

Oracle® Financial Services Lending and Leasing

OAuth2 based Web Services Access Authentication



Release 15.0.0.0.0

G42475-01

September 2025

ORACLE®

Oracle Financial Services Lending and Leasing OAuth2 based Web Services Access Authentication, Release 15.0.0.0.0

G42475-01

Copyright © 2022, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1	Introduction	
1.1	Background	1
1.2	Purpose	1
1.3	Abbreviations	1
2	Web services authentication using OAuth2	
2.1	Understanding OAuth Services	1
2.1.1	Identity Domains	2
2.1.2	Clients	2
2.1.3	Resource Server	2
2.1.4	Resource Owner	2
2.1.5	Types of OAuth REST API	2
3	Enabling OAuth Setup Configurations	
3.1	Enabling OAuth support for OFSLL REST APIs	1
3.2	Identity Domain Creation	1
3.3	Resource Server Creation	3
3.4	Client Creation	4
3.5	Getting Access Token	5
3.5.1	How OFSLL API works with access token?	5
3.5.2	Access Token for CLIENT_CREDENTIALS grant type	6
3.5.3	Access Token for PASSWORD grant type	7
3.5.4	Access Token for JWT_BEARER grant type	8
3.5.5	Access Token for REFRESH_TOKEN grant type	9
3.5.6	How to get access token through Basic Authentication	11
3.5.7	How to access the REST API using the access token	12
3.6	Embedding External Application within OFSLL	12

1

Introduction

- [Background](#)
- [Purpose](#)
- [Abbreviations](#)

1.1 Background

Oracle Financial Services Lending and Leasing (OFSLL) suite is a comprehensive, end-to-end solution that supports full lifecycle of direct and indirect consumer lending business with Origination, Servicing and Collections modules. This enables financial institutions to make faster lending decisions, provide better customer service and minimize delinquency rates through a single integrated platform. It addresses each of the lending processes from design through execution. Its robust architecture and use of leading-edge industry standard products ensure almost limitless scalability.

To extend OFSLL SaaS, OAuth2 can be used for securing OFSLL web services user access Authentication. This document details the process of web services authentication using OAuth services and enabling OAuth setup configurations.

1.2 Purpose

The purpose of this document is to provide detailed information for consulting and partner teams to implement an OAuth2 based REST API access authentication mechanism for OFSLL customers.

1.3 Abbreviations

Table 1-1 Abbreviations

Abbreviation	Detailed Description
OFSLL	Oracle Financial Services Lending and Leasing
IDM	Identity Management
OAuth	Open Authorization
SaaS	Software as a service
PaaS	Product as a service
OAM	Oracle Access Management
API	Application Program Interface
URL	Uniform Resource Locator
XML	Extensible Markup Language
JWT	JSON Web Token
CSF	Critical success factor

2

Web services authentication using OAuth2

Web services authentication using OAuth2 is one of the best approach for securing user authentication to extend OFSLL SaaS. This uses Oracle / Non-Oracle PaaS to authenticate service access request from an external partner application without sharing OFSLL environment access credentials (UID / Password) and leverages the built-in support for OAuth 2.0.

OAuth 2.0 is an open standard token-exchange technology for verifying a user's identity across multiple systems and domains without risking the exposure of a password.

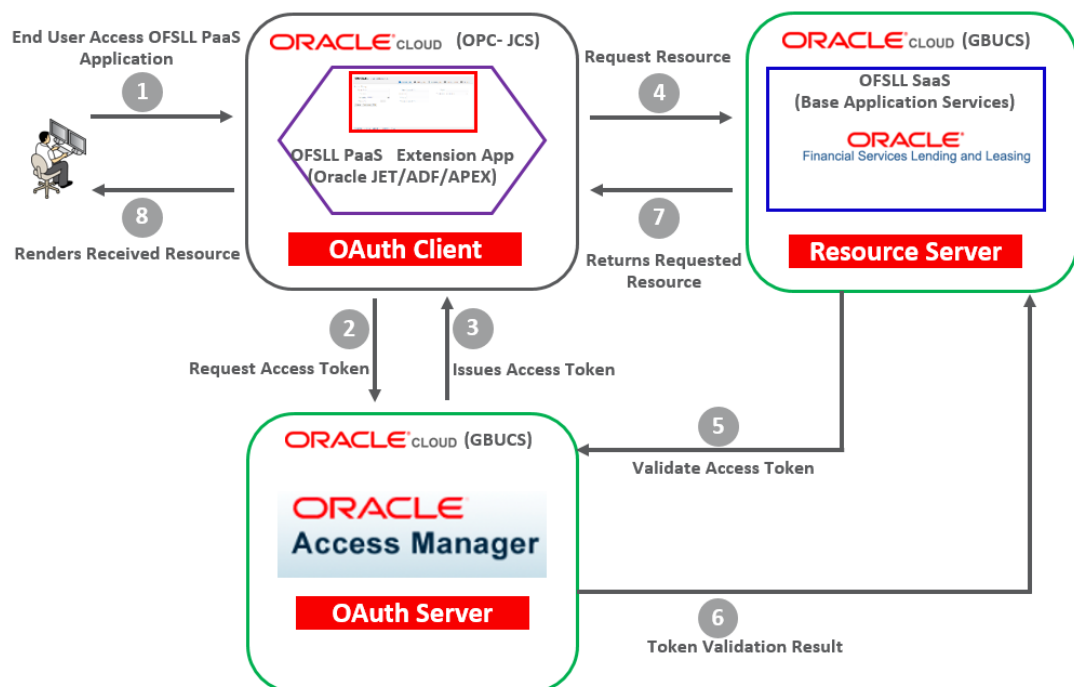
Third-party applications (those not hosted on Oracle Cloud PaaS) can use OAuth for making calls into OFSLL Cloud REST APIs. PaaS / On-Premise application can pass a user's authentication information and request an OAuth token from OFSLL Cloud, and then use the token to interact with an OFSLL Cloud API. PaaS or On-Premise and SaaS components can be with different ID Domains and security is managed with Shared IDM.

- [Understanding OAuth Services](#)

2.1 Understanding OAuth Services

Oracle Access Management (OAM) implemented the OAuth core 2.0 specifications to offer OAuth services. OAuth is an open standard authorization protocol that provides authentication and access control between a Client (such as Web services) and a Resource Owner (Service Provider) on the web.

Figure 2-1 OAuth Services



- [Identity Domains](#)
- [Clients](#)
- [Resource Server](#)
- [Resource Owner](#)
- [Types of OAuth REST API](#)

2.1.1 Identity Domains

The Identity domains are entities that contain all artifacts required to provide standard OAuth services. Identity domains are independent entities and the primary use of this is to provide multi tenants deployments. Each Identity domain will correspond to a tenant. This will also be useful for cloud deployments where each Identity domain can correspond to a separate tenant or entity.

Following are some of the components configured within an OAuth services Identity domain.

- One or More Clients
- One or More Resource Servers

2.1.2 Clients

The client is an application which makes protected resource requests on behalf of the resource owner using its authorization. For example, OFSLL. The Client initiates the OAuth Protocol by invoking the OAuth services. The client may be public or confidential.

There are two types of clients:

- **Confidential Clients:** Web Applications are of confidential client types assigned with a client ID and secret key. These clients can interact with the OAuth services server by sending the Client ID and secret as part of an authorization header.
- **Public Clients:** Public Clients or untrusted clients are assigned with a client ID but no secret key. These are the type of external applications that are not capable of keeping a client password confidential.

2.1.3 Resource Server

The Resource server is the machine on which protected resource is hosted. The Resource server is deployed in a different location from OAM and Client. The Resource server needs to be capable of accepting and responding to protected resource requests using access tokens.

2.1.4 Resource Owner

This is an entity capable of granting access to a protected resource. When the resource owner is a person, it is referred as an end-user.

2.1.5 Types of OAuth REST API

OAuth services are enabled as part of OAM version 12c Installation process. OAM provides an API based approach for configuring OAuth Services. There are 2 types of API OAuth services providers namely Admin API and Runtime API.

The Admin API provides capability to create mandatory admin components like Identity domain, Resource Server and client etc. They must be configured before the client makes the token request.

Note

To Execute Admin API, you can refer to Oracle OAM OAuth REST API documentation available at <https://docs.oracle.com/en/middleware/idm/access-manager/12.2.1.3/oroau/api-admin-identity-domain.html>.

3

Enabling OAuth Setup Configurations

- [Enabling OAuth support for OFSLL REST APIs](#)
- [Identity Domain Creation](#)
- [Resource Server Creation](#)
- [Client Creation](#)
- [Getting Access Token](#)
- [Embedding External Application within OFSLL](#)

3.1 Enabling OAuth support for OFSLL REST APIs

The OAuth support for OFSLL REST API can be enabled with the following steps:

1. Add context Parameters in web.xml
2. Remove URL Security constraint tags in web.xml

Add the below configuration in web.xml of OfsslRestWS.ear:

```
<context-param>
```

```
<description>This parameter will decide the jersey filter to be loaded</description>
```

```
<param-name>OAUTH_AND_BASIC_ENABLED</param-name>
```

```
<param-value>Y</param-value>
```

```
</context-param>
```

3. Remove Security configuration from weblogic.xml as well.

Note

If this context parameter is not set, only the existing basic authentication flow is supported.

3.2 Identity Domain Creation

To create identity domain, any valid reliable REST client application/tool can be used to invoke the REST API. For example, Postman tool.

http:<AdminServerHost:Port>/oam/services/rest/ssa/api/v1/oauthpolicyadmin/
oauthidentitydomain

Request JSON payload

```
{  
  "name": "OFSLL_OAUTH_DOMAIN",  
  "identityProvider": "OUD_LDAP",  
  "description": "OFSLL_OAUTH_DOMAIN",  
}
```

```

"tokenSettings":[{
  "tokenType":"ACCESS_TOKEN",
  "tokenExpiry":3600,
  "lifeCycleEnabled":true,
  "refreshTokenEnabled":true,
  "refreshTokenExpiry":86400,
  "refreshTokenLifeCycleEnabled":true
},
{
  "tokenType":"AUTHZ_CODE",
  "tokenExpiry":3600,
  "lifeCycleEnabled":true,
  "refreshTokenEnabled":true,
  "refreshTokenExpiry":86400,
  "refreshTokenLifeCycleEnabled":true
},
{
  "tokenType":"SSO_LINK_TOKEN",
  "tokenExpiry":3600,
  "lifeCycleEnabled":true,
  "refreshTokenEnabled":true,
  "refreshTokenExpiry":86400,
  "refreshTokenLifeCycleEnabled":false
}],
"errorPageURL":"/oam/pages/error.jsp",
"consentPageURL":"/oam/pages/consent.jsp",
"customAttrs":"Attribute of user in IDStore to store the encrypted secretkey
for TOTP"
}

```

Response JSON payload

```

Sucessfully created entity - OAuthIdentityDomain, detail - OAuth Identity
Domain :: Name
- OFSLL_OAUTH_DOMAIN,
Id - 37b278eb5e894085ab1656b9641cca1a, Description - OFSLL_OAUTH_DOMAIN,
TrustStore Identifiers - [OFSLL_OAUTH_DOMAIN],
Identity Provider - OUD_LDAP, TokenSettings - [{
  "tokenType":"ACCESS_TOKEN",
  "tokenExpiry":3600,
  "lifeCycleEnabled":true,
  "refreshTokenEnabled":true,
  "refreshTokenExpiry":86400,
  "refreshTokenLifeCycleEnabled":true
},
{
  "tokenType":"AUTHZ_CODE",
  "tokenExpiry":3600,
  "lifeCycleEnabled":true,
  "refreshTokenEnabled":true,
  "refreshTokenExpiry":86400,
  "refreshTokenLifeCycleEnabled":true
},
{
  "tokenType":"SSO_LINK_TOKEN",

```

```
"tokenExpiry":3600,
"lifeCycleEnabled":true,
"refreshTokenEnabled":true,
"refreshTokenExpiry":86400,
"refreshTokenLifeCycleEnabled":false}},
ConsentPageURL - oam/pages/consent.jsp,
ErrorPageURL - /oam/pages/error.jsp,
CustomAttrs - Attribute of user in IDStore to store the encrypted secretkey
for TOTP
```

3.3 Resource Server Creation

Resource Server Name: OFSLL_OAUTH_SERVER

Identity Domain: OFSLL_OAUTH_DOMAIN

Request JSON payload

```
{
  "name":"OFSLL_OAUTH_SERVER",
  "description":"OFSLL_OAUTH_SERVER",
  "scopes":[{"
    "scopeName":"OFSLL_REST_ALL",
    "description":"ALLOW_ALL"
  }],
  {
    "scopeName":"OFSLL_REST_NONE",
    "description":"ALLOW_NONE"
  }],
  "tokenAttributes":
  [{"attrName":"sessionId",
    "attrValue":"$session.id",
    "attrType":"DYNAMIC"
  }],
  {
    "attrName":"resSrvAttr",
    "attrValue":"RESOURCECONST",
    "attrType":"STATIC"
  }],
  "idDomain":"OFSLL_OAUTH_DOMAIN",
  "audienceClaim":{"subjects":["OFSLL_B2B_OAUTH_CLIENT"]}}
}
```

Response JSON payload

```
Sucessfully created entity - OAuthResourceServer, detail -
IdentityDomain="OFSLL_OAUTH_DOMAIN,
Name="OFSLL_OAUTH_SERVER", Description="OFSLL_OAUTH_SERVER",
resourceServerId="99a3e782-ce6d-467c-baec-df687fe326a6",
resourceServerNameSpacePrefix="OFSLL_OAUTH_SERVER.",
audienceClaim="{
  "subjects":["OFSLL_B2B_OAUTH_CLIENT"]}",
resServerType="CUSTOM_RESOURCE_SERVER",
Scopes="[{"
  "scopeName":"OFSLL_REST_ALL",
```

```

"description": "ALLOW_ALL"},
{
  "scopeName": "OFSLL_REST_NONE",
  "description": "ALLOW_NONE"},
{
  "scopeName": "DefaultScope",
  "description": "DefaultScope"}],
"tokenAttributes": [{
  "attrName": "sessionId",
  "attrValue": "$session.id",
  "attrType": "DYNAMIC",
  {"attrName": "resSrvAttr", "attrValue": "RESOURCECONST", "attrType": "STATIC"}]

```

3.4 Client Creation

Name: OFSLL_B2B_OAUTH_CLIENT

idDomain: OFSLL_OAUTH_DOMAIN

```

{
  "attributes": [{
    "attrName": "customeAttr1",
    "attrValue": "CustomValue",
    "attrType": "static"
  }],
  "secret": "<custom password>",
  "id": "OFSLL_B2B_OAUTH_CLIENT",
  "scopes": [
    "OFSLL_OAUTH_SERVER.OFSLL_REST_ALL",
    "OFSLL_OAUTH_SERVER.OFSLL_REST_NONE"
  ],
  "clientType": "CONFIDENTIAL_CLIENT",
  "idDomain": "OFSLL_OAUTH_DOMAIN",
  "description": "Client Description",
  "name": "OFSLL_B2B_OAUTH_CLIENT",
  "grantTypes": [
    "PASSWORD", "CLIENT_CREDENTIALS",
    "JWT_BEARER", "REFRESH_TOKEN",
    "AUTHORIZATION_CODE"
  ],
  "defaultScope": "OFSLL_OAUTH_SERVER.OFSLL_REST_ALL"
}

```

Response JSON payload

```

Sucessfully created entity - OAuthClient, detail - OAuth Client - uid =
236936a6-ed77-
4d6a-bcee-c0282554a1a0,
name = OFSLL_B2B_OAUTH_CLIENT, id = OFSLL_B2B_OAUTH_CLIENT,
identityDomain = OFSLL_OAUTH_DOMAIN,
description = Client Description, secret = <custom password>, clientType =
CONFIDENTIAL_CLIENT,
grantTypes = [PASSWORD, CLIENT_CREDENTIALS, JWT_BEARER,
REFRESH_TOKEN, AUTHORIZATION_CODE],

```

```
attributes = [{  
  "attrName": "customeAttr1",  
  "attrValue": "CustomValue",  
  "attrType": STATIC  
},  
{  
  "attrName": "sessionId",  
  "attrValue": "$session.id",  
  "attrType": DYNAMIC  
},  
{  
  "attrName": "resSrvAttr",  
  "attrValue": "RESOURCECONST",  
  "attrType": STATIC  
}],  
scopes = [OFSLL_OAUTH_SERVER.OFSLL_REST_ALL,  
OFSLL_OAUTH_SERVER.OFSLL_REST_NONE],  
defaultScope = OFSLL_OAUTH_SERVER.OFSLL_REST_ALL, redirectURIs = []
```

3.5 Getting Access Token

A client application which wants to obtain an access token from OAuth server can access OFSLL Authentication API which in turn accesses the OAM OAuth API and generates token. The authentication REST service OFSLL provides a wrapper around OAM OAuth API.

- [How OFSLL API works with access token?](#)
- [Access Token for CLIENT_CREDENTIALS grant type](#)
- [Access Token for PASSWORD grant type](#)
- [Access Token for JWT_BEARER grant type](#)
- [Access Token for REFRESH_TOKEN grant type](#)
- [How to get access token through Basic Authentication](#)
- [How to access the REST API using the access token](#)

3.5.1 How OFSLL API works with access token?

1. Client calls OFSLL authentication API (OFSLL REST API) with required headers along with body and obtains the token as response.
2. OFSLL REST API validates the token and retrieves the user ID from access token.
3. If the token is valid, then provides access to the protected resource.

Note

To use OAM OAuth API, update the following OFSLL system parameters with valid values.

Table 3-1 OFSLL system parameters with valid values

OFSLL System Parameter Name	Default Value	Actual Value Required to configure OAuth Feature
OAM_OAUTH_ENABLED_IND	SETME	Y
OAM_OAUTH_TOKEN_URL	SETME	http://<hostname>:<port>/oauth2/rest/token
OAM_OAUTH_TOKEN_VALID_URL	SETME	http://<hostname>:<port>/oauth2/rest/token/info?access_token=<AccessToken>

While client applications are allowed to access OAM OAuth REST API directly, it is recommended for clients to access OFSLL Authentication REST API for all token generation and token validation features.

Authentication Resource URL:

http://<<hostname>>:<<port>>/<<context path>>/service/api/resources/auth/token

3.5.2 Access Token for CLIENT CREDENTIALS grant type

Request JSON payload

```
{
  "AuthRequest": { "GrantType": "CLIENT_CREDENTIALS" }
}
```

Mandatory Request Headers

Table 3-2 Mandatory Request Headers

Headers	Expected Value
X-OAUTH-IDENTITY-DOMAIN-NAME	OFSLL_OAUTH_DOMAIN
Authorization	Bearer <Base64encoded value of client credentials>

Response JSON payload

```
{
  "AuthResponse": {
    "Token":
      "eyJraWwQI0iJPRlNMTF9TU09fVEVTVF9ET01BSU4iLCJ4NXQiOiJjQldCa0pqV2JVdHRHczFmZFdldYzdeE0tMwsiLCJhbgciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbXVtMDBjaWUuaw4ub3JhY2xlLmNvbToxNDEwMCM9YXV0aDIiLCJhdwQiOiJldLCJleHAiOiJlNDU2NjYyNDAsImp0aSI6IjZrTDA4RGxhUXRGYXdlb0xRaGxnLVEiLCJpYXQiOiJlNDU2NjYyNDAsInN1YiI6Ik9GU0xMX0IyQl9KRVRfQ0xJRlU5U1wiY2xpZW50IjoitOTZTTEtfQjJXJCX0PFVF9DTelFTlQlLCJzY29wZSI6WyJPRlNMTF9TU09fVEVTVF9TRVJWRVJfQjJjJCLkFjY291bnREZXRhaWxzIl0sImRvbWVfb2I6Ik9GU0xMX1NTT19URVNUX0RPTUJfJTI9LjJXIN9ogjgGuxSfLSb_tMoi9KSSnUgWar70fj0sqML0Xi0KS1vc7TK0_R8RvcQ_q8T8HpGTumxmXbhH-XuWhSojnpvH_03Jj3EMSp5_w9IVIrKVanXej1teWP9ud01k0mieLLtyY328bonSIT3ljtsviMhDfn06k1Qk7WlFb9CZmkAdEd-B4lZV2hsYr2i2QhVbpyj62tbgtXdkJbeKSaGR62JRGyx4vZ2u9tAmDGk17sxftAFyPqzrLVlh_fmEBvI3jVfacJmDcQBP2Wry8QYppWxulsaF996kdb40sAtl05iK_DMZKtY0wxfTgzat1MZYYpInq871bEMqGFSgw"
```

```
"Expires_in": 3600,
"TokenType": "Bearer",
"Result": {
  "Status": "SUCCESS",
  "StatusDetails": "Token Generated Successfully"
}
}
```

3.5.3 Access Token for PASSWORD grant type

Request JSON payload

```
{ "AuthRequest": {
  "UserName" : "OFSLLSUPR",
  "Password" : "Demo1234",
  "GrantType" : "PASSWORD"
}}
```

Mandatory Request Headers

Table 3-3 Mandatory Request Headers

Headers	Expected Value
X-OAUTH-IDENTITY-DOMAIN-NAME	OFSLL_OAUTH_DOMAIN
Authorization	Bearer <Base64encoded value of client credentials>

Response JSON payload

```
{  
  "AuthResponse": {  
    "Token":  
      "eyJraWwQI0IjPRlNMTF9TU09fVEVTVF9ET01BSU4iLCJ4NXQiOiJjQldCa0pqV2JVdHRHczZmZFdlYzdtE0tMwsiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbXBvMTBDbjaWUuaW4ub3JhY2xlLmNvbToxNDcwMC9yYXV0aDIiLCJhdWQiOi0tdLCJleHAiOiE1NDU2NjYzMjMDIsImp0aSI6IjQ3bnF5Q1RnbnHN1OE1yenp3Mnlzc3ciLCJpYXQiOiE1NDU2NjI3MDIsInN1YiI6Ik9GU0xMU1VQUiIsIk9BVVRlX1RPS0V0IjoizXlkcmFXUWlPaUprWlmaaGRXeDBJaXdPZURWMElqb2lZa3c1VkRjNGJIAe1RakowY1c1eGQyZDRZEPUW5vdFFYWnpJaXdPZWd4bk1qb2lVbE15TlRZawZRLmV5Smx1SEFPt2pFMU5EVTJ0aall6TURJc0ltcDBHu0k2Swp0SFZITjNOM1ZuTVhGQ2MwMXJoalJIVFVGSwJsRWlMQ0pwVhRaU9qRTFORFUyTmpJM01ESXNJbk4xWWlJNklrOUdmMHhNVTFUVVpSXNJbk5sYZNOcGIyNWZhV1FpT2lKM2QwSTVkbU12Y2lWSVFYQ1pPRGxHZGx0ewVYVm5QVDEtYjAxRlNIUkVibGcyVGtsRmRYVXZWM2hZZWtKTlFUMDlJaXdPwkc5dFlxbHVJam9pwkdWbVlyVnNkQ0o5LkdKNlJOM19HUHNSQW0yTmGlbnQiOiJPRlNMTF9CMkJfSkvUX0NMUSUV0VCIsInNjb3BlIjpbIk9GU0xMX1NTT19URVNUX1NFULZFU19CMkIuQWNjb3VudERldGFpbHMixSwizG9tYWluIjoitOTZTEtfU1NPX1RFU1RfRE9NQUL0InO.YJJqj32KhCQfyFuZAi5XAhhBL3s8E29AiJxQGgMrkDU57YIFt5l36bhJUGFRTNXnhZ2Uxp5bhZiZJcmiv0Tqs_j1Iaz0-TkhKCbHX2_-8NhelwEXktTyqx8-9JKak1T8jsknXXKv01FSv46siu2mBSxKul6rw7yeyC-TRiBBmj48h_udlSfLQC98X_5jxxQU8FPcv18Cb9l2HbGh9zuUmEP8G87leYQ7KTMBwbcbQklbAVQVxbF0FVKua2efjw2LIz5X0J_o_U-6GVudCCiQvbeVY3VbUl4hqxJGXCs5e3ub09wPF8flCd05MAStFd30KzpeKxRtGDZXjuD
```

```

g3NSw",
"Expires_in": 3600,
"TokenType": "Bearer",
"RefreshToken":
"A79Gdo4lh0SCGmvmRqWMg==~nHVR44Sa3QZgp13eep108t323SjYEd3r6+IF24xBocT
9SxybWy6PcpHDjSoLT0mW+0cqtfqTenEmoIWcyfh0cTGzcmYCH1KMOMfCGns+M2Kk
wusUCCGWnyrhoUevwhbKI4U20B3E6orBVkZxhtmQLqkATXbvHS0tGq1KIQwrgUCjNlws
SDFgBCj4umfQMilt63pmgcKntwpQc0edxB6y2B9f13BFY8j2D53xogK3coE40pI4f+SufnZ
0Wl+0DkcCGHTfdaDzdcA2TwwA5VVjZaQ16A+nCx144uHaBj1e00piUaypL730tK2N8a
ES1CSDU1ZPjbl3N1EY360VvLJRoxdRq2nL4SgS0wJ7XIdu39wuxoTgtjLBWHQsDEtc0eB
bgFUMA2q8ug29+67cl/9H6Tw0EgF+T981H+7JQTckSrma7gtyMr7MKy0QtmxR4Ns6w=
", "Result": { "Status": "SUCCESS", "StatusDetails": "Token Generated
Successfully"
}
}
}

```

3.5.4 Access Token for JWT_BEARER grant type

This is the grant type is to achieve the seamless SSO between the different mixes of application. This grant type provides facility to link the mainstream application SSO session with OAuth token.

When the SSO session is generated, JWT User token also generated. The generated JWT user token has the SSO “session_id” as part of its claims. The consumer client application must call OFSLL Authentication API with JWT_BEARER token grant type to get access token to access the protected resource.

Note

The rules of SSO session are applied to the OAuth Access token.

Sample Request JSON

```

{
  "AuthRequest": {
    "Assertion": "eyJraWQiOiJkZWZhdWx0IiwieDV0IjoiYkw5VDI4bHhMQjJ0cW5xd2d4Y0F0
QnotQXZzIiwiaWxnIjoiUlMyNTYifQ.eyJleHAiOiE1NDU2NDQ0NTESImp0aSI6I1RUS0lsS
DdWR1VyWVhVbHdyZ2luUWciLCJpYXQiOiE1NDU2NDQ0NTESInN1YiI6Ik9GU0xMU1
VQUiIsInNlc3Npb25faWQiOiJCeW90c2h6LzR3K2hhekVHcnNqWnJBPT1-
bVN2eU5DaEtLa29xTk5tcUIyYQkUvM3lOUTBiNENYVWltQktqWXd1Y1JlZDQYXBJN6a
1pkbnJqYWViOURPbWVirtFBSURocG1QN0tTd1hKUDVFdzRpbmZHTES1VGlsYldDY
UJWLOVmkIxm5K2FaY1oxQ250UTV0VVFUS3ciLCJkb21haw4iOiJkZWZhdWx0In0.
NfLQHdh219p2NjzR44q9xgrQ9m6ky1paJ2GpHf2Re8tXjKyZNFxjYu9Tb78RoX3-
x1sX0dmrRJBmW0_z1vy-
0NrnHkU2fpBrBVdauqsXadCCKFFnkYy8AAJZg2WxyUNmaAcZWPT9z3svcQBHq90Q
MdrkUvq3WbD91LbS5MA5p0kU8LofMn2j8nisoLRaQ904CX1lKPl8jWILxtai-
8hHgZ5t62Z-BYis3m1xiWPJ7zEctMRoule5pyFRYHxwudBht3Y9M04uDEQaIAk3d0uiVDup4eFJBt-
Vt1Jt42f5hX28GyQQNu13s-rVArAXYxHGx4hzNZZTlw9EUdDPuEg",
    "GrantType": "JWT_BEARER"
  }
}

```

Mandatory Request Headers**Table 3-4 Mandatory Request Headers**

Headers	Expected Value
X-OAUTH-IDENTITY-DOMAIN-NAME	OFSLL_OAUTH_DOMAIN
Authorization	Bearer <Base64encoded value of client credentials>

Sample JSON Response

```
{
  "AuthResponse": {
    "Token":
      "eyJraWQiOiJPRlNMTF9TU09fVEVTVF9ET01BSU4iLCJ4NXQiOiJjQldCa0pqV2JvdHRHczFmZFd1YzdtE0tMwsiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbXVtMDBjaWUuaW4ub3JhY2xlLnNvbToxNDUwMC9vYXV0aDIiLCJhdWQiOi01dLCJleHAiOiE1NDU2NzQ1NzQsImp0aSI6InZTcE1LVzlhZlVhZlV2VngxZU5KRUZ1ZVEiLCJpYXQiOiE1NDU2NzA5NzQsInN1YiI6Ik9GU0xMU1VQUiIsImN1c3RvbWVDbHRyMSI6IkN1c3RvbVZhbHVlIiwic2Vzc2lvbkklIjoImZExY2MxOWUtODhkZi00ZDdhLTg5YzQtODFjNmRiMDE5ZDUzZfEZqN2NTcTzQcWlQUVZSNXU4TTNlRVpqbUJEZHVkQm9HeK5sMDBNQkFnS009IiwicmVzU3J2QXR0ciI6IlJFU09VUkNFQ090U1QiLCJjbGllbnQiOiJPRlNMTF9CMkIjSkvUX0NMSUV0VCIsInNjb3BlIjpbIk9GU0xMU1N1NTT19URVNUX1NFU1ZFU19CMkIuQWNBj3VudERldGFpbHMlXSwiZG9tYWluIjoitOTTEtfU1NPX1RFU1RfRE9NQ10In0.guHeG7eZilGwpJhMwLIpH4K3lBgtM8buuwJPIlk6EengFteicbfpd0E3qZwp8SYRFuzvw4FX7wCSbbBt2WM9G4L6uM0NTvZpSTcwUe0ljuysMiCmPzQ-8cSijpM4G55Fb351aulC7eiCNDMtKoH34A2lScX7lamjlpC0u4SV4V-8cB4VviGtrd_sXIq0fgSadpjrXQatuaRID1at4aNoAGv1Da7E4xrMzy9m41cxHtujsNU2aDxG73-b2q0JiNZbvzfzlaaa2pu1T00r1ynZDvbe3STsZkAK01VKFchZmnYW8Tpqovc6MNd0TPyhNFUJHDBsPH-nKV_nkFQHyo0_jw",
    "Expires_in": 3600,
    "TokenType": "Bearer",
    "Result": {
      "Status": "SUCCESS",
      "StatusDetails":
        "Token Generated Successfully"
    }
  }
}
```

3.5.5 Access Token for REFRESH_TOKEN grant type

Sample JSON Request

```
{
  "AuthRequest": {
    "GrantType": "REFRESH_TOKEN",
    "RefreshToken": "Mtn+NHd1zyCwelBiAcfy3w==~ALGXo2ieTTwvnk8tk5H0i5L4FN900wWPCpZgmHMaDX8PgbwQRU/HH+TGtamC5YU4Pqp3ZRM7va/TzIc8EHEQxsfy0e3pBG1/KD2CkfeL0M0PfqstzE1Lq7bkfQxKj9jZNIffvKEHnFVLPgh2XR0xSjIbTK3EeP5Eyoxf7aaTNU79CBM3Ws5mrkGKhj2l2o2LfTTAbw/thEQLK9A7vXlGj8cSAuuFsAREfAy/skriZZfMQKxKY3Ewh1Cm1coBmG5aT3DFe9LxgPuSmght1kLKqyDhjK0n0okU01XsHwPh0cwXgeWB1KXVzd3o06h0eJ/SaTvFIUEEictWAgymGDLsVVDfriZnHVQA05TQsXFskoTPtrjA14C"
  }
}
```

```
PWoibLgYRdiPl0bcj32c+CMmywlcLK/+v4+xh44lBu92fvW/HzPxAWDJ3lPyM2AvgP1SEd
8LiHcrwyh8rR8JTKJpWkNMmxW4S0p/6g//dUiWD9QEGCwUnBINweUpRoA76k2Gbgq+
NJ18ohF8epeUy+ftvjjeefNuoU41KI3mprlrReHuG00I5GJScwC3w1zuEUgJsBZc4QN9Fju
Js/I/aMTPKRT683x33WLQt3NkH0CW+g8XyeiSVaic/k2DtDyPwpnCuzNbZzqvjgx93Zga
o0vBMLDB9+hZzfNMyb0VrIlcdvwegAubETgIpLEdmcu/2Bpc1XjLJgJ8hMd9xE5xrv/7NDg+
sUjpMkrin80nEq0rzUlWLMgC2a105PMgkGA2Rudhm/4VUXzKEK4ItGoR2CEMPHTGrKp
uFvdvZoyjh4JMfwTgH6F1KUV4AMgE+vPzQNEngSxxseewavmJbjB80jGvuC/G00hdY3
YYWvz2CtEWA08261unvuroUceNfGbTSK/Z3x4I8iuCfG8n7ZLyc9a3m8WTVsoodkLnZS
8mYU4dFEXvsS35gnuyzZvXR0BkJ44+2VpfdmB55q0PUziZK2UKZJ1Hg5jqTCwSMDg
+9qWVhbnpdzFtjqETF0edUI7F0QkotXkEHUTMSOTgR4d47pa0JQDlSW3Lr1n8+7YNA/r
KIUTTIoP6I7lcl/rZ2BDazmVgf3axZ/Oo+xbtJCABrfGqNJA10cBf/hJmktSXY+osj4CairKGh
cteFPziE0eo5+sbAsTthAadaLYcPs6/4mNoK7yvyLoxul0EY7CSXZSaP0otsV49LX3fEjH
gkvkDU3dhcPPc9DmlyDDySK018K7wgaPnJtCSu1fq2AwVwDmwRd6BZsAISn3dHqGDU
+XTgr7dt7ag3JyxmtuZQrGJiPbJp5gExgnS6JyJIF2co75kXvWoHm30/p8="
}
}
```

Mandatory Request Headers

Table 3-5 Mandatory Request Headers

Headers	Expected Value
X-OAUTH-IDENTITY-DOMAIN-NAME	OFSLL_OAUTH_DOMAIN
Authorization	Bearer <Base64encoded value of client credentials>

Sample JSON Response

```
{
  "AuthResponse": {
    "Token":
      "eyJraWQiOiJPRlNMTF9TU09fVEVTVF9ET01BSU4iLCJ4NXQiOiJjQldCaOpqV2JvdHRH
      HczFmZFd1YzdtE0tMwsiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwOi8vbXVtMDBja
      WUuaW4ub3JhY2x1LnNvbToxNDEwMC9vYXV0aDIiLCJhdWQiOi0tdLCJleHAiOiJlNDU2
      NjI4MTgsImp0aSI6InZGZ082eUlFb0k2X0xoZ3czcmczTUEiLCJpYXQiOiJlNDU2NjI4MT
      gsInN1YiI6Ik9GU0xMU1VQVU1Sik9BVVRIX1RPS0V0Ijo1ZXlKcmFXUWlPaUprWldaaGRX
      eDBJaXdpZURWME1qb2lZa3c1VkrJNGJIAe1RakowY1c1eGQyZDRZMEZPUW5vdFFY
      WnpJaXdpwVd4bk1qb2lVbE15TlRZaWZRLmV5Smx1SEFpT2pFMU5EVTJ0RFF4T0RBc
      0ltcDBhU0k2SWpGS1ZwbGlibXBFWkVwVdWQk5Tb1JvUkV0TmIzY2lMQ0pwWVhRa
      U9qRTFORFUYtKRBMU9EQXNjbk4xwWlJNklrOUdVMHhNVTFWUVVpSXNjbk5sYzN
      OcGIyNWZhV1FpT2lJemNWRXplbVZ2TldwWlEzVnJhbG5qUW1aRWFfSlJQVDEtU2sx
      amJHMW1TMw8wUmxKUK9GTnJSVXBVXpCdGR6MDlJaXdpwkc5dFlxbHVJam9pw
      kdWbVlYVnNkQ0o5LlpHQWdTZGR5S0szRGplMlZsTUlmbzMxTTV0cFBpaXluUVpGY2R
      iBEFiV2xhektPWVfZb2hqbzdrODQxQm9SMWUtWXZWLXpwbk5hamhCYy1CbzAwZlNs
      VDdsVmNmRXA2ekxUdENHRnc1MkNZRXpfOHpYdjc1YkF2Q2FweGRvZnluUaGFhdFox
      cVF5Qm5TLUJ1MGdKNjJSOTkkaDFwY1FOSmFhWDZ1RkxkSGVoVUlDY1pNLUJwbU
      drbi01TXhHcm5fQnloT2oxc0JnRjZ1SWY0N3d6NU1NOU4zODdHQ29WZDBPR3c0QXlm
      VVk2T2FGS1NOS1hYbnpsYUVDtkktMEJmQXhFQk1SX1oxVE1wZEdSOHkwaHltMWNT
      SzRGYkJjYnQxZn1hYmdLMG1SQ0tFVHdMWFJrcnFMcmkxTnVtbjNKeFhmZVBBSwTVJT
      m1ndDA2U1BVaFpYUEU2ZyIsImN1c3RvbWVDbHRYMSI6IkN1c3RvbVZhbHVlIiwic2Vzc
      2lVbklkIjo1Q09PS0lFX0JB00VEIiwicmVzU3J2QXR0ciI6I1JFU09VUKNFQ090U1Q1LCJjbG
      1lbnQiOiJPRlNMTF9CMkIuQWVudERldGFpbHMxSWiZG9tYWluIjo1T0ZTTExfU1NPX1R
      FU1RfRE9NQUL0In0.BKsW01yBEmc_f0jCdG16DxzKtkkN805VmYlBbyMmmMqznZisyc
```

```

orlzHAZ0RHTDqNLjKdq--
wxzTNQK4PRM9ChBeHKBCU5dzHD64ddbscyt0YxpdPnF0grMZHipIoNC_-
nZxyZRbLI5aQeGPX0Z4qtPEZ1ggBkgoXXa16eJ2JLZbY0tcvPbLcbkfHpMCzw0zi_
o0t30KG9T1931NyMaCvYp40-Z0DTneHc9-
c7cJaj2zVhk0Fej796TTrEHV4jv7p20Tsawkm8vSYmRBv5K1J8M_a1PgEIuqc4kS6d0op
UAJ0KT6C3560MdEpe0_zkXGyfodUFKojdG3PWHXG007ww",
"Expires_in": 3600,
"TokenType": "Bearer",
"Result": {
"Status": "SUCCESS",
"StatusDetails":
"Token Generated Successfully"
}
}
}
}

```

3.5.6 How to get access token through Basic Authentication

Mandatory CSF Key

Table 3-6 Mandatory CSF Key

CSF Map name	Key
ofssl.int.common	ofssl.jwt.JwtSecretKey

The Ofssl.jwt.JwtSecretKey refers to the secret that must be associated at the time of token generation. This is the key would be used to validate the token.

Mandatory Request headers

Table 3-7 Mandatory Request headers

Headers	Expected Value
Content-Type	application/json
Authorization	Bearer <Base64encoded value of resource owner credentials>

Request JSON payload

```

{ "AuthRequest": {
  "GrantType" : "PASSWORD"
}}

```

Response JSON payload

```

{
"AuthResponse": {
"Token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJPRlNMTFNlbnVFIiLCJpc3MiOiJPRlNMTF9SRVNUX0FQSSIsImV4cCI6MTU0NTY3MjEyMSwiYW50IjoxNTQ1Njc4MjIxMjE5Lm5kb3VhZjU5dXt0eXZyY4b0ayz9XpT5J2jYu8zIHR4uvkKanyvRgU10SXhovdyw8zMl_ajqDLdESc_lZv3w",
"Result": {

```

```

"Status": "SUCCESS",
"StatusDetails": "Token Generated Successfully"
}
}
}

```

3.5.7 How to access the REST API using the access token

In Every OFSLL REST API request, please send the following headers with correct values.

Mandatory Request headers

Table 3-8 Mandatory Request headers

Headers	Expected Value
ofsll_access_token	The valid access token received from any of the above mention flow
X-OAUTH-IDENTITY-DOMAIN-NAME	Valid OAuth Identity domain associated with access token

3.6 Embedding External Application within OFSLL

As part of subsequent releases of OFSLL, to embed external application within OFSLL base application, we would provide one external link each under origination, servicing and collection modules. The associated menu links can be enabled through access screens.

Table 3-9 Menu Access Keys

Menu Access Keys
FLL.ORG.EXT.ONE.MENU
FLL.SER.EXT.ONE.MENU
FLL.COL.EXT.ONE.MENU

The URLs for External Link will be defined through System parameters. The following URL keys need to be defined with proper external link.

Table 3-10 URL keys

URL Keys	Example
FLL.ORG.EXT.ONE.URL	http://<<hostname>>:<<port>>/<<contextpath>>/index.html
FLL.SER.EXT.ONE.URL	http://<<hostname>>:<<port>>/<<contextpath>>/index.html
FLL.COL.EXT.ONE.URL	http://<<hostname>>:<<port>>/<<contextpath>>/index.html

Note

The base OFSLL SSO application would send the user identity token called 'authorizedCode' through the URL query parameter which should be read by external application to generate the actual access token (by calling authentication service) in order to access protected OFSLL Rest API.

Request JSON payload for JWT BEARER grant type

```
{
  "AuthRequest": {
    "Assertion": "eyJraWQiOiJkZWZhdWw0IiwieDV0IjoieiYkw5VDI4bHhMqJj0cW5xd2d4Y0FOQnotQXZzIiwiaWxnIjoieiUlMyNTYifQ.eyJleHAiOiE1NDU2NzQ1MDEsImp0aSI6ImRdCuFabERSVfdrX2lwd21aTDBfVHciLCJpYXQ0IjE1NDU2NzA5MDEsInN1YiI6Ik9GU0xMU1VQUiIsInNlc3Npb25fawQ0IjEelVmNlZyN05FQ2NHYNVBbVVINU9RPT1-NmdhemlUU2Y10VdPb0FLZHRhc0h0R3R4L3p6TktSK0lEZDd50G10emRPZ2FMQUk2NjliRytEbzY0NFdGV3NWMTMwS1pUbDJrTwd1OHp5TTFEawtteFdtYVURk0dyUXlidGo3WVB6dlRwdzlbmFVMT3d1cEFBbUpqMi9VLzlVYVUiLCJkb21haw4iOiJkZWZhdWw0In0-Qi4gJ4kiEcxgs51fRU3633RcPMDNjq0PrRnzB0q8M9pKIeRmNe2Zyu7ikBXqIJfMD0Iz-N9hUgvd9i8-5lPeEER15_FqlsPtoCUX3u8NuPPfzqA_xt2LTcc0-6AdGz7QrsqAU_qr3n2FGF5qhiHU7437X_AzoMBwTYovWsl8Rjra_tdWoCMsMRisN7xqIew7Jk3awYQeo0HbwfuVqDE18m67du9rUszNurX483KXwCfZL1ffbqYIFYIGekGpm4AbCq5aazK8-HtrmzKyt-Q1Monx2dOrUorLkM6AtKXT0qdrA2YwASYM96A4ENLTdxjcIyTUDcwIu4WgeBUcwJzw",
    "GrantType": "JWT_BEARER"
  }
}
```

Mandatory Request Headers

Table 3-11 Mandatory Request Headers

Headers	Expected Value
X-OAUTH-IDENTITY-DOMAIN-NAME	OFSLL_OAUTH_DOMAIN
Authorization	Bearer <Base64encoded value of client credentials>

Response JSON payload

```
{
  "AuthResponse": {
    "Token":
      "eyJraWwQI0iJPRlNMtF9TU09fVEVTVF9ET01BSU4iLCJ4NXQiOiJjQldCa0pqV2JvdHRHczFmZFdldYzdtE0tMwsiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwOi8vb3VtMDBjaWUuaw4ub3JhY2xlLmNvbToxNDUwMC9vYXV0aDIiLCJhdWQiOi0tdLCJleHAiOiJlNDU2NjI4MTgsImp0aSI6InZGZ082eU1Fb0k2X0x0Z3czcmczTUEiLCJpYXQiOiJlNDU2NjI3NTgsInN1YiI6Ik9GU0xMU1VQUiIsIk9BVVRlX1RPS0V0IjojZXlKcmFXUWlPaUprWl daaGRXeDBJaXdpZURWMElqb2lZa3c1VkrJNGJlIaE1RakowY1c1eGQyZDRZMEZPUW5vdFFYwmpJaXdpwVd4bklqb2lVbE15TlRZawZRLmV5SmxlSEFpT2pFMU5EVTJ0RFF4T0RBC0ltcDBhU0k2SwpGS1ZwbGlibXBFWkwVwVdWQk5Tb1JvUkV0TmIzY2lMQ0pwwVhRaU9qRTFORFUYtkRBMU9EQXNjBk4xwWlJNk1rOudVMHhNVTFWUUVpSXNjBk5sYzNOcGIyNWZhV1FpT2lJemNWRXplbVZ2TldwWlEzVnJhbGk5QUw1aRWFfSlJ0VDEtU2sx
```

```
amJHMW1TMW8wUmxKUK9GTnJSVXBPVXpCdGR6MDlJaXdpWkc5dFlxbHVJam9pW
kdWbVlYVnNkQ0o5LlpHQWdTZGR5S0szRGp1MlZsTU1mbzMxTTV0cFBpaXluUVpGY2R
ibEFiV2xhektPWVFzb2hqbzdrODQxQm9SMWUtWXZWLXpwbk5hamhCYy1CbzAwZlNs
VDdsVmNmRXA2ekxUdENHRnc1MkNZRXpfOHpYdjC1YkF2Q2FWeGRvZn1UaGFhdFox
cVF5Qm5TLUJ1MGdKNjJS0ThkaDFwY1FOSmFhWDZ1RkxkSGVoVUlDY1pNLUJwbU
drbi01TXhHcm5fQnloT2oxc0JnRjZ1SWY0N3d6NUlN0U4zODdHQ29WZDBPR3c0QXlm
Vvk2T2FGS1N0S1hYbnpsYUVDtkktMEJmQXhFQklSX1oxVE1wZEdS0HkwaHltMWNT
SzRGYkJjYnQxZn1hYmdLMG1SQ0tFVHdMWFJrcnFMcmkxTnVtbjNKeFhmZVBswTVJT
m1ndDA2U1BvaFpYUEU2ZyIsImN1c3RvbWVbDHRyMSI6Ikn1c3RvbVZhbHVlIiwic2Vzc
2lwbklkIjoiQ09PS0lFX0JBU0VEIiwicmVzU3J2QXR0ciI6IlJFU09VUKNFQ090U1QiLCJjbG
llbnQiOiJPRlNMTF9CMkJfSkVUX0NMSUV0VCIsInNjb3BlIjpbIk9GU0xMX1NTT19URVN
UX1NFU1ZFU19CMkIuQWNjb3VudERldGFpbHMiXSwiZG9tYWluIjoiT0ZTTExfU1NPX1R
FU1RfRE9NQUL0In0.BKsw01yBEmc_f0jCdG16DxzKtkN805VmYlBbyMmmMqnziNsync
orlzhAZ0RHTDqNLjKdq--
wxzTNQK4PRM9ChBeHKBCU5dzHD64ddbscyt0YxpdPnF0grMZHipIoNC_-
nZxyZRbLI5aQeGPX0Z4qtPEZ1ggBkgoXXa16eJ2JLZbY0tcvPbLcbkfHpMCzwOzi_
o0t30KG9T1931NyMaCvYp40-Z0DTneHc9-
c7cJaj2zVhk0Fej796TTreHV4jv7p20Tsawkm8vSYmRBv5K1J8M_a1PgEIuqc4kS6d0op
UAJ0KT6C3560MdEpe0_zkXGyfodUFKojdG3PWHXG007ww", "Expires_in": 3600,
"TokenType": "Bearer",
"Result": {
"Status": "SUCCESS",
"StatusDetails": "Token Generated Successfully"
}
}
}
```