



Secure Your APIs with OAuth 2.0 Using webMethods Integration Server



Andi Putra Ogie

Go To Security > OAuth > Client Registration

The screenshot displays the WebMethods Integration Server Administration console. The left sidebar shows the navigation menu with 'Security' expanded and 'OAuth' selected. The main content area shows the 'Administration > OAuth' path and a list of links. The 'Client Registration' link is highlighted with a red box. Below the links are two tables: 'Authorization Server Settings' and 'Resource Server Settings'.

WEBMETHODS
Integration Server

Administration Monitoring

Security ^

- ACLs
- Certificates
- CSRF guard
- Enterprise Gateway rules
- JWT
- Kerberos
- Keystore
- OAuth**
- OpenID
- Outbound passwords
- SAML

Administration > OAuth

OAuth

- [Client Registration](#)
- [Scope Management](#)
- [Tokens](#)
- [Edit OAuth Global Settings](#)
- [Add External Authorization Server](#)

Authorization Server Settings	
Require HTTPS	no
Require PKCE	no
Authorization code expiration interval	600 seconds
Access token expiration interval	3600 seconds
Token endpoint authentication	<input checked="" type="radio"/> Accept existing session <input type="radio"/> Require credentials

Resource Server Settings	
Authorization server	local

External Authorization Servers

Register Client for get Client ID & Client Secret

[Administration](#) > [OAuth](#) > [Client registration](#) > [Edit client registration](#)

Edit client registration

- [Return to Client Registration](#)

Client Configuration

Name	<input type="text"/>
Version	<input type="text"/>
Type	<input type="text" value="Confidential"/>
Description	<input type="text"/>
Redirect URIs	<div><input type="text"/></div> <div>Enter one URI per line</div>
Allowed Grants	<div><input checked="" type="checkbox"/> Authorization Code Grant</div> <div><input type="checkbox"/> Implicit Grant</div> <div><input type="checkbox"/> Client Credentials Grant</div> <div><input type="checkbox"/> Resource Owner Password Credentials Grant</div>
Require PKCE	<div><input checked="" type="radio"/> Use OAuth Global Setting < false ></div> <div><input type="radio"/> No</div> <div><input type="radio"/> Yes</div>

Token

Expiration Interval	<div><input checked="" type="radio"/> Use OAuth Global Setting < 3600 seconds ></div> <div><input type="radio"/> Never Expires</div> <div><input type="radio"/> Expires in <input type="text"/> seconds</div>
Refresh Count	<div><input type="radio"/> Unlimited</div> <div><input checked="" type="radio"/> Limit <input type="text" value="0"/></div>

Go To Security > OAuth > Scope Management

The screenshot displays the WebMethods Integration Server Administration console. The left sidebar shows the 'Security' menu expanded, with 'OAuth' selected. The main content area shows the 'Administration > OAuth' path and a list of links: 'Client Registration', 'Scope Management' (highlighted with a red box), 'Tokens', 'Edit OAuth Global Settings', and 'Add External Authorization Server'. Below the links are two tables: 'Authorization Server Settings' and 'Resource Server Settings'.

WEBMETHODS
Integration Server

Administration Monitoring

Security ^

ACLs

Certificates

CSRF guard

Enterprise Gateway rules

JWT

Kerberos

Keystore

OAuth

OpenID

Outbound passwords

SAML

User management

Administration > OAuth

OAuth

- [Client Registration](#)
- [Scope Management](#)
- [Tokens](#)
- [Edit OAuth Global Settings](#)
- [Add External Authorization Server](#)

Authorization Server Settings	
Require HTTPS	no
Require PKCE	no
Authorization code expiration interval	600 seconds
Access token expiration interval	3600 seconds
Token endpoint authentication	<input checked="" type="radio"/> Accept existing session <input type="radio"/> Require credentials

Resource Server Settings	
Authorization server	local

External Authorization Servers

Create Scope and Associate it

Edit IntScope

- [Return to Scope Management](#)

Scope Configuration

Name	<input type="text" value="IntScope"/>
Description	<input type="text" value="Integration Scope"/>
Folders and services	<input type="text" value="integration.oauth.services:getToken"/> <input type="text" value="integration.oauth.services:IntegrationOAuth"/>
URL templates	<input type="text"/>

Associate scopes to clients

- [Return to Scope Management](#)

Scopes

Select Scope:

Clients associated with Scope

IntegrationAuth (1)

Remaining Clients

----none----

->

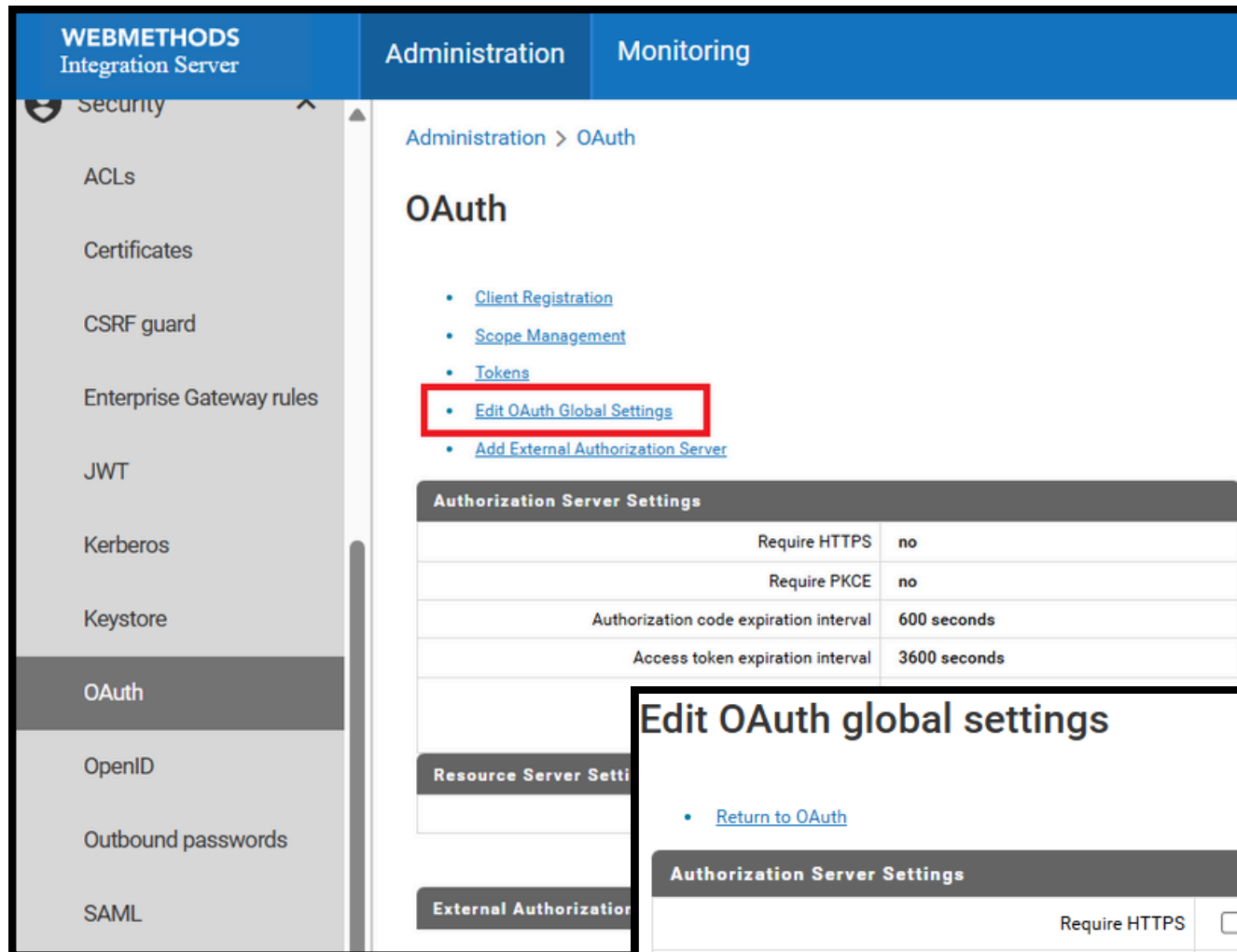
<-



Andi Putra Ogie

Edit Global Settings and Disable HTTPS

if you're running on your localhost



Edit OAuth global settings

[Return to OAuth](#)

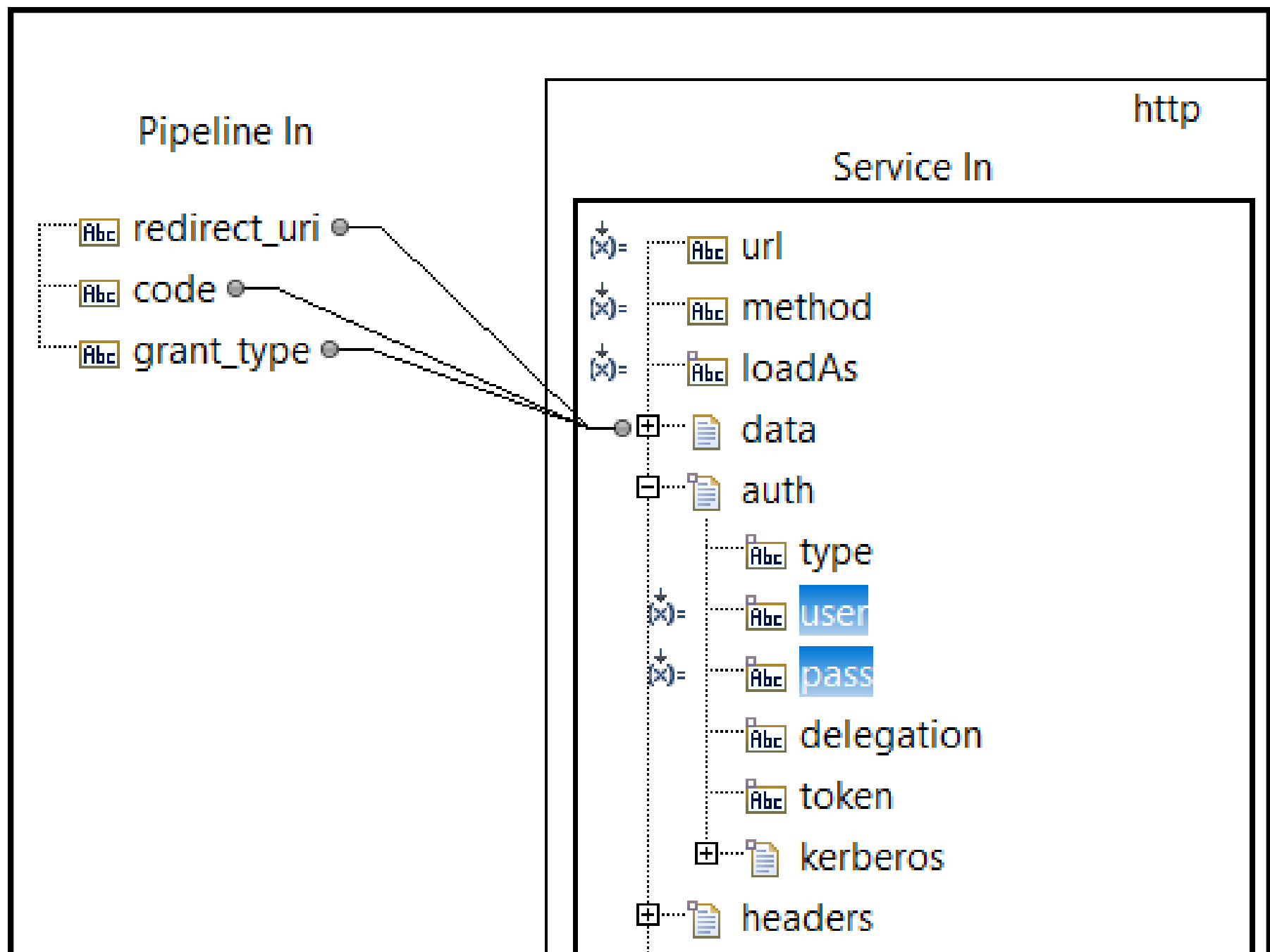
Authorization Server Settings	
Require HTTPS	<input type="checkbox"/>
Require PKCE	<input type="checkbox"/>
Authorization code expiration interval	<input type="text" value="600"/> seconds
Access token expiration interval	<input type="radio"/> Never Expires <input checked="" type="radio"/> Expires in <input type="text" value="3600"/> seconds
Token endpoint authentication	<input checked="" type="radio"/> Accept existing session <input type="radio"/> Require credentials

Resource Server Settings	
Authorization server	<input type="text" value="local"/>

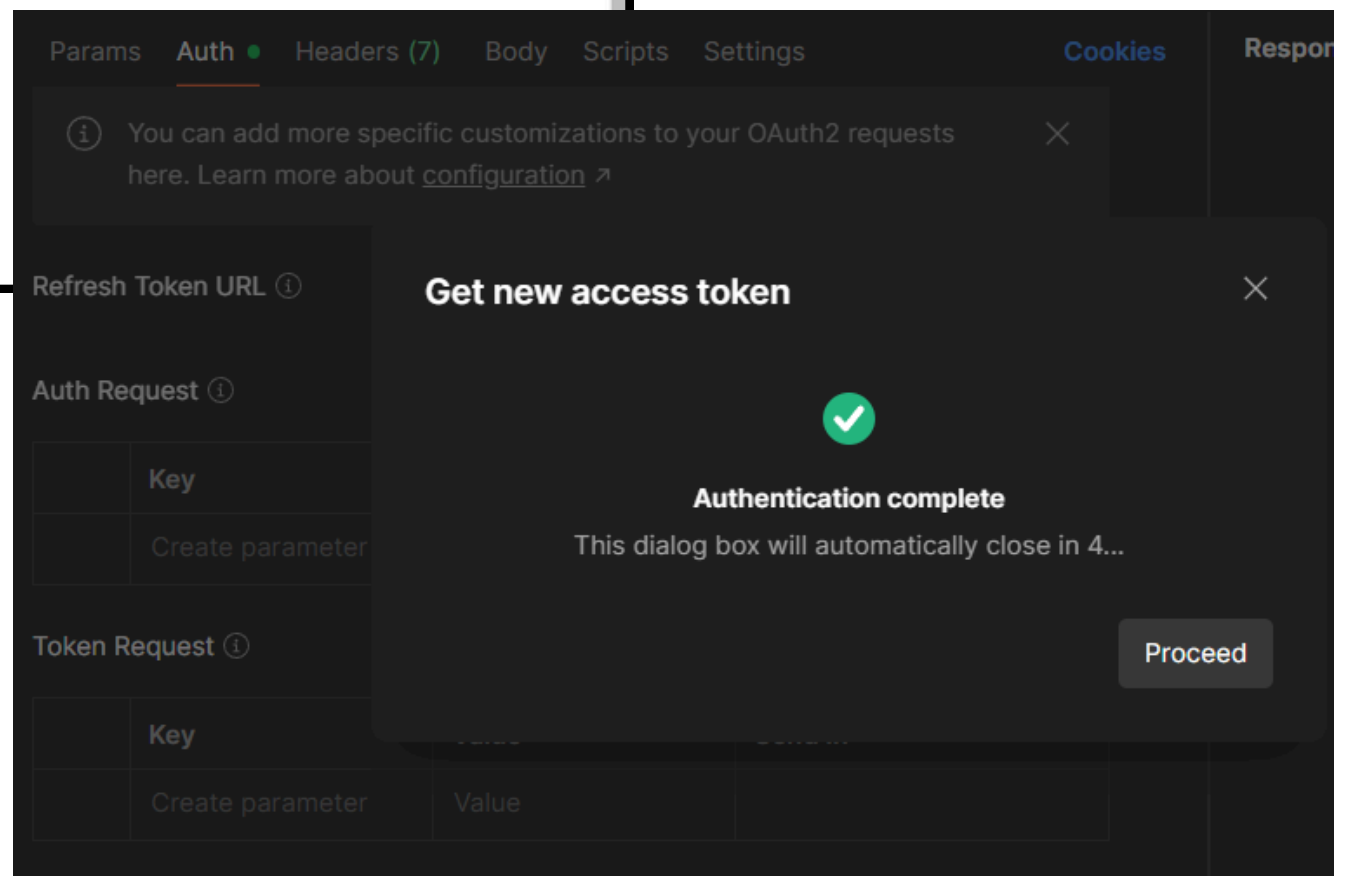
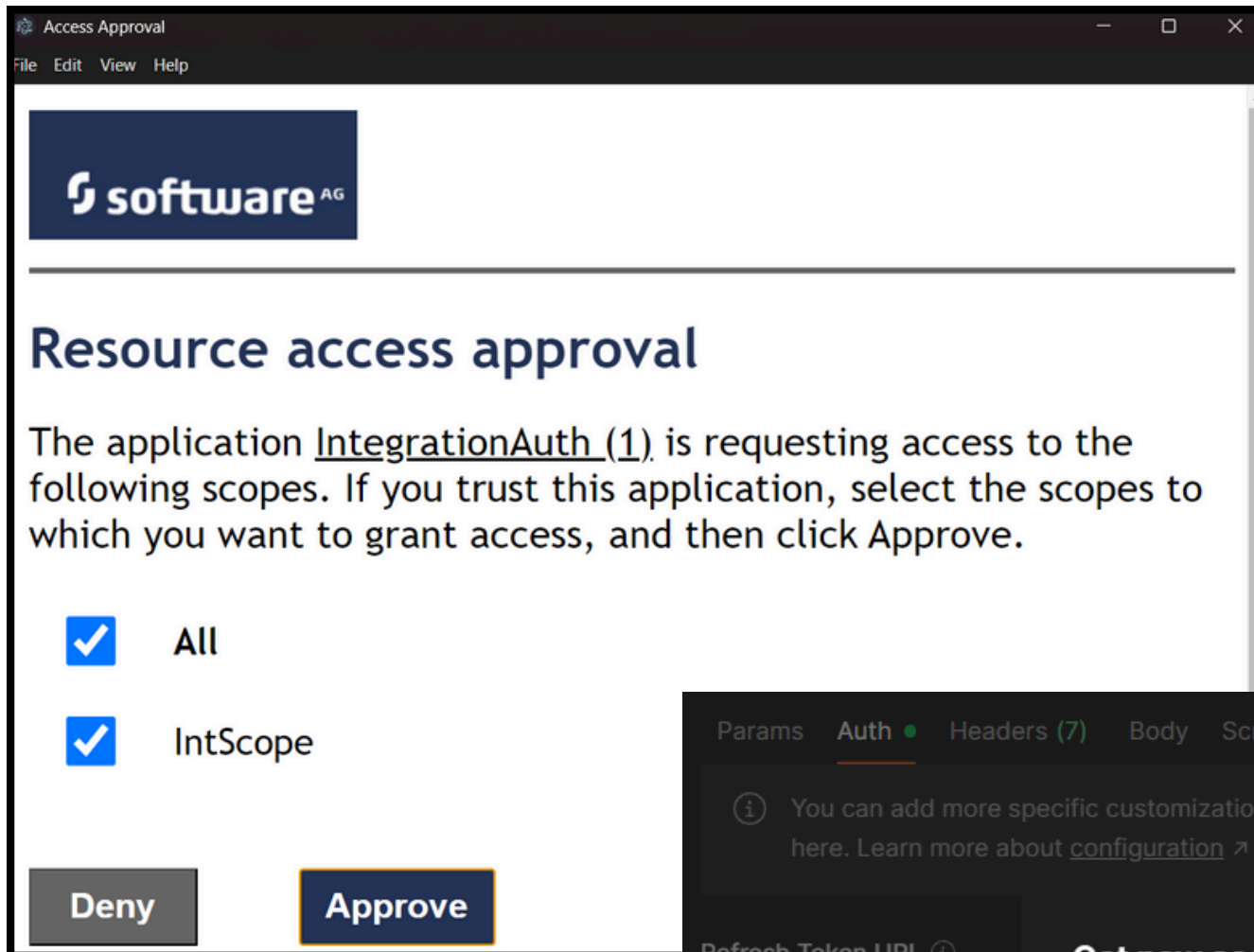
Edit some source from Flow Services

Implementation steps shown here are for reference only.

Full source not shared publicly.



Running on Postman




Access Token Ready to Published

Token Details

Use Token

Token Name

Integration Token 

Access Token

Token Type

Bearer

refresh_token

expires_in

3600

scope

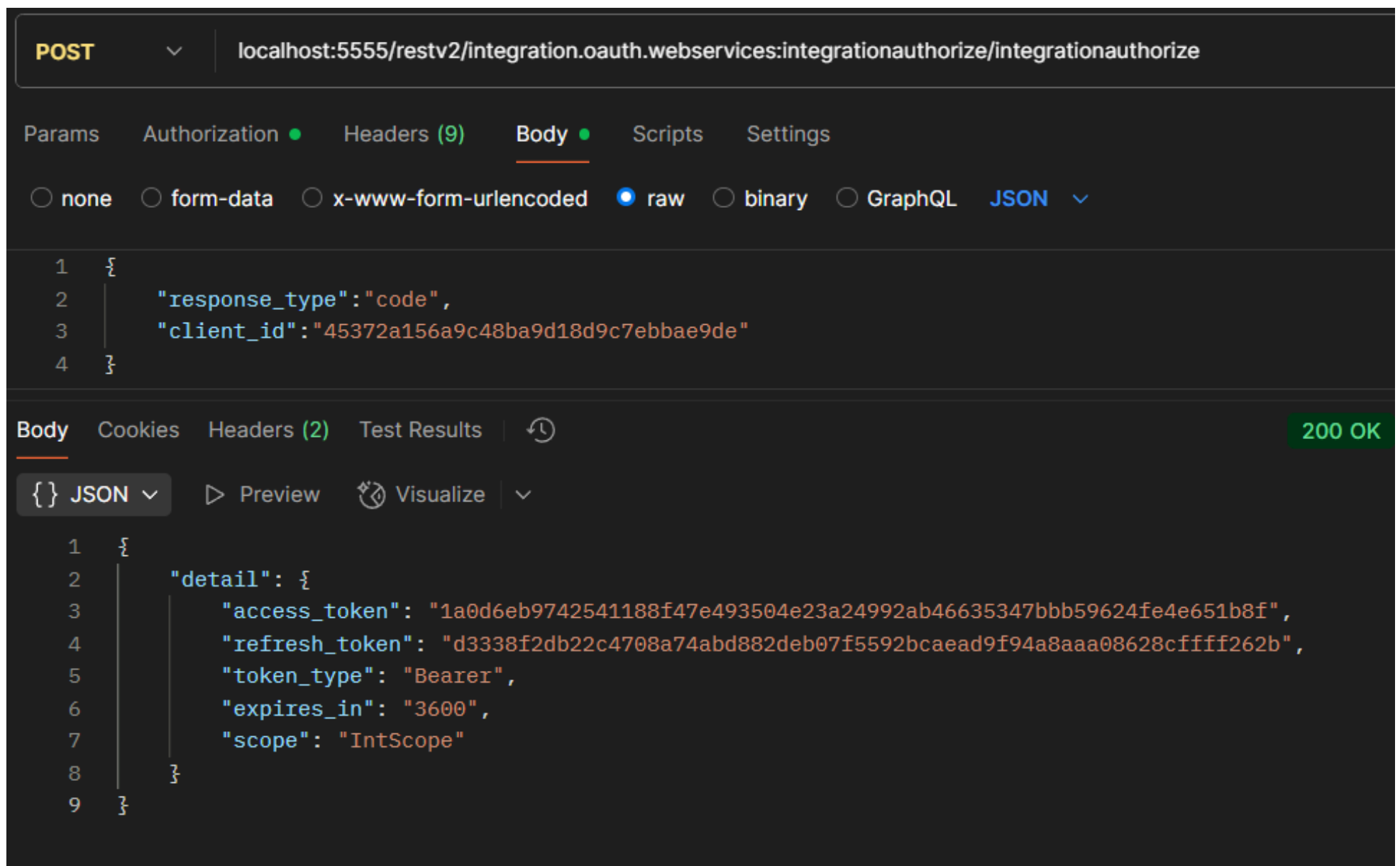
IntScope

access_token_url



Andi Putra Ogie

Also supports token request using body parameters, not just URL encoded params.



Let's connect and grow together
in the integration space.



 **Andi Putra Ogie**

webMethods Developer