RSA Via L&G Connector Datasheet
for
Google DoubleClick for Publishers (DFP)

Table of Contents

Purpose 3
Supported Software 3
Pre-requisites 4
Configuration 6
General 6
Settings 7
Capabilities 7
1. CreateAccount 8
2. EnableAccount 11
3. DisableAccount 11
4. UpdateAccount 12
5. ChangeRoleProfile(Change Approle Of Account) 14

Purpose

This data sheet provides the configuration information required to create a new Google DoubleClick for Publishers (DFP) connector.

Supported Software

RSA Via L&G Version: 6.9.1 and above

Application: Google DFP

Pre-requisites

Google DoubleClick for Publisher (DFP) Connector uses DFP-API. We use Oauth 2.0 for authorization, Hence we require to create Project with New Client ID and a Client Secret with DFP. More Information about Authentication can be found at Google DFP link: https://developers.google.com/doubleclick-publishers/docs/authentication

Create a Client ID and client secret

To use OAuth 2.0 to authorize the DFP API, you must first create a Client ID and a client secret:

1. Go to Google Developers Console: https://console.developers.google.com/

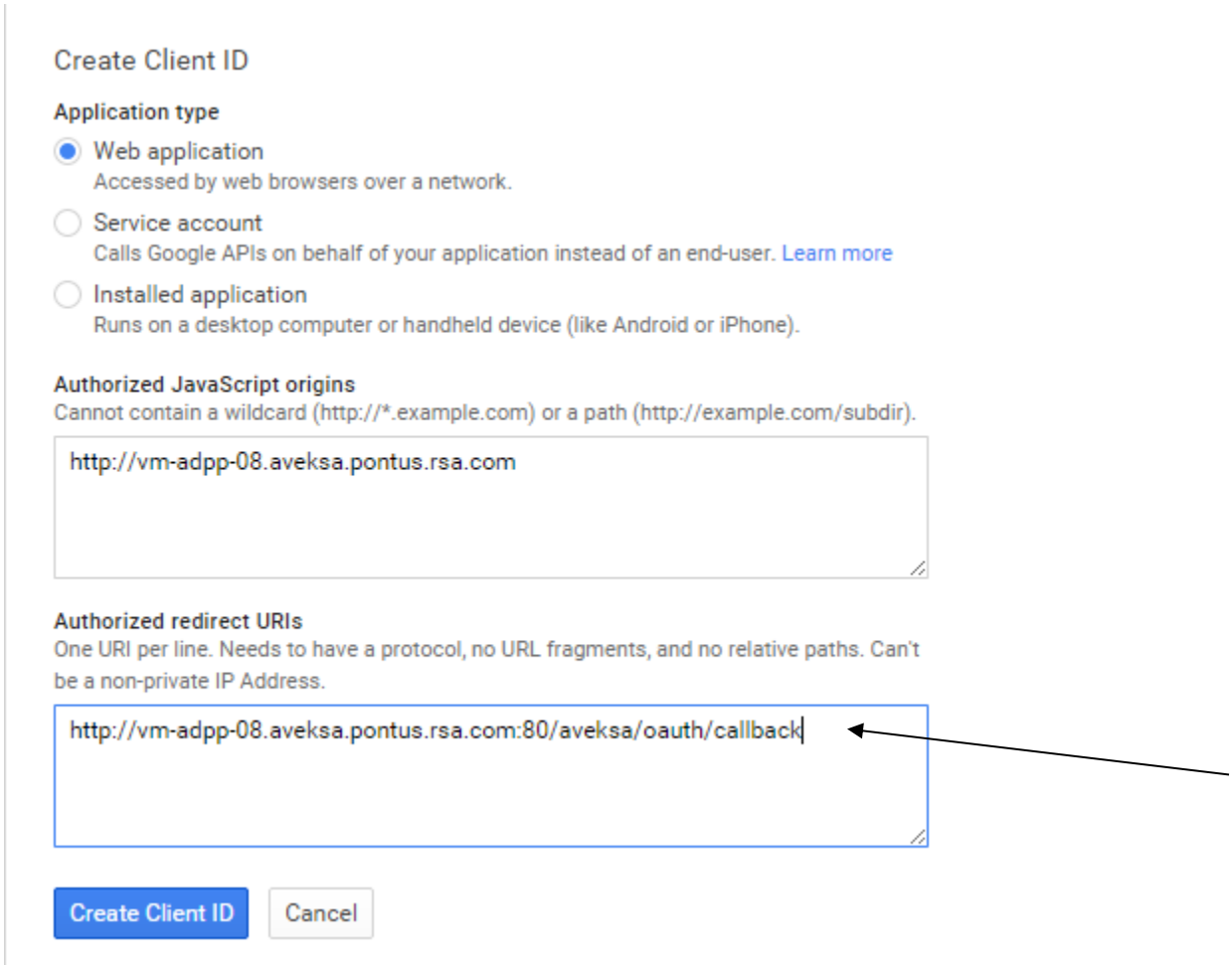
2. Click “CREATE PROJECT” to create a new project.

3. Enter the Project Name (and optionally, choose your own Project ID), and click Create.

4. The newly created project should automatically open. Click APIs & auth to expand the menu, and then click Credentials.

5. Choose Web Application. Provide RSA IMG server URL in JavaScript Origin and Authorized redirect URIs.

6. Click “Create Client ID” to complete the registration.



Note: Make sure the values for Redirect URI and Authorized JavaScript Origins fields are correct.

The **Redirect URIs** registered at GoogleDFP must be the same and must match the application URIs. (http://hostname:port/...)

We should appropriate port Number in AUTHORIZED REDIRECT URI field.

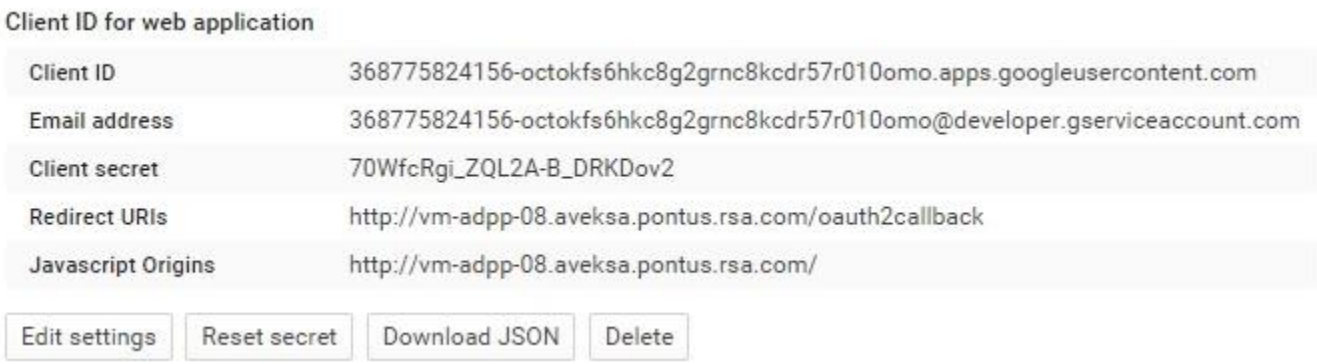
e.g. : if you have deployed RSA IMG server on Linux using JBoss Webserver then default Port would be 80..

Redirect URI: https://<Host>:80/aveksa/oath/callback

Similar way, we should use Port 9080 for WebSphere Application Server in Redirect URI filed.

Redirect URI for WebSphere: https://<Host>:9080/aveksa/oath/callback

7. Client ID and Client Secret will be created and displayed.



Configuration

The Connector creation is made up of three sections:

General – General details about the Connector; viz. the name, type etc.

Settings – The connection settings required to connect the RSA-IMG and the End-point Application in consideration.

Capabilities – These are the list of “verbs” or capabilities that the RSA-IMG Connector supports; for e.g. “Create, Update, Delete, etc.”

General

The following table lists the parameters on the “General” screen, while creating the Connector.

Field Name	**Value**
Name	GoogleDFP Connector
Description	GoogleDFP Connector
Server	AFX Server
Connector Template	GoogleDFP
State	Test
Export As Template	N/A

Note: When you are satisfied your Connector is configured properly change the state to Active. No automated provisioning will occur while in the Test state. It is recommended that you test all enabled commands using the Test Connector Settings and Test Connector Capabilities prior to changing to the Active state.

Settings

The following table lists the parameters on the “Settings” screen, while creating the Connector.

Field Name	**Value**
Client ID	*Created Client ID for the application*
Client Secret	*Client Secret for the application*
Network Code	*Code of your logged on network*
Scope	*Default value of Scope for Google DFP APIs :* *https://www.google.com/apis/ads/publisher*
Authorization URL	*Authorization URL. Default value: https://accounts.google.com/o/oauth2/auth*
Access Token URL	*Access Token URL. Default value:* *https://accounts.google.com/o/oauth2/token*
Proxy Host	*<Enter the proxy host or IP if you are using proxy server to access internet.>*
Proxy Port	*<Enter the proxy port if you are using proxy server to access internet.>*
Proxy Username	*<Enter the proxy username if you are using proxy server to access internet.>*
Proxy Password	*<Enter the proxy password if you are using proxy server to access internet.>*

Capabilities

Following commands are supported by RSA Via L&G Google DFP Connector:

- CreateAccount

- EnableAccount
- DisableAccount
- UpdateAccount
- ChangeRoleProfile

Command Input Parameters

1. *CreateAccount*

The following table lists the parameters on the “Create Account” screen.

Field Name	**Value**
Parameter Name	EmailId
Type	*STRING*
Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	EmailId
Mapping	${User.Email_Address}
Description	EmailId

Field Name	**Value**
Parameter Name	AccountName
Type	*STRING*
Default Value	*None*

Is the parameter required?	**Yes**
Is the parameter encrypted?	**NO**
Display Name	AccountName
Mapping	${AccountTemplate.AccountName}
Description	AccountName

Field Name	**Value**
Parameter Name	RoleName
Type	*STRING*
Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	*RoleName*
Mapping	${AccountTemplate.RoleName}
Description	RoleName

Field Name	**Value**
Parameter Name	Language
Type	*STRING*
Default Value	*None*
Is the parameter required?	**NO**
Is the parameter encrypted?	**No**
Display Name	Language
Mapping	${AccountTemplate.Language}
Description	PreferredLocale

Field Name	**Value**
Parameter Name	ExternalId
Type	*STRING*
Default Value	*None*
Is the parameter required?	**No**
Is the parameter encrypted?	**No**
Display Name	ExternalId
Mapping	${AccountTemplate. ExternalId}

Description	ExternalId

2. EnableAccount

The following table lists the parameters on the “Enable Account” screen.

Field Name	**Value**
Parameter Name	EmailId
Type	*STRING*
Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	*EmailId*
Mapping	*${ User.Email_Address }*
Description	*EmailId*

3. DisableAccount

The following table lists the parameters on the “Disable Account” screen.

Field Name	**Value**
Parameter Name	EmailId
Type	*STRING*

Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	*EmailId*
Mapping	*${ User.Email_Address }*
Description	*EmailId*

4. UpdateAccount

The following table lists the parameters on the “Update Account” screen.

Field Name	**Value**
Parameter Name	AccountName
Type	*STRING*
Default Value	*None*
Is the parameter required?	**No**
Is the parameter encrypted?	**No**
Display Name	*AccountName*
Mapping	*${Account.Name}*

Description	*Updated name of the account*

Field Name	**Value**
Parameter Name	Language
Type	*STRING*
Default Value	*None*
Is the parameter required?	**NO**
Is the parameter encrypted?	**No**
Display Name	Language
Mapping	${AccountTemplate.Language}
Description	PreferredLocale

Field Name	**Value**
Parameter Name	ExternalId
Type	*STRING*
Default Value	*None*
Is the parameter required?	**No**
Is the parameter encrypted?	**No**

Display Name	ExternalId
Mapping	${AccountTemplate. ExternalId}
Description	ExternalId

5. ChangeRoleProfile(Change Approle Of Account)

The following table lists the parameters on the “Change Role Profile” screen.

Field Name	**Value**
Parameter Name	EmailId
Type	*STRING*
Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	*EmailId*
Mapping	*${ User.Email_Address }*
Description	*EmailId*

Field Name	**Value**
Parameter Name	RoleName
Type	*STRING*

Default Value	*None*
Is the parameter required?	**Yes**
Is the parameter encrypted?	**No**
Display Name	*RoleName*
Mapping	${AccountTemplate.RoleName}
Description	RoleName

COPYRIGHTS

TRADEMARKS