Oracle® Commerce Retail Extension Module

Security Guide
Release 16.0
E79483-01

December 2016

Oracle® Commerce Retail Extension Module Security Guide, Release 16.0

E79483-01

Primary Author: Bernadette Goodman

Contributors: Anda Cadar, Nishant Rao, Tony Zgarba

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

Oracle Commerce Retail Extension Module Security Guide, Release 16.0

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 www.oracle.com.

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail applications. Installation and configuration are covered in more detail in the *Oracle Commerce Retail Extension Module Installation Guide*.

This Security Guide provides critical information about the security details of the Oracle Commerce Retail Extension Module, including the following:

- Specific security features and configuration details
- External compliance standards
- Secure product implementation, integration, and administration

Audience

This guide is for:

- Systems administration and operations personnel
- Developers
- Integrators and implementers

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.

Related Documents

For more information, see the following documents in the Oracle Commerce Retail Extension Module 16.0 documentation set:

- *Oracle Commerce Retail Extension Module Implementation Guide*
- *Oracle Commerce Retail Extension Module Installation Guide*
- *Oracle Commerce Retail Extension Module Merchandising Implementation Guide*
- *Oracle Commerce Retail Extension Module Release Notes*

For information on Oracle Commerce Platform, see the Oracle Commerce Platform Release 11.2 documentation set

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 16.0) or a later patch release (for example, 16.0.1). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times **not** be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-**02** is an updated version of a document with part number E123456-**01**.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

(Data Model documents are not available through Oracle Technology Network. You can obtain them through My Oracle Support.)

Conventions

Navigate: This is a navigate statement. It tells you how to get to the start of the procedure and ends with a screen shot of the starting point and the statement “the Window Name window opens.”

```
This is a code sample
   It is used to display examples of code
```

1

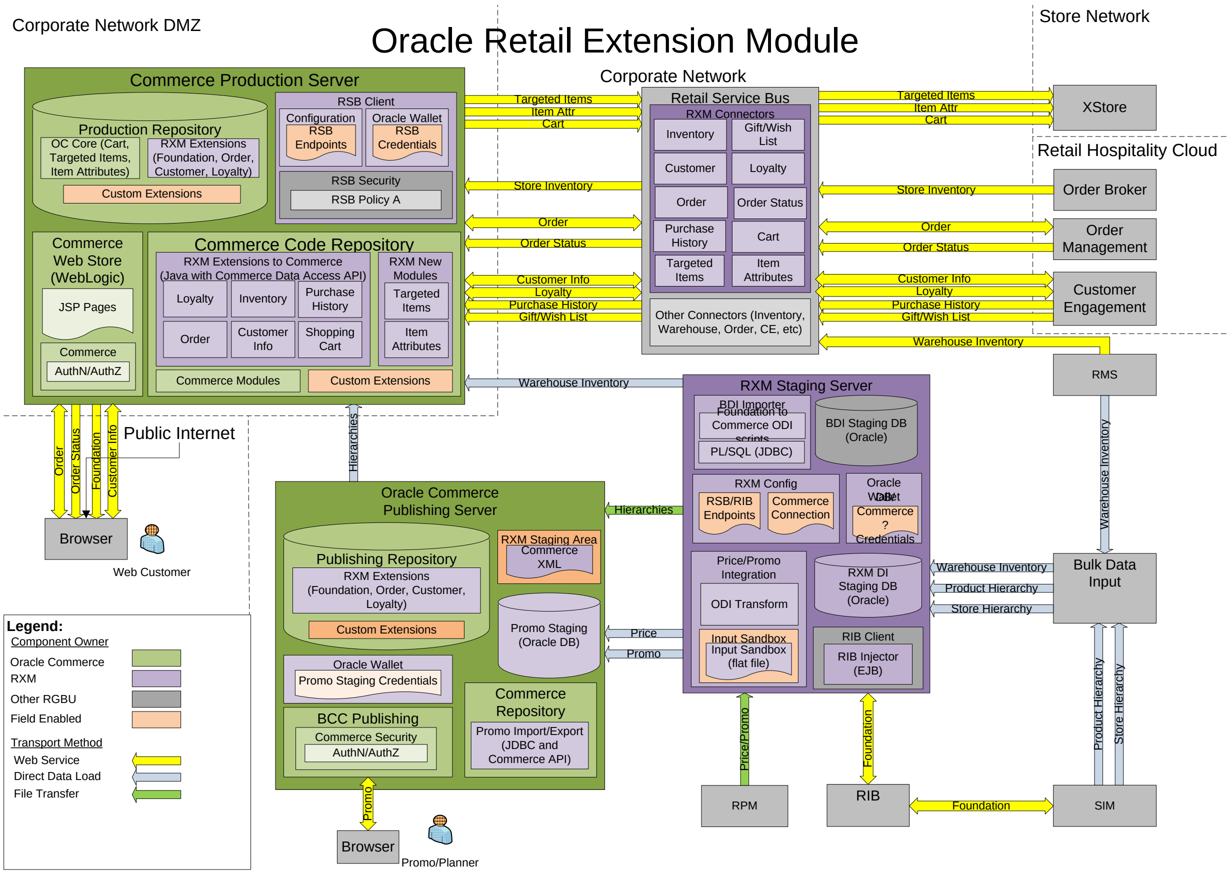
Overview of Security Features

Oracle Commerce Retail Extension Module (RXM) is a retail extension layer on Oracle Commerce 11.2.

RXM plugs into Oracle Commerce to converge retail and store concepts into e-commerce, and online shopping experience into the store applications.

To do this, RXM not only enhances Oracle Commerce functionality but also provides integrations to other Oracle-Retail applications, such as Oracle Retail Customer Engagement (ORCE), Oracle Retail Order Broker (OROB), Oracle Retail Order Management System (OROMS), Oracle Retail Xstore Point of Service (Xstore), and Oracle Retail Merchandise Operations Management (MOM).

The following figure shows a typical deployment of RXM with all the Retail and Oracle Commerce components:



Oracle Retail Extension Module Components

RXM consists of two major components, RXM Commerce Module and RXM Data Integration Module.

RXM Commerce Module

The RXM Commerce Module is a retail extension of Oracle Commerce 11.2. It enhances the Oracle Commerce 11.2 functionality by adding integrations with Oracle Retail Order Management, Oracle Retail Order Broker, Oracle Retail Xstore Point of Service, and Oracle Retail Customer Engagement. RXM Commerce Module consists mainly of SOAP web services.

RXM Commerce Module is deployed on the Oracle Commerce Production Server and on the Oracle Commerce Publishing Server. It runs on Oracle Commerce 11.2 stack with WebLogic 12.1.3. Both Publishing and Production Servers have access to dedicated database instances and are deployed in a corporate data center environment, with computer and physical access restricted to the machines.

RXM is a consumer of SOAP web services for ORCE, OROB, and OROMS integration. These web services are defined by the Oracle Retail Service Bus (RSB). The RSB is built upon Oracle Service Bus, which is an application for de-coupling and virtualizing the merchant's enterprise applications.

RSB comes as part of the Oracle Retail Integration Bus (RIB). RXM, through the RSB, provides decorator packs for each endpoint application. These packs provide transformation between RSB's service definitions and the provider applications' definitions.

RXM is a provider of services for Xstore. These services are also de-coupled and virtualized through the RSB.

RXM is an extension of Oracle Commerce and as such does not have a webstore front. Retailers are responsible for building their own webstore front to access the capabilities of RXM running on the Commerce Production Server. Oracle Commerce out of the box authentication and authorization capabilities are used to connect the webstore front user to the Commerce Production Server.

RXM Data Integration Module

RXM Data Integration Module (RXMDI) is a component that is used for integration with Oracle Retail Merchandising Operations Management (MOM).

MOM uses these frameworks for exporting data:

- A simple flat file extract for prices and promotions from Oracle Retail Price Management (RPM)
- A messaging-based extract through the Retail Integration Bus (RIB)
- A bulk data extract through the Bulk Data Integration framework (BDI).

RXMDI consumes data from all of those sources using Oracle Data Integration (ODI). RIB data is persisted into RXMDI Staging Schema directly using Camel and JPA before being consumed by ODI.

RXMDI and ODI run on the RXM Staging Server deployed at the Corporate Data Center. The RXM Staging server has access to two dedicated Oracle databases: BDI Interface Inbound Schema and RXMDI Staging Schema. RXMDI and ODI run on the Oracle Retail release 16.0 supported stack with Fusion Middleware 12.2.1.

The incremental and bulk data is staged and primarily mapped into XML files for feeding to Oracle Commerce's SQLImport program running on Oracle Commerce Publishing Server, or placed into the Oracle Commerce Production repository directly. The promotional data is mapped to staging tables in Oracle Commerce Publishing for further transformation and import by an RXM scheduled service.

The bulk and incremental data arrives at the BDI Staging database securely.

For information on securing the pipeline, see the *Oracle Retail Merchandising System Installation Guide*, *Oracle Retail Integration Bus Installation Guide*, and *Oracle Commerce Retail Extension Module Installation Guide*.

In regard to the flat files from RPM, RXM assumes the import data files are from a trusted source. It is the retailer's responsibility to ensure the integrity of the import data files and to secure access to the import files on the RXM staging server.

General Security Principles

Keep Software up to Date

One of the principles of good security practice is to keep all software versions and patches up to date. Throughout this document, it is assumed that the versions are Oracle Retail Extension Module 16.0 and Oracle Commerce 11.2

Restrict Network Access to Critical Services

Keep Oracle Commerce Publishing, RXM Staging Server, Retail Service Bus and the databases behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted if necessary.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities. When setting up user privileges, follow the Oracle Commerce best practices outlined in the Oracle Commerce Platform Security Guide.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring.

Auditing and reviewing audit records addresses the third requirement. Each component within a system has some degree of monitoring capability. RXM does not have any additional auditing capabilities besides what Oracle Commerce 11.2 provides out of the box. Follow the Oracle Commerce, WebLogic, and ODI audit advice and best practices and regularly monitor audit records.

Keep up to Date on Latest Security Information

Oracle continually improves its software and documentation. Check frequently for revisions.

Overview of Special Security Requirements

Out of the box Oracle Retail Extension Module –Does not store or transmit credit card, health, or financial data, and therefore does not does not need to satisfy external standards or accreditation agencies such as PA-DSS, PCI, or HIPPA.

When an e-commerce order is placed from an online store built on top of RXM, order payment is required.

Oracle Retail Order Management System – allows e-commerce orders to send credit card in clear text or encrypted.

Out of the box RXM – only sends credit card tokens to OMS. This setting requires retailers to use a tokenization service.

Oracle Commerce 11.2 – provides plug-in points for integrating with a Tokenization service.

The payment information sent to OMS contains the following fields:

Tokenized flag	Indicates whether the number in the cc_number tag is a token. This is set to Y by RXM in the OMS decorator pack to indicate that the number in the cc_number tag is a token and not the actual credit card number.
Auth number	The authorization code received from the Payment authorization service
Expiration date	Credit card expiration date (year and month)
Credit card	The token for the credit card OMS system looks at the setting of the already_tokenized tag to determine if the number in the cc_number tag is the actual credit card number or a token provided by the service bureau.

Dependent Applications

Oracle WebLogic

RXM runs on a WebLogic 12 application server. Proper configuration of this application server is important to insure a secure environment. The following are links to WebLogic security considerations:

Oracle WebLogic 12.2.1 Security Guide

Oracle Weblogic 12.1.3 Security Guide

Oracle Database

RXM runs on Oracle 12c database. Proper configuration of the database is important to insure a secure environment.

The following is the link to Oracle database security considerations:

Oracle Database 12c Release Security Guide

Oracle Data Integrator (ODI)

RXM runs with Oracle Data Integrator 12.2.1. Proper configuration of ODI is important to insure a secure environment.

The following is the link to ODI security considerations:

Oracle Data Integrator 12.2.1 Security Guide

Oracle Retail Service Backbone (RSB)

RXM requires Oracle Retail Service Backbone 16.0. Proper configuration of RSB is important to insure a secure environment. See the *Oracle Retail Service Bus Security Guide*.

Oracle Retail Integration Bus (RIB)

RXM needs Oracle Retail Integration Bus 16.0. Proper configuration of the RIB is important to insure a secure environment. See *the Oracle Retail Integration Bus Security Guide*.

Oracle Commerce 11.2 (OC)

RXM is an extension of Oracle Commerce 11.2. Therefore, you must follow all the Oracle Commerce security best practices and guidelines as well.

The following is the link to Oracle Commerce security considerations:

Oracle Commerce Platform 11.2 Security Guide

Security Considerations for External Applications

Use SSL/TLS (HTTPS)

Information sent over the network and across the internet in clear text can be intercepted. Secure Sockets Layer/Transport Layer Security (SSL/TLS) is an encryption scheme that negotiates an exchange of encryption keys. These keys are packaged in Certificates issued by a Certificate Authority (CA).

Note: Oracle strongly recommends that you use TLS 1.2.

RXM is integrated with external applications in several ways:

- **Flat files:** for RPM
- **JMS Messages:** for Incremental foundation data updates from Retail Merchandising System (RMS)
- **Database to Database Exchange:** for bulk data feeds from RMS
- **Webservices Consumer**: RXM is a consumer of ORCE, OROMS, and OROB web services
- **Webservices Provider**: RXM is a provider of In Store Experience web services for Xstore

Integration with RPM

RPM price and promotion integration is accomplished through flat files.

The RPM flat files are read by ODI from a folder on the RXM Staging server.

You must limit access to the folder that contains the flat files to the same OS user who has permission to install and configure ODI. These can be:

- install owners or administrators (Windows)
- chmod 700, 600, 640 (Linux)

Retailers are responsible for pushing the RPM flat files to the ODI folder for processing.

Note: Oracle strongly recommends using dedicated SFTP servers for transferring the flat files to the ODI folder.

It is the responsibility of the integrator/retailer to configure and manage credentials for the SFTP site.

The flat files are transformed by ODI and stored in RXM Staging Schema. From RXM Staging Schema, ODI moves the RPM promotion data into a folder in the installation directory of Oracle Commerce Business Control Center (BCC) on the Oracle Commerce Publishing Server. Access to BCC install folder and ODI-generated files is limited to BCC install owners or administrators (Windows) or chmod 700 (Linux). From there, data is massaged into Oracle Commerce specific format and pushed to Oracle Commerce Production Server.

Incremental Data Integration through RIB

Incremental MOM updates are sent to RXM through RIB. Data is stored in RXM Staging Schema through Java Persistence Architecture (JPA). From RXM Staging Schema, the RIB data is transformed and moved to either Oracle Commerce Production Schema (Store, Warehouse, and Inventory) or to Oracle Commerce Publishing Server to a folder in the installation directory of Oracle Commerce Business Control Center (BCC).

Access to BCC install folder and ODI-generated files is limited to BCC install owners or administrators (Windows) or chmod 700(Linux).

The RIB application ear for RXM deployed in the RIB application server has a web-based user interface application that can be accessed through HTTP or HTTPS. It is the responsibility of the retailer to configure a valid TLS connection to access the administration GUI over HTTPS.

It is the responsibility of the retailer to deploy RXMDI in a WebLogic-managed server secured with SSL. On the RXM side, in WebLogic, an IntegrationRole must be mapped to a Group (for example, IntegrationGroup). The user in this group is used by RIB to make inject calls in both EJb and WebService class. Without a valid user mapped to the group, integration will not work.

From RXM Staging Schema, the incremental data is transformed and moved by ODI directly to Oracle Commerce Production Schema (Store and Warehouse), or as an XML file (Product Catalog) to Oracle Commerce Publishing Server in a folder in the installation directory of Oracle Commerce Business Control Center.

Bulk Data Integration through RTG/BDI Framework

Bulk data feeds are sent to RXM through the Bulk Data Integration Framework provided by Oracle Retail Technology (RTG). The BdiEdgeAppJobAdminPak16.0.0ForRxm war deployed in WebLogic has a web-based user interface application which can be accessed through HTTP or HTTPS. It is the responsibility of the retailer to configure the system to access the administration GUI over HTTPS. The bulk data feeds are loaded in BDI Staging Schema and moved by ODI to the RXM Staging Schema.

From RXM Staging Schema, the data is transformed and moved by ODI directly to Oracle Commerce Production Schema (Store, Warehouse, Inventory), or as an XML file (Product Catalog) to Oracle Commerce Publishing Server in a folder in the installation directory of Oracle Commerce Business Control Center (BCC).

Access to BCC install folder and ODI-generated files is limited to BCC install owners or administrators (Windows), or chmod 700 (Linux).

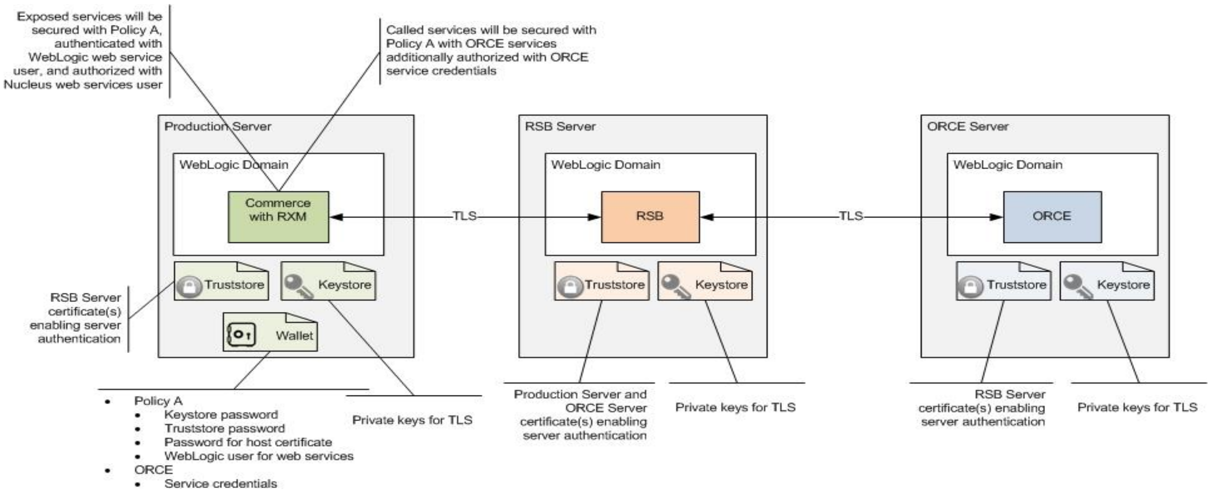
For all the above MOM integrations:

- Access to the BDI Interface Schema, RXM Staging Schemas, Oracle Commerce Publishing Schema, Oracle Commerce Production Schema, and ODI scripts and files must be restricted to an Admin user.
- The credentials used by the ODI Agent to invoke the Foundation data import scenarios that are passed in through the JavaBatch Job are stored in an Oracle wallet.
- It is the responsibility of the retailer to configure SSL for Oracle Data Integrator (ODI).

Web Services Consumer

RXM is a consumer for ORCE, OROMS, and OROB services. These systems are abstracted from RXM by the Oracle Retail Service Backbone (RSB) in the middle. RSB acts as a transport middle layer. Integration consists of several web services deployed on the RSB.

The RSB is an enterprise infrastructure for service-oriented communication. RSB provides an architectural approach that involves Oracle Retail applications being exposed as service providers, and OSB core components, called Decorator Services, wrap the edge-app-services to provide virtualized and operational visibility to Oracle Retail services infrastructure. Finally, the decorator services expose proxy WSDLs that are called by service consumers such as RXM.


Exposed services will be secured with Policy A, authenticated with WebLogic web service user, and authorized with Nucleus web services user
Called services will be secured with Policy A with ORCE services additionally authorized with ORCE service credentials
Production Server
WebLogic Domain
Commerce with RXM
TLS
Truststore
Keystore
Wallet
RSB Server certificate(s) enabling server authentication
Policy A
Keystore password
Truststore password
Password for host certificate
WebLogic user for web services
ORCE
Service credentials
Private keys for TLS
RSB Server
WebLogic Domain
RSB
TLS
Truststore
Keystore
Production Server and ORCE Server certificate(s) enabling server authentication
Private keys for TLS
ORCE Server
WebLogic Domain
ORCE
Truststore
Keystore
RSB Server certificate(s) enabling server authentication
Private keys for TLS

Web Services Integration

Securing the integration involves the following components:

RXM Deployed on the Oracle Commerce Production Server

RXM calls the RSB services over TLS.

RSB Server certificates enabling server authentication are stored in the truststore on Oracle Commerce Production Server.

A keystore, located on the same server, stores the private keys for TLS communication

> **Note:** Oracle strongly recommends using CA-signed certificates for generating keystore and truststore needed for web service security.

RXM ships with a tool (CSM) provided by Oracle Retail to create and maintain a credential store to be used for the secure storage of credentials. The credential store framework (CSF) API is used to access and perform operations on the credential store. CSF provides the following capabilities:

- Enables the secure management of credentials.
- Provides an API for the storage, retrieval, and maintenance of credentials.
- Supports file-based storage, such as Oracle wallet

The following sensitive information is stored in an Oracle Wallet created with the CSM tool:

- Keystore password
- Truststore password
- Password for host certificate
- WebLogic user for web services
- Credentials for accessing the edge applications

The Oracle Wallet location is configured as part of WebLogic installation.

The edge application's credentials are sent in the HTTP request header.

RSB Deployed on the RSB Server

The RSB Soap Services are secured using SOAP Policy Wssp1.2-2007-Https-UsernameToken-Plain.xml over a TLS-encrypted connection.

The RSB proxy service processes the header in RXM's SOAP messages and routes the message to the corresponding edge application.

Edge Applications Deployed on the Cloud

Connections to the edge application's web services use HTTP Basic Authentication (username/password) over TLS. You create the user and password using the edge application's administrative console.

When a web service SOAP message comes into the edge applications, a web service interceptor grabs the message immediately. It checks the HTTP headers to make sure that basic authentication is included. If not, the processing stops and a generic HTTP error is returned. If basic authentication is included, it checks the user/password.

Note: Oracle strongly recommends that you change the web service user passwords on a regular basis (every six months). You must create new web service users and remove old users, allowing for a transition period for deploying these updates.

Web Services Providers

RXM is a service provider for Oracle Retail Xstore Point of Service.

The following services are exposed for Xstore:

- ItemInformationService
- ShoppingCartService
- TargetedItemsService

You need to install the unlimited encryption Java Cryptography Extension (JCE) policy to use the strongest Cipher suite (256 bit encryption) AES_256 for the integration with Oracle Retail Xstore Point of Service.

You can download and install the JCE Unlimited Strength Jurisdiction Policy Files that correspond to the version of your JDK by going to the following link: http://www.oracle.com/technetwork/java/javase/downloads/index.html

The SOAP web services exposed by RXM Services use the JAX-WS API, which is different than the JAX-RPC web service framework provided by the Oracle Commerce Platform.

The services are deployed as part of the RXM ear file on the WebLogic 12.1.3.

These services are secured through the use of Username Token over HTTPS Web Service policy over TLS. It is also secured through HTTP Basic Authentication (username/password).

Through this configuration authentication, authorization and confidentiality are accomplished in the following ways:

- Authentication - Xstore identity is verified based on the username/password credentials that are being sent in request in the HTTP Authentication header (that is, Basic Authentication).
- The Username Token over HTTPS (Policy A) provides a level of authentication because the credential provided in the SOAP header is authenticated by WebLogic.

That credential is assigned to each web service in the Policy A setup. Next, the credential provided in the HTTP header is authenticated by WebLogic. Once all that passes, then that same HTTP header credential is authenticated by Commerce and authorized by the RXM web services.

- Application-level authorization is enabled by default in RXM. A Commerce user with a security role to authorize the web service calls must be defined.
- Confidentiality is provided by TLS

For this integration, RSB acts as a passthrough.

Xstore communications with RXM are secured through the use of Username Token over HTTPS Web Service policy over TLS. They are also secured through HTTP Basic Authentication (username/password).

The user name and password are stored in encrypted form and they are only decrypted when it is necessary to include them in a request to RXM. The user name and password can be changed to whatever is required by the RXM application. The users that are considered to be legitimate are controlled by Oracle Commerce. RXM just uses their mechanisms.

Technical Overview of the Security Features

Security Features of the Application

Personal Identifiable Information (PII)

Personal Identifiable Information is data that can be used to identify a customer. There are international, federal, and state laws addressing consumer PII data breach notification requirements. It is therefore important that PII is protected. Care should be taken in storing this information as well as masking or removing it from any log files.

For RXM, the following extensions are added to the Oracle Commerce User Profile that contain PII data.

Database Table	Extension	Data Type
rxm_user	ext_user_id	String
rxm_user	company_name	String
rxm_user	loy_card_num	String
rxm_email	email_address	String
rxm_phone	phone_number	String
rxm_phone	extension	String

Refer to the following Oracle Commerce documentation for information about PII data in base Oracle Commerce 11.2:

Standard User Profile

Commerce Extensions to User Profile

Secure Storing of PII Data

The Oracle Commerce Platform secured repository system works in conjunction with the Oracle Commerce Platform Security System to provide fine-grained access control to repository item descriptors, individual repository items, and individual properties through Access Control List (ACL) settings. See the **Secured Repositories** section of Oracle Commerce Repository Guide.

User Password Hashing

The Retail Extension Module does not capture, store, or use passwords in the code base. RXM implementers must use Retail Extension Module to build their store front and must follow the Oracle Commerce guidelines for passwords and password management.

For security reasons, ATG Commerce recommends storing passwords in hashed form, so that if an unauthorized person gains access to the database, he or she will not be able to retrieve the actual passwords of Commerce users. Hashing performs a one-way transformation of the password, encrypting it in a way that makes it extremely difficult to reconstruct the original password.

See the Password Hashing section of the Oracle Commerce Personalization Programming Guide.

Password Management Policy

ATG Commerce Password management features include:

- Setting a regular period at which passwords expire
- Defining rules that users must satisfy when creating passwords
- Handling forgotten passwords
- Notifying a user when a password is about to expire
- Forcing all passwords to expire immediately

See the Password Management Features section of Oracle Commerce Personalization Programming Guide.

Cryptography

RXM does not provide any cryptography on its own and delegates all cryptography to either the Commerce Platform or the TLS provider.

Data Validation

All data is communicated within the body of a SOAP message that is sent over a TLS-encrypted connection. Data that makes up the contents of the message is validated for appropriate values using standard XSD validation against the XML before being included in the messages. These values can include no unbounded elements, ensuring that customer IDs and item IDs are limited to a certain number of characters, quantities are only expressed as numbers, and so on.

2

Application Administration

Roles and Permissions

The only additional roles and permissions for RXM are around the web services.

RXM creates the webservices-user-group in the DAS_ACCOUNT table and populates the DAS_NS_ACLS with:

```
ItemInformationService.retrieveItemInformation      0
    Admin$role$administrators-group:execute;Admin$role$webservices-user-
group:execute
ShoppingCartService.removeAllItemsFromCart   0      Admin$role$administrators-
group:execute;Admin$role$webservices-user-group:execute
ShoppingCartService.removeItemsFromCart      0      Admin$role$administrators-
group:execute;Admin$role$webservices-user-group:execute
ShoppingCartService.retrieveShoppingCart     0      Admin$role$administrators-
group:execute;Admin$role$webservices-user-group:execute
TargetedItemsService.queryTargetedItems      0      Admin$role$administrators-
group:execute;Admin$role$webservices-user-group:execute
```

RXM also populates DAS_NUCL_SEC with:

```
ItemInformationService.retrieveItemInformation
    /atg/dynamo/security/SecurityPolicy
ShoppingCartService.removeAllItemsFromCart   /atg/dynamo/security/SecurityPolicy
```

Security Audit Logging

Oracle Retail recommends enabling audit logging for:

- All actions taken by any individual with administrative privileges as assigned in the application.
- Access to application audit trails managed by or within the application.
- Unauthorized attempts to access your administration applications.
- Use of application's identification and authentication mechanisms.

To configure and use security audit to bolster software security, see the Configuring and Using Security Audit section of Oracle Commerce Platform security Guide.

Logging

Logging of system events is controlled by the log4j.xml file on the application server.

Logging levels can be adjusted, but it is recommended that they be left at ERROR.

Sensitive data must not be displayed in log files. If you are extending RXM, follow Oracle Commerce 11.2 best practices and avoid log statements that might compromise sensitive data.

3

Security Guidelines for Developers

Oracle Retail Extension Module exposes SOAP web services for integration with other applications. Oracle Retail Extension Module is also a consumer of SOAP web services.

Developers should take care to ensure secure integration implementations.

Authorization / Authentication

The SOAP web services require user IDs and passwords for authorization.

- User IDs and Passwords must not be hard-coded, shipped, or defaulted in the integrating application.
- Passwords must not be stored in plain text, either in a file or in a database table.
- Passwords must be stored in an encrypted format. You should not create your own password encryption mechanism. Consider storing passwords and other credentials in a wallet, or use an approved algorithm such as one recommended by National Institute of Standards and Technology.

Data Validation

The developer also must validate all data passed to the web services. Special care should be taken if the data is coming from an untrusted source. Checks should be made to prevent very long strings from being passed to the methods. Strings longer than 2 GBs will fail.

Also, external clients receiving data from web services should insure the data is correctly encoded (escaped) to avoid injection flaws.

Personal Identifiable Information (PII)

Personal Identifiable Information is data that can be used to identify a customer. There are international, federal, and state laws addressing consumer PII data breach notification requirements. It is therefore important that PII is protected. Take care in storing this information as well as masking or removing it from any log files.

Safe and Secure Error Handling

Developers must handle all exceptions safely and securely. Take care to respect data types and processing error conditions.

Logging and Error Handling

Log files and error messages can be a source of information that could assist an attacker in gaining unauthorized access to a system. Follow these guidelines to prevent unauthorized access:

- Protect logs from unauthorized access and modification.
- Do not output in error messages sensitive information that could assist an attacker.
- Do not log sensitive information that could assist an attacker, unless for security audit purposes.
- Purge sensitive information from exceptions.

Web Service SOAP Message Processing

- Parse XML using a well-known XML Framework.
- XML Framework should prevent XXE and XEE. Ensure all string values placed into requests sent to RXM APIs are properly encoded to ensure the application is not susceptible to reflected and DOM Cross-Site Scripting (XSS) attacks.

A

Appendix: Database Security

You should secure the database using the recommendations from the Oracle Database 12c Release Security Guide. The following sections provide additional application-specific guidance for securing the database for use with RXM.

Application Schema Owners

The following recommendations are for the schema owners:

- Database Administrators should create an individual schema owner for each application, unless the applications share the same data.
- The schema owners should only have enough rights to install the applications.

Set the following rights when using an Oracle database:

```
*CREATE TABLE
*CREATE VIEW
*CREATE INDEX
*CREATE SEQUENCE
*ALTER SESSION
*CONNECT
*SELECT_CATALOG_ROLE
```

The user ID and password for schema owners must comply with these PA-DSS user and password policies:

- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords used.
- Limit repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to 30 minutes or until an administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to reenter the password in order to reactivate the terminal.

Schema Maintenance

Maintenance scripts must have their own user schema. Oracle Retail recommends creating a limited user at the database to handle schema maintenance (deleting data from the database). You can accomplish this by granting execute rights only on delete store procedures.

Set the following rights when using an Oracle database:

```
*ALTER SESSION
*CONNECT
*SELECT_CATALOG_ROLE
*GRANT EXECUTE on PROCEDURE
```

Set the following rights when using an IBM DB2 database:

```
*CONNECT
*IMPLICIT_SCHEMA
*GRANT EXECUTE on PROCEDURE
```

- Only run maintenance scripts using a non-operating system administrator user ID.
- Run maintenance scripts as part of a secure schedule job.
- An operating system user should not have the ability to log in remotely to the database server.
- An operating system user should only use the scripts for maintenance purposes.
- An operating system user should not have administrator rights.
- An operating system user should not have execute, read, or write permission of any file beyond the file to execute the data maintenance script.

Database Security Considerations

Oracle recommends the following for the database:

- The database server must be in a private network.
- The database server must be in a locked secure facility and inaccessible to non-administrator personnel.
- The database must only be accessed through trusted network hosts.
- The database server must have minimal use of ports and any communications should be under secure protocols.
- The database must be on its own dedicated server.
- The database server must be behind a firewall.
- Any database user beyond the schema application owner must be audited.
- Only minimal rights should be granted to the owner of database processes and files such that only that owner has the right to read and write from the database-related files, and no one else has the capability to read and write from such files.