# Oracle® Retail Data Store
## Security Guide

G11471-01
July 2024

Oracle Retail Data Store Security Guide,

G11471-01

# Contents

# Preface

This guide describes the administration tasks for Oracle Retail Data Store.

### Audience

This guide is intended for administrators, and describes the administration tasks for Oracle Retail Data Store.

### 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.

### 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

### Oracle Help Center (docs.oracle.com)

Oracle Retail Product documentation is available on the following website https://docs.oracle.com/en/industries/retail/html

### Comments and Suggestions

Please give us feedback about Oracle Retail Help and Guides. You can send an e-mail to: retail-doc_us@oracle.com

### Oracle Retail Cloud Services and Business Agility

Oracle Retail Merchandising Cloud Services is hosted in the Oracle Cloud with the security features inherent to Oracle technology and a robust data center classification, providing significant uptime. The Oracle Cloud team is responsible for installing, monitoring, patching, and upgrading retail software.

Included in the service is continuous technical support, access to software feature enhancements, hardware upgrades, and disaster recovery. The Cloud Service model helps to free customer IT resources from the need to perform these tasks, giving retailers greater

business agility to respond to changing technologies and to perform more value-added tasks focused on business processes and innovation.

Oracle Retail Software Cloud Service is acquired exclusively through a subscription service (SaaS) model. This shifts funding from a capital investment in software to an operational expense. Subscription-based pricing for retail applications offers flexibility and cost effectiveness.

1

# Security Features

Oracle Retail Data Store (RDS) provides the following security features.

## Authentication and Single Sign-On

Authentication in RDS is managed through Oracle Cloud Infrastructure Identity and Access Management (OCI IAM). The OCI IAM tenant that protects the RDS tools and extensions is the same tenant that is used by the rest of the Oracle Retail suite of applications, enabling SSO.

## Oracle REST Data Services and Application Express

RDS is provisioned with Application Express (APEX) workspaces for each of the Oracle Retail applications that replicate data to RDS for customer use. Access to these workspaces requires a valid OCI IAM user in the customer's tenant. After being provisioned, the customer is provided with the URLs to access these workspaces. The customer must create a user in OCI IAM with a predefined name; that user will be the initial user that can access the workspaces, and can grant access to other users. See the Implementation Guide for further detail. These workspaces can be used to create custom Oracle REST Data Services (ORDS) Restful web services and custom APEX applications. Once created, these custom web services and APEX applications are protected by OCI IAM, and do not require the additional APEX user credentials to access them.

## Database

When data is replicated into RDS from other Oracle Retail applications, it is stored in schemas that are read-only to the customer. Separate read-write schemas in RDS are made available to the customer to hold their custom extensions for each application. These read-write schemas are accessible and may be manipulated through the APEX workspaces.

When new database objects are replicated into the read-only schemas, they are not initially accessible to the read-write schemas. A process runs periodically that detects new objects and grants read privileges for them to the read-write schema, at which point they may be used in the APEX workspaces for custom extensions.

# 2
# Responsibilities

Oracle Retail and their retail partners work in tandem to secure RDS.

## 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

> **Note:**
>
> Retailers are responsible for using valid, certificate authority (CA) signed certificates for TLS. For more information, see My Oracle Support (Doc ID 2710163.1).

To securely implement Oracle Retail Data Store Cloud Services, 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

Oracle Retail Data Store Cloud Services fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies.

3

# Oracle Retail SaaS Security

Security is a many faceted issue to address. When discussing 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

## 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 via 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

## 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.

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

Before Oracle Retail deploys code to SaaS, Oracle's Global Information Security team performs penetration testing on the cloud service. This penetration testing and remediation prevents software or infrastructure issues in production systems.

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

## 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 personal 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

# 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.

4

# Post Installation Configuration

RDS uses several predefined access roles to refine user access to several capabilities. A user is associated with a role by assigning them to an OCI Group. These groups are created for the client at the time of provisioning.

> **Note:**
>
> It can take up to an hour for a new group assignment to take effect.

## Oracle Data Visualization

Oracle Data Visualization users must be assigned to one of the following groups:

| Group Name | Purpose |
|---|---|
| <tenant-id>-DVConsumer | For report viewers |
| <tenant-id>-DVContentAuthor | For report creators and maintainers |

The tenant ID is made available as part of the client activation process.

## Oracle BI Publisher

Oracle BI Publisher users must be assigned to one of the following groups:

| Group Name | Purpose |
|---|---|
| <tenant-id>-BIConsumer | For report viewers |
| <tenant-id>-BIContentAuthor | For report creators and maintainers |

The tenant ID is made available as part of the client activation process.

## Retail DB Ops Console

Users of the Retail DB Ops Console must be assigned to one of the following groups:

| Group Name | Purpose |
|---|---|
| RDS_MANAGEMENT_VIEWER | Allowed to view system generated AWR reports, Top SQL, DBMS Jobs in production environment |

| Group Name | Purpose |
|---|---|
| RDS_MANAGEMENT_VIEWER_PREPROD | Allowed to view system generated AWR reports, Top SQL, DBMS Jobs in pre-production environments |
| RDS_MANAGEMENT_OWNER | Same as VIEWER plus allowed to create custom AWR reports in production environment |
| RDS_MANAGEMENT_OWNER_PREPROD | Same as VIEWER_PREPROD plus allowed to create custom AWR reports in pre-production environments |
| RDS_MANAGEMENT_ADMINISTRATOR | Same as OWNER plus allowed to view DB Metrics and edit application properties in production environment |
| RDS_MANAGEMENT_ADMINISTRATOR_PREPROD | Same as OWNER_PREPROD plus allowed to view DB Metrics and edit application properties in pre-production environments |