Oracle® Retail Home

Security Guide

Release 19.0.001.7

F30753-01

April 2020

ORACLE®

Oracle Retail Home Security Guide, Release 19.0.001.7

F30753-01

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

Primary Author:

Contributing Author:

Contributor:

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 is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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.

Contents

Send Us Your Comments vii

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix
Customer Support x
Review Patch Documentation x
Improved Process for Oracle Retail Documentation Corrections x
Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com) x
Conventions xi

1 Introduction

Responsibilities 1-1
Retailer Responsibilities 1-1
Oracle Responsibilities 1-1
Oracle Retail SaaS Security 1-2
Secure Product Engineering 1-2
Secure Deployment 1-2
Physical Safeguards 1-2
Network Security 1-3
Infrastructure Security 1-3
Data Security 1-3
Secure Management 1-3
Assessment and Audit 1-4

2 Post Installation Configuration

Configuring Administrator Permissions 2-1

3 Security Features

The Security Model 3-1
Configuring and Using Authentication and Authorization 3-1
Authentication and Authorization for Hosted Containers 3-1
Authentication and Authorization for Weblogic Server 3-1

Configuring and Using the Domain Whitelist 3-2
Configuring the Whitelist for Hosted Containers 3-2
Configuring the Whitelist for Weblogic Server 3-2
Transport Security 3-2

4 Security Considerations for Developers

A Secure Deployment Checklist

B Open Ports

Send Us Your Comments

Oracle Retail Home Security Guide, Release 19.0.001.7

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

This Security Guide provides critical information about the processing and operating details of Product, including the following:

- System configuration settings
- Technical architecture
- Functional integration dataflow across the enterprise
- Batch processing

Audience

This guide is for:

- Systems administration and operations personnel
- Systems analysts
- Integrators and implementers
- Business analysts who need information about Product processes and interfaces

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 in the Oracle Retail Home Release 19.0.001.7 documentation set:

- *Oracle Retail Home User Guide*
- *Oracle Retail Home Administration Guide*

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 3.0) or a later patch release (for example, 3.0.1). If you are installing the base release and additional patch releases, 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 Help Center (docs.oracle.com)

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

https://docs.oracle.com/en/industries/retail/index.html

(Data Model documents can be obtained 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 Introduction

Oracle Retail Home is a portal-based application for the RGBU enterprise, designed to provide a central view and entry point into a customer's Retail applications. The UI provides a tile-based dashboard highlighting important metrics and PKIs across RGBU applications. The dashboards are configured by a Retail Home administrator for each enterprise role.

This document focuses on the secure deployment and configuration of the Retail Home client and services in a cloud environment. This includes deployment in both Weblogic Server and hosted container environments.

Responsibilities

As retailers migrate to the cloud, they must consider how the cloud, and more specifically SaaS, will impact their privacy, security, and compliance efforts. As the cloud service provider, Oracle Retail works together with customers to meet cloud security objectives.

Retailer Responsibilities

At a high level, retailers are responsible for:

- Understanding Oracle's security policies
- Implementing their own corporate policies via Oracle tools
- Creating and administering users via Oracle tools
- 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 uploading data
- Ensuring that end-user devices meet the minimum security requirements
- Generating public/private key pairs as requested by Oracle Retail

To securely implement Retail Home, retailers and their implementation partners should read this document to understand Oracle's security policies. This document summarizes information and contains links to many other Oracle documents.

Oracle Responsibilities

As the cloud service provider, at the highest level Oracle Retail is responsible for:

- building secure software
- provisioning and managing secure environments

- protecting the retailer's data

Retail Home fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. This information is described in great detail later in this document.

Oracle Retail SaaS Security

Security is a many faceted issue to address. To discuss Oracle Retail SaaS security, it helps to define and categorize the many aspects of security. For the purposes of this document, we discuss the following categories of SaaS security:

- Secure Product Engineering
- Secure Deployment
- Secure Management
- Assessment and Audits

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 and 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 through 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 Cloud Service are discussed in detail later in this document.

Secure Deployment

Secure deployment refers to the security of the infrastructure used to deploy the SaaS application. Key issues in secure deployment include Physical Safeguards, Network Security, Infrastructure Security and Data Security.

Physical Safeguards

Oracle Retail SaaS applications are deployed via Oracle Cloud Infrastructure data centers. Access to Oracle Cloud data centers requires special authorization that is monitored and audited. The premises are monitored by CCTV, with entrances

protected by physical barriers and security guards. Governance controls are in place to minimize the resources that are able to access systems. Physical security safeguards are further detailed in Oracle's Cloud Hosting and Delivery Policies.

`http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf`

Network Security

The Oracle Cloud network is isolated from the Oracle Corporate Network. Customer instances are separated down to the VLAN level.

Infrastructure Security

The security of the underlying infrastructure used to deploy Oracle Retail SaaS is regularly hardened. Critical patch updates are applied on a regular schedule. Oracle maintains a running list of critical patch updates and security alerts. Per Oracle's Cloud Hosting and Delivery Policies, these updates are applied to all Oracle SaaS systems.

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 personal data. Where PII data exists in a system, Data Minimization, Right to Access and Right to Forget services exist to support data privacy standards.
- Storage - Oracle Retail applications use encrypted tablespaces to store sensitive data.
- Transit - All data is encrypted in transit, Retail SaaS uses TLS for secure transport of data, as documented in Oracle's Cloud Hosting and Delivery policy.

  `https://www.oracle.com/assets/ocloud-hosting-delivery-policies-3089853.pdf`

- Retail Home also implements role constraints so that users see information relevant to their own jobs.

Secure Management

Oracle Retail manages SaaS based on a well-documented set of security-focused Standard Operating Procedures (SOPs). The SOPs provide direction and describe activities and tasks undertaken by Oracle personnel when delivering services to customers. SOPs are managed centrally and are available to authorized personnel through Oracle's intranet on a need-to-know basis.

All network devices, servers, OS, applications and databases underlying Oracle Retail Cloud Services are configured and maintain auditing and logging. All logs are forwarded to a Security Information and Event Management (SIEM) system. The SIEM is managed by the Security Engineering team and is monitored 24*7 by the GBU Security Operations team. The SIEM is configured to alert the GBU Security Operations team regarding any conditions deemed to be potentially suspicious, for further investigation. Access given to review logs is restricted to a subset of security administrators and security operations personnel only.

Assessment and Audit

Oracle Cloud meets all ISO/IEC 27002 Codes of Practice for Information Security Controls. Third Party Audit Reports and letters of compliance for Oracle Cloud Services are periodically published.

2

Post Installation Configuration

After installing Retail Home, you must configure administrator permissions.

Configuring Administrator Permissions

Administrator users for Retail Home must be assigned the following roles through the authentication provider for the environment:

- RETAIL_HOME_ADMIN
- PLATFORM_SERVICES_ADMINISTRATOR_ABSTRACT

Two additional roles, `RH_ROLE_REQUEST_ABSTRACT` and `RH_ROLE_REMOVE_ABSTRACT`, control permissions for notification administration and need to be assigned to users as well.

3

Security Features

Retail Home has several security features that protect the system and its data. See the following sections for more information.

The Security Model

Retail Home's security requirements come from the need to protect application data from unauthorized changes. This is accomplished by the following security features:

- **Authentication** - Retail Home services restrict access to users that have been authenticated by the configured security provider.
- **Authorization** - Retail Home uses enterprise roles to limit what features individual users can access.
- **Origin Control** - Retail Home services implement the Cross-Origin Resource Sharing (CORS) protocol using a domain whitelist to limit where requests may be made from.
- **Transport Security** - The Retail Home client and services communicate via REST calls from the client. The services also make SOAP calls if configured to use an OBIEE instance. These communications need to be secured.

Configuring and Using Authentication and Authorization

The authentication mechanism for Retail Home depends on whether it is being run inside a hosted container or on a Weblogic Server instance.

Authentication and Authorization for Hosted Containers

When running in a hosted container, Retail Home is deployed behind an Oracle WTSS instance configured to authenticate users against Oracle IDCS. WTSS authenticates with a single sign on for all applications protected by it, which should include all RGBU applications Retail Home is configured for. WTSS and IDCS configuration are covered in their respective documentation.

Retail Home checks for authentication against the same IDCS instance used for authorization.

Authentication and Authorization for Weblogic Server

When running in Weblogic Server, Retail Home can be configured to use authentication and authorization from any supported security provider. This includes running a WTSS instance authenticating via IDCS in front of the Weblogic Server

instance. Refer to the appropriate documentation for securely configuring your chosen security provider.

Configuring and Using the Domain Whitelist

The Retail Home REST services restrict access to clients being served by trusted hosts. This is accomplished using a whitelist of allowed domains. Domains that are not on the whitelist will result in requests being rejected and no CORS headers will be applied to responses.

Configuring the Whitelist for Hosted Containers

When running in a hosted container, the domain whitelist is provided as part of the container configuration. The container handles setting it on the services.

Configuring the Whitelist for Weblogic Server

When installing to a Weblogic Server, the whitelist will be set by default to only contain the domain of the host server. This will disallow connections from clients hosted elsewhere.

Transport Security

To ensure the security of service calls made by Retail Home, follow the following rules when configuring endpoints:

- Always use TLS encryption. Endpoints should be HTTPS URLs and the servers should be configured to use trusted certificates.
- Route access through WTSS or equivalent. Make sure all URLs are to the location exposed on WTSS or will otherwise be independently authenticated.

4

Security Considerations for Developers

The Retail Home services do not support extension by developers. There are no special security considerations for the development of dashboard extensions for the client.

A

Secure Deployment Checklist

The following security checklist covers the main guidelines for securing a Retail Home installation:

1. Restrict network access.
2. Follow the principle of least privilege.
   - Restrict who has the RETAIL_HOME_ADMIN, PLATFORM_SERVICES_ADMINISTRATOR_ABSTRACT, RH_ROLE_REQUEST_ABSTRACT, and RH_ROLE_REMOVE_ABSTRACT roles.
   - Do not use a privileged user to run a Retail Home container.
3. Apply all security updates for Retail Home and the environment.
4. Configure authentication providers.
5. Set the domain whitelist.
6. Use secure endpoints for service configurations.

B

Open Ports

In Weblogic Server, Retail Home listens on the port of the server(s) it is deployed on.

By default, the Retail Home container listens on port 7201. Clients should not directly contact this port; it should only be accessed by connections forwarded by WTSS.