

Oracle® Retail Merchandising Cloud Services

Administration Guide



Release 23.1.301.0

F84045-01

July 2023

ORACLE®

Copyright © 2023, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

Contents

1 Overview

Logging Service Requests (SRs)	1-1
--------------------------------	-----

2 File Transfers

3 Managing User Security

Managing Users in OCI IAM	3-1
Add Groups in OCI IAM	3-1
Add Users in OCI IAM	3-2
Map Groups to Application	3-2
Managing Roles, Duties, and Privileges in the Merchandising Suite	3-3
Manage Duties	3-4
Manage Role Mappings	3-5
Duplicate	3-6
Delete	3-7
Select and Add	3-7
Remap	3-8
Policy Patching	3-8
Copy to Custom	3-9
Sync	3-10
View Permissions	3-10
Overwrite Custom Policies	3-10
Import Custom Policies	3-10
Refresh	3-10
Policy Backups	3-10
Create	3-11
Delete	3-11
Download	3-12
Restore	3-12
Refresh	3-12

4 Manage Data Filtering

Users and Roles	4-2
Adding a User	4-2
Updating a User	4-2
Deleting a Security User	4-3
Managing User Roles	4-3
Uploading Changes	4-3
Security Groups	4-3
Managing Security Groups	4-4
Managing Security Group Translations	4-4
Uploading Changes	4-4
Associate Users to Groups	4-5
Managing Group / User Associations	4-5
Uploading Changes	4-5
Filter Groups	4-6
Managing Group / Organization Associations	4-6
Managing Group / Merchandise Associations	4-6
Uploading Changes	4-7
Associate Locations to Groups	4-7
Create an association between a user group and locations	4-7
Updating an association between a user group and locations	4-8
Deleting an association between a user group and locations	4-8
Uploading Changes	4-8
Order Approval Amount by Role	4-9
Add Order Approval Amounts	4-9
Update Order Approval Amounts	4-9
Delete Role Privileges	4-9
Uploading Changes	4-9

5 Other Settings

Notifications	5-1
Asynchronous Tasks	5-2
Application Properties	5-3
Enabling Attachments	5-3
Enabling Finance Drill to Finance and Reports	5-4
Enabling Slack Integration	5-5
Create a Slack App	5-5
Configure Slack in App Server	5-6
Configure Slack in an Application	5-6
Configuring External Services	5-7

Web Service Configuration	5-7
---------------------------	-----

6 Data Viewer

Workspace	6-1
Users and Roles	6-1
Create a Workspace Viewer	6-1

Preface

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

Audience

This guide is intended for administrators, and describes the administration tasks for Oracle Retail Merchandising Cloud Services.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
<https://support.oracle.com>

When contacting Customer Support, please provide the following:

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

Oracle Help Center (docs.oracle.com)

Oracle Retail Product documentation is available on the following website <https://docs.oracle.com/en/industries/retail/html>

Comments and Suggestions

Please give us feedback about Oracle Retail Help and Guides. You can send an e-mail to: retail-doc_us@oracle.com

Oracle Retail Cloud Services and Business Agility

Oracle Retail Merchandising Cloud Services is hosted in the Oracle Cloud with the security features inherent to Oracle technology and a robust data center classification, providing significant uptime. The Oracle Cloud team is responsible for installing, monitoring, patching, and upgrading retail software.

Included in the service is continuous technical support, access to software feature enhancements, hardware upgrades, and disaster recovery. The Cloud Service model helps to free customer IT resources from the need to perform these tasks, giving retailers greater business agility to respond to changing technologies and to perform more value-added tasks focused on business processes and innovation.

Oracle Retail Software Cloud Service is acquired exclusively through a subscription service (SaaS) model. This shifts funding from a capital investment in software to an operational expense. Subscription-based pricing for retail applications offers flexibility and cost effectiveness.

1

Overview

This document provides a guide to the key tasks of the application administrator of the Merchandising suite of solutions. This includes an overview of file transfers, creating users and assigning them to roles, duties, and privileges, and configuring other features in the solutions.

Logging Service Requests (SRs)

If you have issues that cannot be resolved by consulting this or other Merchandising suite documentation, an SR should be logged with the question. This will allow the requests to be managed through a single point of contact for your environment. This includes activities where you require support from the Oracle Cloud Operations team to complete tasks. The link to use when submitting Service Requests (SR) is:

<https://support.oracle.com>

2

File Transfers

Some of the Merchandising suite integrations involve flat files as inputs or outputs of the process. To support uploading and downloading files in a SaaS implementation, a bucket in Oracle Cloud Infrastructure Object Storage is created for each customer environment.

Oracle Cloud Infrastructure Object Storage service is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. Buckets are logical containers for storing objects. Any type of data, regardless of content type, is stored as an object. An object is composed of the object itself and metadata about the object.

Access to the bucket is through a pre-authenticated request (PAR), which is a URL that requires no further authentication to use to upload or download files to the bucket. To retrieve a PAR, you must use the appropriate file transfer REST service. For more details on the file transfer REST services, see the *Merchandising Operations Guide Volume 2*.

3

Managing User Security

When implementing the Merchandising suite as a cloud service, Merchandising uses Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) as its identity provider:

- Oracle Cloud Infrastructure Identity and Access Management (OCI IAM):

<https://docs.oracle.com/en-us/iaas/Content/Identity/home.htm>

For more information about using OCI IAM and Oracle Retail applications, see Oracle Retail Identity Management for OCI IAM.

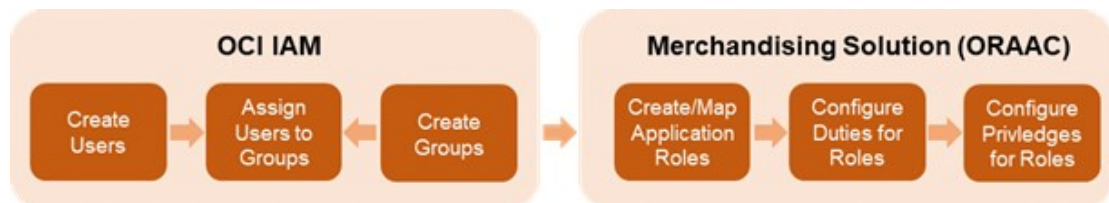
<https://docs.oracle.com/en/industries/retail/retail-identity-management/latest/idmsg/index.html>

Managing Users in OCI IAM

OCI IAM is Oracle's cloud native security and identity platforms. It provides a powerful set of hybrid identity features to maintain a single identity for each user across cloud, mobile, and on-premises applications. OCI IAM both enables single sign on (SSO) across all applications in your Oracle Cloud tenancy.

You can also integrate OCI IAM with other on-premise applications to extend the scope of this federated identity management.

All application user maintenance is performed via OCI IAM. It is also where users are assigned to groups, which are the equivalent to roles (or job roles) in Merchandising.



Add Groups in OCI IAM

For Merchandising Cloud Service implementations, all the default roles are created for you in OCI IAM for both production and non-production environments, including the administration roles described below. The non-production version of the roles will include a "_PREPROD" extension.

This is because a single instance of OCI IAM will hold both production and non-production roles for your Merchandising cloud solutions, so the names need to be differentiated. These roles should not be removed. For the full list of groups/roles that are seeded with each of the Merchandising cloud services, see the volume 2 security guides for each service.

If you want to add roles outside the default roles for the Merchandising solutions, you can initiate that process in OCI IAM by creating a new group.

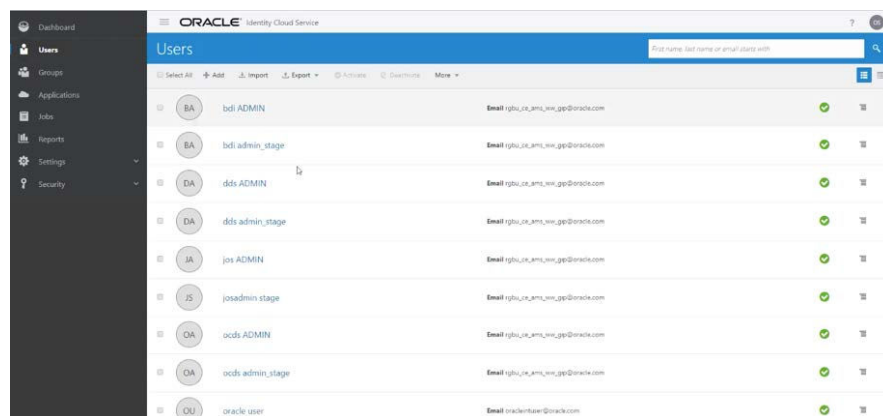
It is recommended you use a similar naming convention as is used for base roles, appending non-production roles with the `_PREPROD` extension so that if you later choose to migrate the configurations between environments, the role names only need to have the extensions updated. You could also use different extensions if creating roles for different purposes. General steps for adding groups in OCI IAM are shown below, but please see the latest OCI IAM documentation for specifics.

Add Users in OCI IAM

General steps for adding users in OCI IAM are shown below, but please see the latest OCI IAM documentation for specifics.

1. In OCI IAM, click on the Users link in the Navigation Drawer.
2. Select Add to add a new user.
3. In the popup, enter the user's name and ID, then click Next.
4. Assign the new user to one or more groups by ticking the appropriate boxes. Use the search box in the popup to narrow down the list, if needed. Then click Finish.

Additionally, several users will be added in OCI IAM for your Merchandising cloud service implementation that are used for running batch processes, web service calls, and so on. These users (e.g., for example, `bdi_admin`, `jos_admin`) will be managed by the Oracle Cloud Operations team and should also not be removed.



Map Groups to Application

When new groups are created in OCI IAM, they must be associated with an appropriate Oracle Retail enterprise role to access the Merchandising suite. This can only be done by users assigned to the administration role in the appropriate solution:

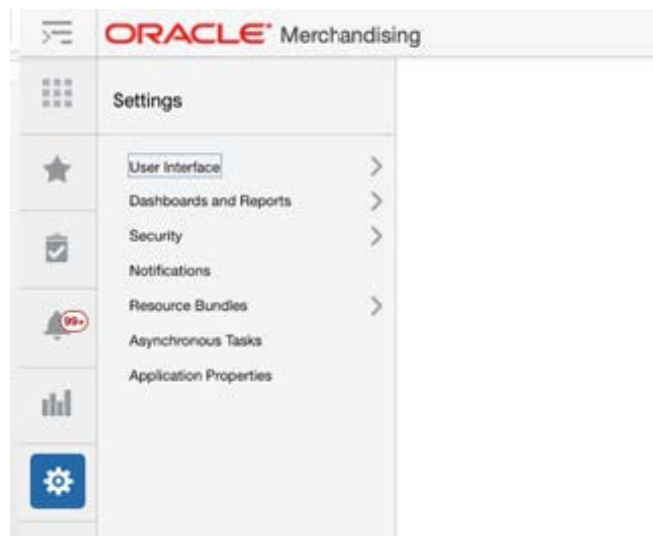
- Merchandising: `RMS_APPLICATION_ADMINISTRATOR_JOB`
- Sales Audit: `RESA_APPLICATION_ADMINISTRATOR_JOB`
- Pricing: `PRICING_APPLICATION_ADMINISTRATOR_JOB`
- Invoice Matching: `REIM_APPLICATION_ADMINISTRATOR_JOB`
- Allocation: `ALLOCATION_APPLICATION_ADMINISTRATOR_JOB`
- Fiscal Management: `RFM_APPLICATION_ADMINISTRATOR_JOB`

The users with application administration roles have permissions that allow them to update the default role to application access mappings based on these two duties:

- SETTINGS_MENU_DUTY
- ADMIN_CONSOLE_DUTY

The Settings Menu Duty provides access to all the menu options under the Settings menu in each of the solutions, except the Security folder. The Admin Console Duty provides access to the Security option. This allows you to create a new role that assigns only the non-security related duties, if desired. The administrative roles provided for each solution are the only roles to which the SETTINGS_MENU_DUTY and ADMIN_CONSOLE_DUTY can be assigned. These duties cannot be assigned to any custom roles.

Figure 3-1 Settings



To make sure the users you create and associate with OCI IAM groups can access functions in the Merchandising cloud services, the last step is to map the OCI IAM group to a role in the appropriate Merchandising cloud service. This is done in the application itself using the Duplicate action. The steps for this are covered in more detail in the Managing Roles, Duties, and Privileges in the Merchandising Suite section below.

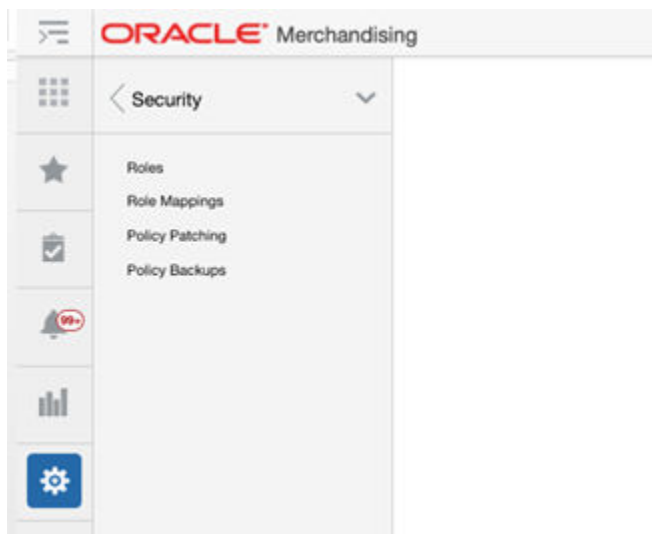
Managing Roles, Duties, and Privileges in the Merchandising Suite

As part of the Merchandising solutions security set up, default enterprise roles and their mappings to application roles are provided with every application. Additionally, each solution has a default configuration of duties assigned to application roles, and privileges assigned to duties.

The details for each of these are outlined in volume 2 of the specific solution's security guide. If you wish to change the privileges assigned to base duties, create new duties, or remove or add duties to default roles or your custom roles, you will do this by accessing the Security menu options in the Settings menu in each of the Merchandising solutions.

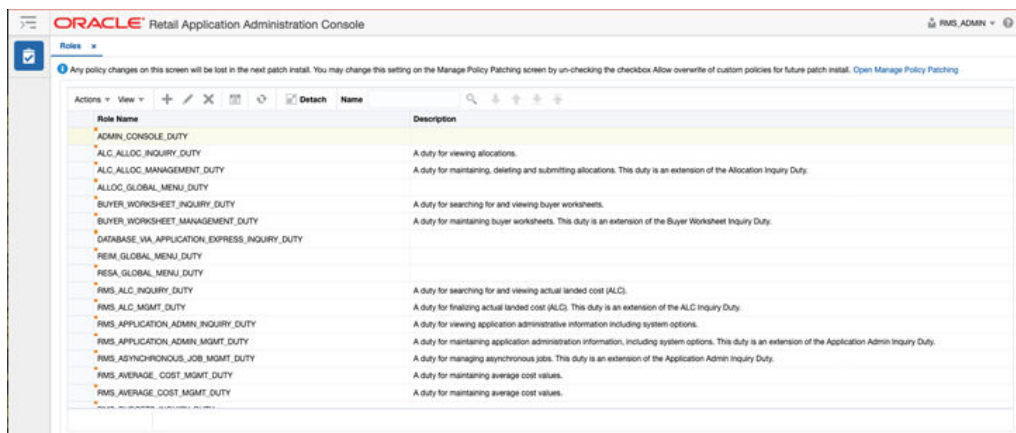
**Note:**

The roles, duties, and privileges for each solution area are viewed and managed separately. For example, you will not be able to view or update Allocation duties when accessing the security setup from the Merchandising solution.

Figure 3-2 Security Roles

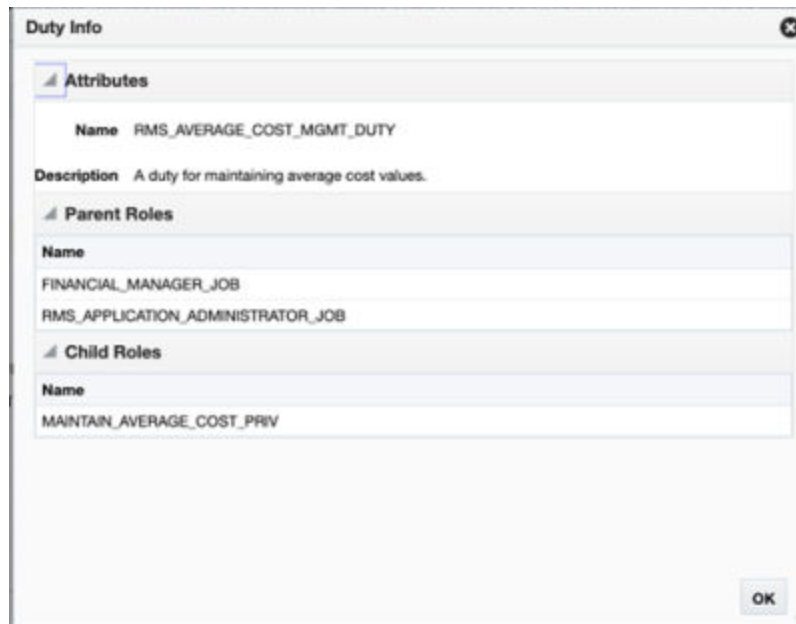
Manage Duties

Clicking on the **Roles** option in the Security menu will launch the Oracle Retail Application Administrator Console. This page allows you to view and edit all the existing duties that exist for the solution, including the description of how a duty is expected to be used. You can also add custom duties or remove duties, as needed.

Figure 3-3 Roles Page

Additionally, hovering over the orange square in the top left of each role name allows you to click on the "carrot" that appears to display additional information about the role, including roles it is assigned to, and which privileges are contained in the duty.

Figure 3-4 Duty Info Pop-up



Manage Role Mappings

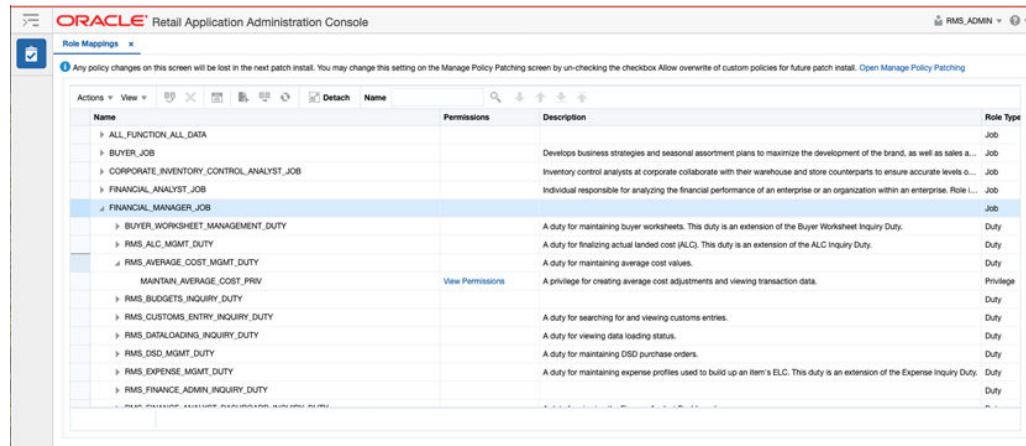
The relationship between roles and duties and/or privileges is managed in the **Role Mappings** page, which is accessed from the Security menu. Like the Roles screen, this will also launch the Oracle Retail Application Administrator Console. In this screen, you will see all the roles that have had duties and privileges assigned.

Clicking on the arrow next to the role name will show you the list of duties currently assigned to the role. Clicking on the arrow next to the duty name will show you the privileges assigned to that duty. Descriptions are also shown for the duties and privileges to help with understanding of what functions they control in the solution.

You can also click on the View Permissions link for privileges to see the technical details related to the privilege.

There are several actions that you can take in this screen: Duplicate, Delete, Select and Add, and Remap. You also have the option to export this list to Excel.

Figure 3-5 Role Mappings Page



Name	Permissions	Description	Role Type
ALL_FUNCTION_ALL_DATA			Job
BUYER_JOB		Develops business strategies and seasonal assortment plans to maximize the development of the brand, as well as sales a...	Job
CORPORATE_INVENTORY_CONTROL_ANALYST_JOB		Inventory control analysts at corporate collaborate with their warehouse and store counterparts to ensure accurate levels o...	Job
FINANCIAL_ANALYST_JOB		Individual responsible for analyzing the financial performance of an enterprise or an organization within an enterprise. Role i...	Job
FINANCIAL_MANAGER_JOB			Job
BUYER_WORKSHEET_MANAGEMENT_DUTY		A duty for maintaining buyer worksheets. This duty is an extension of the Buyer Worksheet Inquiry Duty.	Duty
RMS_ALC_MGMT_DUTY		A duty for finalizing actual landed cost (ALC). This duty is an extension of the ALC Inquiry Duty.	Duty
RMS_AVERAGE_COST_MGMT_DUTY		A duty for maintaining average cost values.	Duty
MANTAIN_AVERAGE_COST_PRIV	View Permissions	A privilege for creating average cost adjustments and viewing transaction data.	Privilege
RMS_BUDGETS_INQUIRY_DUTY			Duty
RMS_CUSTOMS_ENTRY_INQUIRY_DUTY		A duty for searching for and viewing customs entries.	Duty
RMS_DATALOADING_INQUIRY_DUTY		A duty for viewing data loading status.	Duty
RMS_DSD_MGMT_DUTY		A duty for maintaining DSD purchase orders.	Duty
RMS_EXPENSE_MGMT_DUTY		A duty for maintaining expense profiles used to build up an item's ELC. This duty is an extension of the Expense Inquiry Duty.	Duty
RMS_FINANCE_ADMIN_INQUIRY_DUTY			Duty

Duplicate

The Duplicate action allows you to copy the duty and privilege configuration of one role to another. This is used to create the role association in the application with the one created in OCI IAM.

To use this function, highlight the role you wish to copy and select the Duplicate option from the Actions menu or by clicking on the  duplicate icon.

It is best to select a role that has similar duties to the role you are adding, when possible. Then, enter the name of the new role where the copied duties and privileges should be added. The application role must not already have duties/privileges assigned in the solution and must have already been created in OCI IAM prior to this step. Once the new role is created in the solution and the duties and privileges are copied to the new role, you can begin configuring the role by removing any duties or privileges that do not apply or adding new.

Figure 3-6 Duplicate Role Page

Duplicate Role

* New name

Job Role BUYER_JOB

Name	Description	Role Type
▶ BUYER_WORKSHEET_MANAGEMENT_DUTY	A duty for maintaining buyer workshee...	DUTY
MAINTAIN_SHIPMENTS_AND_RECEIPTS_PRIV	A privilege for managing shipments an...	PRIVILEGE
▶ RMS_ASYNCHRONOUS_JOB_MGMT_DUTY	A duty for managing asynchronous job...	DUTY
▶ RMS_BUDGETS_INQUIRY_DUTY		DUTY
▶ RMS_BUDGETS_MGMT_DUTY		DUTY
▶ RMS_BUYER_DASHBOARD_INQUIRY_DUTY	A duty for viewing the Buyer Dashboard.	DUTY
▶ RMS_COMPETITIVE_INQUIRY_DUTY	A duty for viewing Competitive Shop in...	DUTY

OK Cancel

Delete

The Delete action is enabled when a duty or privilege role is selected. To delete a duty assigned to a role or a privilege assigned to a duty, select the Delete option from the Actions menu or click on the  delete icon



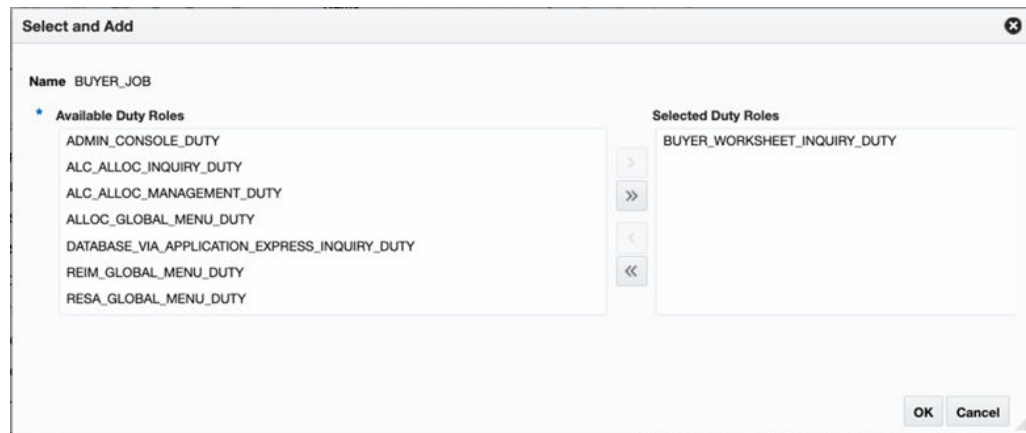
Note:

Any changes to the privileges assigned to duties in this screen will impact all job roles assigned to this duty.

Select and Add

The Select and Add option allows you to add new duties to a role or add new duties or privileges to a duty. To add new duties to a role, highlight the role in the table and then select the Select and Add option in the Actions menu or click on the  add icon.

This will open a popup displaying all the available duties that can be added to the role. Highlight the duties to be added and use the arrows to add to the box on the right. Once all have been added, click OK to save your changes.

Figure 3-7 Select and Add a Page

Similarly, to add privileges or child duties to duty, highlight the duty in the table and select the Select and Add option in the Actions menu or click on the add icon button. Select the duties or privileges from the list of available options and click OK to save your changes. It should be noted that any child duties or privileges you add to a duty would be added to all roles that have the parent duty, not just the selected role

Remap

The Remap action and iconic button  is enabled when a job or duty is selected. The Remap action is used to move mappings 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. It is not recommended that this be used in Merchandising solutions. Instead, create a new role using the Duplicate feature.

Policy Patching

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 that have been applied to the solution.

The latest patch provides a link to synchronize the changes introduced in the patch with your role configurations. The Patch History view also has a check box at the bottom of the page to indicate whether to overwrite your configurations when the application is patched in the future.

By default, this should be unchecked to prevent overwriting of your custom policies when patches are applied, so that you can review and apply changes to how your custom policies have been designed.

Figure 3-8 Policy Patching Page

Version	Install Date	Policy Changes	Policies
19.0.000	11/12/19 12:17 PM	1 Update	Sync with Patch
16.0.030	24/9/19 7:59 AM	4 Updates	
16.0.028.0	12/6/18 3:44 AM		
16.0.027	4/5/18 1:21 AM		
16.0.025	24/1/18 4:05 AM		
16.0.024	9/1/18 12:51 AM		
16.0.023	11/12/17 4:48 AM		
16.0.21.0	19/9/17 11:57 PM		

☒ Allow overwrite of custom policies for future patch install

Click the Sync with Patch link to access the second view, which shows you the base policies and your custom policies.

Figure 3-9 Policy Patching – Base Policies

Select	Name	Permissions	Description
☐	ALL_FUNCTION_ALL_DATA		
☐	BUYER_JOB		
☐	CORPORATE_INVENTORY_CONTROL_ANALYST_JOB		Develops business strategies and seasonal assortment plans to maximize the dev
☐	FINANCIAL_ANALYST_JOB		Inventory control analysts at corporate collaborate with their warehouse and store
☐	FINANCIAL_MANAGER_JOB		Individual responsible for analyzing the financial performance of an enterprise or a
☐	INVENTORY_ANALYST_JOB		
☐	INVENTORY_CONTROL_MANAGER_JOB		Works closely with the buyer to ensure product distribution aligns to strategy. The
☐	INVENTORY_MANAGER_JOB		Inventory control managers develop and implement inventory control procedures
☐	RMS_APPLICATION_ADMINISTRATOR_JOB		An inventory manager is responsible for working with the buying teams to execute
☐	RMS_DATA_STEWARD_JOB		The RMS Application Administrator is a part of a retailer's IT department responsi
☐	SOURCING_ANALYST_JOB		The RMS Data Steward is responsible for the management of foundational data el
☐	SUPPLY_CHAIN_ANALYST_JOB		Manages the sourcing for a retailer, including importing processes, to ensure effici
☐	authenticated-role	View Permissions	Responsible for planning, coordinating and controlling all aspects of supply chain
☐	anonymous-role	View Permissions	

[Overwrite Custom Policies](#) [Import Custom Policies](#) [Done](#)

This view provides a way for you to synchronize the changes introduced in a patch with your configuration. 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 you configured. Details on the changes in duties and privileges are provided in the Advanced Release Notes for each patch.

Copy to Custom

The Copy to Custom action is enabled when a privilege is selected in the Base Policies tab and the privilege does not exist in the custom application policies. The Copy to Custom action copies the privilege to a selected duty in the custom policy setup.

Sync

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

View Permissions

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

Overwrite Custom Policies

The Overwrite Custom Policies action overwrites the current custom policy setup with the base policy in the patched application. The action will cause the loss of your configured policy changes. The action backs up the application policies before overwriting and can be retrieved using the Manage Backups screen.

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 a pop-up, which provides an option to choose a file from your local machine, such as one that you may have created using the Policy Backup screen. This action is useful when migrating policies from one environment to another.

Refresh

The Refresh action is only available in the Custom Policies tab and may be 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.



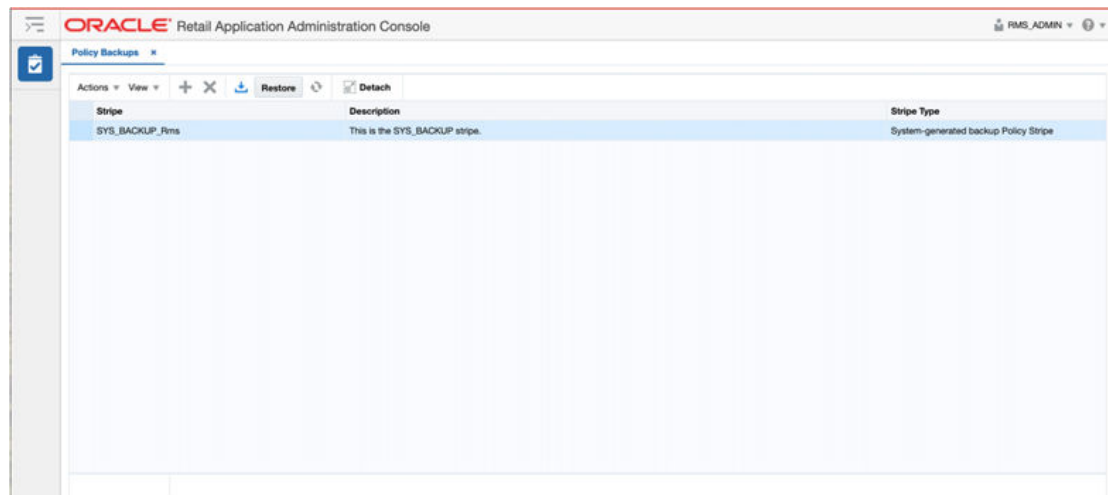
Note:

If a new duty has been introduced in a patch then the Roles page should be used to create the duty and Role Mappings should be used to assign it to the appropriate job roles. Once the new duty role has been created and assigned to a job role, the Copy to Custom action can be used to assign privileges to that duty.

Policy Backups

If a new duty has been introduced in a patch then the Roles page should be used to create the duty and Role Mappings should be used to assign it to the appropriate job roles. Once the new duty role has been created and assigned to a job role, the Copy to Custom action can be used to assign privileges to that duty.

Figure 3-10 Policy Backup Page



The backups can be created by the following actions:

- 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 Policy Patching screen.
- Selecting the Create action on the Manage Backups screen. The user created backup is prefixed with the name USER_BACKUP.
- Using the Overwrite Custom Policies action on the 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.

Create

This action is used to create a backup of the current policies. The backup stripe name is prefixed with the text USER_BACKUP. The create action opens up a popup where you can enter the comments for why the backup is being taken.



Note:

Only one user-initiated backup is allowed. If a backup already exists, it will be overwritten.

Delete

The delete action is used to delete the selected backup stripe.

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 to look at the changes in the backup.

Restore

The Restore action will overwrite the current policy setup with the policies available in the backup.

Refresh

The Refresh action will refresh the backup table.

4

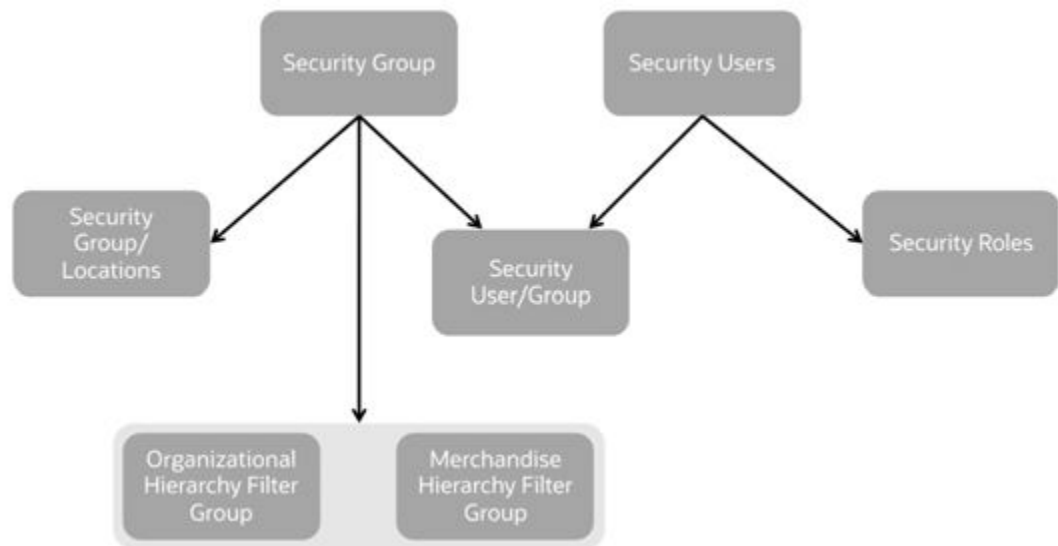
Manage Data Filtering

The Oracle Retail Merchandising suite offers an optional layer of data filtering in the application user interface, which limits the data end users see by levels in the merchandise and organizational hierarchies. Whether or not this is used in your environment is controlled by a system option in Merchandising, which is also where all the configuration for this functionality is managed.

This data level filtering is configured by assigning users to a data security group. If you have turned on this data filtering, you will need to create at least one group and ensure that all your users are added per the directions in the sections below. The group is then assigned to levels of the merchandise and organizational hierarchy. All users within a group will have similar access to a particular section of the merchandise or organizational hierarchy. For example, a group may be defined for a particular division, giving users across application job roles, access to the departments, classes, subclasses, and items in that division. Data filtering is managed in Merchandising, but used in Allocation, Invoice Matching, Pricing, and Sales Audit.

For more information on how filtering is used in each of these solutions, see volume 2 of each solution's security guide.

Figure 4-1 Data Filtering Security Diagram



To setup data filtering, there are several components that must be configured. The sections below outline how to configure each of those components.

Users and Roles

Security users and user roles define who the application users are, what roles they have in your organization, and what applications they are users of. The setup of users within Merchandising is used for data filtering within the Merchandising suite and for managing user Purchase Order approval amounts.



Note:

The role here does not have to be the same as the job roles described in the Managing Roles, Duties, and Privileges section above, however you could use the same names for the roles in data filtering.

The users and user/role combinations for data filtering are managed through spreadsheet download and upload processes. These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To manage users and user/role combinations, you will select the template type of Data Filtering from the Download Data screen and then the template Security Users. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there are two sheets that can be modified - Security Users and Security User Roles.

Adding a User

To add a new user, first download the spreadsheet and open it. All existing users are displayed on the Security Users tab. Navigate to an empty row in the spreadsheet and select the Create action. In the User Sequence column enter a unique, numeric identifier of up to 15 digits in length. Then, enter a value in the Application User ID column.

The value entered should correspond to the identifier for this user that has been defined in the identity management system and is the ID that the user uses to log into the Merchandising solutions. The Database User ID column should be left blank. The manager column is optional but is used by Invoice Matching does for grouping invoices in the Employee Workload report for a Finance Manager.

If entered, the value entered in this column must be an existing user (User Sequence value). Finally, you must enter or select either Yes or No in each of the application user columns to indicate which applications this user will access. You may also specify security user roles for any new users by following the instructions in the Managing User Roles section.

Updating a User

To update an existing user, first download and open the spreadsheet. In the Security User tab all existing users are displayed. Select the action type of Update for the user being updated. You may update the Application User ID, Manager, and application

User Indicator column values. The User Sequence and Database User ID cannot be updated.

Deleting a Security User

To delete an existing Security User, first download and open the spreadsheet. In the Security Users tab, search for the user that is to be deleted. Select the Delete action in the row. Deleting a user will also remove the deleted user's role details.

Managing User Roles

To manage the roles associated with users, first download and open the spreadsheet. Navigate to the Security User Roles tab. All existing user roles are displayed. To define a new security role, navigate to a blank row and select the Create action. Enter the User Sequence from the Security Role tab that corresponds to the user you are adding the role for. Next, in the Role column enter the role for the user.

Only one role may be defined for a user. To change the role of an existing user, search for the user in the sheet. Select the Update action for the user you wish to update and enter the new role for the user. To delete a user role, search for the user in the sheet and select the Delete action in the user's row.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet, save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list.

In this screen, select the template type Data Filtering and the template Security Users. This will generate a process description automatically, but this can be updated if desired. Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.



Note:

Because all the tabs in this spreadsheet have a lot of rows, it's recommended that you delete any you are not updating from the template. This will not remove them from the system, but will make your updates process faster. Worksheets and columns in the spreadsheet **cannot** be removed, however.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

Security Groups

Security groups provide a way to group users for purposes of limiting their data access in the Merchandising solutions. This is done by associating them to the merchandise and/or organizational hierarchies to limit the data that is available to the users. If you have data filtering enabled in Merchandising, you need to create at least one security group.

Security Groups are managed through spreadsheet download and upload processes. These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To manage security groups, you will select the template type of Data Filtering from the Download Data screen and then the template Security Groups. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there are two sheets that can be modified - Security Groups and Security Group Translations.

Managing Security Groups

To manage the security groups, first download and open the spreadsheet. Navigate to the Security Groups tab. All existing user groups are displayed. To define a new security group, navigate to a blank row and select the Create action. Enter a unique, numeric Group ID to identify the group. Next, in the Group Name column enter a name for the group to make it more easily identifiable. Optionally, you may then enter or select a value in the Business Role column.

The valid values for business roles are maintained in the Merchandising Codes and Descriptions function under code type ROLE. They do not drive any specific function in Merchandising, so are for reference purposes only. Finally, you may enter a value in the Comments column, for example, to state the purpose of the group being defined.

To update an existing group, search for the group in the sheet. Select the Update action for the group you wish to update. The Group Name, Business Role, and Comments may be updated. To delete a group, search for the group in the sheet and select the Delete action in the group's row. Groups cannot be deleted until the usage of this group has been removed from dependent tables, as shown in the diagram above.

Managing Security Group Translations

You can also add a translated description for your security groups, if desired. To manage translations for security groups, first download and open the spreadsheet. Navigate to the Security Group Translations tab. All existing group translations are displayed. To add a new translation, navigate to an empty row in the spreadsheet and select the Create action. In the Language column select the language that defines the translated group name.. Enter the Group ID for the group that corresponds to the group ID from the Security Groups tab. In the Group Name column enter the translated string for the group in the selected language. To update a translation, search for the group and language you need to update. Select the Update action and update the value in the Group Name column of the row. To remove a translation, search for the group and language you need to remove and select the Delete action in the row.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet, save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list. In this screen, select the template type Data Filtering and the template Security Groups. This will generate a process description automatically, but this can be updated if desired.

Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

Associate Users to Groups

Security users must be associated to security groups in order for data filtering to be applied when users are in the Merchandising solutions. The user to group associations are managed through spreadsheet download and upload processes. These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To manage these associations, you will select the template type of Data Filtering from the Download Data screen and then the template Associate Users to Groups. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there is one sheet that can be modified - User Groups.

Managing Group / User Associations

To manage the association of users to security groups, first download and open the spreadsheet. All existing associations are displayed in the User Groups tab. To create a new association between a security group and a user, navigate to a blank row and select the Create action. Enter a security group identifier that has been previously defined in the Group ID column. Next, enter user sequence identifier in the User ID column. A user may belong to more than one group. To remove a previously defined association, search for the row containing the association and select the Delete action in the row.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet, save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list. In this screen, select the template type Data Filtering and the template Association Users to Groups. This will generate a process description automatically, but this can be updated if desired. Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.

Note:

Because all the tabs in this spreadsheet have a lot of rows, it's recommended that you delete any you are not updating from the template. This will not remove them from the system, but will make your updates process faster. Worksheets and columns in the spreadsheet cannot be removed, however.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

Filter Groups

Filter groups are a way to associate the defined security groups and the users within the groups to the merchandise and organization hierarchies. These associations control the product and location data that is visible and available for use in the Merchandising solutions for the users in the group.



Note:

If a security group is not assigned to any merchandise or organizational hierarchy data, users in the group are considered "super users" and will have access to all merchandise hierarchies or all organization hierarchies, respectively.

Filter Groups are managed through spreadsheet download and upload processes. These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To manage filter groups, you will select the template type of Data Filtering from the Download Data screen and then the template Filter Groups. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there are two sheets that can be modified - Filter Group Organization and Filter Group Merchandise.

Managing Group / Organization Associations

To manage the association of security groups to the organizational hierarchy, first download and open the spreadsheet. Navigate to the Filter Group Organization tab. All existing associations are displayed. To create a new association between a security group and the organizational hierarchy, navigate to a blank row and select the Create action. Enter a security group identifier that has been previously defined. Next, enter or select a level of the organizational hierarchy in the Filter Org Level column. In the Filter Org ID column enter the identifier for the organizational hierarchy that you are providing the security group access to. For example, if you've chosen Chain as the Filter Org Level you will enter the chain identifier to grant users in the security group with access in the Merchandising applications to locations in the defined chain. To remove a previously defined association, search for the row containing the association and select the Delete action in the group's row.

Managing Group / Merchandise Associations

To manage the association of security groups to the merchandise hierarchy, first download and open the spreadsheet. Navigate to the Filter Group Merchandise tab. All existing associations are displayed. To create a new association between a security group and the merchandise hierarchy, navigate to a blank row and select the Create action. Enter a security group identifier that has been previously defined. Next, enter or select a level of the merchandise hierarchy in the Filter Merch Level column. In the

Filter Merch ID column enter the identifier for the division, group or department that you are providing the security group access to.

For example, if you've chosen Division as the Filter Merch Level you will enter the division identifier to grant users in the security group with access in the Merchandising applications to items in the defined division. If you select Class in the Filter Merch Level column you will need to enter a class identifier in the Filter Merch ID Class column in addition to the department in the Filter Merch ID column .

If you select Subclass in the Filter Merch Level column you will need to provide a subclass identifier in the Filter Merch ID Subclass column in addition to the department and class. To remove a previously defined association, search for the row containing the association and select the Delete action in the group's row.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet, save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list. In this screen, select the template type Data Filtering and the template Filter Groups. This will generate a process description automatically, but this can be updated if desired. Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

Associate Locations to Groups

Associating security groups to locations can be done to manage the locations that a user can view and update transfers in to or out from. The associations of user groups to locations is managed through spreadsheet download and upload processes.

These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To manage the association of user groups to locations, you will select the template type of Data Filtering from the Download Data screen and then the template Associate Locations to Groups. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there is one sheet that can be modified - Location Groups.

Create an association between a user group and locations

To create a new association between a user group and locations, first download the spreadsheet and open it. All existing associations are displayed. Navigate to an empty row in the spreadsheet and select the Create action. In the Column Code column select or enter either Transfers From or Transfers To. Selecting Transfers From indicates that you are intending to define an association to a user group to restrict the transfers users in the group can view or update based on the from location of the transfer. Selecting Transfers To indicates that you are intending to define an association to a user group to restrict the transfers users in the group can view or update based on the to location of the transfer. Next, enter a previously defined security group identifier in the Group ID column. Next, to define the

locations you must enter either a region identifier in the Region column, a district in the District column, a store in the Store column, or a warehouse in the Warehouse column. If defining the locations at a district level you must enter both a region and a district.

Lastly, you must enter or select either Yes or No in the Select Indicator and Update Indicator columns. A value of Yes in the Select Indicator column means users in the group are able to view transfers containing the specified location(s) as the from or to location, depending on the Column Code value. A value of No indicates they will not be able to view them. A value of Yes in the Update Indicator column means users are able to update transfers containing the specified location(s) as the from or to location, depending on the Column Code value. A value of No indicates they will not be able to update them. In order to select Yes in the Update Indicator column, the value in the Select Indicator column must be Yes. Repeat the above steps to define additional associations as required.

Updating an association between a user group and locations

To update an existing association, first download and open the spreadsheet. All existing records are displayed. Select the action type of Update for the user being updated. Only the Select Indicator and Update Indicator may be updated. To redefine a group's association to locations you have to delete and re-create them.

Deleting an association between a user group and locations

To delete an existing association, first download and open the spreadsheet. Search for the record that is to be deleted and select the Delete action in the row.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet, save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list. In this screen, select the template type Data Filtering and the template Association Users to Groups. This will generate a process description automatically, but this can be updated if desired. Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.



Note:

Because all the tabs in this spreadsheet have a lot of rows, it's recommended that you delete any you are not updating from the template. This will not remove them from the system, but will make your updates process faster. Worksheets and columns in the spreadsheet cannot be removed, however.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

Order Approval Amount by Role

An optional layer of validation can be added in Merchandising to approval of purchase orders that restricts users to the ability to approve a purchase order that is valued over a certain amount based on either the cost or retail value of the order. The determination of whether cost or retail is used is based on a system option Order Approval Basis. The approval limitations are defined by role and are always entered in terms of the primary currency for your implementation.

Adding, updating, or removing roles from the order approval limits are managed through spreadsheet download and upload processes. These processes are accessed through the main Merchandising task list under Foundation Data > Download Foundation Data and Foundation Data > Upload Foundation Data.

To add, update, or remove approval limits, select the template type of Security from the Download Data screen and then the template Order Approval Amount by Role. Click the Download button and when prompted, choose to either open the .ods file that is generated or save the file and open it separately in the spreadsheet application of your choice. Once opened, there is one sheet that can be modified - Role Privileges.

Add Order Approval Amounts

To add privileges for a new role, in a blank line in the template, select the action type of Create. Next enter the role ID, which can be up to 30 characters in length. This role ID must match one on the Security User Roles table. Next enter the amount that this role is limited to in the Order Approval Amount column, based on the cost or retail value of the order as described above. This value should be in the primary currency. Any purchase orders that are less than or equal to the amount entered in this field are able to be approved by users assigned to this role. Any that are of a larger value will not be able to be approved. For users that can approve any order, it is recommended that the order approval amount be set to the maximum allowed in this field - 99,999,999,999,999,999.

Update Order Approval Amounts

If you would like to update the order approval amount for any roles, a similar process is followed as that described above for adding limits. First, download the spreadsheet and then find the role that you would like to update. In that row select the action type of Update, and then correct the order approval amount in the spreadsheet.

Delete Role Privileges

If you wish to delete a role, then update the action column to select Delete in the row containing the role you wish to remove. Note that users assigned to roles that are not on this table cannot approve an order, as their upper threshold for approval is assumed to be zero.

Uploading Changes

For all actions defined above, once all the updates have been made to the data in the spreadsheet save the file and close it. Then, return to the Merchandising screens and select Foundation Data > Upload Foundation Data from the main task list. In this screen, select the template type Security and the template Order Approval Amount by Role. This will generate a

process description automatically, but this can be updated if desired. Lastly, select the Browse button and navigate to the directory where you saved the updated spreadsheet.

To review the status of the upload and check whether any errors occurred, select the Foundation Data > Review Status task from the main task list.

See also Download/Upload Data from Spreadsheets and View Data Loading Status in the *Oracle Retail Merchandising Do the Basics User Guide*.

5

Other Settings

Notifications

From the Settings menu, you can access the Notifications option. Selecting this option will open the Notifications page in the Retail Application Administrator Console. This page will display two tables.

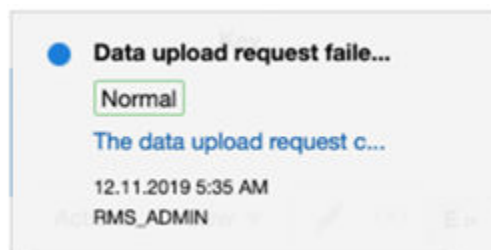
Figure 5-1 Notifications

Name	Retention Days	Type Code	Description	Email Address
Purchase Order Rejected	30	Purchase Order Rejected	Purchase Order Rejected	
Transfer Rejected	30	Transfer Rejected	Transfer Rejected	
PO Induction Upload Complete	30	PO Induction Upload Complete	Order upload request complete	
PO Induction Upload Failed	30	PO Induction Upload Failed	Order upload request failed	
PO Induction Download Complete	30	PO Induction Download Complete	Order download request complete	
PO Induction Download Failed	30	PO Induction Download Failed	Order download request failed	
Item File Upload Complete	30	Item File Upload Complete	Item file upload request complete	
Item File Upload Failed	30	Item File Upload Failed	Item file upload request failed	
PO File Upload Complete	30	PO File Upload Complete	Order file upload request complete	
PO File Upload Failed	30	PO File Upload Failed	Order file upload request failed	
Cost File Upload Complete	30	Cost File Upload Complete	Cost Change file upload request complete	
Cost File Upload Failed	30	Cost File Upload Failed	Cost Change file upload request failed	
New Item Loc Complete	30	New Item Loc Complete	Item Location create request complete	
New Item Loc Failed	30	New Item Loc Failed	Item Location create request failed	
Item Induction Upload Failed	30	Item Induction Upload Failed	Item upload request failed	

The top table shows the notification types that are configured in the solution, along with the number of days that the notifications are retained when they occur for a user. Existing notifications can be edited to change the type code and description, along with the retention days. Retention days must be a number greater than zero, or it can be set to -1 to keep the notification indefinitely, unless deleted by a user. However, this is not recommended.

The description is displayed in the notification displayed to the user:

Figure 5-2 Data Upload Request Notification



You can also add one or more email addresses to have a message sent when the action occurs to trigger a notification.

New notifications can be added in on premise implementation of Merchandising solutions only. Adding new notifications also would require customization if you want the action to be triggered from an action within the application.

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 from user's queues.

The second table in the screen is used to create groups for the notification type

selected in the top table. Click the Create icon button  to create a new group. Then, associate roles or another group with the group by selecting the Add Job Role

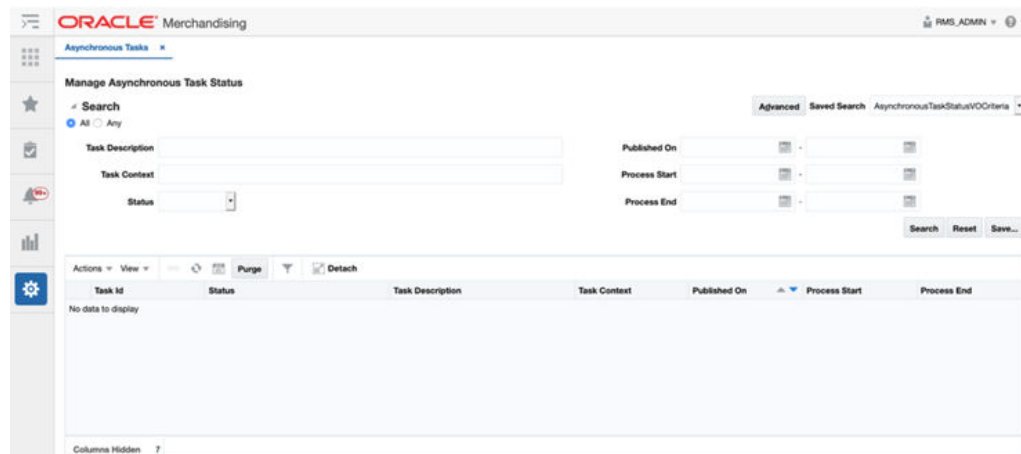
icon button  or the Add Notification Groups icon button . This will allow the notification to be delivered to all users assigned to the roles configured for the group. If no group is assigned, then the notification is delivered to the user who initiated the action the created the notification.

Asynchronous Tasks

Asynchronous tasks are background processes launched by users of the Merchandising solutions. For example, you may use this to troubleshoot an asynchronous task that you failed to receive a notification for. The information in this screen should be included in any SRs logged in helping resolve asynchronous issues. Note: this is not used for Merchandising or Sales Audit.

Administrators can view the latest status of asynchronous tasks through the Manage Asynchronous Task Status page, which is accessed from the Settings menu by selecting Asynchronous Tasks. To view tasks, enter search criteria and click Search. Click the View option in the Actions menu, or the View icon button, to view more details on the task. Click the Refresh option in the Actions menu, or the Refresh icon button, to refresh the data with the latest tasks. You can also purge asynchronous tasks present in the system, if desired. Otherwise, the tasks are purged as configured in Application Properties.

Figure 5-3 Asynchronous Tasks



The screenshot shows the Oracle Merchandising interface for managing asynchronous tasks. The page title is 'Manage Asynchronous Task Status'. It features a search section with fields for 'Task Description', 'Task Context', 'Status', 'Published On', 'Process Start', and 'Process End'. There are also buttons for 'Search', 'Reset', and 'Save...'. Below the search section is a table with columns: 'Task Id', 'Status', 'Task Description', 'Task Context', 'Published On', 'Process Start', and 'Process End'. The table currently shows 'No data to display'. On the left side, there is a sidebar with navigation icons and a 'Settings' icon at the bottom. The top right corner shows the user 'RMS_ADMIN'.

Application Properties

The Application Properties screen allows administrators to search for and modify configuration properties by deployment. There are several functions in the Merchandising cloud services that use these properties:

- Enabling Attachments in Merchandising and Invoice Matching
- Enabling Drill to Finance functions in Merchandising and Sales Audit
- Enabling Slack integration in Merchandising
- Configuring URLs for External Services

Enabling Attachments

To enable the attachments feature in Merchandising and Invoice Matching, you will need to do the following:

1. Select **Settings > Application Properties**
2. In the search criteria, enter RMS or ReIM as the Deploy Name, depending on which solution you are configuring, and type Attachments in the Key Name field. Then click **Search**.
3. This should return one row, similar to what is shown below.

Figure 5-4 Enabling Attachments

The screenshot shows the Oracle Merchandising Application Properties interface. The search criteria are set to Deploy Name: RMS and Key Name: Attachments. The search results table displays one row with the following data:

Deploy Name	Key Name	Key	Current Value	Key Description
Rms	Attachments Feature Enabled	attachments.enabled		Controls whether the attachments feature is enabled or not.

4. Click on the **Edit** icon button or select **Edit** from the Actions menu. This should display a popup that looks like the below image. To enable attachments, change the Current Value to true.

Figure 5-5 Edit Properties

Edit Property

⚠ Any changes to the property settings will impact application behavior. Make sure all the users are logged out before changing any property.

Key attachments.enabled

Attachments Feature Enabled

Controls whether the attachments feature is enabled or not.

Deploy Name Rms

Category Retail Applications Framework Model Layer Properties

Configurable properties affecting the Retail Applications Framework model layer features

Default Value none

Deployment Restart No

Current Value true

Last Updated By

Last Updated Date

Reset to Default OK Cancel

5. Then click **OK** to save your changes.
6. Validate that the Attachments pane is visible in one of the screens that supports this function:
 - **Merchandising:** Item, Item Supplier, Item Supplier Sourcing Country, Item Location, Order Header, and Order Details.
 - **Invoice Matching:** Document Maintenance

To later disable this feature, follow similar steps, but set the Current Value to false instead.

Enabling Finance Drill to Finance and Reports

There are reports and buttons available in the Transaction Data and Fixed Deal Transaction Data screens in Merchandising, as well as in the General Ledger screen in Sales Audit, that allow users to view General Ledger details and also to drill forward into the General Ledger to view the details of how these financial transactions were posted. By default, access to these buttons and reports is disabled in both Merchandising and Sales Audit, since they are only applicable if integrating with PeopleSoft Financials. For more details on these reports and how to access once enabled, see the BI Publisher Reports section of the Merchandising Reports Guide and the Sales Audit Reports Guide. To enable the buttons and reports, log into either Merchandising or Sales Audit and follow these steps:

1. Select **Settings > Application Properties**.
2. In the search criteria, enter RMS (or RESA) as the Deploy Name and type "Drill" in the Key field. Then click **Search**.
3. This should return one row, similar to what is shown below.

Figure 5-6 Application Properties

Deploy Name	Key Name	Key	Current Value
Rms	Drill Forward Service Available	drillforward.service.available	

- Click on the **Edit** icon button or select **Edit** from the Actions menu and change the Current Value to true.
- Then click **OK** to save your changes.

**Note:**

There may be a delay in this taking effect once the change has been made.

Enabling Slack Integration

In the Item and Purchase Orders workflows in Merchandising, you can configure on a feature called Conversations, which allows you to integrate the collaboration tool Slack with Merchandising. When this is enabled, it will allow users of these workflows to collaborate while creating or updating items or managing purchase orders.

This feature works by creating a channel in Slack when you initiate a conversation for a particular item or PO. In this way, you can reply or monitor the details both through the Merchandising application, as well as in your Slack instance. The instructions for doing this are below.

Create a Slack App

First, create a Slack App that is integrated with Merchandising. These are the basic steps for creating an app in Slack calling out the specifics needed to integrate with Merchandising, but please consult the Slack documentation for specifics.

- Log into the appropriate Slack Workspace and Select Create New App.
- Provide a name for your app - this is displayed to the user when they authenticate in Merchandising.
- You are brought to the Basic Information page. In the navigation bar, under Features, select the OAuth & Permissions link.

4. Add a Redirect URL. This should have a format that matches the hostname for your Merchandising environment and ends with `oauth/_callback`, something like `https://xxx-yyy-mfcs-mas.oracleindustry.com/Rms/oauth/_callback`.
5. Scroll down to the Scopes section on the OAuth & Permissions page. Select the Permission Scopes dropdown and select the following scopes then click Save Changes:
 - `chat:write:user`
 - `groups:history`
 - `groups:read`
 - `groups:write`
 - `users:read`
6. Install the Slack App in the Workspace by scrolling back to the top of the OAuth & Permissions link and clicking the Install App to Workspace button.

Configure Slack in App Server

Next, the details of what was configured above will need to be configured in the app server. This needs to be done by the Oracle Cloud Operations team, so will require an SR. In the SR, you will need to include some of the information you set up when you created the app in step 1, including:

- Slack Workspace URL
- Redirect URL
- Client-id and Client-Secrets - these can be found in your new Slack App under the Basic Information link under Settings in the section titled App Credentials. Merchandising will use these to authenticate itself to Slack.

Configure Slack in an Application

Once that step is complete, you will need to configure the related application parameters, following these steps:

1. Select Settings > Applications Properties.
2. In the search criteria, enter RMS as the Deploy Name and type "Conversation" in the Key field. Then click Search.
3. You should see several items listed in the results table. For each of the Key Names listed below, highlight the appropriate row and click on the Edit icon button to make the updates noted:
 - a. Collaboration Conversations Enabled - set current value to true
 - b. Collaboration Conversation Login Scheme - set current value to oauth
 - c. Collaboration Conversation Provider - set current value to slack
 - d. Slack URL - set current value to `https://slack.com`.
 - e. Slack App Redirect URL - set the current value to that described above in the pre-requisites.
 - f. Slack Workspace - set the current value to that described above in the pre-requisites.

These changes will take place immediately after all steps are completed.

Configuring External Services

For several Merchandising services, there is the ability to configure an external URL for the service to use. This is also done in the Application Properties workflow. The services that support this type of configuration are:

Service Name	Application Property Key
General Ledger Account Validation Service	accvalidation.service.url
Drill Back Forward Service	drillforward.service.url
Customer Order Address Service	custordaddress.service.url
Customer Address Service	custaddress.service.url

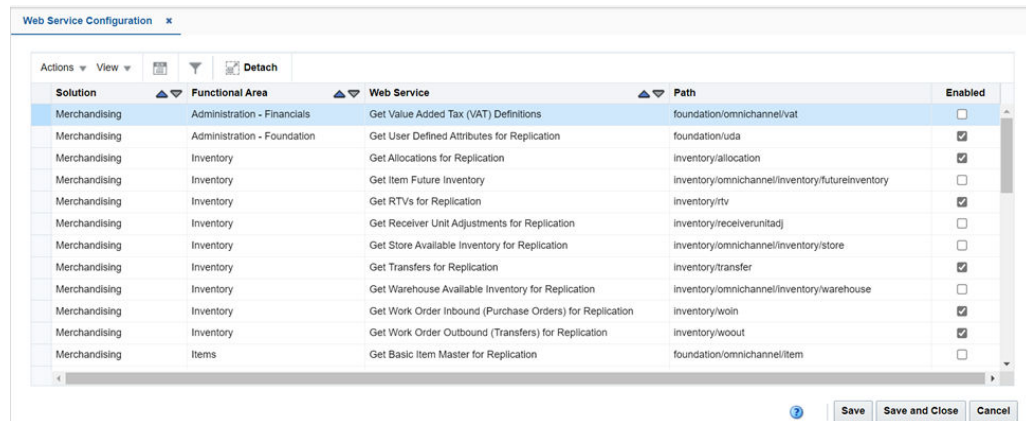
1. To configure the URLs for these functions, log into Merchandising and follow these steps:
2. Select Settings > Application properties from the sidebar menu.
3. Search for the appropriate key, as shown above and click Search.
4. Click on the property and choose Edit.
5. Enter the external URL in the Current Value field.
6. Click on OK to save the updates.

Web Service Configuration

ReSTful web services provide the ability to query data from Merchandising solutions and the ability to create and update data within Merchandising solutions. The Web Service Configuration workflow allows you to enable or disable REST services which require data pre-processing in order to allow consuming systems to replicate the data at their end. If one of these services will not be used, disabling the service via this configuration screen will save system resources by turning off the data processing.

To access the Web Service Configuration page from the Tasks menu, select Application Administration > Web Service Configuration. The Web Service Configuration page appears.

Check or uncheck the Enabled checkbox, to indicate whether or not the service is enabled for integration with external applications. Click on Save or Save and Close to commit the changes.

Figure 5-7 Web Service Configuration Page

The screenshot shows the 'Web Service Configuration' page. At the top, there are tabs for 'Actions', 'View', and 'Detach'. Below these is a table with columns: 'Solution', 'Functional Area', 'Web Service', 'Path', and 'Enabled'. The table lists various web services for the 'Merchandising' solution, categorized by 'Functional Area' (Administration - Financials, Inventory, Items). The 'Enabled' column contains checkboxes, some of which are checked. At the bottom right, there are buttons for 'Save', 'Save and Close', and 'Cancel'.

Solution	Functional Area	Web Service	Path	Enabled
Merchandising	Administration - Financials	Get Value Added Tax (VAT) Definitions	foundation/omnichannel/vat	☐
Merchandising	Administration - Foundation	Get User Defined Attributes for Replication	foundation/uda	☒
Merchandising	Inventory	Get Allocations for Replication	inventory/allocation	☒
Merchandising	Inventory	Get Item Future Inventory	inventory/omnichannel/inventory/futureinventory	☐
Merchandising	Inventory	Get RTVs for Replication	inventory/rtv	☒
Merchandising	Inventory	Get Receiver Unit Adjustments for Replication	inventory/receiverunitadj	☐
Merchandising	Inventory	Get Store Available Inventory for Replication	inventory/omnichannel/inventory/store	☐
Merchandising	Inventory	Get Transfers for Replication	inventory/transfer	☒
Merchandising	Inventory	Get Warehouse Available Inventory for Replication	inventory/omnichannel/inventory/warehouse	☐
Merchandising	Inventory	Get Work Order Inbound (Purchase Orders) for Replication	inventory/woin	☒
Merchandising	Inventory	Get Work Order Outbound (Transfers) for Replication	inventory/woout	☒
Merchandising	Items	Get Basic Item Master for Replication	foundation/omnichannel/item	☐

For more details on how to invoke a service once enabled, see the Web Service Configuration section of the *Merchandising Foundation Cloud Service Operations Guide volume 2*.

6

Data Viewer

Data Viewer is a workspace that provides read-only access to the Merchandising functional data in production environments and read/write access in non-production environments. In production environments, this extension is a workspace for customer support personnel to view the data to troubleshoot issues. In non-production environments, there is more flexibility to assist with conversion of data, configuration of the solution, and some minor data correction, when required. This chapter provides the steps to configure your workspace in a SaaS environment. This will need to be done for each of your environments where you want this enabled.

Workspace

A workspace <RETAILER_WORKSPACE> is predefined for you 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 (in production) or read-write privileges (in non-production) to the Merchandising database tables and views. There are a few tables that are excluded, which are either used internally only (e.g. temp tables) or 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.

For SaaS implementations, the first time that you access the Data Viewer, only the person designated as your initial service administrator (such as, the receiver of the welcome email) will be setup with access. You will need to log in with that username/password in order to provide other users with access, including other administrators. Before you create accounts for your users, you must create users in Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) with the same user name.

Create a Workspace Viewer

Perform the following procedure to create a workspace viewer:

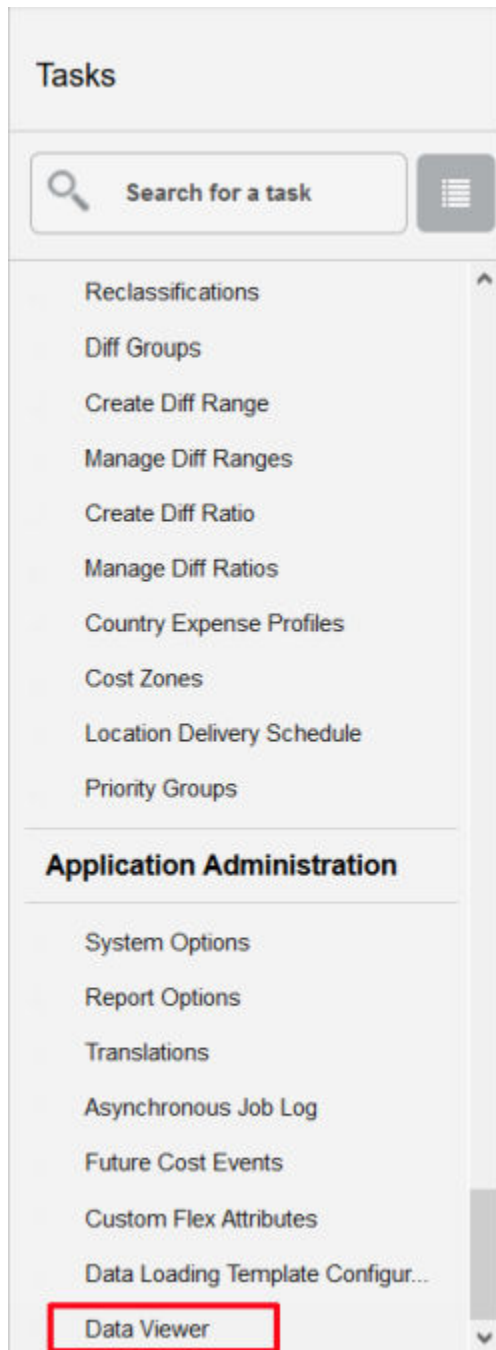
1. Log in to Merchandising.



Although data from other Merchandising cloud services can also be viewed using this capability, the only access for this link is in Merchandising.

2. From the Tasks list, under Application Administration, select Data Viewer.

Figure 6-1 RMFCS Task Menu

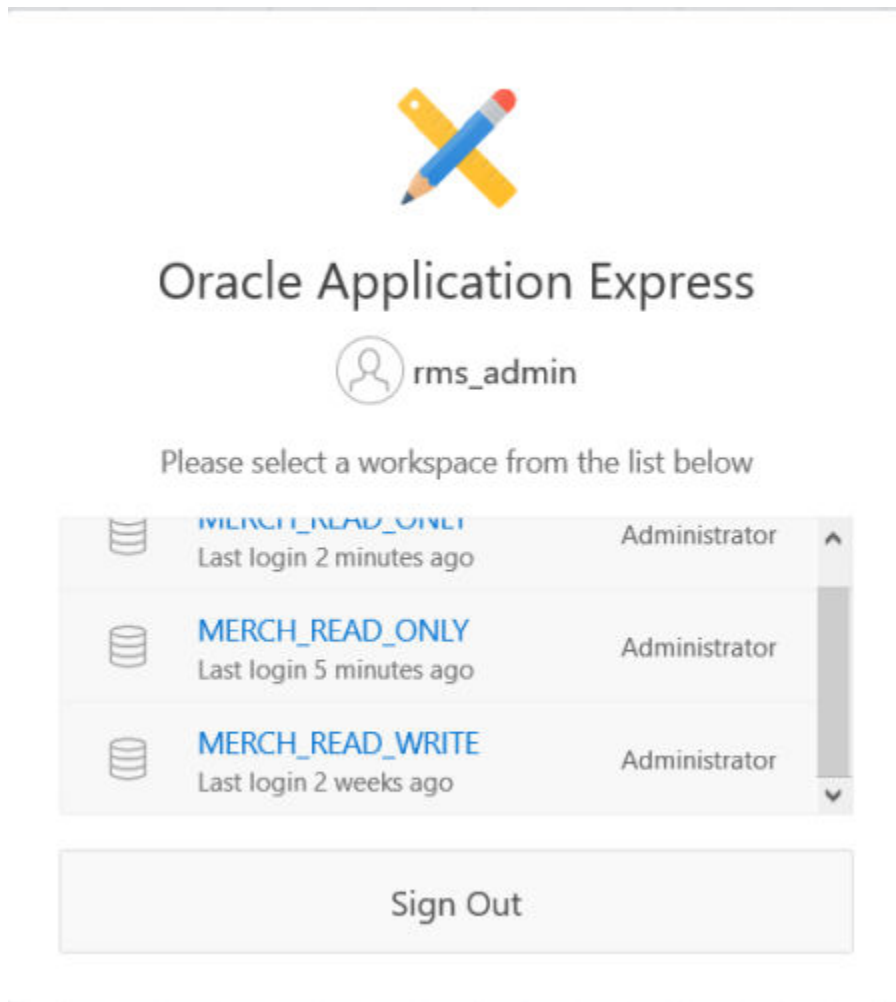


 Note:

If you do not see this link, validate that your role is associated with the DATABASE_VIA_APPLICATION_EXPRESS_INQUIRY_DUTY and/or VIEW_DATABASE_VIA_APPLICATION_EXPRESS_PRIV.

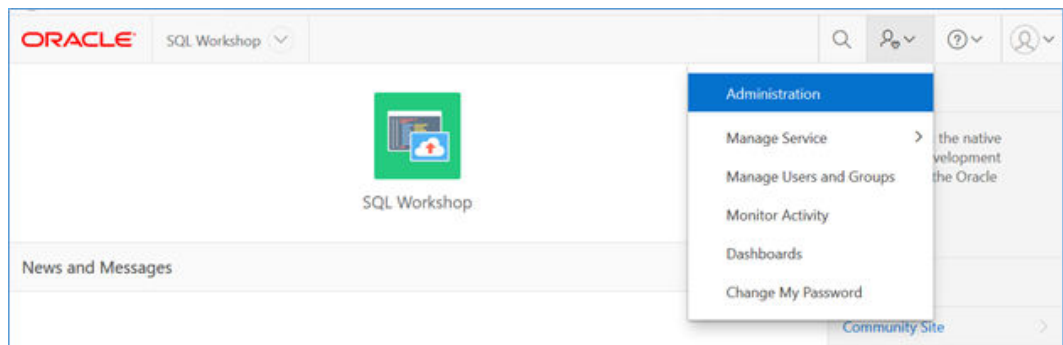
3. Select the appropriate APEX workspace.

Figure 6-2 APEX Workspace Selection Dialog

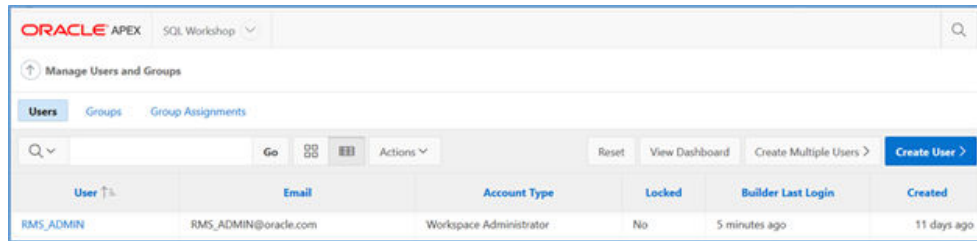


4. From the Administration drop down menu, select Manage Users and Groups.

Figure 6-3 APEX Administration Drop Down Menu



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

Figure 6-4 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 6-5 Oracle APEX Create User Window

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.

**Note:**

The users you are creating in Data Viewer should already exist in IDCS or OCI IAM. See also the Oracle documentation on *Application Express* for more details on using this tool.