Oracle® Financial Crime and Compliance Management Cloud Services

Admin Console User Guide

Release 26.02.01
G51792-06
June 2026

ORACLE

Oracle Financial Crime and Compliance Management Cloud Services Admin Console User Guide, Release 26.02.01

G51792-06

Copyright © 2022, 2026, Oracle and/or its affiliates.

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 Introduction to Admin Console

Accessing Admin Console 1
Setting User Preferences 2
About Notification Services 2

2 System Configuration

Metering 1
Component Details 2
Audit Trail Report 3
Configurations 4
Reports For Download 5
- Data View Summary 5
- Viewing Reports 6
- Editing Report Attributes/Columns 6
  - Creating Attribute Filters for Reports 7
- Data Preview 8
- Exporting Reports 8
- Downloading a Report 8
- Data Maintenance Interface 9

3 Allowing Domains to Receive Email Notifications

4 Identity Management

Users Summary Page 2
- User Details 2
- Mapped/Unmapped Groups 2
- Available Groups 3

Groups Summary Page 3
- Group Details 4
- Mapped/Unmapped Roles 4
- Available Roles 4

Copyright © 2022, 2026, Oracle and/or its affiliates.

Roles Summary Page 5
Creating a New Role 5
Roles Details 6
Mapped/Unmapped Functions 6
Available Functions 6
Functions Summary Page 7
Function Details 7
Folders Summary Page 7
Folder Details 8
Editing Folder Details 8

Copyright © 2022, 2026, Oracle and/or its affiliates.

1

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.

Accessing Admin Console

Access Admin Console from the home page of Financial Services Analytical Applications.

To access the Admin Console, ensure that the cloud administrator grants 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 and Access Managment (IAM).

Before logging into the Admin Console, ensure that:

> **Note**
>
> - The Cloud Administrator who creates your account has granted you administrative privileges to access the Admin Console. For more information on the privileges available, see OFS AML Users and User Privileges.
> - If the Cloud Administrator has granted only Identity Management privileges and no other cloud application privilege, you will be automatically redirected to the Admin Console specific to subscribed cloud service, after a successful login.
> - After a user signs in to the Cloud Service, the user to user-group Mapping created in the IAM Console will onboard into the Master and Mapping Tables. If you unmap a user from a group in the Admin Console, go to the IAM Console and open the **Assign User to Groups**. Unselect the user corresponding to the user group and click **Finish**. This step is mandatory to unmap the user.

To access the Admin Console:

1. Enter the application URL in the browser's address bar to access the Oracle Cloud Account Sign In page.
2. Enter the username and password on the Login page to log in to the **Financial Services Analytical Applications**.

   After successfully logging in, you can view the **Financial Services Analytical Applications** homepage and the list of subscribed cloud applications. Click **Navigation** to hide the Applications Navigation List.
3. Click **Admin Console** at the top of the Financial Services Analytical Applications home page.

   In the Admin Console, you can view the **System Configuration** and **Identity Management** tabs. Use these tabs to perform the following tasks:

   - **Administrator Tasks**:

Copyright © 2022, 2026, Oracle and/or its affiliates.

  - 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**:
  - Authorize the Identity and Access Management Operations in the **Identity Management** tab.

Setting User Preferences

Using the user preferences, you can set the landing page, time zone, locale and the displayed date format.

You can access the **User Preferences** from your **Financial Services Analytical Applications** page.

To access user preferences:

1. Click **User** (user icon) and click **Preferences**.

   Select the following details.

   - **Start Page** - The landing page that is displayed when the user logs in. You can set the landing page to Admin console, default home page or any specific application page.
   - **Time Zone** - The time zone displayed in the application.

     > **Note**
     >
     > If you modify the time zone from the default value, it will not be reflected in the **Investigation Hub** 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.

     > **Note**
     >
     > If you modify the default date format, it will not be reflected in the **Investigation Hub** application.

2. After entering the preferred values, click **Save** to update the user preferences.

About Notification Services

Notification Services generates a job status alert message, for each activated job.

You can access the **Notification Services** from the Admin Console home page.

To access Notification services and view the messages:

1. To view the message alerts, click **Notification Services** (Bell icon).

   The following details are provided in the notification messages.

Copyright © 2022, 2026, Oracle and/or its affiliates.

- **More info,** - view the complete message. The message background is changed to white, after the message is read.
- **Mark All as Read** - move the messages to Read status without opening the messages.
- **BatchRunID** - view more details about a specific job.

The messages are categorized based on the following priorities:

- **Priority 1** -
- **Priority 2** -
- **Priority 3** -

2. Click **Dismiss** to delete an alert.

   Read messages will be deleted automatically, after 7 days. Log in as Administrator to modify the auto delete duration in the **Admin Console > Notification Configuration**. You can set the duration from 1 - 999. The default duration is 7 days.

Copyright © 2022, 2026, Oracle and/or its affiliates.

2

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

View annual usage of transactions and report types.

Use the **Metering** page to view the annual unit usage of the number of transactions and the number of report types within your cloud service.

The following table shows the methodology employed to measure the usage of each of the products.

Table 2-1 Metering Methodology

Product	Metering Methodology
Transaction Monitoring Cloud Service	Number of transactions per month.
Regulatory Reporting Cloud Service	Number of templates configured of a country or jurisdiction for filing to a regulator.
Know Your Customer (KYC) Cloud Service	Count of KYC Checks created for both KYC Onboarding and KYC Continuous Monitoring in the production environment. Metering excludes the deployment initiation batch (first time risk assessment of all existing customers for a client).
Customer Screening Cloud Service	Sum of customers screened via batch per day and via real time for a duration of one month.

Copyright © 2022, 2026, Oracle and/or its affiliates.

Table 2-1 (Cont.) Metering Methodology

Product	Metering Methodology
Transaction Filtering Cloud Service	Sum of transaction messages screened via real time for a duration of one month.
Compliance Agent Cloud Service	Number of experiments run.
Investigation Hub Cloud Service	Pooled Named User (Defined as an individual authorized by you to access the hosted service, regardless of whether the individual is actively accessing the hosted service at any given time during one calendar month).
iHub Real-time Customer Screening	Pooled Named User (Defined as an individual authorized by you to access the hosted service, regardless of whether the individual is actively accessing the hosted service at any given time during one calendar month).
Studio Cloud Service	Number of Transactions
Monitor Cloud Service	Pooled Named User (Defined as an individual authorized by you to access the hosted service, regardless of whether the individual is actively accessing the hosted service at any given time during one calendar month).
Automated Scenario Calibration Cloud Service	Number of transactions per month
AI Assistant Cloud Service (AIACS)	Number of cases having AI generated narrative
Profitability and Balance Sheet Management Base	Per 100k Records Processed
Cash Flow Engine	Per 100k Records Processed
Funds Transfer Pricing	Per 100k Records Processed
Profitability Management	Per 100k Records Processed
Asset Liability Management	Per 100k Records Processed
Profitability Analytics	Per Hosted Named User

Component Details

Use Component Details to view the object storage standard and archive details, and OAUTH authentication details.

Object storage is used for data to which you require fast, immediate, and frequent access. Archive storage is used for data which you do not access regularly but must be retained and preserved for long periods of time.

With every instance of the application provisioned, two buckets are provisioned: a standard storage bucket and an archive storage bucket. The data files that you want to load into the application for processing must be uploaded to the standard storage bucket. The files are automatically moved to the archive storage bucket after a period of 7 days.

To access Component Details:

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

   You can access the following tabs from the Component Details tab:

   - **OCI Console** : Access the **OCI Console URL** from the **OCI Console** tab.

Copyright © 2022, 2026, Oracle and/or its affiliates.

- **Object Storage Standard** : 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.
  Access and copy the following details related to the objects which are currently in use and require fast, immediate, and frequent access.
  - **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
- **Object Storage Archive** : Archive storage is used for storing objects that are not actively in use but need to be retained and preserved for extended periods. Objects are automatically moved from standard to archive storage after 7 days.
  Access and copy the following details related to the archived objects.
  - **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** : Use OAUTH credentials (Client ID and Client secret) are used for implementing authentication in cloud services.
  Access and copy the following OAUTH credentials:
  - **OAUTH Client ID**: ID of the OAuth client used for OAuth authentication performed by IAM during any API calls.
  - **OAUTH Client Secret**: Password of the OAuth client secret used for OAuth authentication performed by IAM during any API calls

Audit Trail Report

Use the Audit Trail Report to check user activities, including logins, added actions, their status, and associated machine names.

To generate an Audit Trail Report:

1. Log in to the **Admin Console**.
2. Go to **System Configuration** and click **Audit Trail Report** to access the **Audit Trail Report** page.
3. Enter the following values and click **Search** to generate the **Audit Trail Report** for all users or a specific user, to view a specific audit trail report.

Table 2-2 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 list of 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.

You can get the following details from an **Audit Trail Report**.

Copyright © 2022, 2026, Oracle and/or its affiliates.

Table 2-3 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. To download the report, click **Download** and select your preferred file format (PDF or Excel). The report will be saved automatically to your system's default download folder.
5. Click **Reset** to clear all values from the filter fields and enter new search criteria.

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.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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

A set of pre-defined and pre-configured reports that are available for users to download.

To access **Reports for Download** from the **Admin Console**, your user profile must be mapped to the Data Maintenance Admin group and the required admin group with Canned report access enabled. .

The **Reports for Download** in the **System Configuration** tab, contains a set of pre-defined and pre-configured reports 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.

Data View Summary

View the list of reports available for download from the Data view summary.

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.

Copyright © 2022, 2026, Oracle and/or its affiliates.

  - **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 Reports.
   - 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

View the report and all the attributes associated in the report on 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 is displayed with the following information:

  - **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.
  - **Data Preview Tab** - The data preview of the report with the selected columns is generated and displayed. You can view up to 50 records on the **Data Preview** page.

Editing Report Attributes/Columns

View the list of columns/attributes present in the selected Data View in the Attributes tab.

To select/deselect report columns to be included in the report:

1. Click **View** to expand the view and see the list of attributes.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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.

   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 and add the report to the **Data Preview** tab.
4. Go to the **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 defined expressions.

You can define a filter expression for specific column(s) 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. On 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.
   - **Type** - Select one of the following filter types:
     - **Static** - Select **Static** to enter a value and execute the filter using only one value. You cannot change the value at a later point.
     - **Dynamic** - Select **Dynamic** to change the filter value when needed.
       After setting the filter type to **Dynamic**, select the **Placeholder** and set one of the default seeded values to process the filter.

     > **Note**
     >
     > Only values that are already seeded in the database table are displayed in the Placeholder drop-down list.

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 steps 2 and 3 to enter multiple filter conditions for various columns.
5. Click **Validate** to verify if the selected filter condition is valid.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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 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 up to 50 records in the **Data preview** page.

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

Exporting Reports

Export the report to a `.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 a successful export.

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

Downloading a Report

Download an exported report from either 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.

Copyright © 2022, 2026, Oracle and/or its affiliates.

  - **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 can 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.

Data Maintenance Interface

The Data Maintenance Interface (DMI) is a secure, web-based tool in Oracle Financial Crime and Compliance Management (FCCM).

DMI allows authorized users to review and manage business layer data, such as customer profiles and business policy-related data. It simplifies data administration, enforces access controls for compliance, supports dynamic updates without backend changes, and maintains comprehensive audit logs for regulatory and internal reviews.

To access the DMI

1. In your web browser, enter the application URL to open the Oracle Cloud Account Sign In page.
2. On the sign-in page, enter your username and password (you must log in as user group DMIADMIN) to access the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service home page. After you sign in, the **Application**s, **Application Administration**, and **Business Processes** tiles are displayed.
3. From the top-right corner of the home page, click the **Admin Console** icon. In the **Admin Console**, you can view the **System Configuration** and **Identity Management** tabs.
4. Under the **System Configuration** tab, click the **Reports** for download tile. The **Data View** page is displayed.
5. Locate a record with **Type** set to **Data Entry**.
6. From the right side of the record, click **Actions** (three dots) and then click **View** or **Edit** the DMI forms. The **Data Entry** page is displayed.
7. From the top-right corner of the **Data Entry** page, select **Ready** under the **Status** drop-down to view/edit the existing DMI forms.

For more information on the tool, see Data Maintenance Interface.

For more information on FCCM product specific use cases, see DMI Use Cases.

Copyright © 2022, 2026, Oracle and/or its affiliates.

3

Allowing Domains to Receive Email Notifications

The application sends email notifications from the following domain. To receive these notifications, you must add this domain to your Allow List: `no-reply-fsgbu-erfplatform@ps1.erf.<region>.ocs.oraclecloud.com`

Replace `<region>` with the value appropriate for your region. Contact Support for details.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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.

Use the following guidelines to manage user creation and group mappings between IDCS/OCI and the Admin Console.

- Create users only in IDCS/OCI.
- You can map users to groups in IDCS/OCI, in the Admin Console, or in both. The system automatically syncs user-to-group mappings from IDCS/OCI to the Admin Console, but not the other way around.
- To unmap a user from a group, manually remove the mapping in both IDCS/OCI and the Admin Console.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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 the Users Summary page:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Users** tile to access the **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.

   To map/unmap a user group, 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 results will show users matching your input.

   At the bottom of the page, adjust the number of entries displayed per page using the up and down arrows in the Records box. To navigate between pages in the View bar, use these buttons:

   - **First page** to go to the first page.
   - **Previous page** to go back.
   - **Next page** to move to the next page.
   - **Last page** to go to the last page.

   You can directly navigate to a specific page by entering its number in the View bar and pressing **Enter**.

User Details

In the User Details, you'll find the User ID and User Name of the selected user from the User Summary page.

- Click a specific user listed in the **User Summary** page and then click **Details** to view the **User ID** and the **User Name** of that user.

Mapped/Unmapped Groups

As an Administrator, you can map/unmap a user to/from a user group from the **Users Summary** page.

To map/unmap a user to a user group:

1. Select the user name in the **Users Summary** page.
2. Select **Mapped Groups** to access the list of groups mapped to the selected user.
3. To map a user group:
   a. Click **New Mapping**.

      The list of user groups you can map the user to appears in the **Available Groups** page.

Copyright © 2022, 2026, Oracle and/or its affiliates.

b. Click **Map**.

A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.

4. To unmap a user group:
   a. Select the check box corresponding to a user group or click **Select All** to choose all available user groups.
   b. Click **Unmap**.

   A confirmation message will be displayed after successful unmapping. The unmapping will be completed after authorization.
5. After mapping/unmapping a user group, ensure to authorize it accordingly. To authorize a mapping/unmapping:
   a. In **Mapped Groups**, select the user-user group mapping or unmapping that requires authorization.
   b. Click **Authorize/Reject** to approve or cancel the mapping/unmapping request.
6. Click on **New Mapping** and then switch to **Authorization View** to retrieve the pending authorization.

> **Note**
>
> Any other user from the requestor is required to authorize any new mapping requests.

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 the Groups Summary page:

1. Click the **Identity Management** tab in the **Admin Console** page.
2. Click the **Groups** tile, to access the **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.
4. Select a group name and click **Mapped Roles** to view the list of roles that are mapped to the particular group.

   To map/unmap roles, refer to mapped/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 results will show users matching your input.

   At the bottom of the page, adjust the number of entries displayed per page using the up and down arrows in the Records box. Use the navigation buttons, to go to the first page,

Copyright © 2022, 2026, Oracle and/or its affiliates.

last page, previous page and next page. You can also directly navigate to a specific page by entering its number in the View bar and pressing **Enter**

Group Details

In the Group Details, you'll find the Group ID, Group Name, and Group Description of the selected user group.

- Click a specific group name listed in the **Group Summary** page and then click **Details** to view the **Group ID**, **Group Name**, and **Group Description** of that user group.

Mapped/Unmapped Roles

As an Administrator, you can map/unmap a role to/from a user group from the **Groups Summary** page.

To map/unmap roles to user groups:

1. Select the user group in the **Groups Summary** page.
2. Select **Mapped Roles** to access the list of roles mapped to the user group.
3. To map roles to user groups:
   a. Click **New Mapping**.

      The list of user roles you can map the group to is displayed in the **Available Roles** page.

   b. Select the check box corresponding to a user role or click **Select All** to select all the available user roles.

   c. Click **Map**.

      A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.
4. To unmap roles from user groups:
   a. Select the check box corresponding to a user role or click **Select All** to select all the available user roles.

   b. Click **Unmap**.

      A confirmation message is displayed after successful unmapping. The unmapping will be completed after authorization.
5. After mapping/unmapping a role, ensure to authorize it accordingly. To authorize a mapping/unmapping:
   a. In **Mapped Roles**, select the role-user group mapping or unmapping that requires approval.

   b. Click **Authorize/Reject** to approve or cancel the mapping/unmapping 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**.

Copyright © 2022, 2026, Oracle and/or its affiliates.

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 the **Roles Summary** page:

1. Click the **Identity Management** tab in the **Admin Console** page.
2. Click the **Roles** tile, to view the **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 Details.
4. Select a role name and click **Mapped Functions** to view the list of functions that are mapped to the particular role.

   You can also unmap a role from a specific function. To map/unmap functions, refer to mapped/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**.

   At the bottom of the page, adjust the number of entries displayed per page using the up and down arrows in the Records box. To navigate between pages in the View bar, use these buttons:

   - **First page** to go to the first page.
   - **Previous page** to go back.
   - **Next page** to move to the next page.
   - **Last page** to go to the last page.

   You can directly navigate to a specific page by entering its number in the View bar and pressing **Enter**.

Creating a New Role

Create roles to manage user access to groups, applications and resources, from the Admin Console.

To create a role, from the Admin Console:

1. Log in to the Cloud Service and click **Admin Console**.

   > **Note**
   >
   > Log in to the Admin Console using the same User ID mapped to the user group.

2. Navigate to **Identity management**.
3. Click **Roles** tile to access **Roles Management**.
4. Click **Add** to view **Add Roles**.
5. Enter the unique **Role Code**, **Role Name** and save the definition.

Copyright © 2022, 2026, Oracle and/or its affiliates.

Roles Details

Access Roles Details, to view the Role Code, Role Name, and Role Description of the selected role.

- Click a specific role listed in the **Roles Summary** page and then click **Details** to view the **Role Code**, **Role Name**, and **Role Description** of that role.

Mapped/Unmapped Functions

As an Administrator, you can map/unmap a role to/from a function user group from the **Roles Summary** page.

To map/unmap roles to functions:

1. Select the role name in the **Roles Summary** page.
2. Select **Mapped Functions** to access the list of functions mapped to the specific role.
3. To map roles to functions:
   a. Click **New Mapping**.

      The list of user functions you can map the role to appears in the **Available Functions** page.

   b. Select the check box corresponding to a function or click **Select All** to select all the available functions.

   c. Click **Map**.

      A confirmation message is displayed after successful mapping. The mapping will be completed after authorization.
4. To unmap roles from functions
   a. Select the check box corresponding to a function or click **Select All** to select all the available functions.

   b. Click **Unmap**.

      A confirmation message is displayed after successful unmapping. The unmapping will be completed after authorization.
5. After mapping/unmapping a function, ensure to authorize it accordingly. To authorize a mapping/unmapping:
   a. In **Mapped Functions**, select the role-function mapping or unmapping that requires approval.

   b. Click **Authorize/Reject** to approve or cancel the mapping/unmapping 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**.

Copyright © 2022, 2026, Oracle and/or its affiliates.

Functions Summary Page

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

To access the **Functions Summary** page:

1. Click the **Identity Management** tab in the **Admin Console** page.
2. Click the **Functions** tile to access the **Functions Summary** page.
3. Select a specific function name in the **Functions Summary** page and then click **Details** to view the associated **Function ID**, **Function Name**, and **Function Description**.

   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**.

   At the bottom of the page, adjust the number of entries displayed per page using the up and down arrows in the Records box. Use the navigation buttons, to go to the first page, last page, previous page and next page. You can also directly navigate to a specific page by entering its number in the View bar and pressing **Enter**.

Function Details

Using the Function Details options, you can view the Function ID, Function Name, and Function Description from the Functions Summary page.

- Click a specific function listed in the **Functions Summary** page and then click **Details** to view the **Function ID**, **Function Name**, and the **Function Description** of that function.

Folders Summary Page

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 the **Folders Summary** page:

1. Click **Identity Management** tab in the **Admin Console** page.
2. Click the **Folders** tile to access the **Folders Summary** page.

   The **Folders Summary** page is displayed.

   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 folder, type the first few letters of the folder name that you want to search in the search box and click **Search**.

   At the bottom of the page, adjust the number of entries displayed per page using the up and down arrows in the Records box. Use the navigation buttons, to go to the first page, last page, previous page and next page. You can also directly navigate to a specific page by entering its number in the View bar and pressing **Enter**.

Copyright © 2022, 2026, Oracle and/or its affiliates.

Folder Details

In the Folder Details, you'll find the Folder ID, Folder Name, and Folder Type of the selected folder from the Folders Summary page.

- Click a specific folder name listed in the **Folders Summary** page and then click **Details** to view the **Folder ID**, **Folder Name**, and **Folder Type** of that user.

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.

Copyright © 2022, 2026, Oracle and/or its affiliates.