Oracle® Retail Mobile Merchandising

Security Guide

Release 16.0

E79520-02

January 2018

ORACLE

Oracle Retail Mobile Merchandising Security Guide, Release 16.0

E79520-02

Primary Author: Harish Ramamurthi / Rakhee Prabhudesai / Glenn Gonzales / Gopal Edara

Contents

3 Security Features

4 Security Considerations for Developers

Send Us Your Comments

Oracle Retail Mobile Merchandising Security Guide, Release 16.0

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our web site at http://www.oracle.com.

Preface

The *Oracle Retail Mobile Merchandising Security Guide* serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail Merchandising Operations Management (MOM) Suite applications. Installation and configuration for each product are covered in more detail in the each product's Installation Guide.

Audience

This document is intended for System Implementers (SIs) and Administrators.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents.

- *Oracle Retail Mobile Merchandising Installation Guide*
- *Oracle Retail Mobile Merchandising User Guide*
- *Oracle Retail Mobile Merchandising Implementation Guide*
- *Oracle Retail Mobile Merchandising Release Notes*
- Oracle Retail Allocation documentation
- Oracle Retail Invoice Matching documentation
- Oracle Retail Merchandising System documentation
- Oracle Retail Trade Management documentation
- Oracle Retail Sales Audit documentation
- Oracle Retail Price Management documentation

- Oracle Retail Active Retail Intelligence documentation

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 16.0) or a later patch release (for example, 16.0.1). If you are installing the base release or additional patches, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is also available on the following web site:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

(Data Model documents are not available through Oracle Technology Network. You can obtain them through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

This chapter gives an overview of the product and explains the general principles of application security.

Product Overview

Oracle Retail Mobile Merchandising provides on-the-go visibility into certain Oracle Retail Merchandising application transactions and provides the ability, in some cases, to take action on existing transactions. The specific functions supported within Mobile Merchandising are:

- Recent Allocations
- Sales Audit (ReSA) Dashboard
- Sales Audit Store Search
- Invoice Matching
- Recent Orders
- Recent Transfers

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up To Date

It is a good practice to keep all software versions and patches up to date.

Restrict Network Access to Critical Services

Keep both the middle-tier and the database behind a firewall. Additionally, place a firewall between the middle-tier and the database. These firewalls ensure that access to these systems is restricted to a known network route which can be monitored and restricted. The alternative is a firewall router that substitutes for multiple and independent firewalls.

If firewalls cannot be used, configure the TNS Listener Valid Node Checking feature which restricts access to IP addresses. Restricting database access by IP address can cause application client/server programs to fail for DHCP clients. Methods to resolve this include using static IP addresses, a software/hardware VPN or Windows Terminal Services, or its equivalent.

Follow the Principle of Least Privilege

The principle of least privilege requires users be given the least amount of access to perform their jobs. Excessive granting of responsibilities, roles, grants, and so on (especially early on in an organization's life cycle when people are few and work needs to be done quickly) often leaves a system open to abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three fundamentals: good security protocols, proper system configuration, and system monitoring. The third requirement is met by auditing and reviewing system records. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. For latest versions, see `https://support.oracle.com` regularly.

2

Secure Installation and Configuration

This chapter outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Understand Your Environment

To better understand security needs, review the following questions:

- **What resources am I protecting?**

  Many resources in the production environment can be protected. This includes information in databases accessed by the Mobile application through Web Services and the integrity of the Mobile application. Identify the resources that need protection when deciding the level of security you must provide.

- **From whom am I protecting the resources?**

  For most Mobile applications, resources must be protected from everyone having access to the Mobile device.

  – Should your employees/specific roles have access to the resources within the Mobile Application?

    Consider giving access to highly confidential data or strategic resources to only a few well trusted roles.

  – Should system administrators have access to all Mobile resources?

    Consider restricting the access of system administrators to the data or resources.

- **What will happen if the protections on strategic resources fail?**

  In some cases, a fault in your security scheme is easily detected and causes nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the Mobile application. Understanding the security ramifications of each resource helps you protect it properly.

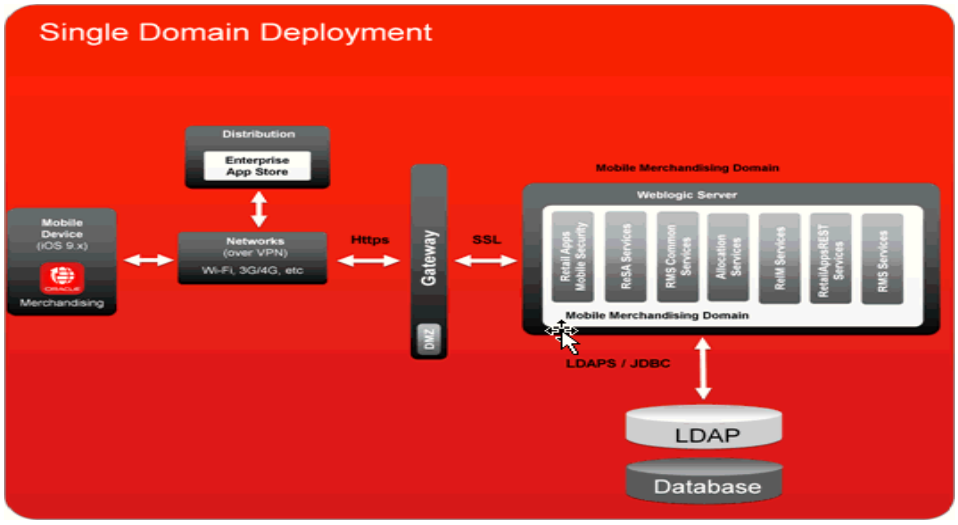
Recommended Deployment Topologies

This section describes the recommended architectures for deploying Oracle Retail Mobile Merchandising to secure its access.

Single Domain Deployment

In the absence of the Enterprise SSO solution, a single domain deployment is recommended to enable SSO control of the features. Since Basic Auth App and all the services reside in the same domain, the user credentials generated by Basic Auth App are valid for all the services deployed in the domain. This allows users to navigate between different features without feature specific login prompts.

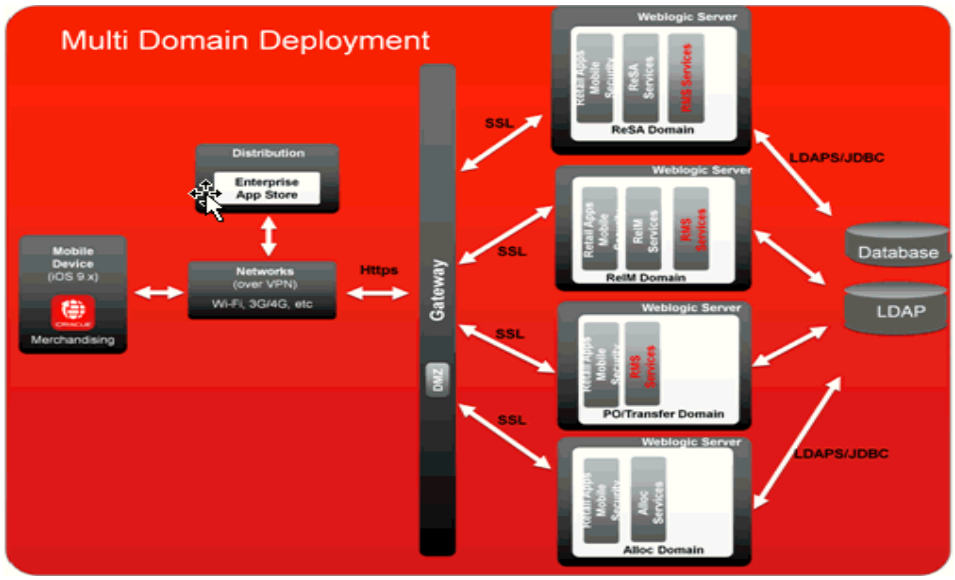
Figure 2–1 Single Domain Deployment Diagram



Multiple Domain Deployment

Multiple domain deployment is the most common deployment scenario where each application feature and its services reside in their own domain. Multiple domain deployment supports feature level authentication where each feature within the Mobile application can be configured to have their own login server. In a non-SSO environment, users are prompted for logins while navigating between the features. In the SSO environment, single login allows users to navigate between the features even though they reside in different domains/servers.

Figure 2–2 Multiple Domain Deployment Diagram



Installing Retail Infrastructure

This section describes steps to install and configure an infrastructure component securely.

Pre-installation of Retail Infrastructure in WebLogic

The Oracle WebLogic Server is primarily used as a Middleware component to deploy Retail Application Services, RetailAppsMobileSecurity, and RetailAppsRESTServices. All the server side components used by the Retail Mobile Merchandising application rely on the security setup used in the Middleware. For more information, see the 'Pre-installation of Retail Infrastructure in WebLogic' section in *Oracle Retail Merchandising Security Guide*.

Post Installation of Retail Infrastructure in Database

The Oracle Retail Application Services, Retail Apps REST Services, and Retail Apps Mobile Access Service uses the Oracle database as the back-end data store. For complete environment security, the database should be secured. For more information, see the 'Post Installation of Retail Infrastructure in Database' section in the *Oracle Retail Merchandising Security Guide*.

Installing Allocation Web Services

Allocation Web Services are packaged as a part of the Allocation's Enterprise Archive (EAR) file as a Web Archive (WAR) within the EAR file. These Web services are installed by default. Allocation Web Services use the J2EE authorization security model. These Web services use the *oracle/http_basic_auth_over_ssl_client_policy* or *oracle/http_http_cookie_client_policy* to support SSL/TSL. For information on the steps related to the installation of Allocation services in secured environment, see Chapter 24 in the *Oracle Retail Allocation Installation Guide*.

Installing ReSA Web Services

The Oracle Retail Sales Audit (ReSA) Web Services are packaged as a part of the ReSA's Enterprise Archive (EAR) file as a Web Archive (WAR) within the EAR file. These Web services are installed by default. ReSA Web Services use the J2EE authorization security model. These Web services use the *oracle/http_basic_auth_over_ssl_client_policy* or *oracle/http_http_cookie_client_policy* to support SSL/TLS. For information on steps related to the installation of ReSA services in secured environment, see Chapter 24 in the *Oracle Retail Sales Audit Installation Guide*.

Installing ReIM Web Services

The Oracle Retail Invoice Matching (ReIM) Web Services are packaged as a part of the ReIM's Enterprise Archive (EAR) file. These services are packaged as a Web Archive (WAR) within the EAR file. These Web services are installed by default. The ReIM Web Services use J2EE authorization security model. These Web services use *oracle/http_basic_auth_over_ssl_client_policy* or *oracle/http_cookie_client_policy* to support SSL/TLS. For information on steps related to the installation of ReIM services in secured environment, see Chapter 14 in *Oracle Retail Invoice Matching Installation Guide*.

Installing RMS Common Web Services

The Oracle Retail Merchandising System (RMS) common Web Services are packaged as a part of the RMS's Enterprise Archive (EAR) file. These services are packaged as a Web Archive (WAR) within the EAR file. These Web services are installed by default. The RMS common Web Services use J2EE authorization security model. These Web services use *oracle/http_basic_auth_over_ssl_client_policy* or *oracle/http_cookie_client_policy* to support SSL/TLS. For information on steps related to the installation of the RMS common services in a secured environment, see Chapter 11 in *Oracle Retail Merchandising System Installation Guide*.

Installing Platform Mobile Security

Platform Mobile Security is used to support Authentication and Authorization features of Retail Mobile Merchandising application. Platform Mobile Security is installed as part of the retail applications. For more information, see the Retail Application's installation guide.

Installing Retail Mobile Merchandising

The Retail Mobile Merchandising application is packaged as the MerchMobileArchive.maa file. Deploying Oracle Retail Mobile Merchandising for use on an iOS device requires that you have a computer running Mac OS X set up for iOS development. For more information on the set up, including secure provisioning profiles and certificates, see Apple's documentation at `https://developer.apple.com/`. For more Oracle specific information, see the *Oracle Retail Mobile Merchandising Installation Guide.*

Post Installation Configuration

The Mobile Merchandising application provides a configuration feature to update the connections.xml file on a mobile device after the application has been installed. It is necessary to host the connections.xml file at a secured location (HTTP Basic authentication) with SSL/TLS setup.

The hosted connections.xml file should contain valid URLs for all connections being used by the application (including the ConfigService and ConfigServiceLogin connections). All the URLs specified in the connections.xml are added to the white list in the application. For more information on securing your configuration, see the *Oracle Retail Mobile Merchandising Implementation Guide*.

Single Sign-On for Services

Oracle supports single sign-on between the Retail Application services using Oracle Access Manager (OAM). For more information, see the Appendix: 'Single Sign-On for WebLogic' in the *Oracle Retail Merchandising System Installation Guide*.

3

Security Features

This chapter outlines the specific security mechanisms offered by the Mobile Merchandising application.

The Security Model

The Mobile Merchandising security model follows the Oracle Fusion Security Model. This model uses Oracle Platform Security Services (OPSS) to fulfil Authentication, Authorization, and Credential management requirements. On the client side, this product uses the Oracle Mobile Application Framework (MAF) security model to protect resources on the device and to communicate with other features within the device. Facets include:

- **Authentication** - Ensuring that only authorized individuals get access to the application and data.
- **Authorization** - Access control to application features. This builds on authentication to ensure that individuals only get appropriate access.
- **Secure Data Storage on the Device** - The Mobile Merchandising application uses a SQLite database that protects locally stored data. MAF applications do not share the SQLite database; the application that creates the database is the only application that can access it. In addition, only users with the correct username and password can access this database.
- **Transport Layer Protection** - It is recommended using SSL/TLS when accessing data over a provider network. Because provider networks can be hacked, never assume that they are safe. SSL should be enforced when the application transports sensitive data. All certificates should be validated to ensure they are legitimate and signed by public authorities.

Configuring and Using Authentication

The Mobile Merchandising application delegates authentication responsibility to the MAF's security components. MAF determines whether access to the application feature requires user authentication when an application feature is secured by a login server. Authentication modes supported in MAF are Basic Auth, OAuth and Web SSO.

The Retail Platform Mobile Basic Auth application is packaged as part of Platform Mobile Security Enterprise Archive (EAR) file. This application is packaged as a Web Archive (WAR) within the EAR file. Retail Mobile Merchandising application uses this application's URL as a login endpoint/server to validate mobile user credentials. It is recommended to use SSL/TSL when accessing login endpoint/server. For more information, see the *Oracle Retail Mobile Merchandising Implementation Guide*.

Configuring and Using Access Control

The Mobile Merchandising application uses MAF's in-built security components and Retail Mobile Access Control Service (ACS) to enforce role based access to Mobile UI features. MAF determines the access to a feature based on the role constraints defined for it.

MAF provides the ability to configure a Retail Mobile Access Control Service to get roles and privileges for a given user. The MAF framework also provides support to validate feature role constraints against the roles returned by Retail Mobile Access Control Service. Features are enabled/disabled based on the verification result.

Introduction to Duty Roles

Duty roles are roles that are associated with a specific task or a logical grouping of tasks. Generally, the list of duties for a job is a good indicator of what duty roles should be defined. Because enterprise roles allow for easier and better management of duty roles, duty roles should normally be granted to enterprise roles and not to specific users.

There are eleven duty roles implemented to control access to features in Retail Mobile Merchandising:

- ALC_MOBILE_MENU_DUTY - To control access to the Allocation Feature
- RESA_MOBILE_MENU_DUTY - To control access to the ReSA Feature
- REIM_MOBILE_MENU_DUTY – To control access to ReIM Feature
- RMS_APPROVE_PURCHASE_ORDER_DUTY – To control access to Recent Orders Feature and provide approve Purchase Order rights
- RMS_MAINTAIN_PURCHASE_ORDER_DUTY – To control access to Recent Orders Feature and provide maintain Purchase Order rights
- RMS_VIEW_PURCHASE_ORDER_DUTY – To control access to Recent Orders Feature
- RMS_APPROVE_TRANSFER_DUTY – To control access to Recent Transfers Feature and provide approve Transfer rights
- RMS_MAINTAIN_TRANSFER_DUTY – To control access to Recent Transfers Feature and provide maintain Transfer rights
- RMS_VIEW_TRANSFER_DUTY – To control access to Recent Transfers Feature
- RMS_APPROVE_INTERCOMPANY_TRANSFER_DUTY – To control access to Recent Transfers Feature and provide approve Intercompany Transfer rights
- RMS_MAINTAIN_INTERCOMPANY_TRANSFER_DUTY – To control access to Recent Transfers Feature and provide maintain Intercompany Transfer rights

Retail Mobile Access Control Service is packaged as part of the Platform Mobile Security Enterprise Archive (EAR) file. This service is packaged as a Web Archive (WAR) within the EAR file. This Service uses *oracle/http_basic_auth_over_ssl_client_policy* or *oracle/http_cookie_client_policy* to support SSL/TLS. For more information, see the *Oracle Retail Mobile Merchandising Implementation Guide*.

Role Mappings

The Mobile Merchandising application is packaged with default role mappings. These role mappings can be changed based on the business needs. Use 'PlatformMobileSecurity' as Application Stripe name to find the default role mappings

in Oracle Fusion Middleware Control. For more information, see the 'Managing Authorization' section in the *Oracle Retail Merchandising Security Guide*.

Configuring and Using Secure Data Storage

The Mobile Merchandising application uses a local SQLite database to persist application state between sessions. This database will be encrypted through the APIs provided by the MAF.

The local database file will be created the first time an application opens a connection to it. It will be encrypted before any queries are allowed to be made using it. The GeneratedPassword class from MAF is provided with the device UUID and is combined with additional random data to create an encryption key. This key is stored in the iOS keychain for future reference. The key is then used to encrypt the newly created database file under the default MAF algorithm (AES 128).

The keychain limits access to any given key to only the application that originally stored it. The keychain file is itself securely encrypted.

The database file is encrypted by MAF's default algorithm (AES 128). While MAF provides two alternative algorithms (RC4 and AES 256), we do not anticipate a change being necessary, as the default option provides sufficient speed and security in storing the data.

For more information on the GeneratedPassword, the encryptDatabase (and its counterpart, decryptDatabase), see *Oracle Fusion Middleware Java API Reference for Oracle Mobile Application Framework*, Section 18.2.7, *How to Encrypt and Decrypt the Database*.

Configuring and Using Transport Layer Protection

Oracle recommends using SSL/TLS when accessing data over a provider network. As provider networks can be hacked, never assume that they are safe. SSL should be enforeced when the application transports sensitive data. All certificates should be validated to verify they are legitimate and signed by public authorities.

For more information, see the
https://docs.oracle.com/middleware/maf242/mobile/develop-maf/understanding-secure-mobile-development-practices.htm#ADFMF24757

For iOS, the Apple application store also requires HTTP-based network requests to be made in HTTPS as part of their App Transport Security (ATS) requirement. Review http://developer.apple.com for more information on ATS.

Configuring Single Sign-On

Oracle Retail Mobile Merchandising supports a Web SSO authentication mode to achieve single sign-on capability across its features.

For more information see section'28.5.5 –How to Configure Web SSO Authentication' in MAF Developers Guide at
https://docs.oracle.com/middleware/maf242/mobile/develop-maf/securing-maf-applications.htm#ADFMF24777

4

Security Considerations for Developers

This chapter covers security considerations for developers.

Reference Information

For more information on how the Mobile Application Framework (MAF) provides protection from common security risks identified by the Open Web Application Security Project (OWASP), refer to:

https://docs.oracle.com/middleware/maf242/mobile/develop-maf/understanding-secure-mobile-development-practices.htm#ADFMF24757