Oracle® Retail Home

Security Guide

Release 3.0.2

F16689-01

February 2019

ORACLE®

Oracle Retail Home Security Guide, Release 3.0.2

F16689-01

Primary Author: Matthew Scheele

Contributing Author: February 2019

Contributor:

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

Oracle Retail Home Security Guide, Release 3.0.2

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 3.0.2 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 Technology Network

Oracle Retail product documentation is 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 these documents 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

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 chapter 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.

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up to Date

Good security requires keeping up to date with the latest releases and patches of installed software. This document assumes Retail Home is up to date and being run in updated and supported environments.

Restrict Network Access to Critical Services

Retail Home uses REST services for communication between the client and server. Ensure that the server is deployed in a secure network environment and that all access goes through appropriate firewalls and authentication mechanisms. Additionally, be sure that other network resources used by the application, such as databases and other RGBU applications, are likewise deployed in secure environments.

Follow the Principle of Least Privilege

Retail Home restricts administrative duties to users assigned administrator roles. Ensure that these roles are not assigned except to users who need them.

When running in a hosted container, Retail Home must use a User ID that can read the wallet files with its credentials. The wallets should therefore be created as a non-root user, and that user should not have any extra permissions beyond what is needed to run the container.

Monitor System Activity

Monitoring the activity on the system is essential to maintaining security. Retail Home services log events to the host machine. These logs should be regularly audited.

Keep Up to Date on the Latest Security Information

The Retail Home software and documentation are regularly updated. Check this document with each update for revisions.

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.