

Cloudpath

Enrollment System

Setting Up Third-Party Authentication Within Cloudpath Using Google™

Software Release 5.1

May 2017

Summary: This document describes how to create a Google application for use with Cloudpath, and how to configure Cloudpath to use the Google application for authentication.

Document Type: Configuration

Audience: Network Administrator



Setting Up Third-Party Authentication Within Cloudpath Using Google

Software Release 5.1

December 2017

Copyright © 2017 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2017 Ruckus Wireless, Inc. All rights reserved.

Setting Up Third-Party Authentication Within Cloudpath Using Google™

Setting Up the Google Application

Before configuring Cloudpath for third-party authentication, you must set up the Google application.

What You Need

- Google login credentials
- Branding information for your application
- Redirect URL for your application

Google App Configuration

This section describes how to create the Google application to use with Cloudpath.

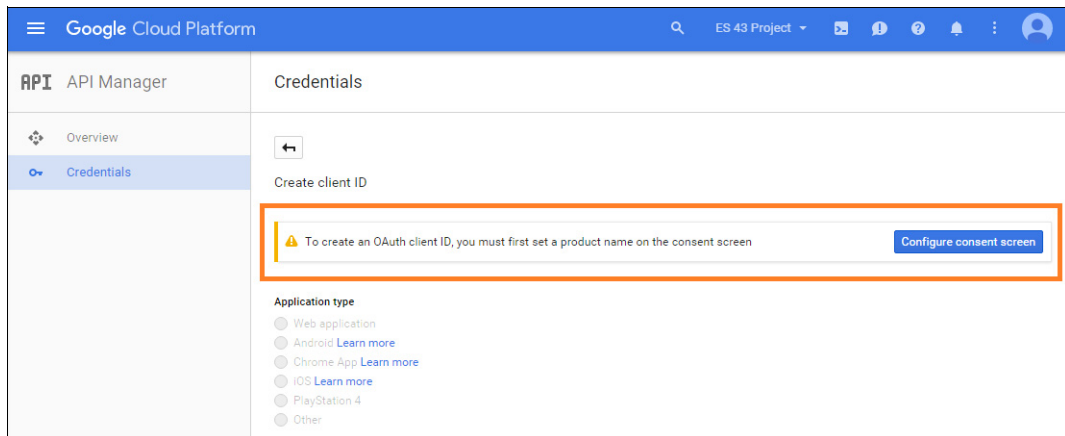
Create Web Application Project

1. Go to <https://console.developers.google.com>.
2. Sign in to your Google account.
3. On the *Google API manager*, create and name an API Project.
4. Select the *Credentials* tab on the left-menu.
5. On the left-menu *Credentials*, tab, there are 3 tabs across the top, *Credentials*, *OAuth consent screen*, and *Domain verification*.

Note >>

Be sure to create the OAuth consent screen first. If you create the Client ID first, a warning displays.

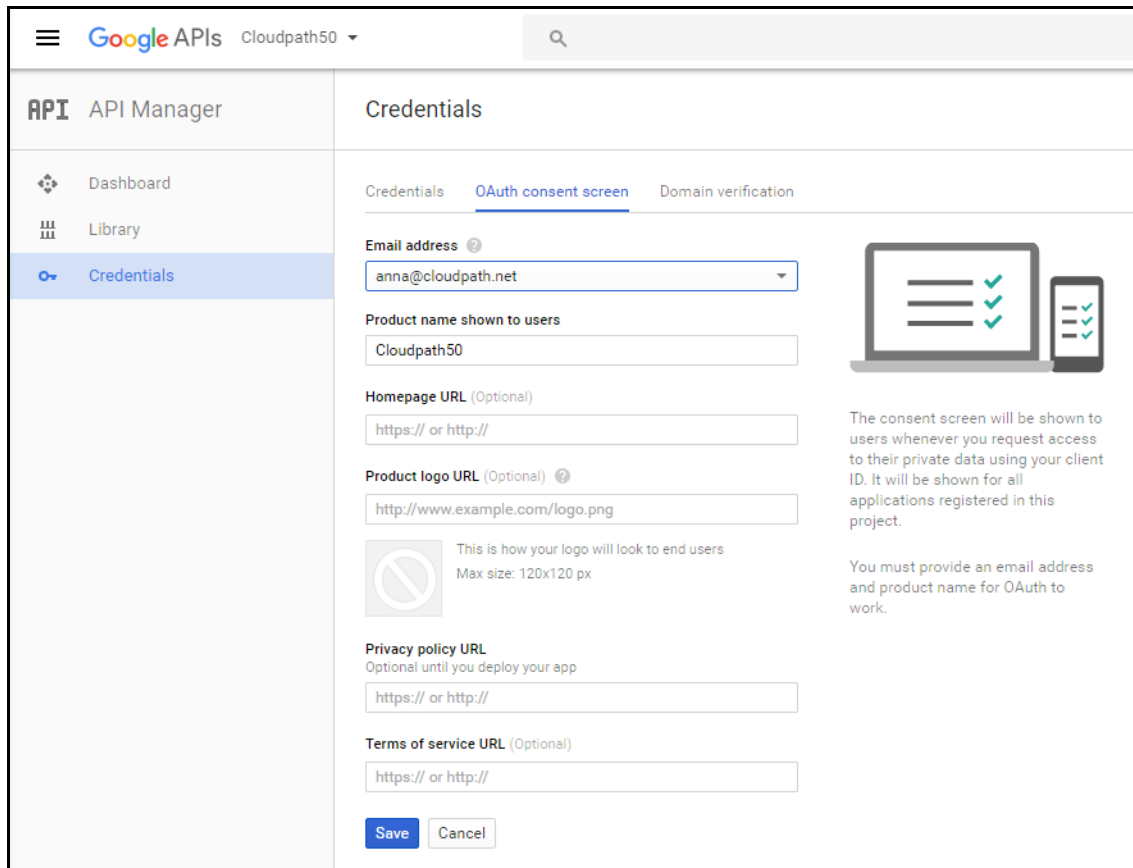
FIGURE 1. Warning Message



Configure OAuth Consent Screen

1. In the API Manager, from the left menu Credentials tab, Select the top-tab *OAuth consent screen*.
The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project
2. Enter the *OAuth Consent Screen* credentials. *Email address* and *Product name* are required. Optionally, you can enter URL and a product logo.

FIGURE 2. OAuth Consent Screen



The screenshot shows the Google APIs console interface for configuring an OAuth consent screen. The left sidebar is titled "API Manager" and has "Credentials" selected. The main content area is titled "Credentials" and has three tabs: "Credentials", "OAuth consent screen" (which is active), and "Domain verification".

The "OAuth consent screen" configuration form includes the following fields:

- Email address**: A dropdown menu with "anna@cloudpath.net" selected.
- Product name shown to users**: A text input field containing "Cloudpath50".
- Homepage URL (Optional)**: A text input field containing "https:// or http://".
- Product logo URL (Optional)**: A text input field containing "http://www.example.com/logo.png".
- Product logo**: A placeholder image with a "no" symbol and the text "This is how your logo will look to end users. Max size: 120x120 px".
- Privacy policy URL**: A text input field containing "https:// or http://".
- Terms of service URL (Optional)**: A text input field containing "https:// or http://".

At the bottom of the form are "Save" and "Cancel" buttons. To the right of the form, there is an illustration of a laptop and a smartphone, both displaying a consent screen with three green checkmarks. Below the illustration, there is explanatory text: "The consent screen will be shown to users whenever you request access to their private data using your client ID. It will be shown for all applications registered in this project." and "You must provide an email address and product name for OAuth to work."

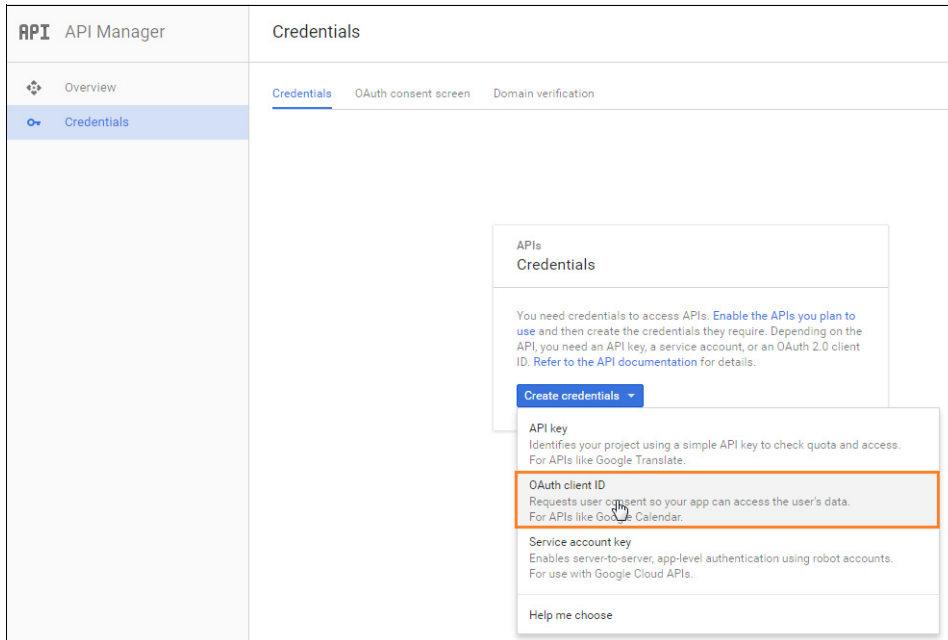
3. Save the OAuth consent screen page.

Create Client ID

1. In the API Manager, from the left-menu *Credentials* tab, select the *Credentials* top-tab.

2. From the *Create Credentials* drop-down menu, select *OAuth Client ID*.

FIGURE 3. Create OAuth Client ID



3. Select *Application Type - Web application*.

FIGURE 4. Create Client ID

The screenshot shows the 'Create client ID' page in the Google API Manager. The left sidebar has 'API Manager' at the top and 'Credentials' selected. The main content area is titled 'Credentials' and has a 'Create client ID' button. Below this, there are several sections:

- Application type:** A list of radio buttons with 'Web application' selected. Other options include 'Android Learn more', 'Chrome App Learn more', 'iOS Learn more', 'PlayStation 4', and 'Other'.
- Name:** A text input field containing 'Cloudpath ES web client'.
- Restrictions:** A section with a heading 'Enter JavaScript origins, redirect URIs, or both'.
 - Authorized JavaScript origins:** A text input field containing 'http://www.example.com'. Below it is a note: 'For use with requests from a browser. This is the origin URI of the client application. Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).'.
 - Authorized redirect URIs:** A text input field containing 'https://testURL.cloudpath.net/enroll/Test/Production/google/'. Below it is a note: 'For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.'

At the bottom of the form are 'Create' and 'Cancel' buttons.

4. Enter the Name for your web application client.
5. On the *Create Client ID* page, leave the *Authorized Javascript origins* field blank.
6. In the *Authorized redirect URIs* field, the entry must be in this format $\${ENROLLER_URL}/enroll/google/$, where $\${ENROLLER_URL}$ is the external URL to which the user is redirected. For multiple redirect URLs, enter one path on each line.

Note >>

Refer to the Google Configuration Redirect URI on the Third-Party Authentication Setup page in the Cloudpath Admin UI.


7. Click *Create*.

The OAuth client ID and client secret for your web application are displayed.


FIGURE 5. OAuth Client Information

OAuth client

Here is your client ID

37123249493-0s284eobl0e8s6bovdp1thabi3e756b.apps.googleusercontent.com 

Here is your client secret

Yd7uMyj7oBMBIXaUk5yuuA6Y 

[OK](#)




Click OK to continue.

View Client ID Details

View your OAuth Client ID list with the left-menu *Credentials*, and top-tab *Credentials*, selected.

FIGURE 6. OAuth Client IDs

API API Manager

-  Dashboard
-  Library
-  Credentials



Credentials

[Credentials](#) [OAuth consent screen](#) [Domain verification](#)

[Create credentials](#) [Delete](#)

Create credentials to access your enabled APIs. [Refer to the API documentation](#) for details.

OAuth 2.0 client IDs

<input type="checkbox"/>	Name	Creation date	Type	Client ID	
<input type="checkbox"/>	Cloudpath50	Oct 28, 2016	Web application	37123249493-0s284eobl0e8s6bovdp1thabi3e756b.apps.googleusercontent.com	 

Click the link in the *Client ID Name* to view the Client ID details, including the *Client ID* and *Client Secret*.

FIGURE 7. Client ID for Web Application

API Manager

Dashboard
Library
Credentials

Credentials

← Download JSON Reset secret Delete

Client ID for Web application

Client ID	37123249493-0s284eobld0e8s6bovpd1thabi3e756b.apps.googleusercontent.com
Client secret	Yd7uMyj7oBMBIxaUk5yuuA6Y
Creation date	Oct 28, 2016, 4:45:05 PM

Name
Cloudpath50

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://anna40.cloudpath.net/enroll/Anna40TestBVT/Production/google ×
http://www.example.com/oauth2callback

Save Cancel

Tip >>

Make note of your *Client ID* and *Client Secret*. You need this information to set up Google authentication within Cloudpath.

Setting Up Cloudpath

After the Google application is set up, configure an authentication step in Cloudpath to prompt the user for the Google credentials.

What You Need

- Google application Client ID
- Google application Client Secret

Cloudpath Configuration

This section describes how to add a step to the enrollment workflow to authenticate a user using the Google application.

How to Add Third-Party Authentication to the Workflow

1. Create an enrollment workflow for third-party authentication.
2. Add an enrollment step, that prompts the user to authenticate through a third-party source.
3. Select *Create a new configuration*.

The *Third-Party Authentication Setup* page allows you to specify which third-party sources are allowed as well as API information related to those sources.

4. Enter the *Name* and *Description* of this configuration.

FIGURE 8. Google Third-Party Authentication Setup

Third-Party Authentication Setup

1 Display Name:

1 Description:

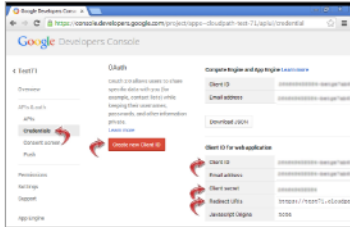
Facebook Configuration

1 Facebook Supported?

Google Configuration

1 Google Supported?

Instructions: The Google Developer's Console is available at <https://console.developers.google.com>. Within the desired project, locate API & Auth->Credentials and create a client ID for a web application.



1 Client ID:

1 Client Secret:

Redirect URIs: Google will need a list of acceptable Redirect URIs. These must be the full enrollment URL + "/google", such as <https://test71.cloudpath.net/enroll/Regression/Test/google>. Multiple URIs may be specified, with one per line.

Based on the current deployment locations, the Redirect URIs should be:
<https://anna43.cloudpath.net/enroll/Anna43TestBVT/Production/google>

LinkedIn Configuration

1 LinkedIn Supported?

Custom OAuth 2.0

1 Custom OAuth 2.0 Configuration

5. In the Google Configuration section, check the *Google Supported?* box.

6. Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.
7. Enter the *Client ID* and *Client Secret* from the Google application.

Note >>

These entries must match what is specified in the Google application.

8. Click **Save**. The Google authentication step is added to your enrollment workflow.

FIGURE 9. Cloudpath Workflow

Configuration > Workflows Add Workflow ▶

Workflows	Status	Enrollment Portal URL	Last Publish Time
Production	● Published	/enroll/Anna43TestBVT/Production/	20170427 1538 MDT

Properties **Enrollment Process** Look & Feel Snapshot(s) Advanced

Step 1: Require the user to accept the AUP **Welcome Message and AUP**

Step 2: All matches in: Visitors Employees +

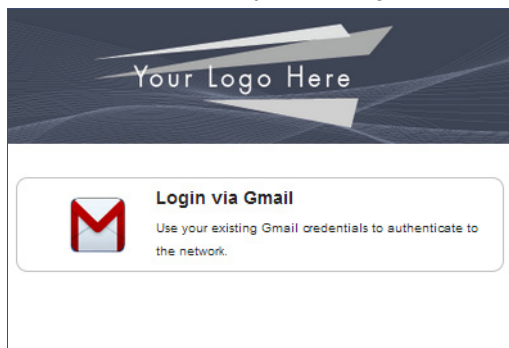
Step 3: Authenticate the user via **Google Authentication**

Result: Move user to **eng-Anna43** and assign certificate using **Guest Policy Templat...**

User Experience

When a user attempts to gain access to your network, they receive the Google authentication prompt during the enrollment process.

FIGURE 10. User Prompt for Google Authentication



After authenticating the user with their Gmail credentials, Cloudpath continues with the enrollment process and moves the user to the secure network.