Oracle Financial Services Profitability Analytics System Administrator User Guide





Oracle Financial Services Profitability Analytics System Administrator User Guide, Release 23.03.01

F82043-01

Copyright © 2022, 2023, 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, and MySQL 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

Use	ers and Roles	
1.1	View List of Application Users	1-1
1.2	Create Application Users	1-1
1.3	Create a User Group	1-4
1.4	Add User to Group	1-4
1.5	Import Application Users	1-5
Use	er Groups	
2.1	Map Application with the User	2-1
2.2	Map Application with the Groups	2-1
2.3	Map Users to Groups	2-1
2.4	Unmap User from Groups	2-3
2.5	Create a User Group	2-3
Use	er Management	
3.1	Application Users	3-1
3.2	User Roles and Privileges	3-1
3.	.2.1 Role Based Access Control	3-2
3.	2.2.2 User Roles and Activities	3-2
3.	2.2.3 User Groups and Activities	3-3
3.	.2.4 User Groups and User Role Mapping	3-3
Con	nfiguring Session Timeout	
4 1	How to configure Session Lifetime Timeout?	4-2



1

Users and Roles

Understand the following terms before you begin performing User Management.

- Users: Customers create users in Identity and Access Management (IAM) and can do the following:
 - Map them to existing groups
 - Create new groups to map them

After users are created, they are synced from IAM to the Cloud Service.

- Groups: Groups are seeded (available out-of-the-box) by your Cloud Service.
 Customers can also create new groups in IAM. After groups are created, they are synced from IAM to the Cloud Service. Groups are mapped to roles using the Cloud Service by the same user that was created using IAM.
- Roles: Roles are seeded by the Cloud Service. Customers can also create new roles using the Cloud Service and assign existing functions to these new roles.
- Functions: Functions are seeded by the Cloud Service. Customers cannot create new functions; however, they can only use the existing functions.

1.1 View List of Application Users

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.

Select the Username in the Users Summary page and then select Details to view the User ID and Username of the selected User.

To search for a specific User, type the first few letters of the Username that you want to search in the **Search** box and click **Search**.

The search result displays the names that consist of your search string in the list of available users.

You can use the navigation buttons at the bottom of this page to move around in different pages. Also, you can enter the number of entries to be listed on a single page in the **Records** box or use the buttons to increase of decrease the number of entries.

Also, you can enter the page number in the **View Bar Control** and jump to the page you want.

1.2 Create Application Users

After you sign in to your IAM console, one of your first tasks is to create additional user accounts. You should assign specific user groups to the user accounts that you are creating.

There are seeded user groups available with the respective services, users must be mapped to one or more of the user groups, depending on the role that they perform.

For example, you can create a user for each member of your team. Each team member can then sign into the account with their credentials. You can also assign each user to specific user groups and apply specific security policies or roles to each group.

You can create the users and map the users to groups for your service. After creating the users, the users will receive a Welcome email. The users must activate their accounts and enter a new password to access the services.

To create users in the IAM Console, perform the following steps:

- 1. In the IAM Console, click the **Profile** icon and select **Identity domain** to add the Application Users.
- 2. In the Identity Domain left pane, click Users and select Create user.
- 3. Enter the following details:

To have the user sign in with their email address:

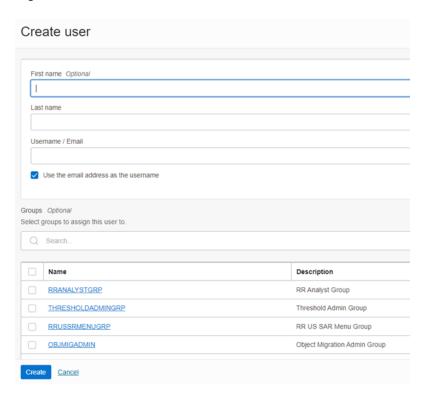
- Leave the Use the email address as the username check box selected.
- In the **Username / Email** field, enter the email address for the user account.

Or

To have the user sign in with their user name:

- Clear the Use the email address as the username check box.
- In the **First name** and **Last name** fields, enter the user name that the user is to use to sign in to the Console.

Figure 1-1 Add User Details





Ensure that you restrict the User Name to the following:

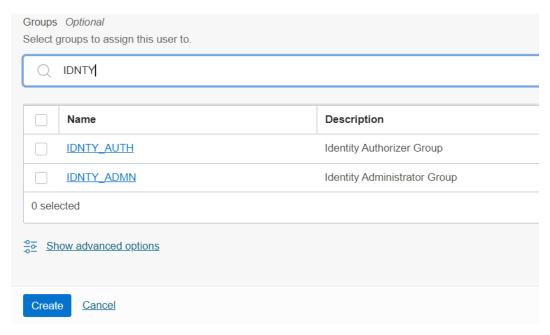
- a. Do not enter your Email ID as the Username and do not select the Use the email address as the username check box.
- Enter a maximum of 20 characters.
- c. Enter Alphanumeric Characters.
- d. Enter only Hyphen (-) and Underscore () Special Characters.
- In the Groups (Optional) section, select the user groups according to your user-specific groups or access.

Note:

After a user sign in to the PBSM Cloud Service, the User to User-Group Mapping created in the **IAM Console** will onboard into the Master and Mapping Tables. Later, if you deselect (remove) a User from a Group in the **Assign User to Groups** Window after provisioning, ensure that you also unmap the User from the corresponding User- Group in the **Admin Console**. This is a mandatory step to complete the unmapping process.

- 5. To create an Identity Administrator or Authorizer user, assign the users to the following:
 - IDNTY_ADMIN: You can use this option to create an Administrator User.
 - **IDNTY AUTH**: You can use this option to create an Authorizer User.

Figure 1-2 Assign Users to Groups Window



6. Click Create.



For Bulk User Creation, you can batch import User Accounts using a commaseparated values (.CSV) file.

1.3 Create a User Group

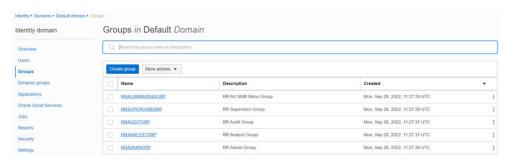
You can create groups to manage user access to applications and resources. A group has no permissions until you do one of the following:

- Write at least one policy that gives that group permission to either the tenancy or a compartment. When writing the policy, you can specify the group by using either the unique name or the group's OCID.
- · Assign the group to an application.

To create a User Group in IAM Console, perform the following steps:

- In the IAM Console, click the **Profile** icon and select **Identity domain** to add a User Group.
- 2. In the Identity Domain left pane, click **Groups** and select **Create group**.

Figure 1-3 Identity Domain



- 3. Enter the following details:
 - The name of the group. This field is mandatory.
 - Description for the group.
- 4. To allow users to request access to this group, select **User can request access**.
- To add users to the group, select the check box for each user that you want to add to the group.
- 6. Click Create.

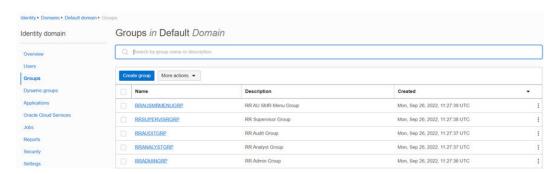
1.4 Add User to Group

To add a User to Group in IAM Console, perform the following steps:

- In the IAM Console, click the Profile icon and select Identity domain: Default to add the User Group.
- In the Identity Domain left pane, click Groups and select the group for which you want to add the users.



Figure 1-4 Groups in Default Domain



- Click Assign user to groups.
- To add users to the group, select the check box for each user that you want to add to the group.
- 5. Click Add.

1.5 Import Application Users

If you are an Administrator, you can batch import User Accounts using a Comma-separated Values (.CSV) file.



Before you can import user accounts, you must create a CSV file that is properly formatted for the import process.

To import user accounts, perform the following steps:

- In the IAM Consoleleft pane, click Users and select More Actions drop down and select Import Users.
- In the Import Users dialog box, click Browse to locate and select the CSV file that contains the user accounts to import.

Note:

Click **Download sample file** in the dialog box to download a sample file and carry out your accounts upload.

- Verify that the path and name of the .CSV file that you selected appear in the Select a file to import field.
- 4. Click Import.



If a user account is missing a required value, such as the user's first name, last name, or username, then Oracle Identity Cloud Service cannot import it. If Oracle Identity Cloud Service cannot import a User Account, then it evaluates the next account in the CSV file.

After Oracle Identity Cloud Service evaluates all User Accounts, the **Jobs** page displays the accounts you have imported. You can also get information related to the successful imports and imports that did not happen due to system errors.



User Groups

User Groups are seeded (available out-of-the-box) by the Cloud Service. Customers can also create new groups in IAM. After groups are created, they are synced from IAM to the Cloud Service. Groups are mapped to roles using the Cloud Service by the same user that was created using IAM.

2.1 Map Application with the User

To map the application to a User Group, log in to IAM and follow these steps:

- 1. Search for the **Domain**.
- Select the **Default Domain** and then from the LHS menu, select **Oracle Cloud Services**.
 The screen displays the various Oracle Cloud Services.
- Select the Cloud Services you are subscribed to like, PBSMCS xxxx-prd and PBSMCS xxxx-nprd.

Where **Description** is mentioned as PBSM Cloud Service.

- 4. From the LHS menu, select **Users**.
- 5. Click **Assign Users**, and then select the user.
- 6. Click Assign.

2.2 Map Application with the Groups

To map the application to a User Group, log in to IAM and follow these steps:

- 1. Search for **Domain**.
- Select the **Default Domain** and then from the LHS menu, select **Oracle Cloud Services**.
 The screen displays the various Oracle Cloud Services.
- Select the Cloud Services you are subscribed to like, PBSMCS xxxx-prd and PBSMCS xxxx-nprd

Where **Description** is mentioned as PBSM Cloud Service.

- From the LHS menu, select Groups.
- 5. Click **Assign Groups**, and then select the relevant **Group**.
- 6. Click Assign.

2.3 Map Users to Groups

If you are an Administrator and want to map a User to a User Group, log in to IDCS and follow these steps:

1. Select the **User Name** in the **Users Summary** page.

- 2. Select Mapped Groups.
- 3. Select the **User Group Name**.

To select a User Group, select the check-box corresponding to the User Group. To select all User Groups displayed on the page, select the check-box marked **Select All**.

4. Click **New Mapping** to map the User to the selected User Group.

Or

Click **Unmap** to remove the User Group-Role Mapping.

If the Unmap action requires authorization, see the Unmap User from Group section for details.

Note:

User-Group mapping changes from IDCS will take some time to sync with your Cloud Service. If these changes are made during the active user session, then it will be reflected on the next login.

After a user signs into the Cloud Service, the User to User-Group Mapping created in the IDCS Console will onboard into the Master and Mapping Tables. If you unmap a User from a Group in the Admin Console, navigate to the associated Console and open the Assign User to Groups Window. Deselect the User corresponding to the User Group and click **Finish**. This is a mandatory step to complete the Unmapping Process.

For more information, refer to Unmap User from Group.

After you click New Mapping, the list of User Groups you can map the user to appears in the Available Groups Summary Page.

5. Select a User Group.

Note:

To select a User Group, select the check box corresponding to the User Group. To select all User Groups displayed on the page, select the check box marked Select All.

If the logged-in user has both Administration and Authorization Entitlements, an Authorization View Toggle Button is available. Enable this button to complete the Authorization Process.

6. Click Map.





To select a User Group, select the check box corresponding to the User Group. To select all User Groups displayed on the page, select the check box marked Select All.

If the logged-in user has both Administration and Authorization Entitlements, an Authorization View Toggle Button is available. Enable this button to complete the Authorization Process.

2.4 Unmap User from Groups

To authorize the unmapping of a User to a User Group, log in to IAM and follow these steps:

- Click Unmapped Groups.
- Click the User Group Name to select the User Group.
- 3. Click Authorize to authorize the unmapping.

Or

Click **Reject** to cancel the Authorization Request.

2.5 Create a User Group

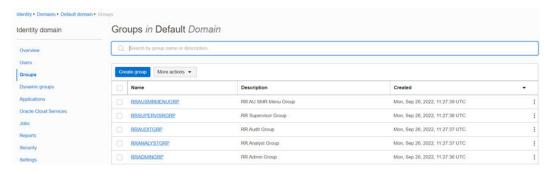
You can create groups to manage user access to applications and resources. A group has no permissions until you do one of the following:

- Write at least one policy that gives that group permission to either the tenancy or a compartment. When writing the policy, you can specify the group by using either the unique name or the group's OCID.
- Assign the group to an application.

To create a User Group in IAM Console, perform the following steps:

- In the IAM Console, click the Profile icon and select Identity domain to add a User Group.
- In the Identity Domain left pane, click Groups and select Create group.

Figure 2-1 Identity Domain



3. Enter the following details:



- The name of the group. This field is mandatory.
- Description for the group.
- **4.** To allow users to request access to this group, select **User can request access**.
- 5. To add users to the group, select the check box for each user that you want to add to the group.
- 6. Click Create.



User Management

During implementation, you prepare your Oracle Application's Cloud Service for the Service Users. The decisions made during this phase determine how you manage users by default. Most of these decisions can be overridden. However, for efficient User Management, Oracle recommends that you configure your environment to reflect both enterprise policy and support most or all users.

For more information, see the View List of Application Users and User Roles and Privileges.

3.1 Application Users

During implementation, you can use the Create User task to create Test Service Users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee Task to create Service Users. The Create User Task is not recommended after the implementation is complete.

For more information, see Create Application Users.

3.2 User Roles and Privileges

Oracle Financial Services Profitability Analytics Cloud Service (PACS) Users are assigned roles through which they gain access to functions and data. Users can have any number of roles.

The following figure shows User Personas and the tasks they can perform:

Figure 3-1 User Personas and Tasks



IDCS Administrator

- Create User
- Map Users to OOB User Groups
- Create User Groups and Roles
- Map Roles to User Group
- Map Functions to Roles



PACS Application Administrator

- Admin Privileges for all modules
- Manage Runchart and Batches
- Set Preferences
- Manage Set Up Configurations



PACS BI Analyst And

PACS Data Analyst

- Manage PACS data
 Create new reports if
- Create new reports if required of existing RPD
- · Manage Dimensions
- View OOTB Reports for Management Reporting and Profitability Insights



PACS Auditor

- Review PACS data integrity
- · Review Process Logs
- · View Reports



- User-Group mapping changes from IDCS will take five minutes to sync with the application. If these changes are made during the active user session then it will be reflected on the next login.
- You can create and manage Application users as required. For example, you can map the Pipeline Admin Group and PACS Admin Group to one user.

3.2.1 Role Based Access Control

Role-based security in Oracle Financial Services Profitability Analytics Cloud Service Controls who can do what and to which data.

The following table provides examples of role-based access.

Role Assigned to a User	Functions which Users with this Role can Perform	Set of Data which Users with the Role can Access when performing the Function
Application Administrators	Perform Application Administrator activities	User Group with Administration Roles across all Service Features
Business Users	Access to the Application to perform tasks	User Group with Business Tasks' Roles across all Service Features

3.2.2 User Roles and Activities

The following User Roles are seeded in the PBSM Cloud Service to facilitate the activities expected from the users mapped to the seeded User Groups:

- Profitability Analytics Administrator
- Profitability Analytics Application Analyst
- Profitability Analytics Application Auditor
- PA BI Data Steward
- PA BI Analyst
- PA BI Auditor
- PA BI LOB Head

In addition to this, Custom User Roles can be created and managed as per requirement.

The user roles Profitability Analytics Application Administrator, Profitability Analytics Application Analyst, and Profitability Analytics Application Auditor are required to access the main application for view, edit and other purposes, based on the User Persona accessing the same. An Analyst User Persona can view all PA Screens and Edit-specific Screens. Similarly, an Admin Persona can view and edit all PA Screens. These different Persona tasks are facilitated by the User Roles. Thus, these three



User Roles facilitate the accesses and activities for the corresponding User Groups that are mentioned in the below table.

The User Roles of - PA BI Data Steward, PA BI Analyst, PA BI Auditor and PA BI LOB Head - are seeded BI Roles to be used for the users to access the Analytics Menu in the PA Application. These four roles are created to facilitate Analytics access for four different types of User Persona. These roles can be mapped to any User Group to provide the Analytics access to users under the User Group.

3.2.3 User Groups and Activities

The following table provides the information on the User Groups and related activities.

User Groups	Activities		
PA Application Administrator	Admin Privileges for all modules		
	 Manage Runchart and Batches 		
	 Set Preferences 		
	 Manage Set Up Configurations 		
IDCS Administrator	 Create Users 		
	 Map Users to the Instance 		
PA Application Analyst	 Set User and Application Preferences 		
	 Set Setup Parameters 		
	 Currency and Rate Management 		
	 Dimension Management 		
	 Data Management: Metadata and Data Loaders 		
	 Data Model Extension 		
	 Create Filters and Expressions 		
	 Create Table Drivers 		
	 Create and Execute Allocation Rules 		
	 Create and Execute Allocation Models 		
	 Schedule Batch Processes 		
	 View Allocation Executions 		
	 View Profitability Analytics Reports 		
PA Application Auditor	 View privileges for all application-specific modules: 		
	 Review/Analyze Results 		
	Review Process Logs		
	 View Reports 		

In addition to this, the following user groups are also seeded viz – PA Authorizer, PA BI Analyst and PA Data Analyst. User roles can be mapped to these groups for efficient management of application. Custom User Groups can also be created and managed as per requirement.

3.2.4 User Groups and User Role Mapping

The following table lists the seeded mapping of User Groups to the User Roles.

User Group	Mapped User Role	
Profitability Analytics Application Administrator	Profitability Analytics Application Administrator	



User Group	Mapped User Role
Profitability Analytics Application Analyst	Profitability Analytics Application Analyst
Profitability Analytics Application Auditor	Profitability Analytics Application Auditor

The BI User Roles of PA BI Data Steward, PA BI Analyst, PA BI Auditor, PA BI LOB Head are not mapped OOTB to any seeded User Group but can be mapped to any User Group to provide the Analytics access to users under than User Group. Customers can custom User Groups and map the seeded or Custom User Roles as it suites the requirement.



4

Configuring Session Timeout

After you complete your tasks, you can sign out of your application. However, sometimes you might get automatically signed out due to session timeouts.

Let us understand how session timeouts work. When you sign in using your credentials, you're authenticated to use the application, and a session is established. During this session, you don't need to re-authenticate. But, for security purposes, your session is configured to be active for a predefined duration, which is called the session timeout period. Your sessions can expire due to various reasons such as leaving your application idle for a period longer than the timeout period. In such cases, you're automatically signed out of the application. Your timeout periods may vary on certain pages. For example, you may observe a longer timeout period on pages that automatically refresh or UIs that open in separate windows or tabs.

This table lists the various types of session timeouts you may experience. After the specified duration, your session expires, and you need to sign in again to continue your work.

Timeout Type	Description	Configurable	Timeout Duration
Session Lifetime Timeout	After you are authenticated in the application, if you are actively working on it, your session remains active for a predefined duration, referred to as the session lifetime timeout period. Your session ends after this period, even if you're using the application.	Yes	8 Hours (Default value)
Inactive Session Timeout	This type of timeout considers the duration you leave your application idle/inactive. After this duration, System automatically terminates the session, and you are signed out of the session.	No	60 Minutes
Browser Inactivity Timeout	This type of timeout considers the duration you leave your browser idle. After this duration, your session is terminated by the System, which automatically	No	60 Minutes



4.1 How to configure Session Lifetime Timeout?

You can configure the Session Lifetime Timeout using your Identity Domain Settings in OCI Console. You need to have the Security Administrator Role mapped to you, to access and modify the settings.

To configure the session timeout:

- 1. Login with your Security Administrator Account.
- 2. Navigate to the Domain page. Click Settings and select Session Settings.
- 3. Specify the Session Duration under Session Limits. Enter the required value. By default, this is set to 480 Minutes.

Figure 4-1 Session Settings



