Oracle Financial Services

Crime and Compliance Management Cloud Service - Get Started

26.02.01
G51796-01
February 2026

Oracle Financial Services Crime and Compliance Management Cloud Service - Get Started, 26.02.01

G51796-01

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 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 - Oracle AML and Financial Crime Compliance Management—Transaction Monitoring.
2. Scroll down and select the Cloud Service that you are subscribed to.
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 and click **Request Now**.

After your interaction with the Oracle Sales team to order the Oracle Cloud Application best suited to your requirements, you will receive an email with a link to activate the service you have ordered.

2

Getting Started with your Cloud Service

To get started, you must activate the subscribed Cloud Service.

After activating the cloud service, you can log in as an administrator and perform the following tasks.

- Create and Activate New Cloud Account
- Access the Cloud Account
- Access Oracle Identity and Access Management (IAM) Console
- Onboard new application users for the subscribed cloud services.

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.

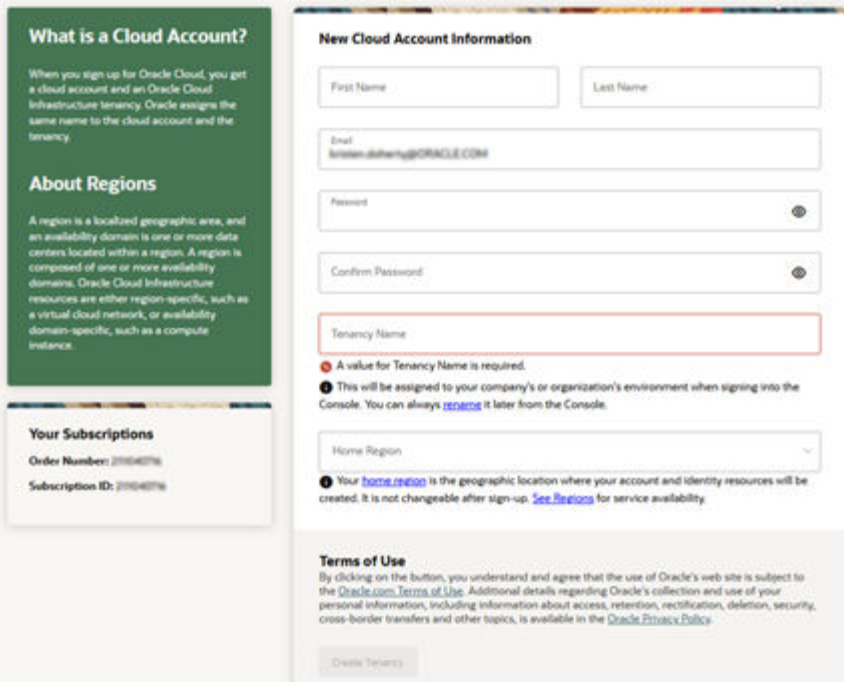
Create and Activate New Cloud Account

After you subscribe to the cloud service, you will receive a **Welcome to Oracle Cloud** email with details to create and activate your cloud account.

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 2-1 New Cloud Account Information page



3. Enter the following details:
   - **First Name** and the **Last Name** of the person who will be the cloud administrator.
   - **Email** address of the person who will be the cloud administrator. Instructions to log into the new Oracle Cloud Account will be sent to this email address.
   - **Password** to access the new cloud account.
   - **Tenancy Name**: New **Tenancy Name** to be associated with the cloud account.

     > **Note**
     >
     > You cannot modify the tenancy name after it is created. Hence, ensure to provide a valid tenancy name, based on your organization's requirements and naming conventions.

   - **Home Region**: Select the **Home Region**, where the account is located. Check the service availability before selecting the home region.
     For assistance regarding home region selection, contact Oracle support. Existing customers have to ensure that the identity resources are located in the home region.

     > **Note**
     >
     > You can subscribe to additional regions but you cannot modify the home region, after provisioning your tenancy.

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

   After successful activation, the cloud account administrator will receive a **Get Started Now with Oracle Cloud** email.

Add to an Existing Oracle Cloud Account

If you already have a cloud account associated with your administrator user name, you can add the newly subscribed cloud service to that account.

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 Cloud Infrastructure Identity and Access Management (IAM) console.

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 **Get Started Now with Oracle Cloud** email, to the email address provided while creating the account.

To access your Cloud account:

1. In the **Get Started Now with Oracle Cloud** email, click **Sign In**.
2. Enter the **Tenancy** name and click **Continue**.
3. Enter the **Username** and **Password** to log in to the **OCI Console** .

   Use the same **Username** and the **Password** that you provided during activation setup.
4. After successful login, proceed with the multi-factor authentication. Select the configured authentication mode and enter the OTP generated using the Oracle Mobile Authenticator application.

   Once the MFA is successfully completed, you can access the **Environment Page**.

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.

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.

Create an Environment

After logging into the Oracle Cloud Infrastructure Console, an Administrator can create one or multiple environments/instances for different user groups.

To create an environment/instance:

1. Log in to **Oracle Cloud Infrastructure Console** (OCI).

   You can view the list of all the environments (instances) provisioned for the one or multiple cloud applications, with the following details:

   - **Name**: The cloud application's instance name.

- **Type**: The instance type.
- **Life cycle status**: The instance status.
- **Region**: The region from where the specific instance is active.
- **Application URL**: The URL to access the instance.

2. From **My Applications**, click the application in which you want to create an environment. Example: Oracle Financial Services Crime and Compliance Management Anti Money Laundering.
3. On the **Overview** page, click **Environments**.
4. From the **Compartments** drop-down list, select the compartment in which you want to create an environment.
5. Click **Create**, to access the list of cloud services to which the customer has subscribed and the region from where these services are operated.
6. (Optional). Select the **Region** to host the OCI environment/instance, from the drop-down list.

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

   > **Note**
   >
   > You can select the region only for the first environment/subscription and for the additionally added instances, the region cannot be modified.

7. Enter the following **Environment Details**, and click **Create**.
   - **Name**: The name of the new environment or instance.

     > **Note**
     >
     > You cannot modify the environment name after the environment is created. Hence, ensure to provide a valid environment name, based on your organization's requirements and naming conventions.

   - **Instance type**: Select one of the following instances:
     - **Production**: If the environment is used for Production activities.
     - **Non-production**: If the environment is used for testing and development purposes. For example, a sandbox environment.
   - **Admin email**: The administrator email ID used to log in to 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 Administrator.

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

After the environment is set to **Active**, click the environment name to view the **Environment details**. Click the Service console URL under **Environment Information** to create users and groups.

Access Oracle 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. 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.

> **Note**
>
> Cloud environments are created under the **Default** identity domain. If you need to assign your environment to a different identity domain, raise a Service Request.

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.

Activate Application User Account

A user provisioned by their administrator can use the specific cloud services they have subscribed to.

When an administrator completes provisioning an application user, the user receives an account activation email from Oracle.

To log in and activate your application user account:

1. Open the email received from Oracle 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 log in.
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 and access the **Welcome Page**.

3

Managing Application Users

An application user can access the subscribed cloud services, based on the roles and groups assigned to them

An administrator can create application users using IAM. They can also batch import several users using a .CSV file.

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

You can map the application users to existing groups based on the roles that they require and their access levels. The access level provided to an application user is based on the following:

- **Groups**: Groups are seeded (available out-of-the-box) by your cloud service. Administrators 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. Administrators 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. Administrators cannot create new functions; however, they can use the existing functions.

Creating New Application 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.

To create users 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 user groups according to your user-specific groups or access, in the **Groups (Optional)**.

> **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.

Bulk Import Application Users

As an administrator, you can batch import user accounts using a `.CSV` file.

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

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 IAM 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 IAM will skip the incomplete account and proceed to the next account in the `.CSV` file.

When Oracle IAM 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.

For information on how to import and export users, groups, and Oracle application roles into and out of an identity domain, see Transferring Data.

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**.
- 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.

4

Managing 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.

Administrators 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.

Creating a New User Group

Create groups to manage user access to applications and resources.

To create a user group :

1. In the IAM Console, click **Profile** and select **Identity Domain**.
2. In the Identity Domain left pane, click **Groups** and select **Create group**.
3. Enter the **Group Name** 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.

Assign Groups to Users

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

Ensure to create a group, before assigning users to the group.

To map a user to a group using 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. Click a specific **User name** to view the user details and assign a group to that particular user.
4. In the left pane, click **Groups** to access the list of groups associated with a user.
5. In the **Groups** pane, click **Assign User to Groups** to view the list of available groups.
6. Check the check box adjacent to each group, to assign the user to that group.
7. After selecting all the required Groups, click **Assign user**.

The user is assigned to the selected groups. You can access the list of groups associated with a user, in the respective **User Details** page.

To dissociate an user from a group, select the group and click **Remove User from the Group**.

5

Mapping Users, Groups and Roles

Applications users can access the subscribed cloud services, based on the groups they are assigned to.

To provide secure and role based access to an application user:

- Map applications to the groups
- Map roles to the groups
- Map application users to the groups, based on their required access levels.

Map Application with the User Groups

After creating a group, you can map the required applications with the group.

To map the application to a user group, log in to IAM and follow these steps:

1. Go to the Navigation menu in the enter the **Domains** in the Search bar to view the **Domains** list.
2. Select the **Default Domain** and then from the LHS menu, select **Oracle Cloud Services**, to view the list of Cloud Services.
3. Select the Cloud Services you are subscribed to (Syntax: **<Cloud_service_name>xxxx-prd** and **<Cloud_service_name>xxxx-nprd**, where **Description** is mentioned as your registered cloud service).
4. From the LHS menu, select **Users** and click **Assign Users**.
5. Select the user and click **Assign**.

Creating a New Role

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

To create a role, from the Admin Console:

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

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

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

Map Roles to User Group

You can map roles to a user group using Admin Console.

To map roles to the user group:

Before mapping the roles to an user group, ensure that the roles are created in the Admin console.

1. From the **Identity Management** tab, Click **Groups** to access the **Groups Management** page.
2. Search for the specific group.
3. Click the **User Group** and click **New Mapping** under the **Mapped Roles** tab.
4. Search for required role names created in **Roles Management** and click **New Mapping** to map each role.
5. Log in as a user with the authorization role and authorize the mapped roles in the **Authorization View**.

A user group is created in the IAM Portal and is mapped to a role created in the Admin Console.

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 you need to authorize an unmap request, 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 **Assign User to Groups**. 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**
>
> 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.

6. Click **Map**.

> **Note**
>
> 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.

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.

6

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 6-1 Session Settings

7

Configuring Federated SSO

Oracle Cloud Infrastructure supports federation with Oracle Identity Cloud Service, and Microsoft Active Directory (via Active Directory Federation Services (AD FS)), Microsoft Azure Active Directory, Okta, and other identity providers that supports the Security Assertion Markup Language (SAML) 2.0 protocol.

To know more about identity federation, see Federating with Identity Providers.

8

Ways to Generate Access Token

An authenticated bearer token is required to invoke an API. The Authentication Process for token generation utilizes cURL Commands in a CLI Tool to generate the access token and invoke REST APIs.

The Authentication Token is generated through the OAuth Client ID and Secret Credentials. 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. Below is a list of authentication steps, with subsequent sections offering detailed information:

1. Create an Integrated (Confidential) Application.
2. Get the OAuth Client ID and Client Secret
3. Generate the access token

After generating an access token, proceed to invoking the APIs.

Create an Integrated (Confidential) Application

You can create an Integrated (Confidential) Application in Oracle Identity / IDCS (OCI IAM) to generate OAuth tokens for making public API calls.

OPC Applications Overview
An OPC app is a pre-created application that's provisioned automatically. The app name uses the following format: the cloud service name followed by your tenant ID. Example: AMLCS bccb73-prd.

To view your available OPC apps:

1. In the OCI Console, select Domains from the menu on the left.
2. Open the Oracle Cloud Services tab.
3. Review the list to see all OPC apps available to you.

Currently, Oracle Public Cloud (OPC) app client credentials are used to generate OAuth token and make public API calls. It is recommended to use Integrated App instead of OPC app for token generation, and maps grant types to typical use cases (service-to-service vs user-role tokens).

Prerequisites

1. Administrative access to your OCI Identity Domain / IDCS console.
2. Appropriate tenancy/domain selected in the Console.
3. If enabling TLS Client Authentication, private key and certificates are required.

Perform the following steps to create an integrated application

1. Sign in to the Oracle Cloud Console and go to Identity -> Identity Domains.
2. Select the domain where you want to create the application.>

3. On the domain details page, choose 'Integrated Applications'.
4. Click 'Add Application' and select 'Confidential Application'.
5. Click 'Launch workflow'.
6. Provide application details such as Name, Description, and Application URL (Redirect URL) if required
   - Application name: You can use the Tenant ID as your application name.
   - Redirect URL. Example: `https://%hostname%/cloudgate/v1/oauth2/callback`
7. Select 'Configure this application as a client now'.
8. Under Grant Types, at minimum enable:
   - Client Credentials
   - Authorization Code
   - Resource Owner
   - Optionally, enable:
     a. Refresh Token (to obtain refresh tokens alongside access tokens).
     b. TLS Client Authentication (for certificate-based client auth).
9. Complete the workflow and select **Finish**. The application is added in a deactivated state.
10. In the 'Application added' dialog, record the Client ID and Client Secret. Store these securely (Example: Vault).
11. On the application details page, click 'Activate' and confirm activation.
12. Post activation: If enabling TLS Client Authentication, import and register client certificate and key.

Note:

- Client Credentials, Authorization Code and Resource Owner are default/commonly required grant types. You can enable other grants as needed.
- To support renewing access tokens, enable the Refresh Token grant type.
- Optionally, enable TLS Client Authentication for certificate-based client authentication.

For more details, see Adding a Confidential Application.

Get the OAuth Client ID and Client Secret

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

You can obtain the OAuth client ID and client secret from:

1. **Integrated application (recommended)**: Obtain the `Client ID` and `Client Secret` from the newly created Integrated (Confidential) Application.
2. **OPC application (will be deprecated in a future release)**: From the **Oracle cloud services** tab in your OCI Console, open your tenant-specific application and obtain the client ID and client secret.

Once you obtain the client ID and client secret, proceed to generate the access token

Generate Access Token Using Different Grant Types

An access token is required to invoke APIs and you can generate the access token using different grant types.

Select a link for more information on each of these grant types:

1. Client Credentials Grant Type
2. Authorization Code Grant Type
3. Resource Owner Password Credentials Grant Type
4. TLS Client Authentication Grant Type
5. Refresh Token Grant Type

Client Credentials Grant Type

When to use: For non-interactive backend services or internal automation tasks.

> **Note**
>
> You can specify the token expiry while generating access token. By default, it is 1 hour.

Sample code

```
curl --location 'https://<idcs_domain>/oauth2/v1/token' --header
"Authorization: Basic $encoded" --header 'Content-Type: application/x-www-
form-urlencoded;charset=UTF-8' --data-urlencode
'grant_type=client_credentials' --data-urlencode 'scope=urn:opc:idm:my-custom-
scope%20urn:opc:resource:expiry=3600'
```

Sample code with mTLS enabled

```
curl --location 'https://<idcs_domain>/oauth2/v1/token' --cacert ./ca.crt --
cert ./client.crt --key ./client.key --header "Authorization: Basic $encoded"
--header 'Content-Type: application/x-www-form-urlencoded;charset=UTF-8' --
data-urlencode 'grant_type=client_credentials' --data-urlencode
'scope=urn:opc:idm:my-custom-scope%20urn:opc:resource:expiry=3600'
```

Sample response

```
{ "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...", "token_type":
"Bearer", "expires_in": 3600, }
```

For more details, see Client Credentials Grant Type

Authorization Code Grant Type

When to use: For web or client apps that require secure user login flow with redirect.

> **Note**
>
> - Provides user identity and roles via id_token.
> - Both access and refresh tokens are issued.
> - Ideal for user-based API calls or delegated permissions.

Sample code

```
curl --location 'https://<idcs_domain>/oauth2/v1/token' --header
"Authorization: Basic $encoded" --header 'Content-Type: application/x-www-
form-urlencoded;charset=UTF-8' --data-urlencode
'grant_type=authorization_code' --data-urlencode 'code=
eyJ4NXQjUzI1NiI6InlMTk16d1FuamZFNXp5U2...'
```

Sample code with mTLS enabled

```
curl --location ' https://<idcs_secure_domain>/oauth2/v1/token' --cacert ./
ca.crt --cert ./client.crt --key ./client.key --header "Authorization:
Basic $encoded" --header 'Content-Type: application/x-www-form-
urlencoded;charset=UTF-8' --data-urlencode 'grant_type= authorization_code' --
data-urlencode 'code= eyJ4NXQjUzI1NiI6InlMTk16d1FuamZFNXp5U2...'
```

Sample response

```
{ "access_token": "eyJraWQiOiJrZXkxIiwiYWxnIjoiUlMyNTYifQ...", "refresh_token":
"bc12cde3-xxxx-xxxx-xxxx-xxxx", "token_type": "Bearer", "expires_in": 3600, }
```

For more details, see Authorization Code Grant Type.

Resource Owner Password Credentials Grant Type

When to use: When user credentials are available, and the client is trusted to store them securely.

> **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.
> - Returns access tokens. Refresh token will be generated by enabling `offline_access`.
> - Suitable for generating user-level tokens tied to roles.

Sample code

```
curl --location 'https://<idcs_domain>/oauth2/v1/token' --header
"Authorization: Basic $encoded" --header 'Content-Type: application/x-www-
```

```
form-urlencoded' --data-urlencode 'grant_type=password' --data-urlencode
'username=dev-user' --data-urlencode 'password=xxxxxxxxx' --data-urlencode
'scope=urn:opc:idm:my-custom-
scope%20urn:opc:resource:expiry=3600%20offline_access'
```

Sample code with mTLS enabled

```
curl --location 'https://<idcs_domain>/oauth2/v1/token' --cacert ./ca.crt --
cert ./client.crt --key ./client.key --header "Authorization: Basic $encoded"
--header 'Content-Type: application/x-www-form-urlencoded' --data-urlencode
'grant_type=password' --data-urlencode 'username=dev-user' --data-urlencode
'password=xxxxxxxxx' --data-urlencode 'scope=urn:opc:idm:my-custom-
scope%20urn:opc:resource:expiry=3600%20offline_access'
```

Sample response

```
{ "access_token": "eyJraWQiOiJrZXkxIiwiYWxnIjoiUlMyNTYifQ...", "refresh_token":
"bc12cde3-xxxx-xxxx-xxxx-xxxx", "token_type": "Bearer", "expires_in": 3600, }
```

For more details, see Resource Owner Password Credentials Grant Type.

TLS Client Authentication Grant Type

When to use: For high-security backend integrations using mutual TLS.

> **Note**
>
> - Access token represents the application, not a user.
> - Refresh token returned only if `offline_access` is enabled in app configuration.

Sample code with mTLS enabled

```
curl --location 'https://<idcs_secure_domain>/oauth2/v1/token' --cacert ./
ca.crt --cert ./client.crt --key ./client.key --header "Authorization:
Basic $encoded" --header 'Content-Type: application/x-www-form-
urlencoded;charset=UTF-8' --data-urlencode 'grant_type=tls_client_auth' --
data-urlencode 'scope=urn:opc:idm:my-custom-
scope%20urn:opc:resource:expiry=3600' --data-urlencode 'client_id=<client_id>'
```

Sample response

```
{ "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6...", "token_type": "Bearer",
"expires_in": 3600, "refresh_token": "9e7d8f4a-xxxx-xxxx-xxxx-xxxx", }
```

For more details, see TLS Client Authentication Grant Type.

Refresh Token Grant Type

When to use: To obtain a new access token without requiring user login.

> **Note**
>
> - New tokens issued without user intervention.
> - Ideal for maintaining long-running sessions securely.
> - Refresh token validity is managed by IDCS configuration.

Sample code

```
curl --location ' https://<idcs_domain>/oauth2/v1/token' --header 'Content-
Type: application/x-www-form-urlencoded' --data-urlencode
'grant_type=refresh_token' --data-urlencode 'refresh_token=9b53e4a2-xxxx-xxxx-
xxxx-xxxx' --data-urlencode 'scope=urn:opc:idm:my-custom-
scope%20urn:opc:resource:expiry=3600'
```

Sample code with mTLS

```
curl --location ' https://<idcs_secure_domain>/oauth2/v1/token' --cacert ./
ca.crt --cert ./client.crt --key ./client.key --header "Authorization:
Basic $encoded" --header 'Content-Type: application/x-www-form-
urlencoded;charset=UTF-8' --data-urlencode 'grant_type=refresh_token' --data-
urlencode 'refresh_token=9b53e4a2-xxxx-xxxx-xxxx-xxxx' --data-urlencode
'scope=urn:opc:idm:my-custom-scope%20urn:opc:resource:expiry=3600'
```

Sample response

```
{ "access_token": "eyJraWQiOiJrZXkxIiwiYWxnIjoiUlMyNTYifQ...", "refresh_token":
"9b53e4a2-xxxx-xxxx-xxxx-xxxx", "token_type": "Bearer", "expires_in": 3600, }
```

For more details, see Refresh Token Grant Type.

Generate Access Token to Execute a Public RESTful API

You can generate access token using TLS to execute a public RESTful API.

Prerequisite: Organization-wide `ca.crt`, `client.crt`, and `client.key` (you can generate `client.crt` and `client.key` using `openssl`.)

Create a `client.crt` using `openssl`

Run the following command:

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt
```

Create a `client.key` using `openssl`

Run the following command:

```
openssl genrsa -out client.key 2048
```

Create an Integrated Application

1. Log in to Admin Console.

2. Under **Domains**, go to **Integrated Applications**.
3. Create a confidential application with an app name. Example: TLS_APP_<tenant.
4. After creating the application, edit the OAuth configuration as follows:
   a. Under the Client configuration, Select "Configure this application as a client now"
   b. Enable the below Auth grant types(TLS should be checked for TLS authorization)
   c. Enable Allow non-HTTPS URLs
   d. Add the redirect URL: http://%hostid%/cloudgate/v1/oauth2/callback
   e. Add the Logout URL: http://%hostid%/cloudgate/v1/oauth2/logout
   f. Set the client type as "Confidential"
   g. Under **Certificate file**, import the `client.crt` generated earlier.
   h. Click **Submit.**
5. Import the following Webtier policy:

```
{
    "cloudgatePolicy": {
        "version": "2.6",
        "requireSecureCookies": true,
        "disableAuthorize": false,
        "allowCors": true,
        "webtierPolicy": [
            {
                "policyName": "default",
                "comment": "",
                "resourceFilters": [
                    {
                        "filter": "/.*",
                        "comment": "Protect all resources",
                        "type": "regex",
                        "method": "oauth",
                        "headers": [
                            {
                                "user_groups": "$subject.user.groups"
                            },
                            {
                                "ofs_remote_user": "$subject.user.userName"
                            },
                            {
                                "ofs_remote_username": "$subject.user.name"
                            },
                            {
                                "ofs_mapped_groups": "$subject.user.groups"
                            },
                            {
                                "ofs_remote_user_email":
"$subject.user.emails"
                            }
                        ],
                        "authorize": false
                    }
                ]
```

```
                }
            ]
        }
    }
```

6. Activate the application.

Creating custom scopes for the Integrated Application (Optional)

After creating the Integrated Application, edit the OAuth configuration as follows:

1. Under Resource Server Configuration, select "Configure this application as a resource server now".
2. Set the access token expiration.
3. Set the primary audience.
4. Under the **Scopes**, click **Add**.
5. Under **Add Scope**, provide the following details:
   a. Scope: `urn:app:tls.test` **Note:** Should begin with `urn` and delimited by ":"(colon)).
   b. Display name: Custom scope.
   c. Click **Add**.
6. Click **Submit**.

Set up Postman to get the TLS token

1. Get the IDCS Host URL from the domain.
2. Click on the URL to get the IDCS configuration details.
   Example: `https://idcs-8523776c08804de1b5613af6d662f94e.identity.oraclecloud.com:443/.well-known/idcs-configuration`
3. Search for "secure_token_endpoint" to get the secure token endpoint.
   Example: `https://idcs-8523776c08804de1b5613af6d662f94e.us-ashburn-idcs-1.secure.identity.oraclecloud.com/oauth2/v1/token`
4. In the Postman, paste the `secure_token_endpoint` in the address bar as follows:
   a. Method: POST
   b. Body:
      i. grant_type: tls_client_auth
      ii. scope: urn:opc:idm:__myscopes__ # if the custom scope is required, the change the scope to <primary_audience><new_scope>
      iii. client_id: caf14860726e48a18b76b80704987285 #(Client ID from the above generated app)
   c. Content-type: `x-www-form-urlencoded` as header.
   d. For custom scope, provide the details as follows:
      i. grant_type: tls_client_auth
      ii. scope: urn:app:tls.auth.test
      iii. client_id: ecccdd63304a4483a9f2bb8e1fdfe45a
5. Click on postman settings and navigate to certificates tab.

6. Enable the CA certificates and upload the ca.crt under the PEM file
7. Click **Add Certificate**.
8. Paste the IDCS host URL of the `secure_token_endpoint` under the Host column
9. Upload the cert and key file downloaded from openSSL.
10. Click the **Add** button to add the certificates and close the dialog box.
11. Select **No Auth** for Authorization.
12. Click the **Send** button to get the token,

Send the request via postman with TLS token and client.crt

1. Paste the endpoint in the address bar with appropriate method type.
2. On the **Authorization** tab, select Auth type as "Bearer token" and paste the token generated.
3. In **Headers** column, set the header as `X-Forwarded-Tls-Client-Cert: <url_encoded_client_crt>`
   a. Only encode the cert part excluding the --Begin – and – end – from the certificate.
   b. For the cert url, encode - https://www.urlencoder.org/
4. Click **Send** for the response.

Invoke the API through the Access Token using TLS

To invoke the API through the generated Access Token using TLS, refer to the following example executed using cURL Commands in the CLI Tool:

A

About the New OCI Console

The new OCI (Oracle Cloud Infrastructure) Console provides feature enhancements while further simplifying the user experience.

Feature Enhancements

- Using the new OCI console, you can log in as an administrator and create new SaaS environments as production and non-production instances (if not already provisioned).
- As an administrator, you get direct access to User Management (adding a user) right after logging in.
- Once migrated to the new OCI console, your environments are also migrated and moved to the new compartments.

User Experience Enhancements

Post migration, you can access your OCI instance using the following URL: https://cloud.oracle.com/

Log in to the new OCI console with the valid credentials, to access the new OCI console dashboard.

Refer to the following table to understand the difference between the OCI Classic console and the new OCI console.

Table A-1 OCI Classic and new OCI login URL

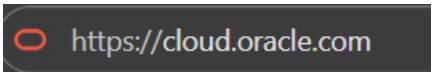
OCI Classic login URL	New OCI login URL
Figure A-1 OCI Classic login URL 	**Figure A-2 New OCI login URL** 

Table A-2 User experience changes between OCI Classic Console and OCI Console

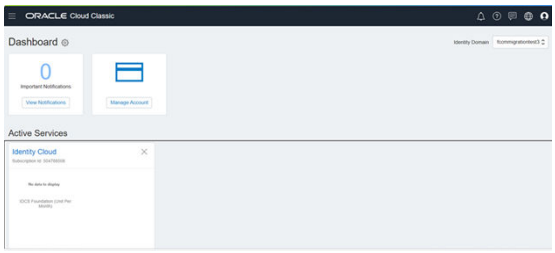
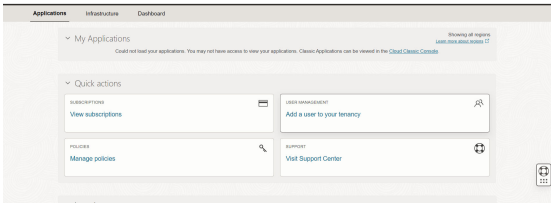
OCI Classic Console	OCI Console
Figure A-3 OCI Classic Console Dashboard 	**Figure A-4 New OCI Console Dashboard** 

Figure A-5 View provisioned environments (Production and Non-Production)