# Oracle® Financial Services Data Foundation Cloud Service for Banking

## Getting Started Guide

Release 26B
G39647-10
May 2026

ORACLE

Oracle Financial Services Data Foundation Cloud Service for Banking Getting Started Guide, Release 26B

G39647-10

# Contents

1

# About This Guide

This section provides supporting information for the Oracle Data Foundation Cloud Services for Banking (DFCS).

### Audience

This document contains release information of Oracle Data Foundation Cloud Services for Banking (DFCS).

### Documentation Accessibility

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

### Access to Oracle Support

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

### Related Resources

- Data Foundation for Banking

### Conventions

The following text conventions are used in this document.

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

2

# Get Help in the Applications

Use help icons to access help in the application.

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

# 3 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).

## 3.1 Supported Web Browsers

Oracle Financial Services Data Foundation Cloud supports 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.

4

# 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 **Data Foundation**.
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. Describe 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.

# 5
# Getting Started

To get started, you must activate the Data Foundation Cloud Service (DFCS). After activating the Cloud Service, you can onboard Application Users to use the subscribed cloud services.

**Figure 5-1 Illustration of the Cloud Subscription Workflow**

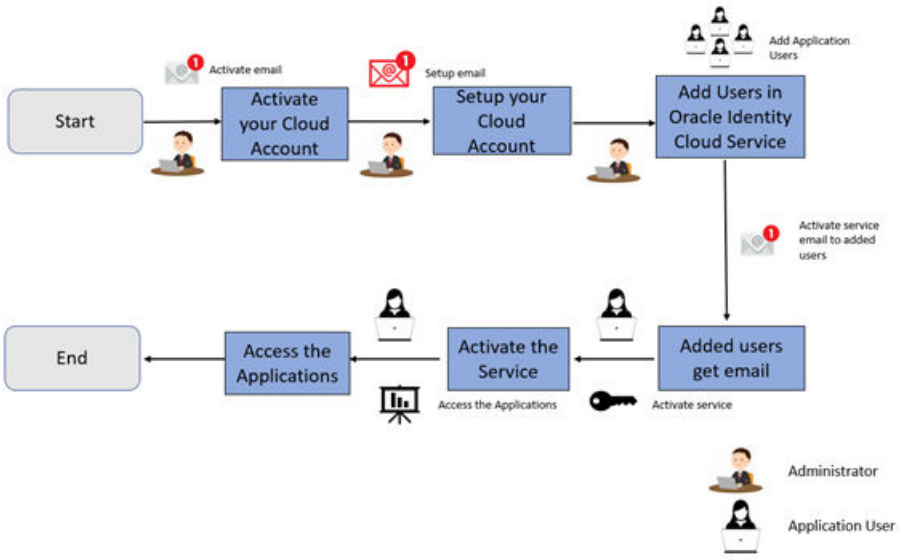



Illustration of the Cloud Subscription Workflow

This document 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 your 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 Application User Account

After the administrator successfully adds an application user, they can log in and activate their cloud account and use the subscribed cloud services provisioned by the administrator.

**Choosing Between a New or Existing Cloud Account**

Every administrator in a cloud account (tenancy) has access to all subscriptions within that account. To ensure that new administrators cannot access existing subscriptions, you should activate new subscriptions in a separate tenancy by creating a new Oracle Cloud Account. If

separate access controls are not needed, you may add new subscriptions to an existing Oracle Cloud Account.

# 5.1 Create and Activate your Cloud Account

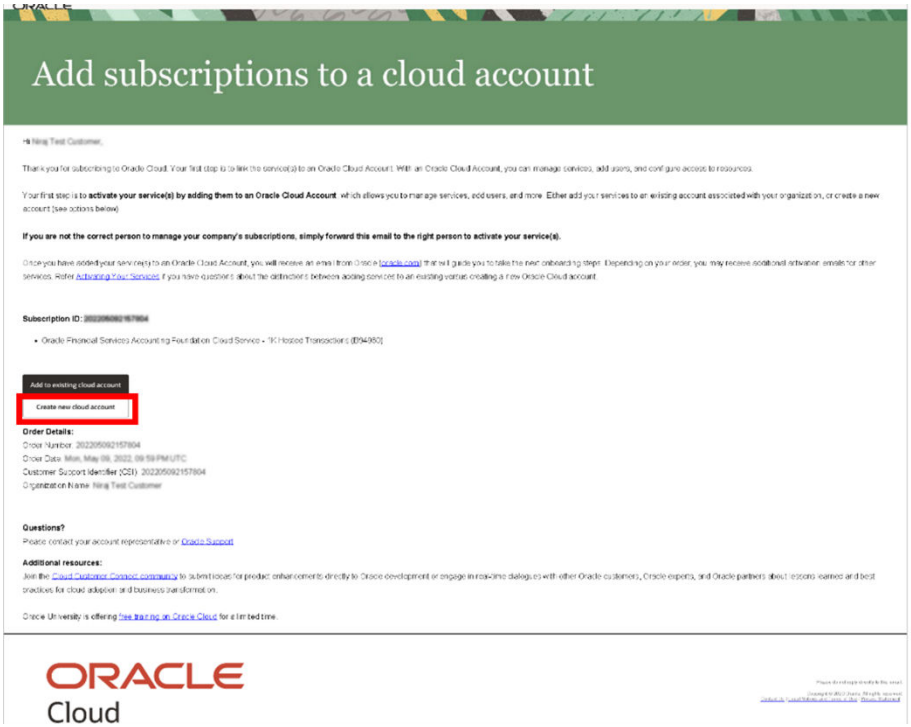
If you are a new Oracle Cloud Applications User, you will receive a Welcome to Oracle Cloud email that asks you to activate your Cloud Account. Follow the instructions in the email to create and activate your new Cloud Account.

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:

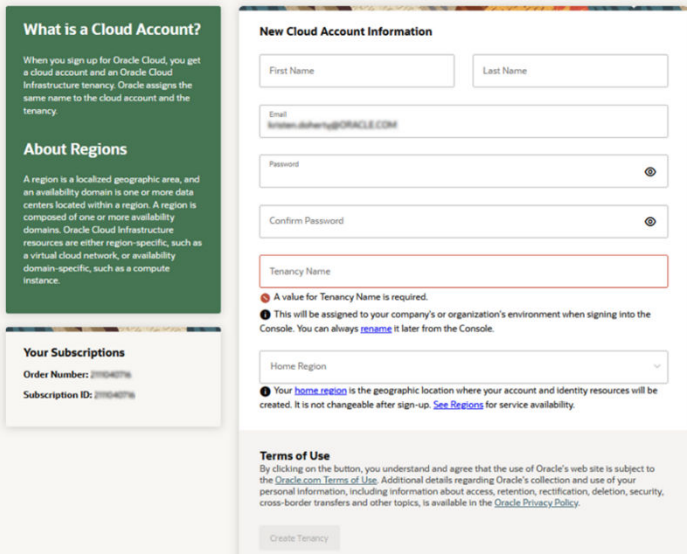
1. Click **Create New Cloud Account** in the email.

**Figure 5-2 Illustration of Welcome to Oracle Cloud - Setup Your Account Email**




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

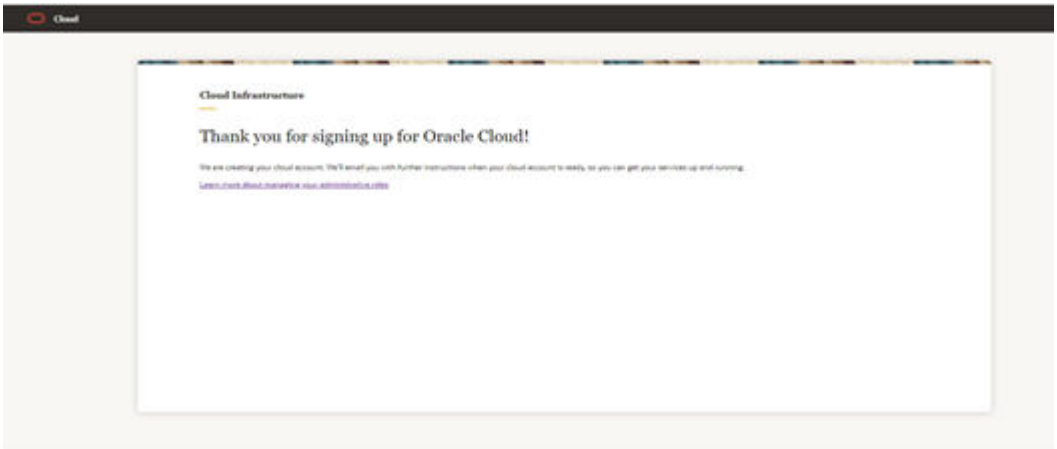
**Figure 5-3 New Cloud Account Information Page**




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.
- Click **Create Tenancy**.
  The New Cloud Creation Confirmation Screen is displayed.

**Figure 5-4 Oracle Cloud Creation Confirmation Screen**

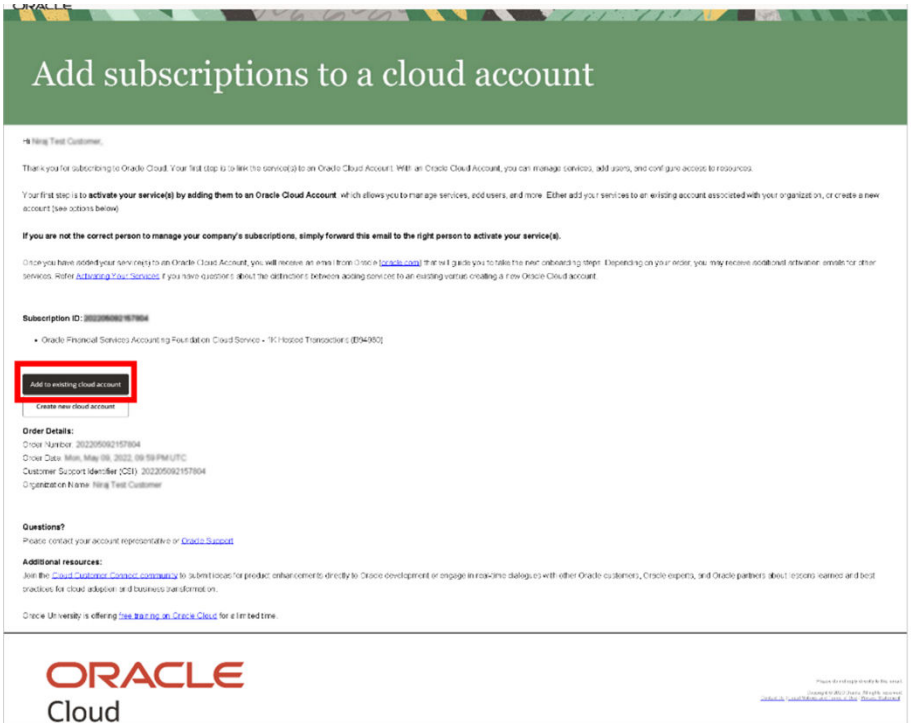



After successful activation, you'll receive a Setup Complete Email.

# 5.2 Add to Existing Cloud Account

As an Administrator, if you already own a Cloud Account and need to use the Data Foundation Cloud Service (DFCS), perform the following steps:

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




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

# 5.3 Access the Cloud Account

As an Administrator, to access the Cloud Account:

1. In the Setup Complete email, click **Sign In**.
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. Click **Reset the Password**.
4. Log in to the **Oracle Cloud Infrastructure Console** again using the new password.
5. Navigate to the **Oracle Cloud Infrastructure Console**, the Application URLs are displayed.

# 5.4 Creating Co-Administrator Users

After you log in to the IAM console, the first task 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 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.

> **Note**
>
> A co-administrator will have the same privileges as the existing administrator.

To create a co-administrator user in the IAM Console:

1. In the IAM Console, select **Domains** (Identity domain) to view the list existing domains.
2. Click the required **Domain Name**, to access the **Domain Details** page.
3. In the left pane, click **Users** and select **Create user**, to proceed with the user creation.
4. Enter the following details:
   - **First Name**, **Last Name** and a valid **Username** and the **Email ID**.

     > **Note**
     >
     > – The username should be alphanumeric and cannot exceed 20 characters. You can enter only hyphen (-) and underscore (_) as special characters.
     >
     > – Uncheck the **Use the email address as the username** check box, as you can only set the username as the login ID and currently setting the email address as the login ID is not supported.

5. Select the **Administrator Group**.

> **Note**
>
> After a user logs in to a specific 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 **Assign User to Groups** 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.

6. After entering the required information, click **Create** to create and add the new user to the User Summary.

You can also batch import several users using a `.CSV` file.

# 5.5 Subscribing to a Disaster Recovery Infrastructure Region

In Oracle Cloud Infrastructure (OCI), a Disaster Recovery (DR) region is a secondary, geographically separate region that helps ensure service continuity.

To maintain high availability, you must subscribe to a DR region as part of your disaster recovery strategy.

For information on how to subscribe to a DR Infrastructure region, see Subscribing to an Infrastructure Region.

# 5.6 Create an Environment

After logging into Oracle Cloud Infrastructure Console, you need to create an instance or multiple instances that can be used by different user groups as a self-service.

To create an instance, follow these steps:

1. Log into Oracle Cloud Infrastructure Console.
2. Under **My Application**, you will see the list of environments (instances) provisioned for the one or multiple cloud applications. The following details are provided for each environment:
   a. **Name**: The given name to the cloud application's instance.
   b. **Type**: The type of the instance.
   c. **Life cycle status**: The status of the instance.
   d. **Region**: The region from where this instance is active.
   e. **Application URL**: The URL to access the instance.
3. Click **Create environment** to display the Create environment screen.
   This screen displays a list of Cloud Services with the details like Subscription ID for which the customer is subscribed to and the Region from where these services are operated.

> **Note**
>
> - For **existing DFCS customers**, the subscription name is **Financial Services for Accounting Foundation**.
> - For **new DFCS customers**, the subscription name is **Oracle Financial Services Data Foundation Cloud Service for Banking**.
>
> To identify a DFCS subscription, click the subscription name and check the instance types. All DFCS instances are prefixed with **DFCS** (for example, **DFCS Production**).

> **Note**
>
> By default, the Cloud Account's home region is displayed, as this is where the cloud environment is deployed. If you want to deploy the Cloud Service environment in a different region, you must subscribe to that specific region. This option is available only when creating an environment for the first time under the subscription. If you are not sure about the Region, contact My Oracle Support (MoS).

4. Under Environment Details, enter the following information:
   - **Name**: The name of the new environment or instance.
   - **Instance type**: Select from the following options:
     - **DFCS Production**: An environment that will be tagged as Production and can be used for Production activities.
     - **DFCS Non-production**: An environment that will be tagged as Non-production and which will be used for testing and development purposes. For example, a sandbox environment. For example, a sandbox environment.
     - **DFCS Additional XS**: For testing extra small-range accounts.
     - **DFCS Additional Small**: For testing small range accounts.
     - **DFCS Additional Medium**: For testing medium range accounts.
     - **DFCS Additional Large**: For testing large range accounts.
     - **DFCS Additional XL**: For testing extra-large range accounts.
     - **Test**: An additional test environment for testing and development purposes.

       > **Note**
       >
       > The range corresponds to different scales of hosted accounts:
       >
       > * Extra Small (XS): Less than 251
       > * Small: 251 - 500
       > * Medium: 501 - 1000
       > * Large: 1001 - 10,000
       > * Extra Large (XL): 10,001 - 150,000

- Admin email: The email ID with which you have logged into the Cloud Console. You can also enter a different email ID that is part of the Cloud tenancy. For more details, see Managing Users.
- Admin first name and Admin last name: The first and last names of the Admin.

> **Note**
>
> You can have one Production, one Non-Production, and multiple test instances. The number of instances you can create is dependent on the number of contract subscriptions you have purchased.

5. Click **Create**.
   The environment details are added to the Oracle Cloud Infrastructure Console under the Environments tab with Creating state. Once completed, the created environment is Active. If there are any issues, you can raise a service ticket with My Oracle Support (MoS).

After the details are displayed with Active state, you can click on the Name to open the Environment details page, where you can check the details. You can click on the Service URL in the details to proceed with User Creation and User Group Creation which are discussed in the subsequent topics.

For more information on the deployment of the application, see the *Domain* section in the Oracle® Data Foundation Cloud Service Data Platform.

# 5.7 Access the Oracle Identity Cloud Service Console

The Oracle Identity Cloud Service integrates directly with existing directories and Identity Management Systems and makes it easy for users to get access to applications. It provides the Security Platform for Oracle Cloud, which allows users to securely and easily access, develop, and deploy business applications such as Oracle Data Foundation Cloud Service (DFCS) and Profitability and Balance Sheet Management Cloud Service (PBSMCS).

Administrators and Application Users can use Oracle Identity Cloud Service 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.

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, navigate to the **Oracle Identity and Access Management (IAM)** Console.

To access the **IAM** Console:

1. Log in to Cloud.Oracle.com, to view all the details pertaining to your cloud order. Access the service link from the console to start using your subscriber cloud service.
2. Enter the **Cloud Account Name** and click **Next** to access the **IAM Console**.
3. Click **Change tenancy** option if you want to use a different tenancy.

4. Ensure that the displayed identity domain matches the expected value.
5. Log in with your **Username** and **Password**.
   As an Administrator, you can create and manage users with 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.

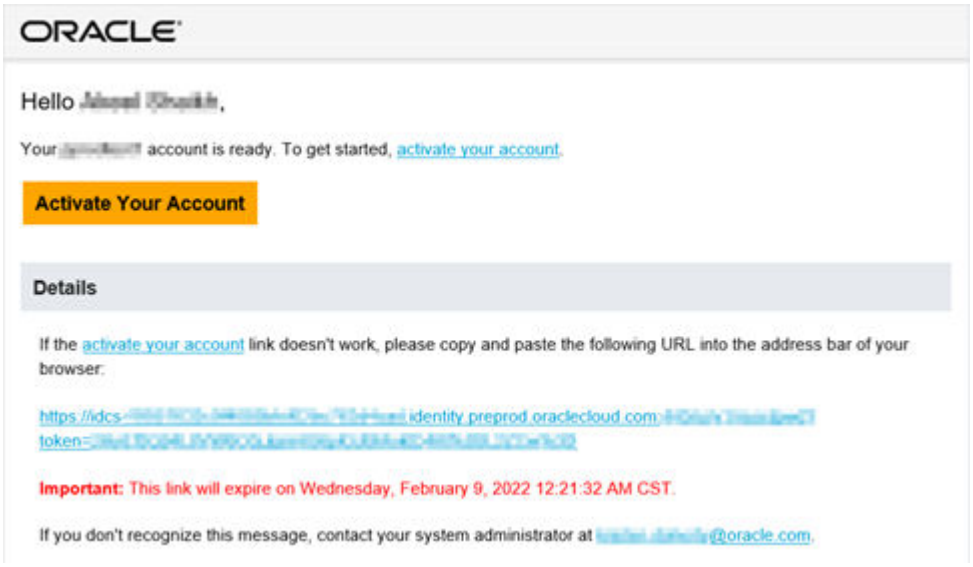
# 5.8 Activate Application User Account

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 5-5 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.

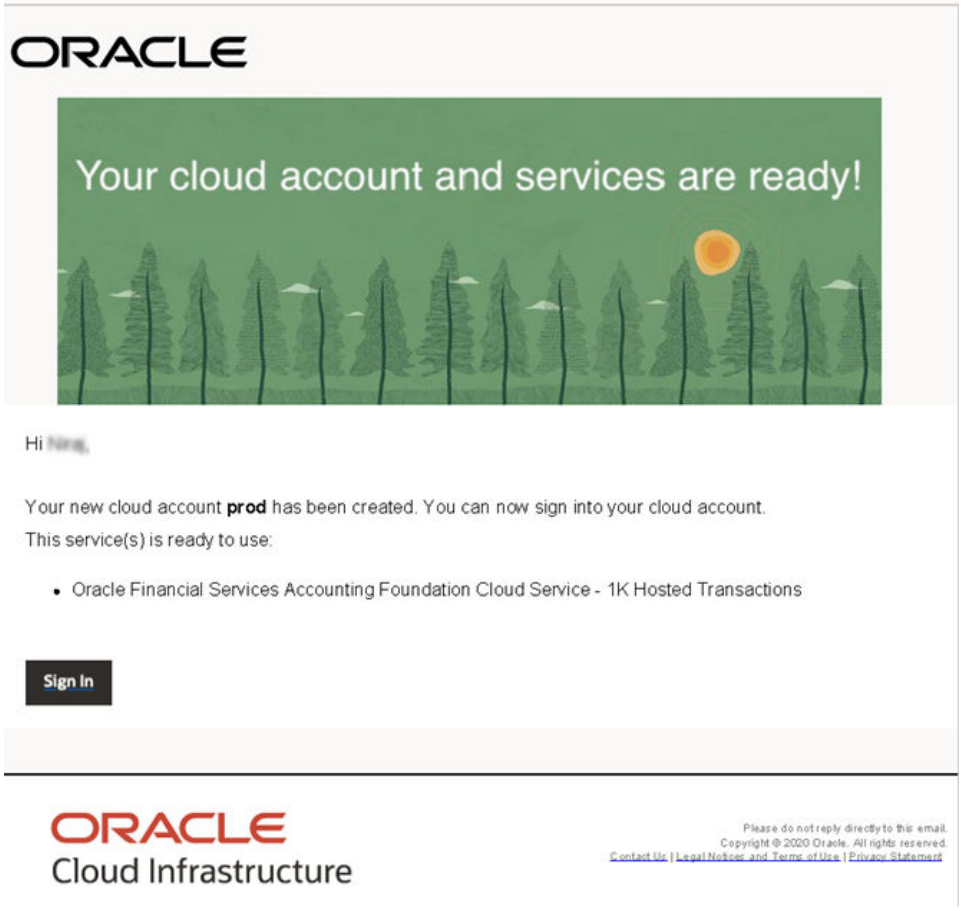
   After the Password is successfully reset, a congratulatory message is displayed.
5. Access the Application URL that your Application Administrator shared with you.
6. Specify your credentials to sign into your account.

   The **Welcome** page is displayed.

# 5.9 Setup your Cloud Account

After successful activation of your cloud account, you will receive a Setup Complete Email with your login credentials.

> **Note**
>
> You need to access the Oracle Cloud Console https://ofsaa.<REGION>.ocs.oraclecloud.com/ui/v1/adminconsole and create your user account before you access the application URL.




1. **Sign In to Oracle Cloud Console**
   - Click the **Sign In** link provided in the email.
   - Enter the **Username** and **Temporary Password** sent in the email.
   - Follow the prompts to **reset your credentials**.
2. **Navigate to Oracle Identity Cloud Service**
   - After logging in, you will be redirected to the **Oracle Cloud Infrastructure Console**.
   - Access the **Oracle Identity Cloud Service (Identity Console)** to onboard cloud service users. For more information about how to access the Identity Cloud, see Access the Oracle Identity Cloud Service Console.
3. **3. Accessing Production and Non-Production Instances**
   - The **Application URL** in the email is for the **Production** instance.
   - To access the **Non-Production** instance, modify the URL by replacing **"-prd"** with **"-nprd"**.

**Example URLs:**

- **Production**: `https://ofsaa.<REGION>.ocs.oraclecloud.com/<TENANT ID>-prd/dfcs`
- **Non-Production**: `https://ofsaa.<REGION>.ocs.oraclecloud.com/<TENANT ID>-nprd/dfcs`

4. **Enter Region and Tenant ID**
   Replace `<REGION>` and `<TENANT ID>` with the appropriate values to access the URLs.

   **Example URL:**

   - `https://ofsaa.useast.ocs.oraclecloud.com/byc8se-prd/dfcs (Production)`
   - `https://ofsaa.useast.ocs.oraclecloud.com/byc8se-nprd/dfcs (Non-Production)`

> **Note**
>
> Ensure you have created the application users and granted privileges to access the application instances. For more details, see Users and Access Privileges. You must share the Application URL details with your application users, which they can use to log in to the application.

6

# Users and Access Privileges

Oracle Financial Services Data Foundation Cloud Service (DFCS) for Banking Users are assigned roles through which they gain access to functions and data. Users can have any number of roles.

To create Users, login to Identity Console with Admin Privileges. For more information, see Create Application Users.

The access Privilege of a **User** is set based on the mapped group. A group represents one or more role for the user. There are pre-defined groups provided in the DFCS. You can map the newly created users to any pre-defined group, based on the user's access requirements. For more information on the list User Groups, see Identity Management.

For more information about managing users, refer to Managing Users.

## 6.1 Role Based Access Control

Role-based security in Oracle Financial Services Data Foundation Cloud Service (DFCS) Controls who can do what and to which data.

**Table 6-1 Role Based Access Control**

| Role Assigned to a User | Functions which Users with the 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 |

## 6.2 Create Application Users

After you sign into your Identity Console, your first task 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, the 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, they will receive a Welcome email. The users must activate their accounts and enter a new Password to access the services.

## 6.3 Using Identity Console (IDCS)

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

1. In the Identity Cloud Service Console, click  from the **Users** tile, to add the Application Users.
2. In the **Add User** page, enter the following information:
   - First Name
   - Last Name
   - Email Address
   - User Name

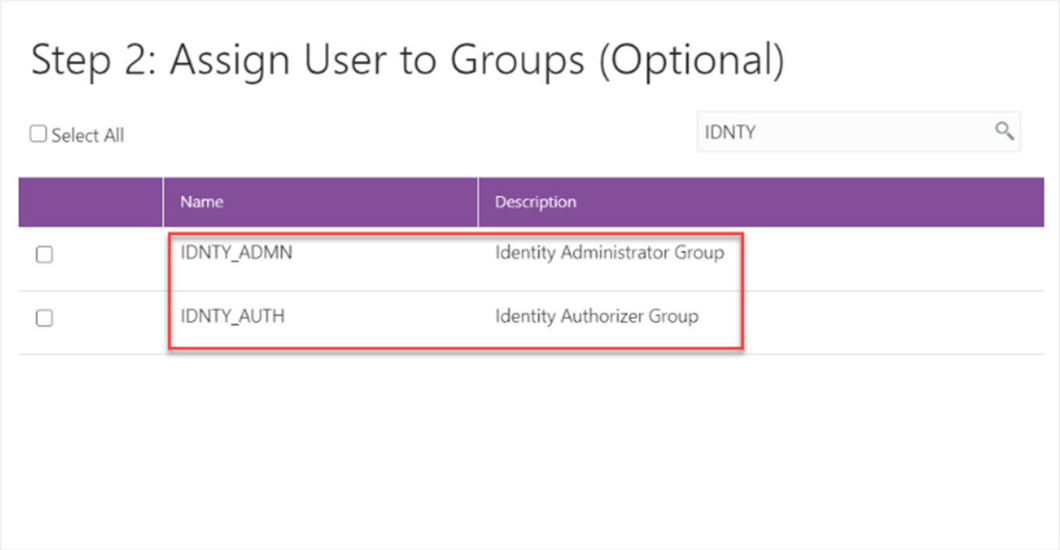
   > **Note**
   >
   > a. Email as user name is not supported. Do not select **Use the email address as the username**.
   >
   > b. Enter a maximum of 20 characters.
   >
   > c. Enter Alphanumeric Characters.
   >
   > d. Enter only Hyphen (-) and Underscore (_) Special Characters.
   >
   > e. The username is case-sensitive and must be created in lowercase letters.

3. Click **Next**.
4. In the **Assign User to Groups (Optional)** window, select the User Groups according to your user-specific groups or access.

   > **Note**
   >
   > After a user signs in to DFCS, the User to User-Group Mapping created in the IDCS 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.

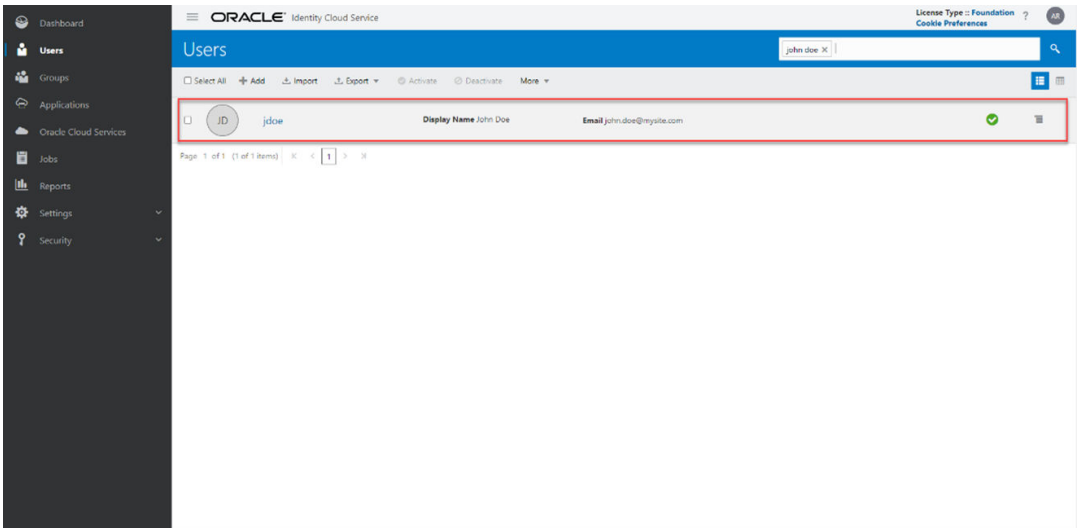
5. To create an Identity Administrator or Authorizer User, assign the users to the following:
   - **IDNTY_ADMIN**: You can use this option to create an Administrator User.
   - **IDNTY_AUTH**: You can use this option to create an Authorizer User.

**Figure 6-1 Assign User to Groups Window**



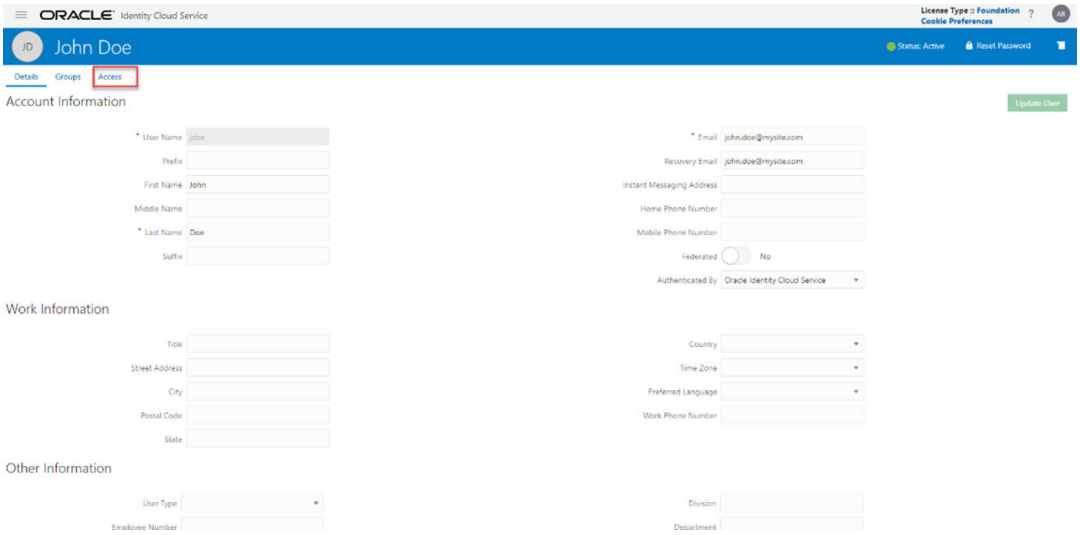

6. Click **Finish**.
   After the successful creation of the user, the added users receive an email to activate their account. The user must activate the account to use the service.
7. From the **Users** window, you can access the newly created user and edit the user details.

**Figure 6-2 Users Window**




8. Select the User that you want to edit the details. In the **User Details** Window, select the **Access** tab.

**Figure 6-3 User Details Window**




9. Click **Assign**.
10. In the **Assign Application** Window, select the appropriate Application Instance to grant access to your user as mentioned below.
    For example:
    - DFCS xxxxx-prd (For Production)
    - DFCS xxxxx-nprd1 or nprd2 (For Non-Production)

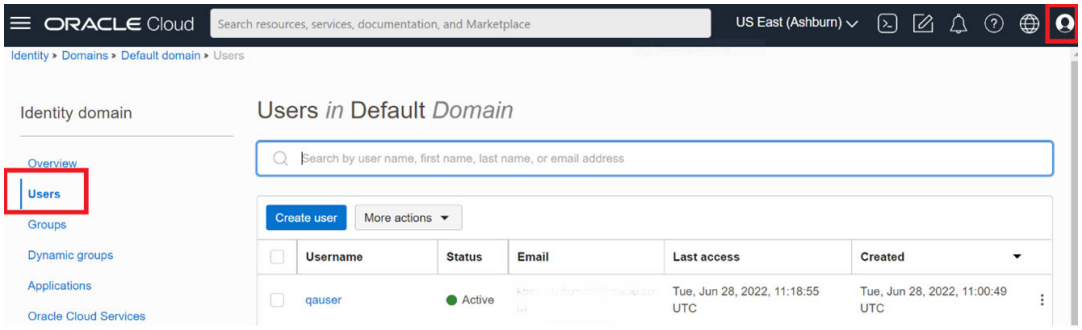
> **Note**
>
> Based on this mapping the users will be able to access the appropriate instance.

11. Click **OK**. For more information, see Create User Accounts.

# 6.4 Using Identity Domain

To create users in Identity Domain, perform the following steps:

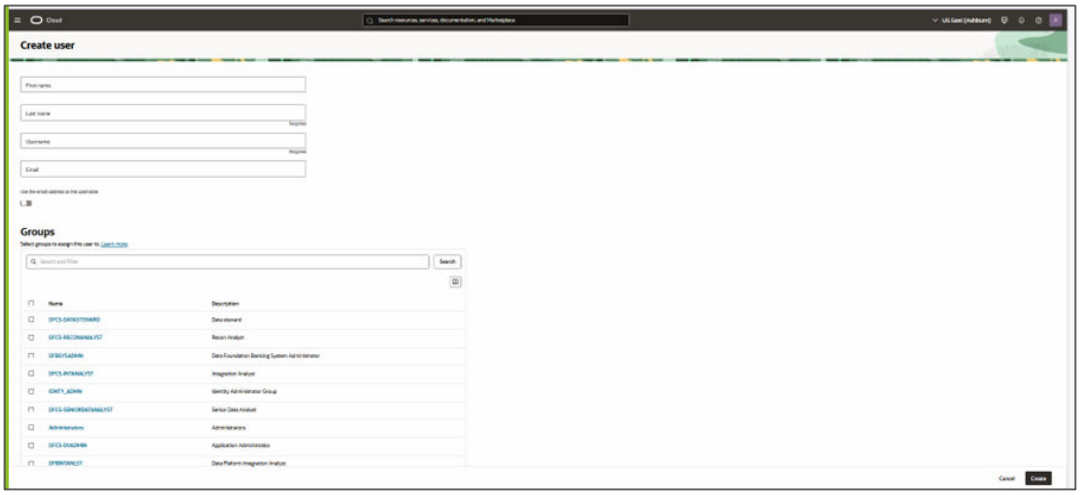
1. Click the **Profile** Icon  and select the appropriate instance.
2. From the LHS menu, select the **Users** option and click **Create user** to add the Application Users.




3. In the **Create User** page, enter the following information:
   - First Name
   - Last Name
   - Email Address
   - User Name

> **Note**
>
> a. Email as user name is not supported. Do not select **Use the email address as the username**.
>
> b. Enter a maximum of 20 characters.
>
> c. Enter Alphanumeric Characters.
>
> d. Enter only Hyphen (-) and Underscore (_) Special Characters.
>
> e. The username is case-sensitive and must be created in lowercase letters.

**Figure 6-4 Create User**




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

5. To create an Identity Administrator or Authorizer User, assign the users to the following:
   a. **IDNTY_ADMIN**: You can use this option to create an Administrator User.
   b. **IDNTY_AUTH**: You can use this option to create an Authorizer User.

**Figure 6-5 Users Mapped**

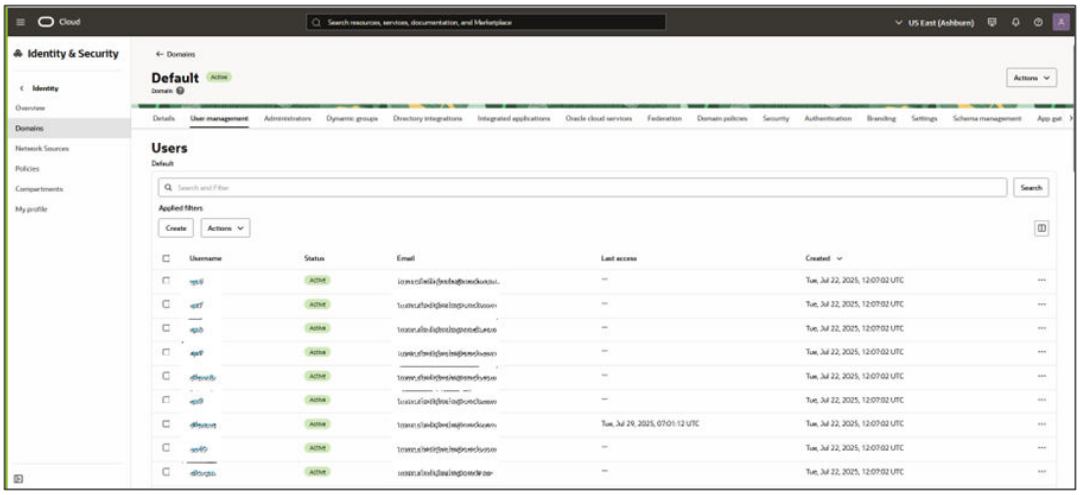
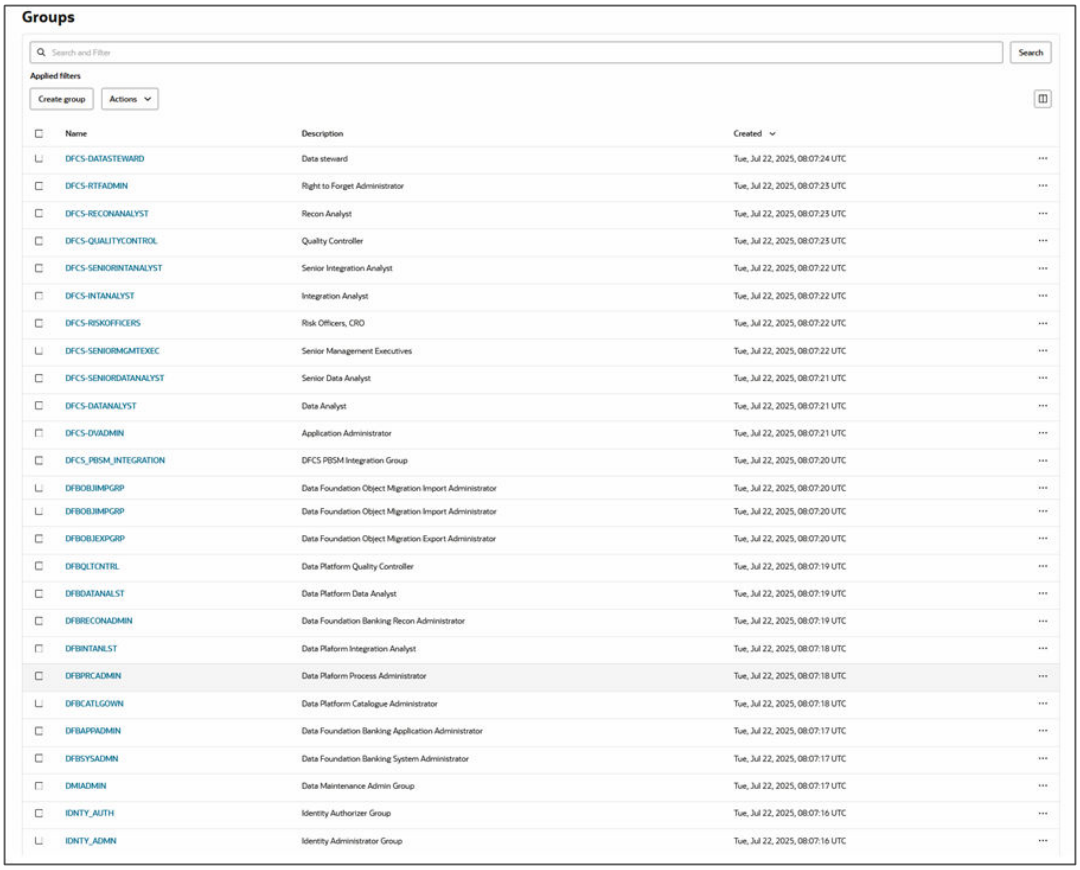



**Figure 6-6 Assign User to Groups Window**

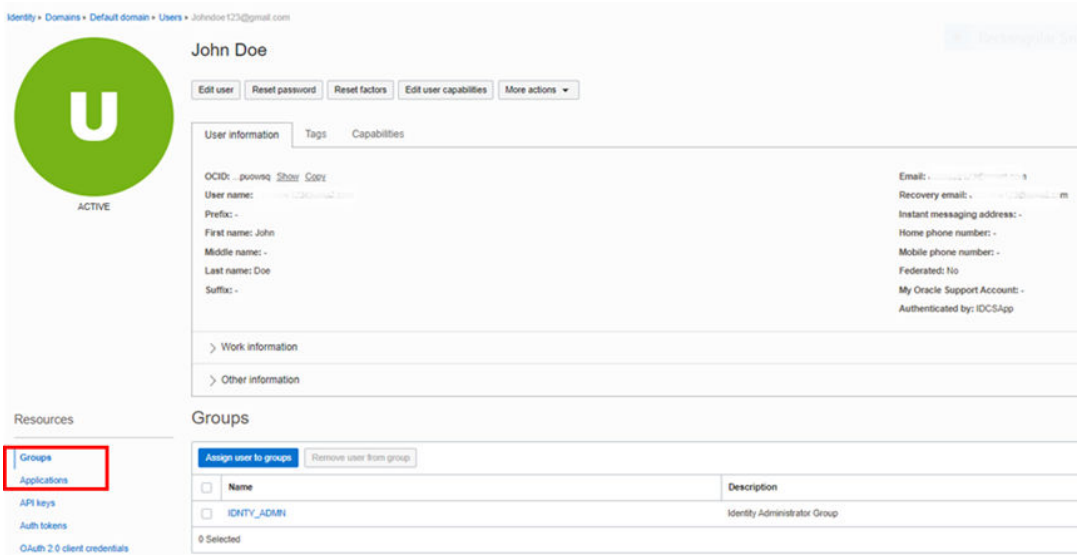



6. Click **Create**.

After the user is successfully created, they will receive an email to activate their account. The user must activate the account to use the service.

7. From the **Users** window, you can access the newly created user and edit the user details.

**Figure 6-7 User Details Window**



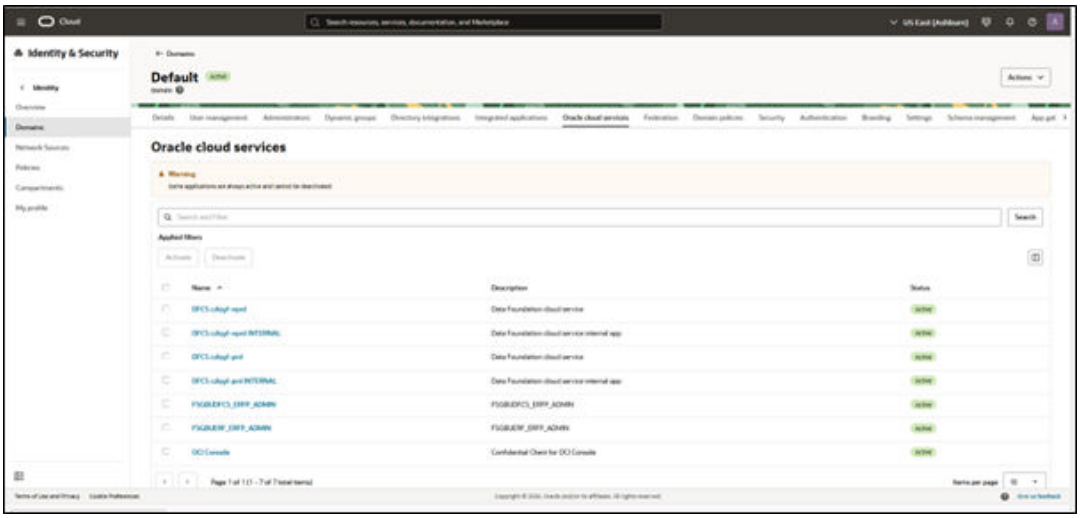

8. From the LHS menu, in the Groups section, select the required group and click **Assign user to groups**.
9. From the LHS menu, click **Oracle Cloud Services** and then select the appropriate application instance to grant access to your user as mentioned here.

   For example:

   a. DFCS xxxxx-prd (For Production)

   b. DFCS xxxxx-nprd1 or nprd2 (For Non-Production)

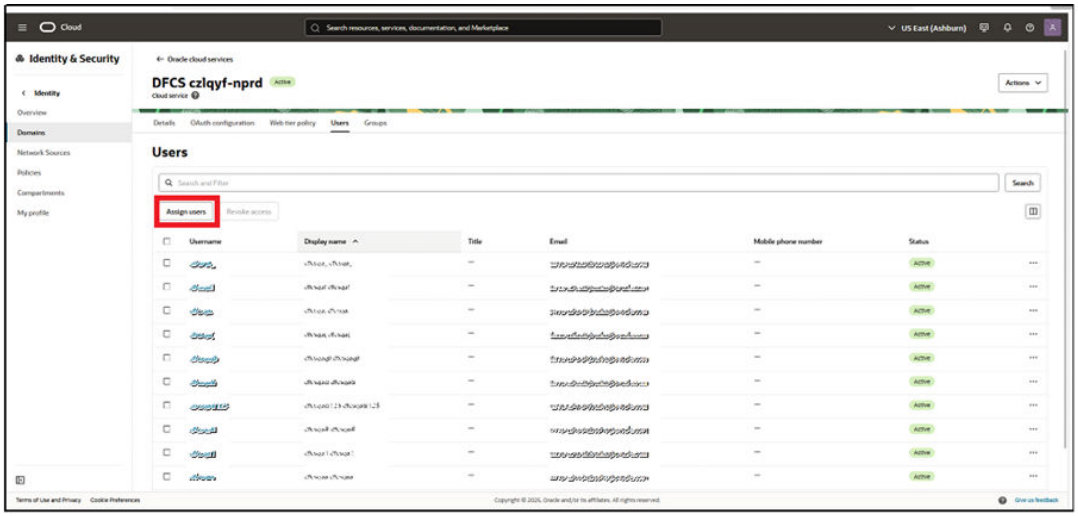
**Figure 6-8 Oracle Cloud Services**



Clicking on the application instance displays the application information.

10. In the left pane, under **Resources** group, click **Users** and select the users who needs to access the instance and click **Assign users**.

**Figure 6-9 Assign users**




> **Note**
>
> Based on this mapping, the users will be able to access the appropriate instance.

# 6.5 Domain Migration

Migration from an existing default domain to a custom domain. This provides guidelines for migrating your existing default domain and data to a custom domain.

### Managing Groups in Oracle Cloud Infrastructure (OCI)

The following steps walk you through the process of locating a domain, creating users, groups, and managing them within the OCI Console.

- **Prerequisites**
  - You must be an **Admin user** in Oracle Identity Cloud Service (IDCS).
  - A **Default Domain**should already exist.
  - Make sure you're logged into Oracle Cloud Console with the necessary permissions.

### Export Users and Groups from the Default Domain

1. Log into IDCS Console
   - Navigate to **Oracle Identity Cloud Service**.
   - Ensure you're viewing the **Default Domain**.
   - *You'll see the domain overview, including domain information, region, and status.*
2. **Export All Users**

a. Go to **Users** in the Default Domain.

b. Click **More Actions** > **Export all users**.

c. As with groups, a popup will appear – click **View Details**.

d. Download the exported user file once the job is complete.

**Note**: Groups are migrated to the domain but **not mapped** to the **tenant or users**. This must be done **manually** after import.

3. **Export All Groups**

   a. Go to **Groups** from the left menu.

   b. Click on **More Actions** > **Export all groups**.

   c. A popup message appears in the top right corner – click **View Details**.

   d. This opens a **Job Details** page: Shows Job ID, OCID (click **Show** to view), progress, success/failure count.

   e. Once complete, click **Download Exported File**. The exported file (typically in CSV format) will be downloaded to your local system.

   **Note:**

   - Export includes group names, descriptions, and other relevant metadata.
   - Failed exports (if any) will be listed with specific error details.

4. **Import Users and Groups into the Custom Domain**

5. **Navigate to the Custom Domain**

   - Go to **Oracle Cloud Console** > **Identity** > **Domains**.
   - Select your **Custom Domain**.

6. **Import Users**

   a. Go to **Users**.

   b. Click **Import Users** > **Import**.

   c. Upload the previously downloaded **user export file** from the Default Domain.

   d. Monitor the import job progress and confirm completion.

7. **Import Groups**

   a. Go to **Groups** in the Custom Domain.

   b. Click **More Actions** > **Import Groups** (if available) or use the import interface.

   c. Upload the **group export file**.

   - **Validating Group Mapping to Users**
     This section details the process for creating users after provisioning a tenant, assigning users to applications, and handling password resets post domain migration.

     > **Note**
     >
     > Verify that all required groups are assigned to the specified user.

     a. Once the tenant has been provisioned, use the search bar to locate the Tenant ID that was recently created.

b. Click on the **Tenant ID** to open the application information window.

c. In the application information window, click on Users.

d. Click **Assign Users**.

> **Note**
>
> Group mapping will be done automatically.

e. After users are assigned, the Application URL will appear in the corresponding field.

f. Click on the assigned User.

g. **Domain Migration and Password Reset**: The user will receive a notification to reset their password. The email will contain a password reset link.

> **Note**
>
> Password reset is triggered automatically once the domain is migrated from the default domain to the custom domain.

8. **Final Validation**

- Go to **Custom Domain > Users** and **Groups**.
- Validate:
  - All users appear as expected.
  - All groups have been imported.
  - Users are assigned to the correct groups (if manually done).
- Check the new tenant association if applicable via Oracle Cloud Services.

7

# 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's 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 up in separate windows or tabs.

**Table 7-1 Configuring Session Timeout**

| Timeout Type | Description | Configurable | Timeout Duration |
|---|---|---|---|
| Session Lifetime Timeout | Once 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.<br>Your session ends after this period, even if you're using the application. | Yes | 8 Hours (Default value) |
| 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 | Yes | Min 5 Minutes - Max 480 Minutes |

## 7.1 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.

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**.
4. Enter the required value. By default, this is set to 480 Minutes.


# 7.2 How to Configure Browser Inactivity Timeout

You can configure the Browser Inactivity Timeout using DFCS application. You need to have the System Administrator Role mapped to you, to access and modify the settings.

1. Log in into the DFCS application.
2. On the **DFCS Home** page, navigate to the **My Profile** and select **System Preferences**.

   The System Preferences page is displayed.
3. Enter the **Browser Inactivity Timeout** value, ranging between 5 minutes and 480 minutes.
4. Click **Save**.

8

# Get the OAuth Client ID and Client Secret from IDCS

This section walks you through the steps to obtain the **OAuth Client ID and Client Secret** from Oracle Identity Cloud Service (IDCS) console.

An OAuth Cliend ID and Client secret are required to generate an access token.

To get the OAuth Client ID and Client Secret:

1. Enter the **Oracle Identity and Access Management (IAM)** URL in the browser's Address bar to access the **Oracle Cloud Account Sign In** page.
2. Log in to **IAM** portal.
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, select the required Cloud Service (in **<Cloud_service_name> <tenant-id>** format) from the list. For example, the cloud service name - **AMLCS tenant-prd**
6. Click the **Configuration** tab.

   > **Note**
   >
   > 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. Proceed to generate the access token.

For more information, see REST APIs for Data Foundation Cloud Service.

# 9 FAQs

This section lists the Frequently Asked Questions (FAQs).

1. What are the Cloud Offerings from Oracle?
   Oracle Cloud offers best-in-class services across Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
2. What are the Cloud Services available?
   You can see the Website to see the Cloud Services available.
3. What are the Supported Browsers for the DFCS?
   The following are the Supported Browsers for the DFCS:
   - Google Chrome
   - Microsoft Edge
   - Mozilla Firefox
4. How and where can I place my Order for Oracle Financial Services Data Foundation Cloud Service?
   You can place your order on the Oracle Cloud website. Review the Order Oracle Cloud Applications topic to know more.
5. How can I activate my cloud account after I purchased the Oracle Financial Services Data Foundation Cloud Service?
   If you are a new Oracle Cloud Applications user, you'll likely receive a Welcome email after your order is processed. You'll receive a *Welcome to Oracle Cloud email* that asks you to activate your cloud account.