Oracle® Retail Allocation

Security Guide

G47902-01
November 2025

Oracle Retail Allocation Security Guide,

G47902-01

Primary Author:

Contributing Authors:

Contributors:

Contents

Send Us Your Comments

Oracle Retail Allocation Security Guide , Release 24.0.101.0.

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

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

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

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

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

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

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

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

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

Preface

Oracle Retail Security Guides contain the requirements and procedures that are necessary for the retailer to secure Oracle Retail products.

Audience

This Installation Guide is written for the following audiences:

- Integrators and implementation staff

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
- Screenshots of each step you take

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Help Center (docs.oracle.com)

Oracle Retail product documentation is also available on the following Web site:

https://docs.oracle.com/en/industries/retail/index.html

(Data Model documents can be obtained through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

This document will cover the aspects of security that were mentioned in the Merchandising Suite Security Guide Volume 1 and describe them in a bit more detail as well as outline how they are used in Allocation specifically.

Application Functional Security

Allocation functional security supports a role-based, declarative model where resources are protected by roles that are assigned to users. Roles are associated to a logical grouping of duties, which in turn are associated to a set of privileges which provide different access rights. In this manner, an application role becomes the container that grants permissions to its members to access the application tasks, screens and the functionalities within.

Roles

Roles, also referred to as Job Roles, align with titles or jobs within a retailer's organization, such as an Allocator or Allocation Manager. Roles are used to classify users based on job responsibilities and actions to be performed in the application. One or more duties as well as individual privileges, if desired, can be assigned to roles. When a user logs into the application, based on the roles assigned to the user, the system determines which privileges have been granted to the user and the system features are enabled accordingly.

Duties

Duties are tasks that one must perform in the context of their job. Duties in Allocation are logical groupings of privileges or other duties that grant users access to a set of functionally related tasks within the application.

Privileges

Privileges are used to grant permission to access links into workflows, screens, actions and in some cases specific fields within the application. Privileges that grant access to related functionality are grouped together into duties that permit a user to perform a complete task to fulfill responsibilities within the context of their job.

Data Filtering

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, it is controlled by a system option in Merchandising, which is also where all of the configuration for this functionality is managed.

This data level filtering is configured by assigning users to a data security group. The group then is assigned to the desired 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.

Within Allocation, there is no additional configuration needed. However, all Allocation users will need to be included in the user/group relationships configured in Merchandising so that they are able to access the data needed to perform their jobs. With data filtering enabled, users will only be able to add items that is part of the merchandise hierarchy to which they have been given data filtering access to an allocation. Likewise, users will only be able to add locations that are part of the organizational hierarchy to which they have been given data filtering access while creating an allocation.

When viewing or maintaining allocations, users will only be able to view and maintain those which have at least one item or location to which they have access. It is important to note that if a user has data filtering access to at least one item or location on an allocation, the user will have the ability to view and modify the entire allocation. If it is desired to not allow users to see allocations for items or locations for which they do not have data filtering access, the data should be created in such a way that users have data filtering access to all items and locations within a given allocation.

To implement data filtering, see Chapter 3, Data Security/Filtering in the *Oracle Retail Merchandising Administration Guide*.

2
Roles

Roles are used to classify users based on job responsibilities and actions to be performed in the application. Using roles, a user's access can be restricted to specific areas or functions within the system. Users must be associated with at least one job role in order to access the application and may be associated with several roles if desired.
For example, within Allocation, a user associated with a business role of an Allocator may be able to perform only the tasks associated to this profile such as searching and viewing allocations, submitting an allocation, viewing size profiles, and so on. He might additionally have view only access to the system options screen, but will not be able to modify anything in the UI. On the other hand, an Allocation Manager will have access to manage and approve allocations, maintain system options, and so on.

Figure 2-1 Allocation Roles

Roles Provided at Initial Setup

A default security configuration is provided with each application during installation and is intended to be used as a starting point as you define the roles that align for your business and users. The provided roles can be modified by adding or removing duties and/or individual privileges to adjust the access granted to the role, or the roles can be deleted completely. Additional roles can be created as well and can be mapped to the desired duties or privileges. Administrator users can change the mappings of roles, duties and privileges in Allocation's User Interface.

Details about how to manage these application security policies are available in Chapter 2, Manage Security Policies in the *Oracle Retail Merchandising Administration Guide*.

There are four roles provided in the default security configuration:

- Application Administrator
- Allocator
- Allocation Manager
- Buyer
- Digital Assistant Chat Viewer

Application Administrator

The Application Administrator is a part of a retailer's IT department responsible for maintaining and configuring the Allocation application. Primary responsibilities include:

- Maintain daily operations, such as daily batch processes of the application
- Supporting end-users and providing the first level of support for the application
- Applying patches and upgrades to the application on a regular basis
- Troubleshooting and resolving product issues
- Setting up users and security privileges for the application

Allocator

An Allocator is mainly responsible for the distribution of selling product supporting the following key business cases; pre-season and initial floor sets and assortments, in season and or point in time replenishment, end of season exit strategies, one time buys, test product and promotional events. Objective of each allocation is to ensure the right volume at the right time is allocated to optimize profitability and aide in decreasing markdown liabilities, by reviewing the sales and stock levels per location. The Allocator will often be the first point of contact for the stores to the merchandising and planning teams. Primary responsibilities include:

- Identify specific opportunities (e.g., sales stock relationships, over under-performing locations, top bottom selling items)
- Recommend action to be taken on identified opportunities
- Maintain store inventory levels for short shelf life items such as seasonal items or initial distributions
- Provide input to central planning organization to inform pre-season FOB strategy and achieve open to buy objectives
- Recommend assortment allocation changes
- Analyze space productivity and recommend or decide changes in space allocations to drive sales
- React to sudden change item location or regional demand

Allocation Manager

An Allocation Manager is responsible for driving inventory strategies that support brand objectives, maximize opportunities, and minimize risk to the business. Allocation managers lead a team of Allocators and are continuously looking for opportunities for improving the efficiencies of allocating merchandise throughout a retailer's supply chain. Key responsibilities include:

- Managing the sales, margin, and inventory turn goals for one or more divisions
- Analyzing historical data and trends to identify risks and opportunities for the business
- Analyzing and executing replenishment strategies for stores and or warehouses

- Working with a cross-functional team both pre-season and in-season to understand the buy plans and shape inventory decisions
- Increase team operational efficiencies by identifying training opportunities, testing new and advanced product features and adapting to change in business model and or company growth

Buyer

Develops business strategies and seasonal assortment plans to maximize the development of the brand, as well as sales and profits for a department or assigned area. Their primary responsibilities are:

- Performing market and competitive analysis and analyze sales trends to keep abreast of current trends
- Developing business strategies outlining strengths, weaknesses, new opportunities and threats

  Analyzing and approving new product or concepts for their department.
- Maintaining relationships, resolve issues and conduct negotiations with significant suppliers and agents
- Managing sales and margin dollar performance against plan
- Recommending adjustments to the plan to maximize sales, profits, and to protect the brand

Digital Assistant Chat Viewer

This role is unique in that it is used to grant access to view and use the digital assistant chat feature. This role should be associated with users who should have access to this feature in addition to any other job roles. This role will only have a single duty mapped to the role. Rather than mapping the same duty to other roles, map this role to users to grant access.

3

Duties and Privileges

Privileges grant access to specific tasks, links, and actions within the application. The access controlled by a particular privilege is fixed and can only be changed by an enhancement to the application. You can control the functions and features to which a user has access by grouping the desired privileges into duties, and assigning the duties to job roles which can then be associated to one or more users

Duties Provided at Initial Setup

As part of this default security configuration, the system privileges have been logically grouped into duties and the duties have been assigned to an initial set of job roles. The provided duties can be modified or deleted and new duties created. Administrator users can change the mappings of roles, duties and privileges in Allocation's User Interface.

Details about how to manage these application security policies are available in Chapter 2, Manage Security Policies in the *Oracle Retail Merchandising Administration Guide*.

Duty Types

Duties provided in the default security configuration follow a general naming convention to indicate the type of privileges grouped within and the level of access provided. In Merchandising, the provided duties are one of the following duty types:

- Inquiry

  An inquiry duty will provide the user the ability to search for and view the associated entity. The provided inquiry duties are used when it is desirable for a user to have visibility to an area, but no option to create or update any information. Inquiry duties are assigned to viewers of an area.

- Management

  A management duty provides the user the ability to maintain the associated entity. The provided management duties are used when it is desirable for a user to have the ability create, update, delete, and, typically, submit information. Management duties always contain the inquiry duty for the same entity. For example, the Allocation Management Duty contains the Allocation Inquiry Duty along with the additional Maintain Allocations Privilege, Delete Allocations Privilege and Submit Allocations Privilege because in order for a user to maintain an entity they must also have the ability to search for, submit and delete the entity. Management duties are assigned to contributors of an area.

- Approval (High Security)

  An approval or high security duty is meant for users with the authority to review and approve or reject submissions and/or the ability to manage high security areas. Users with approval or high security access should always be granted the management duty for the same entity. For example, the Allocation Management Duty and the Allocation Submit Duty are granted along with the Allocation Approval Duty which contains the Approve Allocations Privilege, because in order for a user to approve an entity they must also have the ability to search for, view, maintain, delete and submit the entity. Approval duties are assigned to reviewers of an area.

Duties with no Hierarchical Relationships

There is one privilege used within Allocation that does not have a hierarchical set of duties with increasing levels of access, as described by the duty types above. These duties simply grant access to a single area, such as a dashboard, or they grant access to particular information across several functional areas. Therefore access is either granted or not, there are no access levels. These duties may be classified as management or inquiry duties, depending on if the user can maintain the related data or if access should be view only. For example:

- **Dashboard Inquiry Duty**

  Dashboard duties grant access to view a given dashboard. In order to see the Allocator dashboard, the user must have the View Allocation Dashboard privilege. The Allocator Dashboard contains four reports, Purchase Order Arrivals, Stock to Sales, Sales Top and Sales Bottom. In some cases, access to each report within a given the dashboard may be controlled by separate privileges based on the functional area of the report. However in Allocation, the Allocation Dashboard Privilege will grant the user access to both the dashboard and the four reports within.

- **Batch Management Duty**

  Grants access to execute batch programs. The default security configuration has this duty assigned to the Application Administrator role.

- **Settings Menu Duty**

  Grants access to the Settings menu except for the Security folder. The default security configuration has this duty assigned to the Application Administrator role. This is a limited use duty which cannot be assigned to any other roles aside from the provided application administrator role.

- **Administrator Console Duty**

  Grants access to the Security folder on the Settings menu where security roles, duties and privileges are managed. The default security configuration has this duty assigned to the Application Administrator role. This is a limited use duty which cannot be assigned to any other roles aside from the provided application administrator role.

- **Application Global Menu Duties**

  These duties grant access to links in the Application Navigator which allow users to launch into another application in the Merchandising suite. The default security configuration does not have these duties assigned to any roles.

- **Documentation Summarization Inquiry Duty**

  Grants access to the digital assistant chat feature where users can ask questions and get responses from an AI assistant which utilizes our solution documentation as a source. This is a unique duty in that it should only be associated with the Digital Assistant Chat Viewer role, and the Digital Assistant Chat Viewer role should be associated with any user which should have access rather than associating this duty with the desired role.

Limited Use Duties

There are limited use duties which provide access, but only to the application administrator role provided in the default security configuration. These duties cannot be mapped to any other roles.

- **Settings Menu Duty**

  Grants access to the Settings menu except for the Security folder. The default security configuration has this duty assigned to the Application Administrator role.

- **Administrator Console Duty**

  Grants access to the Security folder on the Settings menu where security roles, duties and privileges are managed. The default security configuration has this duty assigned to the Application Administrator role.

Determining Access for your Organization

When determining access for a given role in your organization, start by categorizing each role with a duty type for each functional area in the application. For example, a Sales Audit Analyst may be a viewer and a contributor store days, transactions, totals and rules. They may have no access to system options, maintaining employees and bank store relationships.

Duty Definitions

For ease of mapping privileges to roles, privileges are logically grouped into duties. Duties may contain one or more privileges as well as other duties.

Table 3-1 lists the privileges contained in each of the predefined duties provided in the default configuration:

Table 3-1 Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Administration - Application Navigator	Allocation Global Menu Duty	This is a duty that is used to grant access to the Allocation link in the Application Navigator in the sidebar menu. To see this link display you must also define the link and URL in the Application Navigator screen in the ORAAC Tasks list. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assigned to any roles in the initial security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - Application Navigator	Invoice Matching Global Menu Duty	This is a duty that is used to grant access to the Invoice Matching link in the Application Navigator in the sidebar menu. To see this link display you must also define the link and URL in the Application Navigator screen in the ORAAC Tasks list. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assigned to any roles in the initial security configuration.	No privileges included, assigning the duty to a role grants access.

Table 3-1 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Administration - Application Navigator	Merchandising Global Menu Duty	This is a duty that is used to grant access to the Merchandising link in the Application Navigator in the sidebar menu. To see this link display you must also define the link and URL in the Application Navigator screen in the ORAAC Tasks list. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assigned to any roles in the initial security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - Application Navigator	Pricing Global Menu Duty	This is a duty that is used to grant access to the Pricing link in the Application Navigator in the sidebar menu. To see this link display you must also define the link and URL in the Application Navigator screen in the ORAAC Tasks list. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assigned to any roles in the initial security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - Application Navigator	Sales Audit Global Menu Duty	This is a duty that is used to grant access to the Sales Audit link in the Application Navigator in the sidebar menu. To see this link display you must also define the link and URL in the Application Navigator screen in the ORAAC Tasks list. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assigned to any roles in the initial security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - Batch	Batch Management Duty	A duty for running batch process.	Execute Batch Jobs Priv
Administration – Documentation Summarization	Documentation Summarization Inquiry Duty	A duty for accessing the documentation summarization feature that allows users to ask the system questions about supported capabilities or how to perform tasks in Allocation. The system will summarize findings from multiple documentation sources and return the relevant results in the chat. Rather than assigning this duty to grant access to a particular role, this duty is assigned to the Digital Assistant Chat Viewer role. This role should be associated with any user for whom you want to grant access.	View Documentation Summarization Priv

Table 3-1 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Administration - Settings Administrator Console	Administrator Console Duty	This is a duty that is used to grant access to the ORAAC Security folder and tasks under this folder on the Settings menu. There are no privileges within the duty, associating this duty to a role will grant access. This duty can only be assigned to the Application Administrator role provided in the default security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - Settings Menu	Settings Menu Duty	A duty for accessing the Settings menu in the sidebar navigation menu, with all non-security related folders and links. This duty can only be assigned to the Application Administrator role provided in the default security configuration.	No privileges included, assigning the duty to a role grants access.
Administration - System Options	System Options Inquiry Duty	A duty for viewing system options.	View System Options Priv
Administration - System Options	User Group Properties Management Duty	A duty for managing user group properties tab system options. This duty is an extension of the System Options Inquiry Duty.	System Options Inquiry Duty Maintain User Group Properties Priv
Administration - System Options	System Properties Management Duty	A duty for managing the system properties tab in system options. This duty is an extension of the System Options Inquiry Duty.	System Options Inquiry Duty Maintain System Properties Priv
Allocations	Allocation Inquiry Duty	A duty for viewing allocations.	Search Allocations Priv View Allocations Priv
Allocations	Allocation Management Duty	A duty for maintaining, deleting and submitting allocations. This duty is an extension of the Allocation Inquiry Duty.	Allocation Inquiry Duty Maintain Allocations Priv Delete Allocations Priv
Allocations	Allocation Submission Duty	A duty for submitting an allocation.	Submit Allocations Priv
Allocations	Allocation Approval Duty	A duty for approving or rejecting an allocation.	Approve Allocations Priv
Auto Quantity Limits	Auto Quantity Limits Inquiry Duty	A duty for viewing Auto Quantity Limits.	Search Auto Quantity Limits Priv View Auto Quantity Limits Priv
Auto Quantity Limits	Auto Quantity Limits Management Duty	A duty for managing Auto Quantity Limits. This duty is an extension of the Auto Quantity Limits Inquiry Duty.	Auto Quantity Limits Inquiry Duty Maintain Auto Quantity Limits Priv
Dashboard	Allocation Dashboard Duty	A duty for viewing the dashboard.	View Allocation Dashboard View Analytic Dashboard Priv

Table 3-1 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Location Groups	Location Groups Search Duty	A duty for searching for allocation location groups.	Search Location Groups Priv
Location Groups	Location Groups Inquiry Duty	A duty for viewing allocation location groups.	View Location Groups Priv
Location Groups	Location Groups Management Duty	A duty for managing allocation location groups. This duty is an extension of the Allocation Location Groups Search and Inquiry Duties.	Location Groups Search Duty Location Groups Inquiry Duty Maintain Location Groups Priv Delete Location Groups Priv
Policy Templates	Policy Template Search Duty	A duty for searching for allocation policy templates.	Search Policy Templates Priv
Policy Templates	Policy Template Inquiry Duty	A duty for viewing allocation policy templates.	View Policy Templates Priv
Policy Templates	Policy Template Management Duty	A duty for managing allocation policy template. This duty is an extension of the Allocation Policy Template Search and Inquiry Duties.	Policy Template Search Duty Policy Template Inquiry Duty Maintain Policy Templates Priv Delete Policy Templates Priv
Size Profiles	Size Profile Inquiry Duty	A duty for viewing size profiles.	Search Size Profiles Priv View Size Profiles Priv
Size Profiles	Size Profile Management Duty	A duty for managing size profiles. This duty is an extension of the Size Profile Inquiry Duty.	Size Profile Inquiry Duty Maintain Size Profiles Priv Delete Size Profiles Priv

Duty to Role Mappings

The job roles provided in the default security configuration have the following duties assigned to control their levels of access:

Table 3-2 Application Administrator

Functional Area	Access Level	Duty Assigned
Administration - Batch	Access Granted	Batch Management Duty
Administration – Documentation Summarization	Access Granted	Assign the Digital Assistant Chat Viewer job role (CHATBOT_VIEW_JOB) to the user to grant access.
Administration - Settings Administrator Console	Access Granted	Administrator Console Duty
Administration - Settings Menu	Access Granted	Settings Menu Duty

Table 3-2 (Cont.) Application Administrator

Functional Area	Access Level	Duty Assigned
Administration - System Options	High Security	System Options User Group Properties Management Duty System Options System Properties Management Duty
Allocations	Approval	Allocation Management Duty Allocation Submission Duty Allocation Approval Duty
Auto Quantity Limits	Management	Auto Quantity Limits Management Duty
Dashboard	Access Granted	Allocation Dashboard Duty
Location Groups	Management	Location Groups Management Duty
Policy Templates	Management	Policy Template Management Duty
Size Profiles	Management	Size Profile Management Duty

Table 3-3 Allocator

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration – Documentation Summarization	Access Granted	Assign the Digital Assistant Chat Viewer job role (CHATBOT_VIEW_JOB) to the user to grant access.
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	Inquiry	System Options Inquiry Duty
Allocations	Approval	Allocation Management Duty Allocation Submission Duty Allocation Approval Duty
Auto Quantity Limits	Management	Auto Quantity Limits Management Duty
Dashboard	Access Granted	Allocation Dashboard Duty
Location Groups	Management	Location Groups Management Duty
Policy Templates	Management	Policy Template Management Duty
Size Profiles	Management	Size Profile Management Duty

Table 3-4 Allocation Manager

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration – Documentation Summarization	Access Granted	Assign the Digital Assistant Chat Viewer job role (CHATBOT_VIEW_JOB) to the user to grant access.

Table 3-4 (Cont.) Allocation Manager

Functional Area	Access Level	Duty Assigned
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	Management	System Options User Group Properties Management Duty
Allocations	Approval	Allocation Management Duty Allocation Submission Duty Allocation Approval Duty
Auto Quantity Limits	Management	Auto Quantity Limits Management Duty
Dashboard	Access Granted	Allocation Dashboard Duty
Location Groups	Management	Location Groups Management Duty
Policy Templates	Management	Policy Template Management Duty
Size Profiles	Management	Size Profile Management Duty

Table 3-5 Buyer

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration – Documentation Summarization	Access Granted	Assign the Digital Assistant Chat Viewer job role (CHATBOT_VIEW_JOB) to the user to grant access.
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	No Access	
Allocations	Inquiry	Allocation Inquiry Duty
Auto Quantity Limits	No Access	
Dashboard	No Access	
Location Groups	Inquiry	Location Groups Search Duty Location Groups Inquiry Duty
Policy Templates	Inquiry	Policy Template Search Duty Policy Template Inquiry Duty
Size Profiles	Inquiry	Size Profile Inquiry Duty

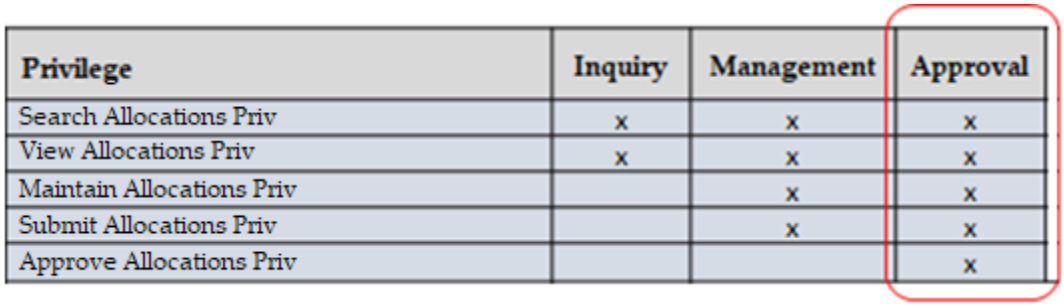
Table 3-6 Digital Assistant Chat Viewer

Functional Area	Access Level	Duty Assigned
Administration – Documentation Summarization	Access Granted	Assign the Digital Assistant Chat Viewer job role (CHATBOT_VIEW_JOB) to the user to grant access.

Privileges

For each functional area in the application there is an associated set of privileges. The privileges build upon each other. For example, in order to be able to approve an allocation, the user must also be able to search for, view, create, maintain and submit allocations. Therefore, the Allocation Approval Duty contains the Search Allocations, View Allocations, Maintain Allocations, Submit Allocations and Approve Allocations privileges.

Figure 3-1 Privileges for Users



Privilege	Inquiry	Management	Approval
Search Allocations Priv	x	x	x
View Allocations Priv	x	x	x
Maintain Allocations Priv		x	x
Submit Allocations Priv		x	x
Approve Allocations Priv			x

Privilege Definitions

Table 3-7 lists all of the privileges available in Allocation:

Table 3-7 Privileges Available in Allocation

Functional Area	Privilege	Privilege Description
Administration - Batch	Execute Batch Jobs Priv	A privilege for running batch jobs in the Allocation application.
Administration - Documentation Summarization	View Documentation Summarization Priv	A privilege for accessing the documentation summarization feature that allows users to ask the system questions about supported capabilities or how to perform tasks in Allocation. The system will summarize findings from multiple documentation sources and return the relevant results.
Administration - System Options	View System Options Priv	A privilege for viewing System Options.
Administration - System Options	Maintain User Group Properties Priv	A privilege for editing the user group properties for System Options.
Administration - System Options	Maintain System Properties Priv	A privilege for editing the System Properties for System Options.
Allocations	Search Allocations Priv	A privilege for searching for allocations.
Allocations	View Allocations Priv	A privilege for viewing an allocation.
Allocations	Maintain Allocations Priv	A privilege for creating, maintaining, and editing an allocation via Create Standard Allocation, Create What-if Allocation, Create Scheduled Allocation, My Worksheets and Quick Create Allocation.
Allocations	Delete Allocations Priv	A privilege for deleting an allocation.
Allocations	Submit Allocations Priv	A privilege for submitting an allocation for approval.

Table 3-7 (Cont.) Privileges Available in Allocation

Functional Area	Privilege	Privilege Description
Allocations	Approve Allocations Priv	A privilege for approving or rejecting an allocation.
Auto Quantity Limits	Search Auto Quantity Limits Priv	A privilege for searching for Auto Quantity Limits.
Auto Quantity Limits	View Auto Quantity Limits Priv	A privilege for viewing for Auto Quantity Limits.
Auto Quantity Limits	Maintain Auto Quantity Limits Priv	A privilege for editing for Auto Quantity Limits.
Dashboard	View Allocation Dashboard Priv	A privilege for viewing the dashboard.
Location Groups	Search Location Groups Priv	A privilege for searching for allocations.
Location Groups	View Location Groups Priv	A privilege for viewing location groups.
Location Groups	Maintain Location Groups Priv	A privilege for creating and editing and location groups.
Location Groups	Delete Location Groups Priv	A privilege for deleting location groups.
Policy Templates	Search Policy Templates Priv	A privilege for searching for policy templates.
Policy Templates	View Policy Templates Priv	A privilege for viewing a Policy Template.
Policy Templates	Maintain Policy Templates Priv	A privilege for creating and editing a Policy Template.
Policy Templates	Delete Policy Templates Priv	A privilege for deleting a Policy Template.
Size Profiles	Search Size Profiles Priv	A privilege for searching Size Profiles.
Size Profiles	View Sizes Profiles Priv	A privilege for viewing a Size Profile.
Size Profiles	Maintain Size Profiles Priv	A privilege for creating and editing and a Size Profile.
Size Profiles	Delete Size Profiles Priv	A privilege for deleting a Size Profile.

A

Appendix A – Role Identifiers

Each role in the system has an identifier which is displayed in the security administration screens with a Role Type of Job. Table A-1 lists each role and its identifier.

Table A-1 Role Identifier

Role	Role Identifier
Application Administrator	ALLOCATION_APPLICATION_ADMINISTRATOR_JOB
Allocator	ALLOCATOR_JOB
Allocation Manager	ALLOCATION_MANAGER_JOB
Buyer	BUYER_JOB
Digital Assistant Chat Viewer	CHATBOT_VIEW_JOB

B

Appendix B – Duty Identifiers

Each duty in the system has an identifier which is displayed in the security administration screens. Table B-1 list of each duty and its identifier.

Table B-1 Duty Identifiers

Functional Area	Duty	Duty Identifier
Administration - Application Navigator	Allocation Global Menu Duty	ALLOC_GLOBAL_MENU_DUTY
Administration - Application Navigator	Invoice Matching Global Menu Duty	REIM_GLOBAL_MENU_DUTY
Administration - Application Navigator	Merchandising Global Menu Duty	RMS_GLOBAL_MENU_DUTY
Administration - Application Navigator	Pricing Global Menu Duty	PRICING_GLOBAL_MENU_DUTY
Administration - Application Navigator	Sales Audit Global Menu Duty	RESA_GLOBAL_MENU_DUTY
Administration - Batch	Batch Management Duty	ALC_ALLOC_BATCH_DUTY
Administration - Documentation Summarization	Documentation Summarization Inquiry Duty	DOCUMENTATION_SUMM_INQUIRY_DUTY
Administration - Settings Administrator Console	Administrator Console Duty	ADMIN_CONSOLE_DUTY
Administration - Settings Menu	Settings Menu Duty	SETTINGS_MENU_DUTY
Administration - System Options	System Options Inquiry Duty	ALC_ALLOC_SYSTEM_OPTIONS_INQUIRY_DUTY
Administration - System Options	User Group Properties Management Duty	ALC_ALLOC_SYSTEM_OPTIONS_USER_GROUP_MANAGEMENT_DUTY
Administration - System Options	System Properties Management Duty	ALC_ALLOC_SYSTEM_OPTIONS_SYSTEM_PROPERTIES_MANAGEMENT_DUTY
Allocations	Allocation Inquiry Duty	ALC_ALLOC_INQUIRY_DUTY
Allocations	Allocation Management Duty	ALC_ALLOC_MANAGEMENT_DUTY
Allocations	Allocation Submission Duty	ALC_ALLOC_SUBMIT_DUTY
Allocations	Allocation Approval Duty	ALC_ALLOC_REVIEW_DUTY
Auto Quantity Limits	Auto Quantity Limits Inquiry Duty	ALC_ALLOC_AUTO_QUANTITY_LIMITS_INQUIRY_DUTY
Auto Quantity Limits	Auto Quantity Limits Management Duty	ALC_ALLOC_AUTO_QUANTITY_LIMITS_MANAGEMENT_DUTY
Dashboard	Allocation Dashboard Duty	ALC_DASHBOARD_DUTY
Location Groups	Location Groups Search Duty	ALC_ALLOC_LOC_GROUPS_SEARCH_DUTY
Location Groups	Location Groups Inquiry Duty	ALC_ALLOC_LOC_GROUPS_INQUIRY_DUTY
Location Groups	Location Groups Management Duty	ALC_ALLOC_LOC_GROUPS_MANAGEMENT_DUTY

Table B-1 (Cont.) Duty Identifiers

Functional Area	Duty	Duty Identifier
Policy Templates	Policy Template Search Duty	ALC_ALLOC_POLICY_MAINTENANCE_SEARCH_DUTY
Policy Templates	Policy Template Inquiry Duty	ALC_ALLOC_POLICY_MAINTENANCE_INQUIRY_DUTY
Policy Templates	Policy Template Management Duty	ALC_ALLOC_POLICY_MAINTENANCE_MANAGEMENT_DUTY
Size Profiles	Size Profile Inquiry Duty	ALC_ALLOC_SIZE_PROFILE_INQUIRY_DUTY
Size Profiles	Size Profile Management Duty	ALC_ALLOC_SIZE_PROFILE_MANAGEMENT_DUTY

C

Appendix C – Privilege Identifiers

Each privilege in the system has an identifier which is displayed in the security administration screens. Table C-1 list of each privilege and its identifier.

Table C-1 Privilege Identifiers

Functional Area	Privilege	Privilege Identifier
Administration - Batch	Execute Batch Jobs Priv	ALC_ALLOC_BATCH_PRIV
Administration - Documentation Summarization	View Documentation Summarization Priv	VIEW_DOCUMENTATION_SUMM_PRIV
Administration - System Options	View System Options Priv	ALC_ALLOC_SYSTEM_OPTIONS_VIEW_PRIV
Administration - System Options	Maintain User Group Properties Priv	ALC_ALLOC_SYSTEM_OPTIONS_USER_GROUP_MAINTAIN_PRIV
Administration - System Options	Maintain System Properties Priv	ALC_ALLOC_SYSTEM_OPTIONS_SYSTEM_PROPERTIES_MAINTAIN_PRIV
Allocations	Search Allocations Priv	ALC_ALLOC_SEARCH_PRIV
Allocations	View Allocations Priv	ALC_ALLOC_VIEW_PRIV
Allocations	Maintain Allocations Priv	ALC_ALLOC_MAINTAIN_PRIV
Allocations	Delete Allocations Priv	ALC_ALLOC_DELETE_PRIV
Allocations	Submit Allocations Priv	ALC_ALLOC_SUBMIT_PRIV
Allocations	Approve Allocations Priv	ALC_ALLOC_REVIEW_PRIV
Auto Quantity Limits	Search Auto Quantity Limits Priv	ALC_ALLOC_AUTO_QUANTITY_LIMITS_SEARCH_PRIV
Auto Quantity Limits	View Auto Quantity Limits Priv	ALC_ALLOC_AUTO_QUANTITY_LIMITS_VIEW_PRIV
Auto Quantity Limits	Maintain Auto Quantity Limits Priv	ALC_ALLOC_AUTO_QUANTITY_LIMITS_MAINTAIN_PRIV
Dashboard	View Allocation Dashboard Priv	ALC_DASHBOARD_PRIV
Location Groups	Search Location Groups Priv	ALC_ALLOC_LOC_GROUPS_SEARCH_PRIV
Location Groups	View Location Groups Priv	ALC_ALLOC_LOC_GROUPS_VIEW_PRIV
Location Groups	Maintain Location Groups Priv	ALC_ALLOC_LOC_GROUPS_MAINTAIN_PRIV
Location Groups	Delete Location Groups Priv	ALC_ALLOC_LOC_GROUPS_DELETE_PRIV
Policy Templates	Search Policy Templates Priv	ALC_ALLOC_POLICY_MAINTENANCE_SEARCH_PRIV
Policy Templates	View Policy Templates Priv	ALC_ALLOC_POLICY_MAINTENANCE_VIEW_PRIV
Policy Templates	Maintain Policy Templates Priv	ALC_ALLOC_POLICY_MAINTENANCE_MAINTAIN_PRIV
Policy Templates	Delete Policy Templates Priv	ALC_ALLOC_POLICY_MAINTENANCE_DELETE_PRIV
Size Profiles	Search Size Profiles Priv	ALC_ALLOC_SIZE_PROFILE_SEARCH_PRIV

Table C-1 (Cont.) Privilege Identifiers

Functional Area	Privilege	Privilege Identifier
Size Profiles	View Sizes Profiles Priv	ALC_ALLOC_SIZE_PROFILE_VIEW_PRIV
Size Profiles	Maintain Size Profiles Priv	ALC_ALLOC_SIZE_PROFILE_MAINTAIN_PRIV
Size Profiles	Delete Size Profiles Priv	ALC_ALLOC_SIZE_PROFILE_DELETE_PRIV

D

Appendix D – Implementation Considerations

This appendix describes duties or privileges needed for implementation.

Retired Duties or Privileges

The following duties and privileges are available in ORAAC for Allocation, but they should not be utilized as they are not used by Allocation and will be completely removed in an upcoming release.

1. If the following duties and privileges are present in ORAAC, do the following:

   In ORAAC, navigate to **Security** -> **Role Mappings** and search for every instance of the following DUTIES and delete them. Then, navigate to **Security** -> **Roles** and delete them.

   - ALC_ALLOC_SUPER_USER_DUTY
   - ALC_BUYER_DASHBOARD_DUTY
   - ROLE_MANAGER_DUTY

2. In ORAAC, navigate to **Security** -> **Role Mappings** and search for every instance of the following PRIVS and delete them.

   - ALC_ALLOC_SUPER_USER_PRIV
   - ALC_BUYER_ANALYTIC_DASHBOARD_PRIV
   - ALC_ANALYTIC_DASHBOARD_PRIV