Oracle® Financial Services Climate Change Analytics Cloud Service

Getting Started with Oracle Cloud

Release 23C
F88934-01
January 2024

Oracle Financial Services Climate Change Analytics Cloud Service Getting Started with Oracle Cloud, Release 23C

F88934-01

Contents

6 User Management

7 Configuring Session Timeout

1

About This Content

This guide provides information on the newly released Oracle Financial Services Climate Change Analytics Cloud Service (OFS CCA CS).

Audience

This document is intended for users of the Oracle Financial Services Climate Change Analytics Cloud Service (OFS CCA CS) application.

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

See these Oracle resources:

- Getting Started with Oracle Cloud
- Admin Console User Guide
- OFS Climate Change Analytics Cloud Service User Guide

Conventions

The following text conventions are used in this document.

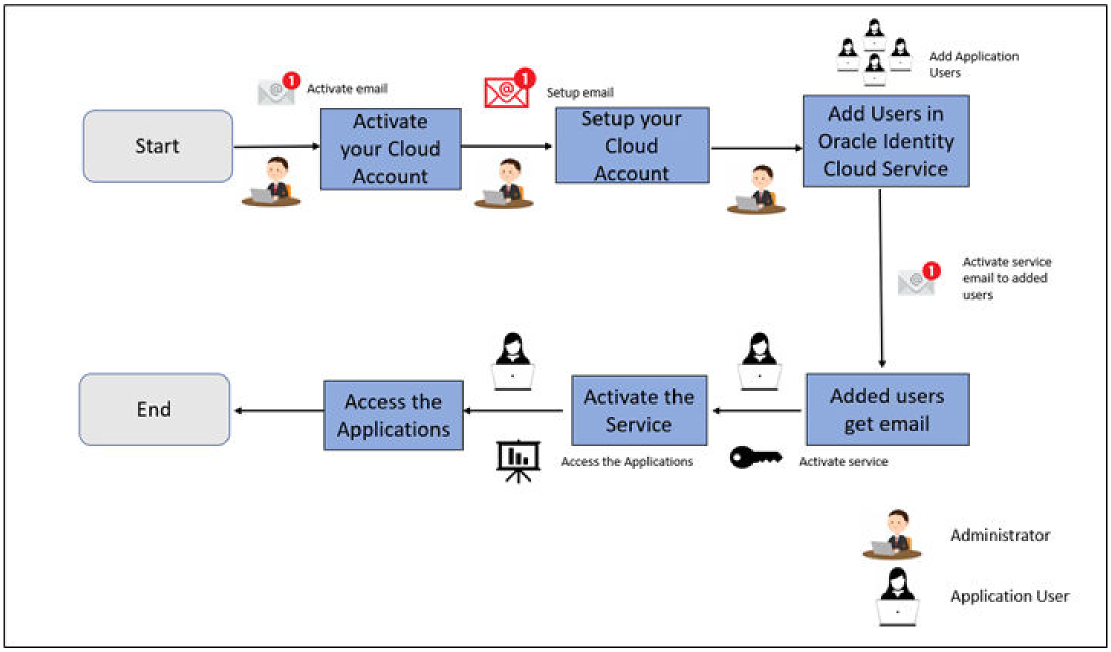
Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates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

2

Get 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 with details to create and activate your Cloud Account.

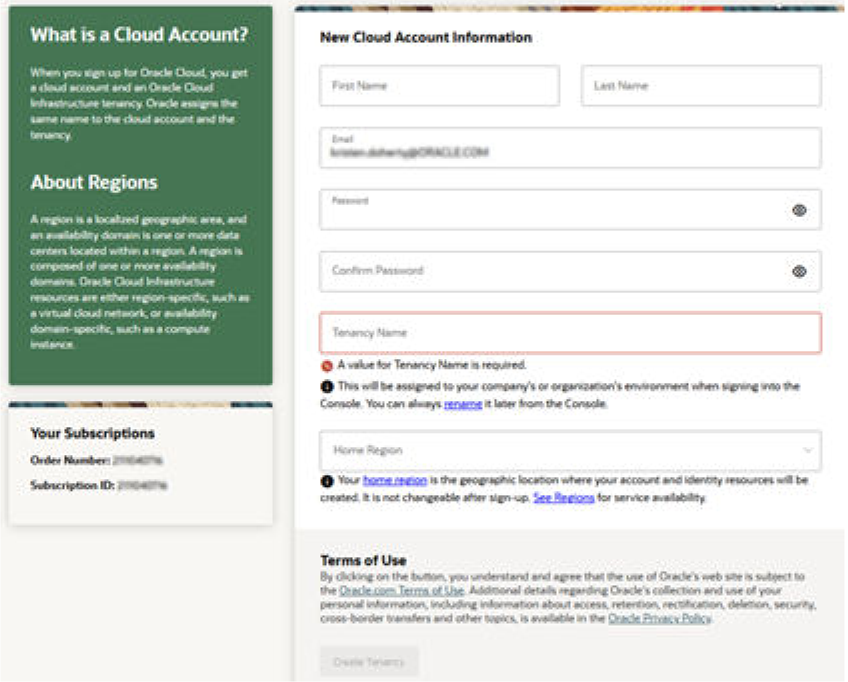
> **Note:**
>
> You must be an Administrator to create and activate the Cloud account.

Once the Cloud account is created and activated, you will receive an activation email with the sign-in details and steps to use your Cloud applications.

To create and activate a new Cloud Account:

1. Click **Create New Cloud Account** in the email.
2. Complete the **New Cloud Account Information** to sign up.

Figure 2-2 New Cloud Account Information page



What is a Cloud Account?

When you sign up for Oracle Cloud, you get a cloud account and an Oracle Cloud Infrastructure tenancy. Oracle assigns the same name to the cloud account and the tenancy.

About Regions

A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Oracle Cloud Infrastructure resources are either region-specific, such as a virtual cloud network, or availability domain-specific, such as a compute instance.

Your Subscriptions

Order Number: [redacted]

Subscription ID: [redacted]

New Cloud Account Information

First Name

Last Name

Email: [redacted]

Password

Confirm Password

Tenancy Name

A value for Tenancy Name is required.

This will be assigned to your company's or organization's environment when signing into the Console. You can always rename it later from the Console.

Home Region

Your home region is the geographic location where your account and identity resources will be created. It is not changeable after sign-up. See Regions for service availability.

Terms of Use

By clicking on the button, you understand and agree that the use of Oracle's web site is subject to the Oracle.com Terms of Use. Additional details regarding Oracle's collection and use of your personal information, including information about access, retention, rectification, deletion, security, cross-border transfers and other topics, is available in the Oracle Privacy Policy.

3. Enter the following details:
   - **First Name** and the **Last Name**.
   - **Email**: Provide the same email address to which the Welcome email was sent. Instructions to log into the new Oracle Cloud Account will be sent to this email address.
   - **Password** to access the New Cloud Account, after the account is activated and an activation email is sent to the specific email address.

   - **Tenancy Name**: New **Tenancy Name** to be associated with the Cloud Account.
   - **Home Region**: Select the **Home Region**, where the Identity Resources and Account are located. Check the service availability before selecting the Home Region.

4. Click **Create Tenancy** to access the **New Cloud Creation Confirmation** page.

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

Add to an Existing Oracle Cloud Account

If you already have a Cloud Account associated with your Administrator user name, you can always add another Cloud Service, if required.

To add an existing Cloud account:

1. In the Welcome email, click **Add** to add an existing cloud account.
2. Perform the steps as mentioned in the Access the Oracle Identity Cloud Service Console section.

Accessing the Cloud Account

An Administrator can access the Cloud Account activated and associated with their email address.

After your new cloud account is created and activated, you will receive a **Setup Complete** email, to the email address provided while creating the account.

To access your Cloud account:

1. In the **Setup Complete** email, click **Sign In** and enter the **Username** and **Password** to access the **Oracle Cloud Console URL**, to log in to the Console. Use the same **Username** and the **Password** that you provided during activation setup.
2. Reset the **Password**.
3. Log in again to the **Oracle Cloud Infrastructure Classic Console** with the new credentials.

   You can now access the subscribed Oracle Cloud applications.

Create an Environment

After logging into the Oracle Cloud Infrastructure Classic Console, you can create one or multiple instances that can be used by different user groups.

To create an instance, follow these steps:

1. Log into Oracle Cloud Infrastructure Classic Console.
   Under **My Applications**, you will see the list of environments (instances) provisioned for the one or mutliple cloud applications. The following details are provided for each environent:
   - **Name**: The given name to the cloud application's instance.
   - **Type**: The type of the instance.
   - **Lifecycle status**: The status of the instance.
   - **Region**: The region from where this instance is active.

- **Application URL**: The URL to access the instance.

2. To create a new environment, click **Create environment**.
   This screen displays a list of Cloud Services to which the customer has subscribed and the Region from where these services are operated.

   > **Note:**
   >
   > If **Region** selection drop-down is displayed, then you must select the appropriate Region as follows.
   >
   > - US East (Ashburn) for United States of America
   > - Japan East (Tokyo) for Japan
   > - Australia east (Sydney) for Australia

   If you are not sure about the Region, contact My Oracle Support (MoS).

3. Under **Environment Details**, enter the following information:
   - **Name**: The name of the new environment or instance.
   - **Instance type**: Select from the following options:
     - **Production**: An environment that will be tagged as Production and can be used for Production activities.
     - **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.
   - **Admin email**: The email ID with which you have logged into the Cloud Console. You can also enter a different email ID that needs to be 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.

4. Click **Create**.
   The environment details are added to the Oracle Cloud Infrastructure Classic Console under the **Environments** tab (visible in the LHS menu). It may take a few hours for the State to change to Active. If there are any issues, you can raise a service ticket with My Oracle Support (MoS) .

After the environment becomes active i.e., the **State** column displays Active, you can click on name link to open the **Environment details** page, and view the details. Under **Environmant Information**, click the Service console URL to create users and groups.

Post Provisioning Step

After you have created the environment, log in as an admin user and perform the following steps:

1. Log in to the **Admin Console**.
2. Click the **Identity Management** tab on the **Admin Console** page.
3. Click the Folders tile to open the **Folders Summary** page.
4. Create a folder by adding the **Folder ID** as *DEFAULT* .

5. Add a name and select a type for the folder in the **Folder Name** and **Folder Type** fields.
6. After creating the default folder, you can view the folder on the **Hierarchy Summary** page.

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

To access the **IAM** Console:

1. Browse 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. Select the **Identity domain** from the drop-down list and click **Next**, to access the **IAM Login** page.
5. Log in with your **Username** and **Password**.

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

An Application User is provisioned by their Administrator, and can use the specific subscribed cloud services.

When an Administrator completes provisioning an application user, they will receive an Account Activation email.

To login and activate your application user account:

1. Open the email received from Oracle Cloud and review the information about your service in the email.

2. Click **Activate Your Account**. You will be prompted to change your password on the initial login.
3. Enter your new credentials in the **Reset Password** window to activate your account. After the password is successfully reset, a **Congratulations** message is displayed.
4. Access the Application URL shared by the Administrator.
5. Enter your credentials to sign in to your account. The Welcome page is displayed.

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).

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 the 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 the Oracle Platform as a Service (PaaS) offering 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 the Oracle Software as a Service (SaaS) offering 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 Google Chrome, Microsoft Edge and Mozilla Firefox.

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

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 **Oracle Financial Services Climate Change Analytics Cloud Service**.
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**.

4 Users and Roles

A brief description of users, roles, groups and functions.

- **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. You can map the groups to roles using the subscribed Cloud Service.
  - **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 use the existing functions.

User Summary- Application Users

View the list of existing application users in the User Summary.

You can view the details of a user and map the user to one or more User Groups.

- To view the **User ID** and **Username** of the selected User - Select the **Username** in the **User Summary** page and select **Details**.
- To search for a specific User, type the first few letters of the required **Username** in the **Search** box and click **Search**.

Navigation Control

- Using the navigation buttons at the bottom of the summary page, you can browse to the 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 or decrease the number of entries.
- Enter the page number in the **View Bar Control** and jump to the required page.

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:

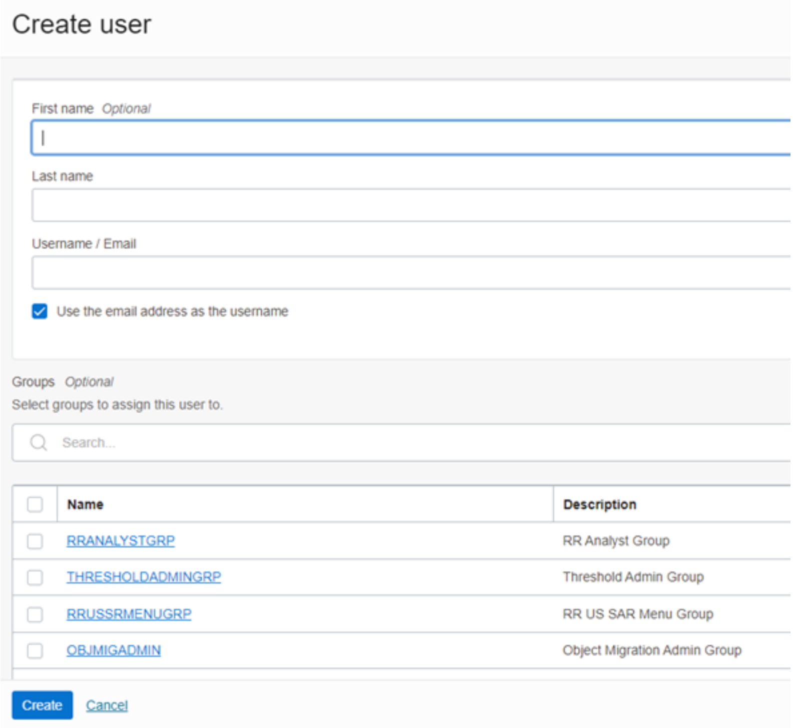
   - Leave the **Use the email address as the username** check box selected.
   - In the **Username / Email** field, enter the email address for the user account.

   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 4-1 Add User Details



Create user

First name *Optional*

Last name

Username / Email

☑ Use the email address as the username

Groups *Optional*

Select groups to assign this user to.

Search...

□	Name	Description
□	RRANALYSTGRP	RR Analyst Group
□	THRESHOLDADMINGRP	Threshold Admin Group
□	RRUSSRMENUGRP	RR US SAR Menu Group
□	OBJMIGADMIN	Object Migration Admin Group

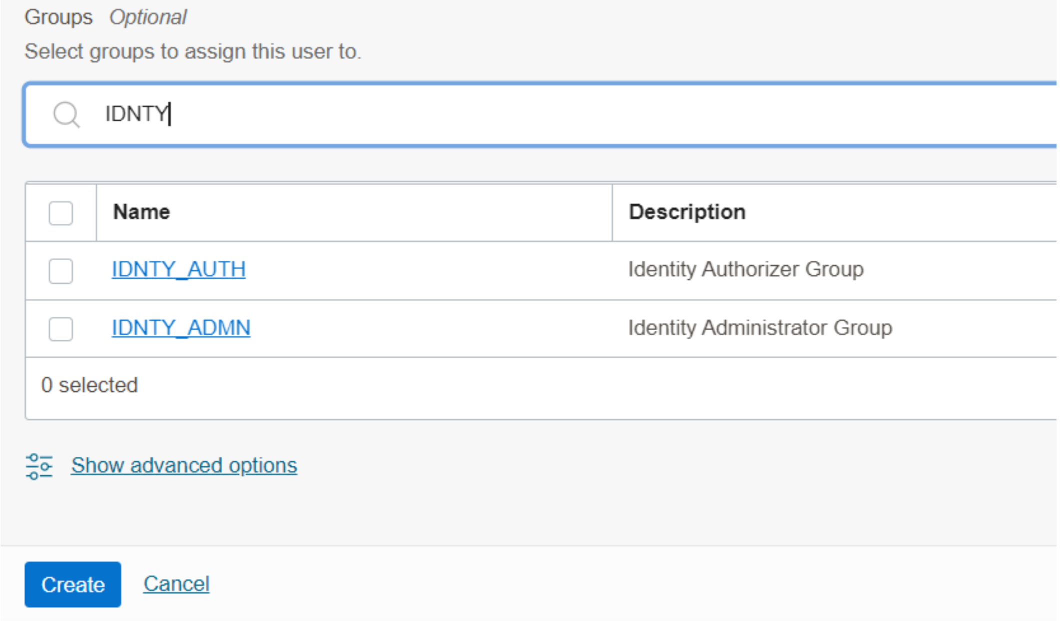
> **Note:**
>
> Ensure that you restrict the User Name to the following:
>
> a. Do not enter your Email ID as the Username and do not select the **Use the email address as the username** check box.
>
> b. Enter a maximum of 20 characters.
>
> c. Enter Alphanumeric Characters.
>
> d. Enter only Hyphen (-) 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 OFS CCA 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 4-2 Assign Users to Groups Window



Groups *Optional*

Select groups to assign this user to.

IDNTY

□	Name	Description
□	IDNTY_AUTH	Identity Authorizer Group
□	IDNTY_ADMN	Identity Administrator Group

0 selected

6. Click **Create**.

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

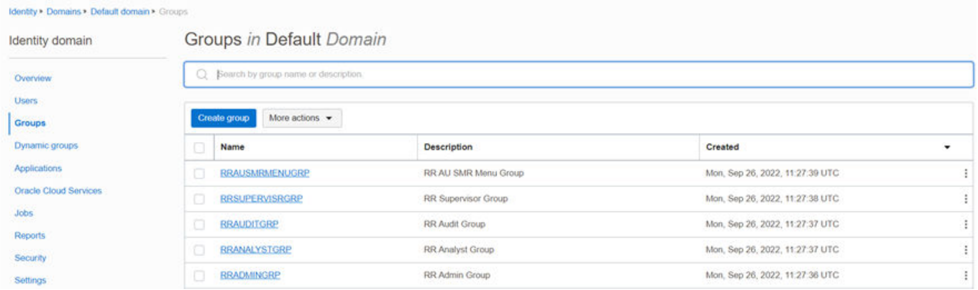
Create a User Group

Create groups to manage user access to applications and resources.

To create a User Group in IAM Console:

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

Figure 4-3 Identity Domain



Groups *in* Default *Domain*

□	Name	Description	Created
□	RRAUSMRMENUGRP	RR AU SMR Menu Group	Mon, Sep 26, 2022, 11:27:39 UTC
□	RRSUPERVISRGRP	RR Supervisor Group	Mon, Sep 26, 2022, 11:27:38 UTC
□	RRAUDITGRP	RR Audit Group	Mon, Sep 26, 2022, 11:27:37 UTC
□	RRANALYSTGRP	RR Analyst Group	Mon, Sep 26, 2022, 11:27:37 UTC
□	RRADMINGRP	RR Admin Group	Mon, Sep 26, 2022, 11:27:36 UTC

3. Enter the **Group Name** (mandatory) and the **Group Description**.
4. Select **User can request access**, to allow users to request access to this group.
5. Check the check box adjacent to each user to add that user to the group.
6. Click **Create** to create the new user group with the selected users.

After creating the user group, you must assign various permissions to the group, using one of the following methods:

- Write at least one policy to give group permission to either the tenancy or a compartment. While writing the policy, specify the group using the unique group name or the group's OCID.
- Assign the group to an application.

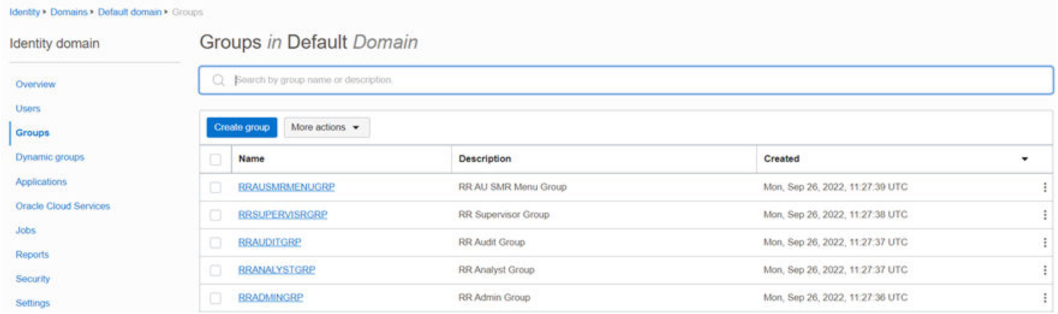
Add User to Group

Add a user to the required group, based on the roles required for the user.

To add a User to Group in IAM Console:

1. In the IAM Console, click the **Profile** and select **Identity domain: Default** 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 4-4   Groups in Default Domain



Groups *in* Default *Domain*

□	Name	Description	Created
□	RRAUSMRMENUGRP	RR AU SMR Menu Group	Mon, Sep 26, 2022, 11:27:39 UTC
□	RRSUPERVISRGRP	RR Supervisor Group	Mon, Sep 26, 2022, 11:27:38 UTC
□	RRAUDITGRP	RR Audit Group	Mon, Sep 26, 2022, 11:27:37 UTC
□	RRANALYSTGRP	RR Analyst Group	Mon, Sep 26, 2022, 11:27:37 UTC
□	RRADMINGRP	RR Admin Group	Mon, Sep 26, 2022, 11:27:36 UTC

3. Click **Assign User to Groups** to view the list of available users.
4. Check the check box adjacent to each user, to add that user to the group.
5. After selecting all the required users, click **Add**.

Import Application Users

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

> **Note:**
>
> Before importing the user accounts, create a .CSV file that is properly formatted for the import process.

To import user accounts:

1. In the IAM Console left pane, click **Users** and select **More Actions** and select **Import Users**.
2. Click **Browse** to locate and select the .CSV file containing the user accounts to import.

   > **Note:**
   >
   > Click **Download sample file** in the dialog box to download a sample file and perform the accounts upload.

3. Verify that the path and name of the selected .CSV is updated in the **Select a file to import**, and click **Import**.

   > **Note:**
   >
   > Oracle Identity Cloud Service cannot import a user account if a mandatory value such as user's first name, last name, or Username, is missing. In such cases, Oracle Identity Cloud Service will skip the incomplete account and proceed to the next account in the .CSV file.

When Oracle Identity Cloud Service evaluates and imports the User Accounts, the imported accounts are updated in the **Jobs**. You can also get information related to the successful/incomplete imports if the import was not completed due to system errors.

5
User Groups

User Groups are seeded (available out-of-the-box) by the Cloud Service. Groups are mapped to roles using the Cloud Service by the same user that was created using IAM.

Customers can also create new groups in IAM. After groups are created, they are synced from IAM to the Cloud Service.

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 the Cloud Services you are subscribed to like, **CCACS xxxx-prd** and **CCACS xxxx-nprd**.

   Where **Description** is mentioned as OFS CCA Cloud Service.
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 the Cloud Services you are subscribed to like, **CCACS xxxx-prd** and **CCACS xxxx-nprd**

   Where **Description** is mentioned as OFS CCA Cloud Service.
4. From the LHS menu, select **Groups**.
5. Click **Assign Groups**, and then select the relevant **Group**.
6. Click **Assign**.

Map Users to Groups

Log in to IAM as an administrator, and map users to user groups.

To map a user to a user group:

1. Select the **User Name** in the **Users Summary**.
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, refer to Unmap User from Group.

> **Note:**
>
> User-Group mapping changes from IAM 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 IAM 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**.

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

Unmap a user from a specific group to revoke the associated functions

Log in to IAM as an administrator to authorize and unmap a user from a specific user group.

To authorize the unmapping of a user from a user group:

1. Click **Unmapped Groups**.
2. Click the **User Group Name** to select the User Group.
3. Click **Authorize** or **Reject** to approve or reject an unmapping request.

Map Roles to User Group

You can map roles to an User group using Admin Console.

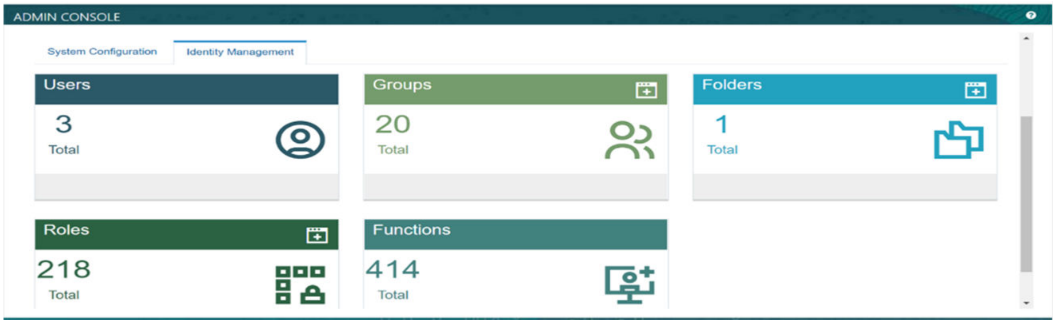
To map Roles to the User Group:

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

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

2. Navigate to **Identity management**.

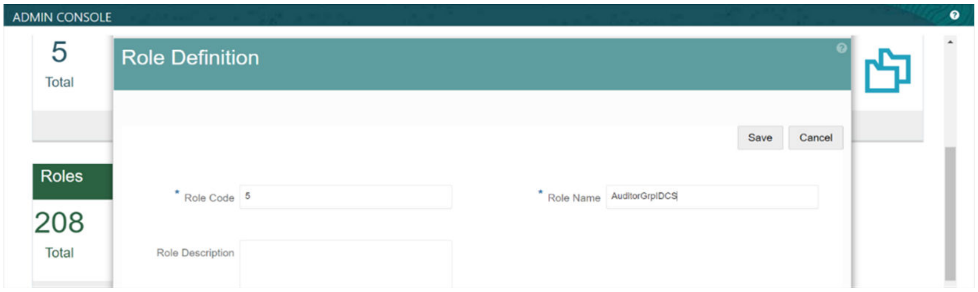
Figure 5-1 Admin Console



3. Click **Roles** tile to access **Roles Management**.
4. Click **Add** to view **Add Roles**.

5. Enter the unique **Role Code**, **Role Name** and save the definition.

Figure 5-2 Admin Console

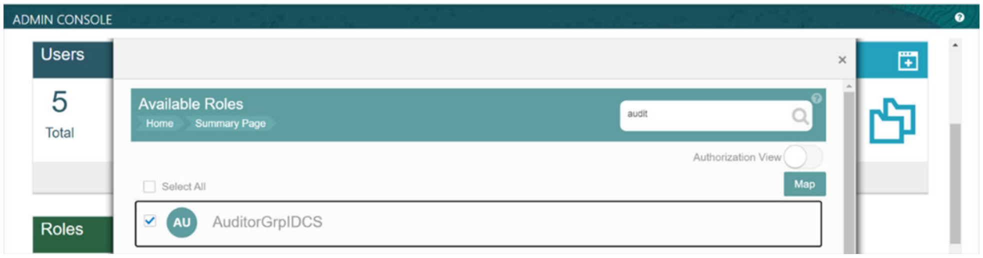


* Role Code 5

* Role Name AuditorGrpIDCS

6. From the **Identity Management** tab, Click **Groups** to access the **Groups Management** page.
7. Search for the specific group created in IAM Portal.
8. Click the **User Group** and click **New Mapping** under the **Mapped Roles** tab.
9. Search for required role names created in **Roles Management** and click **New Mapping** to map each role.

Figure 5-3 Admin Console



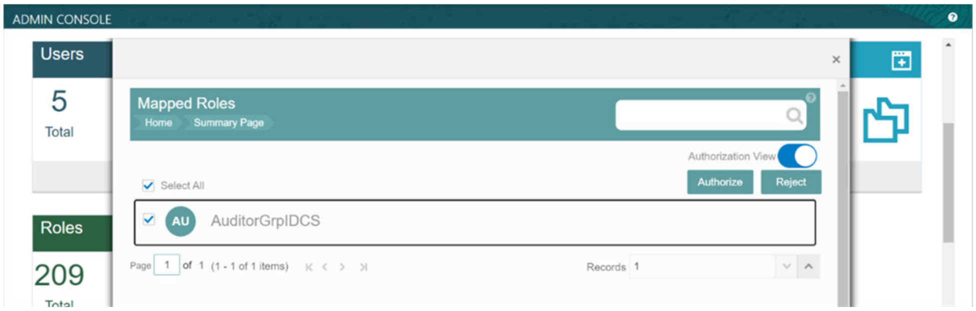
audit

□ Select All

☑ AU AuditorGrpIDCS

10. Log in as a user with Authorization role and authorize the mapped roles in the **Authorization View**

Figure 5-4 Admin Console



☑ Select All

☑ AU AuditorGrpIDCS

Page 1 of 1 (1 - 1 of 1 items)

Records 1

A User group created in IAM Portal and mapped to a Role created in the Admin Console.

6

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 Climate Change Analytics Cloud Service (OFS CCA CS) Users are assigned roles through which they gain access to functions and data. Users can have any number of roles.

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

Table 6-1 User Roles and Privileges

IDCS Administrator	Identity Administrator	Identity Authorizer	Application Users
Create User	Map Users to OOB User Groups	Manage Authorization	Manage OFS CCA CS
Map Users to OOB User Groups	Create User Groups and Roles		Set up Dimensions, Rules, Assumptions, and Processes
Create User Groups	Map Users to User Groups		Execute Processes
	Map Roles to User Group		Generate Reports
	Map Functions to Roles		Review and Analysis Reports

Role Based Access Control

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

The following table provides examples of role-based access.

Table 6-2 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 Oracle Financial Services Climate Change Analytics Cloud Service to facilitate the activities expected from the users mapped to the seeded User Groups:

- CCA Administrator User Group
- CCA Analyst User Group
- CCA Auditor User Group
- CCA Approver User Group

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

The user roles CCA Admin, CCA Analyst, CCA Auditor, and CCA Approver User Group 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 OFS CCA CS Screens and Edit-specific Screens. Similarly, an Admin Persona can view and edit all OFS CCA CS 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 User Groups and Activities table.

User Groups and Activities

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

Table 6-3 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

Table 6-3 (Cont.) User Groups and Activities

User Groups	Activities
CCA Analyst User Group	• Data Management: Metadata and Data Loaders • Schedule Batch Processes
CCA Auditor User Group	• View privileges for all application-specific modules: • Review/Analyze Results • Review Process Logs • View Reports
CCA Administrator User Group	• Set User and Application Preferences • Set Setup Parameters • Currency and Rate Management • Dimension Management
CCA Approver User Group	• Emissions Calculator • Data Model Interface • Data Model Extension • Data Quality Framework

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 6-4 User Group and User Role Mapping

User Group	Mapped User Role
CCA Administrator User Group	CCA Admin
CCA Analyst User Group	CCA Analyst
CCA Auditor User Group	CCA Auditor
CCA Approver User Group	CCA Approver

7 Configuring Session Timeout

Session timeout automatically signs you out of a logged in session after a set time period, for various reasons such as inactive session for a specific time frame.

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

When you sign in using your credentials, you are authenticated to use the application, and a session is established. 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 an inactive session for a specific time period. In such cases, you are 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 user portal/tabs that open in separate windows or tabs.

The various session timeouts and the configuration details are as follows:

Timeout Type	Description	Configurable	Timeout Duration
Session Lifetime Timeout	After authenticating to the application, your current 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	After authenticating to the application, if your session is idle or inactive for a specific time, the System automatically terminates the session, and you are signed out of the session.	No	60 Minutes

Timeout Type	Description	Configurable	Timeout Duration
Browser Inactivity Timeout	After authenticating to the application, if your browser session is idle or inactive for a specific time, the System automatically terminates the session, and you are signed out of the session.	No	60 Minutes

How to configure Session Lifetime Timeout?

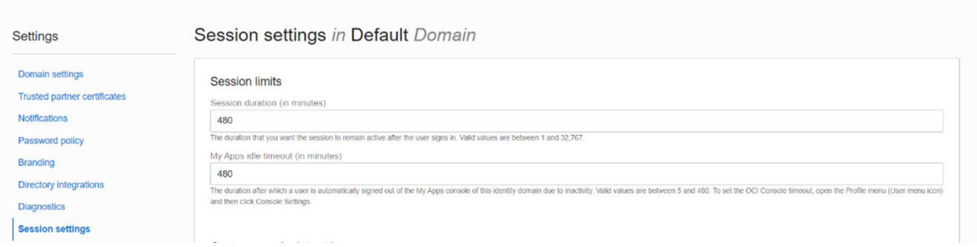
You can configure the Session Lifetime Timeout using your Identity Domain Settings in OCI Console.

Ensure that you have the Security Administrator Role mapped to access and modify the settings.

To configure the session timeout:

1. Log in 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 7-1 Session Settings



Session settings *in* Default *Domain*

Session limits

Session duration (in minutes)

480

The duration that you want the session to remain active after the user signs in. Valid values are between 1 and 32,767.

My Apps idle timeout (in minutes)

480

The duration after which a user is automatically signed out of the My Apps console of this identity domain due to inactivity. Valid values are between 5 and 480. To set the OCI Console timeout, open the Profile menu (User menu icon) and then click Console Settings.