**OAuth2.0 with any(OID/IDAM) user store**

OAuth 2.0 framework provides authentication and authorization.

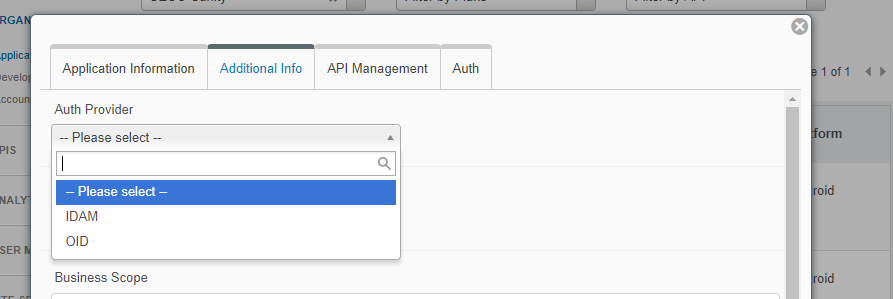
# **Pre-Configurations**

**SECO API Portal:**

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

Select Auth Provider and Authorized Grant Type as shown in Screen shots.

1. **Selecting Auth Provider.**

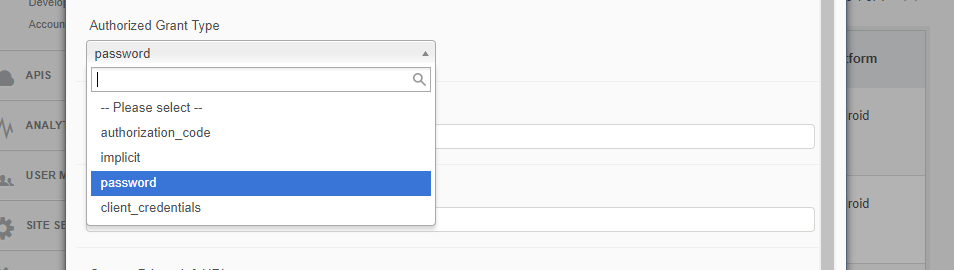


**Note:**

Auth Provider**:** OID - User exists in OID

Auth Provider**:** IDAM - User exists in IDAM

1. **Selecting Authorized Grant Type :**



**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**)

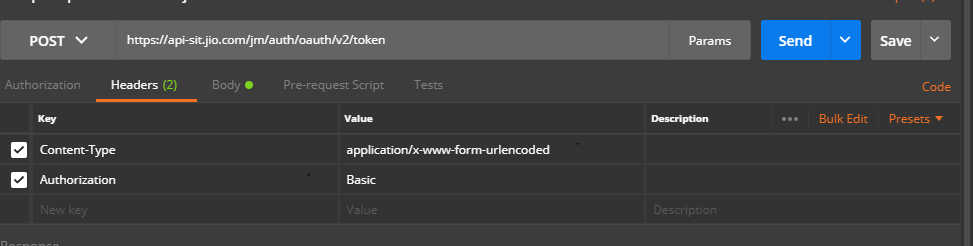
Access the below **URL** with required query and header parameters for **getting/generating** the **access\_token**.

**URL:**

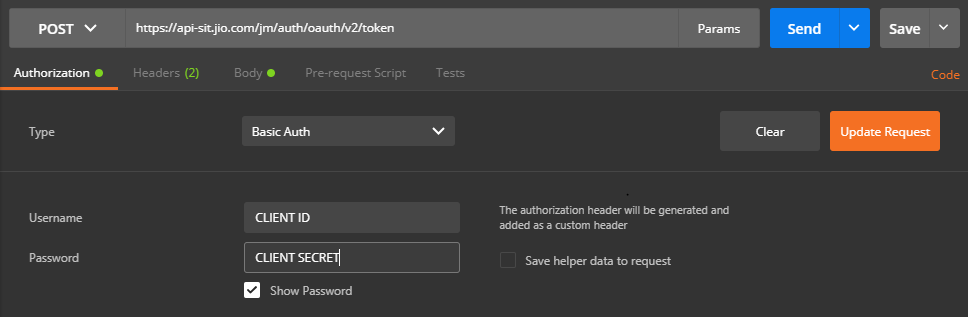
https://<**SECO API Domain** or **IP Address**> :< Port>/jm/auth/oauth/v2/token

**Header Parameters:**

Send below specified header parameters as shown in screen shot.



Add Client\_Id in Username and Client\_Secret in password and click on Update Request. Please follow below screen shot to add Authorization header.



**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

**BODY(x-www-form-urlencoded) Parameters:**

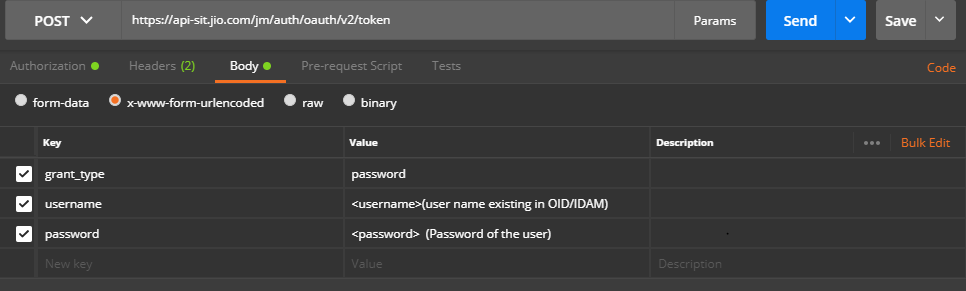
Sending login/authentication credentials in the request body (x-www-form-urlencoded)

**username: <**username**>(**user name existing in OID/IDAM) -- Required

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

**grant\_type:** password

**Please refer screen shot for any confusion.**



**Http Method:**  POST

**Success Response (for** Auth Provider: OID**):**

**{**

**{**

**"access\_token": "e1b0ceac-9a43-4a88-8d1b-1b09cb8992c5",**

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

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

**"refresh\_token": "9c8ab7f7-c052-4a6b-aa3f-3d4846b98c0b",**

**"scope": “agent"**

**}**

**Success Response (for** **Auth Provider: IDAM):**

**{**

**{**

**"access\_token": "5ef54358-2ab2-4cc3-85c6-8303bc13fc04",**

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

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

**"refresh\_token": "54446b19-cc23-40d1-9c5f-bcfd390ef6fb",**

**"scope": "consumer"**

**}**

**Note:**

* 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"**

**}**

**]**

**}**

# **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**)**

**Success Response:**

**{**

“success”: true,

                <Other data based on 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**

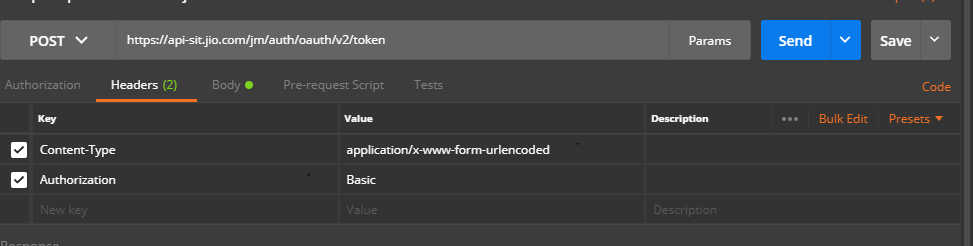
Refresh token request is to be used when the **access token** is expired and want to get the new **access token** without sending the user credentials

**URL:**

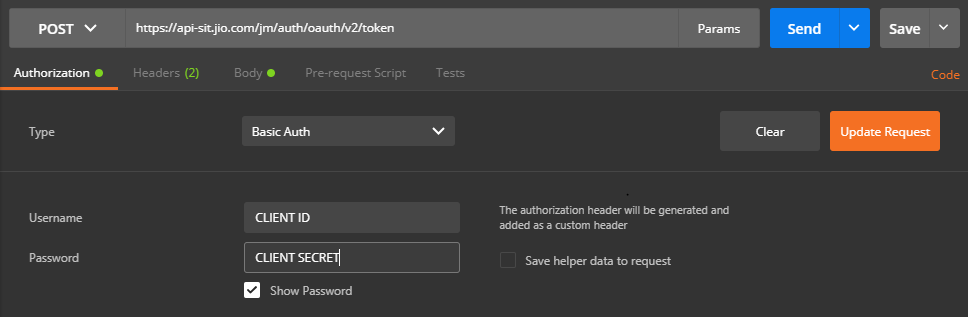
https://<**SECO API Domain** or **IP Address**> :< Port>/jm/auth/oauth/v2/token

**Header Parameters:**

Send below specified header parameters values only which are obtained from the **SECO API Portal** .PFA of screen shot.



Add Client\_Id in Username and Client\_Secret in password and click on Update Request to add Authorization header in request. Please follow below screen shot to add Authorization header.



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

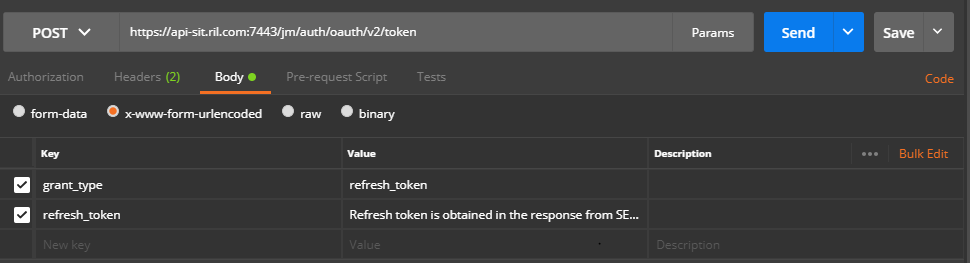
**client\_secret:** API Secret which is obtained from SECO after registering an Application/APP

**BODY(x-www-form-urlencoded) Parameters:**

Sending login/authentication credentials in the request body (x-www-form-urlencoded)

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

**Please refer screen shot for any confusion.**



**Http Method:**  POST

**Success Response (for** Auth Provider: OID**):**

**{**

**{**

**"access\_token": "e1b0ceac-9a43-4a88-8d1b-1b09cb8992c5",**

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

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

**"refresh\_token": "9c8ab7f7-c052-4a6b-aa3f-3d4846b98c0b",**

**"scope": “agent"**

**}**

**Success Response (for** **Auth Provider: IDAM):**

**{**

**{**

**"access\_token": "5ef54358-2ab2-4cc3-85c6-8303bc13fc04",**

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

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

**"refresh\_token": "54446b19-cc23-40d1-9c5f-bcfd390ef6fb",**

**"scope": "consumer"**

**}**

**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 **"**

**}**

**]**

**}**

# **Revoke Token**

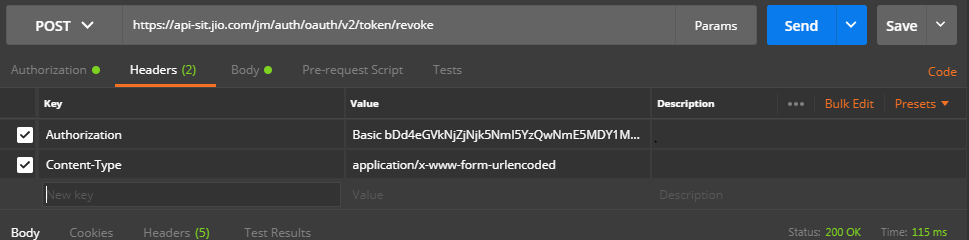
Revoke token request is to be used when the **access token** generated using [Generate Access Token](#_Generate_Access_Token) or [Refresh Token](#_Refresh_Token) need to be deleted from OAuth server. This is usually done when user wants to logout from the OAuth application.

**URL:**

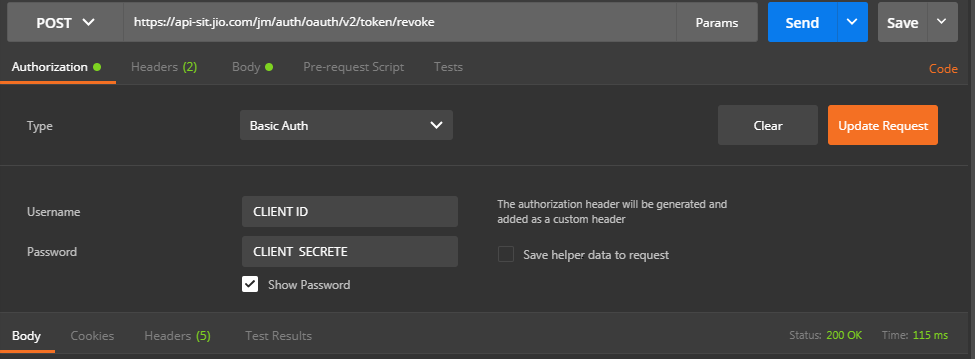
https://<**SECO API Domain** or **IP Address**>:<Port>/jm/auth/oauth/v2/token/revoke

**Header Parameters:**

Send below specified header parameters values only which are obtained from the **SECO API Portal** .PFA of screen shot.



Add Client\_Id in Username and Client\_Secret in password and click on Update Request to add Authorization header in request. Please follow below screen shot to add Authorization header.



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

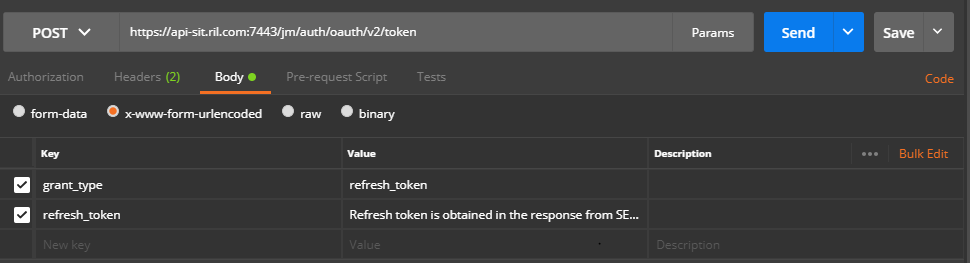
**client\_secret:** API Secret which is obtained from SECO after registering an Application/APP

**BODY(x-www-form-urlencoded) Parameters:**

Sending login/authentication credentials in the request body (x-www-form-urlencoded)

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

**Please refer screen shot for any confusion.**



**Http Method:**  POST

**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"**

**}**

**]**

**}**