Oracle® Retail

XBR*i* Loss Prevention

Release Notes

Release 10.8.3

March 2018

Primary Author: Barbara Clemmer

Contributors: Bill Warrick, Mary Ann Bullis, Mike Zaltsman

Table of Contents

Release Overview

This document covers new security features related to securing personal information, and known and resolved issues for this version. This maintenance release is for Retail & Grocery customers who are or upgrading from XBRi 10.8.2.

Release version	Release Date
10.8.3	03/2018

Functional Enhancements

Full Desc Data View Privilege Option

Full Desc Data View is managed through the application in User Manager. It allows you to perform the following actions related to data privacy.

- **Data Minimization** - The Full Desc Data View privilege option has been added to the Feature Security tab in User Manager. Administrator users can assign the Full Desc Data View feature for any user in order to allow them access to view full data descriptions like names, addresses, email addresses, etc. in certain attributes (see full list in Full Desc Data Attributes description) and in smart linking and watch status.
- **Data Masking** - The existing attributes such as Cashier, Employee, and Customer will now automatically mask private data such as cashier name, employee name, email address, etc. for users who do not have access.
- **Privacy by Design** - After the upgrade, this feature will be turned on automatically for all existing Administrator users. Non-administrator users must have the privilege added.

Report Prompts Added and Modified for Data Protection

New Prompts

- **Data Minimization, Privacy by Design** - The following Object prompts containing (Full Desc) attributes have been added to the individual master reports so a user who has full data access can see the full data if they prefer:

  Cashier Objects (Full Desc)
  Customer Objects (Full Desc)
  District Objects (Full Desc)
  Employee Objects (Full Desc)
  LP District Objects (Full Desc)
  LP Region Objects (Full Desc)
  Region Objects (Full Desc)
  Store Objects (Full Desc)

Modified Prompts

- **Data Minimization, Data Masking, Privacy by Design**
  - The Store Hierarchy Object prompt, included in summary reports in Loss Prevention, was modified to include the attribute Cashier (Full Desc). This additional attribute will only be visible to users with Full Desc Data View privilege.

For example, a user with full data privileges running the Credit/Debit Card Summary report will see the Store Hierarchy Object prompt containing both Cashier and Cashier (Full Desc) attributes for selection. If the user wants to see the full data descriptions, they can add the Cashier (Full Desc) attribute to their report or subscription. Please note: Users who are not privileged will not be able to see the additional attribute in the prompt.

  - The filtering Hierarchy Qualification Prompts were modified to include the (Full Desc) attributes. For example, if a user with Full Desc Data View runs a report with a Hierarchy Qualification Prompt with Cashier, they should also be able to filter on the Cashier (Full Desc) attribute instead of only the masked Cashier attribute. Please note: Users who are not privileged will not be able to see the additional attribute in the prompt.

Reports Added and Modified for Private Data Protection

- **Data Minimization**
  - A new Loss Prevention report called Customer Report (Full Desc) is available for users with Full Desc Data View privileges. The report duplicates the Customer Report in the Master Reports folder, allowing the user to see all of the full descriptions for the Customer without having the masked descriptions included.
  - The Customer Date of Birth Object (Full Desc) was added to the Age Sensitive Transactions report.

Private Data Protection in Subscriptions

- **Data Minimization** - Users without Full Desc Data View privileges will not receive subscription emails if a report with Full Desc Data attributes is included. These users will receive an access error when trying to view the report in the History List or Alert pages.

Private Data Protection in Dashboards

- **Data Masking** - The Sales Activity and KPI dashboards in Loss Prevention have the cashier name masked.

Private Data Protection in Smart Links

- **Data Minimization, Data Masking** - Smart Links have been modified so that the data displayed when the user hovers over an attribute in a report, document, or dashboard that contains personal data, such as Customer or Employee, is determined by the user's Full Desc Data View privileges. If they are allowed to access private data, the full name or description is displayed, otherwise, the masked version is displayed.

Case Management Private Data Protection

- **Data Minimization, Data Masking, Privacy by Design** - After the upgrade, the Case Management feature will be de-selected in User Manager for existing users who are not Administrator users. If a non-Administrator user needs access to Case Management, these users must have their privileges updated by an Administrator to Full Desc Data View access. Cashier name will be masked for users without Full Desc Data View privileges.

Master File Distribution Private Data Protection

- **Data Minimization** - Only users with Full Desc Data View privileges have access to the Master File Distribution Reports folder used to create Dynamic Address Lists.

Report and Feature Restrictions

- **Data Minimization**

  Data Editor

  The Data Editor is now available only to Administrator users with Full Desc Data View privileges.

  Admin Reports

  Admin Reports are now available only to users with Full Desc Data View privileges.

Image Attribute Private Data Protection

- **Data Minimization** - The Cashier image attributes have been removed from the Mobile Dashboard.

New Full Desc Data View Attributes

- **Data Minimization, Data Masking, Privacy by Design** - The following new attributes appended with label (Full Desc) have been added so that users with Full Desc Data View can see the masked data and add these attributes to reports if necessary. Users who are not privileged will not be able to receive or open reports with these attributes in them.

  List of attributes:

  Cashier (Full Desc)

  Cashier Image (Full Desc)

  Custom Store Level1 Email (Full Desc)

  Custom Store Level1 Manager (Full Desc)

  Custom Store Level2 Email (Full Desc)

  Custom Store Level2 Manager (Full Desc)

  Customer (Full Desc)

  Customer Address 1 (Full Desc)

  Customer Address 2 (Full Desc)

  Customer Address 3 (Full Desc)

  Customer City (Full Desc)

  Customer Date of Birth (Full Desc)

  Customer Email (Full Desc)

  Customer First Name (Full Desc)

  Customer Last Name (Full Desc)

  Customer Phone (Full Desc)

  Customer Phone2 (Full Desc)

  Customer State (Full Desc)

  Customer Zip Code (Full Desc)

District Email (Full Desc)
District Manager (Full Desc)
Employee (Full Desc)
Federal ID (Full Desc)
LP District Email (Full Desc)
LP District Manager (Full Desc)
LP Region Email (Full Desc)
LP Region Manager (Full Desc)
Manager (Full Desc)
Region Email (Full Desc)
Region Manager (Full Desc)
ShipTo Address 1 (Full Desc)
ShipTo Address 2 (Full Desc)
ShipTo Address 3 (Full Desc)
ShipTo City (Full Desc)
ShipTo Country (Full Desc)
ShipTo Email (Full Desc)
ShipTo First Name (Full Desc)
ShipTo Last Name (Full Desc)
ShipTo Phone (Full Desc)
ShipTo Phone 2(Full Desc)
ShipTo State (Full Desc)
ShipTo Zip (Full Desc)
Store Email (Full Desc)

Technical Enhancements

Data Purge Process

Data Deletion, Privacy by Design

To enhance data minimization for personal data, a purge process is now configurable for the deletion of inactive Customer, Employee and Store personal data. The application will delete data considered to be personal data in the database, such as customer and ship to names, addresses, email addresses, etc. New settings in pro_sp_variables enable this to be activated when the threshold value reaches the number of days defined. The default setting is 370 days for each:

> **CUSTOMER_INACTIVE_DAYS** - based on number of days since the transaction date that is associated with a customer number. Customer First / Last Name, Shipping Address, Email Address, Shipping First / Last Name, Phone Number, Zip code, State, Country will be deleted from transaction history.
>
> **EMPLOYEE_TERMINATED_DAYS** - based on number of days since the termination date set in the employee master file. Employee first name, last name, federal ID, and employee image data will be deleted from the employee master file.
>
> **STORE_CLOSED_DAYS** - based on number of days since the closed date in the store master file. Manager name and email address will be deleted from the store master file.

NOTE: In order for the purge feature to be activated, calls to the stored procedures need to be added in the daily ETL. Please refer to the 10.8.1 Installation and Configuration Guide for more information.

Integration Enhancements

Right to Access and Right to Erasure

Request for Right to Access, Erase Private Data - The retailer can request specific data, including employee, customer, and user, from the XBRi database using an API. They can also send a request to forget specific data about a customer in the XBRi database through the API. API calls are available to users with corresponding privileges only.

The retailer must install a third-party API tool such as Restlet Client on a Chrome browser. Oracle provides syntax and other required information and a new customer-facing API guide providing step-by-step instructions.

Security Patches

Any identified security risk areas have been addressed through these updates.

Supported Platforms

The XBR^i version 10.8.3 release is supported on the following platforms:

Supported Platforms

Category	Platform	Comments
DBMS	**MS SQL Server 2008, 2012** **Oracle 10g, 11g, 12c**	
OS (Web Server, I-Server)	**Windows Server 2008 R2, 2012**	
OS (Client)	**Windows 7, 10**	
Apple Mac PC and Laptop	**OS X**	For video linking, Apple-compatible video software is required
WEB SERVER	**Apache Tomcat 8 (64 bit)**	
JVM	**JDK 1.8**	JRE 1.8 required for video linking
Browsers		**Comments**
Internet Explorer 11		Compatibility view is not supported
Safari (iPad)		Basic analyst functionality supported on iPad browser
Firefox		Latest version
Google Chrome		Latest version
Mobile Devices (XBR Ingenium mobile)		**Comments**
Apple iPad		iOS9, iOS10, iOS11

Key Known Issues

Category	Reference #	Description
Prompts, Filters, and Custom Groups		When creating prompts, filters, or custom groups through the XBRi Admin facility, be aware that if the full description of a personal data attribute is included, it will be viewable by users without Full Desc Data View access. If you want the full data to be masked for users without Full Desc Data View access, select the masked attribute instead of the full description attribute. If you want the full data to be displayed for users with private data privileges, select the Full Desc attribute and use the Share function to restrict access to only users with Full Desc Data View access.
MFD - subscriptions		When creating Master File Distribution subscriptions, be aware that if the full description of a personal data attribute is included, it will be viewable by the recipient users since these reports are sent via email addresses set up in the master files. If you want the full data to be masked, select the masked attribute instead of the full description attribute in the subscription.
Dashboards		Self Service dashboards that users create through Visual Insight typically contain data from outside the XBRi application, which may contain unmasked personal data viewable to users without Full Desc Data View privileges. Oracle recommends using the Share functionality to restrict access to reports, documents, and dashboards, including the import data brought in through Self-Service BI. The Customer Admin will need to determine by either group(s) or individual(s) who can import data according to their company data privacy policy.
Control Points		If a user with Full Desc Data View access runs a control point with unmasked personal data such as Cashier (Full Desc) and assigns it to a user without Full Desc Data View access, the exception returns an error that the user does not have access to the unmasked personal data. **Workaround:** When a user with Full Desc Data View access runs a control point with unmasked personal data, they should only assign it to users with Full Desc Data View access.

Documentation

In addition to these release notes, the following documentation for XBR^i 10.8.3 maintenance release will be available on or about the date indicated in the OTN library.

Document Title	Release Date	Description
Data Recall/Erase API Guide	03/2018	This guide provides step-by-step instructions on how to install and use an external API to recall or erase specific private data.

The online help for 10.8.2 is accessible from the OTN library as well as from within the application, and has been updated to include private data security enhancements:

Document Title	Release Date	Description
Administrator User Guide	03/2018	This provides the administrator user online help in a format that can be accessed from the OTN library.
Web User Guide	03/2018	This provides the user online help in a format that can be accessed from the OTN library.

The following document for 10.8.1 is accessible from the OTN library and has been updated to include private data security enhancements:

Document Title	Release Date	Description
XBR^{i} 10.8.1 Installation and Configuration Guide(Rev_5)	3/2018	This guide takes you through the upgrade installation of XBR^{i} 10.8.1 in the Oracle data center or at the customer site from database installation through post-installation troubleshooting, application configuration, and mobile configuration.

The following document is accessible from My Oracle Support, and had been updated to include private data security information:

Document Title	Release Date	Description
XBR^{i} 10.8.3 Core Field Mapping Guide	3/2018	This document is intended to describe the CORE POS_STAGING table’s data map.