Oracle® Retail Merchandising Cloud Services

Security Guide

Release 16.0.031

F21283-01

July 2019

ORACLE®

Oracle Retail Merchandising Cloud Services Security Guide, Release 16.0.031

F21283-01

Primary Author: Nathan Young

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 Merchandising Cloud Services Security Guide, Release 16.0.031

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 document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail Merchandising Cloud Services applications.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the above mentioned product, in order to facilitate and support the secure operation of the Oracle Retail Product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

We assume that the readers have general knowledge of administering the underlying technologies and the application.

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

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, 16.0.031). 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.

Convention	Meaning
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

Software as a Service (SaaS) is changing technology today. SaaS applications shift responsibilities from retailers and their data centers to cloud service providers. The cloud service provider is responsible for upgrades, uptime and security. Oracle provides many retail cloud services, including Oracle Retail Merchandising Cloud Services.

The Oracle Retail Merchandising Cloud Service is a suite of software-as-a service solutions that provides retailers with breakthrough capabilities. This includes 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 Cloud Services consists of:

- Oracle Retail Merchandising Foundation Cloud Service
- Oracle Retail Pricing Cloud Service
- Oracle Retail Allocation Cloud Service (optional licensable component)
- Oracle Retail Invoice Matching Cloud Service (optional licensable component)

This document is divided into six main sections:

- Responsibilities – The Responsibilities section of the document discusses the shared responsibility model of security.
- Oracle Retail SaaS Security – This section of the document outlines the policies and procedures Oracle Retail uses to meet its security responsibilities.
- Merchandising Cloud Services Architecture – This section details the architecture of the Merchandising Cloud Service, particularly as it relates to security.
- Merchandising Cloud Services Authentication, Authorization and Data Filtering – This section describes how Merchandising Cloud Service performs authentication and authorization, as well as how data filtering can be applied.
- Additional Secure Set Up for Merchandising Cloud Services – This section describes other security set up that must be performed by retailers and Oracle Retail.
- Frequently Asked Questions – This section includes a number of specific questions related to security that are frequently asked by prospects, customers and implementers.

The goals of this document are to:

- Explain the security responsibilities of Oracle and the Retailer in the SaaS model
- Educate retailers about Oracle's cloud security policies and controls
- Describe Merchandising Cloud Service's
  - general architecture, particularly as it relates to security
  - security features
- Define additional steps customer IT staff must perform to communicate securely with Merchandising Cloud Service
- Guide Customer administrators in the actions they need to perform to
  - create application users
  - assign roles to application users
- Provide answers to frequently asked questions about Merchandising Cloud Service security

2

Responsibilities

As retailers migrate to the cloud, they must consider how the cloud, and more specifically Software-As-A-Service (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 Merchandising Cloud Service, 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

Merchandising Cloud Service fulfills its responsibilities by a combination of corporate level development practices and cloud delivery policies. Sections in this document will describe this information in great detail later in this document.

3

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 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

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 datacenters. 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 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
- Merchandising Cloud Service also implements data filtering so that users see the data stripes relevant to their own jobs. Merchandising Data Filtering is described in more detail later in this document.

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.

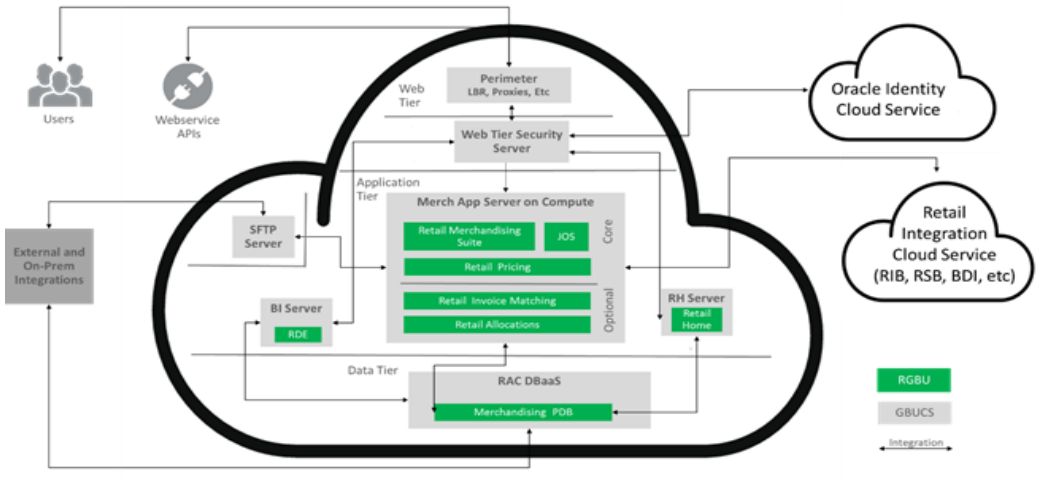
4

Merchandising Cloud Services Architecture

Merchandising Cloud Services is a set of ADF-based Java applications deployed on Oracle's Global Business Unit Cloud Services 3.x Platform Services. The applications are deployed in a highly available, high performance, horizontally scalable architecture. As of release 16.0.030, Merchandising Cloud Services uses Oracle Identity Cloud Service (IDCS) as its identity provider (IDP). Information about logical, physical and data architecture in this document focuses on how the architecture supports security.

Note: Oracle Retail Merchandising Cloud Services deployments currently on versions 16.0.029 and lower currently use an instance of Oracle Identity Management (IDM) Suite within Merchandising Cloud Services as an IDP. As these live customers are upgraded to 16.0.030 and transitioned to GBUCS3, their authentication will be transitioned to use IDCS. Oracle Retail will move any user and group information currently in the live SaaS customer's IDM suite to the customer's IDCS tenancy.

Logical Architecture



Most customer access to the Merchandising Cloud Service is via the web tier. The web tier contains the perimeter network services that protect the Merchandising applications from the internet at large. All traffic from the web tier continues to the Web Tier Security Server (WTSS), which in turn uses the customer's Oracle Identity

Cloud Service (IDCS) tenancy to perform authentication. More information about authentication via IDCS is provided later in this document.

The application tier consists of a number of application servers. These servers provide the Merchandising applications and Job Orchestration (JOS), which allows retailers to schedule Merchandising batch jobs. A BI server provides access to Oracle Business Intelligence Enterprise Edition (OBIEE) reporting. If a customer also uses Oracle Retail Insights Cloud Service, this BI server will also host the ODI jobs that extract facts and measures from Merchandising for RI. RetailHome is a UI component that can serve as a coordinated dashboard for many Oracle Retail cloud services.

The underlying container DBaaS includes one pluggable database (PDB). Applications are able to access the Merchandising schema on the Merchandising PDB. Transparent data encryption (TDE) is set during provisioning. Tablespaces that contain personal data are encrypted.

Merchandising Cloud Services applications integrate with external business systems via:

- Native files upload/download
- Native Rest Services
- Retail Integration Cloud Service, which includes Retail Integration Bus (RIB), Retail Service Bus (RSB) and Bulk Data Integration (BDI)

Merchandising Cloud Services uploads and downloads some files via an SFTP server, which resides in a dedicated network tier. Customer accounts are created in the SFTP server by the GBUCS operations team per a standardized process. All inbound files are scanned by anti-virus and anti-malware software.

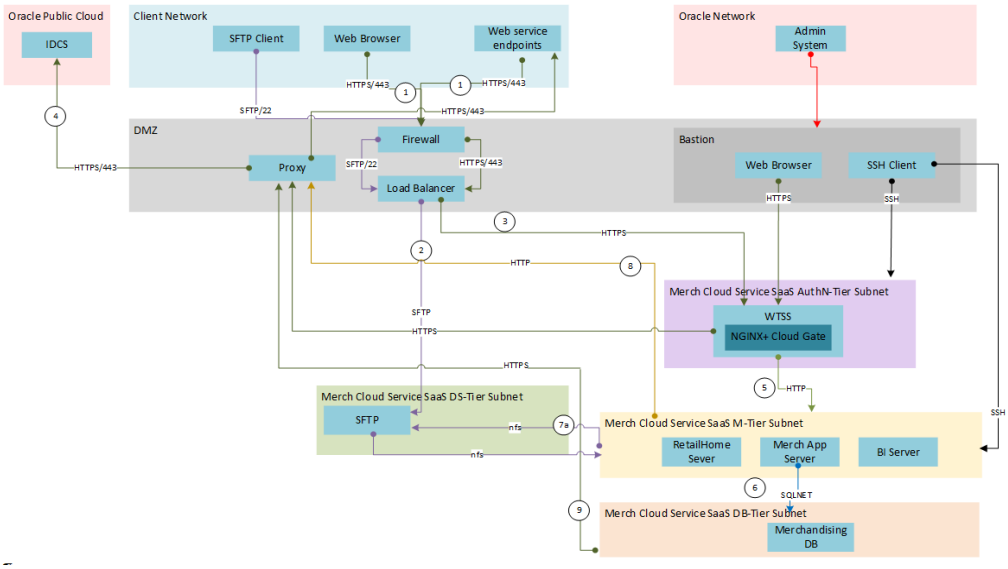
Merchandising Cloud Services authenticates native rest services using OAUTH2.0 via IDCS. As a common authentication pattern is used, web service users are subject to the same strong controls as application users. All rest service calls are logged in the application logs.

All communication between Merchandising Cloud Services and Retail Integration Cloud Service is via secured web services.

Retailers may also choose to replicate a subset of their data from the Merchandising PDB to an external database controlled by the Retailer. The replication uses Oracle Golden Gate. All Golden Gate trail files are encrypted and communicated via https. The retailer is responsible for securing the target destination database.

Physical Architecture

This document does not explain the full physical architecture of the Merchandising Cloud Service, but instead focuses on the high level aspects of this physical architecture that relate to security.



Merchandising Cloud Services is deployed on a collection of single tenant VMs. Each VM resides in an appropriate tier and each tier resides in its own subnet. Communication between tiers within the Merchandising Cloud Service is limited by subnet ingress security lists.

To reduce attack surface, access to the Merchandising Cloud Service from the open internet is very limited. As described in the Logical Architecture section of this document, Business Users (via web browser) and external web service endpoints access application over https/443 (1). Firewall and load balancer in the DMZ pass traffic to the WTSS server in the Authentication Tier (3), which in turn to requests authentication (via outbound proxy) from the customer's Identity Cloud Service (IDCS) tenancy (4). Additionally, authenticated sftp users are able drop and collect files (2).

Within the Merchandising Cloud Service itself, traffic between tiers is very limited. Authenticated requests are passed from the AuthN Tier to the M-Tier (5). Access to the underlying DBaaS is only available via the M-Tier (6). The M-Tier is able to get and place files into storage within the DS-Tier (7), which in turn allows the exchange of files with authenticated sftp users (2). Both outbound web service traffic (8) and replication of data (9) are routed through the outbound proxy in the DMZ.

A subset of Oracle Retail AMS has very limited access to the underlying DBaaS and M-Tier via Bastion host. This access is limited to a small subset of Oracle employees as described in Oracle's Cloud Hosting and Delivery policy.

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

5

Merchandising Cloud Services 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 the Merchandising Cloud Services 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 and IDCS

As of version 16.0.030, Merchandising Cloud Services uses Oracle Identity Cloud Service (IDCS) as its identity provider (IDP).

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

When a user connects to the Merchandising Cloud Service UI, Merchandising Cloud Services redirects application URL requests to the IDCS login screen. IDCS authenticates the user. When a user logs out of the Merchandising Cloud Service, Merchandising invokes an IDCS logout to disable session authentication.

IDCS

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 SSO.

IDCS is available in two tiers: Foundation and Standard.

- 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.
- 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.

Details of the specific features available in each tier and IDCS Standard Tier licensing model are available in Administering Oracle Identity Cloud Service. Merchandising Cloud Services only requires the Foundation Tier, as the Foundation Tier includes key features such as User and Group Management, Self-Service Profile Management and Password Reset, SSO. However, Oracle Retail customers may wish to consider licensing the Standard Tier of IDCS to also have access to more advanced identity features including Identity Synchronization with Microsoft Active Directory, SSO for Third Party Cloud Services and Custom Applications, Multi-Factor Authentication and generic SCIM Templates.

IDCS and Oracle Retail Enterprise Roles

When any Oracle Retail cloud service is provisioned, Oracle Retail's Enterprise Roles are seeded into the customer's IDCS instance as Roles. It is expected that customers will also have other roles defined for other cloud services that use this IDCS instance.

IDCS and Application Users

Upon provisioning a new cloud service instance, Oracle Retail creates a single delegate customer administrator user.

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

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

Authorization

While IDCS has some authorization features, as an ADF application, Merchandising Cloud Services manages this type of access functional security 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. Enterprise Roles are mapped to Merchandising Cloud Services Duties and Privileges. Default mappings of Enterprise to Merchandising Cloud Services Duties and Privileges are provided as part of Merchandise Cloud Service provisioning.

Roles

The default configuration includes the eleven predefined Enterprise security roles listed below:

- Application Administrator
- Data Steward
- Buyer
- Inventory Analyst
- Inventory Manager

- Corporate Inventory Control Analyst
- Inventory Control Manager
- Sourcing Analyst
- Finance Analyst
- Supply Chain Analyst
- Finance Manager

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

One important thing to note is that there is also a mirrored set of these Enterprise roles with the suffix _PREPROD (Data Steward_PREPROD, Buyer_PREPROD, Inventory Analyst_PREPROD, etc) available in IDCS. This set of _PREPROD roles should be used so that users can have different access in non-production vs production systems. For example, it is common for QA employees to have virtually all Enterprise roles, and therefore unlimited access, to non-production systems. However these same QA employees might have limited or no access to production systems.

Duties and Privileges

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

In Merchandising Cloud Services, 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 will be 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.

Table 5–1 Duties and Privileges

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

Table 5–1 (Cont.) Duties and Privileges

Duty	Privileges
Purchase Order Approval	■ All Privileges in Purchase Order Management ■ Approve Purchase Orders

Additionally, two privileges exist that work a bit differently and are intended to help configure the application by retail vertical.

- Use Diffs Priv. This is meant to be assigned to roles that use differentiators for their items. For most fashion or department store retailers, this would likely be associated to all roles. But, for other businesses that may have a mix of fashion items and hardline items, this may only be associated to certain roles in the organization. Users which have this privilege assigned to them will have access to the Diff Matrix, Diff Distribution, Re-distribution by Diff, and the Order, Transfer and Contract Parent/Diff Summary contextual reports. This privilege also provides access to the differentiator container in the Item screen. Users without this privilege will have these hidden from their view.
- Maintain/View Grocery Attributes Priv. Similar to the Use Diffs Priv, it is intended show or hide grocery related attributes for items, such as the catch weight indicator.

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

Data Security/Filtering

Oracle Retail Cloud Service 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.

Data level security is configured by assigning users to a data security group within Merchandising Cloud Services. 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 Cloud Services. These groups are associated with levels of the merchandise and organizational hierarchies. Every application user must also be defined in Merchandising Cloud Services 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 *Merchandising Cloud Services Administration Guide*.

Note: Adding these users to Merchandising Cloud Services for data security/filtering purposes is a manual process (via spreadsheet upload). Users are not automatically loaded from IDCS 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 Cloud Services with IDCS. As authentication is based on user definition in IDCS (which includes Enterprise Role), it is possible that a user could authenticate correctly and reach Merchandise Cloud Service 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 Cloud Services or not associated with a Data Security Group, the user may not see certain types of data in the application.

6

Additional Secure Set Up for Merchandising Cloud Services

This section describes additional security set up that must be performed by retailers and Oracle Retail.

SFTP Inbound/Outbound

As part of the environment provisioning process, Oracle creates an SFTP user account. Details about this account will be sent to the Cloud Service Administrator. After the administrator verifies manual SFTP login, the customer administrator will be asked to generate a 2048 bit RSA public/private SSH key pair. The customer administrator will submit an Oracle Support request, with the public half of the key pair attached. Oracle Retail will configure the public key as an "authorized" key for the customer's account and lock the account's password. Oracle Retail will enforce a key-life policy of one (1) year by expiring the account 365 days after the SSH key is installed. The customer will use the private key for ongoing access to the SFTP server. Multiple public key files per account are supported by Oracle.

More information about SFTP key management is documented in Oracle Cloud Security Practices for Software as a Service (SaaS) Cloud Services.

http://www.oracle.com/us/corporate/contracts/gbu-cloud-services-pillar-3089817.pdf

7

Frequently Asked Questions

This section includes a number of specific questions related to security that are frequently asked by prospects, customers and implementers.

Table 7–1 FAQs

Question	Answer
Does Merchandising Cloud Services support data encryption?	Yes. Sensitive Personal Data is stored in encrypted tablespace. All data is encrypted in transit, Merchandising Cloud Services uses TLS for secure transport of data.
Does Merchandising Cloud Services provide network segregation?	Yes. The Oracle Cloud network is isolated from the Oracle corporate network. Customer instances are separated down to the VLAN level.
Does Merchandising Cloud Services provide secure backups?	Yes. Backup is a standard process for the Merchandising Cloud Services. Database and application servers backed up both incrementally (daily) and fully (weekly). Backups are stored for at least 60 days.
Does Merchandising Cloud Services provide centralized logging?	Yes. All application and infrastructure logs are forwarded to a centralized Security Information and Event Management system.
Does Merchandising Cloud Services provide antivirus?	Yes. All files uploaded into Merchandising Cloud Services are scanned by anti virus and anti malware software. All hosts in the cloud service are regularly patched with the latest critical patch updates.
Does Merchandising Cloud Services provide strong authentication options such as 2-factor, one-time Password?	Multi-Factor Authentication is an option if a customer chooses to license the Standard Tier of IDCS.
Does Merchandising Cloud Services 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 Merchandising Cloud Services implement access lists to secure each tier of the solution?	Yes. Communication between tiers within Merchandising Cloud Services is limited by subnet ingress security lists.
Does Merchandising Cloud Services include and support the capability to change default account passwords?	All user password management occurs in IDCS.

Table 7–1 (Cont.) FAQs

Question	Answer
Does Merchandising Cloud Services support Roles with defined access levels?	Yes. Oracle Retail Enterprise roles span Oracle Retail applications. Within Merchandising Cloud Services, privileges and duties can be assigned to roles to define what is accessible to certain types of users.
Does Merchandising Cloud Services support synchronizing with an external time source?	All hosts within the solution are synchronized to the same time source.
Does Merchandising Cloud Services provide strong password options such as complexity, history, aging, account lockout.	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

A

Appendix: Default Functional Security Implementation

https://docs.oracle.com/cd/E12448_01/rms/pdf/160/rms-160-og3.pdf

Default Security Reference Implementation (but not the sentence 'The source of truth for default reference implementation is jazn-data.xml').

Refer to the tables on pages 29 - 76 of the PDF listed above.