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 27347246 - Security Enhancements for Personal Data

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

- 21863593

> **Note:** The code listed at the My Oracle Support number above is associated in My Oracle Support with a later version of this application; however, you should use that code download location for the line of code referenced in these Release Notes. In other words, the referenced fix above is applicable to multiple versions of this application, including this one.

Data Privacy Overview

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 and/or update their personal information if requested.

Some of the examples of the personal information can be:

- Full Name
- Home address
- Email address
- Date of birth
- Credit card numbers, and so on

The following features are handled as part of MDO / COE data privacy enhancements using the Platform Data Privacy command line tool.

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's 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.

Installation

The services that are part of the Platform Data Privacy command line tool are executable through a command line executable JAR file: RetailAppsDataPrivTool.jar

Setting up the Java Development Kit (JDK)

Java 1.8 is a prerequisite to install and test the Platform Data Privacy command line tool. This section contains instructions on how to set up the Java Development Kit (JDK).

Download and Install Java 8

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

Install in a location on your machine and 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.

Define the JAVA_HOME Variable

Define a new environment system variable named `JAVA_HOME` with a value referring to the path where your JDK is installed. For example:

```
JAVA_HOME=D:\Java\jdk1.8_66
```

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

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.

```
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
```

Platform Data Privacy Command Line Tool

The hotfix contains:

- RetailAppsDataPrivTool.jar
- DATAPRIV-Global.xml
- ContextOverride.properties
- DATAPRIV-ValidateForget.xml
- DATAPRIV-Get.xml
- DATAPRIV-Forget.xml

1. Create a folder called DataPrivacy and copy the RetailAppsDataPrivTool.jar into this folder.
2. Create a folder called config under the DataPrivacy folder and copy the DATAPRIV-Global.xml, ContextOverride.properties, DATAPRIV-ValidateForget.xml, DATAPRIV-Get.xml and DATAPRIV-Forget.xml into this folder.

Configure the Configuration Files

There are few changes necessary to some of the configuration files.

- DATAPRIV-Global.xml
  - No changes necessary to this file.
- ContextOverride.properties.xml
  - Contains details of the connection string to be used in Oracle Wallet.
  - The customer has to update the data source string with the environment database details.
  - The JDBC URL must comply with the following format to reference Oracle Wallet credentials at runtime:
    - A forward slash "/" must be specified BEFORE the "@" character. This instructs the Oracle database driver to be aware of Oracle Wallet aliases.
    - The identifiers following the "@" character must be registered as an alias in the Oracle Wallet. The wallet creation and configuration steps are explained in the next section.
    - Datasource string format - datasource-url=jdbc:oracle:thin:/@hostname:port/SID

      For example: datasource-url=jdbc:oracle:thin:/@myhost:1521/mydb
- DATAPRIV-Get.xml
  - Contains the query or function to perform the right to access.
  - No changes necessary for this file.
- DATAPRIV-Forget.xml

- Contains the query or function to perform the right to forget.
- No changes necessary for this file.

- DATAPRIV-ValidateForget.xml
  - Contains validations to perform prior to right to forget.
  - No changes necessary for this file.

Creating and Configuring Oracle Wallet

The Platform Data Privacy command line tool uses Oracle Wallet to securely store the database credentials. The wallet can be created using the RetailAppsDataPrivTool.jar present in the hotfix.

Here are the steps to be performed to create and configure the Oracle Wallet for the Platform Data Privacy command line tool.

1. Create an empty wallet file in a DataPrivacy directory by running the following command in a command prompt (cmd) in DataPrivacy folder.

   ```
   java -classpath RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI
        -wrl <wallet directory>
        -create
   ```

   For example:

   ```
   java -classpath ./RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -create
   ```

The user will be prompted for a password. This will be the password to 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 command prompt (cmd) in the DataPrivacy folder. This will prompt the user to enter the password created in step 1.

   ```
   java -classpath RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI
        -wrl <wallet directory>
        -createCredential  <db connect string>  <db user>  <db password>
   ```

   The <db connect string> is the database connection string included in a JDBC connection URL in the ContextOverride.properties.xml. It is the part of the JDBC URL after the "@" character.

   It is specified using the format: <hostname>:<port>/<SID>

   For example:

   ```
   myhost:1521/mydb
   ```

   <db user> - DB user to connect to the MDO/COE database.

   <db password> - password to connect to the MDO/COE database.

   For example:

   ```
   java -classpath ./RetailAppsDataPrivTool.jar
   oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet -
   createCredential myhost:1521/mydb coeuser password
   ```

3. Verify the database credentials in the wallet by running the following command in the command prompt (cmd)

```
java -classpath RetailAppsDataPrivTool.jar
oracle.security.pki.OracleSecretStoreTextUI
     -wrl <wallet directory>
     -listCredential
```

For example:

```
java -classpath ./RetailAppsDataPrivTool.jar
oracle.security.pki.OracleSecretStoreTextUI -wrl ./tmp_wallet –listCredential
```

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

Using the Platform Data Privacy Command Line Tool

The Platform Data Privacy command line tool is an executable JAR file that uses the "java –jar" option:

```
java  -Ddatapriv.action=<action>
      -Dinvoked.by=<user ID>
      -DContextOverride.properties=<Context Override Properties file>
      -Duse.jdbc.oracle.wallet=true
      -Doracle.net.wallet_location=<Oracle wallet directory>
      -Dconfig.xml.dir=<configration files directory>
      -Dcustomer.id=<query parameters for the tool>
      -Did.type=employee
      -Doutput.file.dir=<output file directory>
      <other parameters>
      -jar  RetailAppsDataPrivTool.jar
```

The parameters are given to the command line via the system property JVM arguments (-D options).

Understanding the Command Line Parameters

System Property/Parameter	Required	Description
datapriv.action	Always	The data privacy action to be performed: Valid values: ▪ **Access** Retrieve PERSONAL DATA in the system. Required properties to set: customer.id, id.type ▪ **Forget** Remove PERSONAL DATA in the system. Required properties to set: customer.id, id.type
invoked.by	Always	The ID of the user calling the command line tool (for audit purposes)
ContextOverride.properties	Always	The path to a Java properties file that will contain the connection details of the database the Platform Data Privacy command line tool will connect to. Refer to 'Configure the configuration files' for more details.
config.xml.dir	Always	The directory that contains the DATAPRIV configuration XML files.

System Property/Parameter	Required	Description
use.jdbc.oracle.wallet	Always	Set to true to use Oracle Wallet files as a source for database credentials. Refer to 'Creating and configuring Oracle Wallet' for more details.
oracle.net.wallet_location	Always	The path to the Oracle Wallet directory. Refer to 'Creating and configuring Oracle Wallet' for more details.
customer.id	Always	The input parameters to query/update the personal data.
id.type	Always	The query group type for which the data privacy action will be performed. Id.type should be "employee"
output.file.dir	No	The output files directory. The Default is the user's home directory.
datapriv.summary.file.name	No	The output summary file of the action. Defaulted to "ActionSummary-{%datapriv.action%}.xml"
access.output.file.name.no.ext	No	The output file name for access requests. Defaulted to "AccessResults". The file extension depends on access.output.format
access.output.format	No	The output file format for access requests. Valid values: html (default) txt
datapriv.audit.log.dir	No	The directory where the audit log file will be located. The default is the user's home directory.
datapriv.audit.log.name	No	The file name of the audit log file. The default is "datapriv_audit.log"

Understanding the customer.id

The customer.id is the place holder to pass the input parameters to query/update the personal data. It should be the login ID of the employee for which the data needs to be retrieved or removed.

For example: datapriv.action=access query and result.

Query

```
java -DContextOverride.properties=config\ContextOverride.properties
     -Duse.jdbc.oracle.wallet=true
     -Doracle.net.wallet_location=./tmp_wallet
     -Dconfig.xml.dir=config
     -Ddatapriv.action=access
     -Did.type=employee
     -Dcustomer.id=venkat
     -Dinvoked.by=user
     -Doutput.file.dir=Results
     -jar RetailAppsDataPrivTool.jar
```

Result

Employee Information

Login Name	First Name	Last Name	Middle Initial	User Title	Email
JJones	Jeff	Jones		Mr.	JJones@oracle.com

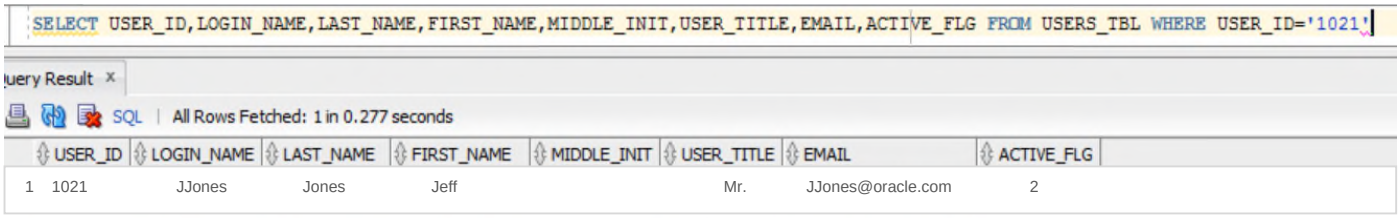
For example: datapriv.action=forget query and result, employee should be in inactive status.

Query

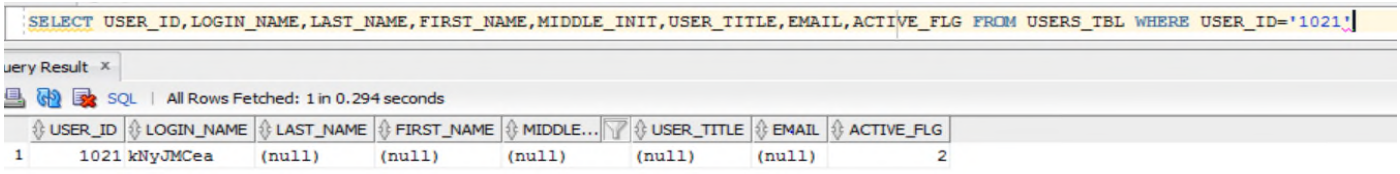
```
java -DContextOverride.properties=config\ContextOverride.properties
         -Duse.jdbc.oracle.wallet=true
    -Doracle.net.wallet_location=./tmp_wallet
    -Dconfig.xml.dir=config
    -Ddatapriv.action=forget
    -Did.type=employee
    -Dcustomer.id=venkat
    -Dinvoked.by=user
    -Doutput.file.dir=Results -jar RetailAppsDataPrivTool.jar
```

Result

Before



After



Understanding the Command Output Files

The command line tool produces the output files after execution. All files are generated by default in the user's home directory. Parameters are available to configure the directory.

Action Summary XML

Each successful call to the tool produces an action summary XML file written in the directory specified in the output.file.dir parameter.

Access Result File

For customer information access results (datapriv.action=access), a readable report file is generated in the format indicated in the access.output.format parameter.

Out-of-the box format options include HTML or Text formats.