

**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.

**Create Client ID**

**Application type**

**Web application**  
 Accessed by web browsers over a network.

**Service account**  
 Calls Google APIs on behalf of your application instead of an end-user. [Learn more](#)

**Installed application**  
 Runs on a desktop computer or handheld device (like Android or iPhone).

**Authorized JavaScript origins**  
 Cannot contain a wildcard (http://\*.example.com) or a path (http://example.com/subdir).

http://vm-adpp-08.aveksa.pontus.rsa.com

**Authorized redirect URIs**  
 One URI per line. Needs to have a protocol, no URL fragments, and no relative paths. Can't be a non-private IP Address.

http://vm-adpp-08.aveksa.pontus.rsa.com:80/aveksa/oauth/callback

[Create Client ID](#) [Cancel](#)

**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.

Client ID for web application

Client ID	368775824156-octokfs6hkc8g2grnc8kcdr57r010omo.apps.googleusercontent.com
Email address	368775824156-octokfs6hkc8g2grnc8kcdr57r010omo@developer.gserviceaccount.com
Client secret	70WfcRgi_ZQL2A-B_DRKDov2
Redirect URIs	http://vm-adpp-08.aveksa.pontus.rsa.com/oauth2callback
Javascript Origins	http://vm-adpp-08.aveksa.pontus.rsa.com/

- 

## 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 : <a href="https://www.google.com/apis/ads/publisher">https://www.google.com/apis/ads/publisher</a>
Authorization URL	Authorization URL. Default value: <a href="https://accounts.google.com/o/oauth2/auth">https://accounts.google.com/o/oauth2/auth</a>
Access Token URL	Access Token URL. Default value: <a href="https://accounts.google.com/o/oauth2/token">https://accounts.google.com/o/oauth2/token</a>
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	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	EmailId
Mapping	#{User.Email_Address}
Description	EmailId

Field Name	Value
Parameter Name	AccountName
Type	<i>STRING</i>
Default Value	<i>None</i>



Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>NO</b>
Display Name	AccountName
Mapping	\${AccountTemplate.AccountName}
Description	AccountName

<b>Field Name</b>	<b>Value</b>
Parameter Name	RoleName
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>RoleName</i>
Mapping	\${AccountTemplate.RoleName}
Description	RoleName

Field Name	Value
Parameter Name	Language
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>NO</b>
Is the parameter encrypted?	<b>No</b>
Display Name	Language
Mapping	\${AccountTemplate.Language}
Description	PreferredLocale

Field Name	Value
Parameter Name	ExternalId
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>No</b>
Is the parameter encrypted?	<b>No</b>
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	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>EmailId</i>
Mapping	<i>\${ User.Email_Address }</i>
Description	<i>EmailId</i>

## 3. DisableAccount

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

Field Name	Value
Parameter Name	EmailId
Type	<i>STRING</i>

Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>EmailId</i>
Mapping	<i>\${ User.Email_Address }</i>
Description	<i>EmailId</i>

#### 4. UpdateAccount

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

Field Name	Value
Parameter Name	AccountName
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>No</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>AccountName</i>
Mapping	<i>\${Account.Name}</i>

Description	<i>Updated name of the account</i>
-------------	------------------------------------

Field Name	Value
Parameter Name	Language
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>NO</b>
Is the parameter encrypted?	<b>No</b>
Display Name	Language
Mapping	<code>\${AccountTemplate.Language}</code>
Description	PreferredLocale

Field Name	Value
Parameter Name	ExternalId
Type	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>No</b>
Is the parameter encrypted?	<b>No</b>

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	<i>STRING</i>
Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>EmailId</i>
Mapping	<i>\${ User.Email_Address }</i>
Description	<i>EmailId</i>

Field Name	Value
Parameter Name	RoleName
Type	<i>STRING</i>

Default Value	<i>None</i>
Is the parameter required?	<b>Yes</b>
Is the parameter encrypted?	<b>No</b>
Display Name	<i>RoleName</i>
Mapping	<code>\${AccountTemplate.RoleName}</code>
Description	RoleName

## COPYRIGHTS

Copyright © 2015 EMC Corporation. All Rights Reserved. Published in the USA.

## TRADEMARKS

RSA, the RSA Logo, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to [www.rsa.com/legal/trademarks\\_list.pdf](http://www.rsa.com/legal/trademarks_list.pdf).