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

24A
F90375-07
March 2024

ORACLE®

Oracle Financial Services Crime and Compliance Management Cloud Service - Get Started, 24A

F90375-07

Contents

6   Authenticating for Token Generation

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 of your need 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 on-board Application Users to use the Cloud Services.

After activating the cloud service, you can log in as an administrator or an application user to perform various tasks.

Administrator Tasks

Log in as an Administrator and complete the following tasks to activate the Cloud Account and on-board Applications Users for the subscribed Cloud Services.

- Create and Activate New Cloud Account
- Access the Cloud Account
- Access the Oracle Identity Cloud Service Console

Application User Tasks

Login as an application user to activate your cloud account and use the Cloud Services that are provisioned by the Administrator.

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 Identity Resources and Account are located. Check the service availability before selecting 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 **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 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 **Setup Complete** email, to the email address provided while creating the account.

To access your Cloud account:

*   In the **Setup Complete** email, click **Sign In** and enter the **Username** and **Password** to access the **OCI Console** , to log in to the Console. Use the same **Username** and the **Password** that you provided during activation setup.

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. 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 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

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

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**.
- 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 log in to the 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 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, click **Profile** 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 set an username as the login ID, uncheck the **Use the email address as the username** check box and enter the required username for the **Username / Email**

   > **Note:**
   >
   > The username should be alphanumeric and cannot exceed 20 characters. You can enter only hyphen (-) and underscore (_) as special characters.

   > **Note:**
   >
   > You can only set the username as the login ID and currently setting the email address as the login ID is not supported.

4. 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.

5. Select one of the following options, to create an Identity **Administrator** or **Authorizer** user :

   • **IDNTY_ADMIN**: Assign the user to create an Administrator User.

   • **IDNTY_AUTH**: Assign the user to create an Authorizer User.

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

For bulk user creation, use batch import user accounts using a `.csv` file.

Create a 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.

Add User to Group

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

To add a user to a group :

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.

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**.

   The selected user is added to the user group.

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.

4
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 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. Search for the required **Domain**.

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**.

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.

Map Roles to User Group

You can map roles to a 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**.

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.

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.

10. 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.

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.

5

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 5-1   Session Settings

6

Authenticating for Token Generation

An Authentication token is required to invoke an API to generate the File Upload/Download PAR URL. 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 created in IAM during Provisioning. The Authentication Token does not require that you log in to the required Cloud Service to invoke the REST APIs from external applications.

Ensure that you have the appropriate log-in credentials to access the required Cloud Service and the appropriate roles to perform specific operations using the API Resources. Below is a list of authentication steps, with subsequent sections offering detailed information:

1. Download application certificate
2. Get the OAuth Client ID and Client Secret
3. Generate the access token
4. Generate refresh token
5. Invoke API using the access token

Download the Application Certificate

The Application Certificate is required for verification purposes when you use cURL commands.

You may choose not to download the certificate if you plan to turn off the cURL Certificate Verification and use an insecure connection (if you add the `--insecure` Flag to the cURL command).

To download the Application Certificate:

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

Get the OAuth Client ID and Client Secret

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 page, select the required Cloud Service Internal Application Service (in **<Cloud_service_name> <tenant-id> INTERNAL** format) from the list. For example, the cloud service name - **PBSMCS**

6. Click the **Configuration** tab.

   The Client ID and Client Secret Details are displayed in the General Information section.

7. Copy the `Client ID` and `Client Secret`.

8. Open a CLI Tool.

9. Proceed to generate the access token.

You can also get the OAuth client ID and client secret using Admin Console.

Generate the Access Token

Access token is required to invoke API and you can generate an access token using cURL commands.

To generate the Access Token, add the Client ID, Client Secret, User Name, and Password using cURL Commands in the CLI Tool. You can use an insecure connection (if you add the `--insecure` / `-k Flag` to the cURL command). The following is an example:

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

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

Sample Code

```
curl -k -i -H "Authorization: Basic
YWFpdGVzdGRldGjEwMDEtcHJkX0FQUElEOjQyYjJlYWVlLTY1OGEtNDgzYi1hMWI2LTBlYzU
0MzBmYWQwNQ==" -H "Content-Type: application/x-www-form-
urlencoded;charset=UTF-8" --request POST https://
iam-0cb0c2b3ba624afca67467fd5eb9db49.identity.c9dev2.oc9qadev.com:443/
oauth2/v1/token -d
"grant_type=password&scope=urn:opc:idm:__myscopes__+offline_access&user
name=cneadmin&password=Password@12345"
```

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

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

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

Sample Access Token (Truncated example)

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

Generate the Refresh Token

Refresh tokens are used to generate access tokens for invoking APIs.

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

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

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

Sample Code

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

cWppMHBkLXByZF9BUFBJRDplZjFjFjMTVmZi1lZDBiLTQxNmItYTFmYy0wNjhlYzM5NmUxM2Y=" -H
        "Content-Type: application/x-www-form-urlencoded;charset=UTF-8" --
request POST
        https://<IdentityDomainURL>/oauth2/v1/token -d

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

ORACLE

Sample Refresh Token (Truncated example)

```
{"access_token":"eyJ4NXQjUzI1NiI6IlF5azRtb3pIakhuQjJoQnVWdmZXZUpVeVZrNH
hUdWd6aWpHSC1pV21xb1EiLCJ4NXQiOiJDRFhHYVlWZXI3STVhQ1l...
...
...
token_type":"Bearer","expires_in":3600,"refresh_token":"AgAgYjA1OGVlMjJ
iMWY2NGU3YWFkM2NjZWNlOTc2MjNiNDgIABA4t8V_dYVyc5lOuKezofTUAAAAMJrpmKRhDW
f3-ejCreU8_Po5Bb95srwUDDs5cV1gT-x26twbAfp_ffMCiEgjqGeDNw=="}
```

Invoke the API using the Access Token

After creating an access token using OAUth Client ID and Client secret, you can invoke the Specific API.

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

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

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

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

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