Oracle® Retail Integration Cloud Service

Integration Security Guide

Release 21.0.000

F39228-01

May 2021

Oracle® Retail Integration Cloud Service Integration Security Guide, Release 21.0.000

F39228-01

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
Customer Support ix
Improved Process for Oracle Retail Documentation Corrections x
Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com) x
Conventions x

1 Introduction

2 Responsibilities

Retailer Responsibilities 2-1
Oracle Responsibilities 2-1

3 Oracle Retail SaaS Security

Secure Product Engineering 3-1
Secure Deployment 3-1
Physical Safeguards 3-2
Network Security 3-2
Infrastructure Security 3-2
Data Security 3-2

4 Secure Management

Assessment and Audit 4-1

5 Integration Cloud Services Architecture

Architecture 5-1

6 Integration Cloud Service Authentication and Authorization

Authentication and IDCS 6-1
DCS 6-1

IDCS and Oracle Retail Enterprise Roles 6-2
IDCS and Application Users 6-2
Authorization 6-2
Roles 6-2
Duties and Privileges 6-3

7 Frequently Asked Questions

G Appendix: Default Functional Security Implementation

Send Us Your Comments

Oracle® Retail Integration Cloud Service Integration Security Guide, Release 21.0.000

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 Integration Cloud Service 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

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

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 Integration Cloud Services.

The Oracle Retail Integration Cloud Service is a suite of software-as-a service solutions that provides retailers with various integration solutions. This includes Retail Integration Bus (RIB), Retail Service Bus (RSB), Bulk Data Integration (BDI), Retail Financial Integration (RFI) and Universal Service Mapper (USM).

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.
- Integration Cloud Service Architecture - This section details the architecture of the Integration Cloud Service, particularly as it relates to security.
- Integration Cloud Service Authentication, and Authorization - This section describes how Integration Cloud Service performs authentication and authorization can be applied.
- 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 Integration 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 Integration 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 Integration 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 Integration 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

Integration 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/anal ysis-testing.html

Specific security details of the Integration 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/ethi cal-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

4 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

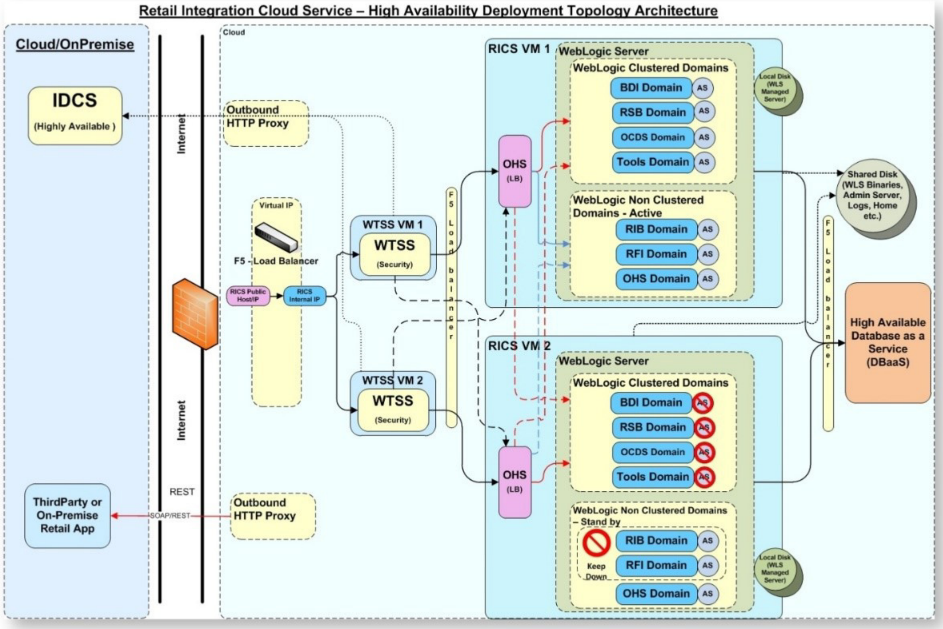
5

Integration Cloud Services Architecture

Integration Cloud Service 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 19.1.000, Integration 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 Integration Cloud Services deployment currently on versions 16.0.029 and lower currently use an instance of Oracle Identity Management (IDM) Suite within Integration 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 not move any user and group information currently in the live SaaS customer's IDM suite to the customer's IDCS tenancy.

Architecture



Most customer access to the Integration Cloud Service is via the web tier. The web tier contains the perimeter network services that protect the Integration 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 Integration applications, which allows integration between Oracle retail applications and external applications. Retail Integration Console (RICS) is a UI component that serves as dashboard for the integration. Retail Home 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 Integration schema on the Integration PDB. Transparent data encryption (TDE) is set during provisioning. Tablespaces that contain personal data are encrypted.

Integration Cloud Services applications integrate with external business systems via:

- Native ReST Services
- SOAP Services

Integration 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.

Integration Cloud Service 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 Integration Cloud Service is limited by subnet ingress security lists.

To reduce attack surface, access to the Integration Cloud Service from the open internet is very limited. Business Users (via web browser) and external web service endpoints access application over https/443 . Firewall and load balancer in the DMZ pass traffic to the WTSS server in the Authentication Tier, which in turn to requests authentication (via outbound proxy) from the customer's Identity Cloud Service (IDCS) tenancy.

Within the Integration Cloud Service itself, traffic between tiers is very limited. Authenticated requests are passed from the AuthN Tier to the M-Tier. Access to the underlying DBaaS is only available via the M-Tier.

Outbound web service traffic is 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

6

Integration Cloud Service Authentication and Authorization

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?).

Authentication and IDCS

As of version 19.1.000, Integration Cloud Service 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 Integration Cloud Service UI, Integration Cloud Services redirects application URL requests to the IDCS login screen. IDCS authenticates the user. When a user logs out of the Integration Cloud Service, Integration invokes an IDCS logout to disable session authentication.

DCS

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.

Integration 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 Integration 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, Integration 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 Integration Cloud Services Duties and Privileges. Default mappings of Enterprise to Integration Cloud Services Duties and Privileges are provided as part of Integration Cloud Service provisioning.

Roles

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

- Application Administrator
- Application Operator
- Application Monitor

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 (Administrator_PREPROD, Operator_PREPROD, Monitor_

PREPROD, and so on) 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 Integration Cloud Service, Enterprise Roles are mapped to Duties and Privileges. Privileges are essentially actions that a user can perform. Duties are collections of related privileges.

In Integration 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.

Table 6–1 Duties and Privileges

Duty	Privileges
Administrator	Access to all operations.
Operator	Access to all operations except create/update/delete operations. Access to start a Process Flow/Job.
Monitor	Only able to view information.

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

7 Frequently Asked Questions

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

Question	Answer
Does Integration Cloud Service support data encryption?	Yes. Sensitive Personal Data is stored in encrypted tablespace. All data is encrypted in transit, Integration Cloud Service uses TLS for secure transport of data.
Does Integration Cloud Service 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 Integration Cloud Service provide secure backups?	Yes. Backup is a standard process for the Integration Cloud Service. Database and application servers backed up both incrementally (daily) and fully (weekly). Backups are stored for at least 60 days.
Does Integration Cloud Service provide centralized logging?	Yes. All application and infrastructure logs are forwarded to a centralized Security Information and Event Management system.
Does Integration Cloud Service provide antivirus?	Yes. All files uploaded into Integration Cloud Service 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 Integration Cloud Service 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 Integration Cloud Service 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 Integration Cloud Service implement access lists to secure each tier of the solution?	Yes. Communication between tiers within Integration Cloud Service is limited by subnet ingress security lists.
Does Integration Cloud Service include and support the capability to change default account passwords?	All user password management occurs in IDCS.
Does Integration Cloud Service support Roles with defined access levels?	Yes. Oracle Retail Enterprise roles span Oracle Retail applications. Within Integration Cloud Service, privileges and duties can be assigned to roles to define what is accessible to certain types of users.

Question	Answer
Does Integration Cloud Service support synchronizing with an external time source?	All hosts within the solution are synchronized to the same time source.
Does Integration Cloud Service 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.