**OAuth2.0 with any(OID/IDAM/JIO AD/ADLDS/HNH/RR mHere/SCRUM and PRMS) user store**

OAuth 2.0 framework provides authentication and authorization.

# **Pre-Configurations**

**SECO API Portal:**

Login into the **SECO API Portal** and edit the **application**. In the edit application screen click **Auth** tab and enter the below values and then click on **save** button

**Callback URL**: https://<**GatewayDomain** or **IPAddress**>:<port>/v1/testabc

**Scope:** agent - User exists in OID

**Scope:** consumer - User exists in IDAM

**Scope:** employee - User exists in JIO AD

**Scope:** hnh - User exists in HNH

**Scope**: remp- User exists in RR mHere

**Scope**: consultant- User exists in SCRUM and PRMS (Non-Employee Authentication)

**Type:** Public

**Steps to be followed for accessing API’s secured by OAuth**

# **Generate Access Token**

Accessing an **OAuth** protected API needs to be sent with **access\_token** along with other required parameters for it. In order to get the **access\_token** user needs to be authenticated first by sending the user credentials against user store (**OID** or **IDAM** or **JIOAD** or **RR mHere** or **SCRUM and PRMS**)

Access the below **URL** with required query and header parameters for **getting/generating** the **access\_token**.

**URL:**

https://<**SECO API Domain** or **IP Address**>:<Port>/auth/oauth/v2/token?**state**=state\_test&**scope**=<scope>&**client\_id**=<**api key**>&client\_secret=<**client secret**>&**grant\_type**=password

**Query Parameters:**

Change the below specified query parameter values only which are obtained from the **SECO API Portal** and keeping the remaining as it is.

**client\_id:** API Key which is obtained from SECO after registering an Application/App

**client\_secret:** API Secret which is obtained from SECO after registering an Application/APP

**scope:** scope which is obtained from SECO after registering an Application/APP.

scope = agent -- For OID

scope = consumer – For IDAM

scope = employee – For JIO Employee AD

scope = hnh – For HNH

scope = remp- For RR mHere

scope = consultant—For SCRUM and PRMS(Non-Employee Authentication)

**Header Parameters:**

Sending login/authentication credentials in the request header

**username: <**username**> (**user name existing in OID/IDAM/JIOAD/ADLDS/HNH/RR mHere/SCRUM and PRMS) -- Required

**password: <**password> (Password of the user) – Required

**Imode**: AUTH- (If scope is remp)- Required for Authentication

**srvc:** <mobile\_service\_provider\_name>- for single user using multipe mobile service provider and scope is agent (For example- srvc:idea)-- Optional

**ttl:<**no. of seconds**> (**No. of seconds the oauth token should/will be active**) --** Optional

**Note:**  Header parameter **ttl** should be an integer value and default value is **3600 seconds**

**Http Method:**  POST

**Success Response (for scope=agent):**

**{**

**"access\_token": "303f564a-2fd9-4199-9f2b-76f7f68f3bd7",**

**"token\_type": "Bearer",**

**"expires\_in": "3600",**

**"refresh\_token": "32ba2b66-ad23-4541-b7a4-4915ef79e733",**

**"scope": "agent",**

**"associate": {**

**"agentCode": "secoadmin",**

**"aadhaarId": "",**

**"name": "secoadmin",**

**"Role": "",**

**"areaOffice": "",**

**"functionalManagerId": "",**

**"lineManagerId": "",**

**"parentCompany": "",**

**"Organization": {**

**"RJILDepartment": "",**

**"Org": "",**

**"name": "",**

**"distributionCenter": "",**

**"city": "",**

**"state": "",**

**"circleId": ""**

**},**

**"ContactDetails": {**

**"email": "",**

**"phoneNumber": ""**

**},**

**"memberOfGroups": [],**

**"group": ""**

**}**

**}**

**Success Response (for scope=consumer):**

**{**

**"access\_token": "5df48180-f484-4bd5-8232-abecc09e9b79",**

**"token\_type": "Bearer",**

**"expires\_in": "3600",**

**"refresh\_token": "f12d1523-780d-4cad-8fcb-237f009225c4",**

**"scope": "consumer",**

**"associate": {**

**"agentCode": "ril1100022470",**

**"ssoToken": "AQIC5wM2LY4SfcyVl9ogrOC9yqGt5YGxeKazPGqQWO56LzM.\*AAJTSQACMDIAAlNLABM0OTIyNjYwOTgxNzA3OTc2NzIwAAJTMQACMDM.\*"**

**}**

**}**

**Success Response (for scope=employee):**

**{**

**"access\_token": "d782b0cf-5cf8-4b46-9cad-75e641639ff6",**

**"token\_type": "Bearer",**

**"expires\_in": "3600",**

**"refresh\_token": "c511fa7f-be78-4195-990d-be714a293c11",**

**"scope": "employee",**

**"associate": {**

**"agentCode": "Jio.Employee",**

**"FirstName": "Jio",**

**"lastName": "Employee",**

**"displayname": "Jio Employee (Consultant)",**

**"username": "Jio.Employee",**

**"Email": "jio.employee@ril.com",**

**"employeeID": "0001",**

**"mobile": "+91991237456",**

**"streetAddress": "TC23 Block D",**

**"dn": ""**

**}**

**}**

**Success Response (for scope=hnh):**

**{**

**"access\_token": "d782b0cf-5cf8-4b46-9cad-75e641639ff6",**

**"token\_type": "Bearer",**

**"expires\_in": "3600",**

**"refresh\_token": "c511fa7f-be78-4195-990d-be714a293c11",**

**"scope": "hnh",**

**"associate": {**

**"agentCode": "Jio.Employee",**

**"firstName": "Jio",**

**"lastName": "Employee",**

**"email": "jio.employee@ril.com",**

**"mobileNumber": "+91991237456",**

**“flag”:”true”**

**}**

**}**

**Success Response (for scope=remp):**

**{**

**"access\_token": "",**

**"token\_type": "",**

**"expires\_in": "",**

**"refresh\_token": "",**

**"scope": "",**

**"associate": {**

**"agentCode": "",**

**"FirstName": “",**

**"lastName": "",**

**"displayname": "",**

**"Email": "",**

**"employeeID": "",**

**"mobile": "",**

**"dn": "",**

**"worklocationID": ""**

**}**

**}**

**Success Response (for scope=consultant):**

**{**

**"access\_token": "",**

**"token\_type": "",**

**"expires\_in": "",**

**"refresh\_token": "",**

**"scope": "",**

**"associate": {**

**"agentCode": "",**

**"FirstName": "",**

**"lastName": "",**

**"displayname": "",**

**"Email": "",**

**"employeeID": "",**

**"mobile": "",**

**"dn": "",**

**"worklocationID": ""**

**}**

**}**

**Note:**

* **agentCode** value needs to be set as **uid** value in subsequent calls.
* **uid** will be used in accessing  the **API’s** and **refresh\_token** service after successful authentication along with other required parameters.
* Also the consumers should store the **refresh\_token** and other user related information on the **client side** so that those can be used whenever required in subsequent calls.

**Possible Failure Responses:**

**1)**

**{**

**"success": false,**

**"errors": [**

**{**

**"code": “400”,**

**"reason": "invalid\_grant",**

**"details": "Resource Owner authentication failed"**

**}**

**]**

**}**

**2.**

**{**

**"success": false,**

**"errors": [**

**{**

**"code": "RIL4G\_T\_SECO\_7026",**

**"reason": "OAuth access token life time is not valid",**

**"details": "OAuth access token life time should be a number"**

**}**

**]**

**}**

**3.**

**{**

**"success": false,**

**"errors": [**

**{**

**"code": "RIL4G\_T\_SECO\_7027",**

**"reason": "OAuth access token life time is not valid",**

**"details": "Max. allowed time for access token is 86400sec"**

**}**

**]**

**}**

# **Accessing OAuth Protected API**

After successful authentication and obtaining the access\_token call the required API that’s protected with OAuth with required parameters and **access\_token** in authorization header.

**URL:**

https://<**SECO API Domain or IP Address**>:<Port>/<URI API>

**Http Method:** POST/GET

**Header Parameters:**

**Authorization:** Bearer **<**access token value**> (Access token** is one of value from response obtained after successful authentication in step 1**)**

**uid: <**agentcode> **(agentCode** is a value from response obtained after successful authentication in step 1**)**

**Success Response:**

**{**

“success”: true,

                <Other data based of the API>

**}**

**Failure Response:**

If the failure is due to invalid or expired Access token, following error is returned.

**{**

**"success": false,**

**"errors": [**

**{**

**"code": “**0**”,**

**"reason": "invalid\_request",**

**"details": "Validation error"**

**}**

**]**

**}**

# **Refresh Token**

Refresh token is request is to be used when the **access token** is expired and want to get the new **access token** without sending the user credentials

**URL:**

https:// <**SECO Domain or IP Address**>:<Port>/auth/oauth/v2/token?client\_id=<**api key**>&client\_secret=<**client secret**> &grant\_type=refresh\_token&refresh\_token=<**refresh token**>&uid=<userid/agentcode>

**Http Method:** POST

**Query Parameters:**

Set values for these query parameters which are obtained from the SECO API Portal and successful authentication

**client\_id:** API Key which is obtained from SECO after registering an Application/App

**client\_secret:** API Secret which is obtained from SECO after registering an Application/APP

**refresh\_token:** Refresh token is obtained in the response from SECO after successful authentication

**Success Response:**

**{**

 **"access\_token": "c51d1431-060a-43c3-b411-96fd508b5e05",**

    "token\_type": "Bearer",

    "expires\_in": 3600,

**"refresh\_token": "8aa5efe3-b1fc-4c9f-8b6c-116061bcecb6"**,

    "scope": "agent",

    "uid": "secoadmin"

**}**

**Failure Response:**

If the failure is due to invalid Refresh token being sent, following error is returned.

**{**

**"success": false,**

**"errors": [**

**{**

**"code": “RIL4G\_T\_SECO\_7021”,**

**"reason": "invalid\_request",**

**"details": "Invalid Request"**

**}**

**]**

**}**

# **Validate OAuth access\_token**

This service is used to verify whether the **access\_token** user has is valid one or not. Any consumer/application having **access\_token** and wanted to interact with other systems without **SECO** should be using this **SECO** service to valid the requestor (i.e. consumer/application) and then only allow or deny the access accordingly.

**URL:**

https://<**SECO API Domain or IP Address**>:<Port>/validate/oauth/token

**Http Method:** POST

**Header Parameters:**

**Authorization:** Bearer **<**access token value**> (Access token** is one of value from response obtained after successful authentication in step 1**)**

**uid: <**agentcode> **(agentCode** is a value from response obtained after successful authentication in step 1**)**

**X-API-Key :** API key obtained from API portal (after adding this API to your application)

**Success Response:** In success response **Http Response Status Code** will be **200 OK** with no content or data.

**Failure Response:**

If the failure is due to invalid or expired Access token, following error is returned.

**{**

**"success": false,**

**"errors": [**

**{**

**"code": “0”,**

**"reason": "invalid\_request",**

**"details": "Validation error"**

**}**

**]**

**}**

# **Revoke Token**

Revoke token request is to be used when the **access token** generated using [Generate Access Token](#_Generate_Access_Token) or [Refresh Token](#_Refresh_Token) need to be deleted from OAuth server. This is usually done when user wants to logout from the OAuth application.

**URL:**

https://<**SECO Domain or IP Address**>:<Port>/auth/oauth/v2/token/revoke?client\_id=<**api key**>&client\_secret=<**client secret**>&token=<accesstoken>&uid=<userid/agentcode> &token\_type\_hint=access\_token

**Http Method:** POST

**Query Parameters:**

Set values for these query parameters which are obtained from the SECO API Portal and successful authentication

**client\_id:** API Key which is obtained from SECO after registering an Application/App

**client\_secret:** API Secret which is obtained from SECO after registering an Application/APP

**token:** Access token obtained in the response after successful authentication from [step1](#_Generate_Access_Token)/[step3](#_Refresh_Token)

**uid: <**agentcode> obtained after successful authentication from step 1

**Success Response:** In success response **Http Response Status Code** will be **200 OK** with no content or data.

**Failure Responses:**

1. If the failure is due to invalid token being sent, following error is returned.

**{**

**"success": false,**

**"errors": [**

**{**

**"code": "RIL4G\_T\_SECO\_7021",**

**"reason": "invalid\_request",**

**"details": "Invalid Request"**

**}**

**]**

**}**

1. If mandatory parameters are not sent in the request.

**{**

**"success": false,**

**"errors": [**

**{**

**"code": "RIL4G\_T\_SECO\_7016",**

**"reason": "Bad Request",**

**"details": "Input data required is missing"**

**}**

**]**

**}**