Oracle® Retail Process Orchestration and Monitoring

Security Guide

Release 24.1.101.0
F90327-01
January 2024

ORACLE

Oracle Retail Process Orchestration and Monitoring Security Guide, Release 24.1.101.0

F90327-01

Contents

Send Us Your Comments

Oracle Retail Process Orchestration and Monitoring Security Guide,

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

The *Oracle Retail Process Orchestration and Monitoring Guide* describes security methods and procedures for Process Orchestration and Monitoring.

Audience

This guide is for system administrators and operations personnel, integrators and implementation staff personnel as well as users of the module.

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 clouds services, including Oracle Retail Process Orchestration and Monitoring Cloud Service.

The Oracle Retail Process Orchestration and Monitoring Cloud Service is a product that helps to run the batches for other retail products offered as cloud service like Merchandising, Retail Insights, and so on.

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.
- Process Orchestration and Monitoring Cloud Service Architecture - This section details the architecture of the Process Orchestration and Monitoring Cloud Service, particularly as it relates to security.
- Process Orchestration and Monitoring Cloud Service Authentication, Authorization and Data Filtering - This section describes how Process Orchestration and Monitoring Cloud Service performs authentication and authorization, as well as how data filtering can be applied.
- Additional Secure Set Up for Process Orchestration and Monitoring Cloud Service Suite - 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 Process Orchestration and Monitoring 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 Process Orchestration and Monitoring 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 Process Orchestration and Monitoring Cloud Service security

2
Responsibilities

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

Retailer Responsibilities

At a high level, retailers are responsible for:

- Understanding Oracle's security policies
- Implementing their own corporate policies through Oracle tools
- Creating and administering users through 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 Process Orchestration and Monitoring 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

Process Orchestration and Monitoring 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.

https://docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm

3

Oracle Retail SaaS Security

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

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

Secure Product Engineering

Oracle builds secure software through a rigorous set of formal, always evolving security standards and practices known as Oracle Software Security Assurance (OSSA). OSSA encompasses every phase of the product development lifecycle.

More information about OSSA can be found at:

https://www.oracle.com/corporate/security-practices/assurance/

The cornerstones of OSSA are Secure Coding Standards and Security Analysis and Testing.

Secure Coding Standards include both general use cases and language specific security practices. More information about these practices can be found at:

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

Security Analysis and Testing includes product specific functional security testing and both static and dynamic analysis of the code base. Static Analysis is performed through tools including both internal Oracle tools and Micro Focus Fortify. Dynamic Analysis focuses on APIs and endpoints, using tools like OWASP ZAP to test interfaces and protocols.

https://www.oracle.com/corporate/security-practices/assurance/development/analysis-testing.html

Specific security details of the Process Orchestration and Monitoring 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 in 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

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.

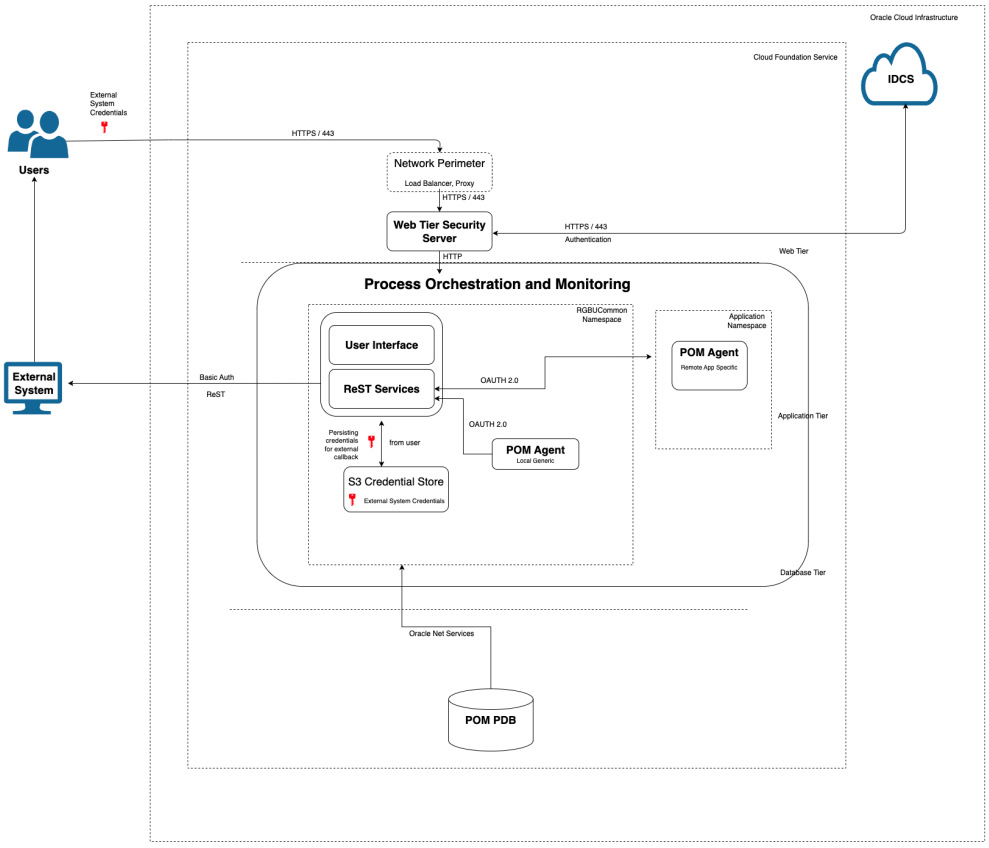
4

Process Orchestration and Monitoring Cloud Service Architecture

Process Orchestration and Monitoring (POM) Cloud Service is a Java based application deployed on Oracle's Cloud Infrastructure. It is used by other retail cloud services to set up, administer, execute and monitor their batch schedules. The applications are deployed in a highly available, high performance, horizontally scalable architecture. POM Cloud Services uses either Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identity provider (IDP). Information about logical, physical and data architecture in this document focuses on how the architecture supports security.

Overall Architecture

This section does not explain the complete architecture of the Process Orchestration and Monitoring Cloud Service, but instead focuses on the high-level aspects that relate to security.



Most customer access to the Process Orchestration and Monitoring (POM) Cloud Service is through the web tier. The web tier contains the perimeter network services that protect the Process Orchestration and Monitoring application and associated 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) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) tenancy to perform authentication. More information about authentication through IDCS or OCI IAM is provided later in this document.

The underlying container DBaaS includes one pluggable database (PDB). Applications are able to access the POM schema on the POM PDB using Oracle Net Services aka SQL*Net. Transparent data encryption (TDE) is set during provisioning.

POM Cloud Service authenticates all internal native rest service calls using OAUTH2.0 through IDCS or OCI IAM. 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.

Rest service calls from external systems (customers) to POM must use OAUTH2.0 (Client Credentials Grant). Refer to the POM Implementation Guide for more information about Invoking POM service using OAUTH2.0.

> **Note:**
>
> ReST service calls from POM to external systems (customers), such as the call for External Status Update, are limited to Basic Auth at this time.

To reduce attack surface, access to the POM Cloud Service from the open internet is very limited. As described in the Architecture section of this document, Business Users (on a web browser) and also any other external web service endpoints access application over https/443.Network Perimeter blocks requests from certain blacklisted IPs as configured. Firewall and load balancer pass traffic to the WTSS server which in turn to requests authentication (through outbound proxy) from the customer's Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) tenancy.

Actual batch job processing is managed by a component called POM Agent which is provided by the POM team to the corresponding Application teams. This component is packaged as part of the Application and communicates with POM through ReST endpoints.

The POM deployment model also provides for the provisioning of a common agent within the same namespace as the POM application in the rgbu-common CoD. This enables various applications to run their ReST-based batches on this agent without the need for deploying their own Agent. This simplifies the applications footprint and their POM adoption. As the POM Agent is capable of running ReST Jobs from multiple Schedules, the common agent makes it possible for multiple applications to use this single common agent for executing batch. Customers can create their own custom schedules and configure those to use this common agent to execute their batch. See the “Custom Schedules” chapter in the *Process Orchestration and Monitoring Implementation Guide* for more information.

Process Orchestration and Monitoring Cloud Service provides an External Status Update feature (aka callback) which sends a batch job's status to the customer's

system. Additionally, POM provides a facility for the customer to create or modify the corresponding URL and credentials which POM then stores in the S3 store.

Similarly, With the introduction of Custom Job Types, POM provides an option to store the related URL(s) required to run the ReST Based Job along with the OAUTH credentials (stored in the S3 store) to access those URLs.

Readers should refer to the following links for additional information about Oracle Cloud delivery and IDCS or OCI IAM.

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

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/manage-oracle-identity-cloud-service-network-permieters.html

5

Process Orchestration and Monitoring Cloud Service Authentication & 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 run a batch job?).

Authentication and IDCS or OCI IAM

As of version 19.0.001, Process Orchestration and Monitoring (POM) Cloud Service Suite uses Oracle Identity Cloud Service (IDCS) or Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identity provider (IDP).

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

When a user connects to the POM User Interface, the request is redirected to the IDCS or OCI IAM login screen. IDCS or OCI IAM authenticates the user. When a user logs out of POM, the IDCS or OCI IAM logout is invoked to disable session authentication.

IDCS and OCI IAM

IDCS and OCI IAM are Oracle's cloud native security and identity platforms. They provide a powerful set of hybrid identity features to maintain a single identity for each user across cloud, mobile, and on-premises applications. IDCS and OCI IAM enable single sign on (SSO) across all applications in a customer's Oracle Cloud tenancy. Customers can also integrate IDCS or OCI IAM with other on-premise applications to extend the scope of this SSO.

IDCS and OCI IAM are 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 or OCI IAM Standard Tier licensing model are available in Administering Oracle Identity Cloud Service. Process Orchestration and Monitoring Cloud Service Suite 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 or OCI IAM 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 or OCI IAM 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 or OCI IAM instance as Roles. It is expected that customers will also have other roles defined for other cloud services that use this IDCS or OCI IAM instance.

IDCS or OCI IAM 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 through IDCS or OCI IAM. A key feature of IDCS or OCI IAM is that basic user maintenance can be further delegated through identity self-service.

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

> **Note:**
>
> IDCS or OCI IAM username is passed to Process Orchestration and Monitoring (POM) as the application user ID. It will be persisted on the database as part of the basic POM transaction audit trail. If the corporate email address is used as the IDCS or OCI IAM username, that email address is persisted to the POM database. To fully inform POM users that their corporate email address will be saved, we recommend that retailer implements IDCS or OCI IAM Terms of Use functionality. The IDCS or OCI IAM Terms of Use feature enables retailers to set the terms and conditions for users to access an application, based on the user's consent. This feature allows the identity domain administrator to set relevant disclaimers for legal or compliance requirements and enforce the terms by refusing the service. The Terms of Use feature can be used to explicitly obtain user consent to persist corporate email address for POM auditing. See Administering Oracle Identity Cloud Service for more information about Terms of Use.
>
> https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/understand-terms-use.html

JET Security

As mentioned earlier, The Process Orchestration and Monitoring (POM) application features a classic ADF User Interface (UI) that is being deprecated as of POM 19.1.002. It is replaced with a JET based UI.

Oracle POM security requirements come from the need to protect application data from unauthorized changes. This is accomplished by the following security features:

- **Authentication** - POM JET UI restrict access to users that have been authenticated by the configured security provider.
- **Authorization** - POM JET UI uses enterprise roles to limit what features individual users can access.
- **Origin Control** - POM JET UI implements the Cross-Origin Resource Sharing (CORS) protocol to allow only same origin.
- **Transport Security** - POM JET UI and services communicate through REST calls. These communications need to be secured.
  - 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 service URLs are at a location exposed on WTSS, otherwise each endpoint will be independently authenticated.

The JET UI and services communicate through ReST calls which are secured using JAX-RS security implementation.

For more information regarding securing Restful Web Services, refer to https://docs.oracle.com/cd/E24329_01/web.1211/e24983/secure.htm#RESTF113

User Roles

Roles are used to classify users based on job responsibilities and actions to be performed in the Oracle Retail Process Orchestration and Monitoring application (POM). Using roles, a user's access can be restricted to specific areas or functions within the application. In POM, users must be associated with at least one job role in order to access the application.

The following topics are covered in this chapter:

- Roles
- Functional Access by Role

Roles

POM comes available with a set of pre-defined roles described in the table below. In addition to the roles, the table contains an alias for each role which is used in the next section for easier reading.

These roles have been given similar access in the new user interface as the access they had in the classic user interface.

Table 5-1 Roles

Role	Alias	Description
BATCH_ADMINISTRATOR_JOB	Administrator	Users within this role are retailer administrators with full access to all POM actions. They monitor, maintain and configure the batch schedules. They may also maintain POM application configurations for efficient operations. They troubleshoot batch issues and work with Oracle support personnel to address those issues. Finally, they may apply batch schedule patches and upgrades. Additionally, users assigned this role are given access to the Oracle AMS Utilities screen.
BATCH_VIEWER_JOB	Viewer	Users within this role are retailer business users responsible for just monitoring batch. They have view access to all POM screens except AMS Utilities.
BATCH_SCHEDULE_CONFIGURATION_MANAGER_JOB	Schedule Config Mgr	Users within this role are typically retailer administrators responsible for just monitoring batch and configuring external dependencies and callbacks into the Company's systems. They have view access to all POM screens except AMS Utilities.
BATCH_SCHEDULE_ADMINISTRATOR_JOB	Schedule Admin	Users within this role are typically retailer administrators responsible for maintaining monitoring and executing batch. They have view access to all POM screens except AMS Utilities. They can perform select activities on the Batch Monitor screen to move the schedule along. They also have update access to the Batch Administration screen. They can also configure some application properties and can configure a new schedule
BATCH_ORACLE_AMS_ADMINISTRATOR_JOB	AMS Admin	Users within this role are typically Oracle AMS administrators who monitor, maintain and configure the batch schedules. They also maintain POM application configurations for efficient operations. They troubleshoot batch issues and work with other Oracle development and support personnel to address those issues. Finally they apply POM and batch schedule patches and upgrades.

Functional Access by Role

This section lists all roles that have update access for each functional aspect of every screen. It is organized by screen, except for the first two tables.

Table 5-2 External Integration

Feature	Roles (aliases) with access
Invoking batch execution from an external system Requesting the status of a batch execution Releasing dependency on an external process	Schedule Admin Administrator AMS Admin

Table 5-3 POM Task Menu

Feature	Roles (aliases) with access
Show Batch Monitoring task	Administrator Viewer Schedule Config Mgr Schedule Admin AMS Admin
Show System Configuration task	Administrator Viewer Schedule Config Mgr Schedule Admin AMS Admin
Show Batch Administration task	Administrator Viewer Schedule Config Mgr Schedule Admin AMS Admin
Show Scheduler Administration task	Administrator Schedule Admin AMS Admin
Show Schedule Maintenance task	Administrator Viewer Schedule Config Mgr Schedule Admin AMS Admin
Show AMS Utilities task	AMS Admin

Table 5-4 Screen: Batch Monitoring

Feature	Roles (aliases) with update access
Buttons for Create Schedule, Close Schedule and Restart Schedule	Schedule Admin Administrator AMS Admin
Jobs table on Batch Monitoring screen - Buttons for Run, Rerun, Hold, Release, Skip, Release Skip, and action for Add Comments	Schedule Admin Administrator AMS Admin
Jobs table Actions menu on Batch Monitoring screen - Edit Parameters (for selected job)	Schedule Admin Administrator AMS Admin
Job Details screen - Enable/Disable External Dependencies	Administrator Schedule Config Mgr Schedule Admin AMS Admin
Job Details screen - Retry Schedule Link button	Administrator AMS Admin
Job Details screen - Retry Callback button	Administrator AMS Admin
Execution Engine display Configuration	Administrator AMS Admin
Download Job Log	All authenticated users
Download Cycle Summary	All authenticated users
Scheduler Tasks Monitoring and actions	Administrator Schedule Admin AMS Admin

Table 5-5 Screen: System Configuration

Feature	Roles (aliases) with update access
System tab - Update actions	Administrator AMS Admin
Schedule tab - Update actions for general & environment settings	Administrator AMS Admin
Schedule tab - Job admin system options dialog	Administrator AMS Admin
Schedule tab - Update actions for MDF configuration	Administrator AMS Admin
Schedule tab - Update actions for job admin throttling configuration	Administrator AMS Admin

Table 5-5 (Cont.) Screen: System Configuration

Feature	Roles (aliases) with update access
System tab - Update actions for external configurations	Business User Administrator Schedule Config Mgr Schedule Admin AMS Admin
Global Edit - Settings updates	Administrator AMS Admin
Global Edit - External Configuration updates	Administrator Schedule Config Mgr Schedule Admin AMS Admin
Configure New Schedule	Administrator Schedule Admin AMS Admin

Table 5-6 Screen: Batch Administration

Feature	Roles (aliases) with update access
Export Config and Import Config buttons	Administrator Schedule Admin AMS Admin
Enable/disable switch on each of the Recurring Flows and Jobs within each Flow	Administrator Schedule Admin AMS Admin
Jobs table on main UI - Edit and Enable/Disable actions	Administrator Schedule Admin AMS Admin
Batch Job Details - Enable/Disable Dependencies	Administrator AMS Admin
Batch Job Details - Create/Enable/Disable/Delete Inter-Schedule Dependencies	Administrator AMS Admin
Batch Job Details - Create/Enable/Disable/Delete Schedule links	Administrator AMS Admin
Batch Job Details - Create/Enable/Disable/Delete External Dependencies	Administrator Schedule Config Mgr Schedule Admin AMS Admin

Table 5-7 Screen: Scheduler Administration

Feature	Roles (aliases) with update access
All Functions on the Scheduler Administration screen	Administrator Schedule Admin AMS Admin

Table 5-8 Screen: Schedule Maintenance

Feature	Roles (aliases) with update access
All actions: Import Latest Schedule button, Upgrade, Retry buttons in table row Download Configuration and download POM seed data	Administrator AMS Admin

Table 5-9 Screen: AMS Utilities

Feature	Roles (aliases) with update access
Manual Job Run Override Job Status Override Execution Request Status	Administrator AMS Admin

Table 5-10 Screen: Application Properties

Feature	Roles (aliases) with update access
Application Properties	Schedule Admin Administrator AMS Admin

Private Data REST Services

This section contains details about the REST Services flavor of the Private Data Services and Tools documented by framework team.

Retailers must call the Private Data REST Service endpoints with the following request headers:

Table 5-11 Request Header

Name	Value	Required	Description
Accept	application/json OR application/xml	Yes	Tells the server the MIME-type of the re-source.
Authorization	OAuth 2.0 using Client Credentials	Yes	Authenticates a user agent with the server

List of Endpoints

The table below shows the details of calling the Private Data Service APIs through REST endpoints:

Action	Endpoint Path	Description

Get a List of Query Group Types	/privatedata/config/{action}	Returns the valid ID types that can be used in private data calls.
		Method
		• _GET
		Accept
		• _application/json
		Path Parameters
		• _action: The private data action for which query group types are being inquired. Valid values include:
		access: access PII data
		forget: remove PII data
		validateForget: check to see if PII data can be removed.
		Response Codes
		• _200 - Success
		• _500 - Internal Server Errors - for all other types of errors (for example, config errors, SQL errors, and so on).
		Success Payloads
		`{`
		`"types": [`
		`"raf",`
		`"supplier",`
		`"customer"`
		`]`
		`}`

Action	Endpoint Path	Description
Get Query Group Type Information (for example, Lookup customer ID)	/privatedata/config/{action}/{id_type}	Returns details of the query group type including the customer ID format required to access or remove PII data. **Method** • _GET **Accept** • _application/json **Path Parameters** • _action: The data privacy action being attempted on the query group type. Valid values include: access: access PII data forget: remove PII data validateForget: check to see if PII data can be removed. • _id_type: The query group type. **Response Codes** • _200 - Success • _400 - Bad Request - Produced for the following situations: Invalid input type • _500 - Internal Server Errors - for all other types of errors (for example, config errors, SQL errors, and so on). **Success Payloads** `{ "customerIdFormat": "{%customer-Id%}::{%divisionId%}::{%groupId%}", "type": "customer" }`

Action	Endpoint Path	Description
Access PII	/privatedata/{id_type}	Retrieves PII in the system **Method** • _GET **Accept** • _application/json • _application/xml **Path Parameters** • _id_type: The query group type for which PII is to be retrieved. **Query Parameters** • _customer_id: (required) The customer ID string to be used in looking up PII. The format of this string must conform to the format indicated for the query group type. • _jsonFormat : The type of JSON format to return. Valid values: "concise" (default) , "full". Applicable only if Accept=application/json. **Response Codes and Error Messages** • _200 - Success • _400 - Bad Request - Produced for the following situations: o Customer ID does not match the required format Invalid input type Missing customer ID Invalid jsonFormat • _500 - Internal Server Errors - for all other types of errors (for example, config errors, SQL errors, and so on). **Success Payloads** • _When Accept=application/json, this API will return PII in JSON format. • _When Accept=application/xml, this API will return PII formatted as an HTML page. • _Refer to section Output Format for Accessing PII for more details.

Action	Endpoint Path	Description
Remove PII	/privatedata/{id_type}	Removes PII from the system. **Method** • _DELETE **Accept** • _application/json **Path Parameters** • _id_type: The query group type for which PII is to be removed. **Query Parameters** • _customer_id: (required) The customer ID string to be used in looking up PII. The format of this string must conform to the format required for the query group type. **Response Codes** • _200 - Success - Delete successful • _412 - Precondition Failed - Una-ble to delete. • _400 - Bad Request - Produced for the following situations: o Customer ID does not match the required format Invalid input type Missing customer ID • _500 - Internal Server Errors - for all other types of errors (for example, config errors, SQL errors, and so on).

Action	Endpoint Path	Description
Validate If PII Can Be Removed	/privatedata/{id_type}/ validate-Forget	Validates whether a customer can be removed from the system. **Method** • _GET **Accept** • _application/json **Path Parameters** • _id_type: The query group type for which PII is to be removed. **Query Parameters** • _customer_id: (required) The customer ID string to be used in looking up PII. The format of this string must conform to the format required for the query group type. **Response Codes** • _200 - Success - Person can be deleted • _412 - Precondition Failed - Per-son cannot be deleted • _400 - Bad Request - Produced for the following situations: o Customer ID does not match the required format Invalid input type Missing customer ID • _500 - Internal Server Errors - for all other types of errors (for example, config errors, sql errors, amd so on).

Output Format for Accessing PII

The following output formats are supported by the REST endpoint for accessing PII:

Format	Description
Concise JSON (default)	Human readable JSON format. Concise but cannot be parsed into a generic stucture at runtime.
Full JSON	Full JSON format that can be parsed electronically. Ideal for importing data into the system (a future functionality)
Human Readable HTML	Human readable HTML format.