How to request oAuth Client?

OAuth2 access is a token used for authorization. This access token provides a session (with scope and expiration), using these tokens will allow your client application to perform tasks in Oracle Identity Cloud Service (IDCS).

The following steps required on how to request an OAuth client integrated with Oracle Identity Cloud Service (IDCS) to access the REST APIs:

1. Start with registering a Trusted Application in IDCS
2. Base64 Encode the Client ID and Client Secret
3. Obtain an Access Token
4. Make a REST Request to the Environment

How oAuth works?

The token validation and authentication/authorization is depending on the application’s design.

If the application runs on Fusion Middleware, OWSM policy can be an option.

JWT validation is done by
- Validate the signature
- Examine attributes in the payload
- expiration
- scope
- audience
After that, identify the subject from the “sub” attribute in the payload, and proceed to authentication and authorization.
If it’s just client credential flow, JWT token validation might be good enough. The implementation varies based on the use case and the requirements.

How to request a new Client ?

1. Understand your application, scope and authentication needed

2. Copy the template "Client Request Template"

3. Fill up the template

4. If there’s product documentation (PaaS/SaaS services) about the oAuth, it’d be helpful too.
   Currently, PaaS services managed in the same IDCS tenancy, OAL GXP Weblogic Domain and EEHO(Fusion Apps) trust the OAL IDCS as the token issuer.

5. Please work with your Technical Project Manager (ATG Contact) to have a Jira Story raised/assigned. You can find details for raising Jira ticket here.
6. Email your TPM once the Jira ticket is logged
7. Wait for the Client Secret

> **Token Issuer Non OAL**
>
> If the POD or env is not listed as part of IDCS OAL, please follow this process to get the token OAuth2 Integration information

Do I need a Client or a Resource?

What is a Resource?

A Resource is an application that can be shared with other teams. Your primary audience and scope can be used for others to invoke end points using your Client as resource. A resource can be re-used for any other client without sharing client id and secret, you only need to share the scope.

What is a Client?

A client is an application that shouldn't be shared with other teams. Your client can invoke other services or resources.

Note. A client can be also a resource.

Client Request Template

⭐ Required

New client_id Request	
IDCS ⭐	□ https://idcs-3522377c0ff14104a3dad0b581a731a1.identity.oraclecloud.com/oauth2/v1/token □ https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com/oauth2/v1/token □ etc
OAL Technical Point of Contact (Usually from Tarun org)⭐	
Requestor's information (Team/Manager/Contact) ⭐	
Brief description how oAuth token is used between client-resource systems. ⭐	
Server/Resource Env Name	
Server/Resource EP Url(s) (Audience)	**Provide explicit URL for each environment** **example: https://gxpet.oracle.com/example/service** **avoid listing same URL for diff environments as** **https://gxpXX.oracle.com/example/service**

Resource Request Template

⭐ Required

New client_id Request Resource	
IDCS ⭐	□ https://idcs-3522377c0ff14104a3dad0b581a731a1.identity.oraclecloud.com/oauth2/v1/token □ https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com/oauth2/v1/token □ etc
OAL Technical Point of Contact (Usually from Tarun org)⭐	
Requestor's information (Team/Manager/Contact) ⭐	
Brief description how oAuth token is used between client-resource systems.⭐	
Server/Resource Env Name ⭐	
Server/Resource EP Url(s) (Audience) ⭐	**Provide explicit URL for each environment** **example: https://gxpet.oracle.com/example/service** **avoid listing same URL for diff environments as**

Client Env Name	
Client Application Name/Type (ex. Java App on FMW, PLSQL in APEX) ⭐	
Is Oracle Web Service Manager(owsm) used for the deployment? ⭐	
Grant/Flow Type (Select applicable) ⭐	☐ client credential ☐ resource owner ☐ authentication code ☐ refresh token ☐ JWT token / trusted client. *Please specify why it's needed and included the certificate (SSL)* ☐ other
Redirection URL(If applicable)	
Resource Owner Information (If applicable)	
Scope(If invoking a resource)	

Fusion OWSM

All Fusion OWSM end points are created as resources and will be using a scope fa/xxxxxx, which will be provided on request.

Note that for fusion services the user is validated, hence Password Credentials or Resource Owner grant type is needed in order to send the user on the JWT token.

	https://gxpXX.oracle.com/example/service
Client Env Name ⭐	
Client Application Name/Type (ex. Java App on FMW, PLSQL in APEX)	
Is Oracle Web Service Manager(owsm) used for the deployment?	
Grant/Flow Type (Select applicable)	☐ client credential ☐ resource owner ☐ authentication code ☐ refresh token ☐ JWT token / trusted client. *Please specify why it's needed and included the certificate (SSL)* ☐ other
Redirection URL(If applicable)	
Resource Owner Information (If applicable)	
Scope(If applicable) ⭐	

How to obtain access token?

1. Review which IDCS tenant
   OAL IDCS corpssononprod
   Token URL:https://idcs-3522377c0ff14104a3dad0b581a731a1.identity.oraclecloud.com/oauth2/v1/token

   OAL IDCS Prod
   Token URL:https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com/oauth2/v1/token
2. Once the client id and client secret has been shared

3. If the application is based in client credential you can run the following lines in cmd

get_access_token_cc.sh

```
# IDCS oAuth server: https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com
# Client ID: cccccccccccccccc
# Client Secret: ssssssssssssssssssss
#######################################
#Example call
cid=cccccccccccccccc
sec=ssssssssssssssssssssss
scope='urn:opc:idm:__myscopes__'  # Default/generic scope
url='https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com/oauth2/v1/token'

curl -i --user "${cid}:${sec}" --header 'ContentType: x-www-form-urlencoded' --request POST "$url" -d
"grant_type=client_credentials&scope=${scope}"
```

4. If the application is based in resource owner psw you can run the following lines in cmd

get_access_token_ro.sh

```
# IDCS oAuth server: https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com
# IDCS Username: username@oracle.com
# IDCS User password: xxxxx
# Client ID: cccccccccccccccc
# Client Secret: sssssssssssssssssssss
#######################################
#Example call


url='https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com/oauth2/v1/token'
idcs_user_name='username@oracle.com'
idcs_user_pwd='xxxxx'
cid=cccccccccccccccc
sec=sssssssssssssssssssss
scope="scope-assigned-for-the=client"
curl -i --user "${cid}:${sec}" -H 'ContentType: x-www-form-urlencoded' --request POST "${url}" \
-d "grant_type=password&scope=${scope}&username=${idcs_user_name}&password=${idcs_user_pwd}"
```

5. The output is the access token

Integrating IDCS application with OSS Application

*(Please note that this setup **is not mandatory** for your oAuth setup)*

*In order to utilise **fusion SaaS role memberships** for authorization in your custom applications, kindly create a new application in OSS and register the required roles there. You can find details on OSS/appl registration here.*

*Once you have completed your setup on OSS, please raise a BUG to OAL Security team (**8491/SECURITY/OTHERS**) requesting role-membership **sync** to be setup between your OSS app and IDCS app. Kindly provide below information in the bug:*

- *OSS application id/name*
- *IDCS application name*
- ***IDCS application- OSS environment** mapping. This lets us know which application in IDCS is linked to which OSS instance (dev, uat, stage, prod). Please note that you would need to setup a separate IDCS app for each instance.*

FAQ

1. **Is it possible to have more than one scope?**
   Yes, it's possible. One client can access many end points
2. **Can I share my client id and my secret?**
   No, you shouldn't share your client id and secret, if someone needs to use same setup from your client, they should be calling your client as resource
3. **Is the scope case sensitive?**
   Yes
4. **Is there any URL that user can directly access to get the token from outside oracle network?**
   Yes, it's the same URL can be called from inside or outside oracle network
5. **I'm not able to generate my token**
   Please review the following:
   a. Scope requested (case sensitive)
   b. The scope is formed by primary audience + scope.
   c. Client Id
   d. Client Secret
6. **"Invalid token does not contain resource id (gxp)"**
   Question: *Using the client ID and secret I am getting the bearer token though when used as Authentication for my Resource URL, it gives the following error: "Invalid token does not contain resource id (gxp)"*
   Answer: This is not an issue on oAuth setup. The reason of that message is because the token expected should include a resource added. Please enter resource and password and try again. Please review Howtoobtainaccesstoken? section script listed on step 3
7. **My application does not have scope**

   Use the dafult generic scope 'urn:opc:idm:__myscopes__'

8. Invalid_Grant. You entered an incorrect user name or password.

A token is requested using grant type not config in the client or the user and password are incorrect.

9. My user does not exists in IDCS/ "Incorrect User"

The user does not exist in non prod tenant of IDCS. To get it there you need to request **Identity Cloud Services [OAL Non-Production Tenant]** from OIM.
The user does not exist in prod tenant of IDCS. To get it there you need to request **Identity Cloud Services [OAL Production Tenant]** from OIM.

10. How can I reset my password in IDCS?

Exists 3 diferent options:

a. If the IDCS account have mailbox assigned use these links
    i. IDCS Prod here
    ii. IDCS Stage here
b. If the IDCS Account haven't a mail box but you want a new mailbox
    i. Follow this steps
c. If the IDCS haven't a mail box but you want to use your personal Mailbox
    i. Create a SR to ATG DevOps to change the "recovery email"
    ii. After the change of the mailbox use these links
        1. IDCS Prod here
        2. IDCS Stage here

11. Error 401: Unauthorized.

This could be for several reasons. Please review the following

a) Able to access to end point with basic auth.
b) Setup requested is the correct one, audience, scope
c) If you are able to generate the token the issue would be the setup requested.
d) If you are testing using postman, clear cache, close and try again

For Fusion Services review as follow:
a) User is able to invoke the service using basic authentication
b) User exists in Fusion Applications POD and has the required roles to invoke the service
c) User exists in OAL IDCS Prod
d) Password is the OAL IDCS Prod User Password
e) Token is generated using 'Password Credentials'
f) Scope is the one provided

12. Error: You entered an incorrect user name or password

Request the entitlement in OIM accordingly to your tenant (see question 9)
Once granted, reset the password (see question 10)

13. 401. Invalid OAuth Client xxxxxxxxxxxxxxx

Review which tenant your client was requested and created. Check Howtoobtainaccesstoken?

14. 404. Your service is not available

Please review your service deployment

15. 400 Bad Request: "invalid_grant","error_description":"Your password is expired.

Reset your IDCS user password Check Step 10

16. 429 HTTP Code

IDCS has the rate limits and they can add more limits. Error(HTTP code=429) is responded when the utilization exceeds the limits. As a common practice in calling API, IDCS oauth/OpenIDC calls should be managed with the resource impact in mind.

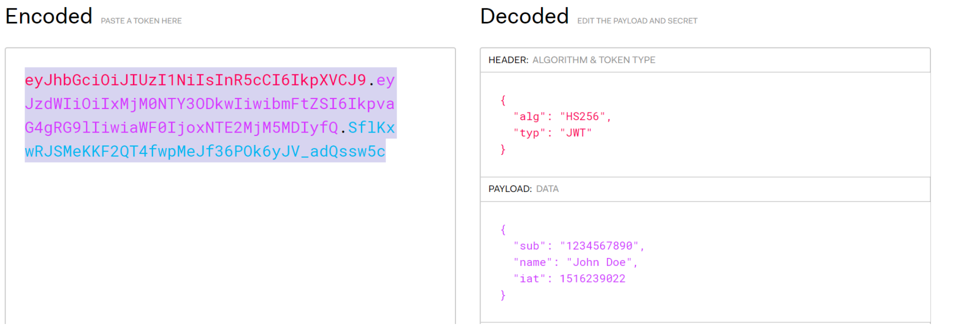
The rate limits can widely impact multiple environments because the activated limits impact other clients using the same IDCS tenancy.

- Estimate/minimize calls for oAuth/OpenIDC at the design time.
- Use caching and reuse given tokens until the token expires
- Handle re-try mechanism wisely. Do not simply resend the token/authorizaton request but limits the retry with a certain interval.

How to debug

1. Log in https://jwt.io/

2. Copy the token in Encoded area



Encoded

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded

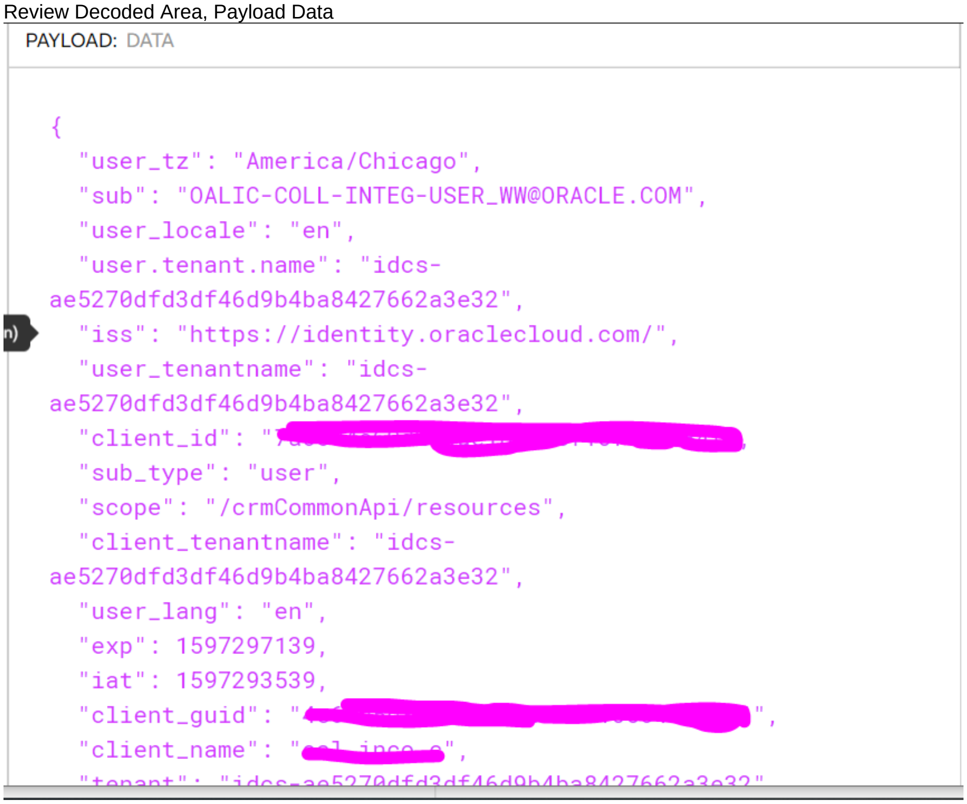
HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

3. Enter
4. Review Decoded Area, Payload Data



PAYLOAD: DATA

```
{
  "user_tz": "America/Chicago",
  "sub": "OALIC-COLL-INTEG-USER_WW@ORACLE.COM",
  "user_locale": "en",
  "user.tenant.name": "idcs-
ae5270dfd3df46d9b4ba8427662a3e32",
  "iss": "https://identity.oraclecloud.com/",
  "user_tenantname": "idcs-
ae5270dfd3df46d9b4ba8427662a3e32",
  "client_id": "[redacted]
  "sub_type": "user",
  "scope": "/crmCommonApi/resources",
  "client_tenantname": "idcs-
ae5270dfd3df46d9b4ba8427662a3e32",
  "user_lang": "en",
  "exp": 1597297139,
  "iat": 1597293539,
  "client_guid": "[redacted]",
  "client_name": "[redacted]",
  "tenant": "idcs-ae5270dfd3df46d9b4ba8427662a3e32"
```

5. Example of payload data

```
{
  "user_tz": "America/Chicago",
  "sub": "XXXXXX-USER_WW@ORACLE.COM",
  "user_locale": "en",
  "user.tenant.name": "idcs-ae5270dfd3df46d9b4ba8427662a3e32",
  "iss": "https://identity.oraclecloud.com/",
  "user_tenantname": "idcs-ae5270dfd3df46d9b4ba8427662a3e32",
  "client_id": "XXXXXXXXXXXXXXXXXXXXXf",
  "sub_type": "user",
  "scope": "/fcrmCommonApi/resources",
  "client_tenantname": "idcs-ae5270dfd3df46d9b4ba8427662a3e32",
  "user_lang": "en",
  "exp": 1597297139,
  "iat": 1597293539,
  "client_guid": "client_idxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "client_name": "client_namexxxxxxxxxxxxxx",
  "tenant": "idcs-ae5270dfd3df46d9b4ba8427662a3e32",
  "jti": "b2b988c4-1e95-46e8-a484-f3bebe4a54fb",
  "user_displayname": "xxxxxxxxx-user_ww",
  "sub_mappingattr": "userName",
  "primTenant": true,
  "tok_type": "AT",
  "ca_guid": "cacct-5c72678f23884aacbec1bfa4ad8d5dbb",
  "aud": [
    "https://efip-test.fa.us6.oraclecloud.com/fcrmCommonApi/resources",
    "https://eeho-test.fa.us2.oraclecloud.com/fcrmCommonApi/resources",
    "https://eeho-dev4.fa.us2.oraclecloud.com/fcrmCommonApi/resources",
    "https://eeho-dev9.fa.us2.oraclecloud.com/fcrmCommonApi/resources",
    "https://efip-dev1.fa.us6.oraclecloud.com/fcrmCommonApi/resources",
    "fa",
    "https://eeho-dev5.fa.us2.oraclecloud.com/fcrmCommonApi/resources",
    "https://eeho.fa.us2.oraclecloud.com/fcrmCommonApi/resources"
  ],
  "user_id": "40115fecfe02443fb5b42657bbe7a05a",
  "tenant_iss": "https://idcs-ae5270dfd3df46d9b4ba8427662a3e32.identity.oraclecloud.com"
}
```

6. Review the **aud:[** section, it should included the audiences added for the scope selected
7. scope: should be the one added while requesting the token