Oracle® Retail Merchandising On Premise

Security Guide

Release 19.0

F26375-01

January 2020

Oracle Retail Merchandising On Premise Security Guide , Release 19.0 for Windows

F26375-01

Primary Author:

Contributing Author:

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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.

Contents

A Appendix A – FAQ

1 Introduction

Security is a key concern for all retailers. The vast majority of press about security in retail systems concerns Point of Sale (POS) and Customer Order Management Systems (OMS) which process highly sensitive data like customer PII (personally identifiable information) and payment card information. However, security in retail ERP systems is also important.

Oracle Retail Merchandising Operations Management Suite

The Oracle Retail Merchandising Operations Management Suite is a collection of customer managed solutions that provides retailer HQ employees with breakthrough retail ERP capabilities. These features include role-based dashboards that surface relevant buying, inventory, pricing and financial information, leveraging retail science and data analytics to accelerate critical decision making. By using Oracle's modern exception-based retailing methodology to identify situations that require attention, the solution vastly reduces the amount of time merchandising professionals spend on nonproductive tasks and frees up more time to focus on strategic business goals.

Oracle Retail Merchandising Operations Management Suite consists of:

- Oracle Retail Merchandising System
- Oracle Retail Pricing (optional licensable component)
- Oracle Retail Allocation (optional licensable component)
- Oracle Retail Invoice Matching (optional licensable component)
- Oracle Retail Sales Audit (optional licensable component)
- Oracle Retail Trade Management (optional licensable component)

Goals

The goals of this document are to:

- Explain the security responsibility in the customer managed model
- Outline the security features in Retail Merchandising Operations Management Suite
- Refer readers to other documentation that details secure product installation and management

2 Responsibilities

Security is a complex topic. While some security concerns are common, every retailer will have slightly different compliance and internal security goals. As the security landscape is so varied, this document cannot prescribe a simple set of required actions. Instead, the document intends to highlight common topics that retailers should plan for in their implementations.

Oracle Retail

In the customer managed model, Oracle Retail is responsible for:

- Starting all work with secure product engineering practices
- Designing applications with securable architecture and technologies
- Installing applications in a secure manner
- Delivering product authentication and authorization features
- Providing guidance which helps retailers use the security features of other Oracle products and services

Retailer

In the customer managed model, the customer/retailer has extensive security responsibilities, including but not limited to

- Procuring the servers where applications and data will be housed
- Regularly hardening servers by applying CPUs (Critical Patch Updates)
- Building and managing the firewalls used to control access to the network
- Controlling the ability to query and extract data from underlying databases
- Monitoring for security warnings, using SIEM and other management practices
- Implementing user management practices
- Ensuring that end-user devices meet the minimum and security requirements
- Ensuring data quality and enforcing end-user devices security controls, so that antivirus, malware and other malicious code checks are performed on data and files before uploads

Customers may choose to fulfill these responsibilities through deployment in a Cloud using either:

- **Infrastructure as a Service** (IaaS)
- **Platform as a Service** (PaaS)

- or **On Premise**

The full scope tasks related to of secure deployment depends on implementation choices made by the retailer and is outside of the scope of this document. However, this document will recommend known Oracle best practices, tools and documents when possible.

3 Oracle Retail Security

There are two components to Oracle Retail Security:

- Secure Product Engineering
- Data Security

Secure Product Engineering

Oracle builds secure software through a rigorous set of formal, always evolving security standards and practices known as Oracle Software Security Assurance (OSSA). OSSA encompasses every phase of the product development lifecycle.

More information about OSSA can be found at:

https://www.oracle.com/corporate/security-practices/assurance/

The cornerstones of OSSA are Secure Coding Standards and Security Analysis & Testing.

Secure Coding Standards include both general use cases and language specific security practices. More information about these practices can be found at:

https://www.oracle.com/corporate/security-practices/assurance/development/

Security Analysis and Testing includes product specific functional security testing and both static and dynamic analysis of the code base. Static Analysis is performed using tools including both internal Oracle tools and HP's Fortify. Dynamic Analysis focuses on APIs and endpoints, using techniques like fuzzing to test interfaces and protocols.

https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html

Specific security details of the Merchandising are discussed in detail later in this document.

Data Security

Oracle Retail uses a number of strategies and policies to ensure the Retailer's data is fully secured:

- Data Design

  Oracle Retail applications avoid storing PII and PCI data. Where PII data exists in a system, Data Minimization, Right to Access and Right to Forget services exist to support data privacy standards such as GDPR & CCPA.

- Storage

Oracle Retail applications use encrypted tablespaces to store sensitive data.

- Merchandising also implements data filtering so that user's see the data stripes relevant to their own jobs. Merchandising Data Filtering is described in more detail later in this document.

4

Merchandising Architecture

This chapter describes:

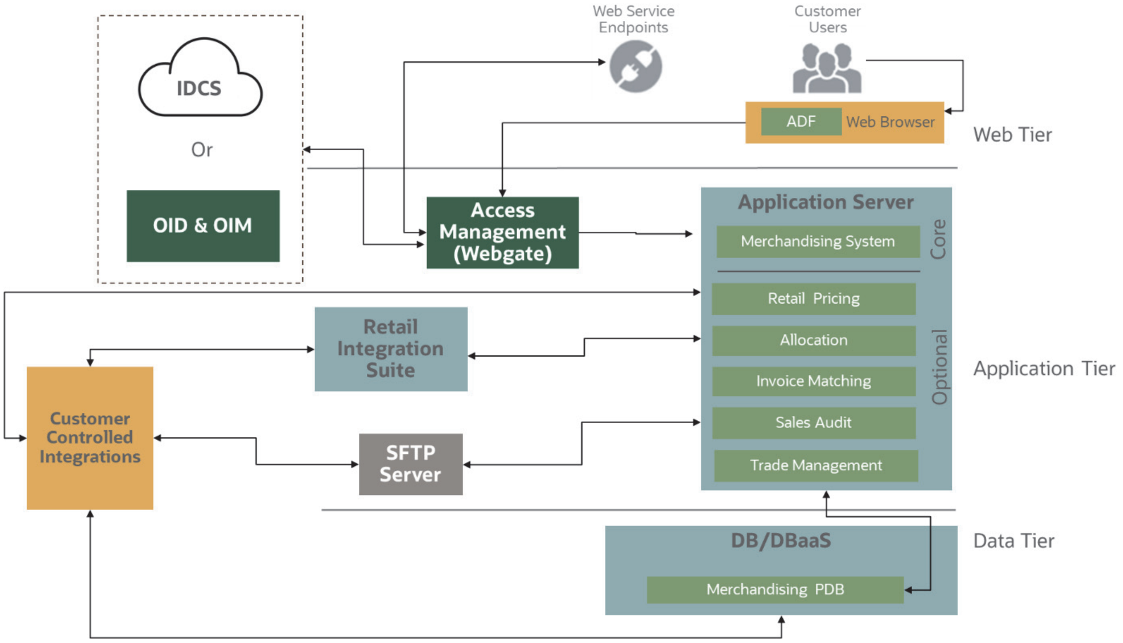
- Logical Architecture
- Integration

Logical Architecture

Most customer access to the Merchandising is accessed using the Web Tier. End users access the applications using a web browser. ReST services are also exposed for a limited set of merchandising business transactions. Retailers should use appropriate perimeter network appliance to protect Merchandising from the internet at large.

Merchandising has been tested using Oracle Access Management Webgate to intercept http requests and forward them appropriately for authentication and authorization.

Figure 4–1 Merchandising Architecture



Merchandising has been tested with two options for AuthN & AuthZ:

- Oracle Identity Management (including Oracle Internet Directory and Oracle Identity Manager)

  `https://www.oracle.com/middleware/technologies/identity-management/`

- Oracle Identity Cloud Service (IDCS)

  `https://www.oracle.com/cloud/paas/identity-cloud-service.html`

The Merchandising Suite consists of a set if ADF-based Java applications. Built in ADF-DVT provides the business intelligence. Additional business processing occurs using scheduled jobs, written in Java, ProC and ksh

The underlying container database includes one pluggable database (PDB). Transparent data encryption (TDE) is set during Merchandising installation (more information can be found in the Merchandising Installation Guide). Tablespaces that contain PII data are encrypted. Applications are able to access the Merchandising schema on the Merchandising PDB.

Customers can optionally also choose to replicate data from the underlying database to DAS (Data Access Schema), a remote target schema for customer integration and reporting. The default implementation for this replication uses Oracle Golden in a secure configuration with encrypted trail files.

Integration

Merchandising integrates with external business systems using three major types of integration:

- Native Files Upload or Download (using SFTP)
- Native Rest Services
- Retail Integration Suite, which includes:
  - Retail Integration Bus (RIB)
  - Retail Service Bus (RSB)
  - Bulk Data Integration (BDI)

Native Files Upload or Download

Merchandising creates and received files from some external systems. Generally, these files are moved using customer controlled SFTP into a directory that Merchandising can access (information about defining this directory can be found in the *Oracle Retail Merchandising Installation Guide*). Customers should implement anti-virus and anti-malware scanning on all inbound files before processing by Merchandising.

Native Rest Services

Merchandising Rest services are secured using basic authentication against an identity provider.

Retail Integration Suite

All communication between Merchandising and the Retail Integration Suite is accessed using secured web services. Further information about security and the Retail Integration Suite can be found in the Retail Integration Suite security guides.

5

Merchandising Authentication, Authorization and Data Filtering

Authentication confirms the identity of a user (*Is this user John Smith?*).

Authorization determines what parts of an application a user can access and what actions the user can perform (*Is John Smith allowed to create a purchase order?*).

Data Filtering is not strictly part of merchandising security model, but can be implemented to further reduce attack surface (*John Smith is allowed to create a purchase order, but only for items in Department 1234*).

Authentication

Merchandising has been tested with two identity providers (IDP):

- Oracle Identity Management (IDM), specifically Oracle Internet Directory (OID)
- Oracle Identity Cloud Service (IDCS)

In either case, the Oracle Access Management Webgate performs the authentication flow. See the Oracle Access Management documentation for more information about OAM and how to configure the Webgate.

https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.3/aiaag/integrating-webgate-oidc-server.html#GUID-60FD7688-25AA-4407-99EC-755792A823FC

Oracle Identity Management

The Oracle Identity Management (IDM) platform delivers scalable solutions for identity governance, access management and directory services. This modern platform helps organizations strengthen security, simplify compliance and capture business opportunities around mobile and social access. Oracle Identity Management is a member of the Oracle Fusion Middleware family of products.

https://www.oracle.com/middleware/technologies/identity-management/

Within the IDM platform, Oracle Internet Directory (OID) is a LDAP v3 compliant directory. Oracle Identity Manager (OIM) provides identity governance.

IDM & Oracle Retail Enterprise Roles

Oracle Retail provides LDIF scripts to load Enterprise Roles into OID. You can find more information about loading these LDIF files in the Merchandising Installation Guides.

OID & Application Users

When application users are created in OID, they must be associated with an appropriate Oracle Retail Enterprise Role to access Merchandising. For more detailed information and procedures, see the *Oracle Fusion Middleware – Administering Oracle Internet Directory*.

`https://docs.oracle.com/en/middleware/idm/internet-directory/12.2.1.4/administer/index.html`

Oracle Identity Cloud Service

Merchandising supports Oracle Identity Cloud Service (IDCS) as an identity provider (IDP).

https://www.oracle.com/cloud/paas/identity-cloud-service.html

IDCS is Oracle's cloud native security and identity platform. It provides a powerful set of hybrid identity features to maintain a single identity for each user across cloud, mobile, and on-premises applications. IDCS enables single sign on (SSO) across all applications in a customer's Oracle Cloud tenancy. Customers can also integrate IDCS with other on premise applications to extend the scope of this federated identity management.

IDCS is available in two tiers:

- Foundation
- Standard

Foundation

Oracle Identity Cloud Service Foundation: Oracle provisions this free version of Oracle Identity Cloud Service for customers that subscribe to Oracle Software-as-a-Service (SaaS), Oracle Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) applications. A customer can use this version to provide basic identity management functionalities, including user management, group management, password management, and basic reporting.

Standard

Oracle Identity Cloud Service Standard: This licensed edition provides customers with an additional set of Oracle Identity Cloud Service features to integrate with other Oracle Cloud services, including Oracle Cloud SaaS and PaaS, custom applications hosted on-premises, on Oracle Cloud, or on a third-party cloud, as well as third-party SaaS applications. Features listed in this pricing tier are applicable for both Enterprise users and Consumer users

IDCS and Oracle Retail Enterprise Roles

Oracle Retail provides LDIF scripts to load Enterprise Roles into IDCS. You can find more information about loading these LDIF files in the Merchandising Installation Guides.

IDCS and Application Users

The customer administrator user has the ability to define password complexity and rotation rules. All Application User maintenance is performed by Customer Administrator using IDCS. A key feature of IDCS is that basic user maintenance can be further delegated using identity self-service.

When application users are created in IDCS, they must be associated with an appropriate Oracle Retail Enterprise Role to access Merchandising. For more detailed information and procedures, see Managing Oracle Identity Cloud Service Users in *Administering Oracle Identity Cloud Service*.

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/manage-oracle-identity-cloud-service-users1.html

Note: IDCS username will be passed to Merchandising as the application User ID. It will be persisted on the database as part of the basic Merchandising transaction audit trail. If corporate e-mail address is used as the IDCS username, corporate e-mail address will be persisted to the Merchandising database. To fully inform Merchandising users that their corporate e-mail address will be saved, we recommend that retailers implement IDCS Terms of Use functionality.

The IDCS Terms of Use feature enables retailers to set the terms and conditions for users to access an application, based on the user's consent. This feature allows the identity domain administrator to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service. The Terms of Use feature can be used to explicitly obtain user consent to persist corporate e-mail address for Merchandising auditing. For more information about Terms of Use, refer to the Administering Oracle Identity Cloud Service.

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/understand-terms-use.html

Authorization

As an ADF application, Merchandising manages authorization to access application functions using Fusion Middleware's security model. Fusion security supports a role-based, declarative model that employs container-managed security where resources are protected by roles that are assigned to users. Duties and privileges provide a further level of control.

Users are associated with Enterprise Roles in IDCS or OID. Enterprise Roles are mapped to Merchandising Duties and Privileges. Default mappings of Enterprise to Merchandising Duties and Privileges are provided as part of Merchandising installation.

Roles

The default configuration includes a number of default roles. This document describes some sample roles for each application in describing the overall security model. For a full set of roles for each Merchandising application, refer to the application specific security guides:

- Merchandising Security Guide Volume 2 - Merchandising and Import Management
- Merchandising Security Guide Volume 2 – Pricing
- Merchandising Security Guide Volume 2 - Sales Audit
- Merchandising Security Guide Volume 2 – Allocation
- Merchandising Security Guide Volume 2 - Invoice Matching

Sample roles include but are not limited

- Application Administrator

- Data Steward
- Buyer
- Inventory Analyst
- Inventory Manager
- Corporate Inventory Control Analyst
- Pricing Analyst
- Allocator

These roles are used in common terminology throughout the business processes defined in the Oracle Retail Reference Model (MOS Doc ID 2458078.1).

Duties and Privileges

Within the Merchandising Suite, Enterprise Roles are mapped to Duties and Privileges. Privileges are essentially actions that a user can perform. Duties are collections of related privileges.

In the Merchandising Suite, role-based security is implemented to control:

- Access to navigational links/tasks in the application. The role associated with the user (for example a Buyer or Inventory Analyst) determines the set of links visible in the task pane.
- Access to various UI widgets in the screens like buttons, menu items, LOVs, Panels and so on. The role determines if the UI widgets are to be shown or hidden and if shown whether they need to be enabled or disabled.
- How the screens are opened, such as in an Edit or View Only mode based on the role the user belongs to and the duties and privileges mapped to that role.

Duties are intended to build on one another and work in a hierarchical manner. The example in the table below illustrates how this works using purchase orders as an example.

The most basic purchase order duty is Purchase Order Inquiry, which grants the user permission to search and view purchase orders. The next level of access is Purchase Order Management, which grants the user the ability to search and view purchase orders, but also maintain and submit them. The final level of access in this example is Purchase Order Approval, which grants the user the ability to approve orders, in addition to searching, viewing, and maintaining them.

Duty	Privileges
Purchase Order Inquiry	Search Purchase Orders View Purchase Orders
Purchase Order Management	All Privileges in Purchase Order Inquiry Maintain Purchase Orders Submit Purchase Orders
Purchase Order Approval	All Privileges in Purchase Order Management Approve Purchase Orders

Application Specific Security Guides

The application specific security guides for each solution in the Merchandising Suite describe the Privileges and Duties for each application. See the following documents for more information:

- Merchandising Suite Security Guide Volume 2 - Merchandising and Import Management
- Merchandising Suite Security Guide Volume 2 – Pricing
- Merchandising Suite Security Guide Volume 2 - Sales Audit
- Merchandising Suite Security Guide Volume – Allocation
- Merchandising Suite Security Guide Volume - Invoice Matching

Administrator users can change the mappings of Enterprise Roles, Duties and Privileges in the Merchandising user interface. Details about how to manage these application security policies are available in Chapter 2, Manage Security Policies in the *Oracle Retail Merchandising Administration Guide*.

Data Security/Filtering

Merchandising offers an additional optional layer of data filtering. Data filtering in the application UI limits the data end users see by levels in the merchandise and organizational hierarchies.

> **Note:** Data Filtering is implemented in all Merchandising Suite applications, with the exception of Allocation.

Data level security is configured by assigning users to a data security group within Merchandising. All users within a group would have similar access to a particular section of the merchandise or organizational hierarchy. For example, a group may be defined for a particular division, giving users across Application Roles access to the departments, classes, subclasses, and items in that division.

To implement data security/filtering, Data Security Groups must be defined in Merchandising. These groups are associated with levels of the merchandise and organizational hierarchies. Every application user must also be defined in Merchandising and assigned to Data Security Groups. The processes for defining these groups, hierarchy associations and users is detailed in Chapter 3, Data Security/Filtering in the *Oracle Retail Merchandising Administration Guide*.

> **Important: It is important to note that adding these users to Merchandising for data security/filtering purposes is a manual process (using a spreadsheet upload). Users are not automatically loaded from the identity provider for data security purposes.**

When considering whether to implement data filtering/security, customers should consider the benefits of data filtering and the processes they would need to implement to synchronize Merchandising with their identity provider. As authentication is based on user definition, it is possible that a user could authenticate correctly and reach Merchandising and based on the mapping of their Enterprise Role to Application Role, be authorized to access various user interfaces. However, if the data filtering/security is in use, and the user is defined in Merchandising or not associated with a Data Security Group, the user may not see certain types of data in the application.

Right to Access and Right to Forget

Merchandising provides a web service interface for Right to Access and Right to Forget. The service provides a REST call to return end-user information based on a provided key, and a REST endpoint for

Merchandising provides three groups (type_id) for right to access and right to forget.

- CustomerRecord

  By providing customer number as key, the end user can access or forget the PII data for the customer, customer address, and history sales information related with this customer.

- Employee

  By providing employee number as key, the end user can access or forget the PII data for the employee.

- Supplier

  By providing primary contact name as key, the end user can access or forget supplier contact name and supplier contact phone number information.

6

Recommendations

This chapter describes recommendations for:

- Deployment
- Infrastructure Security
- Secure Installation

Deployment

In the customer managed model, customers determine their deployment physical architecture. With regard to security, Oracle Retail recommends that customers consider the following:

- Merchandising Suite should be deployed on a collection of servers or Virtual Machines (VMs). Each VM should resides in an appropriate tier and each tier should resides in its own subnet. Communication between tiers should limited by subnet ingress security lists.
- To reduce attack surface, access to Merchandising should be very limited, using appropriate network perimeter devices.
- Both outbound web service traffic and replication of data should be routed through the outbound proxy in the DMZ.

Infrastructure Security

The security of the underlying infrastructure used to deploy Oracle Retail applications must be regularly hardened. Critical patch updates must be applied by the retailer on a regular schedule. Oracle maintains a running list of critical patch updates and security alerts.

https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Before installing Merchandising Suite applications, customers should ensure that underlying Linux VMs are secure. The fundamental principles of using Oracle Linux security are:

- Keep Software Up to Date
- Restrict Network Access
- Follow the Principle of Least Privilege
- Monitor System Activity
- Keep Up to Date on the Latest Security Information

You can find details of all best practices for Oracle Linux security in the Oracle Linux 7 Security Guide

`https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/E54670.pdf`

Secure Installation

The installation instructions for all Merchandising Suite applications have been updated to include security best practices as a default. You can find more information in the Installation Guides for each application in the Merchandising Suite.

A

Appendix A – FAQ

This appendix provides a list of frequently asked questions (FAQs) and answers for Merchandising security.

FAQs

Does the Merchandising support data encryption?

Yes. Sensitive (PII) data is stored in encrypted tablespace.

Does the Merchandising provide strong authentication options such as two-factor or one-time Password?

Multi-Factor Authentication is an option if a customer chooses to license the Standard Tier of IDCS.

Does the Merchandising include a configurable warning banner which is presented upon login?

Terms of Use is an option if a customer chooses to license the Standard Tier of IDCS. It presents disclaimers and acceptable use policies to users.

Does the Merchandising include and support the capability to change default account passwords?

All user password management occurs in the identity provider, either OID or IDCS.

Does the Merchandising support Roles with defined access levels?

Yes. Oracle Retail Enterprise roles span Oracle Retail applications. Within Merchandising, privileges and duties can be assigned to roles to define what is accessible to certain types of users.

Does the Merchandising provide strong password options such as complexity, history, aging, or account lockout?

Password management is strictly the responsibility of the identity provider.

OID provides password policy management functionality. User passwords are validated against policies. Policies define the rules passwords must adhere to. More information about password policies is available at:

https://docs.oracle.com/en/middleware/idm/internet-directory/12.2.1.4/administer/managing-password-policies1.html#GUID-3C7B1B95-ECA3-4831-A93C-1CE0FA1F4D3C

IDCS provides robust password policy management functionality. When a user creates a password, IDCS validates the password against the password policies. More information about password policies is available at

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/manage-oracle-identity-cloud-service-password-policies1.html