

Oracle® Retail Workspace

Administration Guide

Release 13.1.3

January 2011

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Anirudha Accanoor

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

- (i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.
- (ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.
- (iii) the software component known as **Access Via**™ licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.
- (iv) the software component known as **Adobe Flex**™ licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

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

Contents

Send Us Your Comments	vii
Preface	ix
Audience	ix
Related Documents	ix
Customer Support	ix
Review Patch Documentation	x
Oracle Retail Documentation on the Oracle Technology Network	x
Conventions	x
1 Getting Started	
What is Oracle Retail Workspace	1-1
Where Does Workspace Fit in a Retail Enterprise	1-4
Understanding the Workspace User Interface	1-4
Workspace User Interface Components	1-5
Logging On to Workspace	1-5
Setting Up Your User Profile	1-6
Setting Up Hint Question and Answer	1-6
Resetting Your Password	1-8
2 Working with Workspace	
Working with the Dashboards	2-1
Launching Retail and Other Applications	2-1
Accessing the Reports	2-2
Printing the Reports	2-3
Exporting the Reports	2-3
Accessing the Alerts, Worklists, and Workflows Tools	2-3
3 Managing Workspace	
Managing Your Profile	3-1
Viewing Your Profile	3-1
Editing Your Profile	3-2
Resetting Your Account Password	3-2
Searching for Users	3-3

Logging On to My Oracle Support.....	3-3
Managing Users and Roles	3-3
Creating a User.....	3-4
Creating a Single User Account.....	3-4
Creating Multiple User Accounts.....	3-4
Editing a User.....	3-6
Deleting a User.....	3-7
Creating a Role (Group).....	3-7
Editing a Role (Group).....	3-8
Deleting a Role (Group).....	3-9
Managing Access to Workspace Components	3-10
Granting Access Permissions.....	3-10
Granting ADF Permissions.....	3-13
Exporting and Importing Portlet Customizations	3-16
exportPortletPrefs.sh Usage.....	3-17
importPortletPrefs.sh Usage.....	3-17

4 Managing External Applications

Overview of the OSSO External Applications Facility	4-1
Pre-requisites.....	4-2
Supported Types of Authentication.....	4-2
Security Considerations Launching External Applications.....	4-3
Defining an External Application in OSSO	4-3
Launching OSSO External Application Management.....	4-5
Testing an External Application Definition.....	4-6
Obtaining the OSSO External Application ID	4-6
Managing User Credentials	4-7
Configuring Workspace to Launch External Applications via OSSO	4-8
Sample External Application JavaScript and HTML	4-9

Index

Send Us Your Comments

Oracle® Retail Workspace Administration Guide, Release 13.1.3

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

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

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

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

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

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

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

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

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

Preface

The Oracle® Retail Workspace Administration Guide describes the Workspace application user interface and includes information that enables you to manage the users, roles, and application resources effectively.

Audience

This guide is intended for the users and administrators of Workspace and assumes that you are familiar with the following:

- Security (access control, permissions, and authorization)
- Lightweight Directory Access Protocol (LDAP)
- Retail domain metrics and terminology
- Any company-specific policies, such as your naming conventions for merchandise and location hierarchies, naming conventions, and business practices

Note: This guide describes the default implementation and on-screen labels. Your company may have customized the labels. In those situations, the screen labels on your user interface may not match the screen labels described in this guide.

Related Documents

For more information, see the following documents in the Oracle Retail Workspace Release 13.1.3 documentation set:

- *Oracle Retail Workspace Release Notes*
- *Oracle Retail Workspace Installation Guide*
- *Oracle Retail Workspace Implementation Guide*
- *Oracle Retail Workspace Online Help*

Customer Support

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

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 13.1) or a later patch release (for example, 13.1.3). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

Oracle Retail Documentation on the Oracle Technology Network

Documentation is packaged with each Oracle Retail product release. Oracle Retail product documentation is also available on the following Web site:

http://www.oracle.com/technology/documentation/oracle_retail.html

(Data Model documents are not available through Oracle Technology Network. These documents are packaged with released code, or you can obtain them through My Oracle Support.)

Documentation should be available on this Web site within a month after a product release.

Conventions

The following text conventions are used in this document:

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

Getting Started

Welcome to Oracle Retail Workspace. This chapter introduces you to the Workspace application and provides an overview to help you get started.

This chapter includes the following information:

- [What is Oracle Retail Workspace](#)
- [Where Does Workspace Fit in a Retail Enterprise](#)
- [Understanding the Workspace User Interface](#)
- [Logging On to Workspace](#)
- [Setting Up Your User Profile](#)

Important: Most of the user and administrative tools are links to the Oracle Internet Directory (OID) Delegated Administrative Services (DAS) application.

This book describes the administrative tasks that you can perform using the OID DAS application. In case Workspace is not configured to use OID, the DAS features described in this book will not be available.

What is Oracle Retail Workspace

Oracle Retail Workspace is a next generation portal that uses Oracle WebCenter as the underlying technology. The Workspace framework provides an integrated platform that serves as a single point of access to Oracle Retail applications as well as third-party applications. It can be used to display single source or multi-source information in a consolidated view. This content may consist of reporting, action items, and/or messages that enable a user to access critical information in an efficient manner to make business decisions.

Oracle Retail Workspace includes the following features:

- Single Sign-On
- Central Launch
- User Management and Role-Based Security
- Dashboard Creation and Viewing
- Integration with Oracle Business Intelligence Enterprise Edition (BI EE) and Oracle Business Intelligence Publisher (BIP) report servers
- Integration with Oracle Business Intelligence (BI) Delivers Alerts

- Integration with Oracle BPEL Process Manager (BPM) Worklists and Administration Console
- Integration with Oracle Business Process Execution Language (BPEL) Workflows and Administration Tool
- Retailer Specific Customization
- Example Roles and Dashboards

Single Sign-On

Workspace is compliant with Oracle Single-On (OSSO). This enables users to access other OSSO compliant applications through Workspace without the need to log in to each individual application or report. Workspace also provides the ability to map non-OSSO compliant applications' credentials (both Oracle and third-party) through Workspace to allow a seamless interaction between users and Workspace accessible applications.

Central Launch

Workspace provides a central point-of-access to launch applications and reports. This central launch functionality uses OSSO to pre-authenticate user security for Oracle Retail resources. This eliminates the need for the user to log in to each resource that is launched. Workspace also provides the ability to launch third-party applications through external password mapping. This allows third-party applications to behave in a similar manner as Oracle Retail applications.

User Management and Role-based Security

Workspace provides links to OID Delegated Administrative Services. These screens are used by an administrator to manage role based security and by users to manage their profiles.

Workspace provides role based security functionality by utilizing OID DAS user management. Role based security allows resource access to be granted based on a role rather than an individual user. This applies to the accessibility of applications, dashboards, and user administrative tools from Workspace. However, it does not apply to user authorization within those resources. User authorization for the application occurs separately from Workspace and within the application's security management system.

Only OID DAS administrators can manage roles and associated permissions. It is recommended that a Workspace administrator be designated as an OID DAS administrator. This allows the Workspace administrator to manage roles and associated permissions. Role administration includes creating new roles and role hierarchies, editing existing roles, and assigning permissions to resources.

Role based security will manifest itself by displaying the permissible resources in the Workspace navigation pane. All resources that are displayed are then available to the user for launching and viewing.

All users accessing Workspace should belong to the Retail_Workspace_User role. Retailers may define their own specific roles, and may include them as members of the Retail_Workspace_User role.

Dashboard Creation and Viewing

Workspace provides the ability to create custom dashboards that can display a consolidated view of a variety of content. This enables users to view pre-determined critically-deemed information in a single view.

Reporting

Workspace is integrated with the Oracle Business Intelligence Enterprise Edition (BI EE) and Business Intelligence Publisher (BIP) reports servers. Workspace has the ability to display a dynamic list of BI EE and BIP reports that a user has security access to. This list can be configured to display in the Workspace navigation pane. Workspace also provides the ability to display BI EE and BIP reports in dashboard portlets. Reports that are accessed through Workspace will be served directly from the BI EE tool and will consist of the most recent information that is available in BI EE.

Integration with Oracle BI Delivers Alerts

Workspace is integrated with Oracle Business Intelligence (BI) Delivers alerts. Since BI Delivers alerts are part of the BI EE application, this feature can be launched from the navigation pane. It is also possible to display BI Delivers alerts on a dashboard using the Workspace alerts portlet. Alerts that are accessed through Workspace will be served directly from the BI EE tool and will consist of the most recent information that is available in BI EE.

Integration with Oracle BPM Worklists

Workspace is integrated with Oracle BPEL Process Manager (BPM) worklists. The BPM application can be launched from the navigation pane. It is also possible to display BPM worklists on a dashboard portlet. Worklists that are accessed through Workspace will be served directly from the BPM tool and will consist of the most recent information that is available in BPM.

Integration with Oracle BPEL Workflows

Workspace is integrated with Oracle Business Process Execution Language (BPEL) workflows. The BPEL application and BPEL Administration tool can be launched from the navigation pane. It is also possible to display BPEL workflow instances on a dashboard portlet. These workflow instances are linked directly to BPEL workflows in the BPEL Administration tool. Workflows that are accessed through Workspace will be served directly from the BPEL tool and will consist of the most recent information that is available in BPEL.

Retail Specific Configuration

Workspace provides the ability to customize the user experience to fit the unique needs of a retailer. The navigation work lists can be tailored to display only relevant links and to organize them in a manner that makes sense to a retailer's users. Workspace also provides the ability to configure home pages, client branding, and look and feel of the Workspace application.

Example Roles and Dashboards

Upon installation, Workspace is configured with seven predefined roles. These roles are provided as examples and for administrative purposes. The examples include four business roles with predefined permissions to dashboards, applications, and management tools. The administrative roles are for managing roles and permissions. An **Anyone** role is part of the ADF framework and includes all users, both authenticated and unauthenticated.

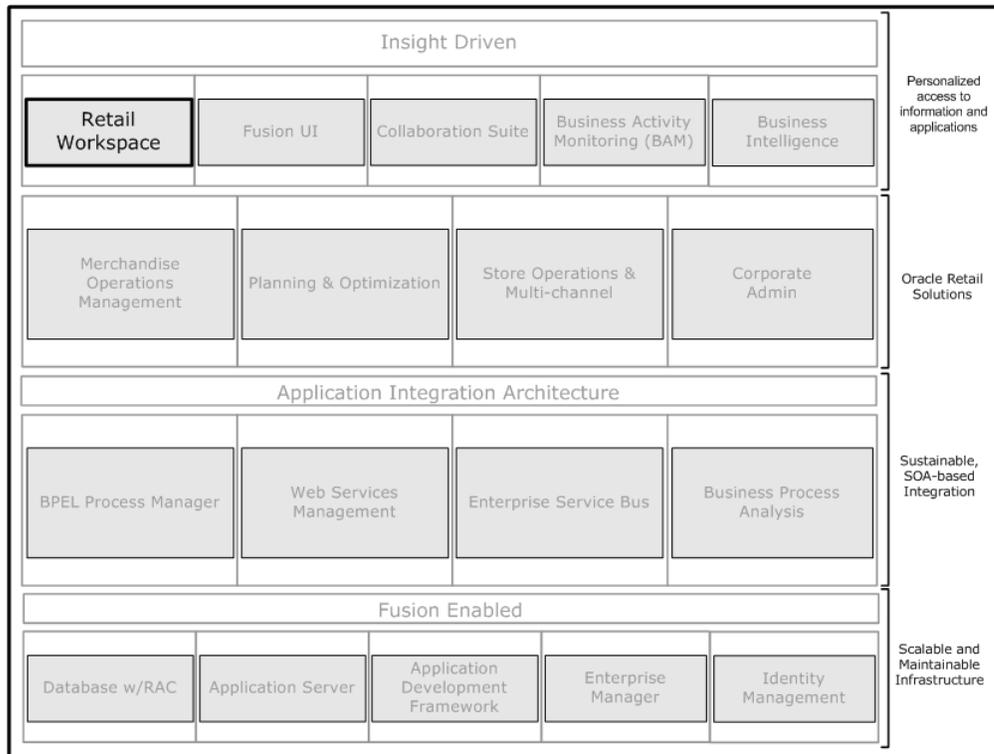
Upon installation, Workspace includes four demonstration dashboards. These dashboards have predefined content that is relevant to an associated business role. The dashboard report content sources are Workspace supported Oracle Retail applications. Therefore, the content of the demonstration dashboards is OSSO compliant.

Where Does Workspace Fit in a Retail Enterprise

The illustration below shows an example of a retail enterprise with the Workspace framework providing a single point of access to the applications and reports.

For more information on the Workspace architecture, refer to the *Oracle Retail Workspace Implementation Guide*.

Figure 1–1 Workspace in a Retail Enterprise



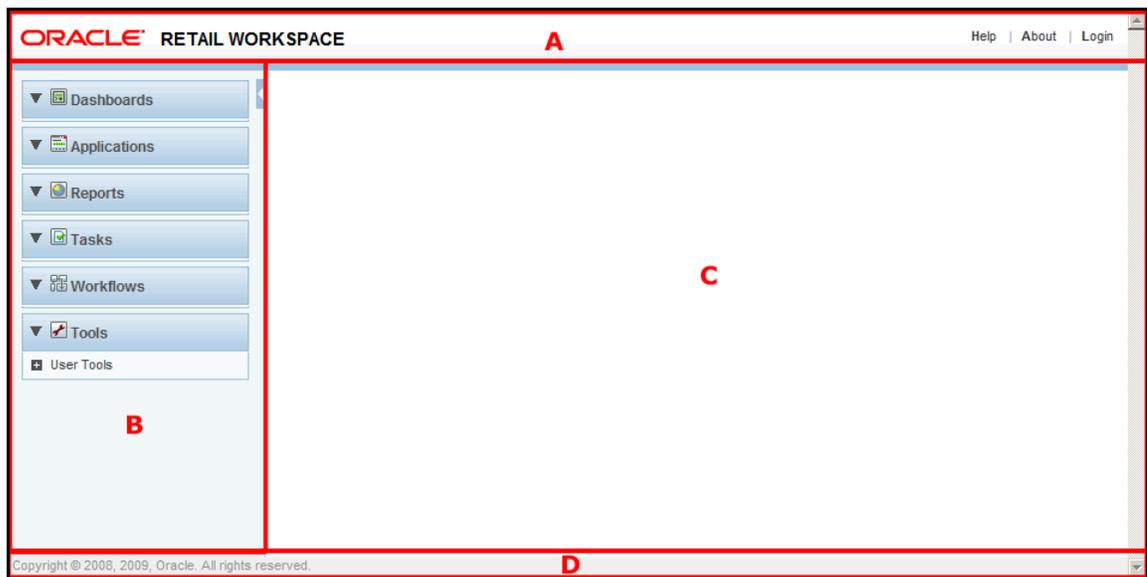
Understanding the Workspace User Interface

The Workspace user interface consists of the following components:

- Global Header
- Navigation Pane
- Content Area
- Footer Area

The following figure highlights the various components of the Workspace user interface:

Figure 1–2 Workspace User Interface



Workspace User Interface Components

The following table describes the various screen components in the Workspace application:

Table 1–1 Workspace User Interface Components

Legend	Screen Area Name	Description
A	Global Header	Displayed at the top of the screen, this area appears across the business applications and custom pages. It includes the application branding, Online Help, Login, and About links.
B	Navigation Pane	Displayed on the left of the screen, this area includes all the worklists accessible to a user. It is a collapsible column. The default Workspace configuration contains the following worklists: <ul style="list-style-type: none"> ■ Applications ■ Dashboards ■ Reports ■ Tasks ■ Workflows ■ Tools
C	Content Area	Displayed on the center of the screen, this area displays the dashboards, reports, and other content.
D	Footer Area	Displayed on the bottom of the screen, this area displays the copyright information.

Logging On to Workspace

Before you log on to the Workspace application, ensure that your system meets the recommended configuration. For more information, see the *Oracle Retail Workspace Installation Guide*.

Once you check the configuration, obtain the following information:

- Uniform Resource Locator, URL – you will need to enter the URL or the Web address of the application in the Web browser to access the application. For example:

`http://yourcompanyname.domain.com`

- User name, Password, and Company Name – based on the tasks you want to perform, obtain a user account (that includes user name, password, and an associated role) to log on to the application.

Note: The application URL is specific to the Oracle Single Sign-On implementation and can be customized at each site. On the Sign In page, the *Company Name* field appears when the OSSO is configured to recognize multiple realms.

To log on to Workspace:

1. Start Internet Explorer.
2. In the **Address** bar, enter the Workspace URL, and press Enter. The Workspace application home page appears.
3. On the top right corner of the page, click **Login**. The **Sign In** page appears.
4. On the **Sign In** page, enter the user name, password, and company name.
5. Click **Login**.

The Workspace application screen appears with access to dashboards, applications, and reports set up for your user account.

Setting Up Your User Profile

The first time you log on to the application, Oracle recommends that you perform the following tasks to maintain a secure access to your account:

- [Setting Up Hint Question and Answer](#)
- [Resetting Your Password](#)

Setting Up Hint Question and Answer

A hint question and answer associated with your user account makes resetting your password secure and convenient.

Note: The Hint feature described in this section is provided by the Delegated Administration Services (DAS) application which is a part of the Oracle Internet Directory (OID). In case Workspace is not configured to use OID, the Hint feature described in this section will not be available.

To set up a hint question and answer:

1. In the Navigation pane, under the **Tools** section, click **User Tools**.
2. Under the **User Tools** menu, click **Edit My Profile**. The **Oracle Identity Management Self Service Console** appears.

Figure 1–3 Edit My Profile Page

3. On the **Self Service Console**, review and edit the preferences and personal information associated with your user account, click **Submit**.
4. On the confirmation screen, click **Ok**. The **Self Service Console Home Page** appears.

Figure 1–4 Self Service Console Page - Home Tab

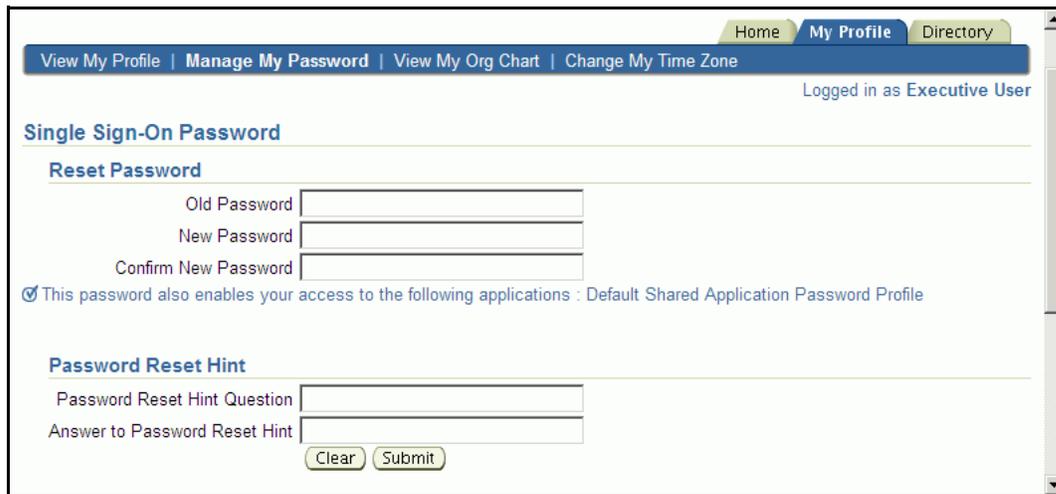
5. Click the **My Profile** tab
Or
On the **Home** tab, click the **My Profile** link.
6. On the **My Profile** tab, click **Manage My Password**. The **Manage Password** page appears.

Figure 1–5 Self Service Console - My Profile Tab



7. On the **Manage My Password** page, in the **Password Reset Hint** section, enter an appropriate hint question and answer in the **Password Reset Hint** and **Answer to Password Reset Hint** fields.

Figure 1–6 Self Service Console - My Profile Tab - Manage My Password Screen



8. Click **Submit**.

Resetting Your Password

Once you set up the hint question and answer, you must also reset your account password. To reset the password, see [Resetting Your Account Password](#).

Working with Workspace

The Workspace application provides a framework and capability to launch the integrated Oracle Retail applications, external applications, tasks, workflows, reporting tools, operational, and analytical reports. This chapter describes how you can effectively use the Workspace application to launch applications, access reports, tasks, and workflows.

This chapter includes the following sections:

- [Working with the Dashboards](#)
- [Launching Retail and Other Applications](#)
- [Accessing the Reports](#)
- [Accessing the Alerts, Worklists, and Workflows Tools](#)

Working with the Dashboards

Workspace installation includes pre-defined dashboard examples and roles to help you build dashboards that best suit your business. For more information on the dashboard examples and roles, see the My Oracle Support Note, *Oracle Retail Workspace Dashboard Examples Guide*.

Launching Retail and Other Applications

Workspace provides the ability to launch Oracle Retail applications using the Single Sign-On mechanism. It also provides the ability to simulate the Single Sign-On launch for external applications that cannot be Single Sign-On enabled or to launch third party applications that can be accessed using a URL. The ability to access applications is based on the roles associated with your user account.

Once configured, all available applications appear under the Applications worklist (in the Navigation pane). The applications are organized under different categories based on the implementation for your business.

To launch an application:

1. In the Navigation pane, under the **Applications** worklist, select the application category.
2. Expand the relevant solution area, and then click the application you want to launch. The application launches in a new Web browser window.

Default Applications Integrated Through the OSSO System

The following Oracle Retail applications are supported through the Oracle Application Server Single Sign-On (OSSO) system:

- Oracle Retail Active Retail Intelligence
- Oracle Retail Allocation
- Oracle Retail Invoice Matching
- Oracle Retail Merchandising System
- Oracle Retail Price Management
- Oracle Retail Store Inventory Management

Note: Release 13.1.2 and Release 13.2 of the Oracle Retail applications listed above are supported.

Oracle Retail Data Warehouse (RDW) is integrated with Workspace through Oracle BI Enterprise Edition, which serves as the front-end reporting tool for RDW.

Other Oracle applications:

- Oracle Business Intelligence Enterprise Edition
- Oracle Business Intelligence Publisher
- Oracle BPEL Process Manager (BPM)
- Oracle Business Process Execution Language (BPEL)

Accessing the Reports

Along with the Retail applications, you can launch reports set up for your business. Unlike the role-based Applications worklist, the ability to access the reports is user-based.

Once configured, all the available reports appear under the relevant reporting tools section in the Reports worklist. When you click on a report, the report launches in the content area.

Note: Oracle supports the use of Oracle's *Business Intelligence Enterprise Edition* and *Business Intelligence Publisher* as the reporting tools in Workspace.

The Workspace application provides the Oracle Application Server Single Sign-On (SSO) support for these reporting tools.

To view a report:

1. In the Navigation pane, under the **Reports** worklist, expand the relevant reporting tool.
2. Navigate through the report categories to the report you want, and then click the report. The report launches in the Content area of Workspace.
3. On the report screen, review or set the filter options, and click **View**.

Since the reports can include huge amounts of information, the Report screen includes some extra menu options that help you filter the information before viewing the report.

Printing the Reports

Once you view the report, you may consider printing the report.

Note: Printing capabilities and options are derived from the reporting tool where the report was created.

To print a report:

1. On the report screen, review the report.
2. Click **Print**. The **Print** dialog box appears.
3. On the **Print** dialog box, set the print options, and click **Print**.

Exporting the Reports

Along with printing the report, you can also export the report information.

Note: Exporting capabilities and options are derived from the reporting tool where the report was created.

To export a report:

1. On the report screen, review the report.
2. Click **Export**. The **Export** dialog box appears.
3. On the **Export** dialog box, set the location and the file type, and then click **Export**.

For more information on using the reports, refer to the applicable reporting tool documentation set (For example, *Oracle Business Intelligence Publisher User's Guide*).

Accessing the Alerts, Worklists, and Workflows Tools

Workspace provides an integration with Oracle BPM worklists, BI Delivers alerts, and BPEL workflows. You can launch these tools as well as display them in a dashboard portlet. Since they are OSSO-enabled, once you log on to the OSSO system, you will not be required to sign in again to launch the application or view the Oracle BPM worklists, BI Delivers alerts, or BPEL workflows. For more information on configuring these tools in the dashboard portlets, refer to the *Oracle Retail Workspace Implementation Guide*.

About Oracle BPM Worklists

Oracle BPM worklists are user-based like reports and only Oracle BPM worklists assigned to a specific user appear on the screen.

About Oracle BI Delivers Alerts

Oracle BI Delivers alerts are user-based like reports and only alerts for a specific user appear on the screen.

About Oracle BPEL Workflows

Oracle BPEL workflows are role-based and Workspace roles can be made to access them. In addition to integration with BPEL workflows, Workspace provides access to the Oracle BPEL Administration tool to administer BPEL workflows.

Managing Workspace

This chapter includes information on the various user management tasks you can perform as an administrator. It also includes information on the self-management features a user can access, such as resetting a password. Finally, it includes information on how to import and export portlet customizations.

All of the user management and self-management features described in this chapter are provided by the Delegated Administration Services (DAS) application. The DAS application is supplied as part of the Oracle Internet Directory (OID) product. In case Workspace is not configured to use OID, the management features described in this chapter will not be available.

This chapter includes the following sections:

- [Managing Your Profile](#), using the User Tools worklist.
- [Managing Users and Roles](#), using the Admin Tools worklist.
- [Managing Access to Workspace Components](#), using the Permissions Management feature.
- [Exporting and Importing Portlet Customizations](#), using the Workspace Export/Import tool.

Managing Your Profile

The *User Tools* worklist provides the following features that help you manage your user profile:

- [Viewing Your Profile](#)
- [Editing Your Profile](#)
- [Resetting Your Account Password](#)
- [Searching for Users](#)
- [Logging On to My Oracle Support](#)

Note: Features in the User Tools worklist are provided through the Oracle Internet Directory (OID) Delegated Administrative Services. For more information on these features, refer to the *Oracle Identity Management Guide to Delegated Administration*.

Viewing Your Profile

To view your profile:

- On the Navigation pane, under **Tools** worklist, expand **User Tools**.
- Click **Account Info** to view the information associated with your user profile. The **View My Profile** page appears and displays the basic, contact, organizational, and provisioning information.

To change this account information, click **Edit My Profile**.

Editing Your Profile

To edit your user profile:

- On the Navigation pane, under **Tools** worklist, expand **User Tools**.
- Click **Edit My Profile** to view and edit the basic, contact, organizational, and provisioning information associated to your user account.

Resetting Your Account Password

Use the *Reset Password* feature to change or reset the password associated with your user account.

Note: For the Reset Password feature to work properly, ensure that you have set up the Hint Question and Answer for your profile. For more information, see [Setting Up Your User Profile](#).

To reset the password:

1. On the Navigation pane, under **Tools** worklist, expand **User Tools**.
2. In the **User Tools** section, click **Reset Password**. The **Reset My Single Sign-On Password** page appears.

Figure 3–1 Self Service Console - Reset My Single Sign-On Password Page

The screenshot shows the Oracle Identity Management Provisioning Console interface. At the top, it says "ORACLE Identity Management Provisioning Console" with a help icon. The main heading is "Reset My Single Sign-On Password". Below this is a progress indicator with three steps: "Confirm Identity", "Confirm Additional Personal Information", and "Reset SSO Password". The "Confirm Identity" step is currently active. The instructions state: "Your identity needs to be confirmed by entering your Single Sign-On user name and name of the company you are associated with. Click on Next to continue." There are two input fields: "User Name" and "Company". At the bottom right, there are "Cancel" and "Next" buttons. The page number "Step 1 of 3" is also visible. The footer contains the text "Copyright ©1996, 2008, Oracle. All rights reserved." and another help link.

3. In the **Confirm Identity** section, enter the **User Name** and **Company**, and then click **Next**. The **Confirm Additional User Information** page appears.

Note: The **Company** field displays only if the OID Delegated Administrative Services (DAS) is enabled for multiple realms.

4. The **Confirm Additional User Information** page displays the hint question that you had set up the first time you logged on to the application. For more information on setting up the hint question, see [Setting Up Hint Question and Answer](#).
5. Type the answer associated with the hint question, and click **Next**.
6. Enter a password you want, and then click **Submit**.

Searching for Users

Use the *User Search* feature to search for users already set up with the application.

To search for a user:

1. On the Navigation pane, under **Tools** worklist, expand **User Tools**.
2. In the **User Tools** section, click User Search. The **Search** page appears.
3. In the **Search for User** field, enter a text string you want, and then click **Go**. Search results relevant to your text input appear on the page.
4. Under the **User ID** column, click a user to view the associated profile.

The View My Profile page appears that displays the profile. To go back to the search results, click **Go Back**.

Logging On to My Oracle Support

Click the **My Oracle Support** link to log on to the My Oracle Support Web page for accessing knowledge base articles and resolving issues with the application. My Oracle Support is not a part of the Single Sign-On integration, and you must log on to the Web site using your My Oracle Support user account.

Managing Users and Roles

The *Admin Tools* worklist includes the following features that help you manage user accounts, roles, access permissions, and application configuration:

- [Creating a User](#)
- [Editing a User](#)
- [Deleting a User](#)
- [Creating a Role \(Group\)](#)
- [Editing a Role \(Group\)](#)
- [Deleting a Role \(Group\)](#)

Ensure that you have appropriate administrative privileges to access and use the features in the Admin Tools worklist.

Note: Most of the features in the Admin Tools worklist are provided through the Oracle Internet Directory (OID) Delegated Administrative Services. For more information on these features, refer to the *Oracle Identity Management Guide to Delegated Administration*.

Creating a User

Use the *Create User* feature to create and configure a Workspace user account.

You can create user accounts in one of the following ways:

- If you need to add one or two user accounts, see [Creating a Single User Account](#).
- If you need to create multiple user accounts all at once, use the Bulk Load feature. For more information, see [Creating Multiple User Accounts](#).

Creating a Single User Account

To create a new user account:

1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Create User**. The **Oracle Identity Management Provisioning Console** appears. This console helps you set up a new user account.

Figure 3–2 Oracle Identity Management Provisioning Console

3. On the **Provisioning Console**, enter appropriate information on the various fields. Ensure that you enter information for fields preceded with an asterisk (*).
4. Click **Submit**.

Creating Multiple User Accounts

The Bulk load feature enables you to create multiple user accounts.

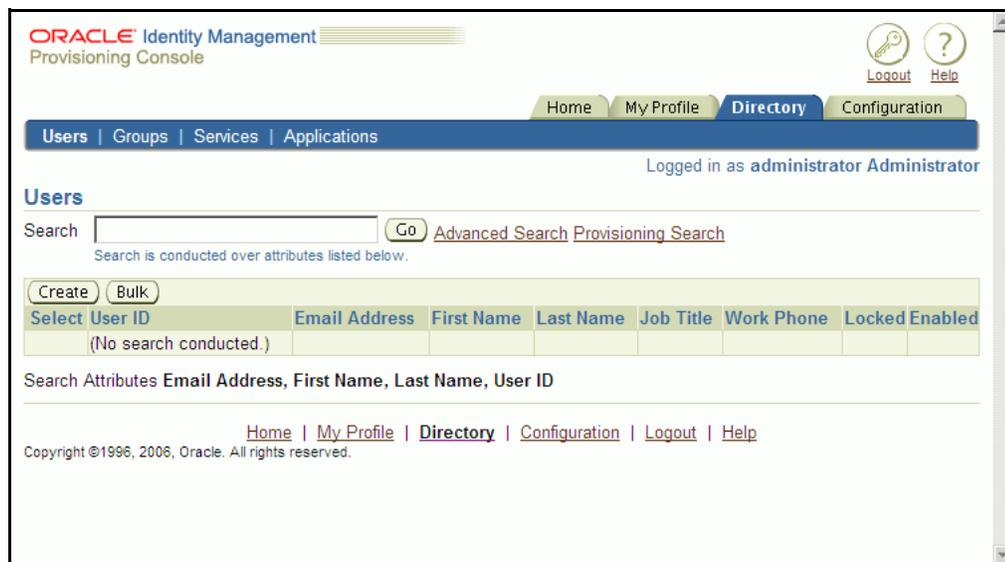
Note: The Bulk load feature requires that you upload an LDAP Data Interchange Format (LDIF) file set up with the new user accounts. Before you access the Bulk load feature, ensure that the LDIF file is set up with the user accounts.

To help you set up an LDIF file, a sample LDIF file is available in the Workspace installation folder.

To create multiple user accounts all at once:

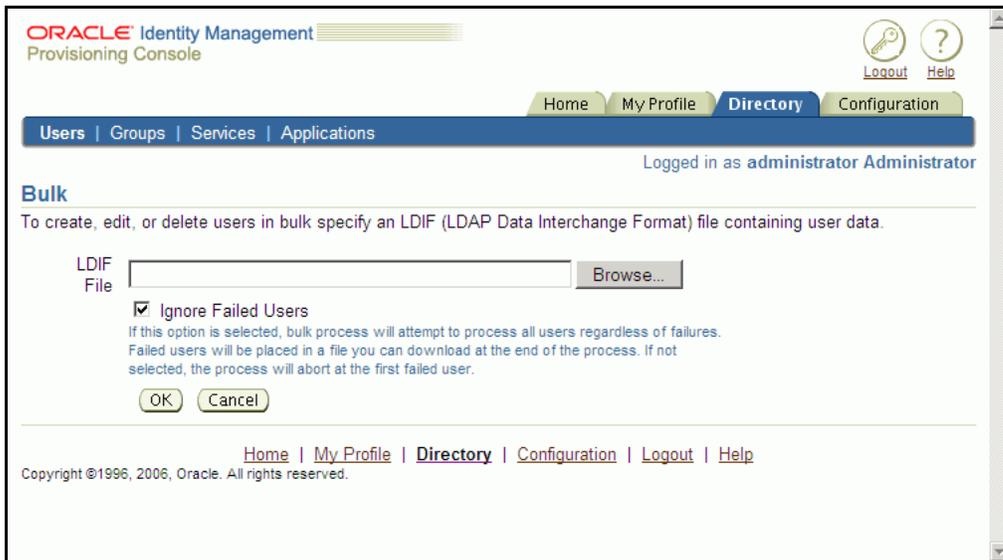
1. Navigate to the **Oracle Identity Management Provisioning Console** home page. You can use the following steps:
 - a. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
 - b. In the **Admin Tools** section, click **Create User**. The **Oracle Identity Management Provisioning Console** appears.
 - c. Click **Cancel**. The **Provisioning Console** home page appears.
2. On the **Provisioning Console** home page, click the **Directory** tab.

Figure 3–3 Oracle Identity Management Provisioning Console - Creating Bulk Users



3. On the **Directory** tab, click **Bulk**.

Figure 3–4 Loading LDIF File



4. Click **Browse** and select the LDIF file set up with the new user accounts.
5. Click **OK**.

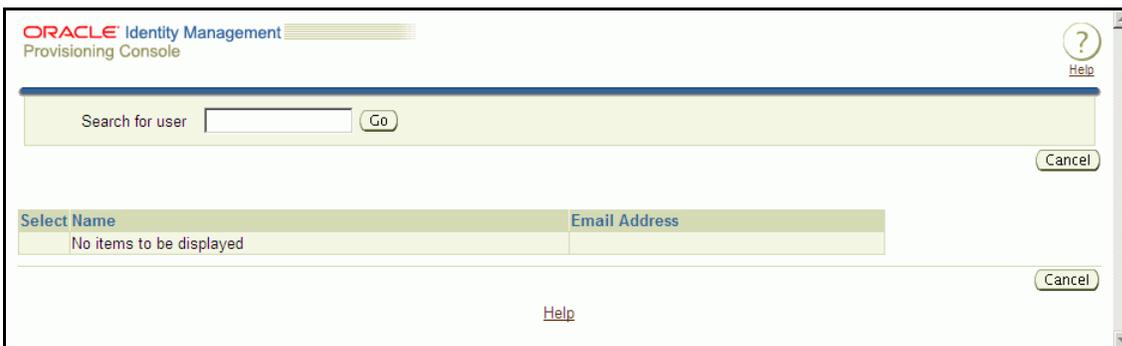
Editing a User

Use the *Edit User* feature to edit an existing user account.

To edit a user account:

1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Edit User**. The **Oracle Identity Management Provisioning Console** appears. This console helps you edit a user account.

Figure 3–5 Oracle Identity Management Provisioning Console - Edit User



3. On the **Provisioning Console**, enter the user name in the **Search for user** field, and click **Go**. User accounts that match the search string appear.
4. Select the user you want, and click **Edit**.
5. Edit the user account information, and click **Submit**. A confirmation message appears.
6. Click **Done**.

- Restart the application server that hosts Workspace.

Note: Changes to the user account take effect once you restart the application server or the OID cache expires.

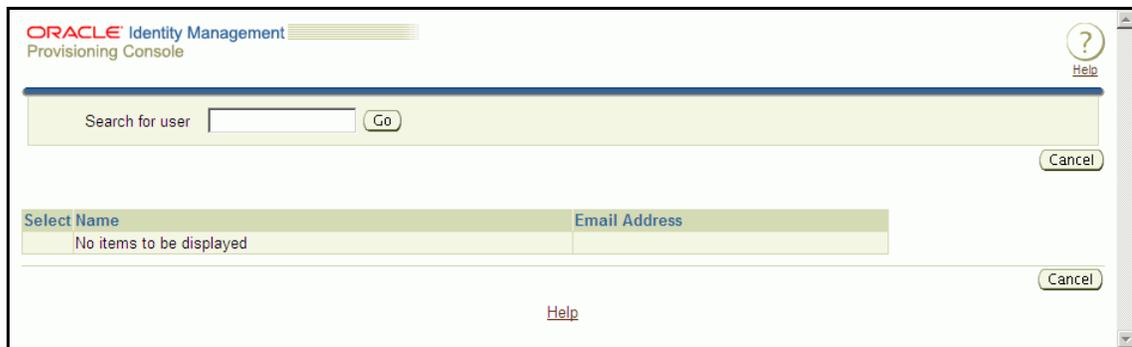
Deleting a User

Use the *Delete User* feature to delete an existing user account.

To delete a user account:

- On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
- In the **Admin Tools** section, click **Delete User**. The **Oracle Identity Management Provisioning Console** appears.

Figure 3–6 Oracle Identity Management Provisioning Console - Delete User



- On the **Provisioning Console**, enter the user name in the **Search for user** field, and click **Go**. User accounts that match the search string appear.
- Select the user you want, and click **Delete**. A confirmation message appears.
- Click **Yes**.

Creating a Role (Group)

Use the *Create Role (Group)* feature to create role-based groups.

Important: When you create a role, ensure that you add the role as a member of the *Retail_Workspace_Users* group.

To create a role-based group:

- On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
- In the **Admin Tools** section, click **Create Role (Group)**. The **Oracle Identity Management Provisioning Console** appears.

Figure 3–7 Oracle Identity Management Provisioning Console - Create Group

3. On the **Provisioning Console**, under the **Basic Information** section, enter the following information:
 - **Name** – Type a group name that represents the relative distinguished name (RDN). RDN is the unique component of a Distinguished Name (DN) in an Internet Directory.
 - **Display Name** – Type a display (more convenient) name for the group.
 - **Description** – Type a description of the group. This field is optional.
 - **Group Visibility** – To hide the group from groups or users other than the owners, select the Private option. If a group is private, it is unusable, therefore when creating or editing a group for Workspace always ensure that the group visibility is public.
 - **Make this group privileged** – Select this check box if you want to assign privileges to this group.
4. In the **Owners** section, click **Add Group**. The **Search and Select: Group** window appears.
5. In the **Search and Select: Group** window, type **Retail** in the **Group Name Begins With** field, and then click **Go**.
6. Once the results appear, select **Retail_Workspace_Users**, and then click **Select**. The **Retail_Workspace_Users** group appears under the Owners list.
7. In the **Members** section, follow steps similar to steps 4–6 to add members (users or groups) to the group.
8. In the **Roles Assignment** section, under the **Select** column, select the check box next to the roles you want to assign to the group
9. Click **Submit**.

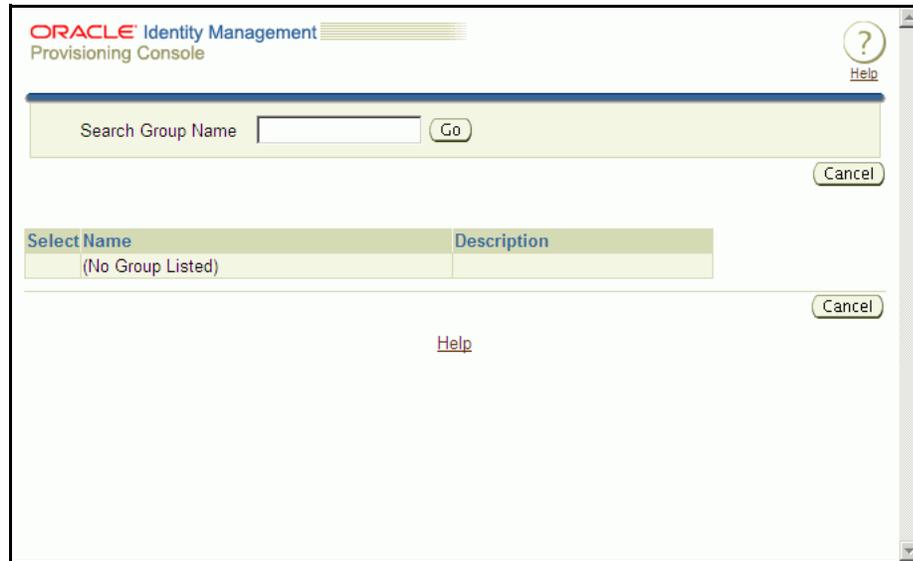
Editing a Role (Group)

Use the *Edit Role (Group)* feature to edit an existing role.

To edit a role:

1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Edit Role (Group)**. The **Oracle Identity Management Provisioning Console** appears.

Figure 3–8 Oracle Identity Management Provisioning Console - Edit Role



3. On the **Provisioning Console**, enter the role name in the **Search for user** field, and click **Go**. User accounts that match the search string appear.
4. Select the role you want, and click **Edit**.
5. Edit the role information, and click **Submit**. A confirmation message appears.
6. Click **Done**.
7. Restart the application server that hosts Workspace.

Note: Changes to the role take effect once you restart the application server or the OID cache expires.

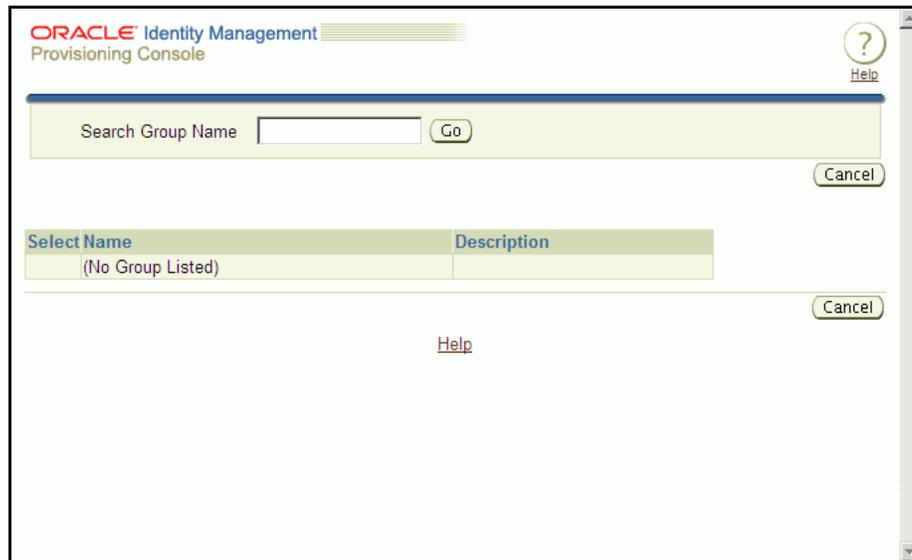
Deleting a Role (Group)

Use the *Delete Role (Group)* feature to delete an existing role-based group.

To delete a role:

1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Delete Role (Group)**. The **Oracle Identity Management Provisioning Console** appears.

Figure 3–9 Oracle Identity Management Provisioning Console - Delete Role



3. On the **Provisioning Console**, enter the role name in the **Search for user** field, and click **Go**. Roles that match the search string appear.
4. Select the role you want, and click **Delete**. A confirmation message appears.
5. Click **Yes**.

Managing Access to Workspace Components

The *Permissions Management* feature enables you to grant or revoke permissions to all the secure elements and nodes that form part of the Workspace framework. This includes access to the dashboards, applications, reports, and tools sections of the application. In addition, ADF Permission Grants can set privileges for selected roles and users of Workspace to customize and personalize portlets on dashboards and other Workspace pages.

This section describes how the Permissions Management feature works when Workspace is configured to use the Oracle Internet Directory (OID) LDAP server. When OID is available, permissions are stored centrally in the OID server. However, if OID is not available, permissions may be stored in multiple files distributed across multiple application server containers. In the latter case, the Permissions Management feature will only display the grants associated with the Workspace container in a read-only manner and an administrator must use command-line utilities for managing the permissions.

Each secured work element will only be displayed to a user when you grant the user appropriate access permissions for that work element. You can assign the access permissions to a specific user or to a group of users (role).

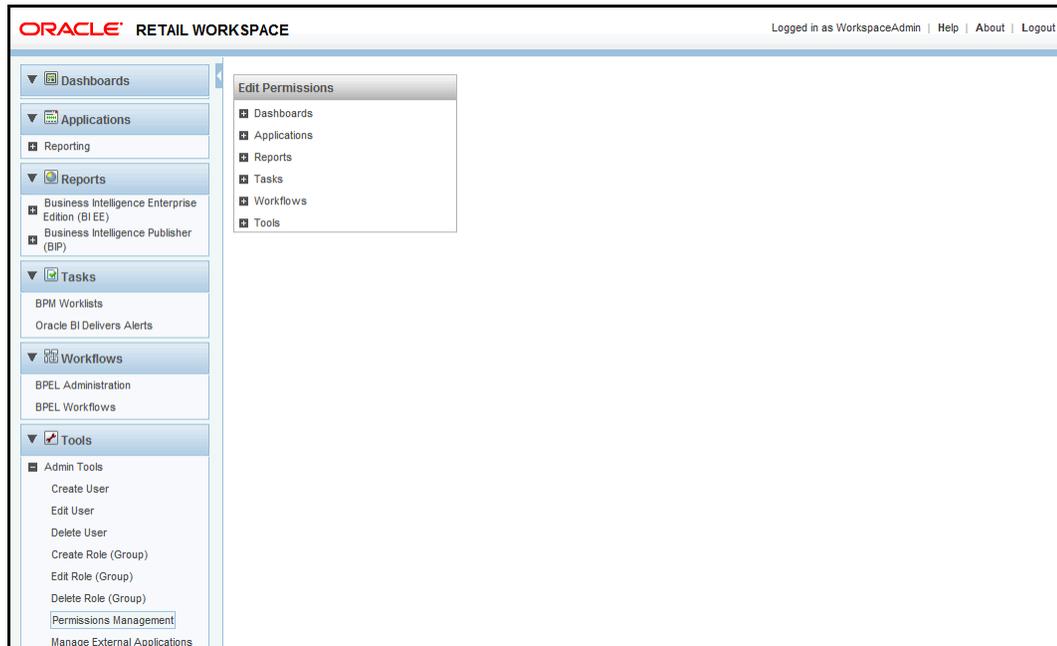
Note: To launch an application, additional permissions and other relevant information may also need to be set up at the application side.

Granting Access Permissions

To grant access permissions to a secure work element:

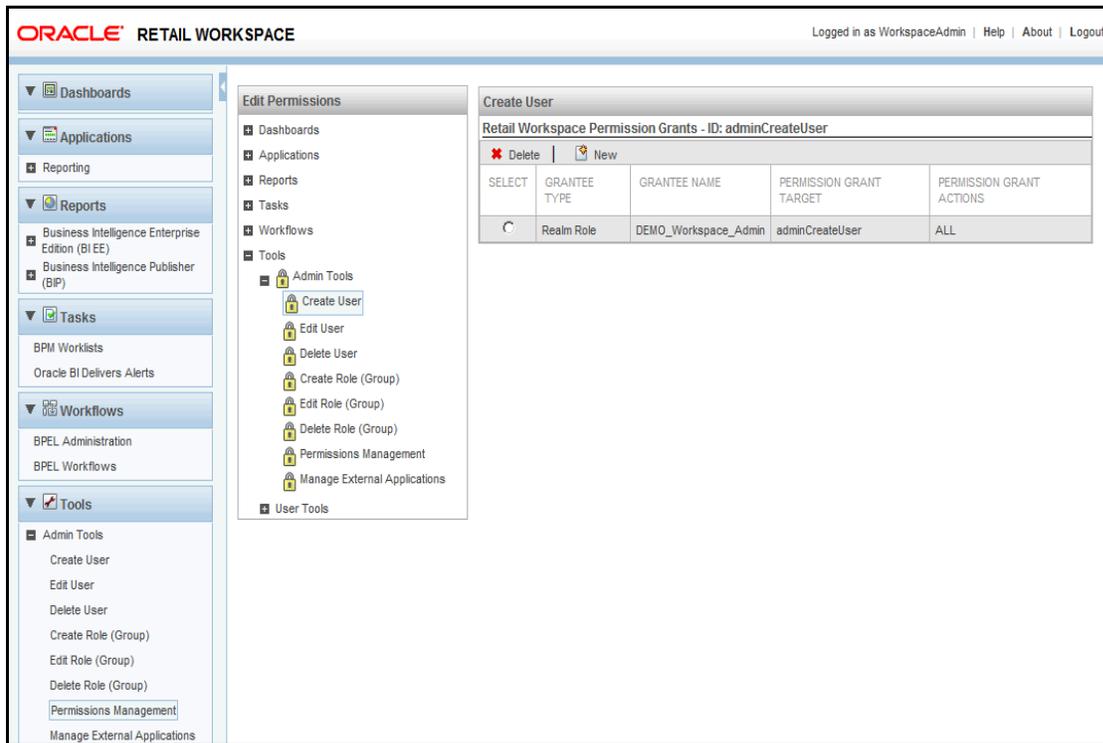
1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Permissions Management**. The **Edit Permissions** page appears in the Content area and displays the work elements in a hierarchy tree structure as they appear in the Navigation area.

Figure 3–10 Edit Permissions Screen in the Content Area



3. Drill down the hierarchy tree and click the desired work element. The **Permissions Grant** area for the work element appears.

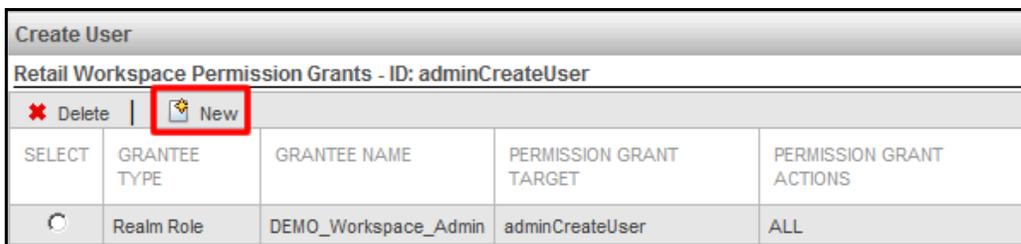
Figure 3–11 Permission Grants Area



Note: In the hierarchy tree, the **Lock** icon next to a work element indicates secure access to the work element. Users with specific permissions can access the work element.

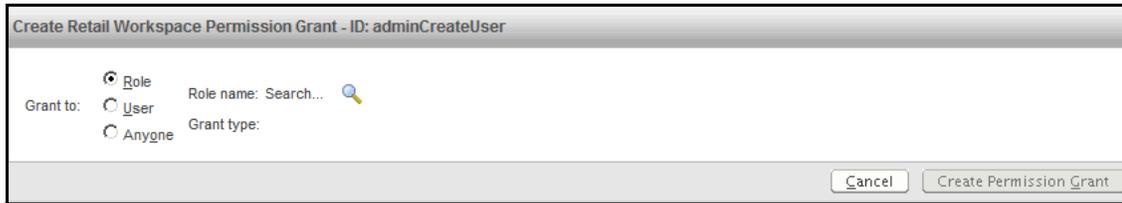
4. Click the **Add New Retail Workspace Grant** icon to grant permissions to this work element for a specific user or role. The **Create Retail Workspace Permission Grant** screen appears.

Figure 3–12 Add New Retail Workspace Grant Icon



5. On the **Create Retail Workspace Permission Grant** screen, use the following steps and select the user or role you want.

Figure 3–13 Create Retail Workspace Permission Grant Screen



6. In the **Grant to** section, select the **Role**, **User**, or **Anyone** option.

The **Anyone** option enables you to grant anonymous access to the work element you want. Once you grant this permission, users can access the work element without logging on to the application.

Note: Although Oracle recommends that you grant permissions to a specific role, you can also choose to grant permissions to specific users when the user's capabilities are not adequately defined by the current set of roles.

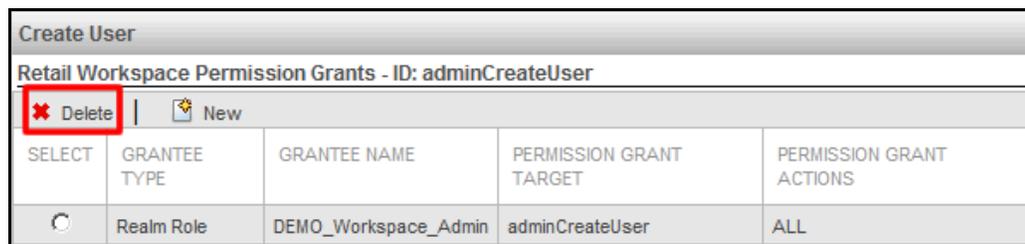
If you want make an application resource available to any user, grant the access to the **Anyone** role.

7. Based on the option you select in the **Grant to:** section, click the **Search** icon to search the user or role you want. The **Search and Select** screen appears.
8. On the **Search and Select** screen, enter a search string, and click **Go**.
9. Select the user or role you want, and then click **Select**.
10. On the **Create Retail Workspace Permission Grant** screen, click **Create Permission Grant**.

To delete a permission grant for a work element:

- In the **Permissions Grant** area, select the permission grant you want to delete, and then click the **Delete Selected Retail Workspace Grant** icon.

Figure 3–14 Delete Selected Retail Workspace Grant Icon

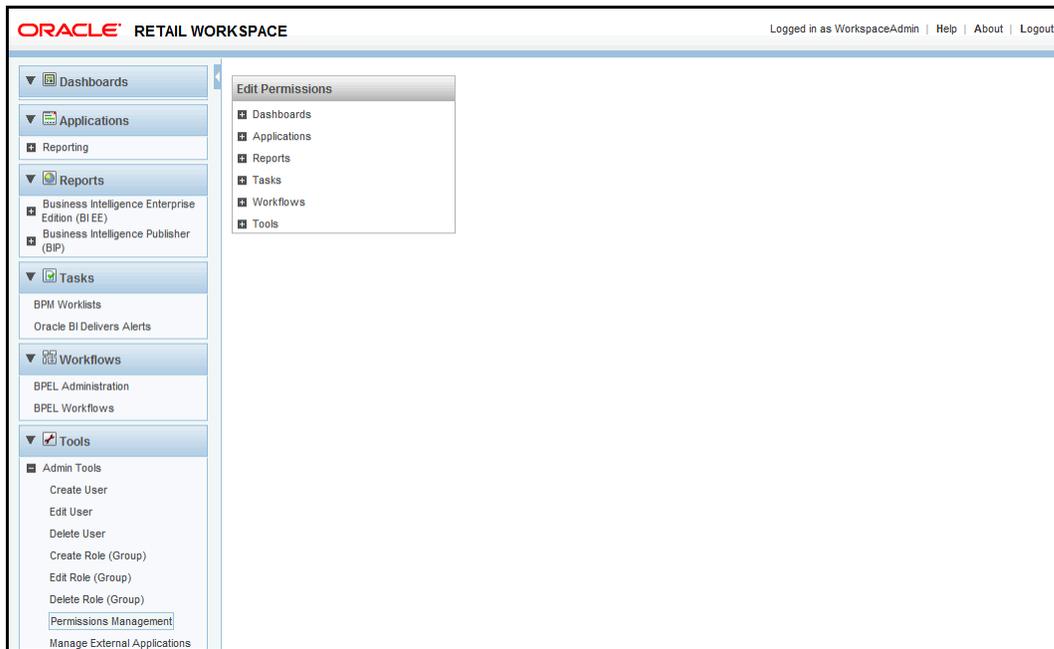


Granting ADF Permissions

To grant ADF permissions to a secure work element:

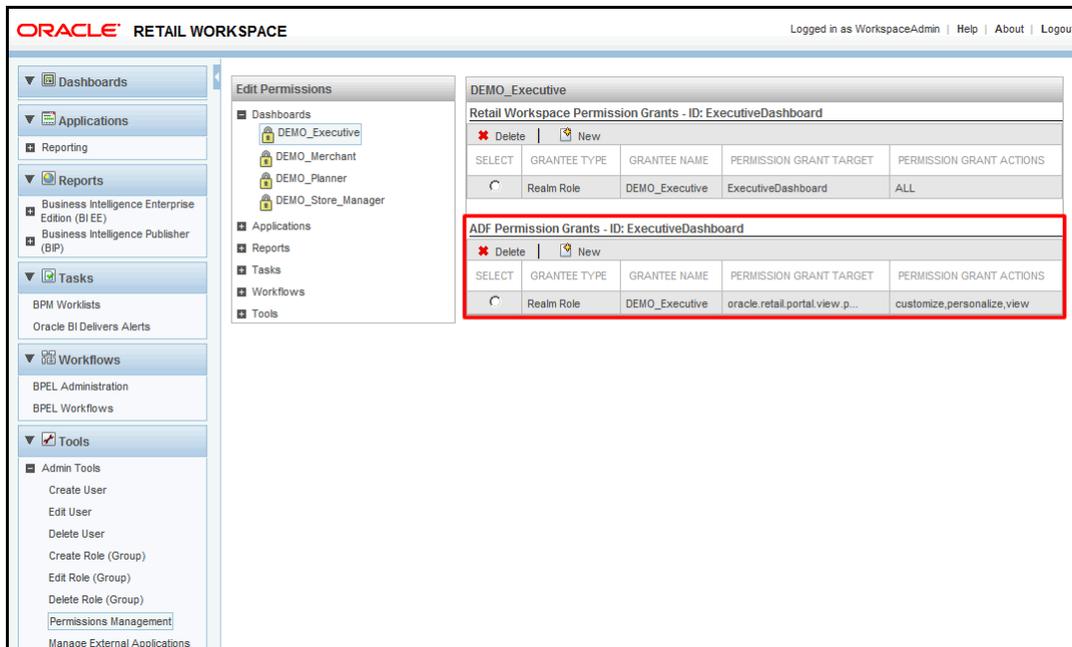
1. On the Navigation pane, under the **Tools** worklist, expand **Admin Tools**.
2. In the **Admin Tools** section, click **Permissions Management**. The **Edit Permissions** page appears in the Content area and displays the work elements in a hierarchy tree structure as they appear in the Navigation area.

Figure 3–15 Edit Permissions Screen in the Content Area



3. Drill down the hierarchy tree and click the desired work element. The **Permissions Grant** area for the work element appears.

Figure 3–16 ADF Permission Grants Area



4. Click the **Add New ADF Permission Grant** icon to grant permissions to the selected work element for a specific user or role. The **Create ADF Permission Grant** screen appears.

Figure 3–17 ADF Permission Grants Area

ADF Permission Grants - ID: ExecutiveDashboard				
✖ Delete		🆕 New		
SELECT	GRANTEE TYPE	GRANTEE NAME	PERMISSION GRANT TARGET	PERMISSION GRANT ACTIONS
<input type="radio"/>	Realm Role	DEMO_Executive	oracle.retail.portal.view.p...	customize,personalize,view

5. On the Create ADF Permission Grant screen, follow the steps described above for selecting the user or role you want.

a. In the **Grant to** section, select the **Role**, **User**, or **Anyone** option.

The **Anyone** option enables you to grant anonymous access to the work element you want. Once you grant this permission, users can access the work element without logging on to the application.

Figure 3–18 Create ADF Permission Grant Screen

Create ADF Permission Grant - ID: ExecutiveDashboard

Grant to: Role Role name: Search...
 User Grant type:
 Anyone

ADF Permission Grants: Customize Personalize View

Note: Although Oracle recommends that you grant permissions to a specific role, you can also choose to grant permissions to specific users when the user's capabilities are not adequately defined by the current set of roles.

If you want make an application resource available to any user, grant the access to the Anyone role.

- b. Based on the option you select in the **Grant to:** section, click the **Search** icon to search the user or role you want. The **Search and Select** screen appears.
 - c. On the **Search and Select** screen, enter a search string, and click **Go**.
 - d. Select the user or role you want, and then click **Select**.
6. By default, all grants will have view privileges. If this role or user should also have customization and personalization privileges, select the relevant check boxes on the screen.

A role or user with *Customize* privileges will be allowed to open a Customization page and enter values to create or update the default settings for all the users.

A role or user with *Personalize* privileges can add or update various settings that override the default settings. The Personalization settings only affect the settings for that user.

Note: Selecting the Anyone check box will disable the Customize and Personalize check boxes. If Customize is selected for a role or a user, the Personalize check box will by default be selected and disabled.

7. On the **Create ADF Permission Grant** screen, click **Create Permission Grant**.

To delete an ADF permission grant for a work element:

- In the **ADFPPermissions Grant** area, select the permission grant you want to delete, and then click the **Delete Selected ADFPermission Grant** icon.

Figure 3–19 Delete ADF Permission Grant Icon

ADF Permission Grants - ID: ExecutiveDashboard				
Delete		New		
SELECT	GRANTEE TYPE	GRANTEE NAME	PERMISSION GRANT TARGET	PERMISSION GRANT ACTIONS
<input type="radio"/>	Realm Role	DEMO_Executive	oracle.retail.portal.view.p...	customize,personalize,view

Exporting and Importing Portlet Customizations

Retail Workspace is a Oracle WebCenter based application with support for run-time customization and personalization of portlets. Portlet customizations are the default preferences that are visible to all users. Portlet personalizations are preferences that are visible only to the user who specified them. With the right permissions, users of Workspace can customize and personalize portlets that appear on the dashboards and other Workspace pages.

Portlet customizations and personalizations are stored in a Metadata Services (MDS) repository. With this capability comes the need for migrating portlet preferences from one environment to another. For example, one may want to migrate customizations from a development environment to a production environment, from one production environment to another, or from one Workspace version to another.

Workspace provides tools for exporting and importing portlet customizations.

Note: As of Oracle WebCenter 10.1.3.4 (on which Workspace 13.1.3 is based), personalizations do not get migrated when using the Export/Import tool. This has been reported as a defect against WebCenter 10.1.3.4.

The portlets provided by Workspace have "allow export" and "allow import" properties enabled by default. This means that after a Workspace portlet is dropped on a dashboard page, any run-time customizations made to the portlet instance will be exported when using the Export tool. This also means that any run-time customizations made while developing and testing a dashboard will be exported with the application EAR file when it is deployed to the production environment.

If you do not want to allow export or import of the customizations you can disable this feature in the Workspace portlets. This can be done by editing *oracle-portlet.xml* and setting the value of the `<allow-export>` and `<allow-import>` elements within each `<portlet-extension>` element and within the `<portlet-app-extension>` element to *false*. The *oracle-portlet.xml* file is located in the WEB-INF directory of the portlet application. For

more information, refer to the section *19.1.3 Implementing Export/Import of Customizations (WSRP 2.0)* of the *Oracle® WebCenter Framework Developer's Guide 10g (10.1.3.2.0)*.

The Workspace Export/Import tool is a utility consisting of the following two shell scripts:

- **exportPortletPrefs.sh** – Used to export the customizations into an EAR file.
- **importPortletPrefs.sh** – Used to import a previously exported EAR file into the application where customizations need to be migrated.

These scripts are located in the *workspace/migration* directory of the *orw-admin-tools.zip* archive which is part of the Workspace application bundle. To obtain or get access to these scripts, you may need to contact the system administrator.

Note: Both the source and target applications should be stopped before exporting and importing customizations.

For the scripts to run, the following environment variables must be set:

- **ORACLE_HOME** – This variable must be set up to point to the Oracle Application Server installation directory.
- **JAVA_HOME** – This variable must be set up to point to the Java installation directory. If this variable is not set, the script defaults to the JDK present in the **ORACLE_HOME**

exportPortletPrefs.sh Usage

```
exportPortletPrefs.sh -oc4jInstance <instanceName>
-applicationName <appName> -exportEar <earName>
```

where,

- **<instanceName>** – Name of the oc4j instance where the source application is deployed.
- **<appName>** – Name of the application from which the customizations need to be exported.
- **<earName>** – Name of the EAR file where the customizations need to be exported. The path for the EAR file can be an absolute path or relative path to the file.

All arguments are mandatory.

For Example:

```
exportPortletPrefs.sh -oc4jInstance dashboards_oc4j
-applicationName DemoExecutiveDashboardApp
-exportEar ExecutiveDashboardCust.ear
```

importPortletPrefs.sh Usage

```
importPortletPrefs.sh -oc4jInstance <instanceName>
-applicationName <appName> -importEar <earName>
```

where,

- **<instanceName>** – Name of the oc4j instance where the application into which the customizations are to be imported is deployed

- <appName> – Name of the application into which the customizations need to be imported
- <earName> – Name of the EAR file from which customizations need to be imported. This may be an absolute path or relative path to the file.

All arguments are mandatory.

For Example:

```
importPortletPrefs.sh -oc4jInstance dashboards_oc4j  
-applicationName DemoExecutiveDashboardApp  
-importEar ExecutiveDashboardCust.ear
```

Managing External Applications

Any application that does not participate in the Oracle Application Server Single Sign-On (OSSO) authentication process is considered as an external application. These applications typically implement their own authentication process, where the users may need to specify a user name and password each time they access the application.

Oracle Application Server Single Sign-On (OSSO) includes a facility that enables you to configure a transparent authentication to the external applications. Once configured, the user credentials are encrypted and stored when the users access the external application for the first time.

Note: This facility is an integral part of the Oracle Portal Development Kit (PDK). Since many of the OSSO external application APIs are exposed as URLs, the facility may be used outside the PDK.

This section introduces you to the administrative aspects of the OSSO external applications and Workspace. It includes the following sections:

- [Overview of the OSSO External Applications Facility](#)
- [Defining an External Application in OSSO](#)
- [Obtaining the OSSO External Application ID](#)
- [Managing User Credentials](#)
- [Configuring Workspace to Launch External Applications via OSSO](#)
- [Sample External Application JavaScript and HTML](#)

For additional information, refer to the *Oracle Retail Workspace Implementation Guide* or the *Oracle Application Server Single Sign-On Administration Guide*.

Overview of the OSSO External Applications Facility

The OSSO *External Application* facility works in the following manner:

1. As an administrator, you first create an external application definition in the OSSO system. This definition includes the URL to which the user credentials are submitted and any other parameters needed to launch the external application.
2. Once configured, if a user wishes to launch the external application and has the OSSO login credentials, the user enters the OSSO "process login" URL, along with the unique OSSO identifier as a parameter.
3. If the OSSO system has not yet stored the user's credentials (user ID and password), the user is prompted for them by the OSSO system.

4. The OSSO system reads the external application definition and the user credentials associated with the application, and creates a URL containing the credentials (based on the authentication scheme). Depending on the external application definition, the Web browser is then redirected or a form is submitted to the application URL.
5. The OSSO external application processes the request made in the step above, and the user gets logged on to the application.

Note: Although the *OSSO External Application* facility deals with a single operation, it does not maintain any state of the user's browser session. It also does not determine whether a specific user is already logged in to the external application.

Some applications require additional processing. For example, an application may require a browser to request a specific URL before accessing the URL used to authenticate the user. Also, this second URL may only be legally accessed when the user has not previously logged into the external application. A category of these applications use the "j_security_check" authentication mechanism. Sample JavaScripts are provided that may be used to provide a Single Sign-On experience with this category of applications.

Pre-requisites

When OSSO is configured to use Oracle Database 10g Release 2 (10.2.0) or later, the `init{SID}.ora` configuration file must contain a specific "event" entry for the *External Applications* facility to work. For more information on this configuration, refer to the **My Oracle Support Note #344602.1 WWC-00006 and WWC-41400 When Trying To Login To An External Application**.

Supported Types of Authentication

The *OSSO External Application* facility supports the following authentication mechanisms:

- BASIC Authentication – The user credentials are supplied to the application as part of the URL. For example,

`http://username:password@host.company.com/appname`

Note: URLs containing the "username:password" construct are not supported in recent versions of Microsoft's Internet Explorer, unless specific Microsoft Windows registry entries are modified. For more information, see the *Help and Support article #834489* on the Microsoft Web site. You may also choose to access the external application via a JavaScript, such as the one used by the *basicAppRemote.html* file described in the *Oracle Retail Workspace Implementation Guide*.

- GET Authentication – The user credentials are passed as parameters in the URL's query string and an HTTP GET operation is performed. The names of these parameters are application specific. The query string may be seen in the Web browser's address bar when the operation has completed.

- **POST Authentication** – The user credentials are passed as parameters within an HTTP POST (form submit) operation. The credentials information is not displayed to the user.

Security Considerations Launching External Applications

The main security consideration for launching an external application is protecting the user name and password from disclosure. The OSSO system stores this information in an encrypted form in the OSSO database. However, unless the URL accessed uses the secure HTTPS protocol, this information is not encrypted when the browser submits the user's credentials to the external application. Unless HTTPS is used with both the OSSO URL and the external application's URL, the user's credentials will be transmitted in clear text or in an easily decoded format. Also, if the "GET" authentication is used, this information may also be displayed in the browser's address bar.

Defining an External Application in OSSO

The *External Applications* facility in OSSO enables you to configure external applications for single sign-on support. This section describes how you can define an external application in the OSSO system.

Important: Before you begin, ensure that you have administrative privileges and your user account is a member of the *iASAdmins* group in order to manage OSSO external application definitions. Members of this group have significant additional privileges as well.

The user ID 'orcladmin' is typically made a member of the *iASAdmins* group when OID is installed. Following is the distinguished name (DN) of the *iASAdmins* group:

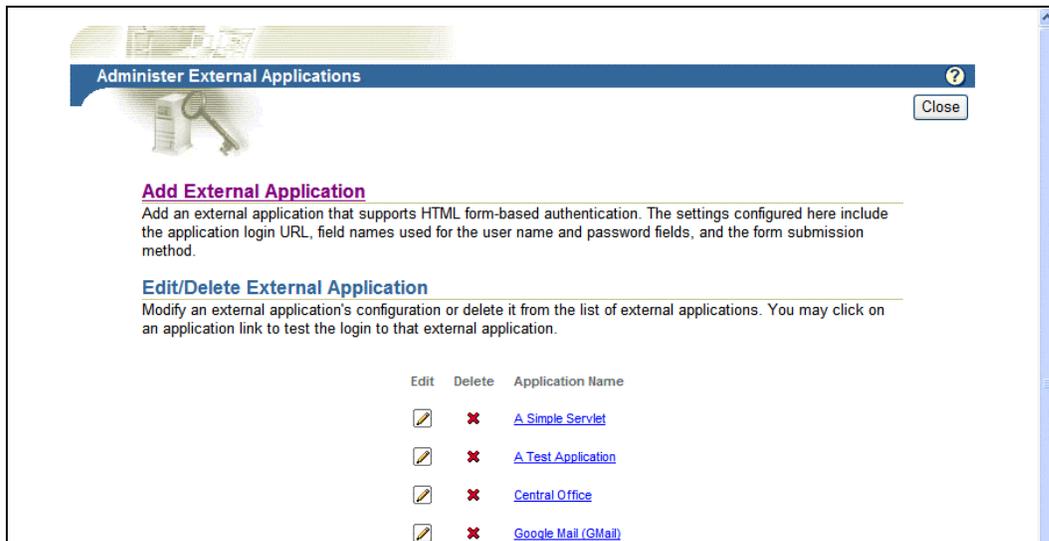
```
cn=iASAdmins,cn=Groups,cn=OracleContext
```

Members can be added to this group using the *ldapadd* command, the *oidadmin* tool, and other LDAP tools.

To define an external application:

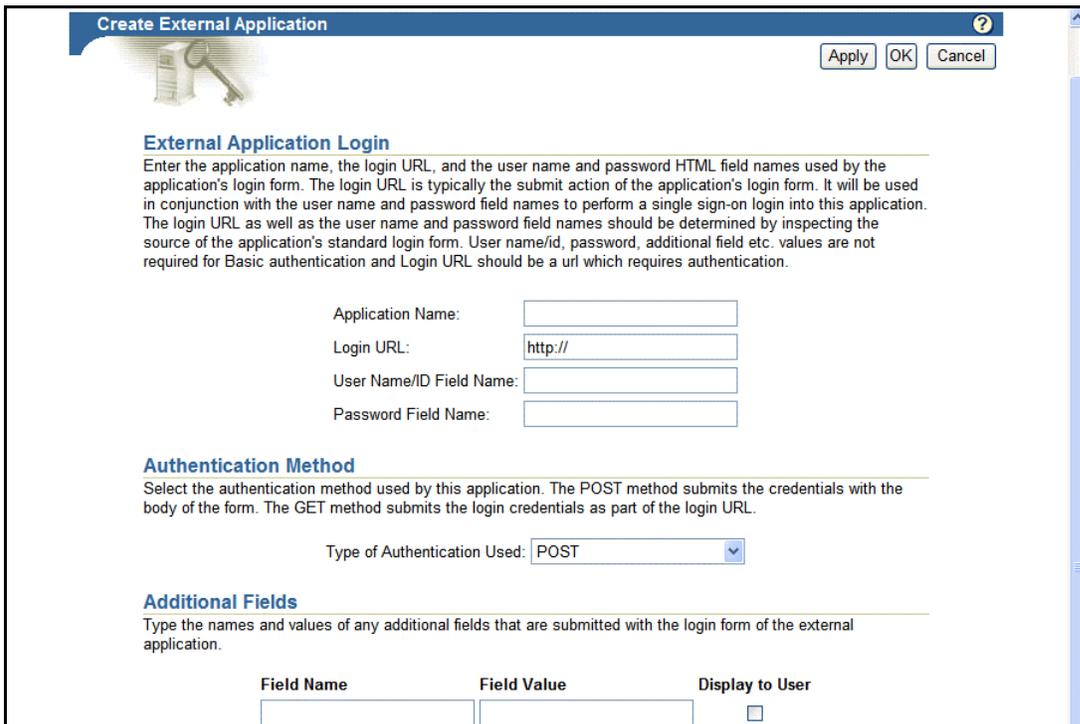
1. Click the OSSO External Application Management URL. For more information, see [Launching OSSO External Application Management](#). The **Administer External Applications** page appears.

Figure 4–1 Administer External Applications Page



2. To add a new external application, click the **Add External Application** link. The **Create External Application** page appears.

Figure 4–2 Create External Application Page



3. On the **Create External Application** page, enter relevant information in the following fields:
 - **Application Name** – Name appearing on the **Administer External Application** page.

- **Login URL** – The URL (host name, port, URI) to which the user credentials are submitted.
- **User Name/ID Field Name** – The name of the **parameter** that identifies the user name or user ID. The value of the parameter with this name is the user ID used to log on to the external application. This field is valid only for the "GET" and "POST" authentication types.
- **Password Field Name** – The name of the **parameter** that identifies the password (associated with the user account) used to log on to the external application. This field is valid only for the "GET" and "POST" authentication types.
- **Type of Authentication Used** – The authentication mechanism to be used for the external application. For more information on the options, see [Supported Types of Authentication](#).
- **Additional Fields** – This section enables you to specify additional parameters associated with the login URL of the external application. These parameters, along with the UserName/ID and the Password fields, may need to be included in the Login URL's query string ("BASIC" or "GET" authentication) or submitted as form input parameters ("POST" authentication). Select the **Display to User** check box to make the field value editable for the users when they specify the user credentials to log on to the external application.

Note: Information stored in **Additional Fields** section is not encrypted within the OSSO database.

You can find additional information on these fields in the chapter "Configuring and Administering External Applications" of the *Oracle Application Server Single Sign-On Administrator's Guide*.

4. Click **OK**. The new external application appears under the **Edit/Delete External Application** section on the **Administer External Applications** page, along with the other external applications.

Determining the Authentication Type and Additional Fields Values

Determining the values used for the "Type of Authentication Used" and the "Additional Fields" table requires an in-depth knowledge of the external application implementation. You can find additional information on the techniques in the *Oracle Single Sign-On Administration Guide* and the *Oracle Retail Workspace Implementation Guide*.

Launching OSSO External Application Management

The Workspace application can be configured to provide a link to the OSSO URL used to manage the external applications. The OSSO URL has the following form:

```
http[s]://[OSSO Host]:[OSSO Port]/sso/pages/eapp.jsp
```

where,

- *http[s]* is "http" or "https".
- *[OSSO Host]* is the host name of the OSSO server.
- *[OSSO Port]* is the associated port number of the OSSO server.

A link to this URL is available in the *sample retail-workspace-page-config.xml* file that gets installed with Workspace. You can find this link under the *Admin Tools* folder in the *Tools* worklist.

Testing an External Application Definition

Once you define the external application, you should test the definition to verify that the external application is configured correctly. To test the external application definition:

- On the **Administer External Application** page (Figure 4–1, "Administer External Applications Page"), in the **Edit/Delete External Application** section, click the application under the **Application Name** link column. If the configuration is accurate, the application will launch in a new browser window using the current definition.

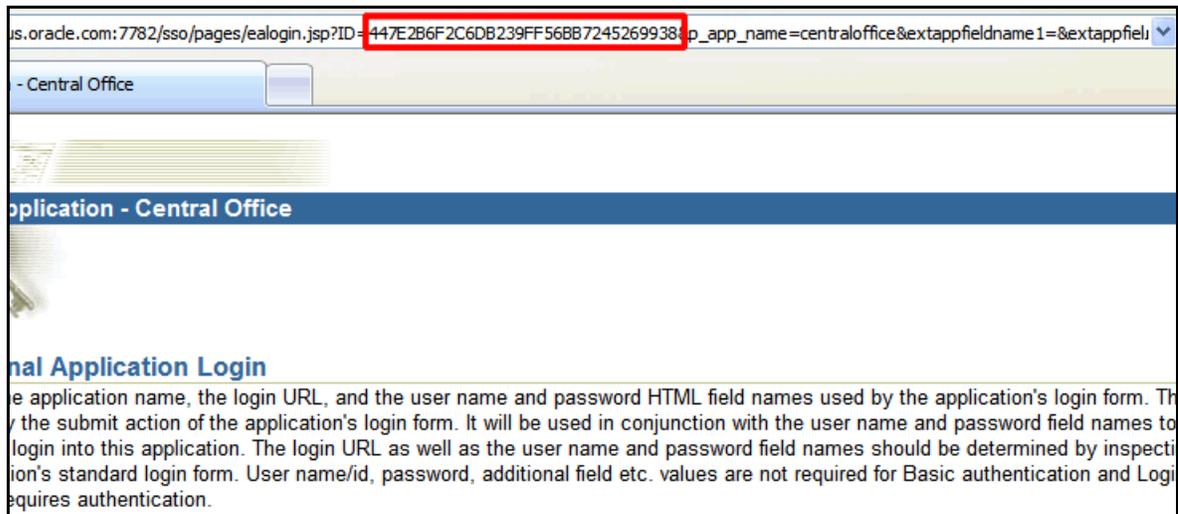
Figure 4–3 External Application Login page

Note: A user's credentials can be defined the first time the external application is accessed. However, other factors may override this capability.

Obtaining the OSSO External Application ID

Each external application definition has a unique identifier. This identifier is presented in many of the URLs within the OSSO system to launch the application or manage the application's definition within OSSO. You must obtain this external application identification number to configure the launch of the application from Workspace (as an administrator) or to create/modify credentials for this application (as a user).

You can obtain the OSSO external application ID from the *ID* parameter found in many of the OSSO URLs. The following figure (Figure 4–4) shows an OSSO External Application with an ID of `447E2B6F2C6DB239FF56BB7245269938`.

Figure 4–4 OSSO URL with the External Application ID

Note: This screen appears when you click the **Edit** link for the application on the **Administer External Applications** page.

Managing User Credentials

User credentials are managed on a per application basis. The users are presented with the following page (Figure 4–5) when they attempt to launch an application before defining the relevant credentials needed for that application.

Figure 4–5 External Application Login page

The screenshot shows the "External Application Login" page. At the top, there is a blue header with the text "Login - Central Office" and a help icon. Below the header, there are "Login" and "Close" buttons. The main content area has a section titled "External Application Login" with a paragraph of text: "Enter your user name (or other form of application identification) and password for this application. You may also enter custom values for any additional login parameters shown. The SSO Server uses this information to login on your behalf. If you click Remember My Login Information For This Application, you will then be logged in automatically each time you access this application." Below this text, there are three input fields: "Application Name: Central Office", "User Name/ID", and "Password". There is also a checkbox labeled "Remember My Login Information For This Application" which is checked. At the bottom right, there are "Login" and "Close" buttons. At the bottom left, there is a copyright notice: "Copyright© 2005, Oracle. All Rights Reserved".

You can also access this page in a stand-alone manner by using its URL and specific query string parameters. The URI and query string segments of the URL are:

`/sso/pages/eallogin.jsp?ID=[OSSO ID]`

where, *[OSSO ID]* is the OSSO External Application ID. The host/port/scheme portions of the URL are the same as used with DAS.

You may leverage the DAS URL managed bean to find the OSSO host/port/scheme segments when configuring the *retail-workspace-page-config.xml* file. The example below shows an entry used to manage user credentials for Central Office:

```
<secure-work-item id="userCredCentralOffice"
  display-string="Central Office (CO) "
  rendered="true"
  launchable="true"
  show-in-content-area="false">
<url>#{dasUrl.baseUrl}/sso/pages/ealogin.jsp</url>
<parameters>
  <parameter name="ID">
    <value>447E2B6F2C6DB239FF56BB7245269938</value>
  </parameter>
</parameters>
</secure-work-item>
```

Configuring Workspace to Launch External Applications via OSSO

This section details the entries in the Workspace configuration file (*retail-workspace-page-config.xml*) needed for launching and managing the external applications.

All of the examples use the *<secure-work-item>* element. You must create a WorkElement permission grant before any users access these entries in the Workspace application. Permission grants can be created using the Permissions Management feature in Workspace (see [Managing Access to Workspace Components](#)). Alternatively, you may define all of the entries below using the *<work-item>* element, indicating no access control and therefore not secure.

Note: Permission grants are cached by the Oracle Application Server container. This cache may take some time before it is refreshed with new information, depending on the configuration of the *jazn.xml* file. The default cache refresh period is one hour.

To configure the Workspace application to launch the external applications, the *retail-workspace-page-config.xml* file must contain the following three entries:

- An entry to launch the external applications administration in order to create, update, or delete the external application definitions in OSSO. The OSSO host/port/scheme information may be retrieved from the DAS URL managed bean found within Workspace.

An example of this entry in the *retail-workspace-page-config.xml* file is:

```
<secure-work-item id="adminExternalApps"
  display-string="#{confMsgs.manageExternalApps} "
  rendered="true"
  launchable="true"
  show-in-content-area="false">
  <url>#{das.Url.baseUrl}/sso/pages/eapp.jsp</url>
</secure-work-item>
```

In the sample *retail-workspace-page-config.xml* file, this entry already exists in the *Admin Tools* folder found in the *Tools* worklist.

- An entry to launch the specific external application. This entry will reference the OSSO external application ID to actually launch the URL. This entry may reference the DAS URL bean to find the OSSO host/port/scheme information.

An example of this entry in the `retail-workspace-page-config.xml` file is:

```
<secure-work-item id="launchMyExternalApp"
  display-string="Launch My External Application"
  rendered="true"
  launchable="true"
  show-in-content-area="false">
  <url>#{dasUrl.baseUrl}/sso/ealoglein</url>
  <parameters>
    <parameter name="ID" >
      <value>B9393469CEC51BDBBD9A8FA37DCDACB2</value>
    </parameter>
  </parameters>
</secure-work-item>
```

- An entry to allow a user to manage the credentials used when launching the external application. This entry is needed in case the user enters the wrong credentials or the credentials change because of some external event. This entry will reference the OSSO External Application ID. This entry may reference the DAS URL bean to find the OSSO host/port/scheme information.

An example of this entry in the `retail-workspace-page-config.xml` file is:

```
<secure-work-item id="userCredForMyExternalApp"
  display-string="Manage Credentials for My External Application"
  rendered="true"
  launchable="true"
  show-in-content-area="false">
  <url>#{dasUrl.baseUrl}/sso/pages/ealoglein.jsp</url>
  <parameters>
    <parameter name="ID" >
      <value>B9393469CEC51BDBBD9A8FA37DCDACB2</value>
    </parameter>
  </parameters>
</secure-work-item>
```

Sample External Application JavaScript and HTML

The OSSO *External Application* facility cannot by itself launch all external applications because of the wide variability in application architectures and implementations.

Also, recent versions of Microsoft Internet Explorer do not support the URL supplied by OSSO for applications using BASIC authentication.

In many cases, launching an application may require the use of additional software, such as JavaScript, to handle these applications. Workspace includes a set of sample HTML and JavaScript files which provide transparent log-on capability for many external applications. An example of an application that may be launched by these scripts is Oracle Retail Central Office. For more information on these scripts, refer to the *Oracle Retail Workspace Implementation Guide*.

Index

A

- access, 3-10
- ADF, 3-13
- admin tools, 3-3
 - create role, 3-7
 - create user, 3-4
 - delete role, 3-9
 - delete user, 3-7
 - edit role, 3-8
 - edit user, 3-6
 - permissions management, 3-10
- application launch, 2-1
- applications
 - supported, 2-2
- authentication, 4-2
 - BASIC, 4-2
 - GET, 4-2
 - POST, 4-3

B

- Bi delivers alerts, 2-3
- BPEL workflows, 2-4
- BPM worklists, 2-3

C

- configure
 - external application, 4-8
- create
 - role, 3-7
 - users, 3-4
 - multiple, 3-5
- customize, 3-16

D

- dashboards, 2-1
 - pre-defined, 2-1
- define
 - external application, 4-3
- delete
 - roles, 3-9
 - users, 3-7

E

- edit
 - profile, 3-2
 - roles, 3-8
 - users, 3-6
- export/import tool, 3-17
- exportPortletPrefs, 3-17
- external application, 4-1
 - configure, 4-8
 - define, 4-3
 - identifier, 4-6
 - manage, 4-5
 - overview, 4-1

G

- grant
 - access permissions, 3-10
 - ADF permissions, 3-13

H

- hint question, 1-6

I

- identification number, 4-6
- importPortletPrefs, 3-17

J

- javascript
 - sample, 4-9

L

- launch
 - reports, 2-2
- launch application, 2-1
- ldif, 3-5
- log on, 1-5
 - set up profile, 1-6

M

- manage

- access, 3-3, 3-10
- roles, 3-3
- user profile, 3-1
- users, 3-3

O

- overview
 - external application, 4-1

P

- password
 - reset, 1-8, 3-2
- permissions, 3-10, 3-13
- permissions management, 3-10
- personalize, 3-16
- portlet
 - customize, 3-16
 - personalize, 3-16

R

- reports
 - launch, 2-2
- reset
 - password, 3-2
- reset password, 1-8
- roles
 - create, 3-7
 - delete, 3-9
 - edit, 3-8

S

- search, 3-3
 - users, 3-3
- set up
 - hint question, 1-6
- supported
 - applications, 2-2

T

- test
 - external application, 4-6

U

- user interface, 1-4
- user profile, 3-1
 - set up, 1-6
- user tools, 3-1
 - edit profile, 3-2
 - reset password, 3-2
 - search users, 3-3
 - view profile, 3-1
- users
 - create, 3-4
 - delete, 3-7
 - edit, 3-6

V

- view
 - profile, 3-1

W

- workspace
 - log on, 1-5
 - user interface, 1-4