Oracle Financial Services

Getting Started with Oracle Cloud Funds Transfer Pricing Cloud Service

Release 22.12.01
F77548-01
January 2023

ORACLE

Oracle Financial Services Getting Started with Oracle Cloud Funds Transfer Pricing Cloud Service, Release 22.12.01

F77548-01

Contents

1

Welcome to Oracle Cloud

Oracle Cloud is the industry's broadest and most integrated cloud provider, with deployment options ranging from the public cloud to your data center. Oracle Cloud offers best-in-class services across Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

About Oracle Cloud

Oracle Cloud is one of the few cloud providers that can offer a complete set of cloud services to meet all your enterprise computing needs.

Use Oracle Infrastructure as a Service (IaaS) offering to quickly set up the virtual machines, storage, and networking capabilities you need to run just about any kind of workload. Your infrastructure is managed, hosted, and supported by Oracle.

Use Oracle Platform as a Service offerings to provision ready-to-use environments for your enterprise IT and development teams, so they can build and deploy applications, based on proven Oracle databases and application servers.

Use Oracle Software as a Service (SaaS) offerings to run your business from the Cloud. Oracle offers cloud-based solutions for Human Capital Management, Enterprise Resource Planning, Supply Chain Management, and many other applications, all managed, hosted, and supported by Oracle.

Supported Web Browsers

Oracle Financial Services Cloud Services support the latest version of the following major browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

For more details, see Oracle Software Web Browser Support Policy.

When sharing a link to a document or folder, users of Microsoft Edge need to use the Show Link button and copy the link shown in the dialog.

Order Oracle Cloud Applications

You can order Oracle Cloud Applications (Software as a Service) offerings by contacting Oracle Sales. After your order is processed, you can then activate your services.

To order a subscription to Oracle Cloud Applications:

1. Go to the Oracle Financial Services Risk and Finance solutions page.
2. Scroll down and select **Funds Transfer Pricing**.

3. Review the features and capabilities of the service and read the Datasheet.
4. When you are ready to order, scroll up and click **Request a Demo**.
5. You can either write an email or click **Request Now** to receive a call from Sales.
6. Enter your **Business email**, select the confirmation check box, and click **Continue**.
7. Provide a description of your need and click **Request Now**.

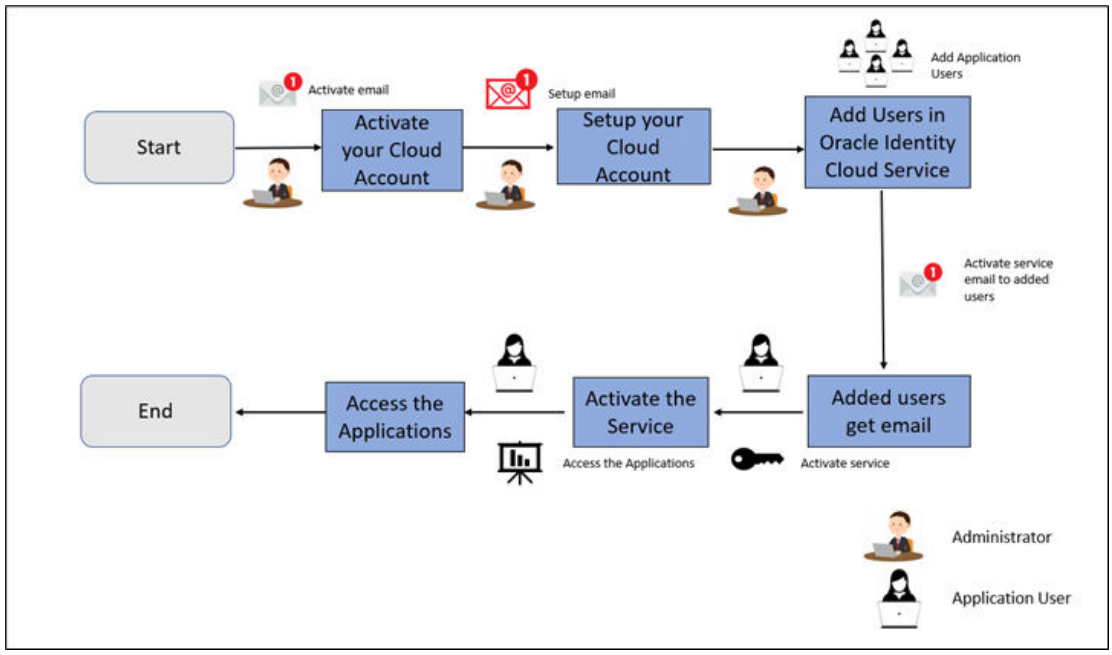
Later, after you have worked with Oracle Sales to order the Oracle Cloud Application best suited to your requirements, you will receive an email, which contains a link you can use to activate the service you have ordered.
To know how to activate, see Create and Activate New Cloud Account.

2

Get Started with Cloud Service

To get started, you must activate the Cloud Service. After activating the Cloud Service, you can onboard Application Users to use the subscribed Cloud Services.

Figure 2-1 Illustration of the Cloud Subscription Workflow



This topic describes the set of actions that can be performed by:

- An **Administrator** to activate the Cloud Account and onboard Applications Users for the subscribed Cloud Services.
  - Create and Activate New Cloud Account
  - Access the Cloud Account
  - Access the Oracle Identity Cloud Service Console
- The **Application Users** to activate and use the Cloud Services that are provisioned by the Administrator.
  - Activate your Account as Application Users

Create and Activate New Cloud Account

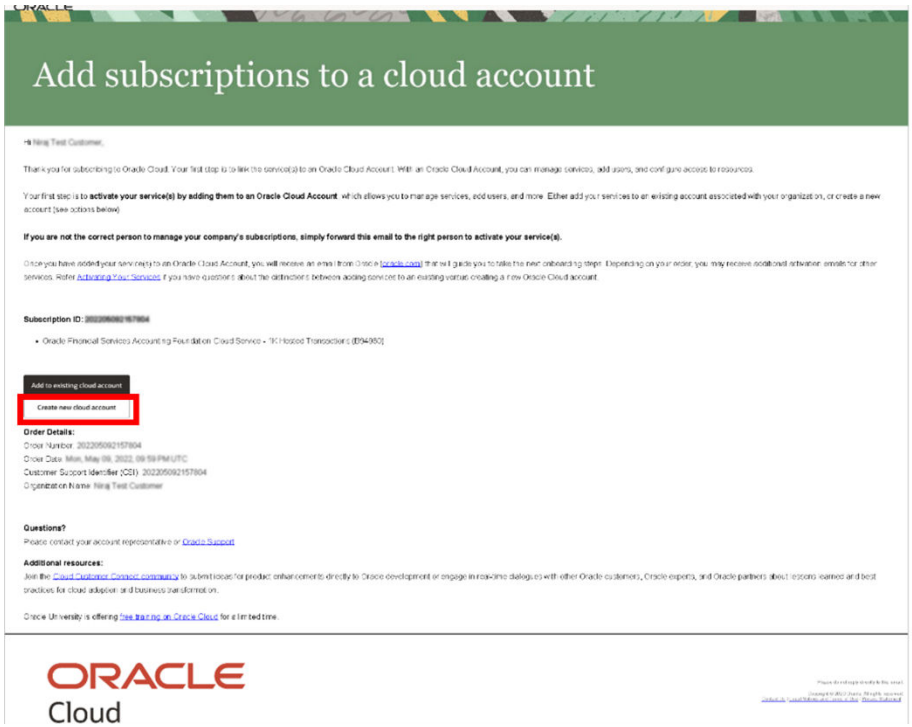
If you are a new Oracle Cloud Applications User, you will receive a Welcome to Oracle Cloud email that asks you to activate your Cloud Account. Follow the instructions in the email to create and activate your new Cloud Account.

You will then receive a follow-up email with the information you need to sign in and start using your Cloud Applications.

As an Administrator, to create and activate your new Cloud Account, perform the following steps:

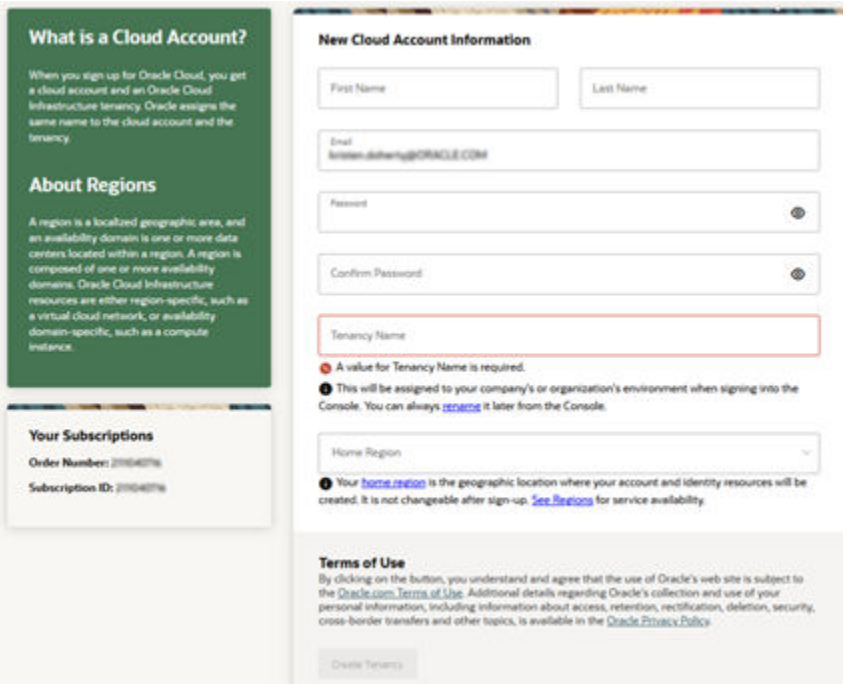
1. Click **Create New Cloud Account** in the email.

Figure 2-2 Illustration of Welcome to Oracle Cloud - Setup your Account email



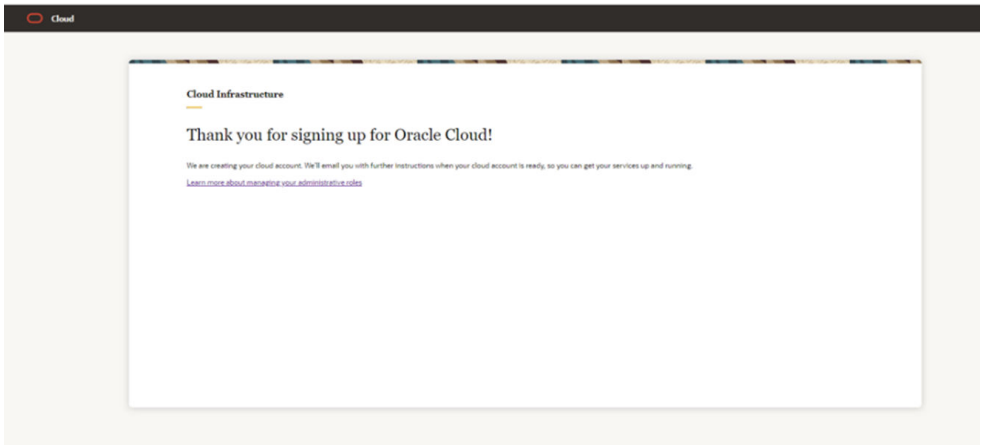
2. Complete the **New Cloud Account Information Form** to sign up.

Figure 2-3 New Cloud Account Information Page



3. Enter the following details:
   - **First Name** and the **Last Name**.
   - **Email**: Provide the same email address which you had given to receive the Welcome email. Instructions to log into your new Oracle Cloud Account will be sent to this email address.
   - **Password** to access the New Cloud Account.
     Re-enter the Password for confirmation. Make a note of the credentials. The same is required to log in after receiving the Activation email.
   - **Tenancy Name**: New Tenancy name to be associated with the Cloud Account.
   - **Home Region**: Select your Home Region, where the Identity Resources and Account are located. Check the service availability before selecting the Home Region.
   - – **First Name** and the **Last Name**.
     – **Email**: Provide the same email address which you had given to receive the Welcome email. Instructions to log into your new Oracle Cloud Account will be sent to this email address.
     – **Password** to access the New Cloud Account.
     Re-enter the Password for confirmation. Make a note of the credentials. The same is required to log in after receiving the Activation email.
     – **Tenancy Name**: New Tenancy name to be associated with the Cloud Account.
     – **Home Region**: Select your Home Region, where the Identity Resources and Account are located. Check the service availability before selecting the Home Region.
4. Click **Create Tenancy**.
5. The **New Cloud Creation Confirmation** screen is displayed.

Figure 2-4 New Cloud Creation Confirmation Screen



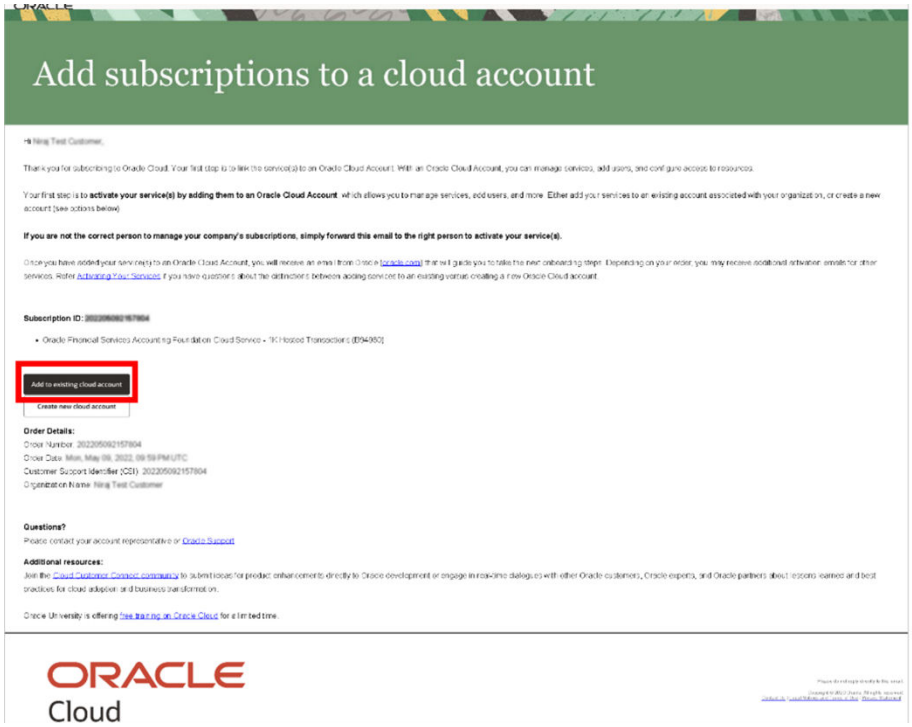
After successful activation, you'll receive a **Setup Complete** email.

Add to Existing Cloud Account

As an Administrator, if you already own a Cloud Account and need to use the Profitability Analytics Cloud Service (PACS), perform the following steps:

1. In the Welcome email, click **Add** to existing cloud account option.

Figure 2-5 Add subscriptions to a cloud account



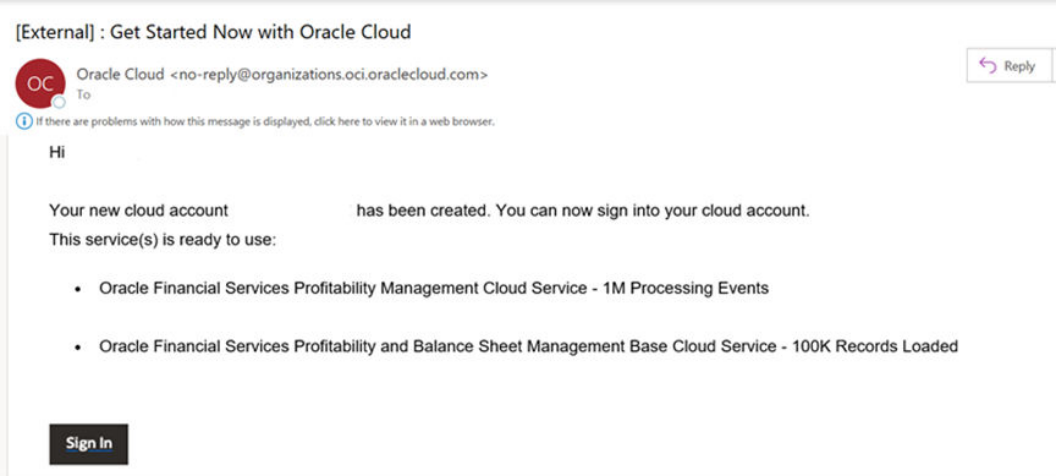
2. Perform the steps as mentioned in the Access the Oracle Identity Cloud Service Console section.

Access the Cloud Account

As an Administrator, to access the Cloud Account:

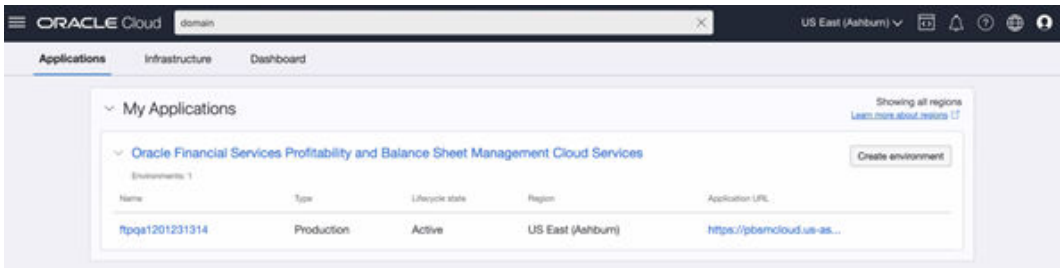
1. In the Setup Complete email, click **Sign In**.

Figure 2-6 Get Started Now with Oracle Cloud



2. Enter the Username and Password to access the **Oracle Cloud Console URL**. Use the same Username and Password that you provided during activation setup.
3. Reset the Password.
4. Re log in to **Oracle Cloud Infrastructure Classic Console** using the new Password.
5. Navigate to the **Oracle Cloud Infrastructure Classic Console**, the Application URLs are displayed.

Figure 2-7 Oracle Cloud



Access the Identity and Access Management

Oracle Cloud Infrastructure Identity and Access Management (IAM) provides identity and access management features such as authentication, single sign-on (SSO), and identity lifecycle management for Oracle Cloud as well as Oracle and non-Oracle applications,

whether SaaS, cloud-hosted, or on-premises. Employees, business partners, and customers can access applications at any time, from anywhere, and on any device in a secure manner.

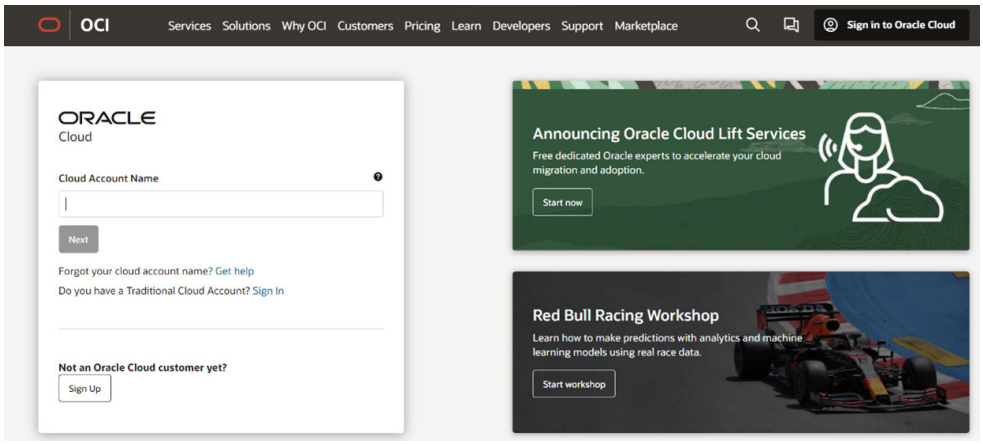
IAM integrates with existing identity stores, external identity providers, and applications across cloud and on-premises to facilitate easy access for end users. It provides the security platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Human Capital Management (HCM) and Oracle Sales Cloud, and platform services such as Oracle Java Cloud Service, Oracle Business Intelligence (BI) Cloud Service, and others. Administrators and users can use IAM to help them effectively and securely create, manage, and use a cloud-based identity management environment without worrying about setting up any infrastructure or platform details.

To add users to your Cloud Services, you need to navigate to the **Oracle Identity and Access Management (IAM)** Console.

To access the **IAM** Console, perform the following steps:

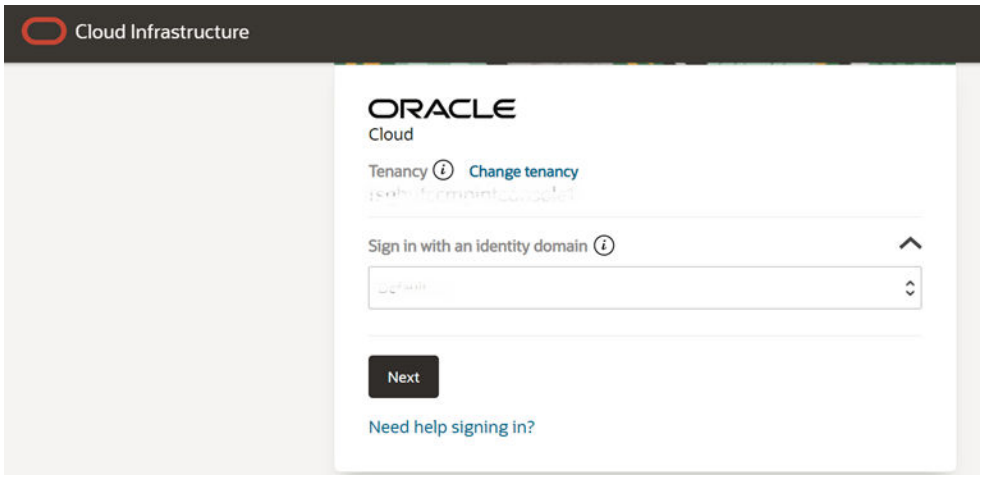
1. Browse to Cloud.Oracle.com.

Figure 2-8 Oracle Cloud Infrastructure Console



2. Enter the **Cloud Account Name** and click **Next** to access the **IAM Console**.

Figure 2-9 Identity Domain Selection Page

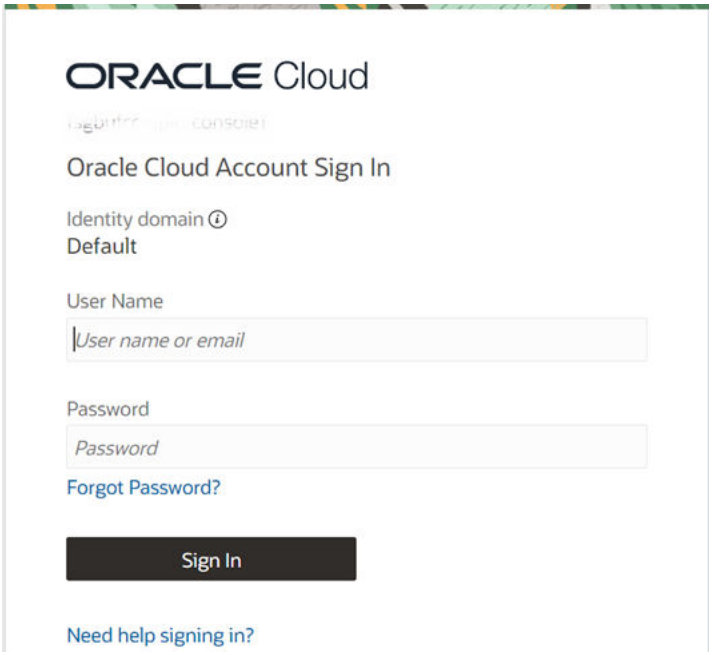


3. Select the **Identity domain** from the drop-down and click **Next**.

   The IAM login page is displayed.

> **Note:**
>
> Click **Change tenancy** option if you want to use a different tenancy.

Figure 2-10 Login Page



As an Administrator, you can create users to have different access rights to the Cloud Service.
For example, the IAM Administrator has superuser privileges for an Oracle Identity and Access Management Domain. This administrator can create users, groups, group memberships, and so on.

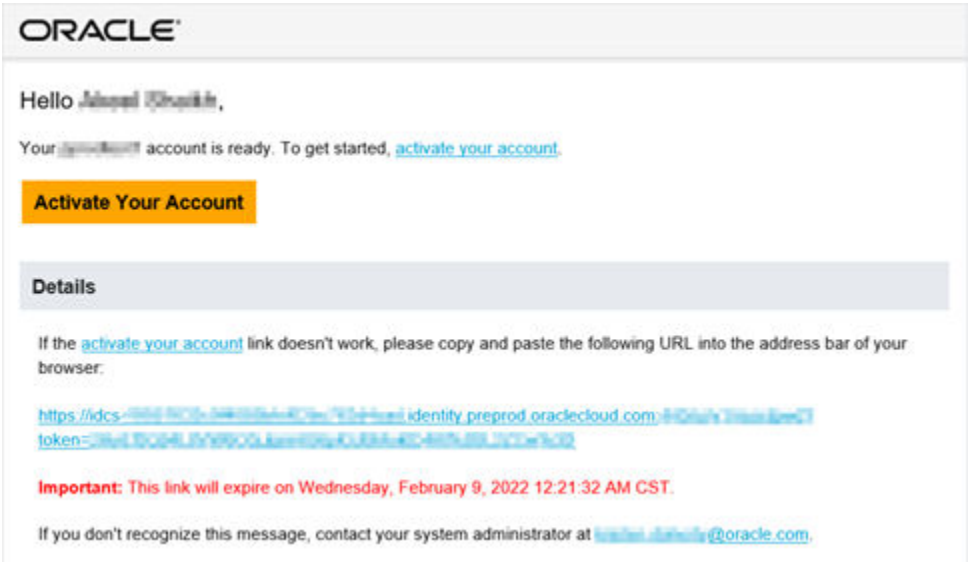
Activate Application User Account

After an Application User has been provisioned by their Administrator, they will receive an Account Activation email.

As an Application User, perform the following steps to login and activate your account:

1. Open the email you received from Oracle Cloud.

Figure 2-11 Email to Activate Your Account



2. Review the information about your service in the email.
3. Click **Activate Your Account**. You will be prompted to change your Password on the initial login.
4. Specify your new credentials in the **Reset Password** window to activate your account. After the Password is successfully reset, the **Congratulations** window is displayed.
5. Access the Application URL that your Application Administrator shared with you.
6. Specify your credentials to sign into your account. The Welcome page is displayed.

3
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 PACS.
- **Groups**: Groups are seeded (available out-of-the-box) by PACS. Customers can also create new groups in IAM. After groups are created, they are synced from IAM to PACS. Groups are mapped to roles using PACS by the same user that was created using IAM.
- **Roles**: Roles are seeded by PACS. Customers can also create new roles using PACS and assign existing functions to these new roles.
- **Functions**: Functions are seeded by PACS. Customers cannot create new functions; however, they can only use the existing functions.

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.

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 on the first page.
- Use the Previous Page Button to view the entries on the previous page.
- Use the Next Page Button to view the entries on the next page.
- Use the Last Page Button to view the entries on 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.

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:

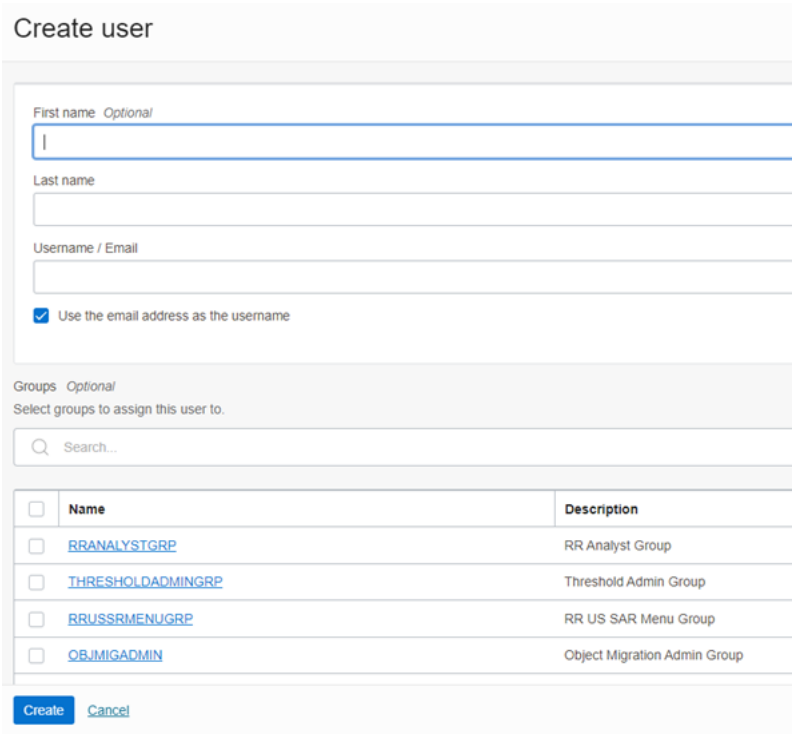
   - Leave the **Use the email address as the username** check box selected.
   - In the **Username / Email** field, enter the email address for the user account.

   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 3-1 Add User Details



> **Note:**
>
> 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.
> b. Enter a maximum of 20 characters.
> c. Enter Alphanumeric Characters.
> d. Enter only Hyphen (-) and Underscore (_) Special Characters.

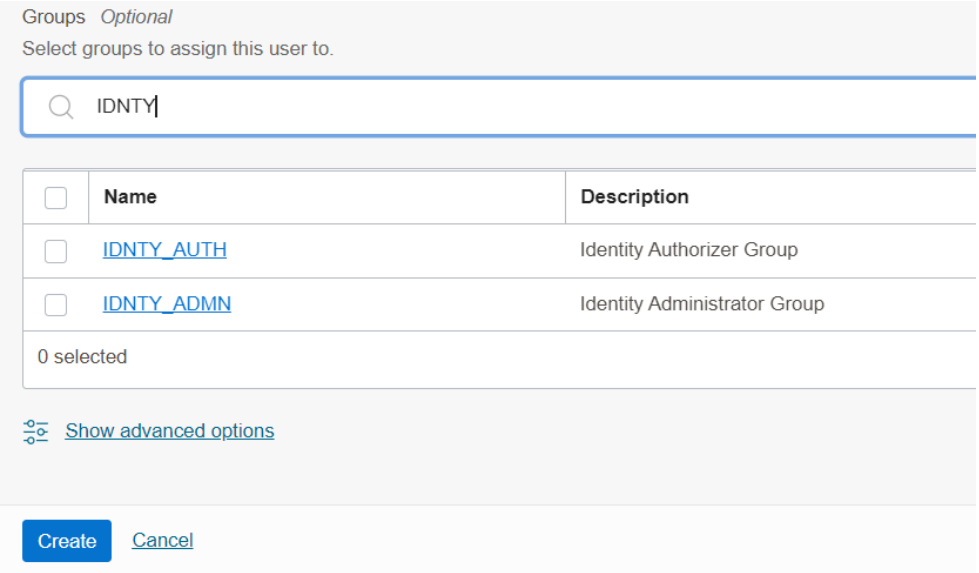
4. In the **Groups (Optional)** section, select the user groups according to your user-specific groups or access.

> **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 3-2 Assign Users to Groups Window



6. Click **Create**.

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

Create a User Group

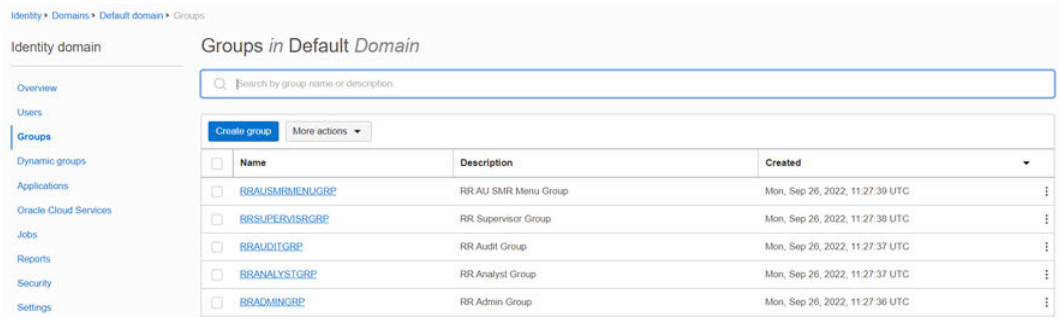
You can create groups to manage user access to applications and resources. A group has no permissions until you do one of the following:

- 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:

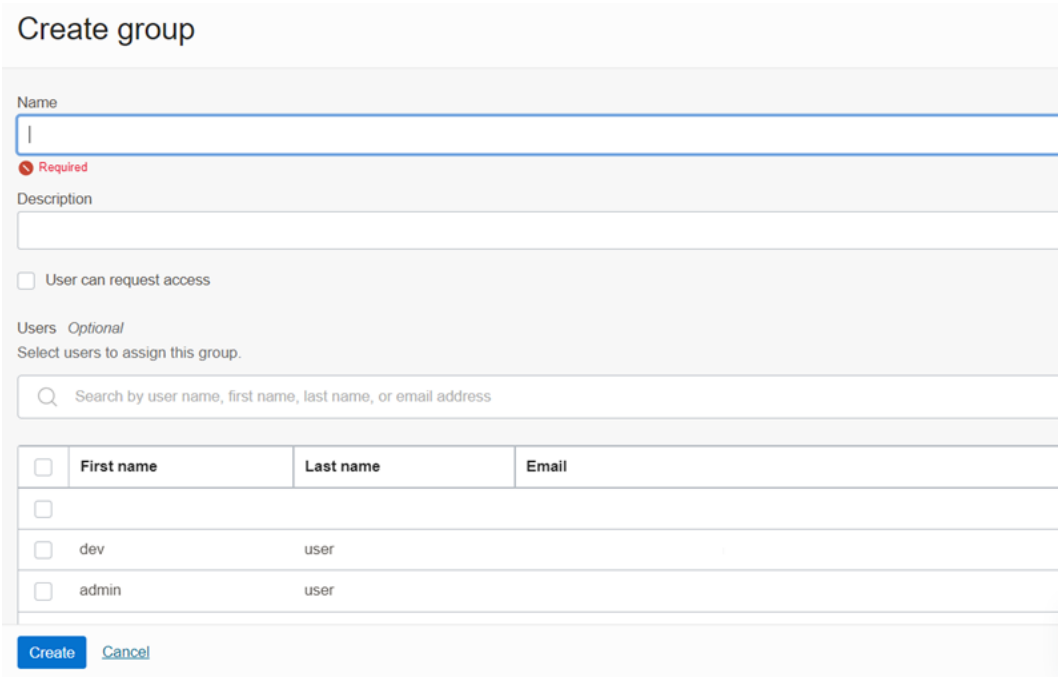
1. In the IAM Console, click the **Profile** icon and select Identity domain to add a User Group.
2. In the Identity Domain left pane, click **Groups** and select **Create group**.

Figure 3-3 Identity Domain



3. Enter the following details:
   - The name of the group. This field is mandatory.
   - The descriptive information about the group.

Figure 3-4 Add Group Details



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 the **Create**.

Add User to Group

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

1. In the IAM Console, click the **Profile** icon and select Identity domain: Default from the to add the User Group.

2. In the Identity Domain left pane, click **Groups** and select the group for which you want to add the users.

Figure 3-5 Groups in Default Domain

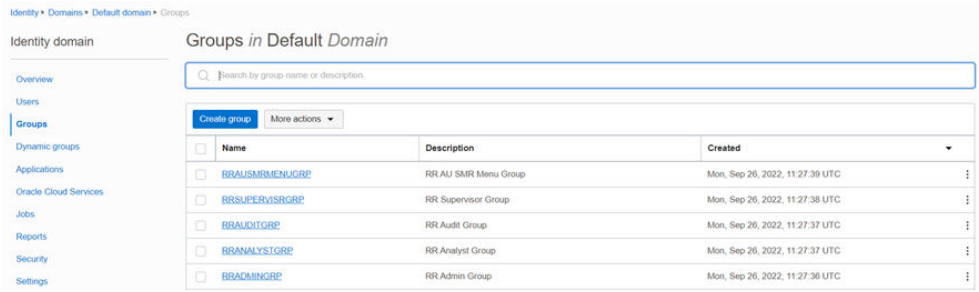
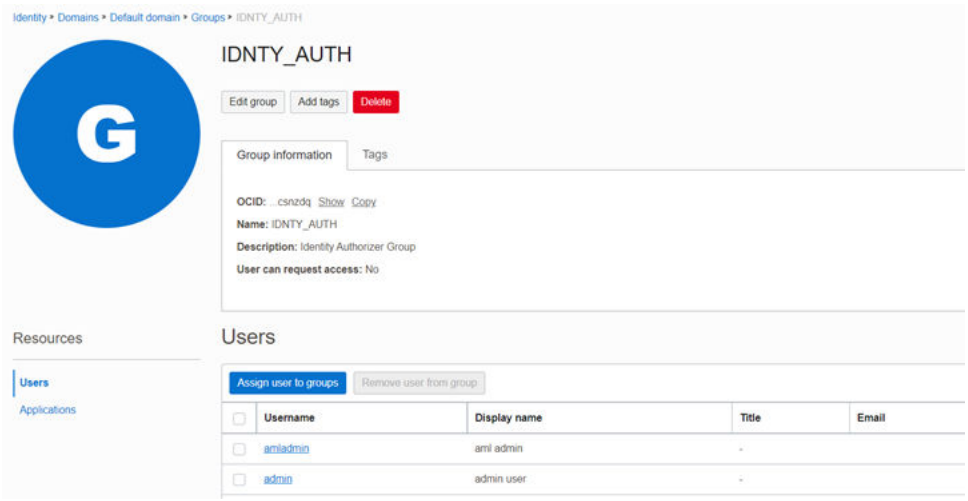


Figure 3-6 Assign Users to Group



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

Import Application Users

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

> **Note:**
>
> 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:

1. In the IAM Consoleleft pane, click Users and select More Actions drop down and select Import Users.
2. 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.

3. 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**.

> **Note:**
>
> 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.

4
User Groups

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

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**.
2. Select the **Default Domain** and then from the LHS menu, select **Oracle Cloud Services**.

   The screen displays the various Oracle Cloud Services.
3. Select **PBSM Cloud Services**.
4. From the LHS menu, select **Users**.
5. Click **Assign Users**, and then select the user.
6. Click **Assign**.

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**.
2. Select the **Default Domain** and then from the LHS menu, select **Oracle Cloud Services**.

   The screen displays the various Oracle Cloud Services.
3. Select **PBSM Cloud Services**.
4. From the LHS menu, select **Groups**.
5. Click **Assign Groups**, and then select the relevant **Group**.
6. Click **Assign**.

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**.

> **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**.

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 the PACS. If these changes are made during the active user session, then it will be reflected on the next login.
> After a user signs into Profitability Analytics Cloud Service (PACS), 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**.

> **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.

Unmap User from Groups

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

1. Click **Unmapped Groups**.
2. 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.

Create a User Group

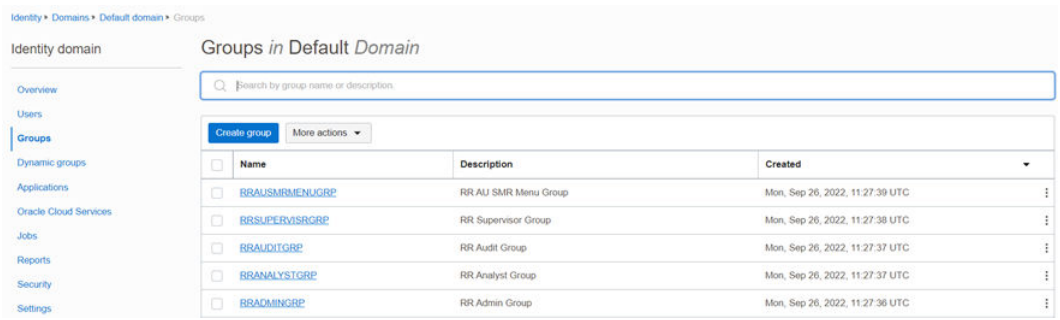
You can create groups to manage user access to applications and resources.
A group has no permissions until you do one of the following:

- 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:

1. 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**.

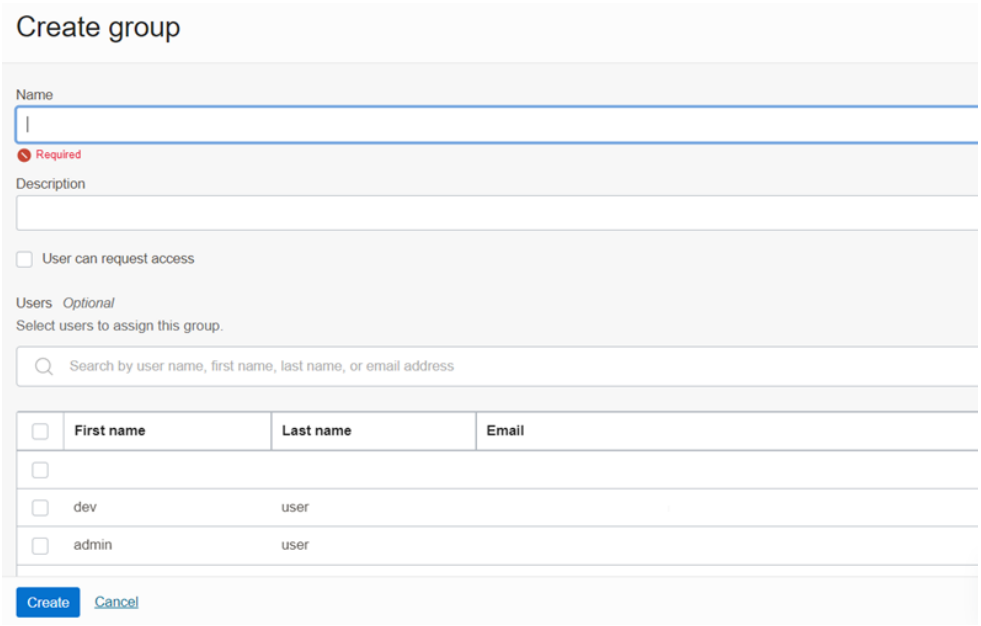
Figure 4-1 Identity Domain



3. Enter the following details:

- The name of the group. This field is mandatory.
- The descriptive information about the group.

Figure 4-2 Add Group Details



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 the **Create**.

5

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.

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.

User Roles and Privileges

Oracle Financial Services Funds Transfer Pricing Cloud Service (FTPCS) 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 5-1 User Personas

> **Note:**
>
> - 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 FTPCS Admin Group to one user.

Role Based Access Control

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

The following table provides examples of role-based access.

Table 5-1 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

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:

- Funds Transfer Pricing Administrator
- Funds Transfer Pricing Application Analyst
- Funds Transfer Pricing Application Auditor
- FTP BI Data Steward
- FTP BI Analyst
- FTP BI Auditor
- FTP BI LOB Head

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

The user roles Funds Transfer Pricing Application Administrator, Funds Transfer Pricing Application Analyst, and Funds Transfer Pricing 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 FTP Screens and Edit-specific Screens. Similarly, an Admin Persona can view and edit all PFT 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 - FTP BI Data Steward, FTP BI Analyst, FTP BI Auditor and FTP BI LOB Head - are seeded BI Roles to be used for the users to access the Analytics Menu in the FTP 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.

User Groups and Activities

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

Table 5-2 User Groups and Activities

User Groups	Activities
Identity Administrator Group	• View Object Storage • View OAuth Credentials • Perform Identity and Access Management Operations
IDCS Administrator	• Create Users • Map Users to the Instance
FTP Administrator	CRUD Privileges to the following modules: • Standard Process • Cash Flow Edits Process • Scheduler • BI Home Page • SQl Query Browser • Raw Data Analysis • Data Insights • Processed Data Insights • Interest Rates • Currency • Currency Rate • Dimension Management • Holiday Calendar • Preferences • Behavior Pattern • Propagation Pattern • Replicating Portfolio • Filter • Cash Flow Edits • Management Ledger Configuration • Transfer Pricing Rule • Add-On Rate Rule • Data Model Extension • Data File Administration

Table 5-2 (Cont.) User Groups and Activities

User Groups	Activities
FTP Application Analyst	CRUD Privileges: • Standard Process • Cash Flow Edits Process • Scheduler • BI Home Page • SQl Query Browser • Raw Data Analysis • Data Insights • Processed Data Insights • Interest Rates • Currency • Currency Rate • Dimension Management • Holiday Calendar • Preferences • Behavior Pattern • Propagation Pattern • Replicating Portfolio • Filter • Cash Flow Edits • Transfer Pricing Rule • Add-On Rate Rule • Data Model Extension • Data File Administration READ Privilege: • Management Ledger Configuration
FTP Application Auditor	• READ privileges for all application-specific modules: • Review/Analyze Results • Review Process Logs • View Reports

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

User Group and User Role Mapping

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

Table 5-3 User Group and User Role Mapping

User Group	Mapped User Role
Funds Transfer Pricing Application Administrator	Funds Transfer Pricing Application Administrator
Funds Transfer Pricing Application Analyst	Funds Transfer Pricing Application Analyst
Funds Transfer Pricing Application Auditor	Funds Transfer Pricing Application Auditor

The BI User Roles of FTP BI Data Steward, FTP BI Analyst, FTP BI Auditor, FTP 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.

6

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

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 6-1 Session Settings

7

Authenticating for Token Generation

The Authentication Process involves the use of cURL Commands in a CLI Tool to generate the access token and invoke REST APIs. An Authentication token is required to invoke an API to generate the File Upload/Download PAR URL.

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 required Cloud Service to invoke the REST APIs from external applications.

Ensure that you have the appropriate log-in credentials to access the required Cloud Service and the appropriate roles to perform specific operations using the API Resources. The following is the list of steps for Authentication and further subsections provide the details:

1. Download the Application Certificate
2. Get the OAuth Client ID and Client Secret
3. Generate the Access Token
4. Invoke the API using the Access Token

Download the Application Certificate

The Application Certificate is required for verification purposes when you use cURL commands. You may choose not to download the certificate if you plan to turn off the cURL Certificate Verification and use an insecure connection (if you add the --insecure Flag to the cURL command).

To download the Application Certificate, complete the following procedure:

1. Log in to your Cloud service.
2. Click **View site information/Verified by** in the Browser URL Address Bar.
3. Select **More information**, to view the certificate.
4. Click **View Certificate** and then click **PEM(cert)** to download the certificate.

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. Click **Navigation** 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 PBSM Internal Application Service (in **PBSMCS <tenant-id> INTERNAL** Format) from the list.
6. Click the **Configuration** Tab.

   The Client ID and Client Secret Details are displayed in the General Information Section.
7. Copy the **Client ID** and **Client Secret**.
8. Open a CLI Tool.
9. Generate the Access Token as shown in the following section.

You can also get the OAuth client ID and client secret using Admin Console. For more information, refer to Using Admin Console.

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. You can use an insecure connection (if you add the --insecure / -k Flag to the cURL command). The following is an example:

```
curl -k -i -H "Authorization: Basic  < Base64 Encoded
      Outh Cred >" -H "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8"
      --request POST https://<idcs_tenant>:443/oauth2/v1/token -d

"grant_type=password&scope=urn:opc:idm:__myscopes__+offline_access&user
name=<userid>&password=<Password>"
```

Sample Code

```
curl -k -i -H "Authorization: Basic
YWFpdGVzdGRldjEwMDEtcHJkX0FQUElEOjQyYjJlYWVlLTY1OGEtNDgzYi1hMWI2LTBlYzU
0MzBmYWQwNQ==" -H "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8" --request POST https://
idcs-0cb0c2b3ba624afca67467fd5eb9db49.identity.c9dev2.oc9qadev.com:443/
oauth2/v1/token -d
"grant_type=password&scope=urn:opc:idm:__myscopes__+offline_access&user
name=cneadmin&password=Password@12345"
```

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

> **Note:**
>
> The Access token expiry (in seconds) is configurable and can be set at the time of generating the access token. In the preceding example, it is set to 3600 seconds ~ 1 hour. By default, the expiry is set to 3600 seconds ~ 1 hour. You can configure this to a value of your choice up to a maximum value of 31536000 seconds ~ 1 year.

The token is sent as a response. Store the token in a secure location.

Sample Access Token (Truncated example)

```
{"access_token":"eyJ4NXQjUzI1NiI6IlF5azRtb3pIakhuQjJoQnVWdmZXZUpVeVZrNHhUdWd6
aWpHSC1pV21xb1EiLCJ4NXQiOiJDRFhHYVlWZXI3STVhQ1l
...
...
DB_be0Rtw1aMxFYg8Ft0VaK14wOVFGhgg1Cr6GiNvbgeYRG5uwgJGqw","token_type":"Bearer
","expires_in":3600,"refresh_token":"AgAgYjA1OGVlMjJiMWY2NGU3YWFkM2NjZWNlOTc2
MjNiNDgIABBmZRHXpaHil2VBXkevFX-
iAAAAMMq9uQDo86eVVVisw3kYn80iX8qRJ2m7hMLmMAh1dY9Wgy-ESu8WYzdTBXOsnwHr7A=="}
```

Generate the Refresh Token

To generate a Access token using Refresh token, use the following Curl command . You can use an insecure connection (if you add the --insecure / -k Flag to the cURL command). The following is an example:

```
curl -k -i -H "Authorization: Basic <base64Encoded clientid:secret>" -H
"Content-Type:
        application/x-www-form-urlencoded;charset=UTF-8" --request POST
        https://<IdentityDomainURL>/oauth2/v1/token -d

"scope=urn:opc:idm:__myscopes__&grant_type=refresh_token&refresh_token=<refre
sh_token>"
```

Sample Code

```
curl -k -i -H "Authorization: Basic

cWppMHBkLXByZF9BUFBJRDplZjFjMTVmZi1lZDBiLTQxNmItYTFmYy0wNjhlYzM5NmUxM2Y=" -H
        "Content-Type: application/x-www-form-urlencoded;charset=UTF-8" --
request POST
        https://<IdentityDomainURL>/oauth2/v1/token -d

"scope=urn:opc:idm:__myscopes__&grant_type=refresh_token&refresh_token=AgAgYj
A1OGVlMjJiMWY2NGU3YWFkM2NjZWNlOTc2MjNiNDgIABBmZRHXpaHil2VBXkevFX-
iAAAAMMq9uQDo86eVVVisw3kYn80iX8qRJ2m7hMLmMAh1dY9Wgy-ESu8WYzdTBXOsnwHr7A=="
```

Sample Refresh Token (Truncated example)

```
{"access_token":"eyJ4NXQjUzI1NiI6IlF5azRtb3pIakhuQjJoQnVWdmZXZUpVeVZrNHhUdWd6
aWpHSC1pV21xb1EiLCJ4NXQiOiJDRFhHYVlWZXI3STVhQ1l...
...
...
token_type":"Bearer","expires_in":3600,"refresh_token":"AgAgYjA1OGVlMjJiMWY2N
GU3YWFkM2NjZWNlOTc2MjNiNDgIABA4t8V_dYVyc5lOuKezofTUAAAAMJrpmKRhDWf3-
ejCreU8_Po5Bb95srwUDDs5cV1gT-x26twbAfp_ffMCiEgjqGeDNw=="}
```

Invoke the API using the Access Token

To invoke the API using the generated Access Token, do as shown in the following example using cURL Commands in the CLI Tool:

```
curl -iL -H "Authorization: Bearer <access token>" -H "Content-Type:
<content_type>" -d "<request_body>" --cacert <certificate(.pem)> -X
<http_verb> <api_url>

curl -iL -H "Authorization: Bearer <AUTH_TOKEN>"

-H "Content-Type: application/json" -d "{\"type\":\"files\",\"data\":
[{\"fileName\":\"testtoken\",\"mimeType\":\"text/plain\",\"fileSize\":

123}]}" --cacert outcert.pem -X POST https://<OCI-URL>/
<TENANT><APP_ID>/dsa/utils/getObjStoreParUrl
```