Oracle® Retail Sales Audit

Security Guide

Release 19.0

F26187-01

January 2020

ORACLE®

Oracle Retail Sales Audit Security Guide , Release 19.0 for Windows

F26187-01

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

Primary Author:

Contributing Author:

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

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

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

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

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

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

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

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

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR

Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

1 Overview

Application Functional Security 1-1
Roles 1-1
Duties 1-1
Privileges 1-1
Data Filtering 1-1

2 Roles

Roles Provided at Initial Setup 2-2

3 Duties and Privileges

Duties Provided at Initial Setup 3-1
Duty to Role Mappings 3-2
Privileges 3-5
Privileges Available in Merchandising 3-6
Privileges for the Predefined Duties 3-9

A Appendix A – Role Identifiers

B Appendix B – Duty Identifiers

C Appendix C – Privilege Identifiers

D Appendix D – Implementation Considerations

New Duties or Privileges D-1
Retired Duties or Privileges D-1

1

Overview

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

Application Functional Security

Sales Audit 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 a Sales Audit Analyst or Sales Audit 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 one must perform in the context of their job. Duties in Sales Audit 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 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 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 Sales Audit, there is no additional configuration that is needed at the merchandise hierarchy level, but for the users to access stores or perform activities at the store level, they need to be assigned to the Location Traits to which the store is mapped against. However, all Sales Audit 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 to a transaction which are a part of the merchandise hierarchy to which they have been given data filtering access. Likewise, users will only be able to create a store day and further add transactions to it for auditing that are part of the organizational hierarchy to which they have been given data filtering access.

When viewing or maintaining store days, users will only be able to view and maintain existing store days for the stores to which they have access. For transactions, users will only be able to view and maintain existing transactions if they have access to at least one item or location contained in the transactions. This is controlled through the manage transaction screens for the transactions.

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

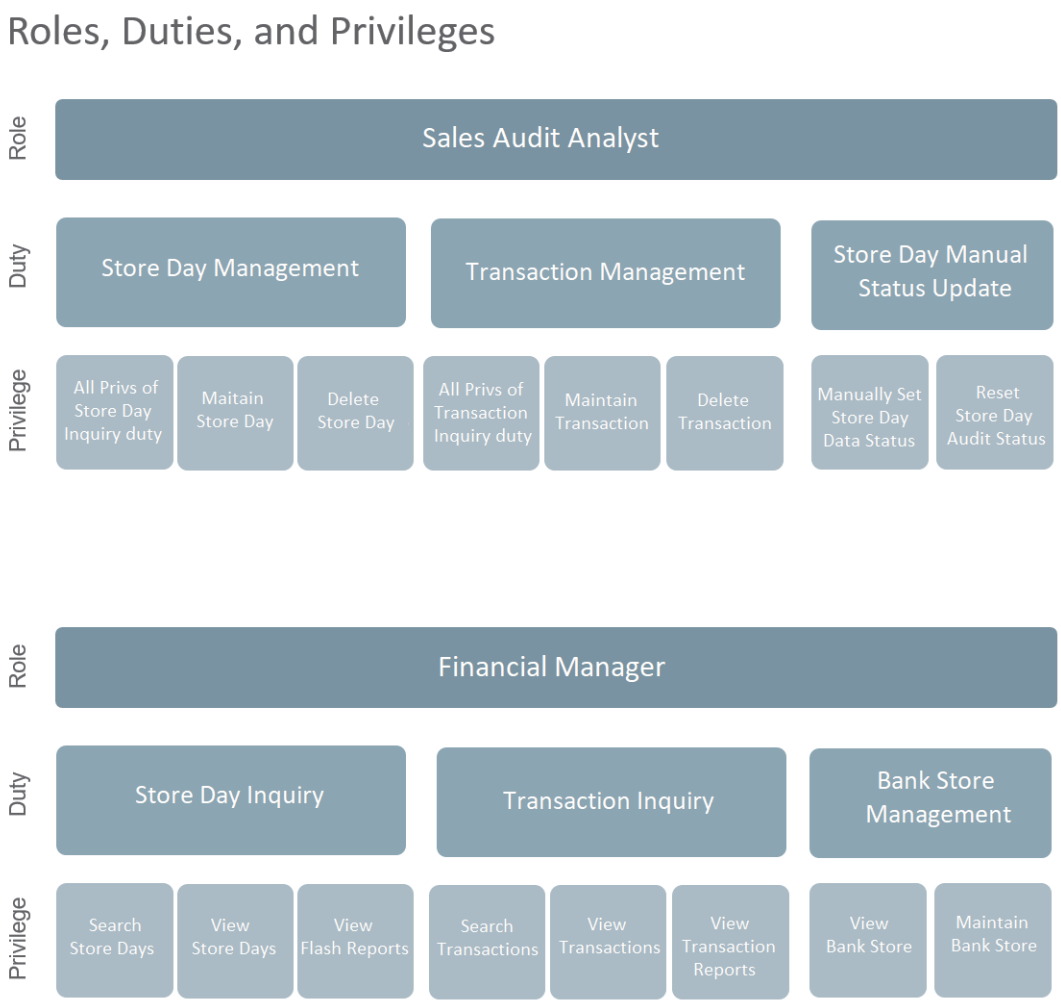
2

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 Sales Audit, a user with a business role of Sales Audit Analyst may be able to perform only the tasks associated to a Sales Audit Analyst job role profile such as, viewing, maintaining and deleting store days and transactions. This role might additionally access to set the store day statuses that might be needed to audit the store days manually. Whereas, a Financial Manager might have access to only search and view store days and transactions, view and maintain bank store relationships. While, an Administrator would require access to all the areas.

Figure 2–1 Sales Audit 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 Sales Audit'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:

- Sales Audit Application Administrator
- Sales Audit Analyst
- Sales Audit Manager
- Financial Manager

Sales Audit Application Administrator

The Application Administrator is a part of a retailer's IT department responsible for maintaining and configuring the Sales Audit 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.

Sales Audit Analyst

The Sales Auditor is responsible for reviewing the sales data from the stores that assigned to them, reviewing any errors or exceptions and investigating and making corrections as necessary to ensure that stores sales logs are clean and closed on a timely basis so that this data can be passed on to other systems such as Merchandising, Inventory, and Financials. Primary responsibilities include; - Review, investigate and correct audit errors - Close each store day in as timely a manner as possible - Identify reasons for Over Shorts and correct if possible - identify any recurring patterns of errors or Over Shorts and raise concerns to manager.

Sales Audit Manager

The Sales Audit Manager manages a team of Sales Auditors who review transactions and any exceptions or errors raised by the sales audit process and systems, investigates the exceptions and makes any corrections that are required so that clean sales data can be passed on to other systems such as Merchandising, Inventory Management, and Financials, among others. The sales audit manager is typically responsible for the same processes and responsibilities at the sales auditors, plus others such as - Managing workload of the auditors - Developing rules for use in the sales audit process - Ensuring all sales auditors are meeting goals and timelines for auditing and closing stores - Helping auditors to identify patterns of irregularities and possible loss prevention issues - Identifying consistent areas of concern across locations.

Financial Manager

Responsible for the financial accounting of a retailer's business, which includes making sure that all financial operations are running smoothly, bills are paid on time, figures are reported timely and accurately, period end books are closed properly. This includes:

- Ensuring period end reporting is completed in a timely manner.
- Ensuring the timely resolution of auditing issues.
- Ensuring in the timely resolution of vendor payment issues, including the resolving cost and other invoicing discrepancies- Identifying risks and opportunity areas to the operations.
- Providing performance reporting highlighting trends and opportunities to assist in improving profits, margins and reducing costs.

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 Sales Audit'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*.

Duties

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 or in other words maintain information in Sales Audit. Management duties may contain either the inquiry duty or the review duty for the same entity. For example, the Transaction Management Duty contains the Transaction Inquiry Duty along with the additional Maintain Transaction Privilege and Delete Transaction Privilege, because in order for users to maintain an entity, they must also have the ability to search for and view the entity. The Error Override Management Duty contains the Edit Override Error Privilege along with Error Override Review Duty. Management duties are assigned to contributors of an area.

- Review

  A review duty is meant for users with the authority to either review, or review and approve submissions. For example, the Total Definition Review duty and Audit Rule Review duty contains the access to approve or disable a Total and a Rule respectively. Also, other Review duties such as Error Override Review duty contains the access to only view the Error List on the screens. Review duties are assigned to reviewers of an area.

There are some duties used within Sales Audit that do 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 or task. 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 it's view only. For example:

- **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 Settings menu, including the Security folder where security roles, duties and privileges are managed. The default security configuration has this duty assigned to the 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. In order to see the links they must also be defined via the Application Navigator screen in the ORAAC Tasks list. . The default security configuration does not have these duties assigned to any roles.

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.

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

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 3–1 Application Administrator

Functional Area	Access Level	Duty Assigned
Administration - Batch	Management	Batch Management Duty
Administration - Settings Administrator Console	Access Granted	Administrator Console Duty
Administration - Settings Menu	Access Granted	Settings Menu Duty
Administration - System Options	Management	Application Administration Management Duty
Administration - Web Services	Access Granted	Web Service Access Duty

Table 3–1 (Cont.) Application Administrator

Functional Area	Access Level	Duty Assigned
Audit Rules	Review	Audit Rule Management Duty Audit Rule Submit Duty Audit Rule Review Duty
Automated Clearing House (ACH)	Management	ACH Information Management Duty
Bank Store	Management	Bank Store Management Duty
Dashboard - Sales Audit	Access Granted	Sales Audit Dashboard Inquiry Duty
Data Loading - Financial Administration	Management	Finance Admin Management Duty
Data Loading - Foundation	Management	Foundation Data via Spreadsheet Management Duty
Data Loading - Status	Management	Data Loading Status Management Duty
Employees	Management	Employee Management Duty
Field Access - Error Override	Management	Error Override Management Duty
Field Access - HQ Reported	Management	Totals HQ Reported Value Management Duty
Field Access - Over/Short	Inquiry	Over/Short Value Inquiry Duty
Field Access - System Calculated	Inquiry	Totals System Calculated Value Inquiry Duty
General Ledger	Inquiry	General Ledger Inquiry Duty
Store Day	Review	Store Day Management Duty Store Day Reopen Duty
Totals Definition	Review	Total Definition Management Duty Total Definition Submit Duty Total Definition Review Duty
Transactions	Review	Transaction Management Duty Transaction Post Void Duty

Table 3–2 Sales Audit Analyst

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	No Access	
Administration - Web Services	No Access	
Audit Rules	Review	Audit Rule Management Duty Audit Rule Submit Duty Audit Rule Review Duty
Automated Clearing House (ACH)	Management	ACH Information Management Duty
Bank Store	No Access	
Dashboard - Sales Audit	Access Granted	Sales Audit Dashboard Inquiry Duty
Data Loading - Financial Administration	No Access	
Data Loading - Foundation	No Access	
Data Loading - Status	No Access	
Employees	No Access	
Field Access - Error Override	Management	Error Override Management Duty

Table 3–2 (Cont.) Sales Audit Analyst

Functional Area	Access Level	Duty Assigned
Field Access - HQ Reported	Management	Totals HQ Reported Value Management Duty
Field Access - Over/Short	Inquiry	Over/Short Value Inquiry Duty
Field Access - System Calculated	Inquiry	Totals System Calculated Value Inquiry Duty
General Ledger	No Access	
Store Day	Management	Store Day Management Duty Store Day Manual Status Update Duty
Totals Definition	Review	Total Definition Management Duty Total Definition Submit Duty Total Definition Review Duty
Transactions	Review	Transaction Management Duty Transaction Post Void Duty

Table 3–3 Sales Audit Manager

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	No Access	
Administration - Web Services	No Access	
Audit Rules	Review	Audit Rule Management Duty Audit Rule Submit Duty Audit Rule Review Duty
Automated Clearing House (ACH)	Management	ACH Information Management Duty
Bank Store	No Access	
Dashboard - Sales Audit	Access Granted	Sales Audit Dashboard Inquiry Duty
Data Loading - Financial Administration	Management	Finance Admin Management Duty
Data Loading - Foundation	Management	Foundation Data via Spreadsheet Management Duty
Data Loading - Status	Management	Data Loading Status Management Duty
Employees	Management	Employee Management Duty
Field Access - Error Override	Management	Error Override Management Duty
Field Access - HQ Reported	Management	Totals HQ Reported Value Management Duty
Field Access - Over/Short	Inquiry	Over/Short Value Inquiry Duty
Field Access - System Calculated	Inquiry	Totals System Calculated Value Inquiry Duty
General Ledger	No Access	

Table 3–3 (Cont.) Sales Audit Manager

Functional Area	Access Level	Duty Assigned
Store Day	Review	Store Day Management Duty Store Day Reopen Duty
Totals Definition	Review	Total Definition Management Duty Total Definition Submit Duty Total Definition Review Duty
Transactions	Review	Transaction Management Duty Transaction Post Void Duty

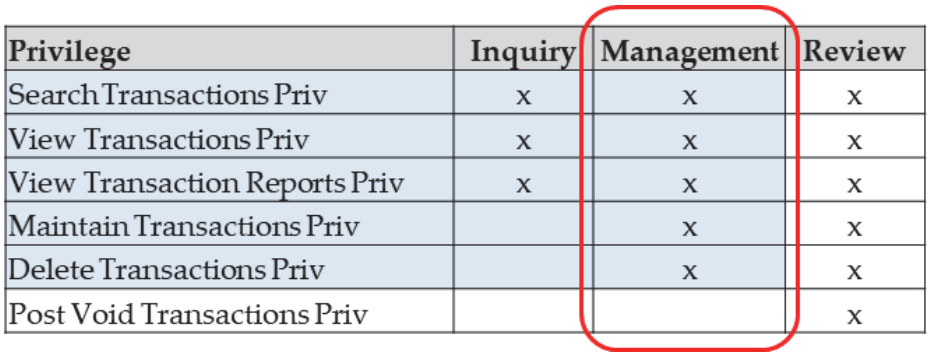
Table 3–4 Financial Manager

Functional Area	Access Level	Duty Assigned
Administration - Batch	No Access	
Administration - Settings Administrator Console	No Access	
Administration - Settings Menu	No Access	
Administration - System Options	No Access	
Administration - Web Services	No Access	
Audit Rules	Inquiry	Audit Rule Inquiry Duty
Automated Clearing House (ACH)	Inquiry	ACH Information Inquiry Duty
Bank Store	Management	Bank Store Management Duty
Dashboard - Sales Audit	Access Granted	Sales Audit Dashboard Inquiry Duty
Data Loading - Financial Administration	Management	Finance Admin Management Duty
Data Loading - Foundation	No Access	
Data Loading - Status	Inquiry	Data Loading Status Inquiry Duty
Employees	No Access	
Field Access - Error Override	Inquiry	Error Override Inquiry Duty
Field Access - HQ Reported	Inquiry	Totals HQ Reported Value Inquiry Duty
Field Access - Over/Short	Inquiry	Over/Short Value Inquiry Duty
Field Access - System Calculated	Inquiry	Totals System Calculated Value Inquiry Duty
General Ledger	Inquiry	General Ledger Inquiry Duty
Store Day	Inquiry	Store Day Inquiry Duty
Totals Definition	Review	Total Definition Management Duty Total Definition Submit Duty Total Definition Review Duty
Transactions	Inquiry	Transaction Inquiry Duty

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 modify a transaction, the user must also be able to search for and view the transactions of a store day. Therefore, the Transaction Management Duty contains the Search Transactions, View Transactions, View Transaction Reports, Maintain Transaction and Delete Transaction privileges.

Figure 3–1 Privileges for Users



Privilege	Inquiry	Management	Review
Search Transactions Priv	x	x	x
View Transactions Priv	x	x	x
View Transaction Reports Priv	x	x	x
Maintain Transactions Priv		x	x
Delete Transactions Priv		x	x
Post Void Transactions Priv			x

Privileges Available in Merchandising

Table 3–5 lists all of the privileges available in Sales Audit, along with the duty type to which they are assigned in the default configuration.

Table 3–5 Privileges Available in Sales Audit

Functional Area	Privilege	Privilege Description
Administration - Batch	Execute Batch Priv	A privilege for running batch
Administration - System Options	View Application Administration Priv	A privilege for viewing system options and the Foundation Data Download screen. Within the Foundation Data Download screen, this privilege provides access the Administration template type in order to download the following to a spreadsheet: Error Messages, Reference Fields, Store Data, and Constants.
Administration - System Options	Maintain Application Administration Priv	A privilege for maintaining system options, and provides access to the Foundation Data Upload screen. Within the Foundation Data Upload screen, this privilege provides access to the Administration template type in order to upload new or updated Error Messages, Reference Fields, Store Data, and Constants.
Administration - Web Services	Maintain Entities via Web Services Priv	A generic privilege for accessing ReST Services
Audit Rules	Search Audit Rule Priv	A privilege for searching for audit rules.
Audit Rules	View Audit Rule Priv	A privilege for viewing audit rules.
Audit Rules	Maintain Audit Rule Priv	A privilege for creating and editing audit rules.
Audit Rules	Delete Audit Rule Priv	A privilege for deleting an audit rule.
Audit Rules	Submit Audit Rule Priv	A privilege for submitting an audit rule for review.
Audit Rules	Approve Audit Rule Priv	A privilege for approving an audit rule.
Audit Rules	Disable Audit Rule Priv	A privilege for disabling an audit rule.
Automated Clearing House (ACH)	View ACH Information Priv	A privilege for viewing Bank ACH and Store ACH information.
Automated Clearing House (ACH)	Maintain ACH Information Priv	A privilege for maintaining Bank ACH and Store ACH information.
Bank Store	View Bank Store Priv	A privilege for viewing Bank Store relationships.
Bank Store	Maintain Bank Store Priv	A privilege for maintaining Bank Store relationships.
Data Loading - Financial Administration	View Finance Admin Priv	A privilege for viewing data under the Finance Administration data loading tempate type via the Foundation Data Download screen, which includes the GL (General Ledger) Cross Reference, Tender Types and Currency Rounding Rules templates.

Table 3–5 (Cont.) Privileges Available in Sales Audit

Functional Area	Privilege	Privilege Description
Data Loading - Financial Administration	Maintain Finance Admin Priv	A privilege for maintaining data under the Finance Administration data loading template via the Foundation Data Upload screen, which includes the GL (General Ledger) Cross Reference, Tender Types and Currency Rounding Rules templates.
Data Loading - Foundation	View ReSA Foundation Data via Spreadsheet Priv	A privilege for viewing data under the Foundation data loading template type via the Foundation Data Download screen, which includes the Location Closings template.
Data Loading - Foundation	Maintain ReSA Foundation Data via Spreadsheet Priv	A privilege for maintaining data under the Foundation data loading template type via the Foundation Data Upload screen, which includes the Location Closings template.
Data Loading - Status	View Data Loading Status Priv	This privilege provides view access to the Data Loading Status screen.
Data Loading - Status	Maintain Data Loading Status Priv	This privilege provides edit access to the Data Loading Status screen.
Employees	View Employees Priv	A privilege for viewing assigned stores for ReSA users via location traits.
Employees	Maintain Employees Priv	A privilege for maintaining assigned stores for ReSA users via location traits.
Field Access - Error Override	View Error Override Priv	A privilege for viewing the Override checkbox on the Error List tab in either the Store Day Summary, Balance Level Summary screens, or on the Sales Audit Errors popup.
Field Access - Error Override	Maintain Error Override Priv	A privilege for editing the Override checkbox on the Error List tab in either the Store Day Summary or Balance Level Summary screens.
Field Access - HQ Reported	View Miscellaneous Totals HQ Reported Value Priv	A privilege for viewing the HQ Reported value on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.
Field Access - HQ Reported	View Over/Short Totals HQ Reported Value Priv	A privilege for viewing the HQ Reported values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens.
Field Access - HQ Reported	Maintain Miscellaneous Totals HQ Reported Value Priv	A privilege for editing the HQ Reported value on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.
Field Access - HQ Reported	Maintain Over/Short Totals HQ Reported Value Priv	A privilege for editing the HQ Reported values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens.
Field Access - Over/Short	View Store Day Summary Over/Short Value Priv	A privilege for viewing the Over/Short value in the Status container in the Store Day Summary screen.
Field Access - Over/Short	View Balance Level Summary Over/Short Value Priv	A privilege for viewing the Over/Short value in the Status container in the Balance Level Summary screen.
Field Access - Over/Short	View Over/Short Totals Trial Over/Short Values Priv	A privilege for viewing the Trial Over/Short values in both the Accounted for and the Accountable containers on the Over/Short Totals tab in either the Store Day Summary or the Balance Level Summary screens.
Field Access - System Calculated	View System Calculated Totals Value Priv	A privilege for viewing the System Reported Totals values in both the Accounted For and the Accountable For containers on the Over/Short Totals tab in either the Store Day Summary or Balance Level Summary screens, as well as on the Miscellaneous Totals tab in either the Store Day Summary or Balance Level Summary screens.

Table 3–5 (Cont.) Privileges Available in Sales Audit

Functional Area	Privilege	Privilege Description
General Ledger	View GL Drill Back Priv	A privilege for viewing General Ledger Drill Back
Store Day	Search Store Days Priv	A privilege for searching for store days and store day total transaction data summary information (transaction data summary).
Store Day	View Flash Reports Priv	A privilege for viewing the Flash Totals and Flash Sales reports accessed via the main Tasks list or via the Store Day Summary screen.
Store Day	View Store Day Priv	A privilege for viewing a store day including error list, over/short totals, miscellaneous totals, combined totals, total export log, revisions of totals (total audit trail), missing transactions, store day import log, store day export log, store day total transaction data summary information (transaction data summary), and comments.
Store Day	Maintain Store Days Priv	A privilege for creating and editing a store day. Editing a store day includes error list, over/short totals, miscellaneous totals, combined totals, total export log, revisions of totals (total audit trail), missing transactions and comments.
Store Day	Delete Store Day Priv	A privilege for deleting a store day.
Store Day	Manually Set Store Day Data Status Priv	A privilege for manually setting a store day's data status.
Store Day	Reset Store Day Audit Status Priv	A privilege for resetting a store day's audit status.
Store Day	Reopen Store Days Priv	A privilege for reopening a store day prior to the account period being closed in RMS for the same store day.
Totals Definition	Search Total Definition Priv	A privilege for searching for total definitions.
Totals Definition	View Total Definition Priv	A privilege for viewing total definitions.
Totals Definition	Maintain Total Definition Priv	A privilege for creating and editing total definitions.
Totals Definition	Delete Total Definition Priv	A privilege for deleting a total definition.
Totals Definition	Submit Total Definition Priv	A privilege for submitting a total definition for review.
Totals Definition	Approve Total Definition Priv	A privilege for approving a total definition.
Totals Definition	Disable Total Definition Priv	A privilege for disabling a total definition.
Transactions	Search Transactions Priv	A privilege for searching for transactions, transaction revisions (audit trail) and transaction summaries (item and tender).
Transactions	View Transactions Priv	A privilege for viewing transactions, transaction revisions (audit trail), transaction summaries (item and tender) and comments.
Transactions	View Transaction Reports Priv	A privilege for viewing the Credit Card Summary, the Transaction Data and the Voucher Activity reports accessed via the main Tasks list.
Transactions	Maintain Transactions Priv	A privilege for creating and editing transactions, mass updating items on transactions via Item Summary, and comments.
Transactions	Delete Transactions Priv	A privilege for deleting transactions
Transactions	Post Void Transactions Priv	A privilege for post voiding transactions

Privileges for the Predefined Duties

Table 3–6 lists the privileges contained in each of the predefined duties provided in the default configuration:

Table 3–6 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. The link must also be added via the Application Navigator screen in order to see the link. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assign to any roles in the default security configuration.	No privileges contained within. 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. The link must also be added via the Application Navigator screen in order to see the link. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assign to any roles in the default security configuration.	No privileges contained within. Assigning the duty to a role grants access.
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. The link must also be added via the Application Navigator screen in order to see the link. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assign to any roles in the default 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. The link must also be added via the Application Navigator screen in order to see the link. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assign to any roles in the default 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. The link must also be added via the Application Navigator screen in order to see the link. There are no privileges within the duty, associating this duty to a role will grant access. This duty is not assign to any roles in the default security configuration.	No privileges contained within. Assigning the duty to a role grants access.
Administration - Batch	Batch Management Duty	A duty for executing batch processes.	Execute Batch Priv
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.	No privileges contained within. Assigning the duty to a role grants access.

Table 3–6 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Administration - Settings Menu	Settings Menu Duty	This is a duty that is used to grant access to the Settings menu in the sidebar navigation menu, with all non-security related folders and links. There are no privileges within this duty, associating the duty to a role will grant access.	No privileges contained within. Assigning the duty to a role grants access.
Administration - System Options	Application Administration Inquiry Duty	A duty for viewing ReSA System Options and downloading data under the Administration template type including Error Messages, Reference Fields, Store Data, and Constants.	View Application Administration Priv
Administration - System Options	Application Administration Management Duty	A duty for managing ReSA System Options and uploading data under the Administration template type including Error Messages, Reference Fields, Store Data, and Constants. This duty is an extension of the Application Administration Inquiry Duty.	Application Administration Inquiry Duty Maintain Application Administration Priv
Administration - Web Services	Web Service Access Duty	A duty for granting the ability to execute web services.	Maintain Entities via Web Services Priv
Audit Rules	Audit Rule Inquiry Duty	A duty for viewing audit rules.	Search Audit Rule Priv View Audit Rule Priv
Audit Rules	Audit Rule Management Duty	A duty for managing audit rules. This duty is an extension of the Audit Rule Inquiry Duty.	Audit Rule Inquiry Duty Maintain Audit Rule Priv Delete Audit Rule Priv
Audit Rules	Audit Rule Submit Duty	A duty for submitting an audit rule for approval.	Submit Audit Rule Priv
Audit Rules	Audit Rule Review Duty	A duty for approving or disabling an audit rule.	Approve Audit Rule Priv Disable Audit Rule Priv
Automated Clearing House (ACH)	ACH Information Inquiry Duty	A duty for viewing ACH information including Bank ACH and Store ACH.	View ACH Information Priv
Automated Clearing House (ACH)	ACH Information Management Duty	A duty for managing ACH information. This duty is an extension of the ACH Information Inquiry Duty.	ACH Information Inquiry Duty Maintain ACH Information Priv
Bank Store	Bank Store Inquiry Duty	A duty for viewing Bank Store.	View Bank Store Priv
Bank Store	Bank Store Management Duty	A duty for managing Bank Store. This duty is an extension of the Bank Store Inquiry Duty.	Bank Store Inquiry Duty Maintain Bank Store Priv
Dashboard - Sales Audit	Sales Audit Dashboard Inquiry Duty	A duty for viewing the Sales Audit Dashboard.	View Sales Audit Dashboard Priv
Data Loading - Financial Administration	Finance Admin Inquiry Duty	A duty for downloading data under the Finance Administration template type including GL (General Ledger) Cross Reference, Tender Types and Currency Rounding Rules.	View Finance Admin Priv
Data Loading - Financial Administration	Finance Admin Management Duty	A duty for uploading data under the Finance Administration template type including GL (General Ledger) Cross Reference and Currency Rounding Rules. This duty is an extension of the Finance Admin Inquiry Duty.	Finance Admin Inquiry Duty Maintain Finance Admin Priv
Data Loading - Foundation	Foundation Data via Spreadsheet Inquiry Duty	A duty for downloading data under the Foundation template type including Location Closings.	View Foundation Data via Spreadsheet Priv

Table 3–6 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Data Loading - Foundation	Foundation Data via Spreadsheet Management Duty	A duty for uploading data under the Foundation template type including Location Closings. This duty is an extension of the Foundation Data via Spreadsheet Inquiry Duty.	Foundation Data Admin Inquiry Duty Maintain Foundation Data via Spreadsheet Priv
Data Loading - Status	Data Loading Status Inquiry Duty	A duty for viewing data loading status.	View Data Loading Status Priv
Data Loading - Status	Data Loading Status Management Duty	A duty for maintaining data loading status. This duty is an extension of the Data Loading Status Inquiry Duty.	Data Loading Status Inquiry Duty Maintain Data Loading Status Priv
Employees	Employee Inquiry Duty	A duty for viewing Employee.	View Employees Priv
Employees	Employee Management Duty	A duty for managing Employee. This duty is an extension of the Employee Inquiry Duty.	Employee Inquiry Duty Maintain Employees Priv
Field Access - Error Override	Error Override Inquiry Duty	A duty for viewing the Override checkbox on the Error List tab on either the Store Day Summary or Balance Level Summary screens, or on the Sales Audit Errors popup.	View Error Override Priv
Field Access - Error Override	Error Override Management Duty	A duty for the ability to override errors by checking the Override checkbox on the Error List tab on either the Store Day Summary or Balance Level Summary screens.	Error Override Review Duty Edit Error Override Priv
Field Access - HQ Reported	Totals HQ Reported Value Inquiry Duty	A duty for viewing the HQ Reported values on both the Over/Short Totals and Miscellaneous Totals tabs on either the Store Day Summary or Balance Level Summary screens.	View Over/Short Totals HQ Reported Value Priv View Miscellaneous Totals HQ Reported Value Priv
Field Access - HQ Reported	Totals HQ Reported Value Management Duty	A duty for the ability to override errors by checking the Override checkbox on the Error List tab on either the Store Day Summary or Balance Level Summary screens.	Totals HQ Reported Value Review Duty Maintain Over/Short Totals HQ Reported Value Priv Maintain Miscellaneous Totals HQ Reported Value Priv
Field Access - Over/Short	Over/Short Value Inquiry Duty	A duty for viewing the Over/Short values in the Status container on either the Store Day Summary or Balance Level Summary screens as well as the Trial Over/Short values on the Over/Short Totals tabs in either the Store Day Summary or Balance Level Summary screens.	View Store Day Summary Over/Short Value Priv View Balance Level Summary Over/Short Value Priv View Over/Short Totals Trial Over/Short Values Priv
Field Access - System Calculated	Totals System Calculated Value Inquiry Duty	A duty for viewing the System Reported values on both the Over/Short Totals and Miscellaneous Totals tabs on either the Store Day Summary or Balance Level Summary screens.	View System Calculated Totals Value Priv
General Ledger	General Ledger Inquiry Duty	A duty for viewing GL drill back.	View GL Drill Back Priv
Store Day	Store Day Inquiry Duty	A duty for viewing store days.	Search Store Days Priv View Store Days Priv View Flash Reports Priv

Table 3–6 (Cont.) Privileges for Predefined Duties

Functional Area	Duty	Duty Description	Duties and Privileges Contained Within
Store Day	Store Day Management Duty	A duty for managing Store Days. This duty is an extension of the Store Day Inquiry Duty.	Store Day Inquiry Duty Maintain Store Days Priv Delete Store Days Priv
Store Day	Store Day Manual Status Update Duty	A duty for setting a Store Day's Data Status and Audit Status.	Manually Set Store Day Data Status Priv Reset Store Day Audit Status Priv
Store Day	Store Day Reopen Duty	A duty for reopening a store day.	Store Day Manual Status Update Duty Reopen Store Day Priv
Total Definitions	Total Definition Inquiry Duty	A duty for viewing total definitions.	Search Total Definition Priv View Total Definition Priv
Total Definitions	Total Definition Management Duty	A duty for managing total definitions. This duty is an extension of the Total Definition Inquiry Duty.	Total Definition Inquiry Duty Maintain Total Definition Priv Delete Total Definition Priv
Total Definitions	Total Definition Submit Duty	A duty for submitting a Total Definition for approval.	Submit Total Definition Priv
Total Definitions	Total Definition Review Duty	A duty for approving or disabling a total definition.	Approve Total Definition Priv Disable Total Definition Priv
Transactions	Transaction Inquiry Duty	A duty for viewing transactions, transaction revisions and transaction summaries.	Search Transactions Priv View Transactions Priv View Transaction Reports Priv
Transactions	Transaction Management Duty	A duty for managing transactions. This duty is an extension of the Transaction Inquiry Duty.	Transaction Inquiry Duty Maintain Transaction Priv Delete Transaction Priv
Transactions	Transaction Post Void Duty	A duty for post voiding a transaction.	Post Void Transaction Priv

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
Sales Audit Application Administrator	RESA_APPLICATION_ADMINISTRATOR_JOB
Sales Audit Analyst	SALES_AUDIT_ANALYST_JOB
Sales Audit Manager	SALES_AUDIT_MANAGER_JOB
Financial Manager	FINANCE_MANAGER_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	RESA_BATCH_DUTY
Administration - Settings Administrator Console	Administrator Console Duty	ADMIN_CONSOLE_DUTY
Administration - Settings Menu	Settings Menu Duty	SETTINGS_MENU_DUTY
Administration - System Options	Application Administration Inquiry Duty	RESA_APPLICATION_ADMINISTRATION_INQUIRY_DUTY
Administration - System Options	Application Administration Management Duty	RESA_APPLICATION_ADMINISTRATION_MGMT_DUTY
Audit Rules	Audit Rule Inquiry Duty	RESA_AUDITRULE_INQUIRY_DUTY
Audit Rules	Audit Rule Management Duty	RESA_AUDITRULE_MGMT_DUTY
Audit Rules	Audit Rule Submit Duty	RESA_AUDITRULE_SUBMIT_DUTY
Audit Rules	Audit Rule Review Duty	RESA_AUDITRULE_REVIEW_DUTY
Automated Clearing House (ACH)	ACH Information Inquiry Duty	RESA_ACHINFO_INQUIRY_DUTY
Automated Clearing House (ACH)	ACH Information Management Duty	RESA_ACHINFO_MGMT_DUTY
Bank Store	Bank Store Inquiry Duty	RESA_BANK_STORE_INQUIRY_DUTY
Bank Store	Bank Store Management Duty	RESA_BANK_STORE_MGMT_DUTY

Table B–1 (Cont.) Duty Identifiers

Functional Area	Duty	Duty Identifier
Data Loading - Financial Administration	Finance Admin Inquiry Duty	RESA_FINANCE_ADMIN_INQUIRY_DUTY
Data Loading - Financial Administration	Finance Admin Management Duty	RESA_FINANCE_ADMIN_MGMT_DUTY
Data Loading - Foundation	Foundation Data via Spreadsheet Inquiry Duty	RESA_FOUNDATION_DATA_VIA_ SPREADSHEET_INQUIRY_DUTY
Data Loading - Foundation	Foundation Data via Spreadsheet Management Duty	RESA_FOUNDATION_DATA_VIA_ SPREADSHEET_MGMT_DUTY
Data Loading - Status	Data Loading Status Inquiry Duty	RESA_DATA_LOADING_STATUS_INQUIRY_ DUTY
Data Loading - Status	Data Loading Status Management Duty	RESA_DATA_LOADING_STATUS_MGMT_DUTY
Employees	Employee Inquiry Duty	RESA_EMPLOYEE_INQUIRY_DUTY
Employees	Employee Management Duty	RESA_EMPLOYEE_MGMT_DUTY
Field Access - Error Override	Error Override Inquiry Duty	RESA_ERRORLIST_OVERRIDE_REVIEW_DUTY
Field Access - Error Override	Error Override Management Duty	RESA_ERRORLIST_OVERRIDE_MGMT_DUTY
Field Access - HQ Reported	Totals HQ Reported Value Inquiry Duty	RESA_TOTALSHQ_REPORTEDVALUE_REVIEW_ DUTY
Field Access - HQ Reported	Totals HQ Reported Value Management Duty	RESA_TOTALSHQ_REPORTEDVALUE_MGMT_ DUTY
Field Access - Over/Short	Over/Short Value Inquiry Duty	RESA_OVERSHORT_VALUE_REVIEW_DUTY
Field Access - System Calculated	Totals System Calculated Value Inquiry Duty	RESA_TOTALS_SYSTEMREPORTEDVALUE_ REVIEW_DUTY
General Ledger	General Ledger Inquiry Duty	RESA_GENERAL_LEDGER_INQUIRY_DUTY
Store Day	Store Day Inquiry Duty	RESA_STOREDAY_INQUIRY_DUTY
Store Day	Store Day Management Duty	RESA_STOREDAY_MGMT_DUTY
Store Day	Store Day Manual Status Update Duty	RESA_STOREDAY_MANUAL_STATUS_UPDATE_ DUTY
Store Day	Store Day Reopen Duty	RESA_STOREDAY_REOPEN_DUTY
Total Definitions	Total Definition Inquiry Duty	RESA_TOTAL_DEFINITION_INQUIRY_DUTY
Total Definitions	Total Definition Management Duty	RESA_TOTAL_DEFINITION_MGMT_DUTY
Total Definitions	Total Definition Submit Duty	RESA_TOTAL_DEFINITION_SUBMIT_DUTY
Total Definitions	Total Definition Review Duty	RESA_TOTAL_DEFINITION_REVIEW_DUTY

Table B–1 (Cont.) Duty Identifiers

Functional Area	Duty	Duty Identifier
Transactions	Transaction Inquiry Duty	RESA_TRANSACTION_INQUIRY_DUTY
Transactions	Transaction Management Duty	RESA_TRANSACTION_MGMT_DUTY
Transactions	Transaction Post Void Duty	RESA_TRANSACTION_POST_VOID_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 Priv	RESA_BATCH_PRIV
Administration - System Options	View Application Administration Priv	VIEW_APPLICATION_ADMINISTRATION_PRIV
Administration - System Options	Maintain Application Administration Priv	MAINTAIN_APPLICATION_ADMINISTRATION_PRIV
Administration - Web Services	Maintain Entities via Web Services Priv	MERCH_SERVICE_ACCESS_PRIV
Audit Rules	Search Audit Rule Priv	SEARCH_AUDITRULE_PRIV
Audit Rules	View Audit Rule Priv	VIEW_AUDITRULE_PRIV
Audit Rules	Maintain Audit Rule Priv	MAINTAIN_AUDITRULE_PRIV
Audit Rules	Delete Audit Rule Priv	DELETE_AUDITRULE_PRIV
Audit Rules	Submit Audit Rule Priv	SUBMIT_AUDITRULE_PRIV
Audit Rules	Approve Audit Rule Priv	APPROVE_AUDITRULE_PRIV
Audit Rules	Disable Audit Rule Priv	DISABLE_AUDITRULE_PRIV
Automated Clearing House (ACH)	View ACH Information Priv	VIEW_ACHINFO_PRIV
Automated Clearing House (ACH)	Maintain ACH Information Priv	MAINTAIN_ACHINFO_PRIV
Bank Store	View Bank Store Priv	VIEW_BANK_STORE_PRIV
Bank Store	Maintain Bank Store Priv	MAINTAIN_BANK_STORE_PRIV
Data Loading - Financial Administration	View Finance Admin Priv	VIEW_FINANCE_ADMIN_PRIV
Data Loading - Financial Administration	Maintain Finance Admin Priv	MAINTAIN_FINANCE_ADMIN_PRIV
Data Loading - Foundation	View ReSA Foundation Data via Spreadsheet Priv	VIEW_FOUNDATION_DATA_VIA_SPREADSHEET_PRIV
Data Loading - Foundation	Maintain ReSA Foundation Data via Spreadsheet Priv	MAINTAIN_FOUNDATION_DATA_VIA_SPREADSHEET_PRIV
Data Loading - Status	View Data Loading Status Priv	VIEW_DATA_LOADING_STATUS_PRIV

Table C–1 (Cont.) Privilege Identifiers

Functional Area	Privilege	Privilege Identifier
Data Loading - Status	Maintain Data Loading Status Priv	MAINTAIN_DATA_LOADING_STATUS_PRIV
Employees	View Employees Priv	VIEW_EMPLOYEE_PRIV
Employees	Maintain Employees Priv	MAINTAIN_EMPLOYEE_PRIV
Field Access - Error Override	View Error Override Priv	FA_VIEW_ERRORLIST_OVERRIDE_PRIV
Field Access - Error Override	Maintain Error Override Priv	FA_MAINTAIN_ERRORLIST_OVERRIDE_PRIV
Field Access - HQ Reported	View Miscellaneous Totals HQ Reported Value Priv	FA_VIEW_MISC_TOTALSHQ_REPORTEDVALUE_PRIV
Field Access - HQ Reported	View Over/Short Totals HQ Reported Value Priv	FA_VIEW_OVERSHORT_TOTALSHQ_REPORTEDVALUE_PRIV
Field Access - HQ Reported	Maintain Miscellaneous Totals HQ Reported Value Priv	FA_MAINTAIN_MISC_TOTALSHQ_REPORTEDVALUE_PRIV
Field Access - HQ Reported	Maintain Over/Short Totals HQ Reported Value Priv	FA_MAINTAIN_OVERSHORT_TOTALSHQ_REPORTEDVALUE_PRIV
Field Access - Over/Short	View Store Day Summary Over/Short Value Priv	FA_VIEW_STOREDAY_SUMMARY_OVERSHORT_VALUE_PRIV
Field Access - Over/Short	View Balance Level Summary Over/Short Value Priv	FA_VIEW_BALANCELEVEL_SUMMARY_OVERSHORT_VALUE_PRIV
Field Access - Over/Short	View Over/Short Totals Trial Over/Short Values Priv	FA_VIEW_OVERSHORT_TOTALS_TRIAL_VALUES_PRIV
Field Access - System Calculated	View System Calculated Totals Value Priv	FA_VIEW_SYSTEMCALCULATED_TOTALSVALUE_PRIV
General Ledger	View GL Drill Back Priv	VIEW_GL_DRILLBACK_PRIV
Store Day	Search Store Days Priv	SEARCH_STOREDAY_PRIV
Store Day	View Flash Reports Priv	VIEW_FLASH_REPORTS_PRIV
Store Day	View Store Day Priv	VIEW_STOREDAY_PRIV
Store Day	Maintain Store Days Priv	MAINTAIN_STOREDAY_PRIV
Store Day	Delete Store Day Priv	DELETE_STOREDAY_PRIV
Store Day	Manually Set Store Day Data Status Priv	SET_STOREDAY_DATA_STATUS_PRIV
Store Day	Reset Store Day Audit Status Priv	RESET_STOREDAY_AUDIT_STATUS_PRIV
Store Day	Reopen Store Days Priv	REOPEN_STOREDAYS_PRIV
Totals Definition	Search Total Definition Priv	SEARCH_TOTAL_DEFINITION_PRIV
Totals Definition	View Total Definition Priv	VIEW_TOTAL_DEFINITION_PRIV
Totals Definition	Maintain Total Definition Priv	MAINTAIN_TOTAL_DEFINITION_PRIV
Totals Definition	Delete Total Definition Priv	DELETE_TOTAL_DEFINITION_PRIV
Totals Definition	Submit Total Definition Priv	SUBMIT_TOTAL_DEFINITION_PRIV
Totals Definition	Approve Total Definition Priv	APPROVE_TOTAL_DEFINITION_PRIV
Totals Definition	Disable Total Definition Priv	DISABLE_TOTAL_DEFINITION_PRIV

Table C–1 (Cont.) Privilege Identifiers

Functional Area	Privilege	Privilege Identifier
Transactions	Search Transactions Priv	SEARCH_TRANSACTIONS_PRIV
Transactions	View Transactions Priv	VIEW_TRANSACTIONS_PRIV
Transactions	View Transaction Reports Priv	VIEW_TRANSACTION_REPORTS_PRIV
Transactions	Maintain Transactions Priv	MAINTAIN_TRANSACTION_PRIV
Transactions	Delete Transactions Priv	DELETE_TRANSACTION_PRIV
Transactions	Post Void Transactions Priv	POST_VOID_TRANSACTION_PRIV

D

Appendix D – Implementation Considerations

This appendix describes duties or privileges needed for implementation.

New Duties or Privileges

There is an existing View GL Drillback privilege that is part of the GL Cross Reference Inquiry duty that is being retired. This privilege needs to be placed in a new duty before removing the existing duty.

1. In ORAAC, navigate to **Security** -> **Roles** and add the following duty:

   RESA_GENERAL_LEDGER_INQUIRY_DUTY

2. This duty should then be added to the job roles that require view access to General Ledger Drillback information.

   This is performed by selecting **Settings** > **Security** > **Role Mappings** and then selecting the job roles that will be assigned the duty and click **Select and Add**.

3. In the **Select and Add** popup choose the new duty. The default base configuration would assign this duty to the following roles:

   RESA_APPLICATION_ADMINISTRATOR_JOB

   FINANCIAL_MANAGER_JOB

4. Add the View GL Drillback Privilege to the New Duty associated with each role. This is performed by selecting **Settings** > **Security** > **Role Mappings** and for each role desired, select the new duty and click **Select and Add**.

5. In the **Select and Add** popup, choose the VIEW_GL_DRILLBACK_PRIV.

Retired Duties or Privileges

The following duties and privileges may be available in ORAAC for Sales Audit, but they should not be utilized as they are not used by the application 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 PRIVS and delete them.

   - VIEW_CURRENCY_ROUNDING_RULES_PRIV
   - MAINTAIN_CURRENCY_ROUNDING_RULES_PRIV
   - VIEW_ERRORMSG_PRIV

- MAINTAIN_ERRORMSG_PRIV
- VIEW_GLCROSSREF_PRIV
- MAINTAIN_GLCROSSREF_PRIV
- VIEW_REFERENCE_FIELDS_PRIV
- MAINTAIN_REFERENCE_FIELDS_PRIV
- VIEW_STORE_DATA_PRIV
- MAINTAIN_STORE_DATA_PRIV
- RAAC_NOTIFICATION_MANAGE_PRIVILEGE

2. The View GL Drillback Privilege (VIEW_GL_DRILLBACK_PRIV) will need to be removed from all instances of the GL Cross reference Duty (RESA_GLCROSSREF_INQUIRY_DUTY) to which it is associated before the duty can be removed below.

   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.

   - RESA_CURRENCY_ROUNDING_RULES_INQUIRY_DUTY
   - RESA_CURRENCY_ROUNDING_RULES_MGMT_DUTY
   - RESA_ERRORMSG_INQUIRY_DUTY
   - RESA_ERRORMSG_MGMT_DUTY
   - RESA_GLCROSSREF_INQUIRY_DUTY
   - RESA_GLCROSSREF_MGMT_DUTY
   - RESA_REFERENCE_FIELDS_INQUIRY_DUTY
   - RESA_REFERENCE_FIELDS_MGMT_DUTY
   - RESA_STORE_DATA_INQUIRY_DUTY
   - RESA_STORE_DATA_MGMT_DUTY
   - ROLE_MANAGER_DUTY