

Oracle® Retail Merchandising Cloud Services
Administration Guide
Release 16.0.031
F21413-03

March 2020

Copyright © 2019, Oracle and/or its affiliates. All rights reserved.

Primary Author: Nathan Young

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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	ix
Preface	xi
Audience.....	xi
Customer Support.....	xi
Improved Process for Oracle Retail Documentation Corrections	xi
Oracle Retail Documentation on the Oracle Technology Network	xii
Conventions	xii
1 Administrative Tasks	
Oracle Support	1-1
Oracle Identity Cloud Service User and Group Management	1-1
Retail Merchandising Cloud Services Default Enterprise Roles.....	1-1
Nightly Batch File Uploads	1-3
Adding Authorized Keys.....	1-3
Steps – Login to WinSCP	1-4
Uploading Batch Files	1-6
Download Batch Files.....	1-8
2 Manage Security Policies	
Navigation	2-2
Accessing RAAC	2-2
Roles Explained	2-3
Job Roles	2-3
Duty Roles.....	2-3
Privilege Roles	2-3
Security	2-3
Task Flows.....	2-4
Manage Duty Roles.....	2-5
Add	2-5
Add a Duty Role	2-5
Edit	2-6
Edit a Duty Role.....	2-6
Delete	2-6
Delete a Duty Role.....	2-6

Export to Excel.....	2-7
Manage Roles Mapping	2-7
Duplicate	2-7
Duplicate a Job Role	2-8
Delete	2-8
Export to Excel.....	2-9
Select and Add.....	2-9
Select and Add a Duty	2-9
Remap	2-9
Remap a Role.....	2-10
Manage Policy Patching.....	2-10
Copy to Custom.....	2-12
Copy Privilege/Duty to Duty/Role.....	2-12
Sync	2-13
Synchronize Permissions in a Privilege.....	2-13
View Permissions	2-14
Overwrite Custom Policies	2-14
Import Custom Policies.....	2-15
Done	2-15
Refresh	2-15
Manage Backups.....	2-15
Create	2-16
Delete	2-16
Download.....	2-17
Restore	2-17
Refresh	2-18

3 Data Security/Filtering

Data Security/Filtering Implementation.....	3-1
Setup Security Groups.....	3-1
Setup Security User and Security User Role	3-5
Map Security User to Security Group	3-10
Assign Groups to Hierarchies	3-14
Setup Purchase Order Approval Limits	3-19

4 Application Customization

User Interface Customization	4-2
Tasks Menu Customization	4-3
Task Menu Model XML Items	4-5
Task Menu Model Item Attributes	4-5
Task Menu Model Item Sub-elements	4-8
Securing Access to Items.....	4-8
Reports Menu Customization	4-9
Sidebar Menu Customization.....	4-10
Sidebar Menu Model XML Items	4-11
Sidebar Menu Model Item Attributes	4-12
Sidebar Model Item Sub-elements.....	4-12

Application Navigator.....	4-12
Add	4-13
Add an Application Navigator URL.....	4-13
Modify	4-13
Duplicate	4-13
Delete	4-14
Export to Excel.....	4-14
Dashboards and Reports.....	4-14
Dashboard Customization.....	4-15
Understanding Design Pattern of Included Dashboards.....	4-17
The Dashboard Prompt Configuration XML File.....	4-21
Refreshing Reports on Prompt Changes	4-23
Adding or Replacing a Report in an Included Dashboard	4-24
Removing a Report from an Included Dashboard	4-24
Change the Layout Of an Included Dashboard.....	4-24
Reports.....	4-25
Reports Customization.....	4-28
Adding a URL based Contextual Report	4-29
Adding a DVT Taskflow based Contextual Report.....	4-30
Notifications.....	4-32
Notification Types.....	4-32
Add	4-32
Add a Notification Type	4-32
Edit	4-33
Edit a Notification Type.....	4-33
Delete	4-34
Delete a Notification Type.....	4-34
Export to Excel.....	4-34
Notification Groups and Roles.....	4-35
Create/Add Notification Group.....	4-35
Create a Notification Group.....	4-35
Add Job Role.....	4-35
Add a Job Role.....	4-35
Edit	4-36
Edit a Notification Group	4-36
Delete	4-36
Delete a Notification Type.....	4-36
Export to Excel.....	4-37
Resource Bundles	4-37
Resources and Customizations Explained	4-37
Task Flows.....	4-38
Resource Text Strings	4-38
View	4-39
Add or Edit	4-39
Remove Customization.....	4-39
Export to CSV	4-40
Import CSV File.....	4-40

Importing Customizations from a CSV File.....	4-40
Lookups.....	4-41
Add.....	4-41
Edit	4-42
Delete	4-42
Save / Cancel.....	4-43
Asynchronous Tasks.....	4-44
View	4-44
Purge Task.....	4-45
Export to Excel.....	4-46
Application Properties	4-46

5 Merchandising Data Viewer

Workspace.....	5-1
Users and Roles.....	5-1
Create a Workspace Viewer.....	5-1

Send Us Your Comments

Oracle® Retail Merchandising Cloud Services Administration Guide, Release 16.0.031

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at <http://www.oracle.com>.

Preface

This guide describes the administration tasks for Oracle Retail Merchandising Cloud Services.

Audience

This guide is intended for administrators.

This guide describes the administration tasks for Oracle Retail Merchandising Cloud Services.

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.

Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

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

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the

same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

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

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

Administrative Tasks

This chapter describes the processes for maintaining users and roles as well as batch processes. For information regarding standard end user activities like creating and viewing reports, please see the *Oracle Retail Merchandising Cloud Services User Guides*.

Oracle Support

It is considered to be a best practice to have all Oracle Retail Merchandising Cloud Services support requests submitted through a single point of contact for that customer environment; the client designated administrator is usually designated to perform this role.

The link to use when submitting Service Requests (SR) is:

<https://support.oracle.com>

Oracle Identity Cloud Service User and Group Management

Oracle Identity Cloud Service (IDCS) provides an innovative, fully integrated service that delivers all the core identity and access management capabilities through a multi-tenant Cloud platform.

For instructions on managing users and groups in IDCS, follow the Manage Users and Groups IDCS document at the following URL:

<https://docs.oracle.com/en/cloud/paas/identity-cloud/index.html>

Retail Merchandising Cloud Services Default Enterprise Roles

Retail Merchandising Cloud Services is built with role-based access. Permissions are associated with roles.

The following roles are available for RMS and ReSA:

Table 1–1 Retail Merchandising Cloud Services Default Enterprise Roles

Module	Default Enterprise Roles	Corresponding Application Roles
Merchandising	Application Administrator	RMS Application Administrator
Merchandising	Data Steward	RMS Data Steward
Merchandising	Buyer	Buyer
Merchandising	Inventory Analyst	Inventory Analyst
Merchandising	Inventory Manager	Inventory Manager

Table 1–1 (Cont.) Retail Merchandising Cloud Services Default Enterprise Roles

Module	Default Enterprise Roles	Corresponding Application Roles
Merchandising	Corporate Inventory Control Analyst	Corporate Inventory Control Analyst
Merchandising	Inventory Control Manager	Inventory Control Manager
Merchandising	Sourcing Analyst	Sourcing Analyst
Merchandising	Finance Analyst	Finance Analyst
Merchandising	Supply Chain Analyst	Supply Chain Analyst
Merchandising	Finance Manager	Finance Manager
Sales Audit	Sales Audit Analyst	Sales Audit Analyst
Sales Audit	Sales Audit Manager	Sales Audit Manager
Sales Audit	Application Administrator	RESA Application Administrator
Sales Audit	Finance Manager	Finance Manager
Batch Schedule	Batch Business	Batch Business
Pricing	Application Administrator	Pricing Application Administrator
Pricing	Data Steward	Pricing Data Steward
Pricing	Pricing Analyst	Pricing Analyst
Pricing	Pricing Manager	Pricing Manager
Pricing	Promotion Planner	Promotion Planner
Pricing	Promotion Manager	Promotion Manager
Invoice Matching	Accounts Payable Specialist	Accounts Payable Specialist
Invoice Matching	Finance Manager	Finance Manager
Invoice Matching	Buyer	Buyer
Invoice Matching	Corporate Inventory Control Analyst	Corporate Inventory Control Analyst
Invoice Matching	Application Administrator	ReIM Application Administrator
Invoice Matching	Finance Analyst	Finance Analyst
Invoice Matching	Accounts Payable Manager	Accounts Payable Manager
Invoice Matching	Data Steward	Data Steward
Allocation	Application Administrator	Allocation Application Administrator
Allocation	Allocation Manager	Allocation Manager
Allocation	Allocator	Allocator
Allocation	Buyer	Buyer

Note: A new DATAPRIV_ADMINISTRATOR_REST_API_ROLE and DATA_PRIVACY_ADMINISTRATOR_JOB was created which are not associated to application users. These should be assigned to the users that invoke ReST services.

Nightly Batch File Uploads

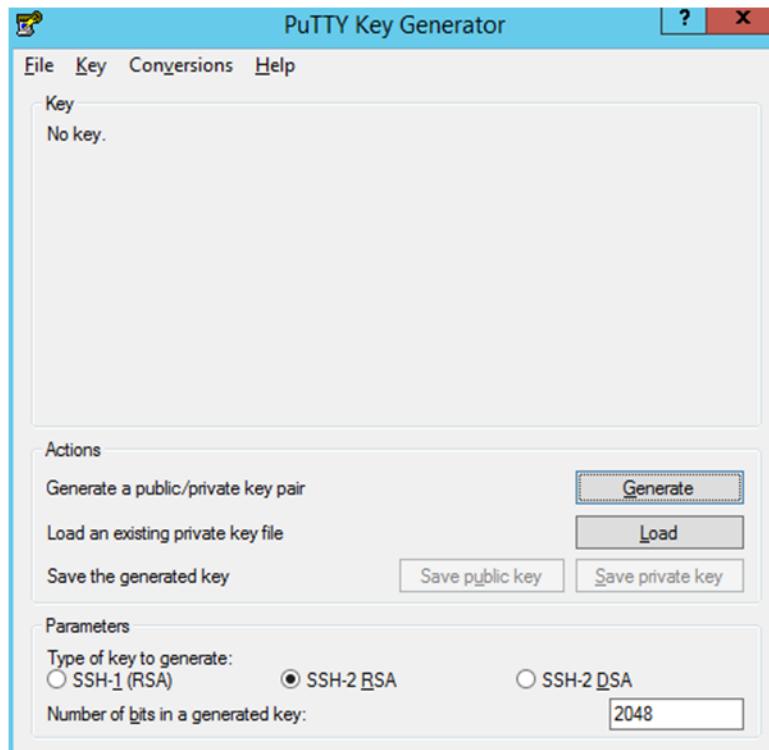
The following is the file upload process. For details regarding file contents and formatting please refer to the Oracle Retail Insights Cloud Services Integration Guide. The Private/Public Keys must be generated and the public Key must be associated with your SFTP Account for the file uploads. The [Adding Authorized Keys](#) section describes the step-by-step method to generate the Keys (2048 bit RSA Keys).

Adding Authorized Keys

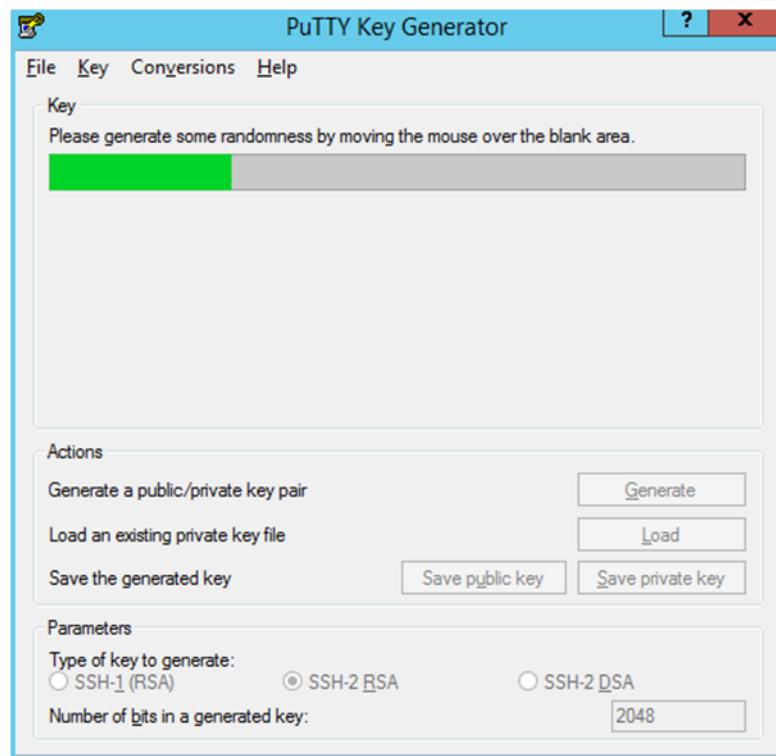
The following is the process to generate a 2048 bit RSA key and add the same to the SFTP server. This is done with the help of WinSCP tool on Windows. However the same can be done using ssh-keygen on Linux as well.

1. Launch WinSCP and select Tools -> Run PuttyGen.
2. Select "SSH-2 RSA" for the type of key to generate and enter "2048" for the number of bits in a generated key field and click **Generate**.

Figure 1-1 Key Generator



3. Move the mouse over the blank space in the window until the key is generated.

Figure 1–2 Key Generator Progress

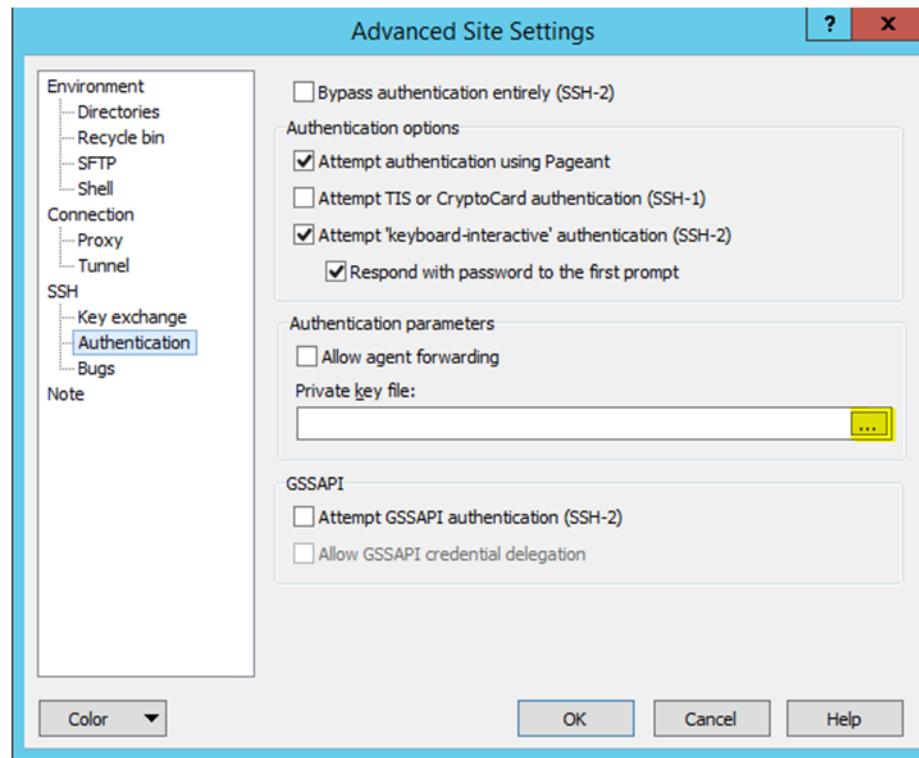
4. Once the key is generated, click the **Save public key** button to save the public key to a file.
5. Click the **Save private key** button to save the Private key to a file. Confirm to save it with/without a passphrase.
6. Open an SR with Oracle Support, to associate the Public half of the Key with your SFTP account (attach the Key with the SR).

Steps – Login to WinSCP

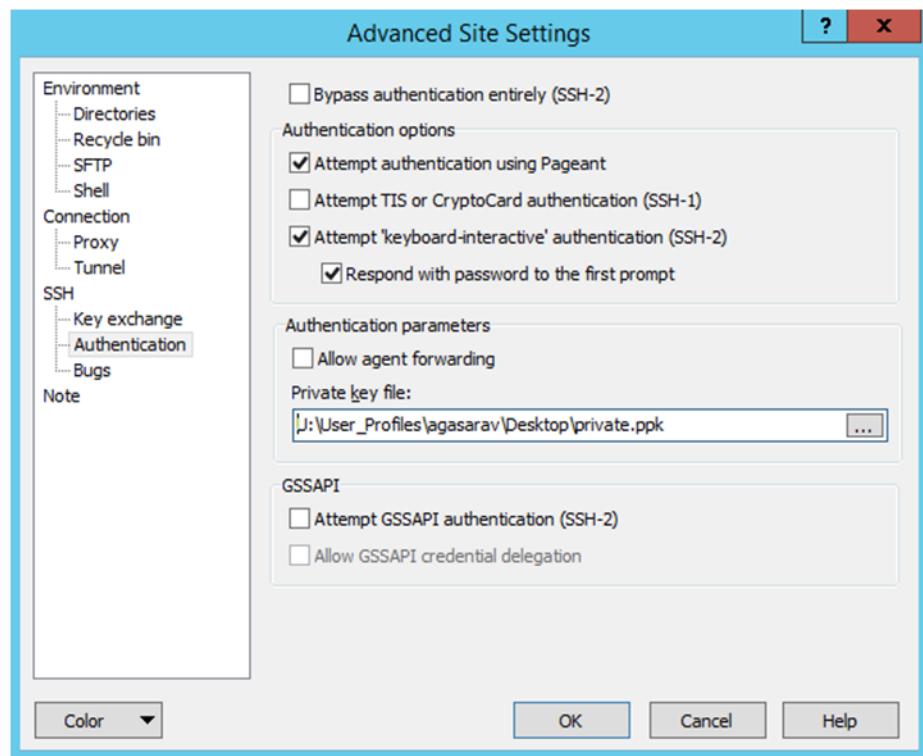
The Upload steps uses the private key generated in the earlier section.

1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the username and click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click the **Browse** button and select the private key created in the earlier section.

Figure 1–3 Advanced Site Settings Dialog



5. After loading the private key file, click **OK**.

Figure 1–4 Private Key File Loaded

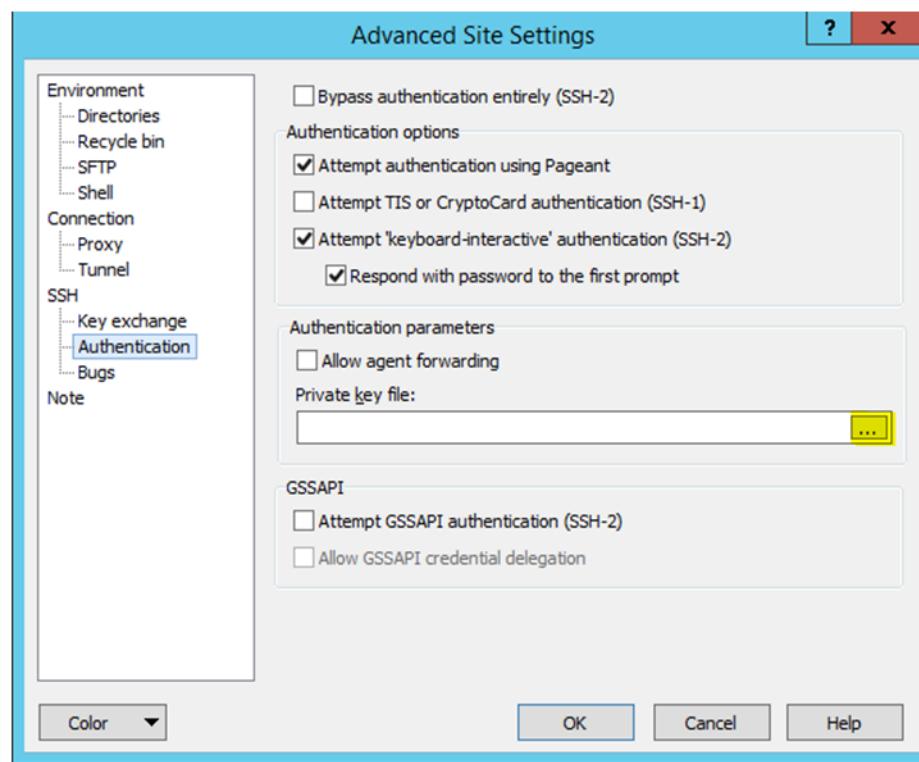
6. Click **Login**. The window does not prompt for a password and logs into the SFTP server. Provide a passphrase if one has been set up.

Uploading Batch Files

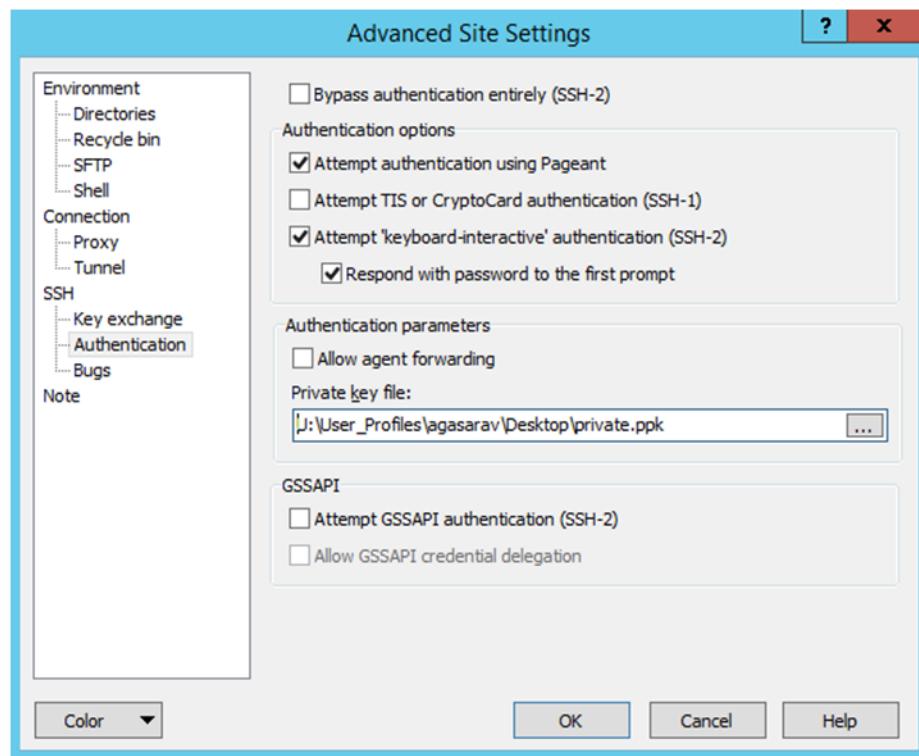
The Upload steps use the private key generated in the earlier section.

1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the username and click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click the **Browse** button and select the private key created in the earlier section.

Figure 1–5 Advanced Site Settings Dialog



5. After loading the private key file, click **OK**.

Figure 1–6 Private Key File Loaded

6. Click **Login**. The window does not prompt for a password and logs into the SFTP server. Provide a passphrase if one has been set up.
7. Transfer all data files to the directory /<SFTP User>.
8. For each data file transferred to /<SFTP User>, transfer a corresponding file <filename>.complete

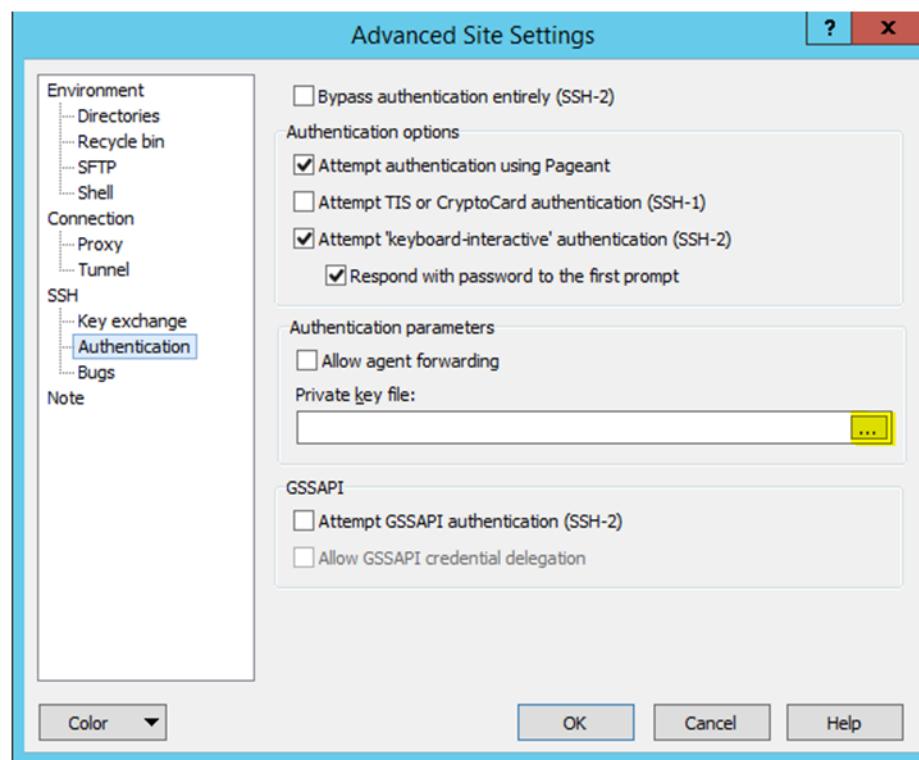
For example, if data_file1.dat, data_file2.dat, data_file3.dmp are the files to transfer, then transfer the below files to the /<SFTP User>/ directory.

```
data_file1.dat.complete
data_file2.dat.complete
data_file3.dmp.complete
```

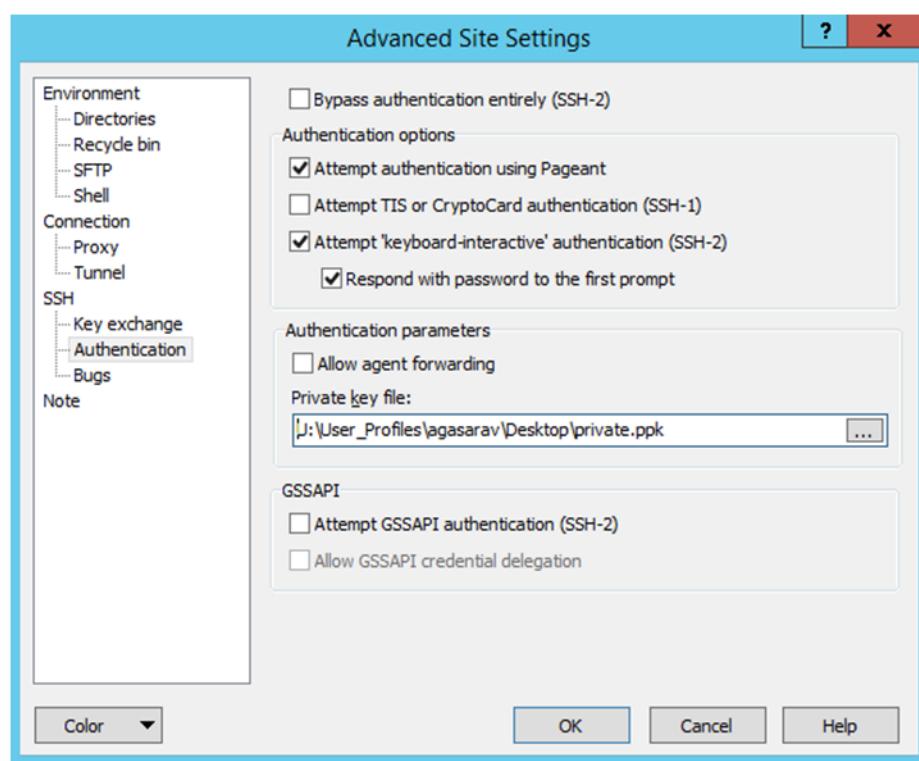
Download Batch Files

1. Launch WinSCP and connect to <SFTP Server> using port 22.
2. Enter the username and click **Advanced**.
3. Click **Authentication**.
4. In the Private Key File field, click the **Browse** button and select the private key created in the earlier section.

Figure 1–7 Advanced Site Settings Dialog



5. After loading the private key file, click **OK**.

Figure 1–8 Private Key File Loaded

6. Click **Login**. The window does not prompt for a password and logs into the SFTP server. Provide a passphrase if one has been set up.
7. Change directory to /<SFTP User>/EXPORT.
8. Download all data files.

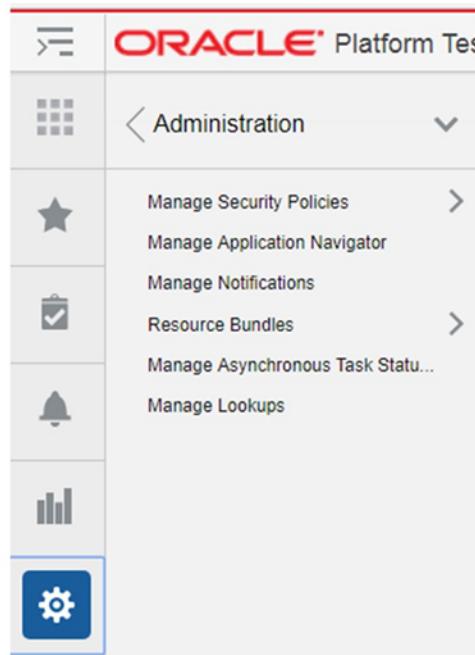
2

Manage Security Policies

As part of the Oracle Retail application security set up, default enterprise roles and their mappings to application roles are provided with every application. These enterprise roles/groups may not map one-to-one to retailers' security groups. The Manage Security Policies option in the Administration menu, accessed through the Settings icon on the task bar, provides a way for retailers to modify the default enterprise roles so they map to their security groups. It also provides a way for the retailers to change the mappings of the enterprise roles/groups to the application roles.

Note: Merchandising maintains various policy stripes in the OPSS schema. The policy stripes are maintained to ensure that the changes done by the retailer on the application security setup are preserved on the subsequent patch installs. A policy patching screen is also provided where the retailers can merge the changes introduced in a patch with the changes done in the application policy setup.

Figure 2–1 Administration Menu



Navigation

Access to this functionality is available only for users with the following job roles:

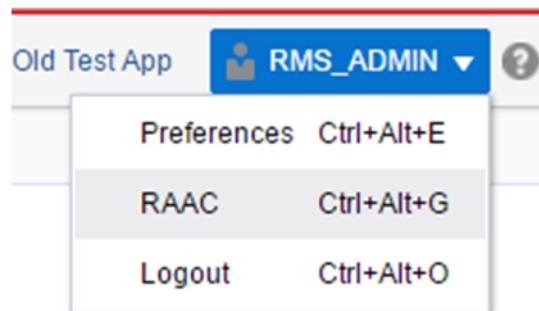
Table 2–1 RAAC Security Privileges

Role	Duty	Privilege
ReIM Application Administrator	Admin Duty	Application Navigator Privilege
		Role Manager Privilege
		Notification Manage Privilege
		Resource Customization Privilege
Allocation Application Administrator	Admin Duty	Application Navigator Privilege
		Role Manager Privilege
		Notification Manage Privilege
		Resource Customization Privilege
Pricing Application Administrator	Admin Duty	Application Navigator Privilege
		Role Manager Privilege
		Notification Manage Privilege
		Resource Customization Privilege
ReSA Application Administrator	Admin Duty	Role Manager Privilege
		Application Navigator Privilege
		Notification Manage Privilege
		Resource Customization Privilege
RMS Application Administrator	Admin Duty	Role Manager Privilege
		Application Navigator Privilege
		Notification Manage Privilege
		Resource Customization Privilege

Accessing RAAC

RAAC is accessed through either the links in the Administration menu of the Settings menu or through the RAAC link in the administrator's user menu on the Global (top) bar of the screen.

1. Click the RAAC application link in the user menu.

Figure 2–2 RAAC User Menu

A new tab window or browser window is launched (depending on your browser settings).

2. From the Retail applications' login screen (for non-single sign-on), enter your username and password.

Roles Explained

The following is an explanation of Enterprise (or Job) Roles and Application (or Duty and Privilege) roles:

Job Roles

Job roles are called as such because they closely map to the jobs commonly found in most retailer organizations.

Naming Convention: All retail Job role names end with '_JOB'.

Example: ALLOCATOR_JOB.

Duty Roles

Duties are tasks or responsibilities one must do on a job.

Duty roles are roles that are associated with a specific duty or a logical grouping of tasks. Generally, the list of duties for a job is a good indicator of what duty roles should be defined.

Duties that you create should be self-contained and pluggable into any existing or new job role.

Naming Convention: All retail duty role names end with '_DUTY'.

Example: ALC_ALLOC_POLICY_MAINTENANCE_MANAGEMENT_DUTY.

Privilege Roles

Privilege is the logical collection of permissions. A privilege can be associated with any number of UI components. Privileges are expressed as application roles.

Naming Convention: All retail privilege role names end with '_PRIV'.

Example: ALC_ALLOC_SEARCH_PRIV

Security

RAAC uses ADF security to implement functional security. The enforcement of functional security is delegated to the Fusion Middleware.

RAAC allows retailers to tailor Oracle Retail applications' default security models to their enterprise business model. This tool also helps retailers manage their Retail applications' security metadata. RAAC provides:

- The ability to create new Application Roles (DUTY) through the Manage Roles Mapping task.
- The ability for a retailer to change the default roles mapping based on its business needs.
- The ability for clients to backup the roles mapping to a file in their local file system.
- The ability for a retailer to preserve the changes done to the default application policies beyond patch installs and merge the policy changes introduced in a patch with the policy changes done by the retailer.
- The ability for a retailer to backup the roles mapping to a backup OPSS Stripe. The backup stripe can be used to download the backup policies at any time or to restore the application policies using the backup policies.

Note: The Roles mapping changes in RAAC will only change the launching application's functional behavior and not the RAAC application itself.

For additional information on changing the RAAC application Roles Mapping, see the Managing Policies with Fusion Middleware Control section in the *Securing Applications with Oracle Platform Security Services Guide*.

Task Flows

The Manage Security Policies area of RAAC consists of the following task flows to fulfill the above mentioned business requirements.

- Manage Duty Roles
- Manage Roles Mapping
- Manage Policy Patching
- Manage Backups

It is advisable that before starting to customize the Security Policies, the user should use the Manage Backups feature to make a backup of the current policies.

Manage Duty Roles

Figure 2–3 Manage Duty Roles Screen

Role Name	Description
ADMIN_CONSOLE_DUTY	A duty for searching for and viewing actual landed cost (ALC).
ALC_ALLOC_INQUIRY_DUTY	A duty for finalizing actual landed cost (ALC). This duty is an extension of the ALC Inquiry Duty.
ALC_ALLOC_MANAGEMENT_DUTY	A duty for viewing application administrative information including system options.
ALLOC_GLOBAL_MENU_DUTY	A duty for managing asynchronous jobs. This duty is an extension of the Application Admin Inquiry Duty.
REIM_GLOBAL_MENU_DUTY	A duty for managing average cost values.
RESA_GLOBAL_MENU_DUTY	A duty for managing average cost values.
RMS_ALC_INQUIRY_DUTY	A duty for managing average cost values.
RMS_ALC_MGMT_DUTY	A duty for managing average cost values.
RMS_APPLICATION_ADMIN_INQUIRY_DUTY	A duty for managing average cost values.
RMS_APPLICATION_ADMIN_MGMT_DUTY	A duty for managing average cost values.
RMS_ASYNCRONOUS_JOB_MGMT_DUTY	A duty for managing average cost values.
RMS_AVERAGE_COST_MGMT_DUTY	A duty for managing average cost values.
RMS_AVERAGE_COST_MONT_DUTY	A duty for managing average cost values.
RMS_BUDGETS_INQUIRY_DUTY	A duty for managing average cost values.

The Manage Duty Role task flow allows users to create or delete duties. Users can create a new duty role to map according to the retailers enterprise business model.

When a user clicks the manage duty role task flow from the regional area, it opens a new tab in the local area. A table is displayed with all the duties associated with the application. The table toolbar has the following action menu:

- Add
- Edit
- Delete
- Export to Excel

A quick search component is provided on the table toolbar to quickly look up any desired record.

Add

The Add action is enabled at all times and allows you to add a new duty role.

Add a Duty Role

1. From the Actions menu, select Add. The Add Duty Role dialog is displayed.

Figure 2–4 Add Duty Role Dialog

Add Duty Role	
Name	<input type="text"/>
Description	<input type="text"/>
OK Cancel	

2. Enter a duty name and (optionally) a description for the new duty role and click OK.

Upon entering a name and moving to the Description field or when you click OK, RAAC performs a validation to prevent name duplication. If the name entered already exists, the following error message is displayed; A Duty with this name

already exists. Enter a unique name. If the duty name is unique, the new duty is created.

All newly created duties are reflected in the Policy Store, allowing them to be mapped to a role.

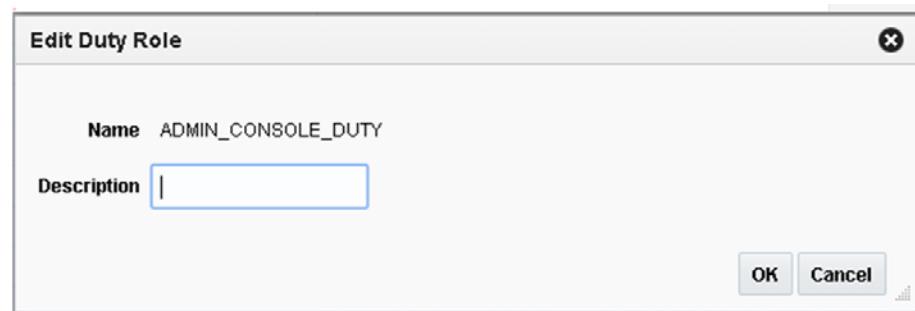
Edit

The Edit action is enabled when a duty role is selected. The Edit action is used to add or modify the description of an existing duty role.

Edit a Duty Role

1. Select the duty role you want to edit.
2. From the Actions menu, select Edit. The Edit Duty Role dialog is displayed.

Figure 2–5 Edit Duty Role Dialog



3. Add or modify the description of the duty role and click OK. Any updates to the description are updated to the mapping that the duty is mapped against.

Delete

The Delete action is enabled when you select a level that can be deleted from the database.

Only empty duty roles that do not contain any child duty or child privilege roles can be deleted. This is because a child privilege is associated with application code. Therefore, to delete the duty role, you must first remove all mappings between the duty and the child duties and privileges. If you attempt to delete a duty role without first removing the mapping, the following error message is displayed: You cannot delete duty because it has duties or privileges associated with it. Remove these mappings using Manage Roles Mapping task.

Delete a Duty Role

1. Select the duty role you want to delete.
2. From the Actions menu, select Delete. The Confirm dialog is displayed.

Figure 2–6 Delete Duty Role Confirmation Dialog



3. Click Yes to delete the selected duty role.

Export to Excel

The Export to Excel action is enabled whenever you have the Manage Duty Roles window open. This action allows you to export the Manage Duty Roles list to a Microsoft Excel spreadsheet.

Manage Roles Mapping

Figure 2–7 Manage Roles Mapping Screen

Name	Permissions	Description	Role Type
ALL_FUNCTION_ALL_DATA			Job
BUYER_JOB			Job
CORPORATE_INVENTORY_CONTROL_ANALYST_JOB			Job
FINANCIAL_ANALYST_JOB			Job
FINANCIAL_MANAGER_JOB			Job
INVENTORY_ANALYST_JOB			Job
INVENTORY_CONTROL_MANAGER_JOB			Job
INVENTORY_MANAGER_JOB			Job
RMS_APPLICATION_ADMINISTRATOR_JOB			Job
RMS_DATA_STEWARD_JOB			Job
SOURCING_ANALYST_JOB			Job
SUPPLY_CHAIN_ANALYST_JOB			Job
authenticated role			Application Default
anonymous role			Application Default

The Manage Roles Mapping task allows a user to add or remove duties or privileges associated with a job role.

When the user clicks on the Manage Roles Mapping link, a new tab is opened in the local area that displays a tree table with the already associated roles of the respective application (that is, the source application from which RAAC was launched). You can then choose to perform the following actions:

- Duplicate
- Delete
- Export to Excel
- Select and Add
- Remap

A quick search component is provided on the table toolbar to quickly look up any desired record.

Duplicate

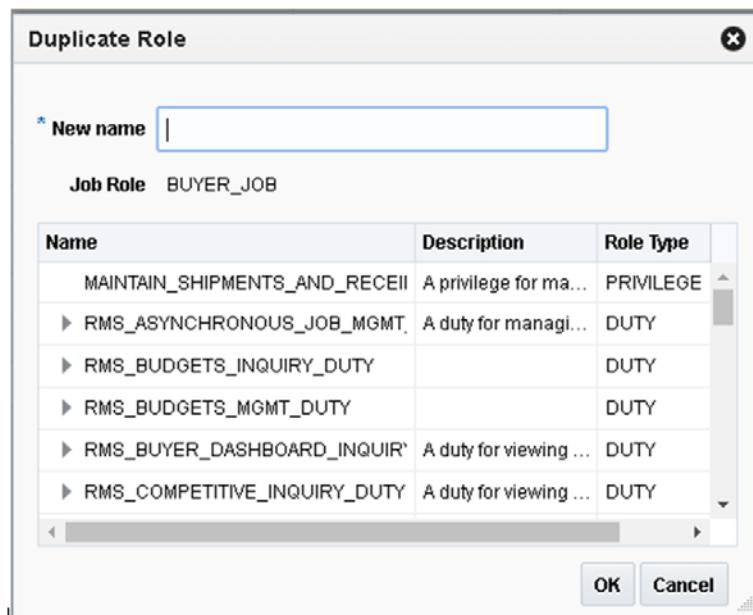
The Duplicate action allows you to copy and paste existing job roles to create a new role. For example:

Within a retailer enterprise security system there are two security groups called Allocator_xyz and Assistant_Allocator_xyz. By default, only the Allocator role is provided. The Assistant Allocator role is a trimmed down version of the Allocator role with fewer privileges. You can use the Duplicate action to copy the Allocator role and then edit the privileges of the new role.

Duplicate a Job Role

1. Select the job role you want to duplicate.
2. From the Actions menu, select Duplicate. The Duplicate Role dialog is displayed.

Figure 2–8 Duplicate Role Dialog



3. Enter a name for the duplicated role and click OK.

Upon clicking OK or tabbing out of the field, the New name is validated. The validation checks for a valid name in the enterprise security solution of the retailer. If it finds a match, then it allows the user to proceed. If the name is not valid, an error is displayed.

Delete

The Delete action is enabled when a duty or privilege role is selected.

Duty Role: When the user selects a duty and clicks Delete, the user is prompted with a warning message. Click 'Yes' and the selected duty role mapping will be removed from the corresponding Job role. All other Job roles mappings with that duty role will not be affected.

Privilege Role: When the user selects a privilege and clicks Delete, the user is prompted with a warning message. Click 'Yes' and the selected privilege role mapping will be removed from the corresponding duty role. All the Job roles having that duty role mapping will lose that privilege.

Note: The Delete action does not delete the role from the application policies, it only removes the mapping.

Export to Excel

The Export to Excel action is enabled whenever you have the Manage Roles Mapping window open. This action allows you to export the Manage Roles Mapping list to a Microsoft Excel spreadsheet.

Select and Add

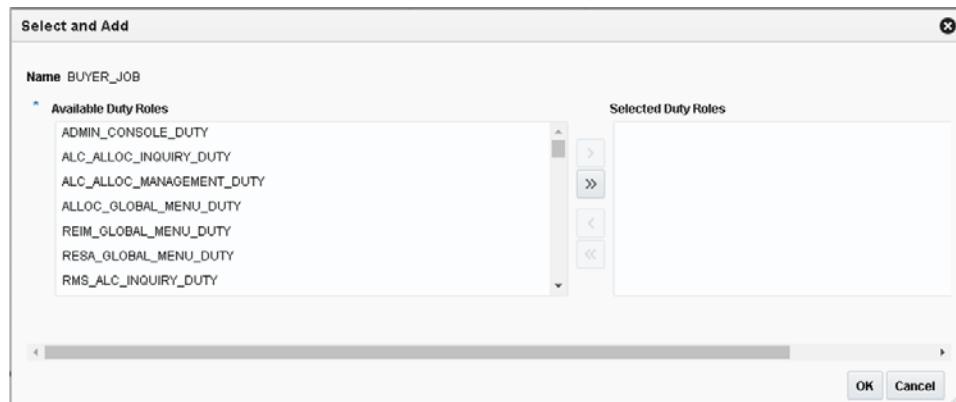
Select and Add is enabled when a job or a duty is selected. Select and Add allows you to do the following:

- Add duty roles to job roles
- Add duty and privilege roles to duty roles

Select and Add a Duty

1. Select the job role to which you want to add a duty role.
2. From the Actions menu, select Select and Add. The Select and Add dialog is displayed.

Figure 2–9 Select and Add Dialog



The Select and Add dialog has selected job or duty name displayed and a shuttle component for the user to select from all the available duties or privileges for the applications.

3. Select one or multiple duties and privileges and click OK to select and add them to the job role.

If you select a duty level then all the associated privileges with it are inherited to the job role. If a privilege is selected then only that privilege is added under the selected duty role.

Note: To add a new job role, the user should use the Duplicate feature.

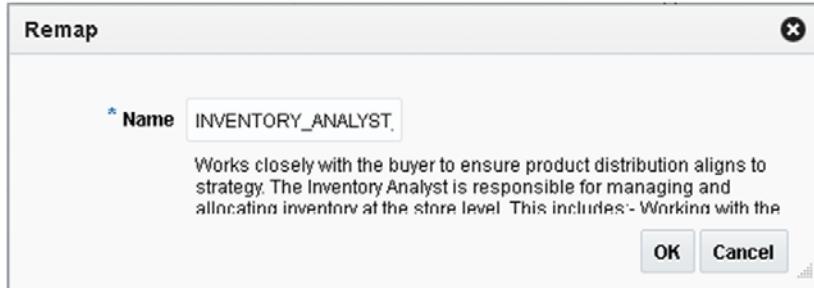
Remap

The Remap action is enabled when a job or duty is selected. The Remap action is used to move mapping from one role to another role. During this process, a new role is created and all the associated roles beneath the previous role are moved into the new role, leaving the old role as an orphan or with other roles associated with it.

Remap a Role

1. Select the role you want to remap.
2. From the Actions menu, select Remap. The Remap dialog is displayed.

Figure 2–10 Remap Dialog



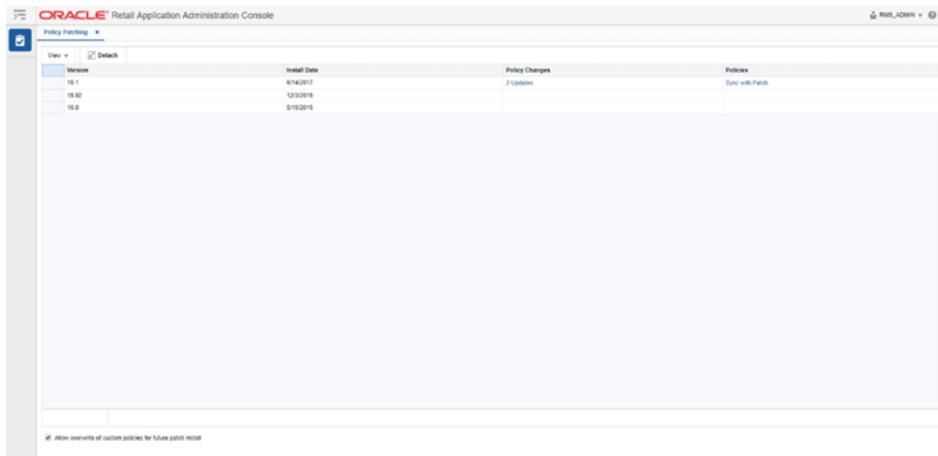
3. Enter a Name and (optionally) a Description for the remapped role.

Upon clicking OK, the New name is validated. The validation checks for a valid name in the enterprise security solution of the retailer. If it finds a match, then it allows the user to proceed. If the name is not valid, an error is displayed.

Job roles are handled in a different manner. When a job role is selected and remapped it will just change the current mapping to the new mapping without creating any new job role to be left as an orphan. This validation should be done once the user enters the new name and clicks OK. If there is no matching record found an error is displayed.

Manage Policy Patching

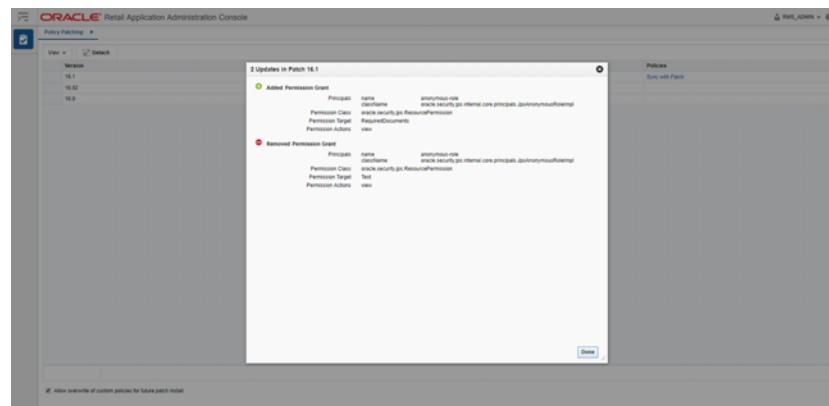
Figure 2–11 Manage Policy Patching Screen Patch History View



The Policy Patching screen displays two different views. The first view is called the Patch History view. The Patch History view displays the list of patches applied to the application. The latest patch provides links to view the changes introduced in a patch and to synchronize the changes introduced in the patch with the changes done by the retailer on the applications policies. The Patch History view also provides a check box to allow overwrite of the application policies for future patch installs. When this check box is unchecked, the application installer will not overwrite any changes done by the

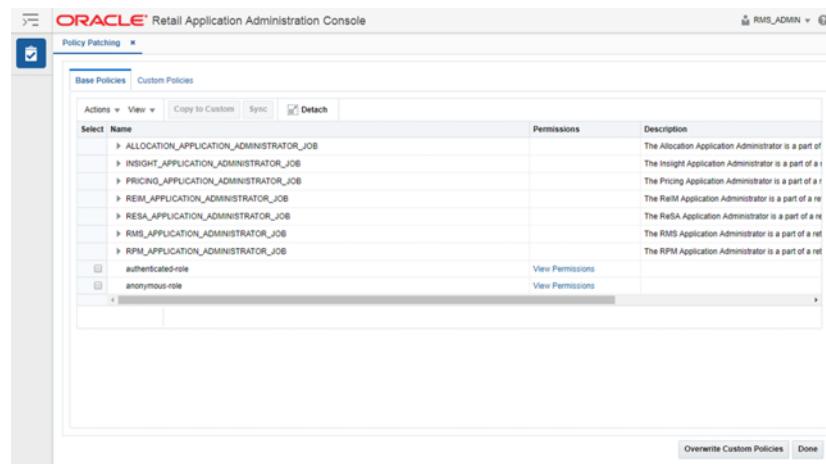
retailer on the application policies. The retailer should merge the changes introduced in the patch with the changes done on the application policies using the Sync with Patch view. When the checkbox is checked, the application installer will overwrite the application policies with the ones in the patch. The installer backs up the custom policies before overwriting application policies. The backups can be managed using the Policy Backups screen.

Figure 2–12 Policy Changes



The Policy Changes column displays a link, which shows the number of updates made to the application policies in the current patch. Clicking on the link opens up a popup, which lists all the updates done to the policies. The user can view the updates and go to the Sync With Patch View to merge the changes to the current application policy.

Figure 2–13 Manage Policy Patching Screen Sync With Patch View



The Policy Patching Screen Sync provides a way for the retailer to synchronize the changes introduced in a patch with the changes done on the application policy setup. The Sync with Patch view displays two different tabs. The first tab called Base Policies displays the application policies that came in the patched application. The second tab called Custom Policies displays the application policies that the retailer has changed as per its business needs. The retailer can merge the changes introduced in the patch with the custom policy change using this view. In order to find what changes have been introduced in a patch, the retailer should go back to the policy history view and look at the policy changes using the Updates link.

The Sync with Patch view in the Policy Patching screen provides the following actions:

- Copy to Custom
- Sync
- View Permissions
- Overwrite Custom Policies
- Done
- Refresh

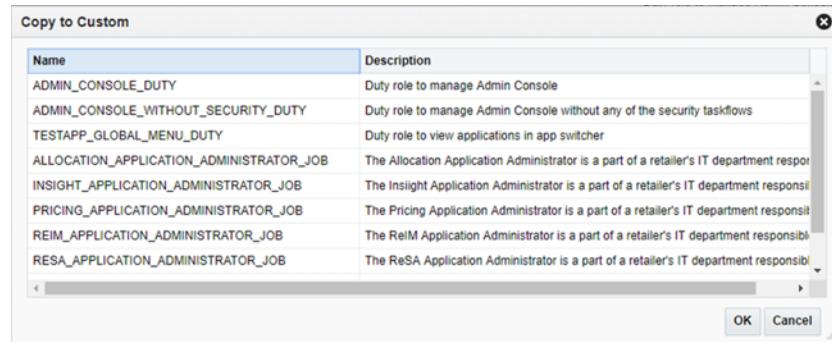
Copy to Custom

The Copy to Custom action is enabled for the privileges or duties, which are newly introduced in patch and are not available in the custom policies. The Copy to Custom action copies the privilege or duty to the selected duty or role in the custom application policy setup.

Copy Privilege/Duty to Duty/Role

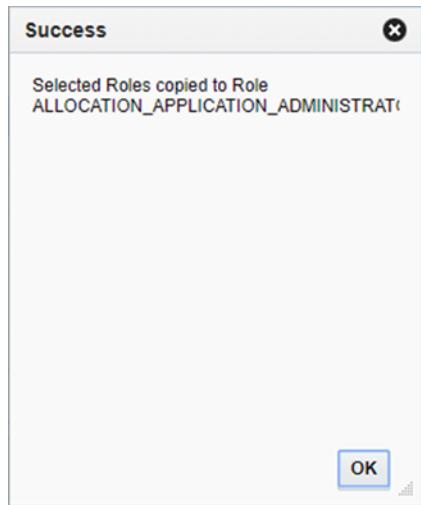
1. Select the privilege/duty in the base policies.
2. If the privilege/duty is newly introduced in a patch and does not exist in the custom policies, the Copy to Custom action will be enabled.
3. Click on Copy to Custom action to display the Copy to Custom Dialog.

Figure 2–14 Copy to Custom Dialog



4. Select the duty/role where the privilege/duty should be copied.
5. Click OK to copy the privilege/duty to selected duty/role.
6. Successful copy will display the success dialog.

Figure 2–15 Copy to Custom Success Dialog



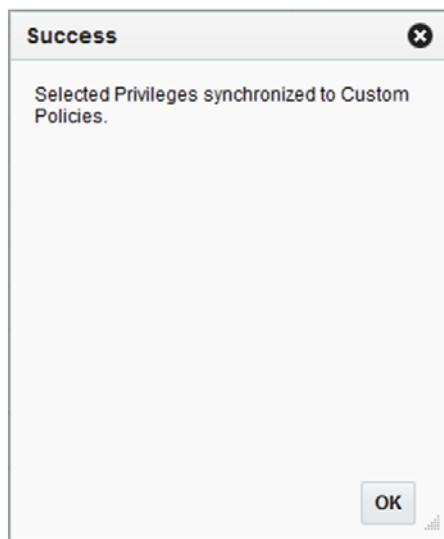
Sync

The Sync action is enabled when a privilege is selected and the privilege exists in the custom application policies. The Sync action synchronizes the permissions in the selected privilege with the same privilege in the custom application policy setup.

Synchronize Permissions in a Privilege

1. Select privilege in base policies.
2. If the privilege exists in the custom policies then the Sync action will be enabled.
3. Click on Sync to synchronize the permissions with the same privilege in the custom policy setup.
4. Successful sync will display the success dialog.

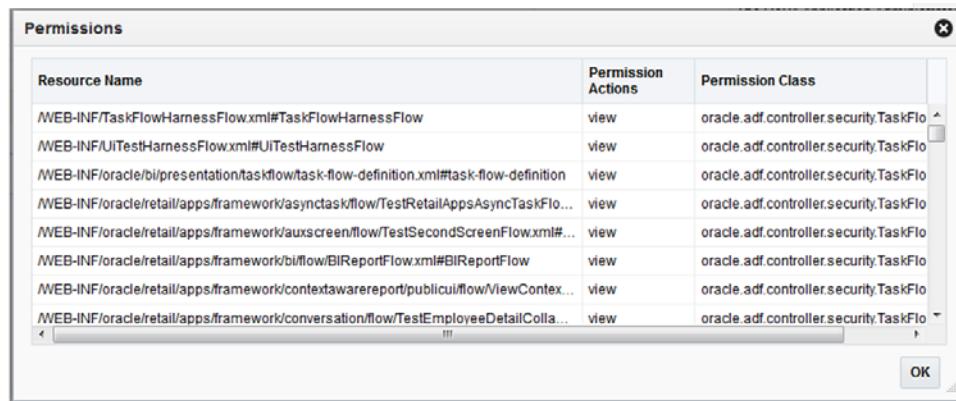
Figure 2–16 Sync Success Dialog



View Permissions

The View Permissions link is used to display the permissions associated with a privilege. This link opens up a popup that displays the Resource Name, Permission Actions and Permission Class for permissions.

Figure 2–17 View Permissions Dialog



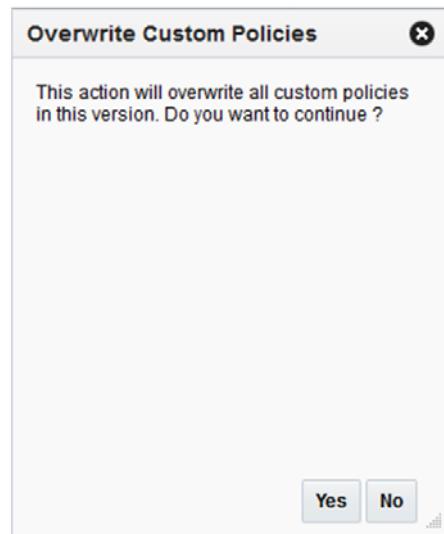
The screenshot shows a modal dialog titled "Permissions". It contains a table with three columns: "Resource Name", "Permission Actions", and "Permission Class". The "Resource Name" column lists various XML file paths, such as "/WEB-INF/TaskFlowHarnessFlow.xml#TaskFlowHarnessFlow" and "/WEB-INF/oracle/bi/presentation/taskflow/task-flow-definition.xml#task-flow-definition". The "Permission Actions" column shows "view" for all entries. The "Permission Class" column shows "oracle.adf.controller.security.TaskFlo" repeated multiple times. At the bottom right of the dialog is an "OK" button.

Resource Name	Permission Actions	Permission Class
/WEB-INF/TaskFlowHarnessFlow.xml#TaskFlowHarnessFlow	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/UITestHarnessFlow.xml#UITestHarnessFlow	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/bi/presentation/taskflow/task-flow-definition.xml#task-flow-definition	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/retail/apps/framework/asynctask/flow/TestRetailAppsAsyncTaskFlo...	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/retail/apps/framework/auxscreen/flow/TestSecondScreenFlow.xml#...	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/retail/apps/framework/bilflow/BIReportFlow.xml#BIReportFlow	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/retail/apps/framework/contextawarereport/publicflow/ViewContex...	view	oracle.adf.controller.security.TaskFlo
/WEB-INF/oracle/retail/apps/framework/conversation/flow/TestEmployeeDetailColla...	view	oracle.adf.controller.security.TaskFlo
!!!		

Overwrite Custom Policies

The Overwrite Custom Policies action overwrites the current application policy setup with the application policies available in the patched application. The action will cause the loss of any changes done by the retailer on the application policies. The action displays a warning popup before overwriting application policies with the patched policies. The action also backs up the application policies before overwriting and can be retrieved using the Backups screen.

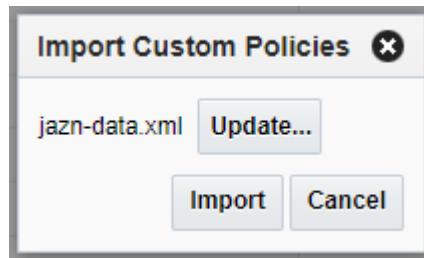
Figure 2–18 Overwrite Custom Policies Dialog



Import Custom Policies

The Import Custom Policies action overwrites the current application policy setup with the application policies available in a jazn-data.xml file. The action opens up a dialog, which provides an option to choose a jazn-data.xml file from the local machine. The user can select a jazn-data.xml file and use it to overwrite the current application policy. This action is useful when migrating policies from one environment to another. The user can backup and download the policies from one environment using the Policy Backup screen and import them into another environment using the Import Custom Policies action.

Figure 2–19 Import Custom Policies Dialog



Done

The Done action takes the user back to the Patch History view of the Policy Patching screen.

Refresh

The Refresh action is only available in the Custom Policies tab of the Sync with Patch view of the Policy Patching screen. The action is used to refresh the custom application policies. The action can be used to verify the changes in the custom policies after a successful Sync or Copy to Custom action from the base policies.

Manage Backups

Figure 2–20 Manage Backups

Name	Description	Stripe Type	Created By	Creation Date
USER_BACKUP_RetailAppFrameworkTest	Backup of current policies	User-generated backup Policy Stripe	Retail_Admin	7/27/17 8:54 AM
SYS_BACKUP_RetailAppFrameworkTest	Auto-generated backup prior to overwriting Custom Policies with Base Policies	System-generated backup Policy Stripe	Retail_Admin	7/27/17 10:45 AM

The Manage Backups screen is used to maintain the application policy backups. The backups can be used to restore the application policies back to the original state if something goes wrong with the application policy setup. The backups can be created by the following actions

- Installer creates a backup before overwriting the application policies during a patch install. The installer created backup is prefixed with the name SYS_BACKUP. The installer overwrites the application policies and creates a backup only if the 'Allow Overwrite of Custom Policies' flag is checked in the Manage Policy Patching screen.
- A user can create a backup using the Create action on the Manage Backups screen. The user created backup is prefixed with the name USER_BACKUP.
- A user can initiate a backup using the 'Overwrite Custom Policies' action on the Manage Policy Patching screen. The Overwrite Custom Policies action creates a backup before overwriting the custom policies. The backup created by the Overwrite Custom Policies action is prefixed with the name SYS_BACKUP.

The Manage Backups screen provides the following actions:

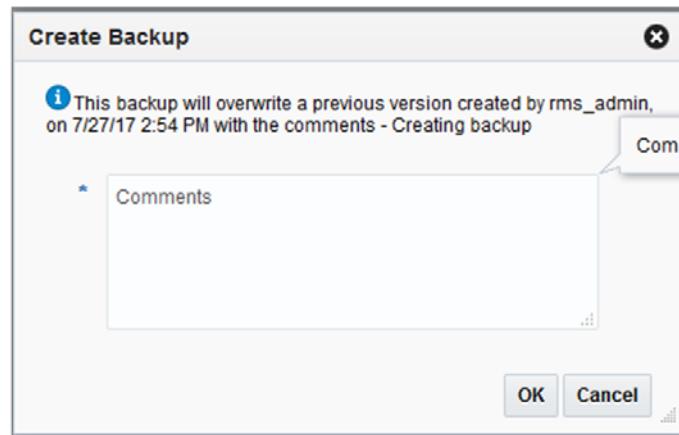
- Create
- Delete
- Download
- Restore
- Refresh

Create

The Create action is used to create a backup of the current application policies. The backup stripe name will be prefixed with the text USER_BACKUP. The create action opens up a popup where the user can enter the comments for the backup.

The RAAC application allows only one user initiated backup. If a backup was already created by an administrator for the current application policies, it will be overwritten.

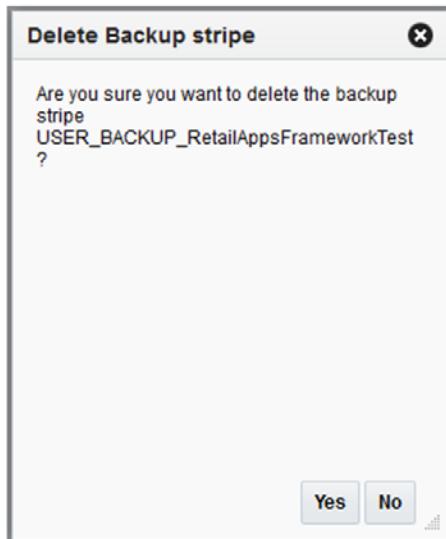
Figure 2–21 Create Backup Dialog



Delete

The delete action is used to delete the selected backup stripe. A confirmation dialog is displayed before deleting the backup.

Figure 2–22 Delete Backup Confirmation Dialog



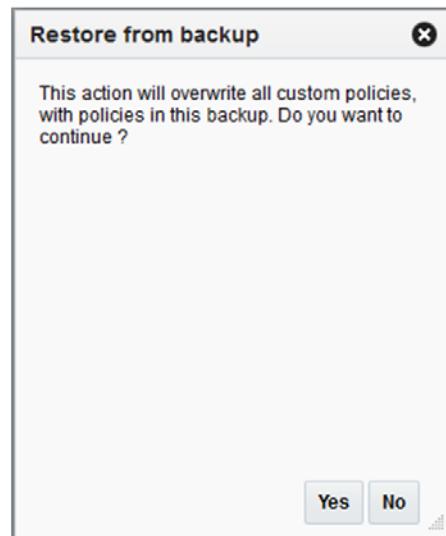
Download

The download action is used to download the selected backup stripe in an xml format. It will generate a file called backup.xml which can be stored on the device where the browser is running. The xml file can be opened in JDeveloper to look at the changes in the backup.

Restore

The Restore action will overwrite the current application policy setup with the application policies available in the backup. A confirmation dialog is displayed to the user before restoring.

Figure 2–23 Restore from Backup Dialog



Refresh

The Refresh action will refresh the backup table.

3

Data Security/Filtering

Data Security/Filtering Implementation

If Data Level Security is enabled in Merchandising, then for the users to have access to the data, the below must be setup through the Data Upload Utility available in Merchandising. This is used both in the core Merchandising solution, as well as Allocation, Invoice Match, Pricing, and Sales Audit.

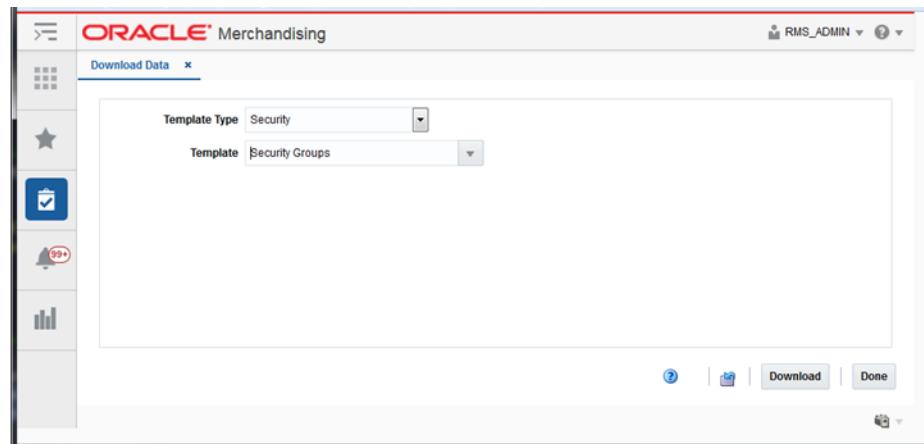
- Security Groups
- Security User and Security User Role
- Security User and Security Group mapping information
- Merchandise Hierarchy LOV filtering access information
- Purchase Order Approval Limits

Setup Security Groups

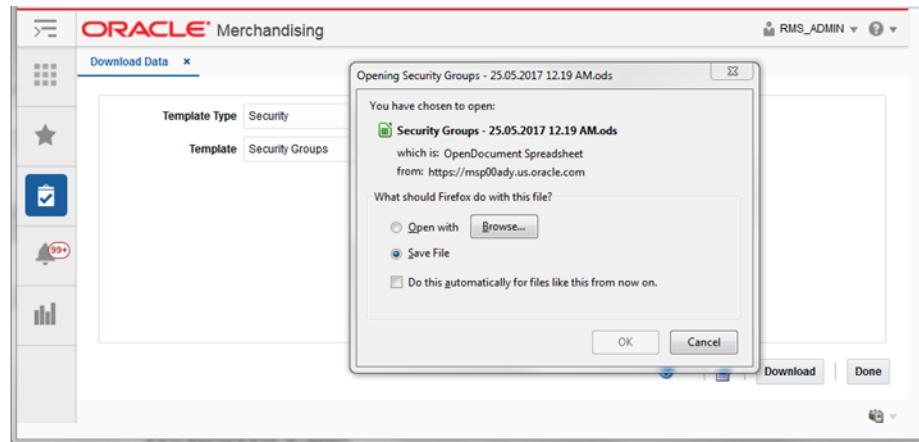
Perform the following procedure to define a Security Group in the system.

1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Security Groups'.

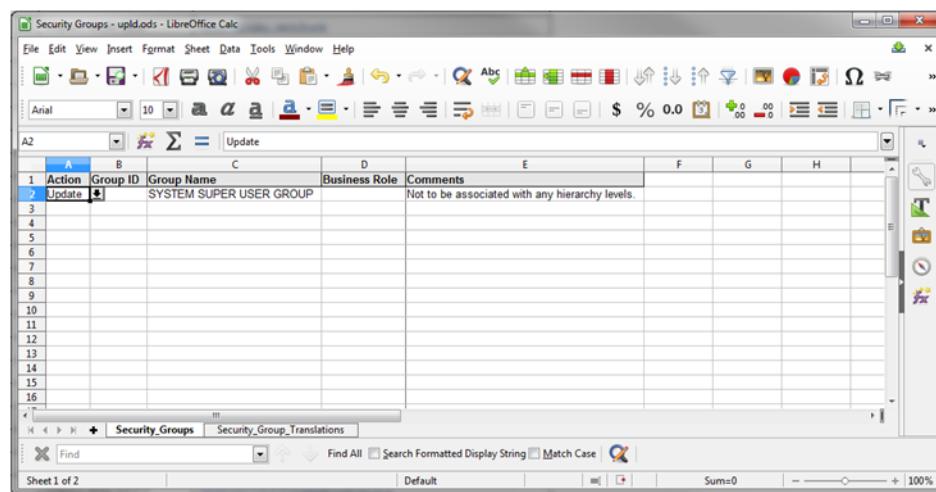
Figure 3–1 Download Security Groups Template Spreadsheet



3. Click the **Download** button.
4. Save File to a local directory location when prompted.

Figure 3–2 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 3–3 Open File

7. Save As <file name>.

Figure 3–4 Save as <File Name>

Action	Group ID	Group Name	Business Role	Comments
Update	1001	SYSTEM SUPER USER GROUP		Not to be associated with any hierarchy levels.
	3			
	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	13			
	14			
	15			
	16			

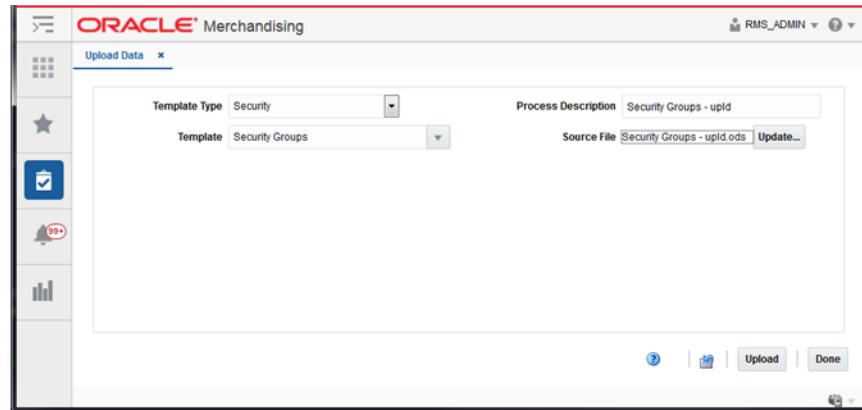
8. In the Security_Groups tab, enter/select the following:
 - Action: 'Create'
 - Group ID: <Group ID>
 - Group Name: <Group Name>
 - Business Role: <role> (optional)
 - Comments: <comments> (optional)
9. In the Security_Groups_Translations tab, enter the translated Security Group descriptions (optional).

Figure 3–5 Enter Security Groups information

Action	Group ID	Group Name	Business Role	Comments
Update	1001	SYSTEM SUPER USER GROUP		Not to be associated with any hierarchy levels.
Create	1001	TEST USER GROUP		Test User Group
	4			
	5			
	6			
	7			
	8			
	9			
	10			
	11			
	12			
	13			
	14			
	15			
	16			

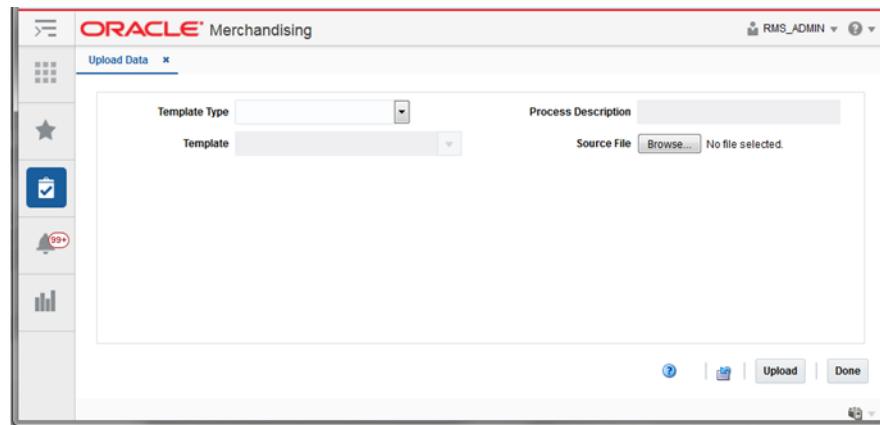
10. Save and Close the file.
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Security Groups'
 - Enter new Process Description or retain as is
 - Browse and select the Source file that was created in Step 10

Figure 3–6 Upload Security Groups Information



13. Click the **Upload** button.

Figure 3–7 Upload Security Group Information Complete



14. Click the **Done** button.
15. View the newly created Security Group by downloading the Security Groups spreadsheet (Steps 1 - 6).

Figure 3–8 View newly created Security Group

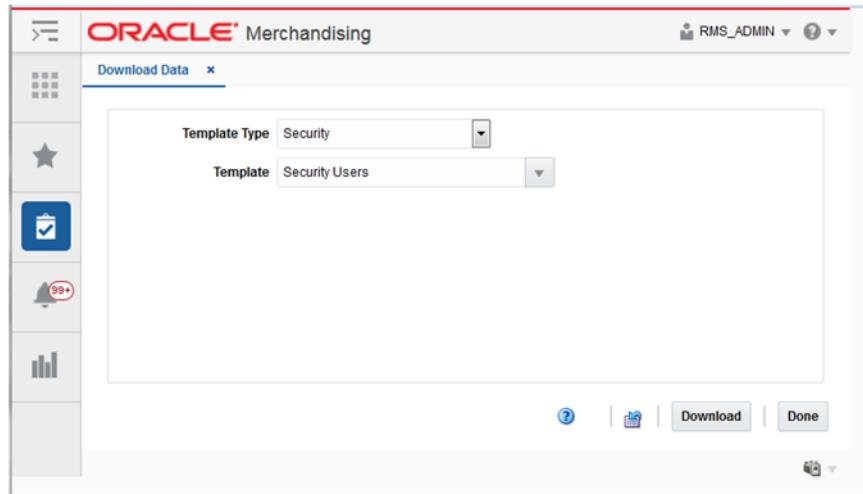
Action	Group ID	Group Name	Business Role	Comments	F	G	H
2. Update	1	SYSTEM SUPER USER GROUP		Not to be associated with any hierarchy levels.			
3. Update	1001	QIM TEST USER GROUP		QIM Test User Group			
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							

Note: The system generated Group ID. This Group ID should be mapped to the Security Users.

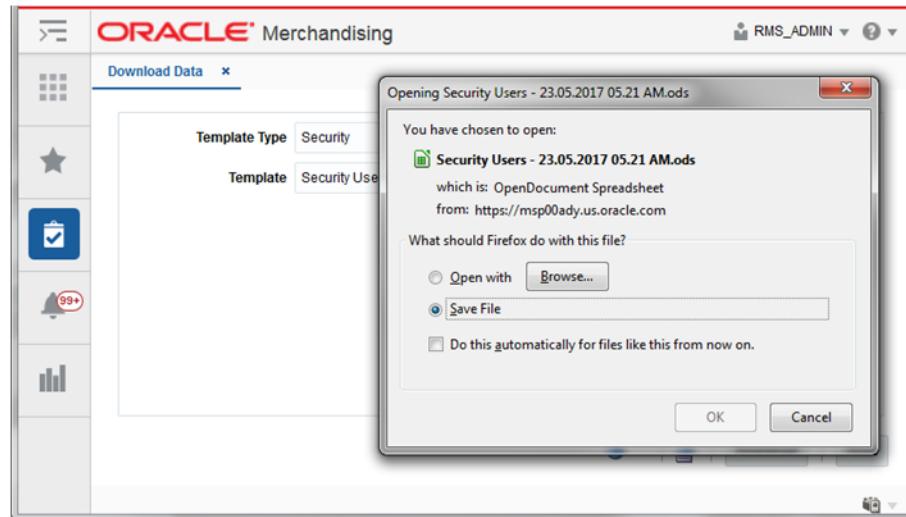
Setup Security User and Security User Role

The Application (LDAP) User ID used to login to the RMS application must be defined as a Security User.

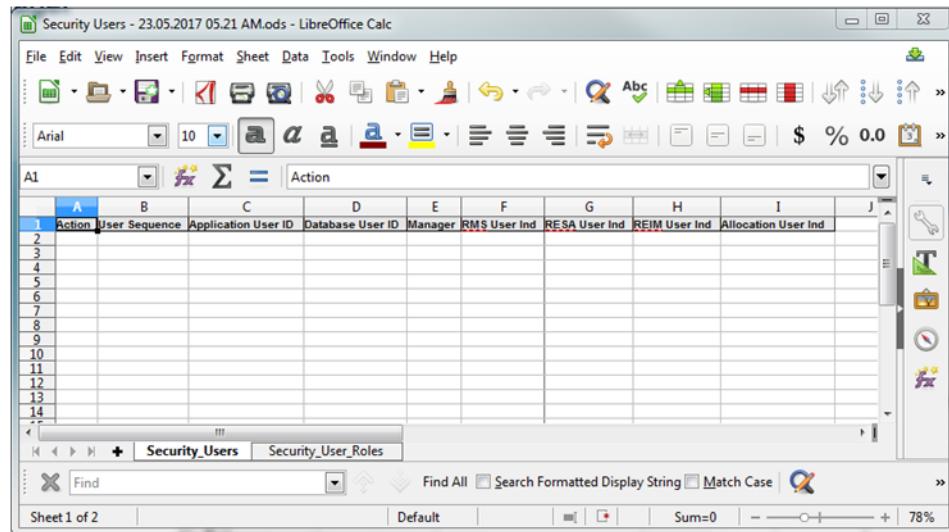
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Security Users'.

Figure 3–9 Download Security Users template spreadsheet

3. Click the **Download** button.
4. Save File to local directory location when prompted.

Figure 3–10 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 3–11 Open File

7. Save As <file name>.

Figure 3–12 Save as <File Name>

The screenshot shows a LibreOffice Calc spreadsheet titled "Security Users - uplid.ods - LibreOffice Calc". The menu bar includes File, Edit, View, Insert, Format, Sheet, Data, Tools, Window, and Help. The toolbar contains various icons for file operations, cell styling, and data manipulation. The formula bar shows "Action". The current cell is A1. The table has columns labeled "Action", "User Sequence", "Application User ID", "Database User ID", "Manager", "RMS User Ind", "RESA User Ind", "REIM User Ind", and "Allocation User Ind". Rows 1 through 16 are present, with rows 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, and 16 being empty. The bottom of the screen shows the status bar with "Sheet 1 of 2", "Default", "Sum:0", and a zoom level of 100%.

- 8.** In the Security_Users tab, enter/select the following:

- Action: 'Create'
 - User Sequence: <number>
 - Application User ID: <Application User ID>
 - RMS User Ind: Yes
 - ReSA User Ind: Yes/No
 - ReIM User Ind: Yes/No
 - Allocation User Ind: Yes/No

Figure 3–13 Security Users Information

The screenshot shows a LibreOffice Calc spreadsheet titled "Security Users - upld.ods - LibreOffice Calc". The menu bar includes File, Edit, View, Insert, Format, Sheet, Data, Tools, Window, Help. The toolbar has various icons for file operations, text styles, and data manipulation. The spreadsheet has a header row with columns A through L. Row 1 contains column headers: Action, User Sequence, Application User ID, Database User ID, Manager, RMS User Ind, RESA User, PREIM User ID, Allocation L, and Allocation R. Row 2 contains data: Create, 15001, OIM TEST, (empty), Yes, No, No, No, (empty). Rows 3 through 12 are empty. The bottom navigation bar shows tabs for Security_Users and Security_User_Roles, along with search and filter tools.

- 9.** In the Security_User_Roles tab, enter/select the following:

Note: Proceed to set up Security User Role, only if Role Privileges have been setup.

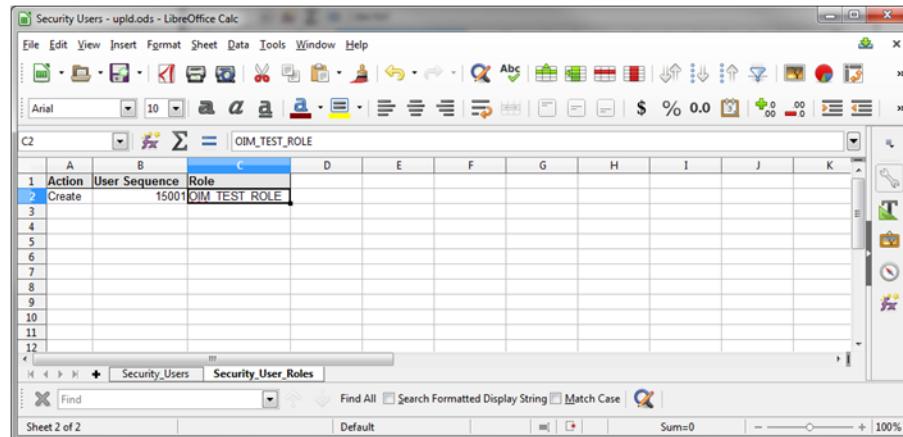
- Action: 'Create'

- User Sequence: <number>

Note: This must be the User Sequence provided in the Security_Users tab.

- Role: <Role>

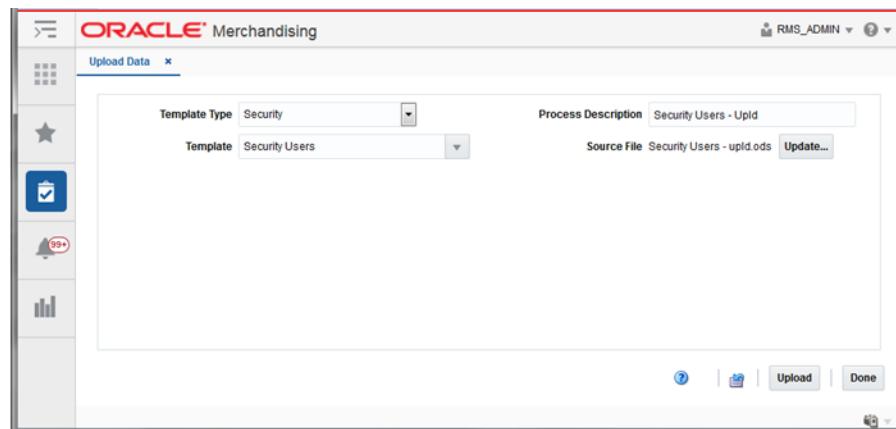
Figure 3–14 Security User Roles Information



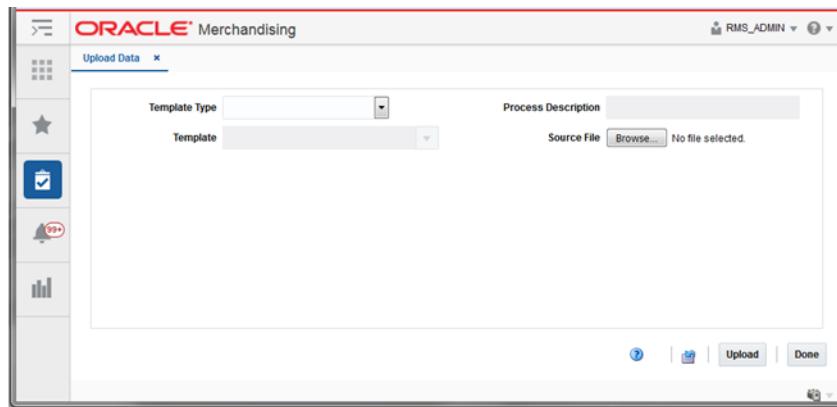
A	B	C
1 Action	User Sequence	Role
2 Create	15001	OIM TEST ROLE
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

10. Save and Close the file.
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Security Users'
 - Enter Process Description or retain as is
 - Browse and select the Source file that was created in Step 10

Figure 3–15 Upload Security Users Information



13. Click the **Upload** button.

Figure 3–16 Upload Security Users Information Complete

14. Click the **Done** button.
15. View the newly created Security User and Security User Role by downloading the Security Users spreadsheet (Steps 1 - 6).

Figure 3–17 View newly created Security User and Security Role Mapping information

Action	User Sequence	Application	Database User	Manager	RMS User Ind	RESA User	PREIM User Ind	Allocation User Ind
Update	15001	OIM TEST			Yes	No	No	No
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

Figure 3–18 View newly created Security User Role mapping information

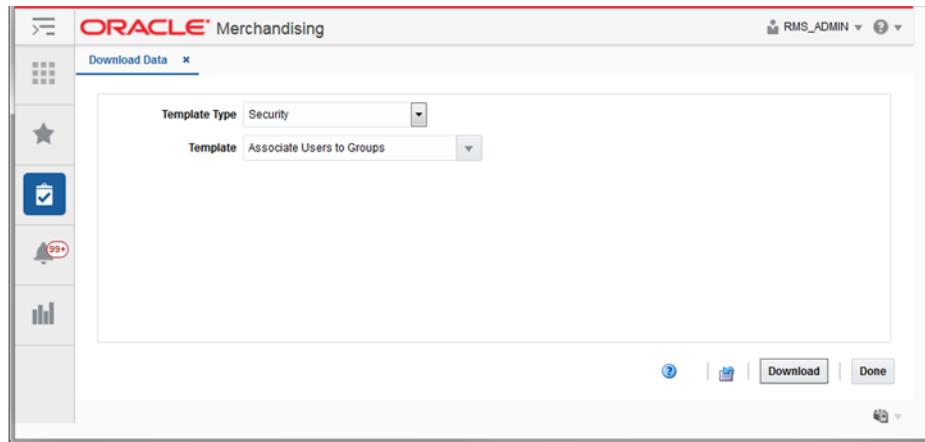
Note the system generated User Sequence. This Security User (User Sequence) will be mapped to the Security Group.

Map Security User to Security Group

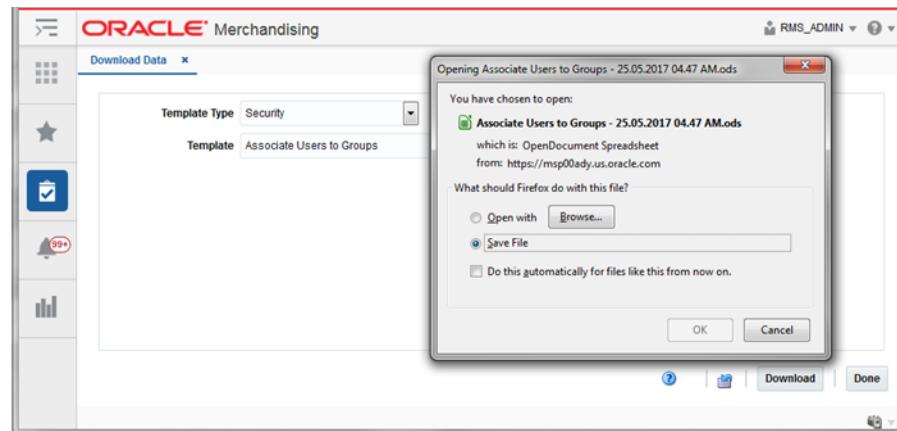
The security user must be assigned to a security group. This is achieved by associating the User Sequence assigned to the Application User ID with a Security User Group.

1. Navigate to Foundation Data > Data Loading > Download.
 2. In the Download Data screen, select Template Type as 'Security' and Template as 'Associate Users to Groups'.

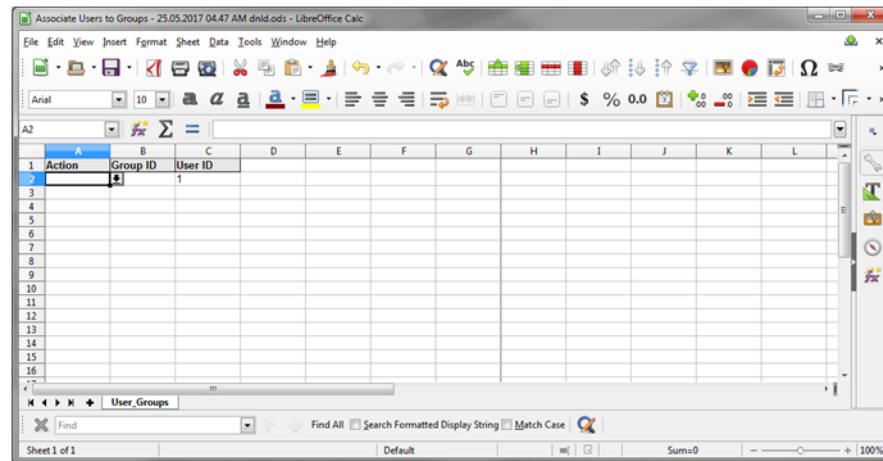
Figure 3–19 Download Associate User to Groups Template Spreadsheet



3. Click the **Download** button.
 4. Save the file to a local directory location when prompted.

Figure 3–20 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 3–21 Open File

7. Save As <file name>.

Figure 3–22 Save as <File Name>

A	B	C	D	E	F	G	H	I	J	K	L
1	Action	Group ID	User ID								
2	Create	1001	15001								
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											

8. In the User_Groups tab, enter/select the following:

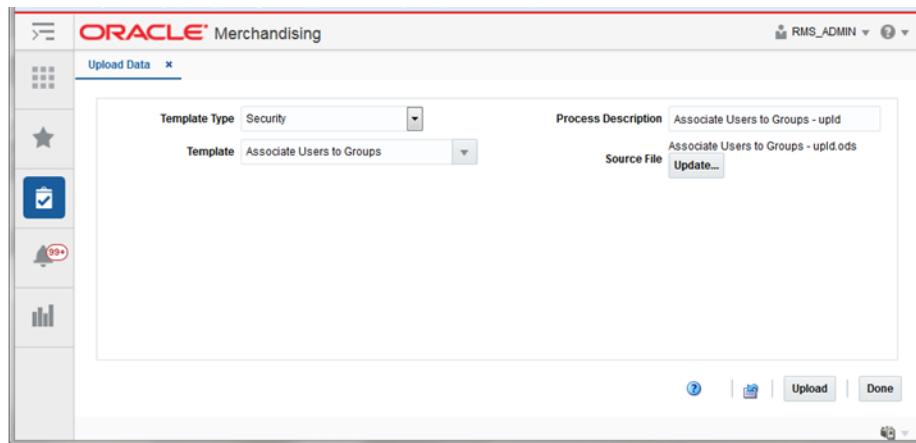
- Action: 'Create'
- Group ID: <Group ID>
- User ID: <User ID>

Figure 3–23 Enter User Groups information

A	B	C	D	E	F	G	H	I	J	K	L
1	Action	Group ID	User ID								
2	Create	1001	15001								
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											

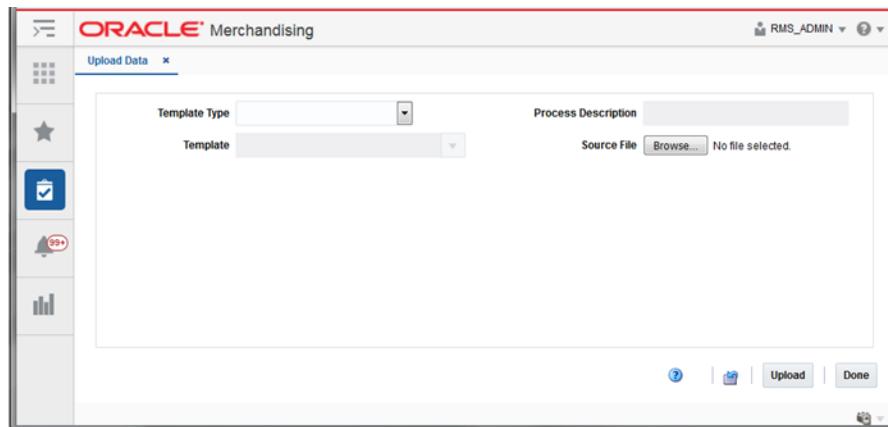
9. Save and Close the file.
10. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
11. In the Upload Data screen, select:
- Template Type as 'Security'
 - Template as 'Associate Users to Groups'
 - Enter new Process Description or retain as is
 - Browse and select the Source file that was created in Step 9

Figure 3–24 Upload User Groups Information



12. Click the **Upload** button.

Figure 3–25 Upload User Groups Information Complete



13. Click the **Done** button.
14. View the newly created User Groups mapping by downloading the User Groups spreadsheet (Steps 1 - 6).

Figure 3–26 View Newly Created User Group Association

Action	Group ID	User ID
	1001	15001

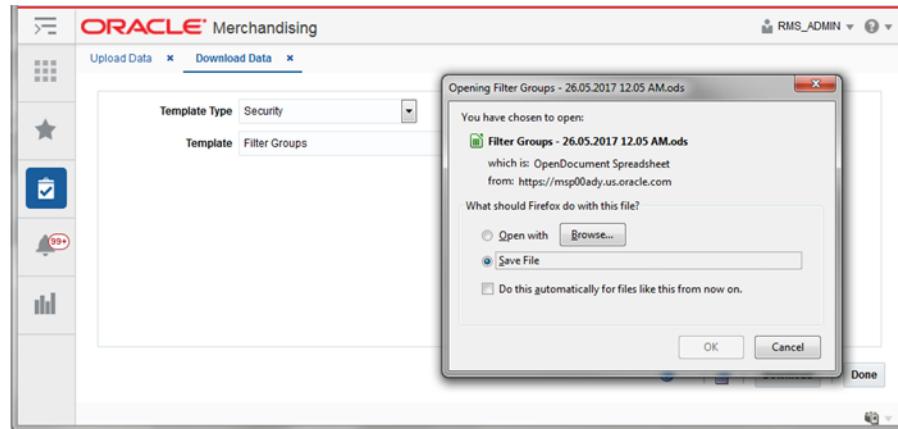
Assign Groups to Hierarchies

The security group can only access the merchandise hierarchies and organization hierarchies assigned to the user through Filter Groups. If a security group is not assigned to any Filter Group then the users in the group are considered 'super users' and will have access to all merchandise hierarchies or all organization hierarchies respectively.

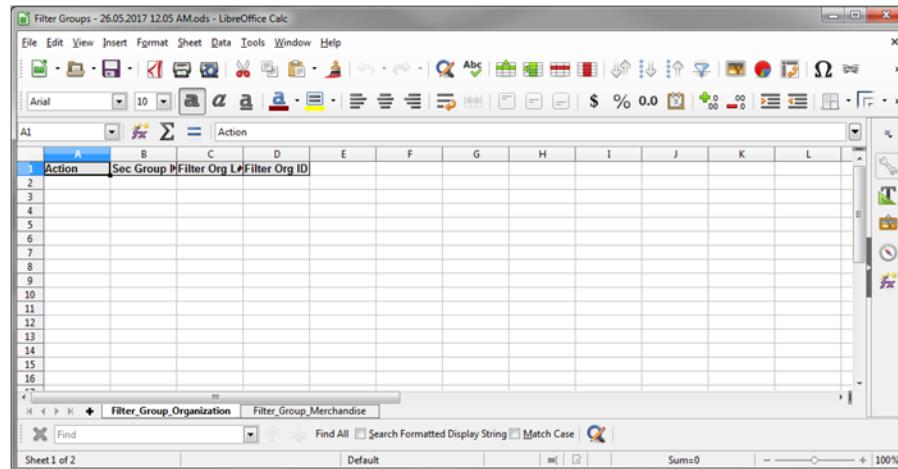
1. Navigate to Foundation Data > Data Loading > Download.
2. In the Download Data screen, select Template Type as 'Security' and Template as 'Filter Groups'.

Figure 3–27 Download Filter Groups Template Spreadsheet

3. Click the **Download** button.
4. Save File to local directory location when prompted.

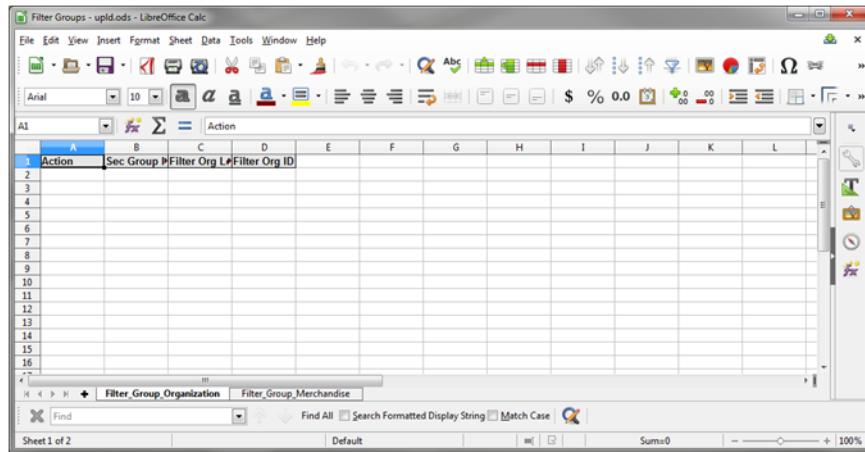
Figure 3–28 Save File

5. Click the **Done** button.
6. Open the downloaded file.

Figure 3–29 Open File

7. Save As <file name>.

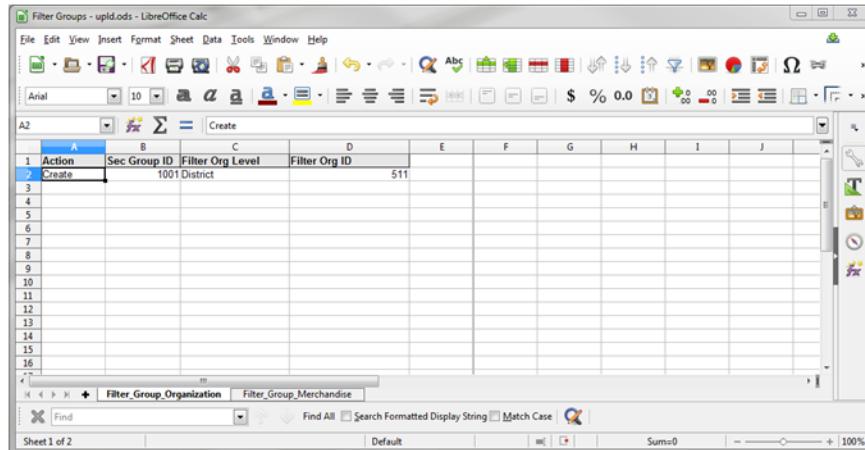
Figure 3–30 Save as <File Name>



8. In the Filter_Group_Organization tab, enter/select the following:

 - Action: 'Create'
 - Sec Group ID: <User Security group ID>
 - Filter Org Level: <Organization hierarchy level>
 - Filter Org ID: <ID of the Organization hierarchy level>

Figure 3–31 Enter Filter Group Organization information



9. In the Filter_Group_Merchandise tab, enter/select the following:

 - Action: 'Create'
 - Sec Group ID: <User Security group ID>
 - Filter Merch Level: <Organization hierarchy level>
 - Filter Merch ID: <ID of the Merchandise hierarchy level>
 - Filter Merch ID Class: <Class ID of the Merchandise hierarchy level> (optional depending on the selected Filter Merch Level)

- Filter Merch ID Subclass: <Subclass ID of the Merchandise hierarchy level> (optional depending on the selected Filter Merch Level)

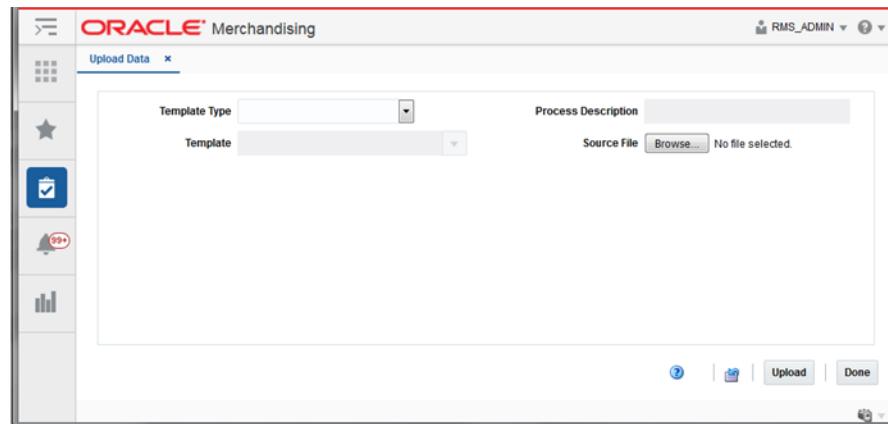
Figure 3–32 Enter Filter Group Merchandise information

Action	Sec Group ID	Filter Merch Level	Filter Merch ID	Filter Merch ID Class	Filter Merch ID Subclass	G	H	I	J
Create	1001 Class		511						
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									

10. Save and close the file.
11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Filter Groups'
 - Enter new Process Description or retain as is
 - Browse and select the Source file that was created in Step 10

Figure 3–33 Upload Filter Groups Information

13. Click the **Upload** button.

Figure 3–34 Upload Filter Groups Information Complete

14. Click the **Done** button.
15. View the newly created Filter Groups mapping by downloading the Filter Groups spreadsheet (Steps 1 - 6).

Figure 3–35 View Newly Created Filter Groups

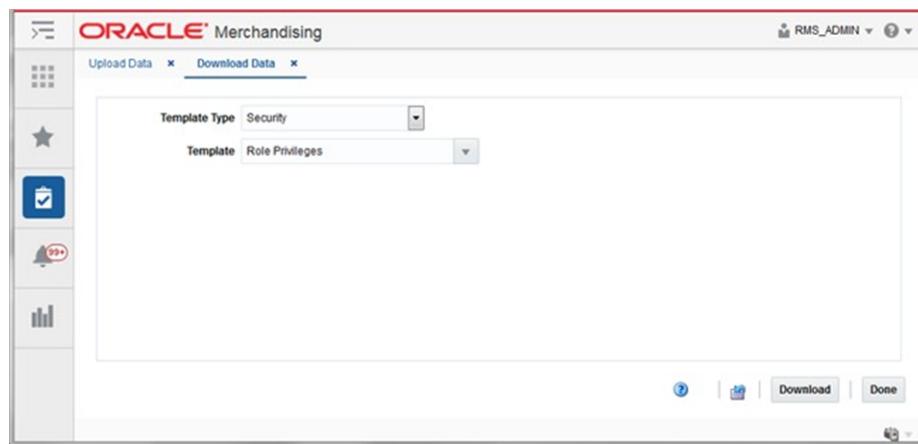
Figure 3–36 Newly Created Filter Groups

Action	Sec Group	Filter Merch	Filter Merch	Filter Merch	ID Subclass
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

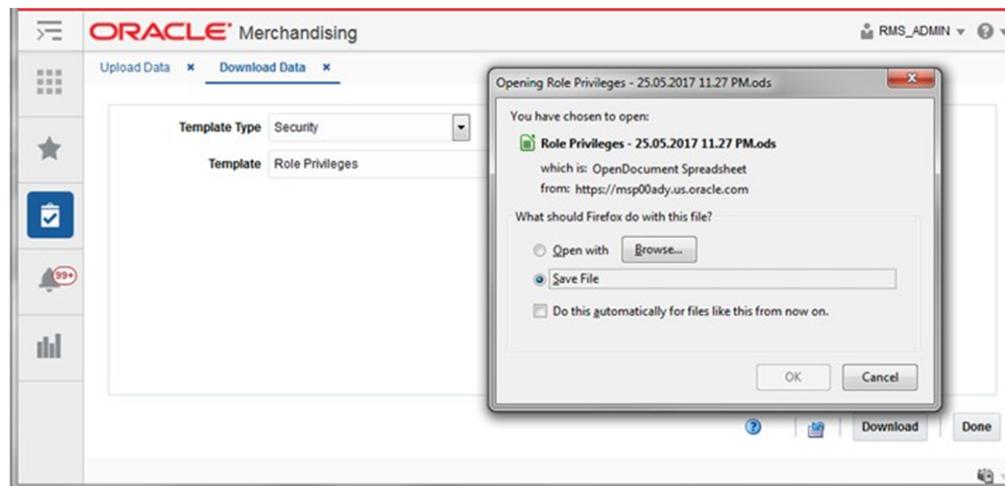
Setup Purchase Order Approval Limits

The setup of role privileges can be used to manage the size of a purchase order that a user can approve. The basis of this is either cost or retail based on the system option configuration. This setup is not required if user roles will not have an approval limit.

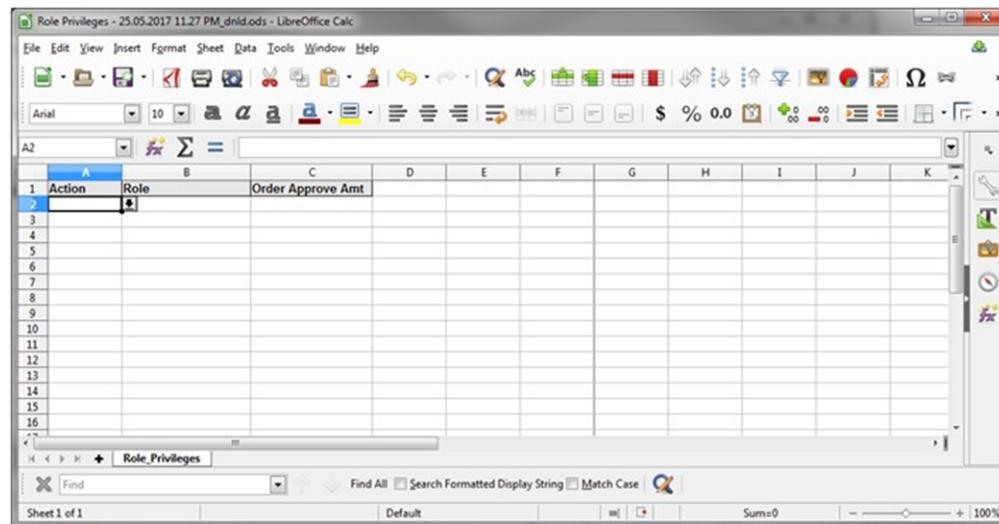
1. Log into the RMS Application.
2. Navigate to Foundation Data > Data Loading > Download.
3. In the Download Data screen, select:
 - Template Type as 'Security'
 - Template as 'Role Privileges'

Figure 3–37 Download Security Privileges Template Spreadsheet

4. Click the **Download** button.
5. Save File to the local directory location when prompted.

Figure 3–38 Save File

6. Click the **Done** button.
7. Open the downloaded file.

Figure 3–39 Open File

8. Save As <file name>.

Figure 3–40 Save as <File Name>

Role Privileges - upld.ods - LibreOffice Calc

Action	Role	Order Approve Amt
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

9. In the Role_Privileges tab, enter/select the following:

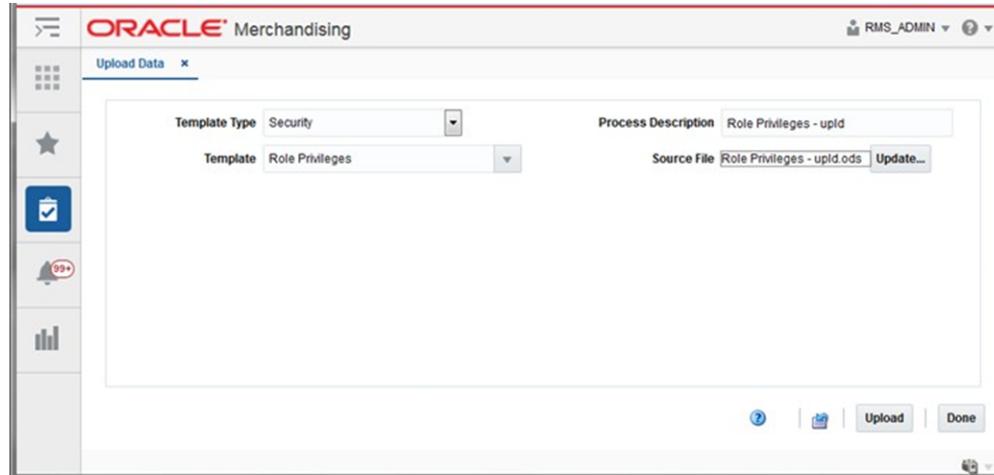
 - Action: 'Create'
 - Role: <Role>
 - Order Approve Amt: < Upper limit that the role will be able to approve on an order>

Figure 3–41 Enter Role Privileges Information

10. Save and Close the file.
 11. In the RMS Application, navigate to Foundation Data > Data Loading > Upload.
 12. In the Upload Data screen, select:
 - Template Type as 'Security'
 - Template as 'Role Privileges'

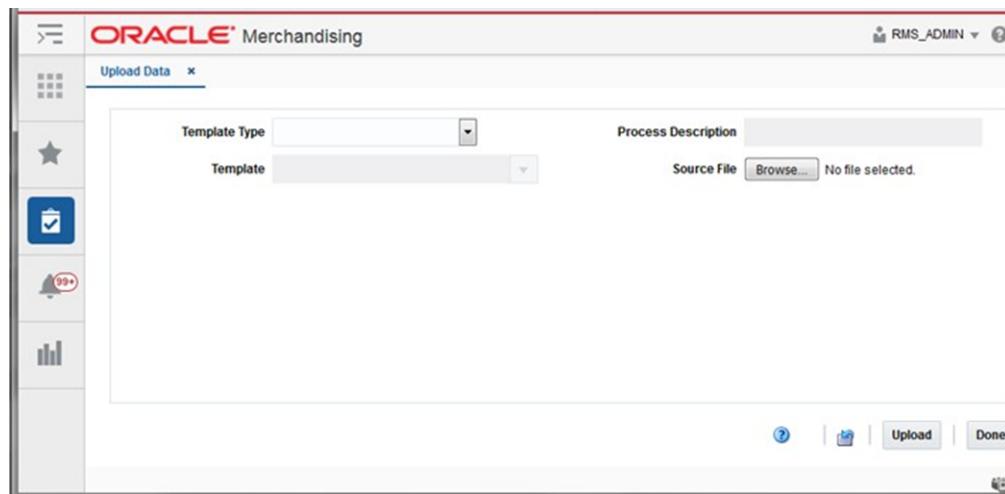
- Enter new Process Description or retain as is
- Browse and select the Source file that was created in Step 10

Figure 3–42 Upload Role Privileges Information



13. Click the **Upload** button.

Figure 3–43 Upload Role Privileges Information Complete



14. Click the **Done** button.

15. View the newly created Role Privileges by downloading the Role privileges spreadsheet (Steps 2 - 7).

Figure 3–44 View Newly Created Role Privilege

The screenshot shows a LibreOffice Calc spreadsheet window titled "Role Privileges - 25.05.2017 11:47 PM_dnid.ods - LibreOffice Calc". The spreadsheet has a single row of data:

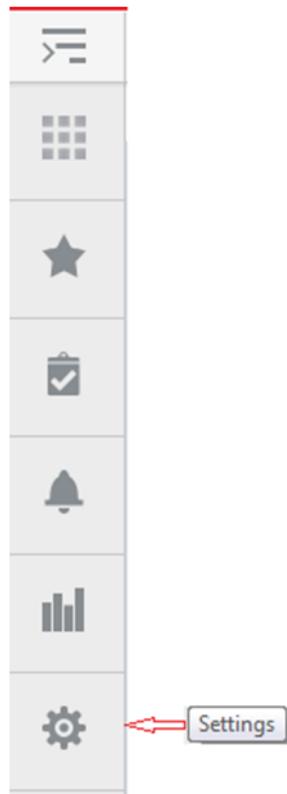
Action	Role	Order Approve Amt
2	Update	OIM_TEST_>99999999999
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

4

Application Customization

The Oracle Retail Application provides different administrative options for administering various functionality in the application. These include the User Interface, Dashboards and Reports, Security, Notifications, Resource Bundles, Asynchronous Tasks, Lookups, Application Properties. The administrative options can be accessed using the Settings menu in the navigation toolbar. The Settings icon is available only to the administrator users.

Figure 4–1 Settings Icon

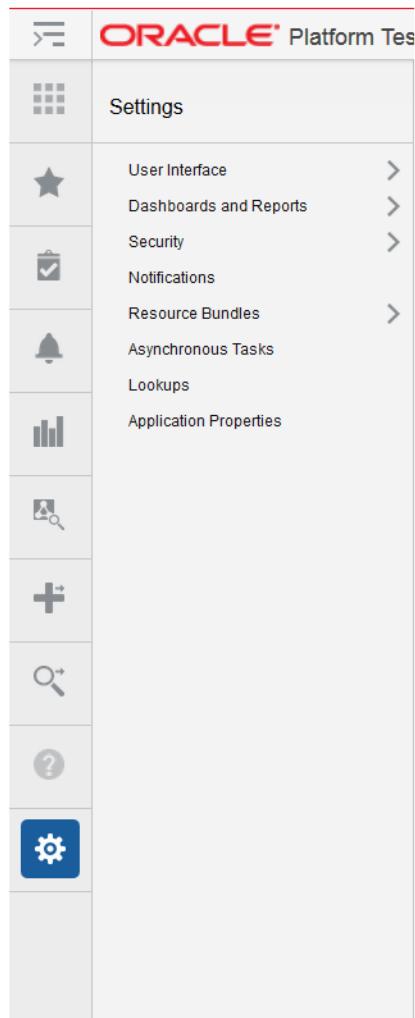


Following are the options in the Settings menu:

- User Interface
- Dashboard and Reports
- Security

- Notifications
- Resource Bundles
- Asynchronous Tasks
- Lookups
- Application Properties

Figure 4–2 Settings Menu



User Interface Customization

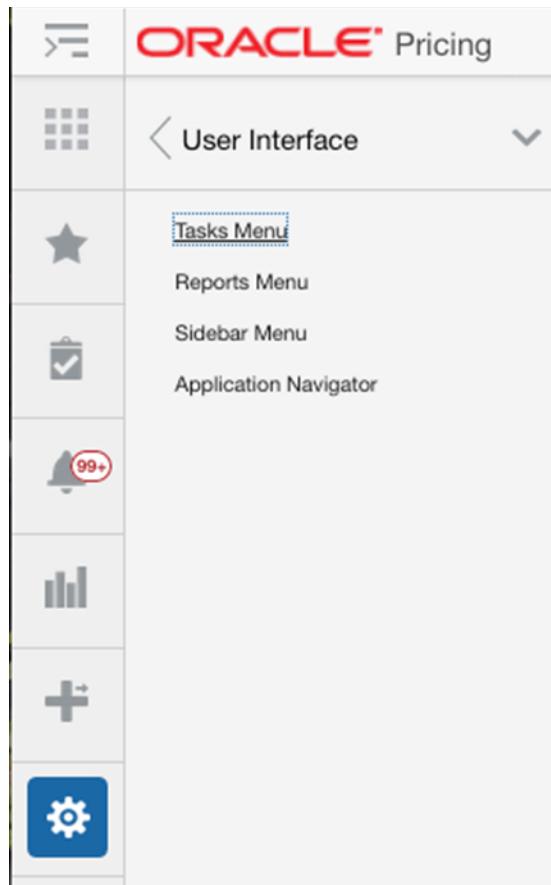
Application customization is an option in the Settings menu that can be used by an administrator to customize the look and feel in the Merchandising solutions. The administrator can customize the task menu, reports menu, and the sidebar menu using the User Interface option.

Following are the menu items available in the User Interface menu.

- Tasks Menu
- Reports Menu

- Sidebar Menu
- Application Navigator

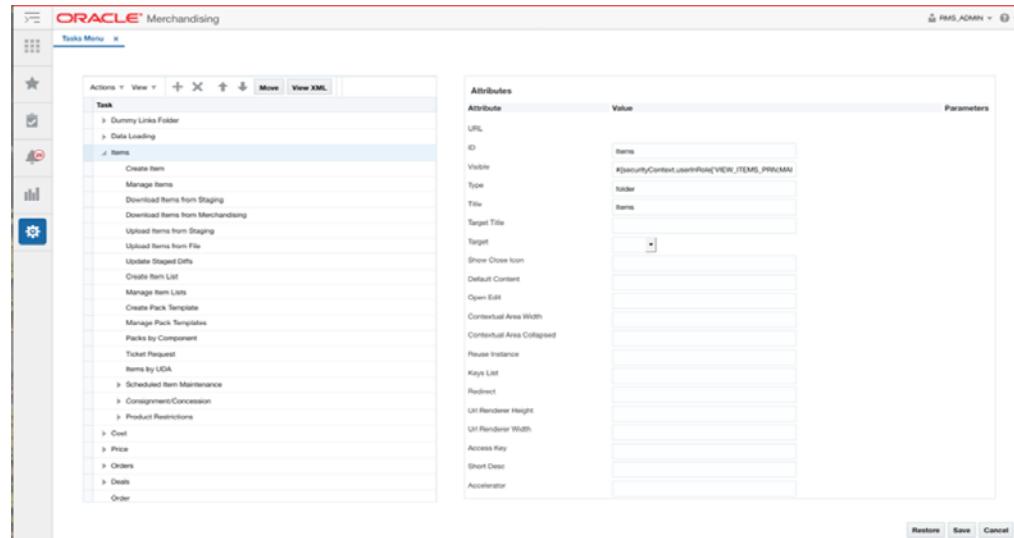
Figure 4-3 User Interface Menu



Tasks Menu Customization

The Tasks Menu link opens an application tab showing the screen for the tasks menu customization. An administrator can add, modify or remove the tasks available in the tasks menu using the Tasks Menu customization screen.

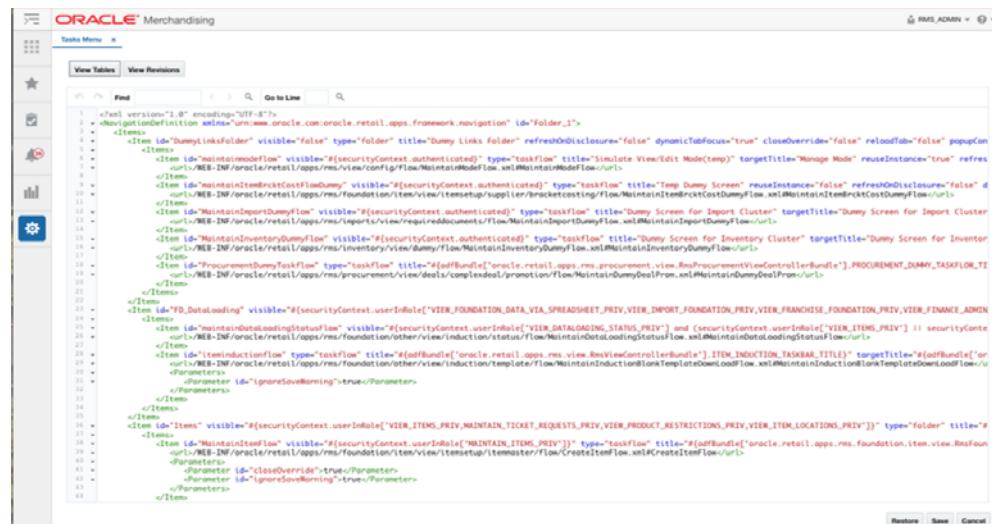
Figure 4–4 Tasks Menu



The Tasks Menu customization tab displays buttons to save, restore or cancel the changes. The Save button saves the changes to the tasks menu. The changes are immediately reflected in the tasks menu. The Cancel button closes the tab without saving the changes. The Restore button replaces the customized menu with the original menu shipped with the Retail Application.

The administrator can also click on the 'View XML' button to view the xml version of the tasks menu model file. The View XML button opens the task menu model file in an XML editor. The XML View contains a 'View Tables' button which takes the user back to the tables view.

Figure 4–5 Tasks Menu Customization XML



Note: The changes done to the tasks menu are lost after an upgrade of the application. You should manually reapply the changes after the upgrade. The 'View Revisions' button on the Tasks Menu XML screen displays all the prior revisions of the tasks menu.

You can choose a version of the application to view the base and customized task menu model file for that version.

You can also compare the two files to view your customizations.

The task menu model xml file uses the xml schema definition called NavigationModel.xsd for xml validation. The Navigation Model schema definition file is used to validate any changes done by the administrator on the task menu xml file. The Task Menu model file consists of a hierarchy of Item elements. Each element represents a menu item in the task menu. The Item element can either be a folder or has a URL, list of attributes and parameters that identify the task menu item.

Task Menu Model XML Items

An item in the task menu model renders as either a launchable link or a submenu in the Tasks menu of the Retail Application. A new item can be added to add a new link or submenu. An existing Item can be modified to change an existing link or submenu. Below is the example of a task menu model Item.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NavigationDefinition ... >
    <Items>
        <Item id="myFolder" title="My Folder" type="folder">
            <Items>
                <Item id="myContent" type="taskflow"
                      title="My Content">
                    <url>
                        /WEB-INF/mycompany/CustomDashboardTaskFlow.xml#CustomDashboardTaskFlow
                    </url>
                    <Parameters>
                        <Parameter id="productName">"Acme"</Parameter>
                    </Parameters>
                </Item>
            </Items>
        </Item>
    </Items>
</NavigationDefinition>
```

Task Menu Model Item Attributes

The following attributes apply to an Item element in the task menu model xml file.

Table 4–1 Task Menu Model Item Attributes

Attribute	Description
visible	Indicates if the item should be rendered (visible) or not. It can be an EL Expression that evaluates to true or false. Or it can be a plain string value equal to "true" or "false". Defaults to "true".

Table 4–1 (Cont.) Task Menu Model Item Attributes

Attribute	Description
type	Indicates the type of the item. The main values are "folder", "taskflow", "link". The type "folder" indicates that the item contains additional sub-navigation items. The type "taskflow" indicates it is a task flow, and the type "link" is used for URLs.
title	The attribute title is used to provide the title of the sidebar item. This attribute is a required attribute.
targetTitle	The attribute targetTitle is used to provide the title of the tab in the content area. This attribute is an optional attribute. If not provided, the value of the title attribute will be used as the title of the tab in the content area.
accessKey	The attribute accessKey is used to specify the keyboard keystroke or a group of keystrokes that are used to access the navigation item using the keyboard.
shortDesc	The attribute shortDesc is used to provide the description of the navigation item which will be displayed when the user hovers over a menu item.
showCloseIcon	Mainly used when the content is being rendered in a popup, and indicates if the 'x' icon should show or not on the top right corner of the popup to facilitate manual closing of the popup. Takes the values "true" or "false". Defaults to "false".
defaultContent	Indicates whether the corresponding items from the model show up by default in tabs in the content area when the page template loads. Takes values "true" or "false", or may even take an EL Expression evaluating to "true" or "false".
reuseInstance	The attribute reuseInstance is used to specify whether the navigation items with the same title and url will use the same tab or not. When this attribute is set to false, the request to open the content for that navigation item will always use a new tab. When the attribute is true, the navigation items with the same title and url will share the same tab in the content area. It defaults to true.
keysList	Takes name value pairs separated by a semicolon. The attribute keysList provides a way to differentiate two navigation items with the same title and url. If keysList is not provided, then the two navigation items with the same title and url will always use the same tab. When the keysList is provided, it provides uniqueness to the navigation items with the same title and url enabling them to use different tabs. Example <code>keysList="key1=value1;key2=value2"</code>
urlRendererHeight, urlRendererWidth	Example values are shown below. These used in the case of a popup and indicate the height and width of the popup. <code>urlRendererHeight="200px" urlRender-erWidth="200px"</code>
reloadTab	When this attribute is set to true, an already opened tab will be reloaded with the new input parameters for the taskflow. When it is set to false, a previously opened tab will only be re-focused, but not reloaded with new input parameters for the taskflow.

Table 4–1 (Cont.) Task Menu Model Item Attributes

Attribute	Description
refreshOnDisclosure	When the navigation item has refreshOnDisclosure attribute set to true then the tab displaying that item in the Content Area will be refreshed every time it's disclosed. The attribute can take either of the two values true or false. Default is false. The attribute is useful in the scenarios where we want to display to the user the latest information from the database every time he/she comes back to the tab. The attribute should be used with caution because if the data in that tab is not committed before leaving the tab then the uncommitted data will be lost upon coming back to the tab.
dynamicTabFocus	When a navigation item is invoked, the tab displaying that item will have its text focused. To override this behavior, set dynamicTabFocus to "false". This attribute defaults to "true".
popupId	Applicable only when target="_popup". Must be a number between 1 and 15. This attribute allows consuming applications to target a specific popup within the UI Shell. The framework provides 15 popups that consuming applications can take advantage of. In case this attribute has not been specified, a default popup will be used by the framework. This default popup will not store its dimensions in MDS.
popupContentHeight	Applicable only when target="_popup". This attribute is used to provide the height in pixels of the resulting popup dialog window.
popupContentWidth	Applicable only when target="_popup". This attribute is used to provide the width in pixels for the resulting popup dialog window.
popupStretchChildren	Applicable only when target="_popup". This attribute is used to indicate the stretching behavior for the contents of the resulting popup window. The contents are referred to as child components. Valid values are: <ul style="list-style-type: none"> ▪ none - does not attempt to stretch any children (the default value and value you need to use if you have more than a single child; also the value you need to use if the child does not support being stretched). ▪ first - stretches the first child (not to be used if you have multiple children as such usage will produce unreliable results; also not to be used if the child does not support being stretched).
popupResize	Applicable only when target="_popup". This attribute is used to indicate the resulting popup window's resizing behavior. Valid values are: <ul style="list-style-type: none"> ▪ on - user can resize the dialog with their mouse by dragging any of the dialog edges. ▪ off - the dialog automatically sizes its contents if popupStretchChildren is set to "none"
popupHelpTopicId	Applicable only when target="_popup". This attribute is used to look up a topic in a help-Provider for the resulting popup window.

Table 4–1 (Cont.) Task Menu Model Item Attributes

Attribute	Description
popupShortDesc	Applicable only when target="_popup". This attribute is used to provide short description of the resulting popup window.
contentListener	Specifies the fully qualified name of the class implementing the ContentListener interface. This allows applications to have the ability to inject any session or request values before opening tabs.
tabShortDesc	Specifies the text to be shown when the user hovers over the application tab. Using this attribute application team can keep the title short and the tabShortDesc as fully qualified tab name which can be shown as the tooltip of the tab. This attribute will be displayed as tab title in screen reader mode.

Task Menu Model Item Sub-elements

The following are the sub-elements of the Item element in the task menu model.

Table 4–2 Task Menu Model Item Sub-elements

Element	Description
url	The location of the item being launched. If the type is "taskflow" - then the URL element must contain the path to the task flow XML. If the type is "link" - then the URL of the external system must be indicated in this subelement. The entire URL must be marked as character data (e.g. enclosed in CDATA).
Parameter	The <Parameters> sub-element within <Item> should list all the parameters to the dashboard page if there are any. Each parameter is represented as a <Parameter> element inside <Parameters>. The <Parameter> id should be the actual parameter reference name recognized by the dashboard URL. The value of each <Parameter> is a string value. This is the only supported data type.

Securing Access to Items

To restrict access to menu items to specific security roles, set the visible property on the <Item> element for the URL to an Expression Language (EL) expression that calls ADF's securityContext API's isUserInRole method. Example:

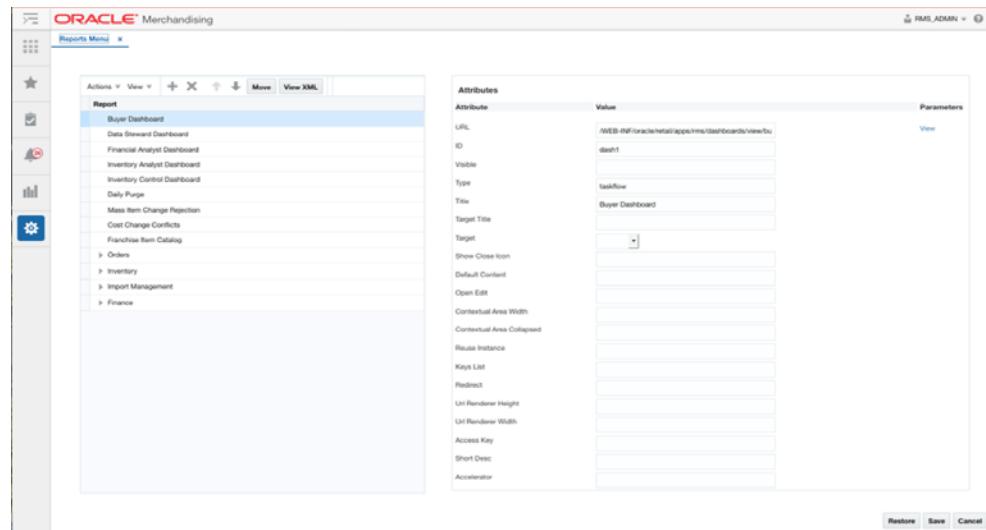
```
<Item id="myDashboard1"
      type="link"
      title="Profitability Dashboard"
      visible="#{securityContext.isUserInRole['BUYER_JOB']} ">
```

The parameter to the securityContext.isUserInRole method is a logical security role that is configured for the Retail Application. The API returns true if the user is included in the specified security role. If the user is not authenticated or is not found in the role, the API returns false.

Reports Menu Customization

The Reports Menu link opens an application tab showing the screen for the reports menu customization. An administrator can add, modify or remove the reports available in the reports menu using the Report Menu customization screen.

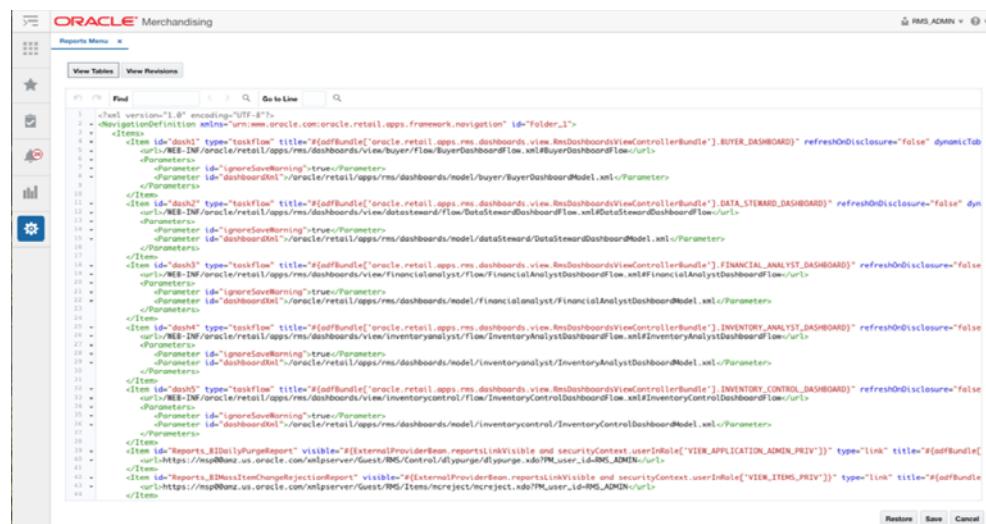
Figure 4-6 Reports Menu Customization Screen



The Reports Menu customization tab displays buttons to save, restore or cancel the changes. The Save button saves the changes to the reports menu. The changes are immediately reflected in the reports menu. The Cancel button closes the tab without saving the changes. The Restore button replaces the customized menu with the original menu shipped with the Retail Application.

The administrator can also click on the 'View XML' button to view the xml version of the reports menu model file. The View XML button opens the report menu model file in an XML editor. The XML View contains a 'View Tables' button which takes the user back to the tables view.

Figure 4-7 Reports Menu Customization XML



Note: The changes done to the reports menu are lost after an upgrade of the application. You should manually reapply the changes after the upgrade. The 'View Revisions' button on the Reports Menu XML screen displays all the prior revisions of the reports menu.

You can choose a version of the application to view the base and customized reports menu model file for that version.

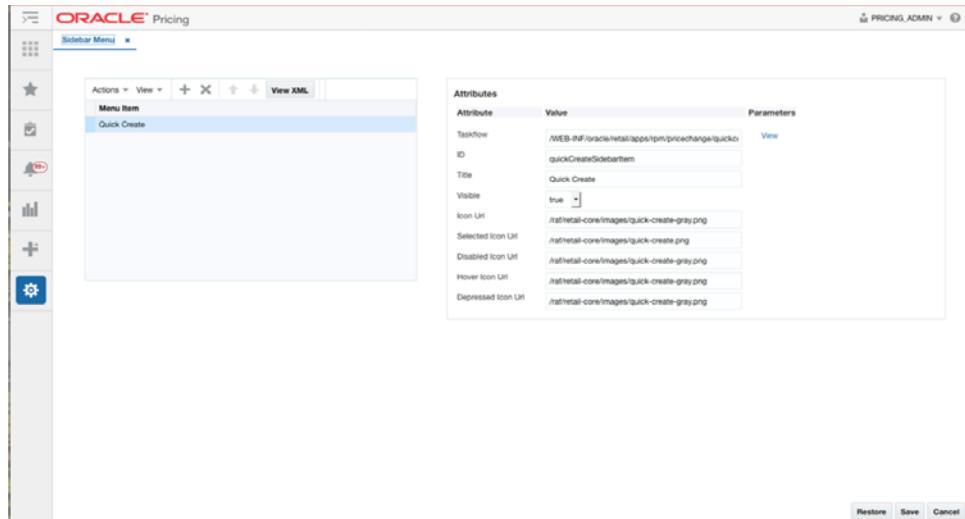
You can also compare the two files to view your customizations.

The reports menu uses the same NavigationModel.xsd file used by the task menu. The attributes defined for the task menu apply to the reports menu as well. Please refer to the Task Menu Customization section above for the details on how to customize the reports menu.

Sidebar Menu Customization

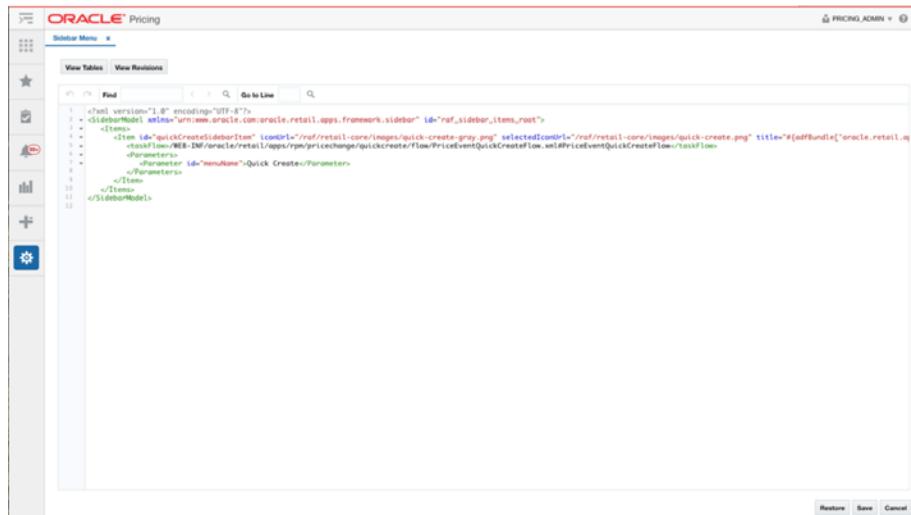
The Sidebar Menu link opens an application tab showing the screen for the sidebar menu customization. An administrator can add, modify or remove the icons available in the sidebar menu using the Sidebar Menu customization screen.

Figure 4–8 Sidebar Menu Customization Screen



The Sidebar Menu customization tab displays buttons to save, restore or cancel the changes. The Save button saves the changes to the sidebar menu. The changes are immediately reflected in the sidebar menu. The Cancel button closes the tab without saving the changes. The Restore button replaces the customized menu with the original menu shipped with the Retail Application.

The administrator can also click on the 'View XML' button to view the xml version of the sidebar menu model file. The View XML button opens the sidebar menu model file in an XML editor. The XML View contains a 'View Tables' button which takes the user back to the tables view.

Figure 4-9 Sidebar Menu Customization XML

Note: The changes done to the sidebar menu are lost after an upgrade of the application. You should manually reapply the changes after the upgrade. The 'View Revisions' button on the Sidebar Menu XML screen displays all the prior revisions of the sidebar menu.

You can choose a version of the application to view the base and customized sidebar menu model file for that version.

You can also compare the two files to view your customizations.

The sidebar menu uses a schema called sidebarSchema.xsd for the validation of the sidebar items. The sidebar xml model file consists of Item elements similar to the Item element in the task menu. The Item element in the sidebar xml model has a different set of attributes.

Sidebar Menu Model XML Items

An item element in the sidebar model xml file renders as a launchable icon in the sidebar. The sidebar has a fixed set of icons and a variable set of icons. Only the variable icons can be customized using the sidebar model xml file. The fixed set of icons cannot be customized. A new sidebar Item can be added to add a new icon on the sidebar. Below is the example of a sidebar menu model Item.

```

<?xml version="1.0" encoding="UTF-8" ?>
<SidebarModel id="raf_sidebar_items_root"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:www.oracle.com:oracle.retail.apps.framework.sidebar
    classpath:oracle/retail/apps/framework/uishell/common/sidebar/sidebarSchema.xsd"
  xmlns="urn:www.oracle.com:oracle.retail.apps.framework.sidebar">
  <Items>
    <Item id="quickCreateSidebarItem" title="Quick Create"
      iconUrl="/raf/retail-core/images/quick-create-gray.png"
      selectedIconUrl="/raf/retail-core/images/quick-create.png" title="#{adfBundle['oracle.retail.q
        raf.sidebar.items_root.quickCreateSidebarItem.title']}">
      <Parameters>
        <Parameter id="menuName">Quick Create</Parameters>
    </Item>
  </Items>
</SidebarModel>

```

```
</Items>
</SidebarModel>
```

Sidebar Menu Model Item Attributes

The following attributes apply to an Item element in the sidebar menu model xml file.

Table 4–3 Sidebar Menu Model Item Attributes

Attribute	Description
id	The id of the sidebar item.
title	The title of the sidebar icon.
visible	The visible attribute controls the visibility of the sidebar item.
iconUrl	The icon that is displayed for the sidebar item.
selectedIconUrl	The icon that is displayed when the sidebar item is selected.
disabledIconUrl	The icon that is displayed when the sidebar item is disabled.
hoverIconUrl	The icon that is displayed when the sidebar item is hovered on.
depressedIconUrl	The icon that is displayed when the sidebar item is depressed.

Sidebar Model Item Sub-elements

The following are the sub-elements of the Item element in the sidebar model.

Table 4–4 Sidebar Model Item Sub-elements

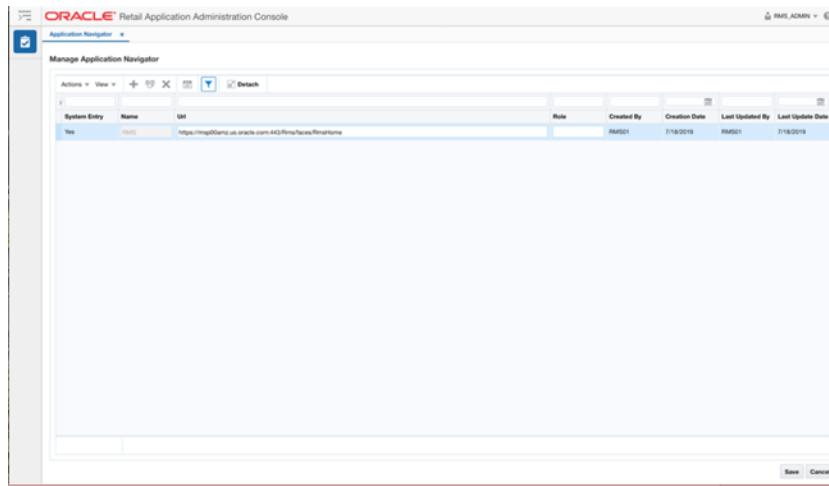
Element	Description
taskFlow	The URL of the taskflow being launched.
Parameter	<p>The <Parameters> sub-element within <Item> should list all the parameters to the sidebar taskflow if there are any. Each parameter is represented as a <Parameter> element inside <Parameters>.</p> <p>The <Parameter> id should be the actual parameter reference name recognized by the taskflow URL.</p> <p>The value of each <Parameter> is a string value. This is the only supported data type.</p>

Application Navigator

Application Navigator allows users to launch different applications from their current application. This lets users shuffle between multiple applications based on their privileges and avoid having to open a new tab and enter a new URL to launch an application. Users can instead click on the application, which will launch that application in a new tab or window based on the browser settings. If the application is a Single Sign-On (SSO) deployment then the user will be logged in by default and the default application page is displayed. If the deployment is non-SSO then the user is prompted to log in.

If a user has access to multiple applications (based on their defined role) they are able to see the list of available applications under the Application Navigator menu. If a user does not have access to any other applications, only the current application name will be displayed in the application navigator list.

The Application Navigator link opens in a new browser window using the Oracle Retail Administration Admin Console (RAAC) application.

Figure 4–10 Application Navigator Screen

In order for users to see an application in the Application Navigator menu, they need to belong to the role associated with that application on the Application Navigator screen. Only an application administrator is aware of the links to the different installed applications. The Application Navigator screen provides the ability to add, modify and remove the links so they appear or not appear in the Application Navigator menu. The application administrator can determine which application role has access to which application based on customer's security model. For example, suppose Allocation users belonging to Allocation role X are to see the Invoice Match application link in the Allocation's Application Navigator menu. The administrator would launch the Application Navigator screen, add an entry for Invoice Match and enter X for the role.

Add

The Add action is enabled at all times and allows an administrator to add a new Application Navigator URL.

Add an Application Navigator URL

1. From the Actions menu, select Add. A new, empty Application Navigator entry is added to the Manage Application Navigator table.
2. Enter a name, the application URL, and the role to which the URL applies. The remaining columns are populated automatically.
3. System records cannot be inserted from the Manage Application Navigator screen. This will be created once per application by the installer at the application install time.

Modify

While all the columns on a row can be modified, only the ROLE and URL columns of a System Record can be modified by the administrators.

Duplicate

The Duplicate action adds a copy of each selected row below its originating row. The object name or unique identifier of the duplicate row is "Copy of Object Name" and appears in edit mode. Validation is performed so that a user is not presented with multiple applications with the same application name.

When a system record is duplicated, a copy of the record is created with the System Entry column set to 'N' and thus made available on the Application Navigator list.

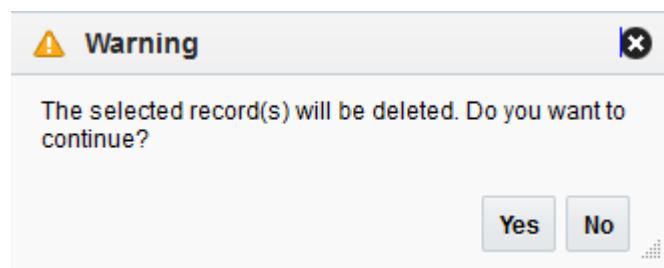
Delete

The Delete action is enabled when an entry is selected.

When the user selects an application navigator entry and clicks Delete, the user is prompted with a warning message. Click Yes and the selected entry is removed.

A system entry record set to Yes cannot be deleted from RAAC.

Figure 4–11 Delete Application Navigator Confirmation Dialog



Export to Excel

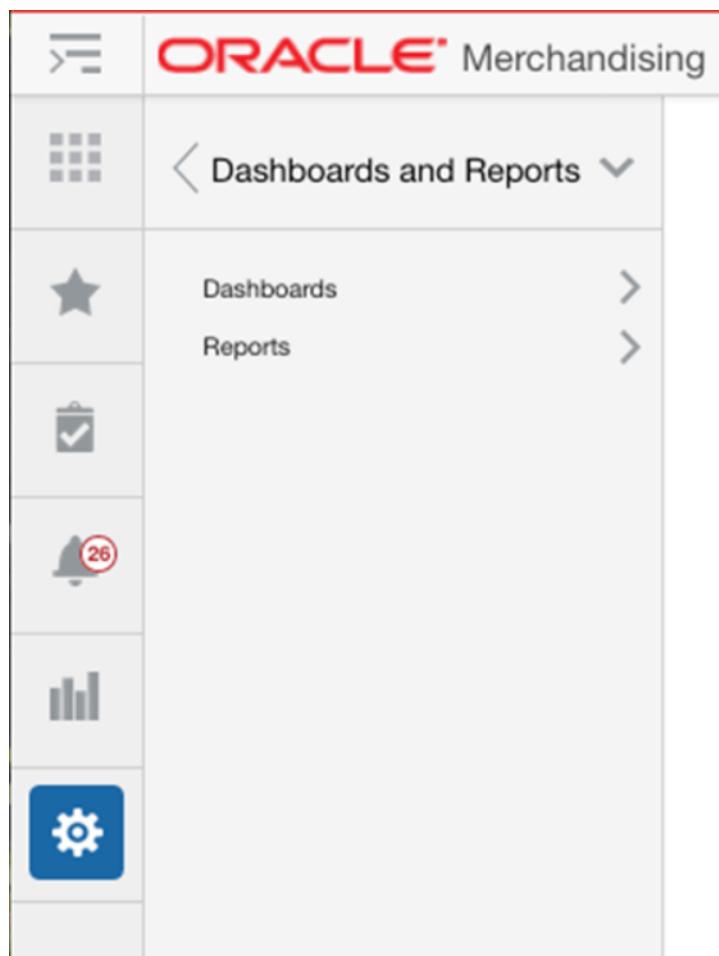
The Export to Excel action is enabled whenever you have the Manage Application Navigator window open. This action allows you to export the Manage Application Navigator list to a Microsoft Excel spreadsheet.

Dashboards and Reports

The Dashboards and Reports menu option in the settings menu can be used by an administrator to configure the dashboards and the contextual reports. The administrator can add or replace reports, change the dashboard and report layout.

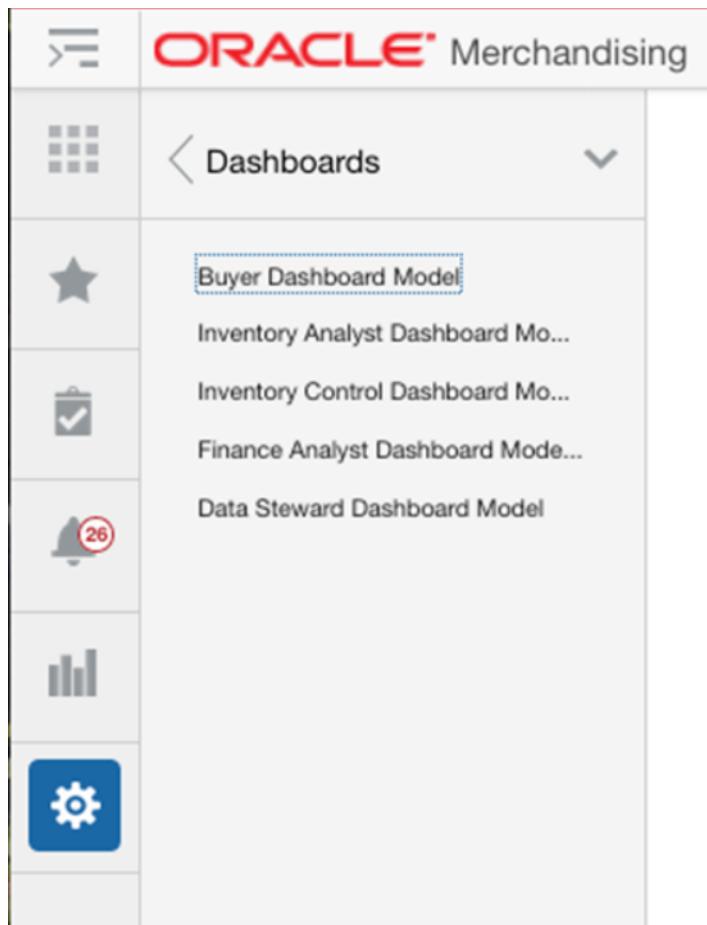
Following are the options available in the Dashboards and Reports menu.

- Dashboards
- Reports

Figure 4–12 Dashboards and Reports Menu

Dashboard Customization

The Dashboards link displays the list of dashboards available in the application.

Figure 4–13 Dashboards Menu

When a dashboard name is clicked, it opens the dashboard customization screen in an application tab. The dashboard reports can be added, modified or removed from the dashboard. The dashboard layout can also be changed using the dashboard customization screen.

Figure 4–14 Dashboards Customization Screen

Attribute	Value	Parameters
URL	/MEIS-INF/oracle/retail/apps/rms/dashboards/viewBu	View
Width	100%	
Height	auto	
Item Type	prompt	
ID	filter	

The Dashboard customization tab displays buttons to save, restore or cancel the changes. The Save button saves the changes to the dashboard. The dashboard customization changes are not immediately reflected in the dashboard. The dashboard tab should be closed and reopened for the customization changes to be applied to the dashboard. The Cancel button closes the tab without saving the changes. The Restore button replaces the customized dashboard with the original dashboard shipped with the Retail Application.

The administrator can also click on the 'View XML' button to view the xml version of the dashboard model file. The View XML button opens the dashboard model file in an XML editor. The XML View contains a 'View Tables' button which takes the user back to the tables view.

Note: The changes done to the dashboard are lost after an upgrade of the application. You should manually reapply the changes after the upgrade. The 'View Revisions' button on the Dashboard XML screen displays all the prior revisions of the dashboard.

You can choose a version of the application to view the base and customized dashboard model file for that version.

You can also compare the two files to view their customizations.

Retail Dashboards display the status of metrics and key performance indicators relevant to the Retail Application. They are typically tailored for specific roles and they allow users to easily monitor the status of the current data within the application.

Users can access the dashboards from the application's Reports menu.

Understanding Design Pattern of Included Dashboards

Depicted below is an example of a dashboard that might appear in Allocation:

Figure 4–15 Dashboard Example

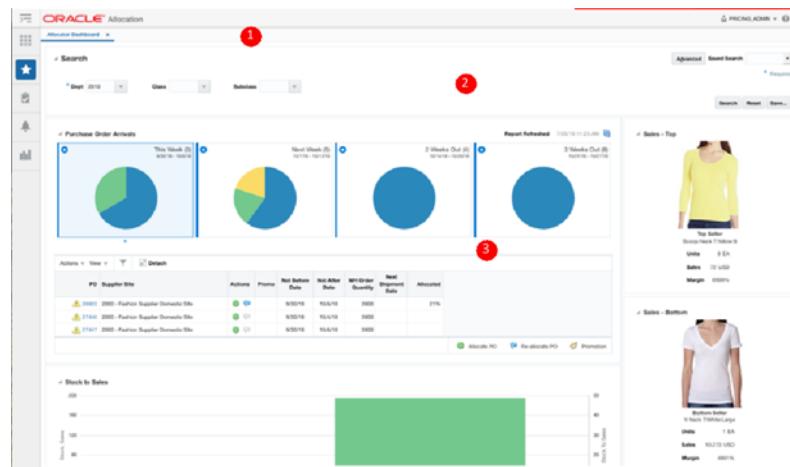
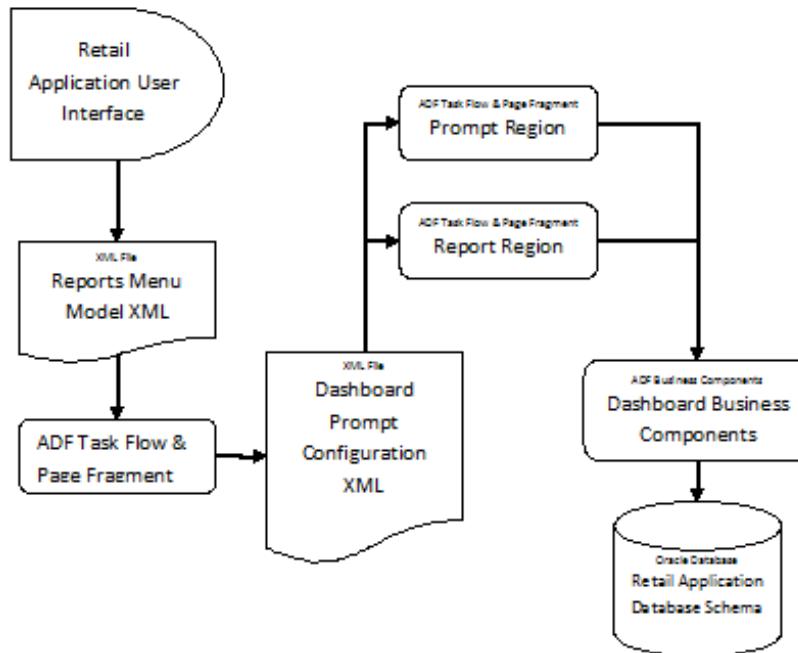


Table 4–5 Dashboard Region Descriptions

Number	Region	Description
1	Dashboard Page	A page rendering a dashboard. A dashboard is composed of 1 or more reports. The dashboard page is launched as a tab within the application
2	Prompt Region	The prompt region contains a set of editable input components that allow users to modify the parameters of the various reports in the dashboard. This allows users to see different sets of data for the same set of reports.
3	Report Region	A report region shows the various reports that are currently configured in the dashboard.

The prompts and regions are configured in an XML file called a Dashboard Prompt Configuration XML. The dashboard prompt XML arranges visually the prompts and regions on the dashboard page.

The representation of the dashboards is depicted in the diagram below:

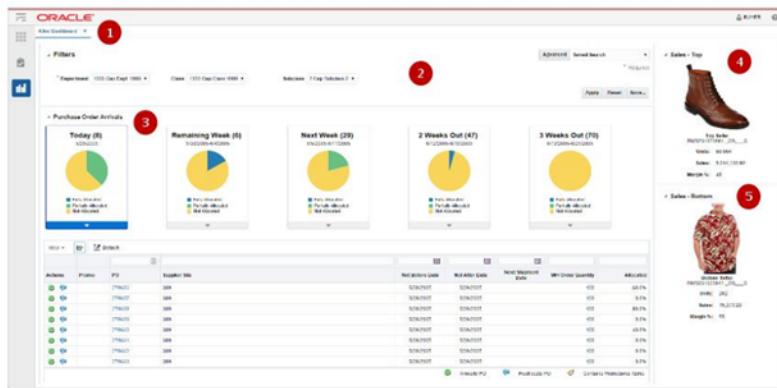
Figure 4–16 Representation of a Dashboard

The dashboard task flow is launchable from the Retail Application User Interface's Reports Menu. In order to make the report launchable, the dashboard task flow is registered in the application's reports menu model XML.

A set of ADF business components enable data from the Retail Application schema to be rendered in the report regions.

The figure below shows a rendering of a dashboard (called Allocations Dashboard) in a Retail Application:

Figure 4–17 Example Allocations Dashboard



The different parts of this example dashboard are described below:

Table 4–6 Allocation Dashboard Region Descriptions

Number	Region	Description
1	Dashboard Page	The Allocations Dashboard example contains 1 prompt and 3 reports. It is implemented as an ADF bounded task flow called AllocDashboardFlow.
2	Prompt Region	This is the prompt region that users modify to change the view of the various reports in this dashboard. It is implemented as an ADF bounded task flow called DashboardFilterFlow.
3	Order Status Report	A report region showing a row of information tiles and a detail table. It is implemented as an ADF bounded task flow called OrderStatusFlow.
4	Top Seller Report	A report region showing the top selling item. It is implemented as an ADF bounded task flow called TopSellerFlow.
5	Bottom Seller Report	A report region showing the bottom selling item. It is implemented as an ADF bounded task flow called BottomSellerFlow.

The reports menu model XML file (as shown below) contains an item called allocDashboard registering the task flow, AllocDashboardFlow, into the reports menu. Note that the dashboard task flow includes a parameter called dashboardConfigXML which references the location of the Dashboard Prompt Configuration XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NavigationDefinition id="Folder_1"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="urn:www.oracle.com:oracle.retail.apps.framework.navigation"
    >
```

```

  xsi:schemaLocation="urn:www.oracle.com:oracle.retail.apps.framework.navigation
  classpath:oracle/retail/apps/framework/uishell/navigation/model/schema/NavigationM
  odel.xsd">
    <Items>
      <Item id="allocDashboard" title="Alloc Dashboard"
        shortDesc="Alloc Dashboard"
        type="taskflow">
        <url>/WEB-INF/AllocDashboardFlow.xml#AllocDashboardFlow</url>
        <Parameters>
          <Parameter
            id="dashboardConfigXML"/>/oracle/AllocDashboardPrompt.xml</Parameter>
        <Parameters>
      </Item>
    </Items>
  </NavigationDefinition>

```

The Dashboard Prompt Configuration XML file for this example is called the AllocDashboardPrompt.xml and it contains the following entries:

```

<?xml version="1.0" encoding="UTF-8" ?>
<Dashboard layout="column"
  xmlns="urn:www.oracle.com:oracle.retail.apps.framework.dashboard"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

  xsi:schemaLocation="urn:www.oracle.com:oracle.retail.apps.framework.dashboard
  classpath:oracle/retail/apps/framework/dashboard/model/schema/dashboardSchema.xsd"
>
  <Vectors>
    <Vector>
      <Items>
        <Item id="filter" type="prompt">
          <url>/WEB-INF/DashboardFilterFlow.xml#DashboardFilterFlow</url>
          </Item>
        <Item id="orderStatus" type="report">
          <url>/WEB-INF/oracle/retail/apps/framework/dvtcontextawarereport/publicui/flow/DVT
          ContextAwareReportFlow.xml#DVTContextAwareReportFlow</url>
          <Parameters>
            <Parameter
              id="taskflowURL"/>/WEB-INF/OrderStatusFlow.xml#OrderStatusFlow</Parameter>
            <Parameter id="parameterName1">departmentIds</Parameter>
            <Parameter id="payloadKeyName1">DepartmentId</Parameter>
            <Parameter id="parameterName2">classIds</Parameter>
            <Parameter id="payloadKeyName2">ClassId</Parameter>
            <Parameter id="parameterName3">subclassIds</Parameter>
            <Parameter id="payloadKeyName3">SubclassId</Parameter>
          </Parameters>
        </Item>
      </Items>
    </Vector>
    <Vector width="300px">
      <Items>
        <Item id="topSeller" type="report">
          <url>/WEB-INF/oracle/retail/apps/framework/dvtcontextawarereport/publicui/flow/DVT
          ContextAwareReportFlow.xml#DVTContextAwareReportFlow</url>
          <Parameters>
            <Parameter
              id="taskflowURL"/>/WEB-INF/oracle/retail/apps/flow/TopSellerFlow.xml#TopSellerFlow<
              /Parameter>
            <Parameter id="parameterName1">departmentIds</Parameter>

```

```

<Parameter id="payloadKeyName1">DepartmentId</Parameter>
<Parameter id="parameterName2">classIds</Parameter>
<Parameter id="payloadKeyName2">ClassId</Parameter>
<Parameter id="parameterName3">subclassIds</Parameter>
<Parameter id="payloadKeyName3">SubclassId</Parameter>
</Parameters>
</Item>
<Item id="bottomSeller" type="report">

<url>/WEB-INF/oracle/retail/apps/framework/dvtcontextawarereport/publicui/flow/DVT
ContextAwareReportFlow.xml#DVTContextAwareReportFlow</url>
<Parameters>
<Parameter
id="taskflowURL">/WEB-INF/oracle/retail/apps/flow/BottomSellerFlow.xml#BottomSelle
rFlow</Parameter>
<Parameter id="parameterName1">departmentIds</Parameter>
<Parameter id="payloadKeyName1">DepartmentId</Parameter>
<Parameter id="parameterName2">classIds</Parameter>
<Parameter id="payloadKeyName2">ClassId</Parameter>
<Parameter id="parameterName3">subclassIds</Parameter>
<Parameter id="payloadKeyName3">SubclassId</Parameter>
</Parameters>
</Item>
</Items>
</Vector>
</Vectors>
</Dashboard>

```

The file registers the prompts and regions into a hierarchy of vectors and items. The structure of the dashboard prompt configuration XML file is explained in the following section.

The Dashboard Prompt Configuration XML File

The Dashboard Prompt Configuration XML file can be modified to change the dashboard layout or add or remove reports from the Dashboard. The root element of the model file is the "Dashboard" element. Other than schema and namespace information, the "Dashboard" element has a "layout" attribute that must be provided, and must contain a value of either "row" or "column". This attribute arranges the regions of the dashboard in rows or columns.

Inside the "Dashboard" element is a "Vectors" element, which contains a list of "Vector" elements. If the dashboard layout="row", then each "Vector" corresponds to a single row in the dashboard. Conversely, if layout="column", then each "Vector" corresponds to a column. To add a new row or column, simply add another "Vector" element inside the "Vectors" element.

Up to 12 rows and 6 columns can be displayed in a dashboard, not including separate header and footer regions. Any items beyond 12 rows or 6 columns will not appear on the dashboard.

Rows in the dashboard display from top to bottom. If layout="row", the first "Vector" will appear toward the top of the page. Columns appear from left to right, so if layout="column", the first "Vector" will appear toward the left of the page.

Each "Vector" element contains an "Items" element, which contains a list of "Item" elements. The xml structure for "Item" elements is very similar to the tasks or reports sidebar menu models.

The following attributes are supported on dashboard items:

Table 4-7 Supported Attributes

Name	Description	Required
id	A unique id for this region	Yes
type	The type of content contained in this region. Valid values: prompt, report	Yes
width	The width of this region. See below for more details.	No
height	The height of a region. See below for more details.	No
url	The task flow url to open in this region	Yes
Parameters	Parameters to be sent to the URL	No

In addition to the items arranged in rows or columns, you can add a header and footer region to the dashboard. Both horizontally span the full width of the dashboard, with the header appearing at the top and the footer appearing at the bottom. These can be added in the model by specifying a "HeaderItem" or "FooterItem" child of the root "Dashboard" element. These regions support all the same properties as other items in the dashboard.

Vectors and items expose width and height attributes to enable applications to resize elements to best fit on the dashboard. Certain rules and best practices apply when using these attributes.

First, if the dashboard is in row layout, then all items in a row must have the same height. The height attribute from the vector is used to specify the height of every item in that row. Since rows are assumed to span the full width, the vector width is ignored in this layout.

In the same way, when the dashboard is arranged in column layout, all items in a column must have the same width. The vector width is used to specify the width of every item in that column. Columns should expand vertically to accommodate all content, allowing a scrollbar if necessary. Therefore, vector height is ignored in this layout.

In addition to the width and height attributes, a vector also provides a dimensionsFrom attribute. The valid values of the dimensionsFrom attribute can be auto, child or parent. The dimensionsFrom attribute is used to specify whether the Items in the vector inherit their dimensions from the parent decorative box or not. When the dimensionsFrom attribute is parent, the Items in the vector will be stretched to fill any available space in the vector. When the dimensionsFrom attribute is child, the Items in the vector won't stretch but will display scroll bars if they cannot be accommodated in the available space in the decorative box. The default value of the dimensionsFrom attribute is 'auto' which gives preference to the child dimensions.

The following table indicates which attributes are used, based on which dashboard layout has been selected.

Table 4-8 Supported Attributes

	Row layout	Column layout
Vector width	ignored	valid
Vector height	valid	ignored
Item height	ignored	valid
Item width	valid	ignored

In column layout, either every vector width should be provided, or every width should be omitted. If all widths are omitted, columns default to divide the total width evenly. When the widths are omitted, the dimensionsFrom attribute of the vector can be set to parent if stretching of the Items is desired. If widths are provided, they should be specified as a percentage, and the sum of all widths should equal 100%.

In row layout, heights may be specified or omitted as desired. If a row's height is omitted, it will default to get the dimension from the content inside the regions. When the row's height is omitted, the dimensionsFrom attribute of the vector can be set to parent if stretching of the Items is desired. Heights should be specified using an exact unit such as px or em. Percentages should not be used.

If these rules and best practices are ignored, results may be inconsistent or undesirable. Items may not size as intended, and horizontal scrollbars or nested vertical scrollbars may appear.

In addition to resizing entire rows or columns, individual items inside the row or column can also be resized. As mentioned above, items in a row should all have the same height, so in row layout, item height is ignored and only item width is valid. And items in a column should have the same width, so item width is ignored and only item height is valid. See the table above for details.

The same rules and best practices that apply to vector height and width also apply to setting item height and width.

Refreshing Reports on Prompt Changes

When the user changes a value on the dashboard prompt, that value translates as a parameter change on the different reports on the dashboard.

This is accomplished through a feature in ADF called Contextual Events. To put simply, contextual events are signals that a page in a task flow can generate for which pages in other task flows can listen and react to. For the included dashboards, prompt regions generate a contextual event whenever the user changes a prompt field value. When a report "hears" an event, it will process the contextual event information (called a payload) to extract the changed prompt value, use that value as a parameter to the report query and refresh the report region.

In the example depicted in the previous section, the Dashboard Prompt Configuration XML file shows all three reports registered under a wrapper task flow called the DVTContextAwareReportFlow.

```
<Item id="bottomSeller" type="report">

<url>/WEB-INF/oracle/retail/apps/framework/dvtcontextawarereport/publicui/flow/DVT
ContextAwareReportFlow.xml#DVTContextAwareReportFlow</url>
    <Parameters>
        <Parameter
id="taskflowURL">/WEB-INF/oracle/retail/apps/flow/BottomSellerFlow.xml#BottomSelle
rFlow</Parameter>
        <Parameter id="parameterName1">departmentIds</Parameter>
        <Parameter id="payloadKeyName1">DepartmentId</Parameter>
        <Parameter id="parameterName2">classIds</Parameter>
        <Parameter id="payloadKeyName2">ClassId</Parameter>
        <Parameter id="parameterName3">subclassIds</Parameter>
        <Parameter id="payloadKeyName3">SubClassId</Parameter>
    </Parameters>
</Item>
```

The DVTContextAwareReportFlow wrapper task flow enables a report to listen to contextual events generated by prompt regions.

Note the pairs of parameterNameN and payloadKeyNameN registered in the <Parameters> section for the report task flow BottomSellerFlow. A pair of parameter name and payload key name tells the framework what prompt value is mapped to a specific report parameter. From the example above, parameterName1 is specified as "departmentIds" and payloadKeyName1 as "departmentIds". This means the following:

- There is a task flow parameter for the BottomSellerFlow called "departmentIds"
- When the user changes the value of the department ID in the prompt region, the system will generate a contextual event with the new department value stored as reference "DepartmentId".
- The report is context aware (as indicated by the wrapper task flow - DVTContextAwareReportFlow). When the report detects the contextual event, the framework will get the new department ID value from the payload by using the key "DepartmentId", use it to update the BottomSellerFlow task flow's "departmentId" parameter, and refresh the report region.

Adding or Replacing a Report in an Included Dashboard

This section discusses the steps needed to add or replace a report on an included dashboard.

1. In the Settings Menu, click on the Dashboard folder and then click on the name of the Dashboard.
2. Note the new report's task flow URL and parameters.
3. Modify the Dashboard Prompt Configuration XML file to add an item or replace an existing item for the new report.
4. If the report has to refresh when a prompt on the dashboard is changed by the user, make sure that report task flow is wrapped in a DVTContextAwareTaskFlow for its item entry in the dashboard prompt configuration XML file.
5. Test the Dashboard.

Removing a Report from an Included Dashboard

This section discusses the steps needed to remove a report from an included dashboard.

1. In the Settings Menu, click on the Dashboard folder and then click on the name of the Dashboard.
2. Modify the dashboard prompt configuration XML file and remove the report. You may need to readjust the position of the other reports.
3. Test the Dashboard.

Change the Layout Of an Included Dashboard

This section discusses the steps needed to change the layout of the reports in included dashboards.

1. In the Settings Menu, click on the Dashboard folder and then click on the name of the Dashboard.

2. Modify the dashboard prompt configuration XML file and rearrange the position of the item entries. Save the dashboard configuration file.
3. Reopen and test the Dashboard.

Reports

The Reports link displays the list of contextual reports in the application. When a report name is clicked, it opens the contextual report customization screen in an application tab. The reports can be added, modified or removed from the contextual area. The reports layout can also be changed by using the reports customization screen.

Figure 4–18 Reports List

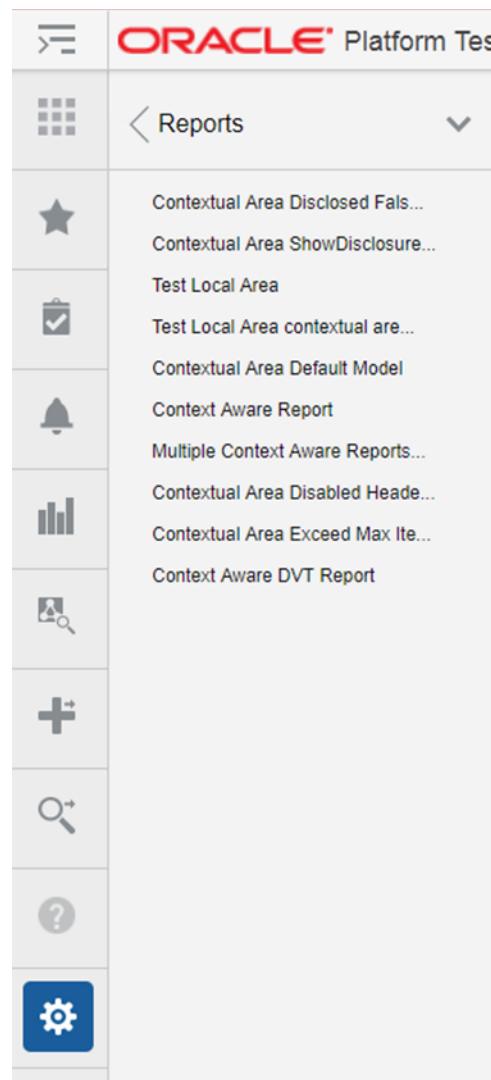
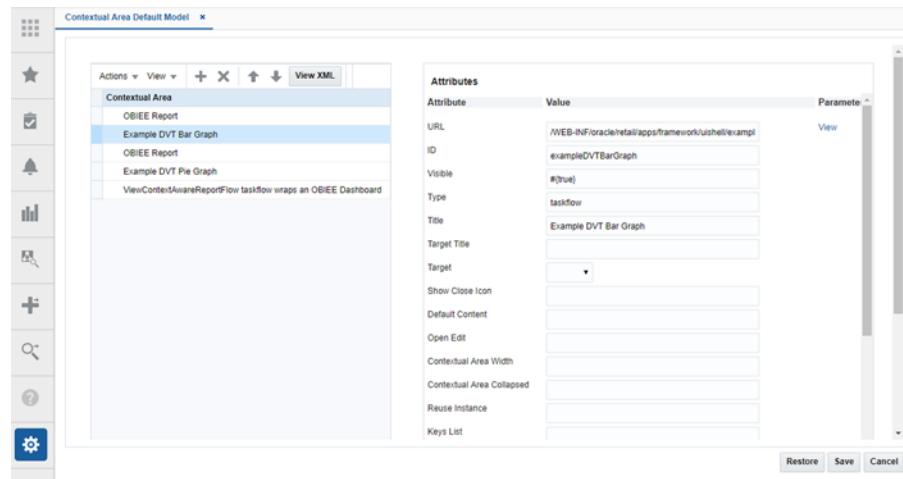
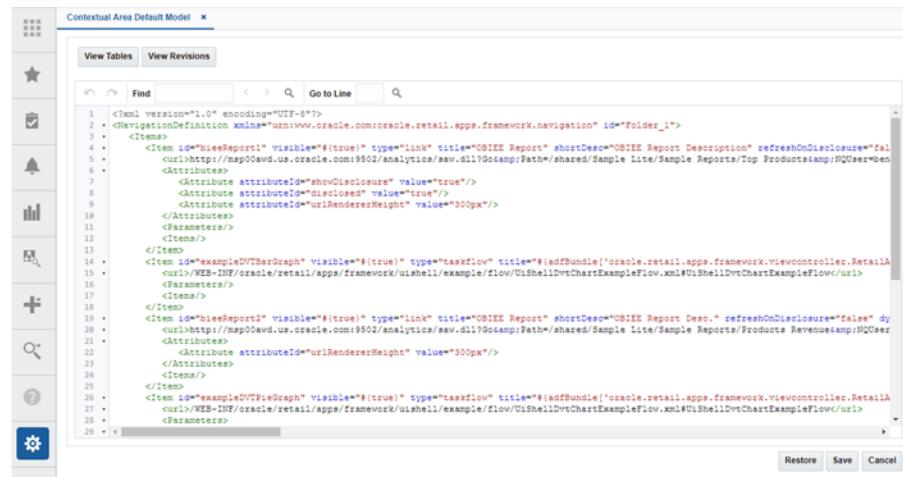


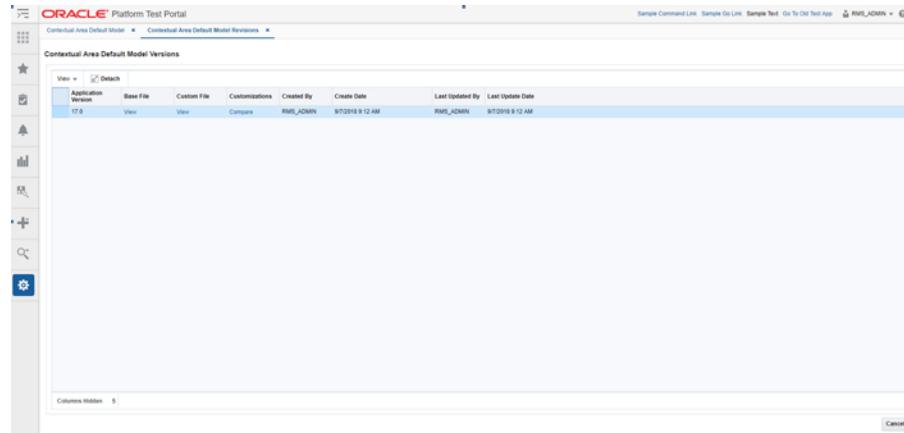
Figure 4–19 Reports Customization Screen

The Reports customization tab displays buttons to save, restore or cancel the changes. The Save button saves the changes to the contextual area reports. The report customization changes are not immediately reflected in the report. The contextual area tab should be closed and reopened for the customization changes to be applied. The Cancel button closes the tab without saving the changes. The Restore button replaces the customized report with the original report shipped with the Retail Application.

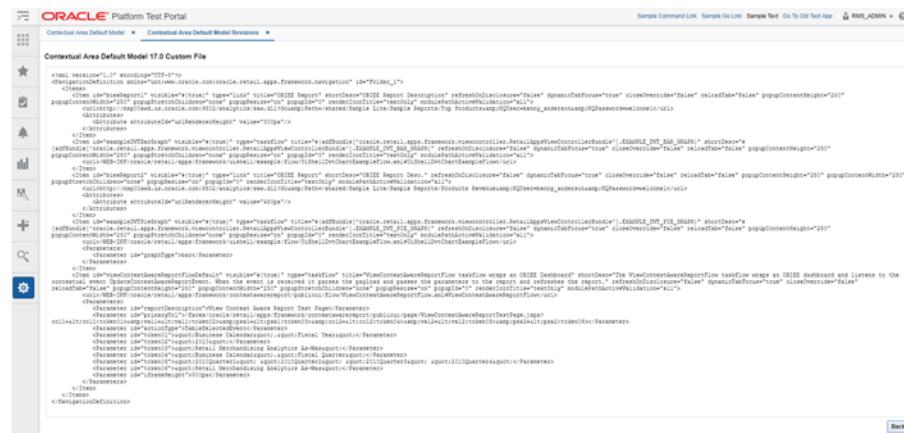
The administrator can also click on the 'View XML' button to view the xml version of the contextual area model file. The View XML button opens the contextual area model file in an XML editor. The XML View contains a 'View Tables' button which takes the user back to the tables view.

Figure 4–20 Contextual Area Customization XML

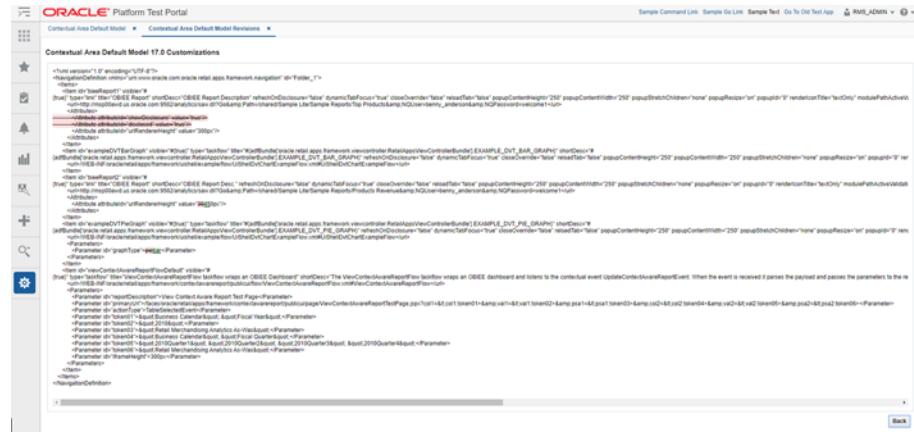
Note that the changes done to the reports are lost after an upgrade of the application. The user should manually reapply the changes after the upgrade. The 'View Revisions' button on the Reports XML screen displays all the prior revisions of the report.

Figure 4–21 Reports Revisions List

The user can choose a version of the application to view the base and customized contextual area reports model file for that version.

Figure 4–22 Reports Custom File

The user can also compare the two files to view their customizations.

Figure 4–23 Reports Customizations

Reports Customization

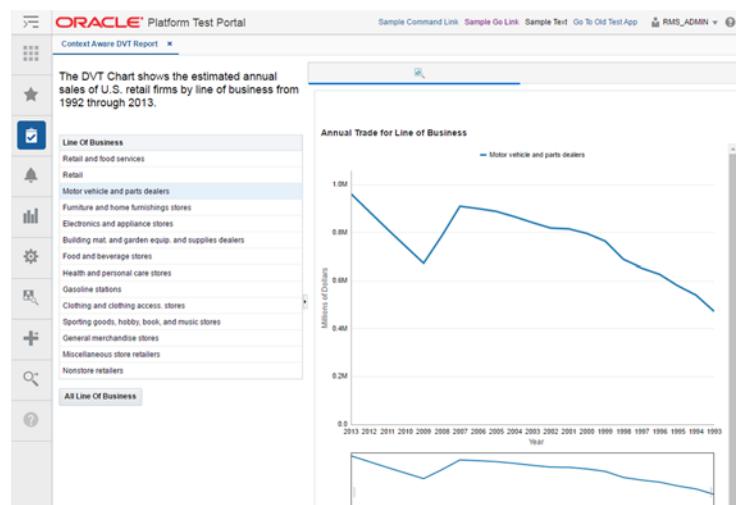
Contextual Reports are reports that appear in a task flow's contextual area section. Contextual Area is a collapsible section to the right of the local area that provides a space to present information that can assist users in completing their tasks.

Since, the information presented in the contextual area is dependent on the task or workflow the user is on, contextual areas are associated to task flows and there can be only one contextual area per task flow.

Within a contextual area - multiple contextual reports can be configured.

Each contextual report can change its contents depending on the action being performed in the user's current workflow.

For example, in the screenshot below, as the user selects the line of business from the table, the line chart will show the annual trade for the selected line of business.

Figure 4–24 Contextual Area Example

Each task flow publishes contextual business events on key activities happening in the screen. Contextual reports can listen to those events and change its content depending on the payload information associated with the event.

Contextual reports can either be ADF based DVT reports or can be maintained in a separate BI reporting tool. The ADF based DVT reports are ADF taskflows, which are built using the ADF Data Visualization components. The reports maintained in an external reporting tool are URLs accessible in a web browser via a URL. Oracle Retail recommends using Oracle Business Intelligence Enterprise Edition (Oracle BI EE) for an external reporting tool.

The contextual reports are added into a Retail Application by modifying the task flow's contextual area model XML file.

Adding a URL based Contextual Report

Adding a contextual report to a task flow entails the modification of the task flow's Contextual Area Model XML file. Multiple reports can be added to the model. Each report is rendered in a collapsible panel box.

Before adding a URL based contextual report, the retailer must have:

- Obtained information about the Retail Application's list of contextual business events that can be broadcast from various workflows. Please refer to the application operations guide for the list of business events.
- Created one or more contextual BI reports in the BI reporting tool (e.g. Oracle BI EE).
- The web URL for each report must be available in order to proceed with the steps in this section.
- Any parameters to configure the content of the report must be known and should be accessible as parameters to the dashboard's URL.

Once the above pre-requisites have been satisfied, proceed with the following steps:

1. In the Settings Menu, click on the Contextual Area folder and then click on the Contextual Area taskflow name.
2. This will open the taskflow's contextual area model xml file.
3. Add an `<Item>` element within the topmost `<Items>` element that references the task flow called `ViewContextAwareReportFlow`. The `ViewContextAwareReportFlow` is a framework for rendering URL based reports that will be aware of contextual business events emanating from the Retail Application task flows.
4. Make sure that the `<Item>` id is unique. Make sure the `<Item>` type is "taskflow". Provide a meaningful title.
5. Populate the parameters to the `ViewContextAwareReportFlow` by adding the following `<Parameter>/<Parameters>` elements.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NavigationDefinition ... >
    <Items>

        <Item id="showCustomerMetric"
              type="taskflow"
              title="Customer Metric">
            <url>
                /WEB-INF/oracle/retail/apps/framework/contextawarereport/publicui/flow/ViewCont
                extAwareReportFlow.xml#ViewContextAwareReportFlow
            </url>
        </Item>
    </Items>
</NavigationDefinition>

```

```

        <Parameter id="reportDescription">Item Metric</Parameter>
        <Parameter
    id="actionType">AllocMaintItemSelectedEvent</Parameter>
        <Parameter id="primaryUrl">
<![CDATA[/faces/oracle/retail/apps/framework/contextawarereport/publicui/page/V
iewContextAwareReportTestPage.jspx?paramItemId=<selectedItemId>&paramItemType=<
selectedItemType:token01>&paramLanguage=<language>]]>
        </Parameter>
        <Parameter id="token01">regular</Parameter>
    </Parameters>

</Item>

</Items>
</NavigationDefinition>

```

Note the following:

- The <Parameter id="reportDescription"> element is the title of the contextual area report. Set this to a meaningful value.
 - The <Parameter id="actionType"> element indicates the contextual business event name the report will listen to.
 - The <Parameter id="primaryUrl"> element indicates the URL to the contextual area report in the BI server. The entire URL must be marked as character data (e.g. enclosed in CDATA). Note that the parameters to the URL are tokenized. The example above uses a test page called ViewContextAwareReportTestPage.jspx which can be replaced with the actual report URL.
 - The "paramItemId=<selectedItemId>" portion of the URL instructs the system to pass the contextual business event payload value called selectedItemId into the URL parameter paramItemId when rendering the contextual report.
 - The "paramItemType=<selectedItemType:token01>" portion of the URL instructs the system to pass the contextual business event payload value called selectedItemType into the URL parameter paramItemType when rendering the contextual report. If that payload value is empty or null at runtime, then a default value of regular is used as referenced in a <Parameter id="token01"> entry. The colon symbol separates the payload value from the default value if the payload value is null.
 - The "paramLanguage=<language>" portion of the URL instructs the system about the current locale of the user. The "language" identifier is a reference to a value in the contextual event payload. This is a built-in value that all Retail Application contextual business event payloads will have.
 - The <Parameter id="token01"> element holds the default value for the URL parameter selectedItemType. Token parameters hold default values and you can define up to 20 default value tokens.
6. Test the Retail Application. Go to the flow where the report was added and verify that the report is rendered correctly.

Adding a DVT Taskflow based Contextual Report

Before adding a DVT taskflow based contextual report, the retailer must have:

- Obtained information about the Retail Application's list of contextual business events that can be broadcast from various workflows. Please refer to the application operations guide for the list of business events.

- Created one or more taskflows using the ADF DVT components. Any parameters to configure the content of the report must be known and should be accessible as taskflow parameters.

Once the above prerequisites have been satisfied, proceed with the following steps:

1. In the Settings Menu, click on the Contextual Area folder and then click on the Contextual Area taskflow name.
2. This will open the taskflow's contextual area model xml file.
3. Add an `<Item>` element within the topmost `<Items>` element that references the task flow called `DVTContextAwareReportFlow`. The `DVTContextAwareReportFlow` is a framework for rendering ADF DVT based reports that will be aware of contextual business events emanating from the Retail Application task flows.
4. Make sure that the `<Item>` id is unique. Make sure the `<Item>` type is "taskflow". Provide a meaningful title.
5. Populate the parameters to the `DVTContextAwareReportFlow` by adding the following `<Parameter>/<Parameters>` elements.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NavigationDefinition ... >
    <Items>

        <Item id="showCustomerMetric"
              type="taskflow"
              title="Customer Metric">
            <url>
/WEB-INF/oracle/retail/apps/framework/dvtcontextawarereport/publicui/flow/DVTCO
ntextAwareReportFlow.xml#DVTContextAwareReportFlow
            </url>
            <Parameters>
                <Parameter
id="taskflowURL">/WEB-INF/oracle/retail/apps/framework/uishell/navigation/conte
xtualarea/flow/ItemMetricFlow.xml#ItemMetricFlow</Parameter>
                <Parameter id="parameterName1">itemId</Parameter>
                <Parameter id="payloadKeyName1">ItemId</Parameter>
                <Parameter
id="parameterValue1">#{payload.valueMap['ItemId']}</Parameter>
                <Parameter id="refreshOnDisclosure">#{true}</Parameter>
            </Parameters>
        </Item>

    </Items>
</NavigationDefinition>

```

Note the following:

- The `<Parameter id="taskflowURL">` element is the URL of the DVT taskflow that will be displayed in the contextual area.
- The `<Parameter id="parameterName1">` element indicates a parameter for the DVT taskflow. A maximum of 15 parameters can be specified.
- The `<Parameter id="payloadKeyName1">` element indicates the name of the payload key that maps to the taskflow parameter `parameterName1`. A maximum of 15 payload keys can be specified. The value of the payload key in the event payload will be used for the parameter in the DVT taskflow.
- The `<Parameter id="parameterValue1">` element holds the default value of the DVT taskflow. A maximum of 15 parameter values can be specified.

- The <Parameter id="refreshOnDisclosure"> element is used to refresh the DVT taskflow on the disclosure of the tab.
6. Test the Retail Application. Go to the flow where the report was added and verify that the report is rendered correctly.

Notifications

From the RAAC left hand navigation menu, the user can access the Manage Notifications link. The Manage Notifications tab displays the Manage Notifications table. This table is laid out using a master table and a detail table. The master table consists of Notification Types and the detail table consists of Notification Groups and Roles associated with the notification types.

Figure 4–25 Notifications Screen

Name	Retention Days	Type Code	Description	Email Address
Calculated	Undefined	CALCULATED	Calculated Allocation	
Error	Undefined	ERROR	Error in Calculation	

Name	Description
BUYERS_GROUP_RAFTEST	Meant for Buyer

Notification Types

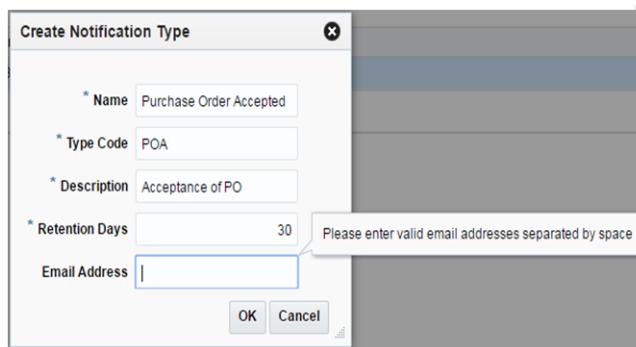
Notification Types drive how users are notified about the result of their action. This result can be communicated to one user or a group of users based on the job roles.

Add

The Add action is enabled at all times and allows you to add a new notification type.

Add a Notification Type

1. From the Actions menu, select Add. The Create Notification Type dialog is displayed.

Figure 4–26 Create Notification Type Dialog

2. Each notification type requires the following information:

- Name – The name of the notification type
- Type Code – A meaningful name to identify the notification type
The type code provides applications a way to uniquely identify a notification type.
- Description – The description of the notification type
- Retention Days – The number of days a notification of this type should be retained

The reason for capturing Retention Days information at Notification Type level itself, is that it gives users the flexibility to delete certain Types of notifications quickly without cluttering notification views. To retain records infinitely, this value should be set to -1.

Note: Administrators are discouraged from using '-1' for Retention Days as associated notifications will never be purged automatically. Only a system administrator can delete those manually through a sql script or direct row deletes through a sql tool.

Note: Retention Days cannot be set to zero.

- Email Address - Email addresses that must be notified in case a notification of this type is created. Multiple email addresses may be provided here, separated by blank space. This is an optional field, and can be skipped.

Note: To be able to send emails for notifications, the Retail Alert Manager application must be deployed.

3. Click OK to create the new notification type.

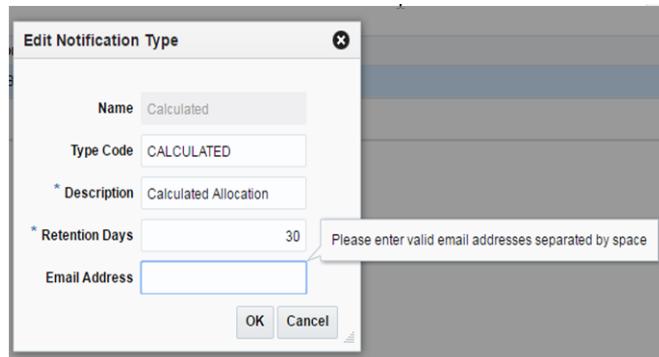
Edit

The Edit action is enabled when a notification type is selected. The Edit action is used to add or modify the description and retention days of an existing notification type.

Edit a Notification Type

1. Select the notification type you want to edit.
2. From the Actions menu, select Edit. The Edit Duty Role dialog is displayed.

Figure 4–27 Edit Notification Type Dialog



3. Modify the type code, description, retention days or associated email addresses of the notification type and click OK.

Delete

The Delete action is enabled when you select a notification type that can be deleted from the database.

Deleting a notification type removes the notification type and all of the notification type's associated roles and groups. Any past notifications are also removed in order to maintain data integrity.

Delete a Notification Type

1. Select the notification type you want to delete.
2. From the Actions menu, select Delete. The Confirm dialog is displayed.

Figure 4–28 Delete Notification Type Confirmation Dialog



3. Click OK to delete the selected notification type.

Export to Excel

The Export to Excel action is enabled whenever you have the Manage Notifications window open. This action allows you to export the Notification Types list to a Microsoft Excel spreadsheet.

Notification Groups and Roles

The Notification Groups and Roles table consists of all the roles associated with a notification type master record. If there are no records associated with the notification type then a "no data to display" message appears in the Notification Groups and Roles table when the notification type is selected in the Notification Types table.

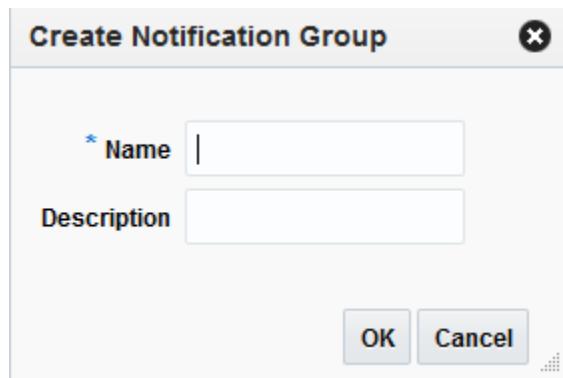
Create/Add Notification Group

The Create action is enabled at all times when a notification type is selected and allows you to create a new notification group associated with the selected notification type.

Create a Notification Group

- From the Actions menu, select Create (or Add Notification Groups). The Create Notification Group dialog is displayed.

Figure 4–29 Create Notification Group Dialog



- Enter a name and (optionally) a description of the group.
- Click OK to create the new notification group.

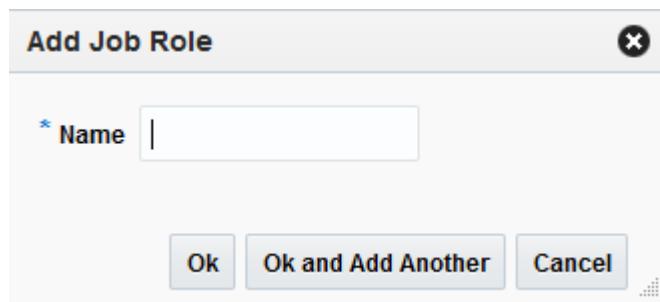
Add Job Role

Once a notification group is created, you can add job roles that apply to the selected group.

Add a Job Role

- From the Actions menu, select Add job Role. The Add Job Role dialog is displayed.

Figure 4–30 Create Job Role Dialog



2. Enter a name for the job role.
3. Click OK to create the new job role or OK and Add Another to create additional job roles.

Upon clicking OK or OK and Add Another, the New name is validated. The validation checks for a valid name in the enterprise security solution of the retailer. If it finds a match, then it allows the user to proceed. If the name is not valid, an error is displayed.

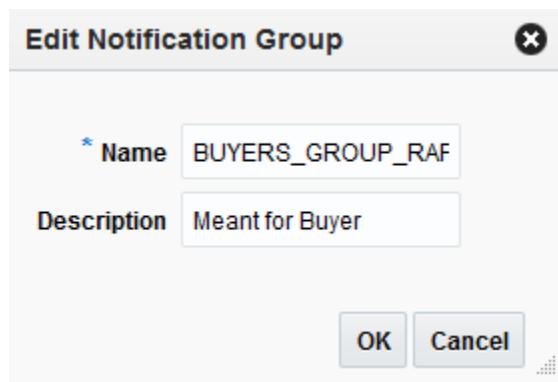
Edit

The Edit action is enabled when a notification group or job role is selected. The Edit action is used to modify the name and description of an existing notification group or job role.

Edit a Notification Group

1. Select the notification group or job role you want to edit.
2. From the Actions menu, select Edit. The Edit Notification Group (or Edit Job Role) dialog is displayed.

Figure 4–31 Edit Notification Group Dialog



3. Modify the notification group or job role attributes and click OK.

Upon clicking OK, the New name is validated. The validation checks for a valid name in the enterprise security solution of the retailer. If it finds a match, then it allows the user to proceed. If the name is not valid, an error is displayed.

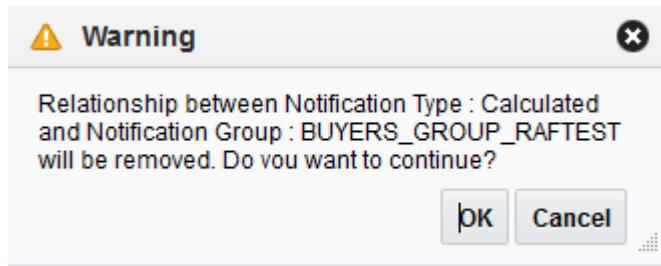
Delete

The Delete action is enabled when you select a notification group or job role that can be deleted from the database.

Deleting a notification type removes the notification type and all of the notification type's associated roles and groups. Any past notifications are also removed in order to maintain data integrity.

Delete a Notification Type

1. Select the notification type you want to delete.
2. From the Actions menu, select Delete. The Confirm dialog is displayed.

Figure 4–32 Delete Notification Group Confirmation Dialog

3. Click OK to delete the selected notification group or job role.

Export to Excel

The Export to Excel action is enabled whenever you have the Manage Notifications window open. This action allows you to export the Notification Groups and Roles list to a Microsoft Excel spreadsheet.

Resource Bundles

All Oracle Retail applications come packaged with resource bundles, files that contain text resources. These text resources appear throughout the Oracle Retail application as instructions, messages, labels, errors, virtually any text that appears in the application comes from a resource bundle.

Many Oracle Retail applications support the ability for retailers to customize the text that appears in the Oracle Retail application to better match that retailer's business language. The capability to change the text for a resource is provided through the Resource Bundles area of RAAC. Retailers can customize text resources for any Oracle Retail supported language.

Resources and Customizations Explained

All text resources in the Oracle Retail application have the following values:

- **Base Application Code** – This value identifies the Oracle Retail application that owns this text resource.
- **Language** – This value identifies the language of the text resource.
- **Bundle** – This value identifies the bundle file where this text resource resides.
- **Resource** – This value is the unique name that can be used to get the text for this resource.
- **Base Text** – This value is the text provided by the Oracle Retail application. This is the text that will appear in the application by default.

Every text resource in Oracle Retail applications is uniquely identified by the combination of Application Code, Language, Bundle, and Resource.

A resource customization is a change that a retailer made to the text of a resource. In addition to the values above, customizations also have the following values:

- **Custom Text** – This is the custom text provided by the retailer for the resource.
- **Text** – This is the text that will actually appear in the Oracle Retail application. If a retailer has provided custom text for the resource, then this value will display the retailer's custom text. Otherwise, it will display the base text provided by the Oracle Retail application.

Task Flows

The Resource Bundles area of RAAC consists of the following task flows:

- Resource Text Strings
- Imports Management

Resource Text Strings

From the RAAC left hand navigation menu, the user can access the Resource Text Strings link. The Resource Text Strings screen provides the capability to customize the resources present in the resource bundles in an application. The user can search the resources in the application using the Bundle, Language, Resource, Contains Custom Text, or Text fields.

Figure 4–33 Resource Text Strings Screen

Resource	Base Text	Text	Contains Custom Text	Updated Date	Updated By
ANY	Anyone	Anyone	No		
APPLICATION_CODE	Application Code	Application Code	No		
ASYNC_TASK_APPLICATION_MODULE	Asynchronous Task Application Module	Asynchronous Task Application Module	No		
CRITICAL	Critical	Critical	No		
DESCRIPTION_IS_MANDATORY	Description is Mandatory	Description is Mandatory	No		
REPORT_TYPE	Report Type	Report Type	No		
LOOKUP_CODE_MUST_BE_UNIQUE	The lookup code must be unique	The lookup code must be unique	No		
LOOKUP_CODE_MUST_BE_UNIQUE_FOR	Lookup code must be unique for a lookup type	Lookup code must be unique for a lookup type	No		
LOOKUP_TYPE_MUST_BE_UNIQUE	The lookup type must be unique	The lookup type must be unique	No		
LOOKUP_VALUE_UNIQUE	The lookup type and code must be unique	The lookup type and code must be unique	No		
NORMAL	Normal	Normal	No		
RETAIL_APP_CMR_CMRL_SELECTION	RE	RE	No		
RETAIL_APP_CMR_CMRL_SELECTION	RE	RE	No		
RETAIL_APP_CMRL_SELECTION	A record with the value [RE]_CMRL_SELECTION already exists. Enter a unique val	A record with the value [RE]_CMRL_SELECTION already exists. Enter a unique val	No		
RETAIL_APP_CMRL_SELECTION	RE	RE	No		
RETAIL_APP_CMRL_SELECTION	The value of the attribute ATTRIBUTE_NAME is not valid. A valid value	The value of the attribute ATTRIBUTE_NAME is not valid. A valid value	No		
RETAIL_APP_CMRL_SELECTION	Users attempt to update a record correctly in use but cannot, with the exception they will be able do so soon.	Users attempt to update a record correctly in use but cannot, with the exception they will be able do so soon.	No		

The results table in the Resource Text Strings screen will display the Resource, Base Text, Text, Contains Custom Text, Updated Date, and Updated By columns for the resources matching the entered search criteria. If there is a custom value present for a resource, it will be displayed in the Text column along with the date and the user who customized that entry. The Contains Custom Text column will display Yes if a custom value is present for a resource. If there is no custom value present for a resource, the Text column will display the base text and the Updated Date and Updated By columns will be displayed empty. The Contains Custom Text column will display No in this scenario. The user can view, add, edit, or remove custom text for a resource using this screen.

The user can also export the results table to an Excel CSV file, or import an Excel CSV file with customized resources using this screen. The export and import actions allow the user to provide custom text for many resources at one time, and upload all the custom values in a single action in RAAC.

Figure 4–34 View, Add, Edit or Remove Custom Text

Actions ▾	View ▾	Format ▾					
Edit View Remove Customization Copy							

Base Text
Anyone

View

The user can view a resource, base text and custom text using the View menu item or the binoculars icon. The View option opens up a popup showing the resource, its base text and custom text. Only one record can be viewed at a time in a popup. If more than one record or no record is selected, a warning is displayed to the user.

Figure 4–35 View Resource Text



Add or Edit

The user can add or edit the custom text for a resource using the Edit menu item or the pencil icon. If no custom text is present for a resource, a new custom text will be added. If a custom text is already present for a resource, it will be modified. The Updated Date and Updated By columns will be changed to reflect the addition or modification. The Edit option opens up a popup showing the resource, its base text and editable custom text. Only one record can be edited at a time in a popup. If more than one record or no record is selected, a warning is displayed to the user. The Edit popup can also be opened by double clicking a record on the results table.

Figure 4–36 Edit Resource Text



Remove Customization

The user can remove the custom text for one, many or all the selected resources using the Remove Customization menu item or the cross icon. The user can select a single or multiple records and remove custom values for the records. The Remove Customization option will give a confirmation warning message before the custom text is removed for the selected records. The base text is not impacted by the Remove Customization operation.

Figure 4–37 Delete Custom Text Confirmation Dialog



Export to CSV

The user can export the details of the resources from the results table to an Excel CSV file. When the user selects the Export to CSV action, the browser will perform its download behavior. Depending on the user's browser preferences, the browser may prompt the user asking whether the exported file should be opened or saved, what program should be used to open the file, or where on the user's computer the file should be saved.

Import CSV File

See [Importing Customizations from a CSV File](#) for more details.

Importing Customizations from a CSV File

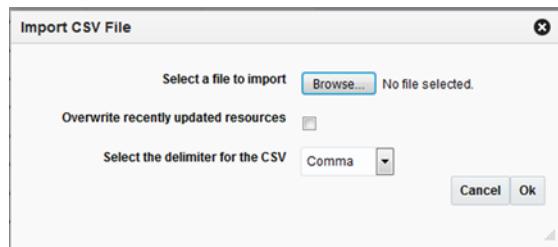
The user can change the values in the Text column of an exported CSV, and then import the CSV file. When the user does this, the values of the Text column are imported into the custom text of each newly customized resource. The user can customize multiple rows with a single action by importing a file which contains multiple customized rows. Importing a file that has not been modified will do nothing, since the text for each resource is already exactly the same in RAAC the Oracle Retail application.

The imported file must meet the following assumptions for the import to succeed:

- The imported file must be a well-formed CSV file. The user can use any compatible program to edit the exported CSV file, as long as the program is able to read the CSV file and save it again in CSV format.
- The user should only edit values in the Text column. If the user edits any of the values in the Base Application Code, Language, Bundle, or Resource columns, the import may fail, or invalid customizations may be created.
- The user can only add or edit customizations in the import. The user cannot remove customizations using import. Deleting the contents of the Text field or copying the Source Text into the Text field will cause the row to be ignored.
- The size of the imported file is limited to 2000 KB. Users will not be allowed to upload a file larger than this.

When the user selects the Import CSV file action, a popup opens prompting the user to select a file to import.

Figure 4–38 Import CSV File Dialog



It is possible that, after a user exports resources to a CSV file, but before the user imports the file into RAAC, another user may go to RAAC and customize one or more of the exported resources. In this case, the values of resources in RAAC would be newer than the values in the exported file. In order to ensure that an import does not inadvertently overwrite these values, the import action will skip resources that have

been recently updated in RAAC, and notify the user. The user can tell the import to instead use the values from the imported file by selecting the "Overwrite recently updated resources" checkbox on the import popup.

Lookups

Lookup records in Oracle Retail Applications represent items that users can select in dropdown and list-of-value inputs in application screens. Examples include:

- Location Types (warehouse or store)
- Clearance Status (worksheet, submitted, rejected, approved, etc)
- Markup Types (cost or retail)

These lookups are stored in the database tables RTC_LOOKUP_TYPES_B and RTC_LOOKUP_VALUES_B.

Administrators can customize these lookups through the Oracle Retail Application's Settings menu.

From the Settings menu, the user can access the Manage Lookups screen under the Administration submenu. This feature is not accessible from the RAAC left hand navigation menu since it is packaged with the application itself rather than the RAAC application. The Manage Lookups screen displays the lookup types and their associated lookup values for the Retail Application. The Manage Lookups screen shows information about the lookup types and values such as the Lookup Code, Meaning, Description, System flag, and for the Lookup Value only - an Enabled flag. Users are also able to create, update, delete, cancel, and save changes made to the lookup types and values.

Figure 4-39 Lookups Screen

Lookup Type Code	Meaning	Description	System
ALLOC_STATUS	Allocation record status	The set of valid status an allocation record can be on at any given time.	No

Lookup Value Code	Meaning	Description	Enabled	System
A	Approved	The allocation record has been approved	Yes	No
C	Calculation	The allocation record is being processed in the system.	Yes	No

Add

The user can add a lookup type by clicking on the Add menu item or the Add icon of the Lookup Type table toolbar. The user can enter the lookup type's Code, Meaning, and Description. The system column is non-editable and will always be set to No when a user creates a new record. Lookup Types must be unique, so if a user enters an already existing Lookup Type Code, an error message will display.

Figure 4–40 Add Lookup Type Screen

Lookup Type Code	Meaning	Description
ALLOC_STATUS	Allocation record status	The set of valid status an allocation record can be on at any given time.
CUSTOM_TYPE	Custom Type	This is a custom lookup type.

To associate a lookup value with the lookup type, the user can click on the Add menu item or the Add icon of the Lookup Values table toolbar. The user can enter the lookup value's Code, Meaning, Description, and Enabled flag. The system flag is also non-editable.

Figure 4–41 Add Lookup Value Screen

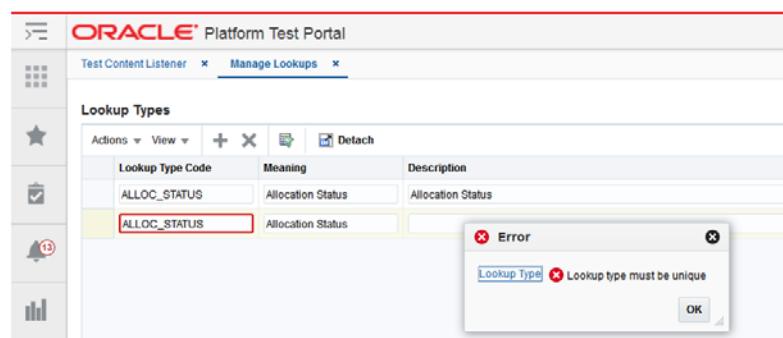
Lookup Value Code	Meaning	Description
C	Custom	This is a custom lookup value.

Edit

The Lookup Types and Lookup Value tables are editable so the user can readily update the records. All columns are editable except for the system column. The Lookup Code, however, cannot be edited if it is a system record.

If a lookup type or lookup value is a System record, the user will not be able to update the lookup code for that record.

Lookup code must be unique, so if a user updates to an already existing Lookup Type or Lookup Value Code, an error message will display.

Figure 4–42 Edit Lookup Type (Existing Lookup Code)

Delete

The user can delete a lookup type or lookup value by clicking on the Delete menu item or the Delete icon of the Lookup table toolbar. To delete a lookup type or lookup value,

the user should select a record then click either the Delete menu item or the Delete icon.

The Delete function is applicable only to Non-System records. When a user selects a system record, the Delete menu item and the Delete icon are disabled.

Figure 4–43 Delete Lookup Type

Lookup Types			
Actions	View	+	X
			Detach
Lookup Type Code	Meaning	Description	System
ALLOC_STATUS	Allocation record status	The set of valid status an allocation record can be on at any given time.	No
CUSTOM_TYPE	Custom Type	This is a custom lookup type.	No

Figure 4–44 Delete Lookup Type (Disabled Delete Button on System Records)

Lookup Types			
Actions	View	+	X
			Detach
Lookup Type Code	Meaning	Description	System
ALLOC_STATUS	Allocation record status	The set of valid status an allocation record can be on at any given time.	Yes
CUSTOM_TYPE	Custom Type	This is a custom lookup type.	No

Figure 4–45 Delete Lookup Value

Lookup Values					
Actions	View	+	X	Detach	
Lookup Value Code	Meaning	Description	Enabled	System	
C	Custom	This is a custom lookup value.	Yes	No	

Figure 4–46 Delete Lookup Value (Disabled Delete Button on System Records)

Lookup Values					
Actions	View	+	X	Detach	
Lookup Value Code	Meaning	Description	Enabled	System	
A	Approved	The allocation record has been approved.	Yes	Yes	
C	Calculation	The allocation record is being processed in the system.	Yes	No	

Save / Cancel

Save and Cancel buttons are also available to commit and rollback the changes made to the records. These buttons are located at the bottom right section of the Manage Lookups screen.

The user can save changes made to both the lookup types and lookup values tables using the Save button. All changes made using the screen's Add, Edit, and Delete functions will take effect once the user clicks on the Save button.

The user may also use the cancel button to undo changes made to both the lookup types and lookup value tables. However, the Cancel button may only undo changes that have not yet been saved. All previously saved changes may not be undone using the Cancel button.

Clicking on the Cancel button also closes the Manage Lookups screen after the rollback is complete.

Asynchronous Tasks

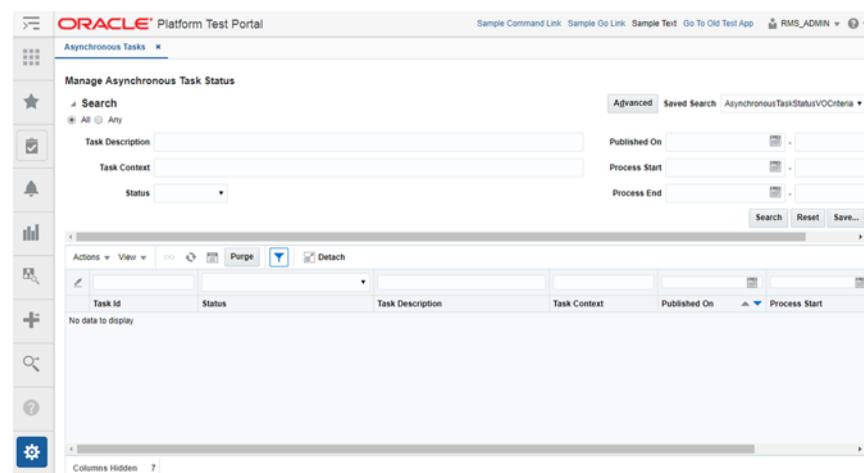
Asynchronous tasks are background processes launched by users of Oracle Retail Applications. An example of a background process is the calculation of allocations.

Each asynchronous task is logged in the database table called RAF_ASYNC_TASKS.

Administrators can view the latest status of asynchronous tasks through the Manage Asynchronous Task Status function from the Oracle Retail Application's Settings menu.

The user can access the Manage Asynchronous Task Status function from the Administration submenu under the Settings menu. This feature is not accessible from the RAAC left hand navigation menu since it is packaged with the application itself rather than the RAAC application. The Manage Resource Asynchronous Task Status screen displays the Asynchronous Task records. Users are able to search for a certain asynchronous task and view a task. Users are also able to purge asynchronous tasks present in the system.

Figure 4–47 Asynchronous Tasks Screen

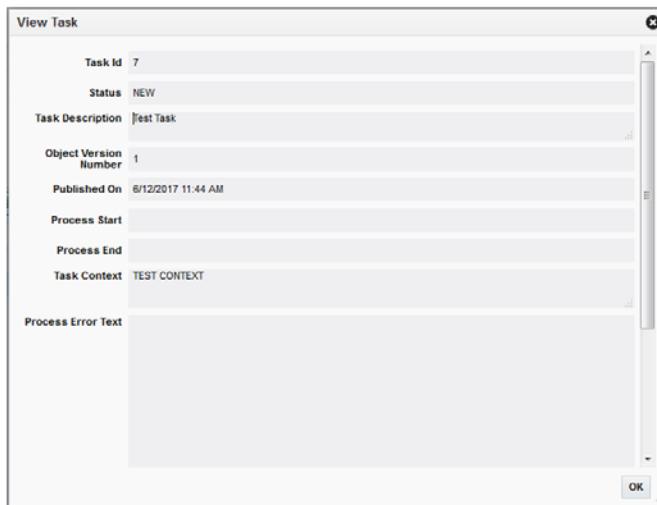


View

The user can view additional details for the selected asynchronous task by clicking on the View Actions menu item or the View icon of the table toolbar. The View option opens up a popup showing additional details for the selected asynchronous task. Only one record can be viewed at a time in a popup.

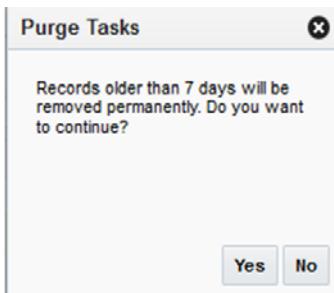
Figure 4–48 Action Menu



Figure 4–49 View Additional Details

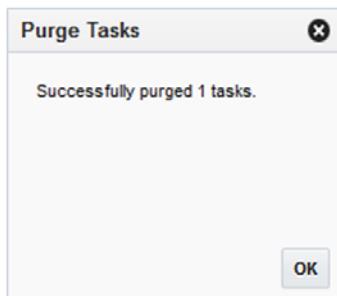
Purge Task

The user can purge asynchronous task records in the system. The number of days is defined in the `async.task.purge.retention.days` property which can be updated through the Manage Application Properties feature described above in this chapter. The Purge can be invoked through the table toolbar Purge button or Purge Actions menu item.

Figure 4–50 Purge Tasks Dialog

When the Purge action is complete, a popup will appear showing the number of purged asynchronous task records

Figure 4–51 Purge Tasks Success Dialog



Export to Excel

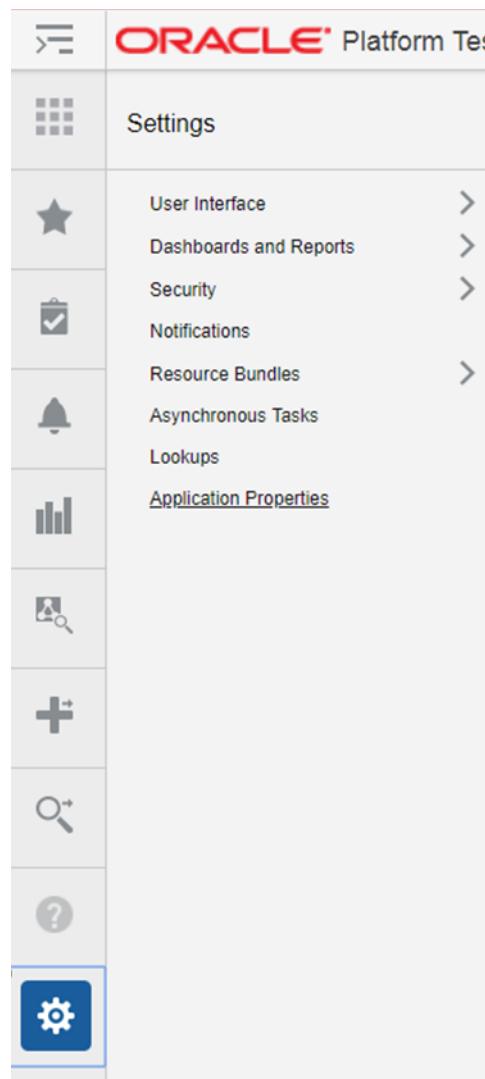
The Export to Excel action is enabled whenever Asynchronous Task records are present in the table. This action allows the user to export the Asynchronous Task records to a Microsoft Excel spreadsheet.

Application Properties

Configuration properties are key-value pairs recognized by Retail Applications during runtime to control application behavior. For instance, a property may exist to turn off certain features within the application.

Administrators of Retail Applications can access the Application Properties screen from the Settings menu to view and edit configuration properties.

Figure 4–52 Application Properties Settings Menu



The Application Properties screen allows administrators to search for configuration properties by deployment (a required criteria). Properties can also be searched by keywords against key names and descriptions.

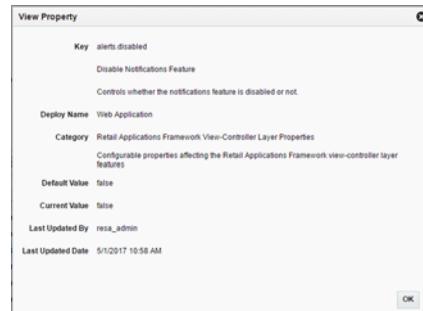
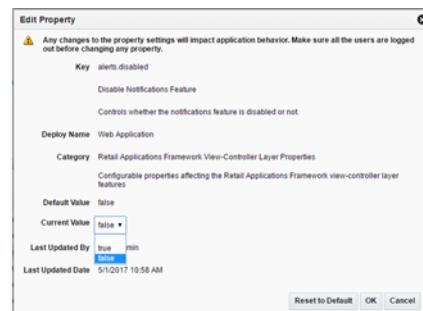
Figure 4–53 Application Properties Query Panel

The screenshot shows a table of application properties. The columns are Deploy Name, Key Name, Key, Current Value, Default Value, Deployment Restart, and Key. The rows show various properties like alerts.application.code, alerts.chunk.size, alerts.disabled, etc.

Deploy Name	Key Name	Key	Current Value	Default Value	Deployment Restart	Key
Web Application	Alerts Application Code	alerts.application.code	RATTEST	No	Yes	The
Web Application	Alerts Chunk Size	alerts.chunk.size	30	No	No	The
Web Application	Disable Notifications Feature	alerts.disabled	false	No	No	Conf
Web Application	Force One Instance of Alert Manager	alerts.force.register.manager	false	No	No	Set 1
Web Application	Alerts Initial Delay	alerts.initial.delay	1	Yes	Yes	Num
Web Application	Alerts Poll Interval	alerts.poll.interval	600	Yes	Yes	The
Web Application	Alerts Framework Datasource JNDI Name	alerts.retail.datasource.jndi	jdbc/RetailPlatfo...	Yes	Yes	JND
Web Application	Alerts Framework Mail Session JNDI Name	mail/RAFMailsession.jndi	mail/RAFMailsession.jndi	Yes	Yes	JND
Web Application	Alerts Wait Threshold	alerts.wait.threshold	900	No	No	Num

Properties matching the search criteria are displayed in a table from which a user can perform the following actions:

- View details of a property
- Edit a property
- Export properties to CSV

Figure 4–54 Application Properties View Popup**Figure 4–55 Application Properties Edit Popup**

5

Merchandising Data Viewer

Data Viewer is a workspace that provides read-only access to the Merchandising functional data. This extension is a workspace for customer support personnel to view the data. This chapter provides the steps to configure the retailer workspace for the retailer in a cloud environment.

Workspace

A workspace <RETAILER_WORKSPACE> is predefined for the retailer and is where workspace users can view the application data. The workspace has the privilege to the allocated <RETAILER_WORKSPACE_SCHEMA> database schema. The schema has the synonyms with READ ONLY privileges to all the database tables and views except for internal and the tables in the encrypted schema.

Users and Roles

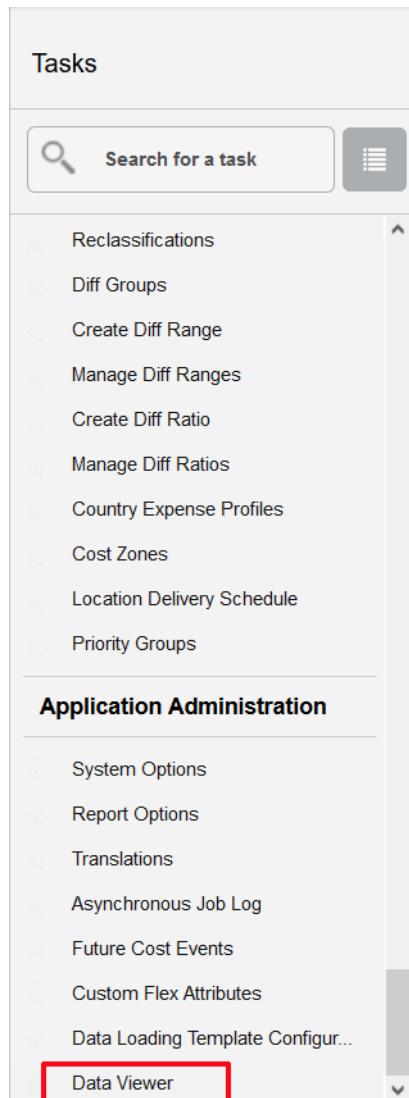
Data Viewer has two types of users, workspace viewer and workspace administrators. As a workspace administrator, you can create and edit workspace viewer accounts, monitor the activities. Before you create an account for the workspace viewer, you must create a user in Identity Cloud Service (IDCS) with the same user name.

Create a Workspace Viewer

Perform the following procedure to create a workspace viewer:

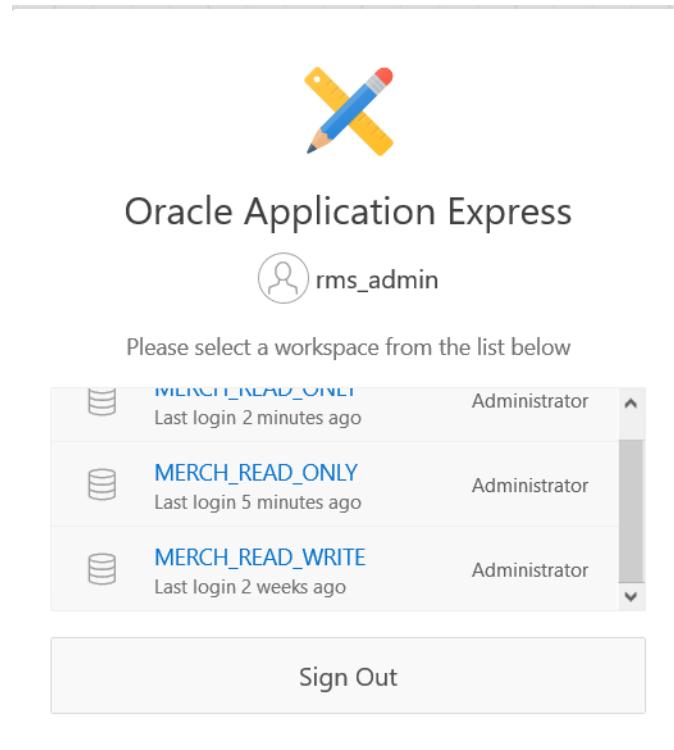
1. Log in to Oracle Retail Merchandising Foundation Cloud Service.
2. From the Tasks list, under Application Administration, select Data Viewer.

Figure 5–1 RMFCS Tasks Menu

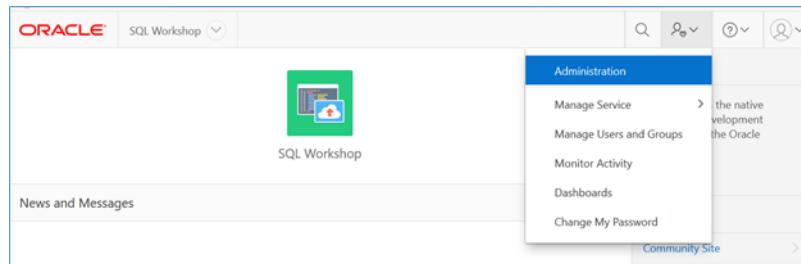


Note: To gain access to the Data Viewer, you need to have access to the newly created duty "VIEW_DATABASE_VIA_APPLICATION_EXPRESS_PRIV" added via ORAAC.

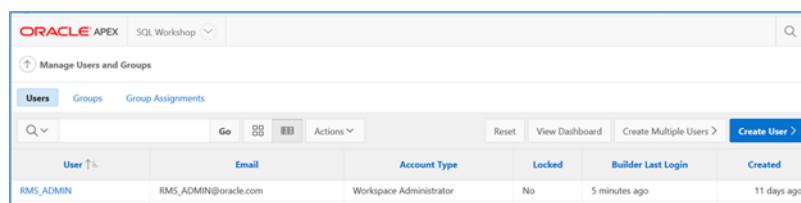
3. Select an associated APEX workspace.

Figure 5–2 APEX Workspace Selection Dialog

- From the Administration drop down menu, select Manage Users and Groups.

Figure 5–3 APEX Administration Drop Down Menu

- From the Manage Users and Groups window, click Create User.

Figure 5–4 Oracle APEX Manage Users and Groups Window

6. From the Oracle APEX Create User window, create a new workspace viewer account and ensure that the default <RETAILER_WORKSPACE_SCHEMA> is assigned.

Figure 5–5 Oracle APEX Create User Window

The screenshot shows the Oracle APEX Create User window. At the top, there are tabs for 'User Identification' (selected), 'Account Privileges', 'Password (For authentication against workspace ...)', and 'Group Assignments'. Below the tabs, the 'User Identification' section contains fields for 'Username' (filled with 'WORKSPACER'), 'Email Address' (filled with 'WORKSPACER@GMAIL.COM'), 'First Name' (filled with 'WORKSPACER'), 'Last Name' (filled with 'WORKSPACER'), and 'Description' (empty). There is also a 'Default Date Format' dropdown. The 'Account Privileges' section includes a 'Default Schema' dropdown set to 'MERCH_READONLY_USER', a 'Accessible Schemas (null for all)' dropdown, and two radio button groups for 'User is a workspace administrator' (set to 'No') and 'User is a developer' (set to 'Yes'). On the right side of the window, there is a sidebar titled 'Users' with descriptive text about user roles and permissions.

7. Assign the new workspace viewer with the following settings:
 - User is a workspace administrator – No
 - User is a developer – Yes
 - App Builder Access – No
 - SQL Workshop Access – Yes
 - Team Development Access – No
 - Set Account Availability – Unlocked
 - Require Change of Password on First Use – No
8. Once all information is entered, click Create User to complete the user creation.