

Oracle® Financial Services IFRS 9 Solution Cloud Service Admin Console



Release 25A
G37836-01
April 2025

ORACLE®

Oracle Financial Services IFRS 9 Solution Cloud Service Admin Console, Release 25A

G37836-01

Copyright © 2024, 2025, Oracle and/or its affiliates.

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

1 About This Content

2 Introduction to Admin Console

Administrator Tasks	2-1
Authorizer Tasks	2-1

3 System Configuration

Metering	3-1
Component Details	3-1
OCI Console	3-1
Object Storage Archive	3-2
OAUTH Creds	3-2
Object Storage Standard	3-3
Audit Trail Report	3-4
Configurations	3-5
Reports For Download	3-6
Prerequisites	3-6
Access Reports for Download	3-6
Data Reporting - Data View	3-6
View the Report Details	3-7
Apply a Custom Filter to the Data View	3-7

4 Identity Management

Users Summary Page	4-1
User Details	4-2
Mapped and Unmapped Groups	4-3
Mapped Groups	4-4
Unmapped Groups	4-5
Groups Summary Page	4-5
Group Details	4-6
Mapped and Unmapped Roles	4-6

Mapped Roles	4-8
Unmapped Roles	4-8
Available Roles	4-9
Roles Summary Page	4-9
Roles Details	4-10
Mapped and Unmapped Functions	4-11
Mapped Functions	4-12
Unmapped Functions	4-12
Folders Summary Page	4-13
Folder Details	4-14
Editing Folder Details	4-15
Functions Summary Page	4-15
Function Details	4-17
Mapped and Unmapped Functions	4-17
Mapped Functions	4-19
Unmapped Functions	4-19

1

About This Content

This guide provides information on the newly released Oracle Financial Services IFRS 9 Solution Cloud Service (OFS IFRS9SCS).

Audience

This document is intended for users of the Oracle Financial Services IFRS 9 Solution Cloud Service (OFS IFRS9SCS) application.

Documentation Accessibility

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

Access to Oracle Support

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

Related Resources

See these [Oracle resources](#):

- Getting Started with Oracle Cloud
- Admin Console User Guide
- Oracle Financial Services IFRS 9 Solution Cloud Service User Guide

Conventions

The following text conventions are used in this document.

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

2

Introduction to Admin Console

Use the Admin Console to perform System Configuration and Identity Management.

[Admin Console](#) is the single point of access to manage identity functions and view administrative features such as Metering, Audit Trail Report and other miscellaneous configuration details in the Cloud Service.

Administrator Tasks

As an Administrator, use the Admin Console to perform the following tasks:

- View the Metering Report, Audit Trial Report, Object Storage, and Object Authentication (OAUTH) credential details in the System Configuration tab.
- Perform the Identity and Access Management operations in the Identity Management tab.

Authorizer Tasks

As an Authorizer, use the **Admin Console** to authorize the Identity and Access Management Operations in the **Identity Management** tab.

3

System Configuration

Administrators can monitor the usage of service units and user activities through the System Configuration.

With System Configuration, administrators can view the consumption of service units. You can also view the following:

- The Audit Report to see what actions the users have performed in the application and when they have performed them
- The provisioned object storage details and the OAuth authentication details
- The production instance URL and the email ID of the login user

The components are as follows:

- **Metering:** Click **Metering** to view the usage of services using the Metering Report.
- **Audit Trail Report:** Click **Audit Trail Report** to view details such as the user's login and logout information, the action they performed, the status of the actions, and the date and time of each action.
- **Component Details:** Click **Component Details** to view details such as the Object Storage, Pre-Authenticated Request (PAR) URL, and OAuth authentication details.
- **Configurations:** Click **Configurations** to specify the instance name and the user(s) who receive emails related to operations tasks.

Metering

Use the **Metering** page to view the monthly unit usage of the number of transactions and the number of report types within the Cloud Service.

Component Details

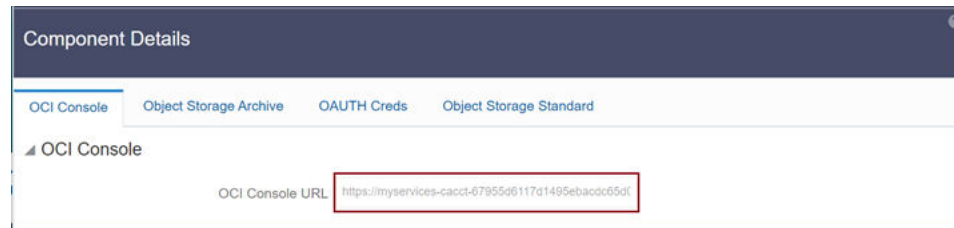
Use the Component Details page to view the OCI Console, Object Storage Standard and Archive details, and OAUTH Authentication details.

To access Component Details window:

1. Login to the Admin Console.
2. Go to **System Configuration** tab, and click **Component Details** tile.

OCI Console

Click **OCI Console** tab to view and copy the OCI Console details.

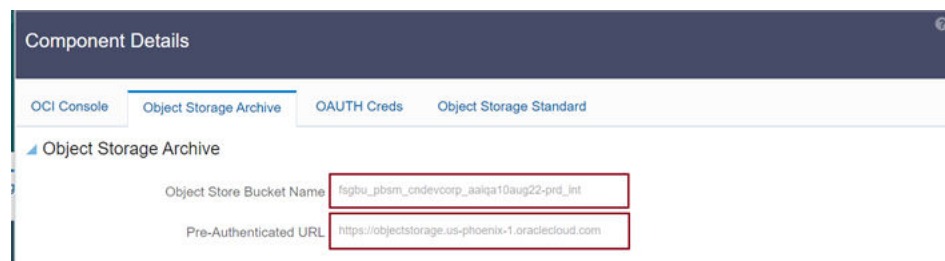
Figure 3-1 OCI Console Page

Object Storage Archive

When you provision an instance of the application, two buckets, a Standard Storage Bucket and an ArchiveStorage Bucket are automatically provisioned. The objects data that you want to load into the application for processing must be uploaded to the Standard Storage Bucket.

Archive Storage is used for storing objects which are not in use but must be retained and preserved for long periods of time. Objects are automatically moved from standard to archive storage, after 7 days.

Click **Object Storage Archive** Tab to view and copy the **Object Store Bucket Name** and the **Pre-Authenticated URL**.

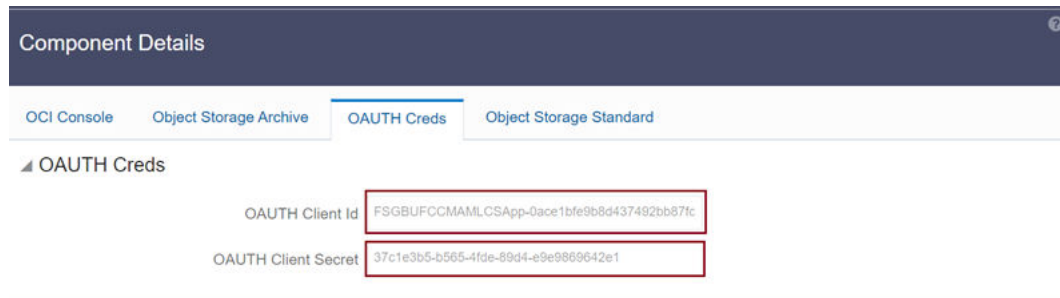
Figure 3-2 Object Storage Archive Page

Field	Description
Object Store Bucket Name	The logical container in which objects are stored.
Pre-Authenticated URL (PAR URL)	Request that enables you to access a bucket without providing any credentials.

OAuth Creds

The OAuth Creds is used for implementing authentication in Cloud Services.

Click OAuth Creds tab to view and copy the OAuth Client ID and OAuth Client Secret details.

Figure 3-3 OAUTH Creds Page

Component Details

OCI Console Object Storage Archive **OAUTH Creds** Object Storage Standard

▲ OAUTH Creds

OAUTH Client Id F5GBUFCCMAMLCApp-0ace1bfe9b8d437492bb87fc

OAUTH Client Secret 37c1e3b5-b565-4fde-89d4-e9e9869642e1

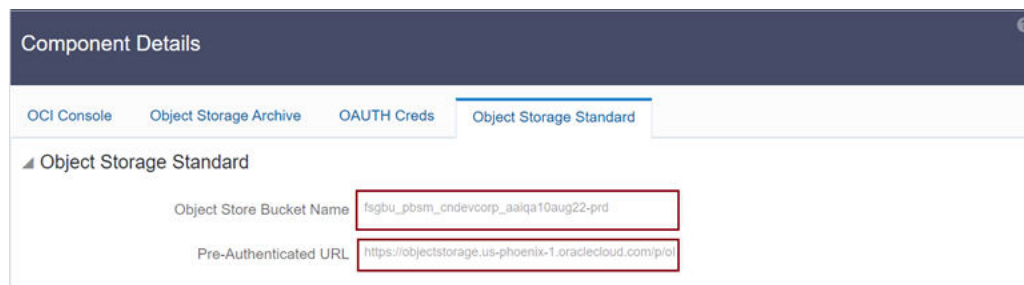
Table 3-1 Field Description

Field	Description
OAUTH Client ID	ID of the OAuth client used for OAuthAuthentication performed by IDCS while doing any API calls.
OAUTH Client Secret	Password of the OAuth client secret used for OAuth Authentication performed by IDCS while doing any API calls.

Object Storage Standard

Object Storage Standard is used for storing objects which are currently in use and require fast, immediate, and frequent access.

Click Object Storage Standard tab to view and copy the Object Store Bucket Name and the Pre-Authenticated URL.

Figure 3-4 Object Storage Standards Page

Component Details

OCI Console Object Storage Archive OAUTH Creds **Object Storage Standard**

▲ Object Storage Standard

Object Store Bucket Name fsgbu_pbsm_cndevcorp_aaiqa10aug22-prd

Pre-Authenticated URL https://objectstorage.us-phoenix-1.oraclecloud.com/p/oi

Table 3-2 Field Description

Field	Description
Object Store Bucket Name	The logical container in which objects are stored
Pre-Authenticated URL (PAR URL)	Request that enables you to access a bucket without providing any credentials.

Audit Trail Report

You can use Audit Trail Report to view details of the user's activities such as Login, Add Action, Status of the Action, and the Machine Name.

To generate an Audit Trail Report, follow these steps:

1. Login to the Admin Console.
2. Go to **System Configuration** tab, and click **Audit Trail Report** tile. The **Audit Trail Report** page is displayed.

Figure 3-5 Audit Trail Report

The screenshot shows the 'Audit Trail Report' page. It features a 'Search and Filter' section with the following fields: 'User Name' (set to 'All'), 'Action' (set to 'All'), 'From Date' (set to '09/07/2022'), 'To Date' (set to '09/22/2022'), and 'Action Detail' (with a 'Search Code...' input). There are 'Reset' and 'Search' buttons in the top right corner of the filter section.

3. Enter the following values and click Search to generate the Audit Trail Report for all users or a specific user.

Table 3-3 Audit Trail Report Filters

Field	Description
User Name	Enter or Search for a user name to view the report for the selected user.
Action	Select the Action from the actions. to generate a report for a specific action.
From Date	Select the Start Date for the report.
To Date	Select the End Date for the report.
Action Detail	Enter the string to search and filter the Audit Trail Report for a specific action.

Figure 3-6 OAUTH Creds Page

The screenshot shows the 'Audit Trail Report' page with a single record displayed. The record details are: User Name: Admin User, Action Detail: User: TEST_ADMIN logged in, Action Code: Login, Operation Time: 12-SEP-22 05:05:58.8 33502 +00:00, Status: Successful, and Action Subtype: -. The page shows 'Page 1 of 1 (1 - 1 of 1 items)' and 'Records 1'.

Table 3-4 Audit Trail Report Details

Field	Description
User Name	The user name selected in the User Name filter field.
Action Details	The action selected in the Action Detail filter field.
Action Code	The type of action performed by the user.
Status	The status of the action performed. The values are Successful or Failure.
Action Subtype	The sub type of the action.
Operation Time	The date and time of the action performed.

4. Click **Reset** to clear all values from the filter fields and enter new search criteria. The report filters are described in the following table:

Configurations

Use the Configurations page to update user preferences, master encryption key, notification preferences, and allowed email domains.

You can set the user preferences such as time zone and locale, master encryption key, notification configuration details, and update allowed email domains using the **Configurations** page.

To update the configuration details from the **System Configuration** tab:

1. Click the **Configurations** tile, to view and edit the user preferences, master encryption key and the notification details.
2. Click the required tab and modify the details.

-
- [Preferences](#)
 - [Master Encryption Key](#)
 - [Notification Configuration](#)
 - [Email Domains](#)

Preferences

Select the following details in the **Preferences** tab and click **Save** to update the details.

- **Time Zone** - The time zone displayed in the application.
- **Locale** - The language to access the application. The default value is **en - US English**.
- **Date Format** - The format in which the date is displayed.

Master Encryption Key

Enter the **Master Encryption key** and click **Save** to update the key value.

Notification Configuration

Enter the number of days after which the notification will be deleted automatically, and click **Save**.

Email Domains

Enter the allowed email domains, and click **Save**. Separate domains with commas, omitting the '@' symbol. Example: oracle.com, gmail.com.

Note:

Only users with the domains specified here will receive email notifications. To allow all domains, leave the field blank.

Reports For Download

The Reports for Download tile in the Admin Console consists of a set of pre-defined and pre-configured reports that are available for download. You can use the functions in the interface such as filter and sort to segregate the data and drill down to the details of the reports. You can then investigate the information, analyze, and export the data in CSV format.

In the Admin Console, you can download reports from Reports for Download in the System Configuration tab.

Prerequisites

To use Reports for Download from the Admin Console, your user profile must be mapped to the Data Maintenance Admin group to access the Reports for Download menu.

Access Reports for Download

To access the Data View window, click **Reports for Download** in the **System Configuration** tab. The **Data Reporting - Data View Page** is displayed.

Data Reporting - Data View

You can view the list of reports available for download, from the Data Entry window. Use one of the following criteria to view various reports.

- To search reports, click the Search field to display the search criteria pop-up. Enter search terms in the Name, Description, or Created By fields, or use a combination of the fields, and click Search.
The search result displays reports that match the criteria.
- To sort reports, click the Sort By drop-down and select from the options: Name, Description, or Created By.
The reports are displayed in ascending order for the selected option.
- To view the report creation and modification details, click the More Options (three dots) icon of a report to display the pop-up with the details for the following:
 - **Created By** - Displays the User ID of the user who created the report.

- **Created Date** - Displays the date and time of the creation of the report.
- **Last Modified By** - Displays the User ID of the user who last modified the report.
- **Last Modified Date** - Displays the date and time of the last modification of the report.
- **Authorizer** - Displays the User ID of the authorizer who approved the report to be displayed in the window.
- **Authorizer Comments** - Displays the comments entered by the authorizer when approving the report to be displayed in the window.
- To view a report, mouse over the record, and the hidden menu appears. Click View from the menu.
The details for the selected report are displayed in the Data Entry window.

View the Report Details

The Data Entry window is the interface where you can apply filter conditions (optional) on the reports and export the details.

You can apply the filter conditions (optional) to the reports in the Attributes Selection tab, and the results are displayed in the Data Preview tab from where you can export the report in the CSV format.

The procedure to view report details is described as follows:

1. In the **Data View** window, click **Attributes Selection**.
The Attributes Selection tab displays the details for the database table name in View Name and the table columns in Attribute Name. Expand View Name to display the columns in Attribute Name.
2. Click **Apply**.
The Data Preview tab displays the report details. The number of records displayed in the Data Preview tab is pre-configured in the system. However, you can export the details in the CSV format by clicking Download CSV.

Apply a Custom Filter to the Data View

In addition to the reports that you can view, you can also use the filter provided in the Data View window to custom filter the data in the reports for analysis purposes.

To apply a custom filter to the data view, follow these steps:

1. Click **Launch Filter** Condition to display the Filter Condition window.
2. Select **AND** or **OR** from the drop-down.
3. Select the required report column from **Select a Column**.
4. Select the required condition from **Select a Condition**.
5. Click **+ Condition** to add more conditions and click **+ Group** to add more groups.
Repeat the selection procedure to add details. To remove a condition or group, click Remove.
6. Click **Apply** in the **Filter Condition** window to save the custom filter condition.
7. Click **Apply** in the **Attributes Selection** tab.

The Data Preview tab displays the results of the Attributes filtered in the Attributes Selection tab. The number of records displayed in the preview is pre-configured in the system. However, you can export the details in the CSV format by clicking Download CSV.

4

Identity Management

Using Identity Management, administrators can manage fine-grained and coarse-grained entitlements. Coarse-grained entitlements consist of fewer functions than fine-grained entitlements. Authorizers can authorize the entitlement mappings.

The various **components** of Identity Management are:

- **Users:** A user is a person who has access to **Admin Console** and can perform specific actions based on the user group or groups they are mapped to. Before you can map a user to a user group, your Administrator must have created and authorized the user. After the user is authorized, they are added in the [Users Summary](#). Click **Users** to access the **Users Summary** page.
- **Groups:** Groups are a set of users who can perform specific activities. For example, the administrator role performs administrative activities. Any user who belongs to a specific user group can access the roles mapped to that user group. To add a user group, click **Add** in the **Groups** tile. Click **Groups** to view the list of user groups in [Groups Summary](#).
- **Roles:** Roles are a set of functions grouped together and having specific privileges. Any user who belongs to a specific role can access functions mapped to that role. Click **Add** to add a role or click **Roles** to view the list of roles in **Roles Summary**. To add a user role, click **Add** in the **Roles** tile. Click **Roles** to view the list of user groups in [Roles Summary](#).
- **Folders:** Folders are used to control access rights on defined list of objects. They are mapped to a specific Information Domain. Click **Folders** to view the list of folders and edit the access rights in [Folders Summary](#).
- **Functions:** Functions enable users to perform a specific activity. Any user who belongs to a specific function can access the folders mapped to the function. Click **Functions** to view the list of functions in [Functions Summary](#).



Note:

Only those user groups and roles which are authorized are displayed in the **Groups Summary** page and **Roles Summary** page, respectively.

Users Summary Page

The Users Summary page shows the list of available users. You can view the details of a user and map the user to one or more user groups.

To access Users Summary page, complete the following steps:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Users** tile.
The **Users Summary** page is displayed.

Figure 4-1 Users Summary Page

3. Select a specific User Name in the Users Summary page and then click **Details** to view the associated User ID and User Name.
4. Select a User name and click Mapped Groups to view the list of groups that are mapped to the particular user. For more information about mapped groups, refer to [Mapped and Unmapped Groups](#).
You can also Unmap an user from a specific group. For more information, refer to [Mapped and Unmapped Groups](#).

To search for a specific user, type the first few letters of the user name that you want to search in the Search box and click Search. The search results display the names that consist of your search string in the list of available users.

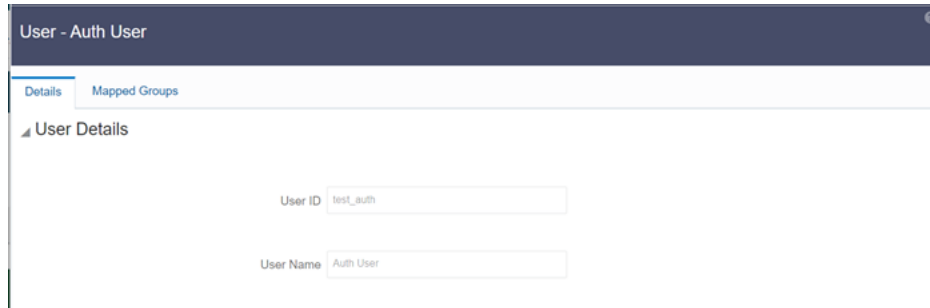
At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

- Use the First page  button to view the entries in the first page.
- Use the Previous page  button to view the entries in the previous page.
- Use the Next page  button to view the entries in the next page.
- Use the Last page  button to view the entries in the last page.

You can also navigate to the desired page. To do this, enter the page number in the View bar control and press Enter.

User Details

Click a specific User listed in the User Summary page and click Details to view the User ID and the User name of that user.

Figure 4-2 User Details Page

The screenshot shows a web interface for 'User - Auth User'. It has two tabs: 'Details' (selected) and 'Mapped Groups'. Under the 'Details' tab, there is a section titled 'User Details' containing two input fields: 'User ID' with the value 'test_auth' and 'User Name' with the value 'Auth User'.

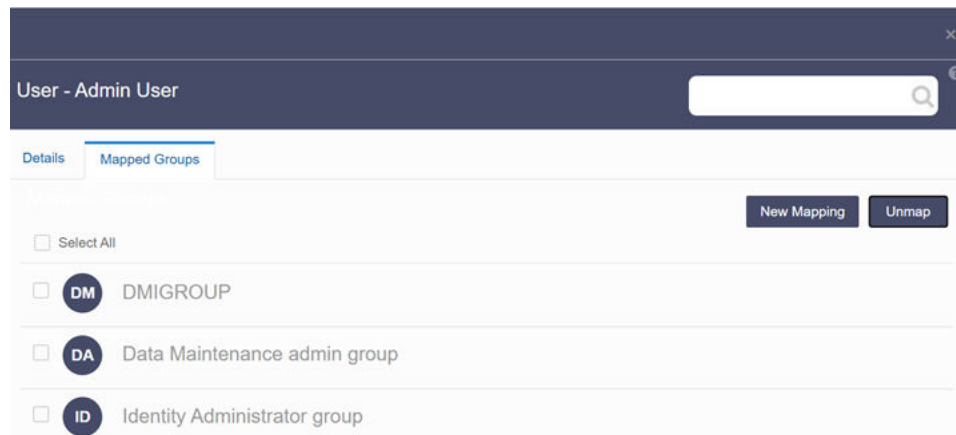
Mapped and Unmapped Groups

If you are an Administrator, you can map and unmap a user to a User group, from the **Users Summary** page.

Mapped Groups

Complete the following steps, to map an user to a User Group.

1. Select the **User name** in the **Users Summary** page.
2. Select **Mapped Groups**.
The list of groups mapped to the specific user is displayed.

Figure 4-3 Mapped Groups

The screenshot shows a web interface for 'User - Admin User'. It has two tabs: 'Details' and 'Mapped Groups' (selected). In the 'Mapped Groups' tab, there are two buttons: 'New Mapping' and 'Unmap'. Below these buttons is a list of groups with checkboxes and labels: 'DM DMIGROUP', 'DA Data Maintenance admin group', and 'ID Identity Administrator group'. There is also a 'Select All' checkbox at the top left of the list.

3. Click **New Mapping**.
After you click New Mapping, the list of user groups you can map the user to appears in the **Available Groups** page.
4. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an Authorizer and want to authorize a mapping, follow these steps:

- In **Mapped Groups**, select the user group name.
- Click **Authorize** to authorize the user-user group mapping.
Click **Reject** to cancel the authorization request.

Unmapped Groups

To unmap a user from a user group, complete the following steps.

1. Select the User name in the Users Summary page.
2. Select **Mapped Groups**.
The list of groups mapped to the specific user is displayed.
3. Select the check box corresponding to a User Group or click Select All to select all the available User groups.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Groups, select the user group name.
2. Click **Authorize** to authorize the user-user group unmapping.
Click **Reject** to cancel the authorization request.

Available Groups

Click **New Mapping** to view the list of user groups you can map to the user.

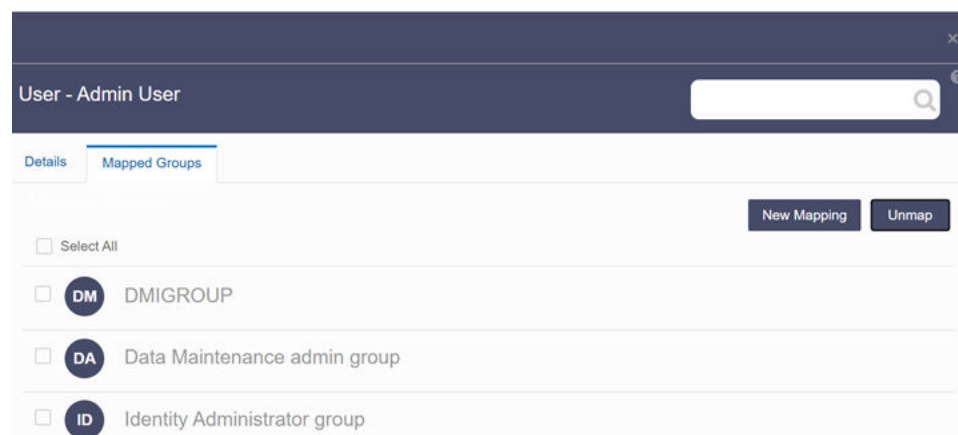
To select a user group, select the check box corresponding to the user group. To select all user groups, click **Select All**.

Mapped Groups

Complete the following steps, to map an user to a User Group.

1. Select the **User name** in the **Users Summary** page.
2. Select **Mapped Groups**.
The list of groups mapped to the specific user is displayed.

Figure 4-4 Mapped Groups



3. Click **New Mapping**.
After you click New Mapping, the list of user groups you can map the user to appears in the **Available Groups** page.

4. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an Authorizer and want to authorize a mapping, follow these steps:

- In **Mapped Groups**, select the user group name.
- Click **Authorize** to authorize the user-user group mapping.
Click **Reject** to cancel the authorization request.

Unmapped Groups

To unmap a user from a user group, complete the following steps.

1. Select the User name in the Users Summary page.
2. Select **Mapped Groups**.
The list of groups mapped to the specific user is displayed.
3. Select the check box corresponding to a User Group or click Select All to select all the available User groups.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Groups, select the user group name.
2. Click **Authorize** to authorize the user-user group unmapping.
Click **Reject** to cancel the authorization request.

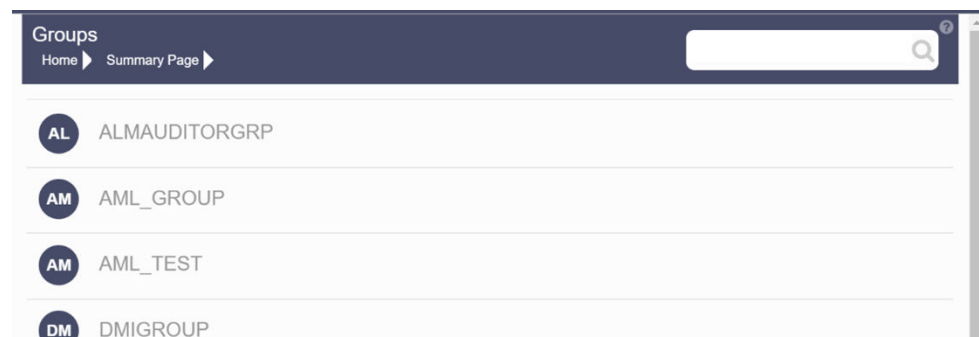
Groups Summary Page

The Groups Summary page shows the list of available groups. You can view the details of a group and map the group to one or more user roles.

To access the Groups Summary page:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Groups** tile.
The Groups Summary page is displayed.

Figure 4-5 Groups Summary Page



3. Select a specific Group Name in the Groups Summary page and then click Details to view the associated Group ID, Group Name and Group Description. For more information refer to [Group Details](#).
4. Select a Group name and click Mapped Roles to view the list of Roles that are mapped to the particular Group. For more information about mapped groups, refer to [Mapped and Unmapped Roles](#).
You can also Unmap a group from a specific Role. For more information, refer to [Mapped and Unmapped Roles](#).

To search for a specific user group, type the first few letters of the user group name that you want to search in the search box and click Search. The search results display the names that consist of your search string in the list of available users.

At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

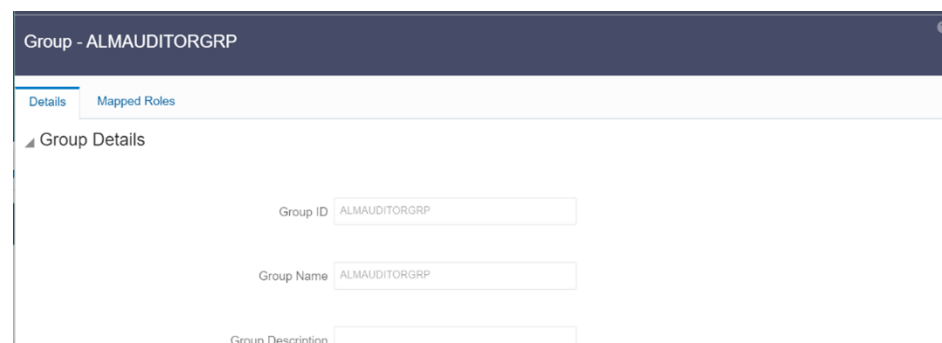
- Use the First page  button to view the entries in the first page.
- Use the Previous page  button to view the entries in the previous page.
- Use the Next page  button to view the entries in the next page.
- Use the Last page  button to view the entries in the last page.

You can also navigate to the desired page. To do this, enter the page number in the View bar control and press Enter.

Group Details

Select the Group name in the Groups Summary page and then select Details to view the Group ID, Group Name and Group Description.

Figure 4-6 Group Details Page



Group - ALMAUDITORGRP

Details Mapped Roles

Group Details

Group ID ALMAUDITORGRP

Group Name ALMAUDITORGRP

Group Description

Mapped and Unmapped Roles

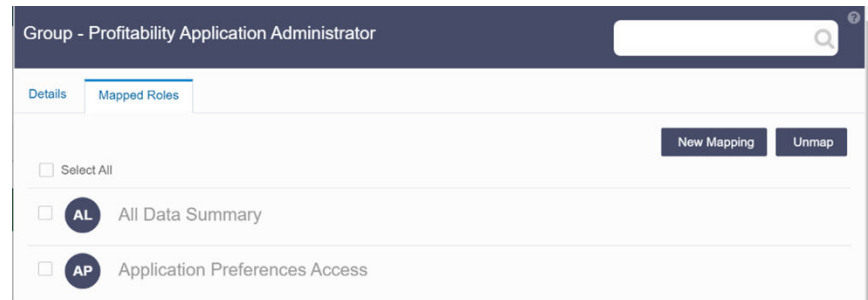
If you are an administrator, you can map and unmap a Group to a User Role, from the Groups Summary page.

Mapped Roles

Complete the following steps, to map an user to a User Group.

1. Select the User name in the Groups Summary page.
2. Select Mapped Roles.
The list of Roles mapped to the specific user is displayed.

Figure 4-7 Mapped Roles



3. Click **New Mapping**.
After you click New Mapping, the list of user Roles you can map the group to appears in the **Available Roles** page.
4. Select the check box corresponding to a User Role or click **Select All** to select all the available User Roles.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Roles**, select the user Role name.
2. Click **Authorize** to authorize the user-user group mapping.
Click **Reject** to cancel the authorization request.

Unmapped Roles

To unmap a Group from a Role, complete the following steps.

1. Select the Group name in the **Groups Summary** page.
2. Select **Mapped Roles**.
The list of Roles mapped to the specific user is displayed.
3. Select the check box corresponding to a User Role or click **Select All** to select all the available User Roles.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

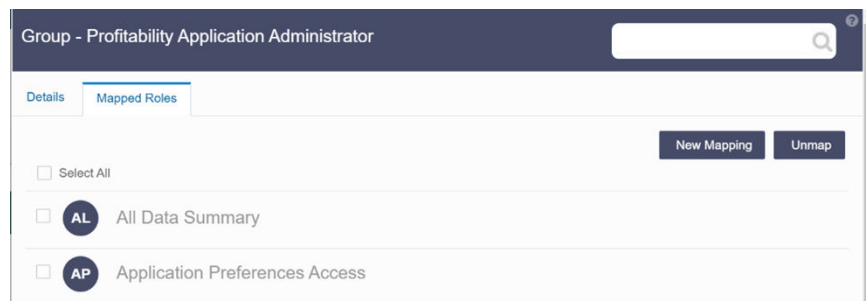
1. In **Mapped Roles**, select the user group name.
2. Click **Authorize** to authorize the user-user Role unmapping.
Click **Reject** to cancel the authorization request.

Mapped Roles

Complete the following steps, to map an user to a User Group.

1. Select the User name in the Groups Summary page.
2. Select Mapped Roles.
The list of Roles mapped to the specific user is displayed.

Figure 4-8 Mapped Roles



3. Click **New Mapping**.
After you click New Mapping, the list of user Roles you can map the group to appears in the **Available Roles** page.
4. Select the check box corresponding to a User Role or click **Select All** to select all the available User Roles.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Roles**, select the user Role name.
2. Click **Authorize** to authorize the user-user group mapping.
Click **Reject** to cancel the authorization request.

Unmapped Roles

To unmap a Group from a Role, complete the following steps.

1. Select the Group name in the **Groups Summary** page.
2. Select **Mapped Roles**.
The list of Roles mapped to the specific user is displayed.
3. Select the check box corresponding to a User Role or click **Select All** to select all the available User Roles.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Roles**, select the user group name.
2. Click **Authorize** to authorize the user-user Role unmapping.
Click **Reject** to cancel the authorization request.

Available Roles

Click New Mapping to view the list of roles you can map to the user group.

To select a role, select the check box corresponding to the role. To select all roles, select the check box marked **Select All**.

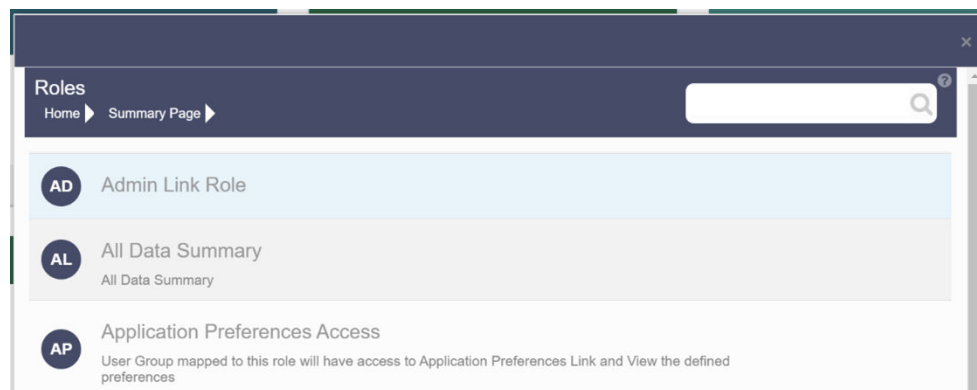
Roles Summary Page

The Roles Summary page shows the list of available User Roles. You can view the details of a Role and map the Role to one or more user Functions.

To access Roles Summary page, complete the following steps:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Roles** tile.
The **Roles Summary** page is displayed.

Figure 4-9 Roles Summary Page



3. Select a specific Role Name in the Roles Summary page and then click Details to view the associated Role Code, Role Name and Role Description. For more information refer to [Role Details](#).
4. Select a Role name and click Mapped Functions to view the list of Functions that are mapped to the particular Role. For more information about mapped Functions, refer to [Mapped and Unmapped Functions](#).
You can also Unmap a Role from a specific Function. For more information, refer to [Mapped and Unmapped Functions](#).

To search for a specific role, type the first few letters of the role name that you want to search in the Search box and click Search. The search results display the names that consist of your search string in the list of available users.

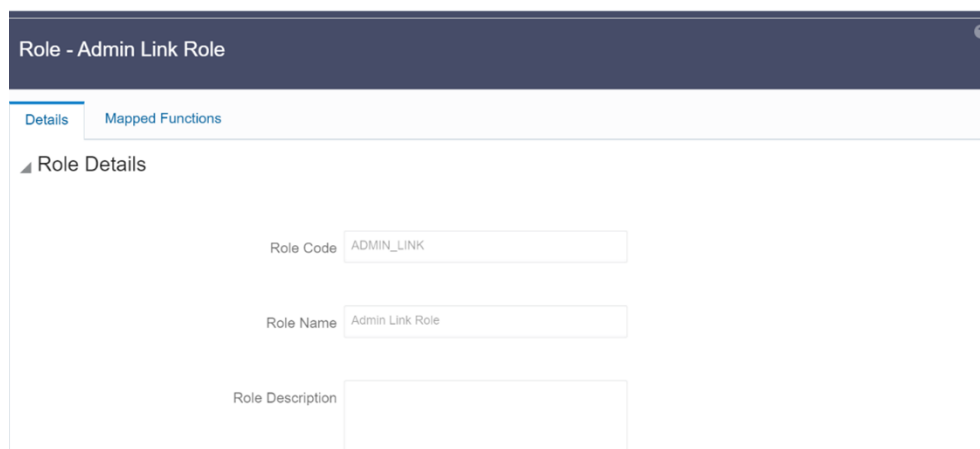
At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

- Use the First page  button to view the entries in the first page.
- Use the Previous page  button to view the entries in the previous page.
- Use the Next page  button to view the entries in the next page.
- Use the Last page  button to view the entries in the last page.
You can also navigate to the desired page. To do this, enter the page number in the View bar control and press Enter.

Roles Details

Click a specific Role listed in the Roles Summary page and click Details to view the Group ID, Group name and the description of that group.

Figure 4-10 Roles Details Page

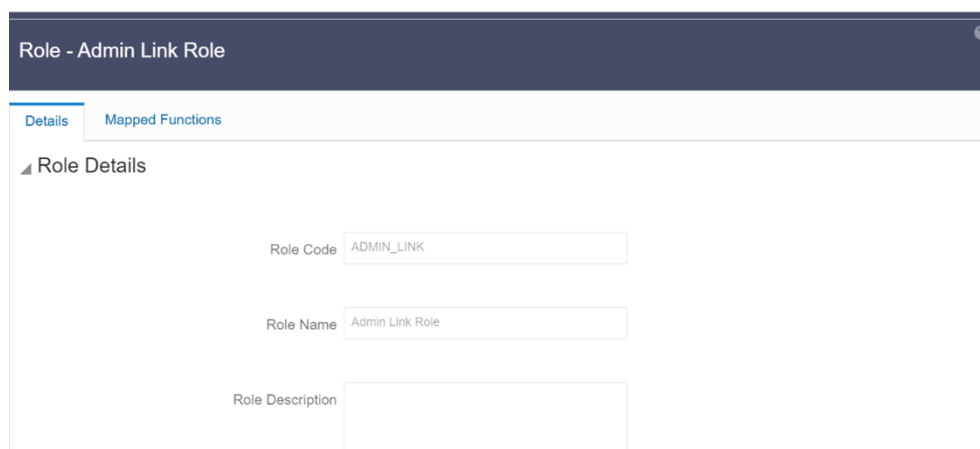


The screenshot shows a web interface for 'Role - Admin Link Role'. It has two tabs: 'Details' (selected) and 'Mapped Functions'. Under the 'Details' tab, there is a section titled 'Role Details' with a small triangle icon. Below this, there are three input fields: 'Role Code' with the value 'ADMIN_LINK', 'Role Name' with the value 'Admin Link Role', and 'Role Description' which is empty.

Roles Details

Click a specific Role listed in the Roles Summary page and click Details to view the Group ID, Group name and the description of that group.

Figure 4-11 Roles Details Page



This screenshot is identical to Figure 4-10, showing the 'Role - Admin Link Role' details page. It features the 'Details' tab selected, the 'Role Details' section, and the input fields for 'Role Code' (ADMIN_LINK), 'Role Name' (Admin Link Role), and an empty 'Role Description' field.

Mapped and Unmapped Functions

If you are an administrator, you can map and unmap a User Role to a Function, from the Roles Summary page.

Mapped Functions

Complete the following steps, to map a Role to a Function.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific user is displayed.

Figure 4-12 Mapped Functions



3. Click **New Mapping**.
After you click New Mapping, the list of user Functions you can map the Role to appears in the **Available Functions** page.
4. Select the check box corresponding to a Function or click Select All to select all the available Functions.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Functions, select the Function Name.
2. Click **Authorize** to authorize the Role Function mapping.
Click **Reject** to cancel the authorization request.

Unmapped Functions

To unmap a Role from a Function, complete the following steps.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific Role is displayed.
3. Select the check box corresponding to a Function or click Select All to select all the available Functions.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Functions**, select the Function Name
2. Click **Authorize** to authorize the Role Functions unmapping.
Click **Reject** to cancel the authorization request.

Available Functions

Click **New Mapping** to view the list of functions that you can map to a role.

To select a function, select the check box corresponding to the function. To select all functions, click **Select All**.

Mapped Functions

Complete the following steps, to map a Role to a Function.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific user is displayed.

Figure 4-13 Mapped Functions



3. Click **New Mapping**.
After you click New Mapping, the list of user Functions you can map the Role to appears in the **Available Functions** page.
4. Select the check box corresponding to a Function or click Select All to select all the available Functions.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Functions, select the Function Name.
2. Click **Authorize** to authorize the Role Function mapping.
Click **Reject** to cancel the authorization request.

Unmapped Functions

To unmap a Role from a Function, complete the following steps.

1. Select the Role name in the **Roles Summary** page.

2. Select **Mapped Functions**.
The list of Functions mapped to the specific Role is displayed.
3. Select the check box corresponding to a Function or click Select All to select all the available Functions.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Functions**, select the Function Name
2. Click **Authorize** to authorize the Role Functions unmapping.
Click **Reject** to cancel the authorization request.

Folders Summary Page

You can create multiple Folders, store objects and assign access rights based on the security level of the user.

The Folders Summary page shows the list of available groups. You can view the details of a group and map the group to one or more user Roles.

To access Folders Summary page, complete the following steps:

- Click **Identity Management** tab in the **Admin Console** page.
- Click the **Folders** tile, to access the Folders Summary page.
The **Folders Summary** page is displayed.

Figure 4-14 Folders Summary Page



Select a specific Folder Name in the Folders Summary page and then click Details to view the associated Folder ID, Folder Name and Folder Type. For more information refer to [Folder Details](#).

To search for a specific user group, type the first few letters of the user group name that you want to search in the search box and click Search. The search results display the names that consist of your search string in the list of available users.

At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

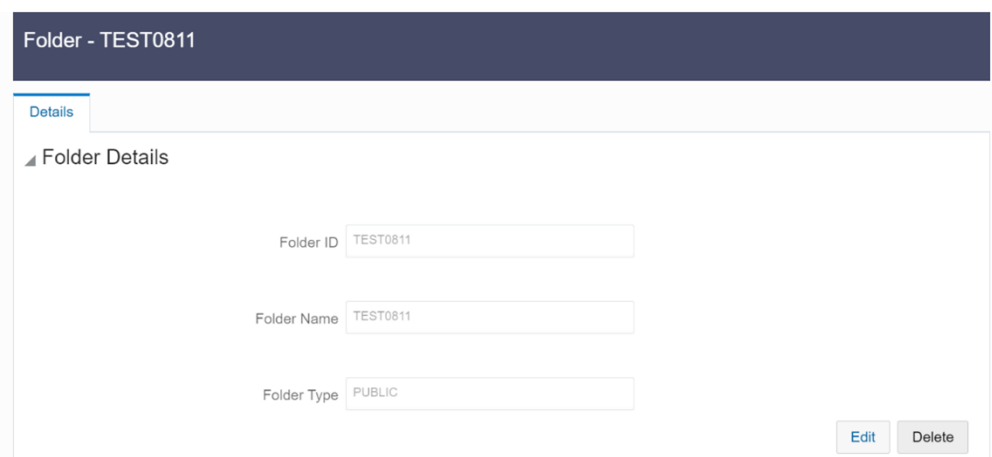
- Use the First page  button to view the entries in the first page.
- Use the Previous page  button to view the entries in the previous page.
- Use the Next page  button to view the entries in the next page.
- Use the Last page  button to view the entries in the last page.

You can also navigate to the desired page. To do this, enter the page number in the View bar control and press Enter.

Folder Details

Select the Folder name in the Folders Summary page and then select Details to view the Folder ID, Folder Name, and Folder Type of the selected Folder.

Figure 4-15 Folder Details



Folder - TEST0811

Details

Folder Details

Folder ID: TEST0811

Folder Name: TEST0811

Folder Type: PUBLIC

Edit Delete

Editing Folder Details

You can edit the Folder Type from the folder details page.

1. Click **Edit** button on the **Folder Details** page.
2. Set the Folder Type to one of the following options:
 - **Public** - These folders are accessible to all users.
 - **Private** - These Folders can be viewed only by the users associated with that folder.
 - **Shared** - These folders can be accessed by those users mapped to specific User groups. These User groups are mapped to specific roles that are associated with the folder.

Folder Details

Select the Folder name in the Folders Summary page and then select Details to view the Folder ID, Folder Name, and Folder Type of the selected Folder.

Figure 4-16 Folder Details

Folder - TEST0811

Details

Folder Details

Folder ID: TEST0811

Folder Name: TEST0811

Folder Type: PUBLIC

Edit Delete

Editing Folder Details

You can edit the Folder Type from the folder details page.

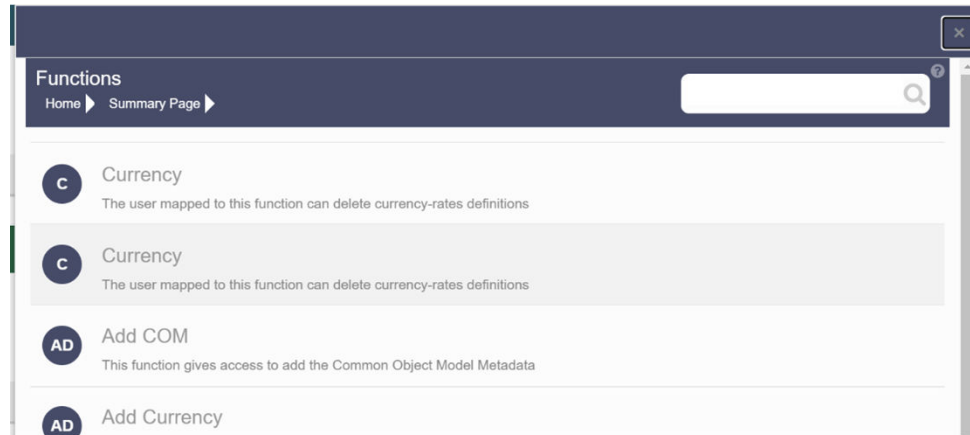
1. Click **Edit** on the **Folder Details** page.
2. Set the Folder Type to one of the following options:
 - **Public** - These folders are accessible to all users.
 - **Private** - These folders can be viewed only by the users associated with that folder.
 - **Shared** - These folders can be accessed by users mapped to specific user groups. These user groups are mapped to specific roles that are associated with the folder.

Functions Summary Page

The Functions Summary page shows the list of available functions. You can view the Function details.

To access Functions Summary page, complete the following steps:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Functions** tile. The **Functions Summary** page is displayed.

Figure 4-17 Functions Summary page

3. Select a specific Folder Name in the Functions Summary page and then click Details to view the associated Function ID, Function Name and Function Description. For more information refer to [Function Details](#).

To search for a specific function, type the first few letters of the function name that you want to search in the search box and click Search. The search results display the names that consist of your search string in the list of available users.

At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

- Use the First page  button to view the entries in the first page.
- Use the Previous page  button to view the entries in the previous page.
- Use the Next page  button to view the entries in the next page.
- Use the Last page  button to view the entries in the last page.

You can also navigate to the desired page. To do this, enter the page number in the View bar control and press **Enter**.

Function Details

Select a function name in the Functions Summary page and then select Details to view the Function ID, Function Name, and Function Description of the selected function.

Figure 4-18 Function Details

Function - Currency

Details

Function Details

Function ID CRRLSL

Function Name Currency

Function Description The user mapped to this function can delete currency-rates definitions

Function Details

Select the function name in the Functions Summary page and then select Details to view the Function ID, Function Name, and Function Description of the selected function.

Figure 4-19 Function Details

Function - Currency

Details

Function Details

Function ID CRRLSL

Function Name Currency

Function Description The user mapped to this function can delete currency-rates definitions

Mapped and Unmapped Functions

If you are an administrator, you can map and unmap a User Role to a Function, from the Roles Summary page.

Mapped Functions

Complete the following steps, to map a Role to a Function.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific user is displayed.

Figure 4-20 Mapped Functions

3. Click **New Mapping**.
After you click New Mapping, the list of user Functions you can map the Role to appears in the **Available Functions** [page](#).
4. Select the check box corresponding to a Function or click Select All to select all the available Functions.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Functions, select the Function Name.
2. Click **Authorize** to authorize the Role Function mapping.
Click **Reject** to cancel the authorization request.

Unmapped Functions

To unmap a Role from a Function, complete the following steps.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific Role is displayed.
3. Select the check box corresponding to a Function or click Select All to select all the available Functions.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Functions**, select the Function Name
2. Click **Authorize** to authorize the Role Functions unmapping.
Click **Reject** to cancel the authorization request.

Available Functions

Click **New Mapping** to view the list of functions that you can map to a role.

To select a function, select the check box corresponding to the function. To select all functions, click **Select All**.

Mapped Functions

Complete the following steps, to map a Role to a Function.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific user is displayed.

Figure 4-21 Mapped Functions



3. Click **New Mapping**.
After you click New Mapping, the list of user Functions you can map the Role to appears in the **Available Functions** page.
4. Select the check box corresponding to a Function or click Select All to select all the available Functions.
5. Click **Map**.
A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In Mapped Functions, select the Function Name.
2. Click **Authorize** to authorize the Role Function mapping.
Click **Reject** to cancel the authorization request.

Unmapped Functions

To unmap a Role from a Function, complete the following steps.

1. Select the Role name in the **Roles Summary** page.
2. Select **Mapped Functions**.
The list of Functions mapped to the specific Role is displayed.
3. Select the check box corresponding to a Function or click Select All to select all the available Functions.
4. Click **Unmap**.
A confirmation message is displayed after successful unmapping. The mapping will be completed after authorization.

If you are an authorizer and want to authorize a mapping, follow these steps:

1. In **Mapped Functions**, select the Function Name

2. Click **Authorize** to authorize the Role Functions unmapping.
Click **Reject** to cancel the authorization request.