
  
Enter wallet password:  
List credential (index: connect_string username)  
1: msp00bpz.us.oracle.com:1521/dolsp20app rms01app
```

Make sure the credential information shown by the command is as expected.

Using the Platform Data Privacy Command Line Tool

The tool can be tested in the command line mode using the scripts. The user with admin privileges should run these scripts because the RTF script will delete/update (mask) the data from the tables which are not recoverable.

RTA is used to get the personal data from the ReIM database in an html and xml output format. To run RTA, follow the instructions below:

1. Run RTA.sh script with the following mandatory parameters.
 - First , Last Name & Email of users using separator '::'
 - Invoked By - The user who is running this script.
 - Methods - getReimUser

For UNIX Environments:

For example:

```
/RTA.sh <method_type> <First_Name>::<Last_Name> ::<Email> <Invoked_By> [Maintain  
sequence of input parameters is mandatory]
```

For Windows Environment:

For example:

```
RTA.bat <method_type> <First_Name>::<Last_Name> ::<Email > <Invoked_By> [Maintain  
sequence of input parameters is mandatory]
```

Note: RTA can fetch a maximum of 5 records. If there are more records, the following line will be displayed in the XML output file.

More Rows found for the query but was limited to 5

RTF is used to update the personal data from the ReIM database. To run RTA, use the following instructions:

2. Run RTF.sh script with the following mandatory parameters.
 - ID - User Name
 - Invoked By - The user who is running this script.
 - Methods - forgetReimUser

For UNIX Environments:

For example:

```
RTF.sh <method_type> <Id> <Invoked_By> [Maintain sequence of input parameters  
is mandatory]
```

For Windows Environments:

For Example:

RTF.bat <method_type> <Id> <Invoked_By> [Maintain sequence of input parameters is mandatory]

3. Validate is used to validate forget Personal Data. To run Validate, use the following instructions:

Run the Validate.sh script with following mandatory parameters.

- ID - User Name
- Invoked By - The user who is running this script.
- Methods - validateReimUser

For UNIX Environment:

For example:

Validate.sh <method_type> <Id> <Invoked_By> [Maintain sequence of input parameters is mandatory]

For Windows Environment:

For example:

Validate.bat <method_type> <Id> <Invoked_By> [Maintain sequence of input parameters is mandatory]

Database Tables Impacted Due to RTA/RTF Operations in ReIM

IM_USER_AUTHORIZATION

Output Files

The Output files are located inside below locations:

Windows:

%DATAPRIV_DIR%/Get_Output

%DATAPRIV_DIR%/Validate_Output

UNIX:

DATAPRIV_DIR/Get_Output

\$DATAPRIV_DIR/Validate_Output

Examples of HTML files:

RTA FILE:

User's Information

USERNAME	FIRSTNAME	LASTNAME	EMAIL
RETAIL.USER	RETAIL	USER	RETAIL.USER1@ORACLE.COM

Validate Files

Validate User's Information

USERNAME	FIRSTNAME	LASTNAME	EMAIL
XXXXXX	XXXX	XXXXX	XXXXX@XXXXX

2018, Oracle and/or its affiliates. All rights reserved.

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 software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware and documentation may provide access to or information on 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. 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.

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

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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 on 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. 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.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.