Oracle® Financial Crime and Compliance Management Cloud Services

Admin Console User Guide

Release 23.05.01
F81703-01
May 2023

Oracle Financial Crime and Compliance Management Cloud Services Admin Console User Guide, Release 23.05.01

F81703-01

Contents

4 Identity Management

5 Authentication

6 Export API

7 Download API

1
Get Help

Topics:

- Share Your Feedback
- #unique_13

Related Topics

- Get Help in the Applications
  Use help icons to access help in the application.
- Learn About Accessibility
- Get Support
- Get Training
- Join Our Community
- Share Your Feedback
  We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we would like to hear from you.
- Before You Begin
  See the following Document:

Get Help in the Applications

Use help icons to access help in the application.

Note that not all pages have help icons. You can also access the Oracle Help Center to find guides and videos.

Additional Resources

- Community: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.
- Training: Take courses on Oracle Cloud from Oracle University.

Learn About Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program. Videos included in this guide are provided as a media alternative for text-based topics, and are also available in this guide.

Get Support

You can get support at My Oracle Support.

For accessibility support, visit Oracle Accessibility Learning and Support.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at Oracle University.

Join Our Community

Use Cloud Customer Connect to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we would like to hear from you.

You can email your feedback to My Oracle Support.

Thanks for helping us improve our user assistance!

Before You Begin

See the following Document:

- See What's New

2 Introduction to Admin Console

Use the Admin Console to perform System Configuration and Identity Management. It is a 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 Profitability and Balance Sheet Management Cloud Service (PBSMCS).

To access the Admin Console, the PBSM Cloud Administrator must have granted you administrative privileges by mapping your user account to the Identity Administrator and Identity Authorizer user groups. These user groups are seeded in Oracle Identity Cloud Service (IDCS).

When you access the Admin Console, you see the System Configuration and Identity Management tabs. Use these tabs to perform the following tasks:

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

Using System Configuration, Administrators can view how many units of a service have been consumed. 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 it
- 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 the details of the user's login and logout details, the action they performed, the status of the action, and the date and time when the action was performed.
- **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 or users 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 PBSM Cloud Service.

Component Details

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

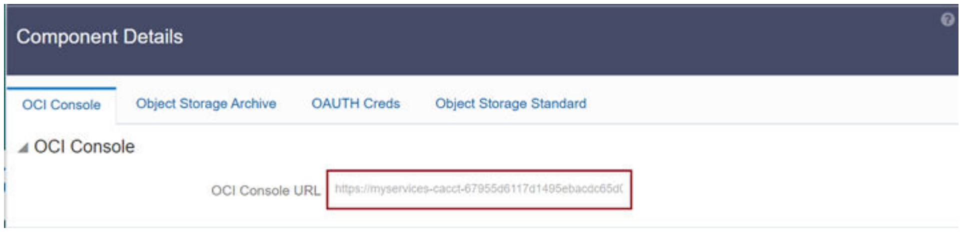
To access Component Details Window

1. Login to PBSM 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



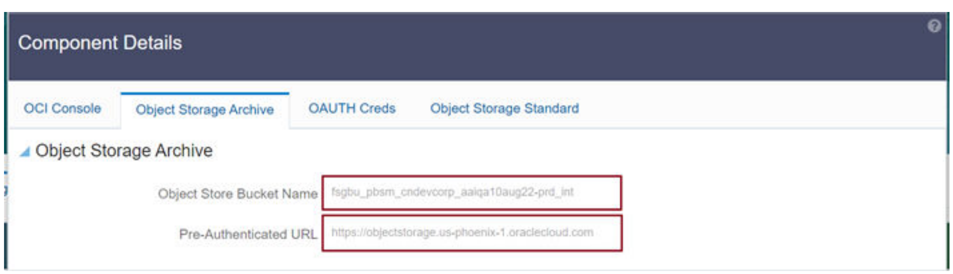
Object Storage Archive

When you provision an instance of the application, two buckets, a standard storage bucket and an archive storage 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

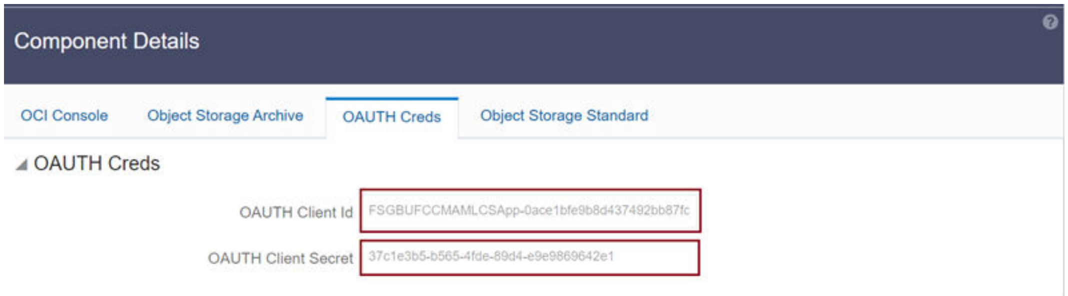


Table 3-1 Field Description

Field	Description
OAUTH Client ID	ID of the OAuth client used for OAuth authentication 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

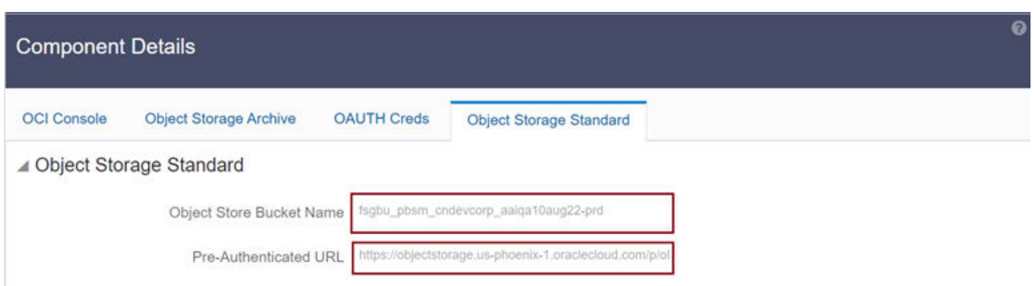


Table 3-2 Field Description

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.

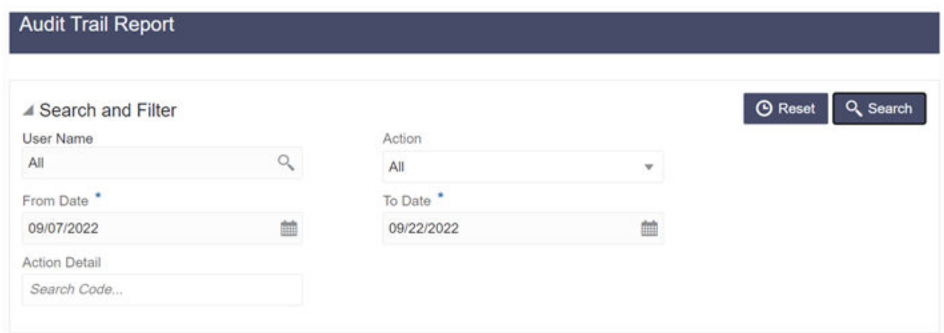
Audit Trail Report

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 PBSM 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



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

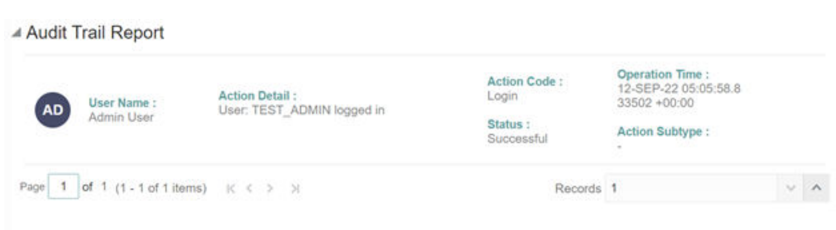


Table 3-4 Audit Trail Report Details

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:

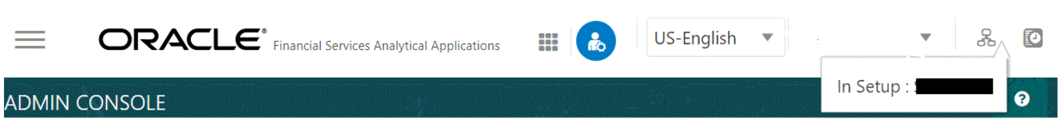
Configurations

Use the Configurations page to specify the values for the instance name and Email ID of the operations user.

To provide the values, follow these steps:

1. Enter the instance name in the Configurations page. For example, UAT, SIT, or PROD. You can provide alphanumeric characters and special characters such as hyphen (-) or underscore (_). The name you specify in this field is displayed when you click In Setup as shown in the following image:

Figure 3-7 Displayed Instance Name



This allows you to know the instance or setup you are working on at the moment, when you have multiple UI windows open simultaneously from different setups.

2. Enter one or more operations user's Email IDs in the Operations User Email-ID field of the Configurations window. The operations user receives Emails about any operations tasks such as batch or task failure. You can enter multiple email IDs separated by a comma (as comma-separated values).

3. Click **Save** after the changes.

Reports For Download

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

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.

Data View Summary

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

To access the Data View Summary:

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

   The list of seeded reports in displayed, with the following details.

   - **Name** - The unique name of the report.
     Click the report name to view the report details.
   - **Description** - The detailed description about the report.
   - **Created By** - Displays the User ID of the user who created the report.
     Click **More Options** (three dots), to view the following details related to report creation and modification.
     – **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.

   Use one of the following options, to filter and view a specific report.

   - Enter the specific search terms in the Name, Description, or Created By fields, or use a combination of the fields, and click **Search**. The reports matching the search criteria are displayed.
   - 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.
2. Click the report name, to view the report details.
3. Click **More Options** (three dots) next to the Report name, to perform the following tasks:
   - Click **Export** from the drop-down list, to export a report. For more information, refer to, Exporting a Report.
   - Click **Download Reports** from the drop-down list, to download a report in the CSV format. For more information, refer to, Downloading a Report.

Viewing Reports

You can view all the attributes included in the report, in the Report Details page.

To access the details of a specific report,

- Click on a report in the **Data View Summary** page to view the report details.

  The Report Details page with the following information is displayed.

  - **Code**: - The unique identifier associated with the selected report. This code is used by the Export API as the **ReportNm** input parameter. For more information about the Report name (**ReportNm**) parameter, refer to
    - End Point Details for Export API
    - End Point Details for Status API
  - **Name**:The report name.
  - **Description**:The description of the report.
  - **Attributes Tab**: The the list of columns/Attributes present in the selected Data View. You can edit the attributes list required for a specific report. For more information about editing attributes/columns refer to Editing Report Attributes/Columns.
  - **Data Preview Tab** - The Data preview of the report with the selected columns is generated and displayed. You can view up-to 50 records in the Data preview page. For more information, refer to Data Preview.

Editing Report Attributes/Columns

You can view the list of columns/Attributes present in the selected Data View, in the Attributes tab.

Refer to the following procedure, to select/deselect the coulmns, to be included in the report. By default, all the columns are selected.

1. Click the View, to expand the view and see the list of attributes.
2. Select /deselect the attributes/columns to be included in the report. By default, all the attributes are selected.

   To filter the columns based on specific criteria, click Filter. Enter the required expression to filter the attributes. For more information, refer to Creating Attribute Filters for Reports.

   At any point, you can click **Reset**, to clear the attribute filters.
3. After adding/removing the required columns and applying the filter, click **Apply** to save the changes.

   The report is included in the Data preview tab.
4. Go to **Data Preview** Tab, to view the report.

Creating Attribute Filters for Reports

Filters allow you to include a specific set of data in the report, using the defined expressions.

You can define a filter expression, for a specific column/columns, during report generation. To create a filter condition,

1. Click **Filter** in the **Report Details** page.

   The Filter Condition to include the required filters is displayed.

2. In the filter Condition page, enter the following details:
   - **Select Column** - Select a column from the drop-down list, for which you want to set a filter condition.
     To search for a specific column name, type a few letters from the column name in the Select Column text box and press Enter.
   - **Conditions** – Select one of the following comparison operators, to filter the data for the selected column.
     – **Comparison** - '=', '!=', '< >', '>', '<', >=, <=,'IN', 'NOT IN', 'ANY', 'BETWEEN', 'LIKE', 'IS NULL', and 'IS NOT NULL'.
   - **Value** - Enter the condition value to filter the data and generate the report. For Date column, select the Date using the calendar.

3. After entering the required filter condition, click **Add** to add the filter condition.

   The filter condition is added to the **Expressions Built** pane.

4. Repeat Step 2 and 3 to enter multiple filter conditions, for various columns.

5. Click **Validate** to verify if the selected filter condition is valid.

6. After entering the required filter conditions, click **Apply**, to add the filter condition to the report.

   The filter conditions are included in the **Attributes** tab.

   At any point of time, after validating/applying the filters you can modify or delete the filter conditions using one of the following tasks:
   - Click **Update Filter Changes**, to update a filter expression.
   - Click **Reset**, to clear all the validated filters and add new filter conditions.
   - Click **Delete** to delete a filter condition.

Data Preview

You can access the preview of the report generated based on the attributes/columns and the filters selected in the **Attributes** tab.

You can view upto 50 records in the **Data preview** page.

After verifying the details in the preview, you can export the report to CSV format and download the report to your local directory.

Related Topics

- Exporting a Report
  You can export the report to .CSV file , from the **Data Preview** tab.
- Downloading a Report
  You can download an exported report, from the Data Preview tab or the Report summary page.

Exporting a Report

You can export the report to .CSV file , from the **Data Preview** tab.

You can export the report from the Data Preview tab or the Report Summary page.

- After validating the information in the preview,
  - To export the report form Data Preview tab, click **Export CSV**.
  - To export the report from the Report Summary page, click **More Options** (3 dots) and select **Export**.

  A confirmation message is displayed after successful export.

  After exporting the report, go to Download Reports, to download the report in .CSV format.

Downloading a Report

You can download an exported report, from the Data Preview tab or the Report summary page.

All the reports exported to CSV format are listed in the **Report Available for Download** page.

The report must be exported and the status is set to **Completed**, for downloading the report.

To download a report,

- Click **Download Reports** from the Data Preview page, to view the list of **Reports Available for Download**.

  All the reports available for download are displayed with the following details:
  - **Filename** - The report filename.
  - **Status** - The export status of the report.
    - **Pending** - denotes that the report export is yet to start and is in the queue.
    - **Running** - denotes that the report export is in progress.
    - **Completed** - denotes that the CSV file is exported and the report is ready for download.
  - **Download** - Click to download the report to the local directory. Select the local directory to download the report and enter a valid filename and click **Save**.
  - **Download Link** - Click to copy the download link. You can paste the link in a browser, to download the report.
  - **Delete** - Delete the report, after confirmation.

  You n download the report from the Report Summary page. Click **More Options** (three dots) next to the report name and click **Download Reports,** to download a selected report.

4

Identity Management

Using Identity Management, Administrators can manage fine-grained and coarse-grained entitlements that consist of fewer functions than fine-grained entitlements) entitlements. Authorizers can authorize the entitlement mappings. The components are as follows:

- **Users**: A user is a person who has access to 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 page. Click **Users** to view the list of available users in the Users Summary page.
- **Groups**: Groups are a set of users that 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. Click **Add** to add a user group or click **Groups** to view the list of user groups in the Groups Summary page.
- **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 the role. Click **Add** to add a role or click **Roles** to view the list of roles in the Roles Summary page.
- **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 the Folders Summary page.
- **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 the Functions Summary page.

> **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:

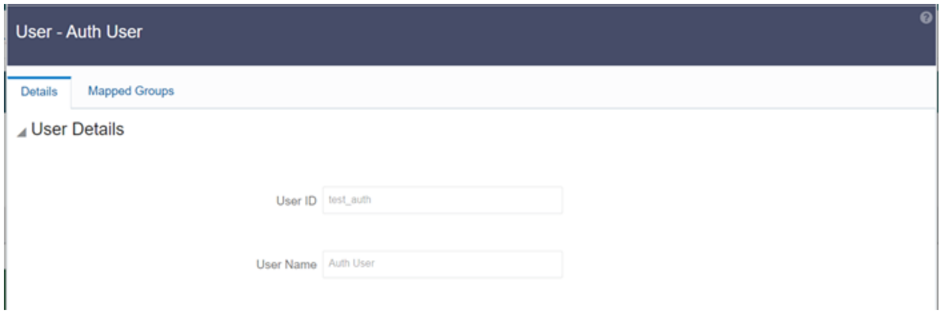
- Use the First page button to view the entries in the first page.
- Use the Previous page button to view the entries in the previous page.
- Use the Next page button to view the entries in the next page.
- Use the Last page button to view the entries in the last page.

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



Mapped and Unmapped Groups

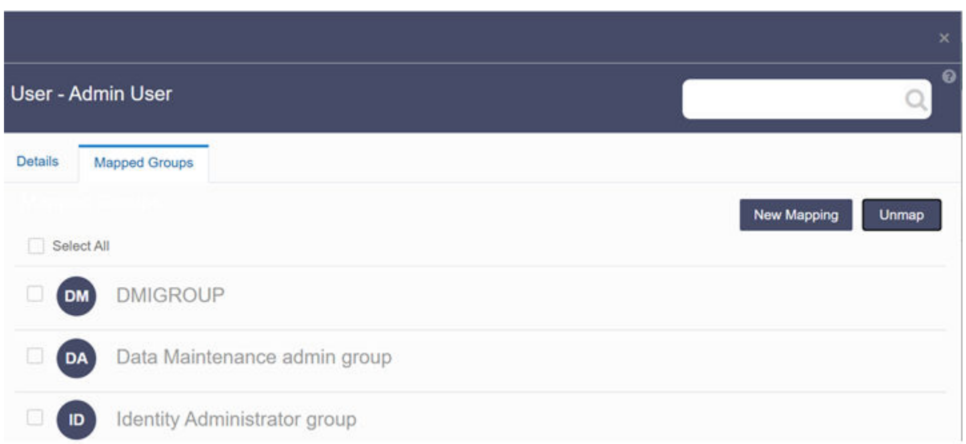
If you are an Administrator, you can map and unmap a user to a User group, from the **Users Summary** page.

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

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.

Related Topics

- Available Groups
  Click New Mapping to view the list of user groups you can map to the user.

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**.

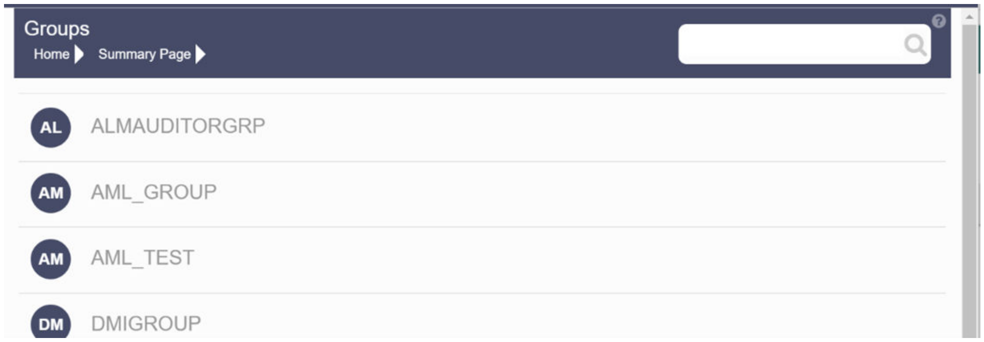
Groups Summary Page

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 Groups Summary page, complete the following steps:

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

Figure 4-4 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:

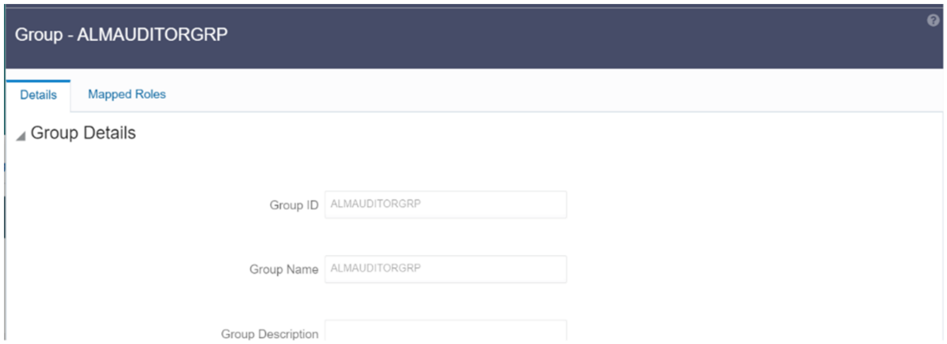
- Use the First page button to view the entries in the first page.
- Use the Previous page button to view the entries in the previous page.
- Use the Next page button to view the entries in the next page.
- Use the Last page button to view the entries in the last page.

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 4-5 Group Details Page



Mapped and Unmapped Roles

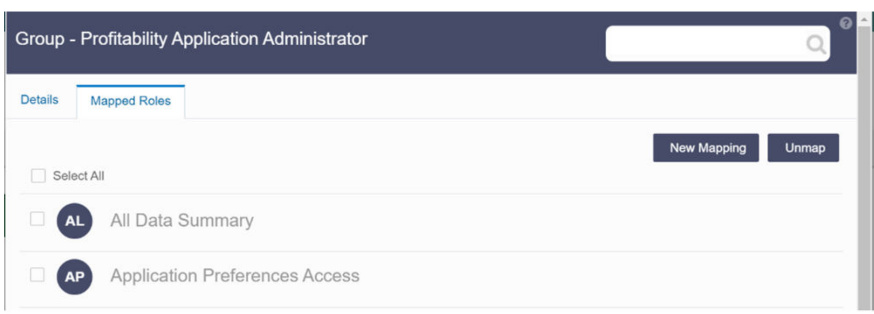
If you are an administrator, you can map and unmap a Group to a User Role, from the Groups Summary page.

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 4-6 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.

Related Topics

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

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:

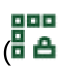
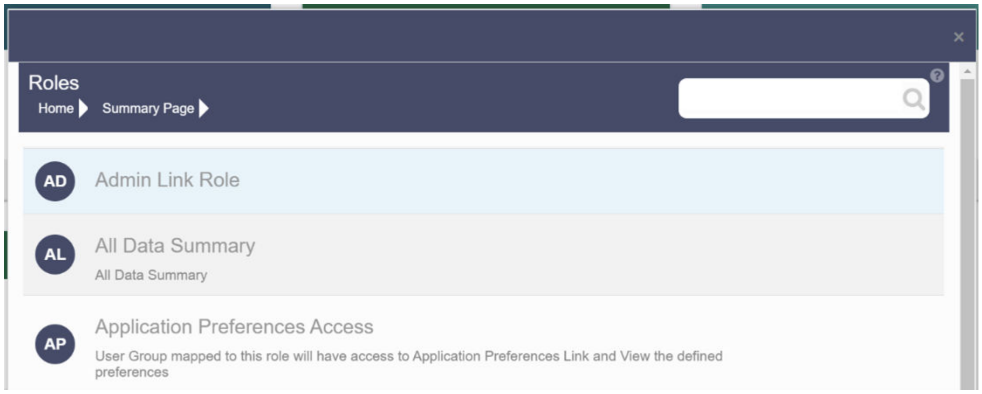
1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Roles** tile ().
   The **Roles Summary** page is displayed.

Figure 4-7 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 Roles 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.

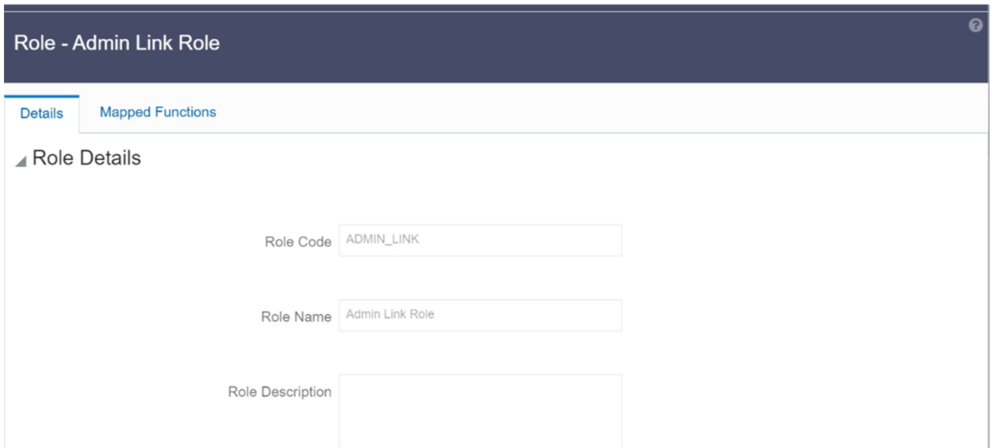
At the bottom of the page, you can enter the number of entries that are available on a single page in the Records box. You can increase or decrease the number of entries that are displayed using the up and down arrows. To navigate between pages in the View bar, use the following buttons:

- 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 4-8 Roles Details Page



Mapped and Unmapped Functions

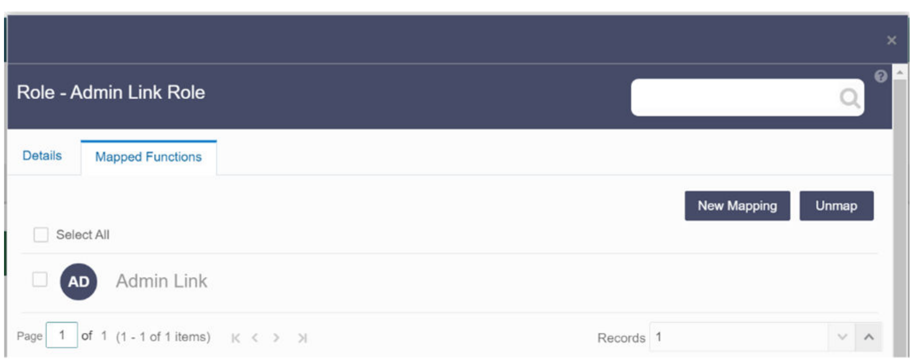
If you are an administrator, you can map and unmap a User Role to a Function, from the Roles Summary page.

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 4-9 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.

Related Topics

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

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**.

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 ().
  The **Folders Summary** page is displayed.

Figure 4-10   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:

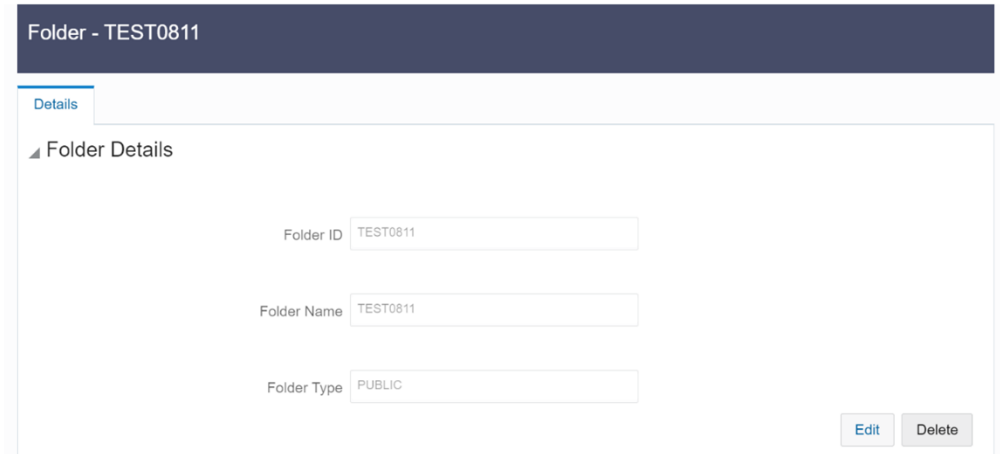
- Use the First page button to view the entries in the first page.
- Use the Previous page button to view the entries in the previous page.
- Use the Next page button to view the entries in the next page.
- Use the Last page button to view the entries in the last page.

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 pageand then select Details to view the Folder ID, Folder Name, and Folder Type of the selected Folder.

Figure 4-11 Folder Details



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.

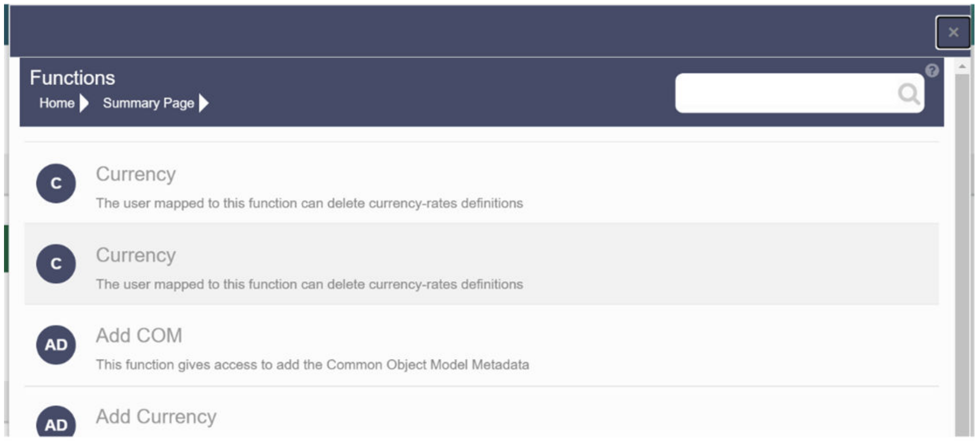
Functions Summary Page

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 4-12 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 Functions 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:

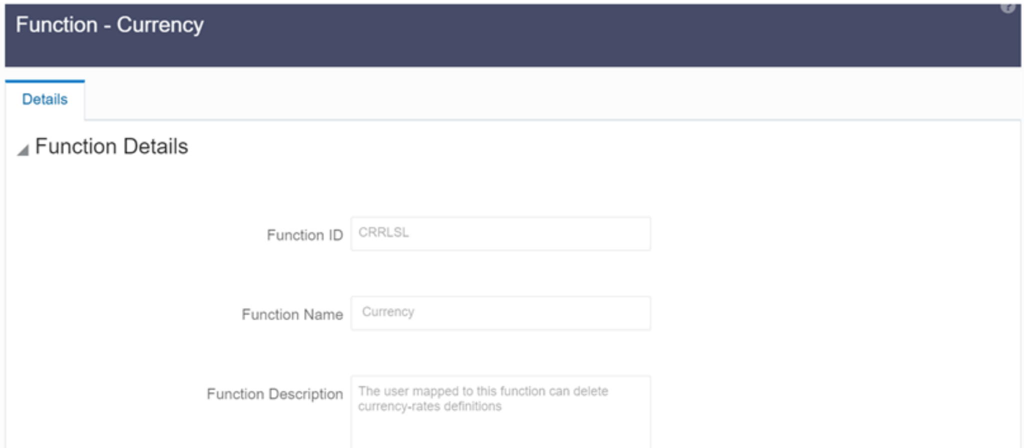
- Use the First page button to view the entries in the first page.
- Use the Previous page button to view the entries in the previous page.
- Use the Next page button to view the entries in the next page.
- Use the Last page button to view the entries in the last page.

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 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 4-13 Function Details



Mapped and Unmapped Functions

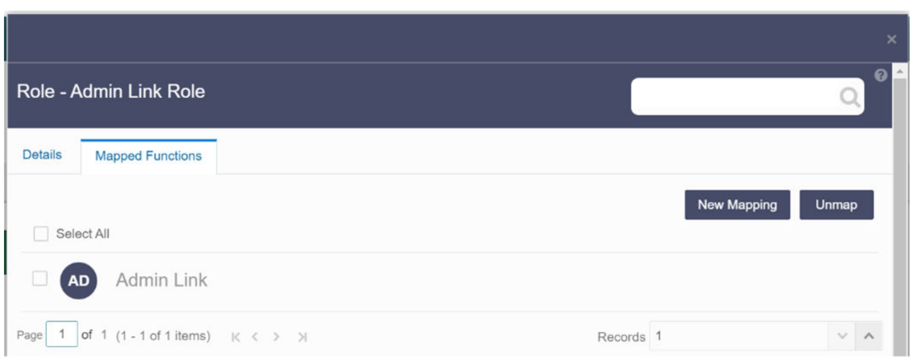
If you are an administrator, you can map and unmap a User Role to a Function, from the Roles Summary page.

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 4-14 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.

Related Topics

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

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.

5
Authentication

The Authentication Process involves the use of cURL Commands in a CLI Tool to generate the access token and invoke REST APIs. The Authentication Token is generated through the OAuth Client ID and Secret Credentials created in IAM/IDCS during Provisioning. The Authentication Token does not require that you log in to the FCCM Application to invoke the REST APIs from external applications.

Ensure that you have the appropriate log-in credentials to access the respective Cloud Service and the appropriate roles to perform specific operations using the API Resources. The user should be mapped to **Data Maintenance admin group** with **FILE_ADV Role**.

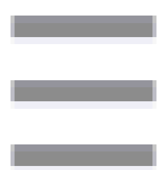
The following is the list of steps for Authentication and further subsections provide the details:

1. Get the OAuth Client ID and Client Secret
2. Generate the Access Token

Get the OAuth Client ID and Client Secret

To get the OAuth Client ID and Client Secret, follow these steps:

1. Enter the IDCS URL in the Browser's URL Address Bar.

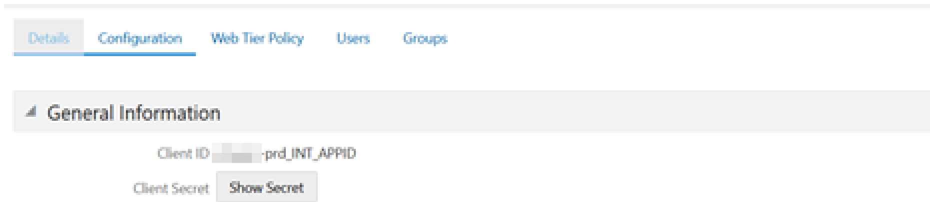
   The **Oracle Cloud Account Sign In** Window appears.
2. Log in to **Oracle Identity Cloud Service** (IDCS).
3. Select the Navigation  Icon to view a list of available functions.
4. Select **Oracle Cloud Services**.

   For more information, see Access Service Consoles from **Administering Oracle Identity Cloud Service**.
5. From the Oracle Cloud Services Window, select the required FCCM Internal Application Service (in **AMLCS <tenant-id>** Format) from the list.

   > **Note:**
   >
   > If you are retrieving ERP ESS Job Details API, select the required AMLCS Application Service (in **AMLCS <tenant-id>** Format) from the list. Ensure you use the same **AMLCS <tenant-id>** while generating the Access Token.
6. Click the **Configuration** Tab.

The Client ID and Client Secret Details are displayed in the General Information Section.

Figure 5-1 Client ID and Client Secret



7. Copy the **Client ID** and **Client Secret**.
8. Open a CLI Tool.
9. Generate the Access Token.

Generate the Access Token

To generate the Access Token, add the Client ID, Client Secret, User Name, and Password using cURL Commands in the CLI Tool. The following is an example:

```
First generates basic base64 encoded authorization token using below
command
echo -n
"<tenant_oauth_app_client_id>:<tenant_oauth_app_client_secret>" |
base64 -w 0

Use the output of above to generate bearer token
curl -H "Authorization: Basic <base64 encoded
tenant_oauth_app_client_id:tenant_oauth_app_client_secret>" -H
"Content-Type:
application/x-www-form-urlencoded;charset=UTF-8" --request POST
https://<idcs-
URL.identity>.<TENANT>.com/oauth2/v1/token
 -d "grant_type=client_credentials&scope=urn:opc:idm:__myscopes__"
```

After generating the Access Token, invoke the API as shown in the following section.

6 Export API

Export API are utilized to submit request to export a report to CSV format. You can submit upto 5 requests in parallel with an interval of 2 minutes.

End Point Details

- **Method** – POST
- **REST Endpoint -** /aai-dmi-service/vw/v1/repgen

Table 6-1 Request Headers Details

Header Name	Description	Example
Content-Type	The media type of the body of the request. Required for POST and PUT requests, and the supported types vary with each endpoint.	Application/Json
srvc_id	The unique service ID associated with the report. • **Data Type**: String • **Mandatory**: Yes	OFS_COMM
appId	Respective application ID of the cloud service • **Data Type**: String • **Mandatory**: Yes	OFS_AMLCS
reportNm	The auto-generated code for the specific report. You can get this code from the Report Details page. For more information refer to Viewing Reports. • **Data Type**: String • **Mandatory**: Yes	OFS_AMLCS_1d312c
reportType	The report file format. • **Data Type**: String • **Mandatory**: Yes	CSV
reportDefType	The report definition type. • **Data Type**: String • **Mandatory**: Yes	V - the report is based on a database view.

Table 6-1 (Cont.) Request Headers Details

Header Name	Description	Example
ofs_remote_user	The login name of the user exporting the report. The OFS remote user should be authenticated and a token must be generated for the user credentials. For more information, refer to Authentication. • **Data Type**: String • **Mandatory**: Yes	

Request JSON Parameters

Table 6-2 Request JSON Parameters

Key Field	Value
filterCriteria	The filter conditions set to include a specific set of data in the report, using the defined expressions. You can add the filter criteria in the Filter Conditions page. For more information, refer to Creating Attribute Filters for Reports

Request JSON Sample when there is no filter

```
{ "filterCriteria": ""}
```

Request JSON Sample when filter applied

```
{ "filterCriteria": "FCC_CANNED_STG_CASA.V_ACCOUNT_NUMBER
<'10'FCC_CANNED_STG_CASA.V_ACCT_DISPLAY_NAME = 'Stuart Ferguson'"}
```

Response JSON Parameters

This section provides the list of parameters in the JSON Response.

Response JSON Sample when records are less than 5000

The report is generated and included in the response. Copy the response to a text editor and save it as a CSV file.

Sample Response

```
"D_ACCT_CLOSED_DATE,D_ACCT_OPEN_DATE,D_ACCT_STATUS_DATE,D_ACTUAL_RENEWA
L_DATE,D_ADJUSMENT_EFFECTIVE_DATE,D_ATM_ISSUED_DATE,D_BILLING_CYCLE_DAT
E,D_CR_LINE_INC_LAST_REJECT_DATE,….Stuart
Ferguson,,,,A,,,,,,,,,,,,,,,,,,GEN,,,,,,,,,,,,,,,,,,,CU-101833842885,C
R,AMEA,MAN,,,,,,,,,,,,,,,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,30120409CU101,,IND,,,,,,,,,,,,,,,,,,,,,Y,,,,,,,,,,,,,,,,,
"
```

Response JSON Sample when records are Greater than 5000

Sample Response

{"requestInstanceId":"reportInstatnceId:40","status":"RUNNING"}

7 Download API

This API helps to generate a pre-authenticated URL (PAR URL), to download the report in CSV format, if the number of records in a report is more than 5000.

The status response can contain the following values:

- **COMPLETED** - When the export API execution is completed successfully and response is generated for
  - Number of records below 5000
  - Number of records above 5000
- **PENDING** - denotes that the report export is yet to start and is in the queue.
- **RUNNING** - When the API execution is in progress.
- **FAILED** - When the Export API execution is not completed successfully.

End Point Details

- **Method** – POST
- **REST Endpoint** - /aai-dmi-service/vw/v1/repgenstatus

Table 7-1 Request JSON Parameters

Header Name	Description	Example
Content-Type	The media type of the body of the request. Required for POST and PUT requests, and the supported types vary with each endpoint.	Application/Json
srvc_id	The unique service ID associated with the report. • **Data Type**: String • **Mandatory**: Yes	OFS_COMM
appId	Respective application ID of the cloud service • **Data Type**: String • **Mandatory**: Yes	OFS_AMLCS
reportNm	The auto-generated code for the specific report. You can get this code from the Report Details page. For more information refer to Viewing Reports. • **Data Type**: String • **Mandatory**: Yes	OFS_AMLCS_1d312c
reportType	The report file format. • **Data Type**: String • **Mandatory**: Yes	CSV

Table 7-1 (Cont.) Request JSON Parameters

Header Name	Description	Example
reportDefType	The report definition type. • **Data Type**: String • **Mandatory**: Yes	V - the report is based on a database view.
ofs_remote_user	The login name of the user exporting the report. The OFS remote user should be authenticated and a token must be generated for the user credentials. For more information, refer to Authentication. • **Data Type**: String • **Mandatory**: Yes	
reportInstanceID	The instance ID of the report which is being exported. You can get the report instance ID from Response JSON Parameters • **Data Type**: Integer • **Mandatory**: Yes	40

Response JSON Parameters

This section provides the list of parameters in the JSON Response.

Table 7-2 POST JSON Response

Name	Type	Description
`requestInstanceId`	STRING	Request Instance ID of the export process
`downloadlink`		Click the link to download the document
`status`	STRING	Status of the export

Sample Response

- The following sample response is generated, when the Download report request is in progress.

```
{   "requestInstanceId":"161","status":"RUNNING"}
```

- The following sample response is generated , when the download request is processed and the PAR URL to download the report is included in the response. You can copy the PAR URL and paste it in a Web browser, to download the report in CSV format.

```
"requestInstanceId":"183","downloadLink":
"https://objectstorage.us-phoenix-1.oraclecloud.com/p/V9CMuA-
pFmoZ6xs_JzB1N4SaLWWCmsp38kAH-IOCeIuz-zdxP8Px6SW7Y_zon9yb/n/
oraclegbudevcorp/b/fsgbu_aml_cndevcorp_kdlyds-prd_default/o/default/2023-05-23/vnc/
```

4eac548e-65e8-4baf-a1bf-5e3ab9c7455e?httpResponseContentDisposition=ATTACHMENT%3B%20filename%3DCR_2023-05-231684845302475.csv","status":"COMPLETE"

- The following sample response is generated , when the download request is in pending status.

```
"{"requestInstanceId":"161","status":"PENDING"}
```