Oracle® Retail Process Orchestration and Monitoring

Security Guide

Release 19.0

F25985-01

January 2020

ORACLE

Oracle Retail Processing Orchestration and Monitoring Security Guide, Release 19.0

F25985-01

Primary Author:

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 Process Orchestration and Monitoring Guide, Release Release 19.0

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 the tracking and managing of batch jobs.

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 4.0) or a later patch release (for example, 4.0.1). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all

releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix 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 them 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 - 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

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 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 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

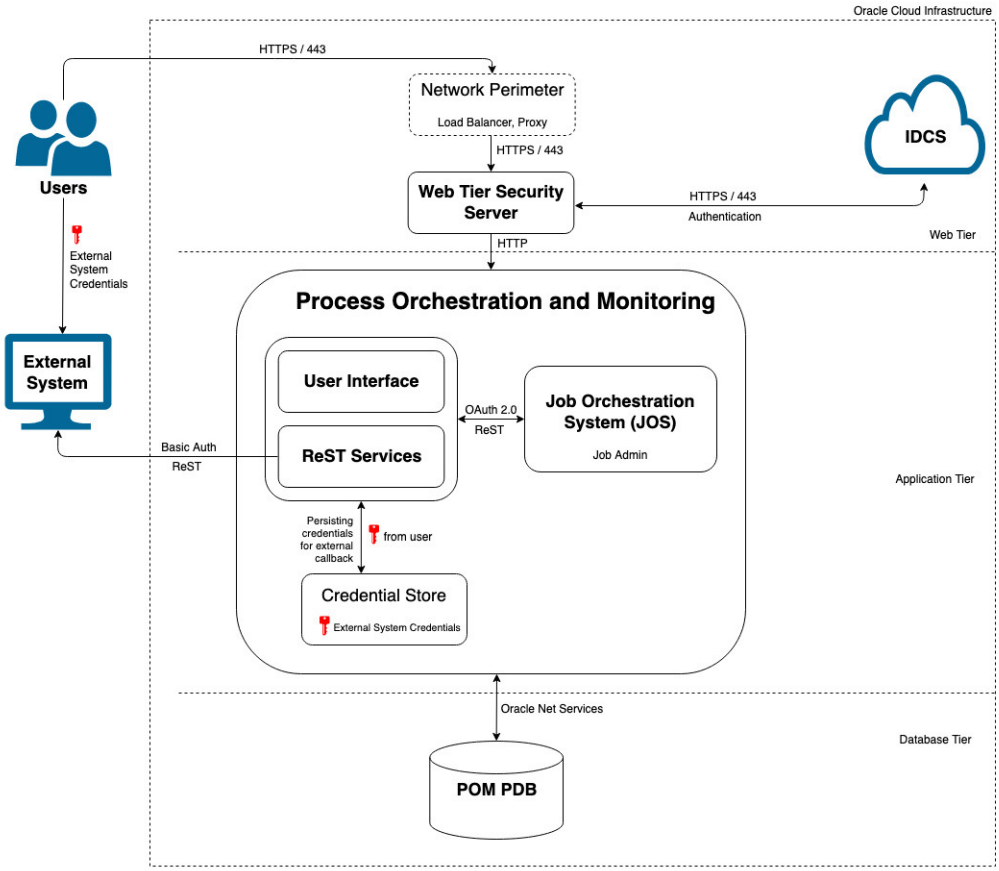
Process Orchestration and Monitoring Cloud Service Architecture

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.

Note: Oracle Retail Process Orchestration and Monitoring Cloud Service deployments currently on versions 19.0 and lower currently use an instance of Oracle Identity Management (IDM) Suite within Process Orchestration and Monitoring Cloud Services as an IDP. As these live customers are upgraded to 19.0.001 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.

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 Cloud Service is through the web tier. The web tier contains the perimeter network services that protect the Process Orchestration and Monitoring 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 through IDCS is provided later in this document.

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

Process Orchestration and Monitoring Cloud Service 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.

To reduce attack surface, access to the Process Orchestration and Monitoring 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) tenancy.

Process Orchestration and Monitoring Cloud Service relies on the JOS (Jos Orchestration System) from the RTG (Retail Trade Group) team to run the batches and

this component is installed as part of the POM installation itself. All the communication between core POM components and JOS happens through ReST using OAUTH 2.0 if the IDCS URL has been configured which is true for the most cases else it would be Basic Auth.

Process Orchestration and Monitoring Cloud Service provide the user a feature called external callback to notify batch status to an external system configured by the user. Also, it provides a way to create or modify credentials for accessing those external systems through its UI so that the user can modify passwords according the password policies they follow. We are using Basic Authentication ReST calls for sending update the external system using the credentials from the user which is stored in the WebLogic credentials store.

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

As of version 19.0.001, Process Orchestration and Monitoring Cloud Service Suite 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 Process Orchestration and Monitoring Cloud Service UI, Process Orchestration and Monitoring Cloud Service Suite redirects application URL requests to the IDCS login screen. IDCS authenticates the user. When a user logs out of the Process Orchestration and Monitoring Cloud Service, Process Orchestration and Monitoring 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.

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

When application users are created in IDCS, 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 username will be passed to Process Orchestration and Monitoring as the application user ID. It will be persisted on the database as part of the basic Process Orchestration and Monitoring transaction audit trail. If corporate email address is used as the IDCS username, corporate email address will be persisted to the Process Orchestration and Monitoring database. To fully inform Process Orchestration and Monitoring users that their corporate email address will be saved, we recommend that retailers implement IDCS Terms of Use functionality. The IDCS 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 Process Orchestration and Monitoring 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

---

Authorization

While IDCS has some authorization features, as an ADF application, Process Orchestration and Monitoring Cloud Service 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 Duties and Privileges. Default mappings of Enterprise to Duties and Privileges are provided as part of Process Orchestration and Monitoring Cloud Service provisioning.

ADF Security

Process Orchestration and Monitoring (POM) is basically an ADF applications so all the native ADF security features are used.

ADF Security provides the following core benefits:

- Declarative, permission-based protection for ADF security-aware resources, such as ADF bounded task flows, top-level web pages that use ADF bindings, and attributes defined by ADF entity objects and their attributes.
- Dynamic user authentication. When you use ADF Security, the application will dynamically prompt the user to log in if the user is not yet authenticated and tries to access a page that is not granted to the anonymous-role role. In the application's web.xml file, a security constraint is applied to the ADF authentication servlet so that login is triggered through the Java EE web container before any secured resources can be accessed. After the user successfully logs in, the ADF authentication servlet runs to verify whether the authenticated user has view access to the requested page.
- Permission checking within the web page. At runtime, the security policy you define for ADF resources is enforced using standard JAAS permission authorization to determine the user's access rights. If your application requires it, you can use Expression Language (EL) to perform runtime permission checks within the web page to hide components that should not be visible to the user.
- Simplifies securing of applications by providing an abstraction layer between the application and various security providers. Calls from the application to the security layer can be made through standards-based APIs, so developers do not have to deal with implementation details of the security providers.

Refer Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server - https://docs.oracle.com/middleware/1212/wls/SCOVR/toc.htm

Roles

Roles	Duty	List of Privileges
Batch Administrator Job	System Administrator Duty	View Historical Batch Logs Priv Maintain Batch Monitoring Privilege Maintain Batch Administration Privilege View Application Logs Priv
Batch Business Job	Business User Duty	View Batch Monitoring Privilege External Configuration Priv
Batch Monitoring Job	Batch Monitoring User Duty	View Historical Batch Logs Priv Maintain Batch Monitoring Privilege View Application Logs Priv

Duties and Privileges

Table 5–1 Duties

Duty	Description	List of Privileges
Business User Duty	A duty for monitoring batch as a business user.	View Batch Monitoring Privilege External Configuration Priv
System Administration Duty	A duty for maintaining application administration information.	View Historical Batch Logs Priv Maintain Batch Monitoring Privilege Maintain Batch Administration Privilege View Application Logs Priv
Batch Monitoring User Duty	A duty for maintaining the batch monitoring screen.	View Historical Batch Logs Priv Maintain Batch Monitoring Privilege View Application Logs Priv

Table 5–2 Privileges

Name	Description
Maintain Batch Administration Priv	This privilege provides maintain access to Batch Administration Screen
Maintain Batch Monitoring Priv	This privilege provides maintain access to Batch Administration Screen as well as Batch Schedule Viewer Screen. This Privilege also allows to use the Action items in the above-mentioned Screen.
View Batch Monitoring Priv	A privilege for viewing Batch Monitoring Screen
View Application Logs Priv	A privilege for viewing application logs
View Historical Batch Logs Priv	This privilege provides view access to the Historic Batch Logs stored.
External Configuration Priv	This privilege provides access to the External System Configuration Screen.