

Cloudpath

Enrollment System

Setting Up Third-Party Authentication Within the Cloudpath ES Using Google™

Software Release 4.3

April 2016

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

Document Type: Configuration

Audience: Network Administrator



Setting Up Third-Party Authentication Within Cloudpath ES Using Google

Software Release 4.3

April 2016

Copyright © 2016 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 © 2016 Ruckus Wireless, Inc. All rights reserved.

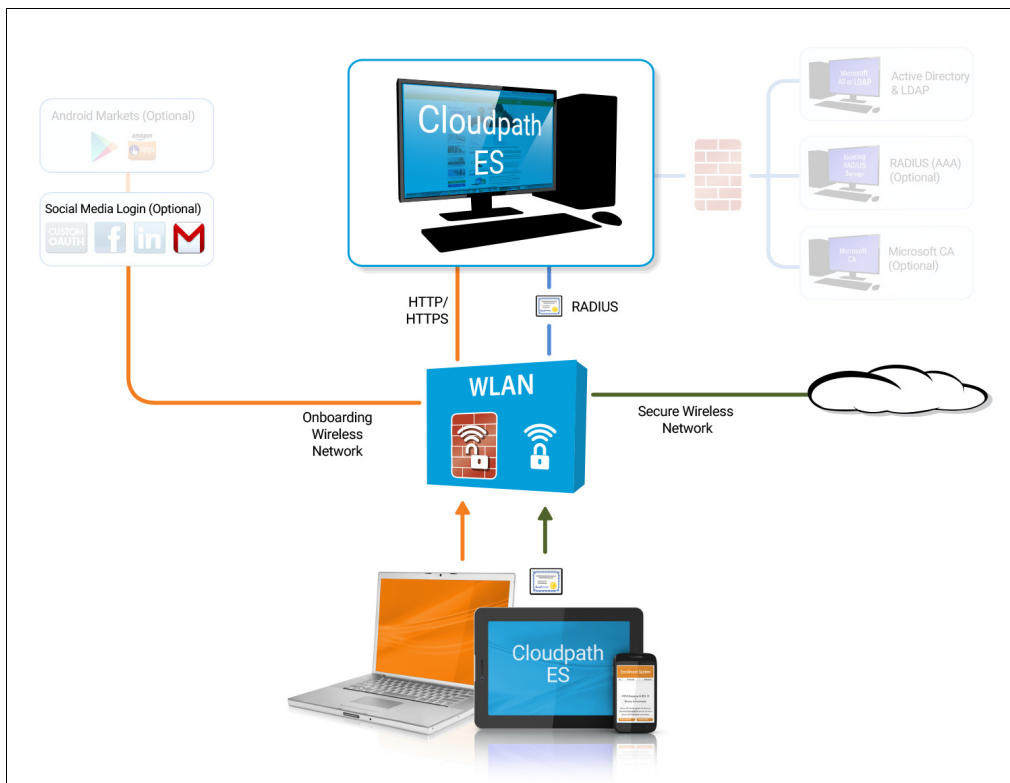
Setting Up Third-Party Authentication Within the CloudpathES Using Google™

Overview

The Cloudpath Enrollment System (ES) automates WPA2-Enterprise configuration on any device that connects to the network and automatically connects the device to a secure SSID. This *Automated Device Enablement* means authorized devices onboard simply and securely, with the appropriate level of access. By using the ES with Automated Device Enablement, the user gets configured and connected, regardless of device type, ownership, or level of access.

The flexible workflow engine gives network administrators further control by blending traditional policies (Active Directory, RADIUS, and integration with Microsoft CA) with additional policy capabilities (LinkedIn, Facebook, and Google Gmail). When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self-service access for all devices.

FIGURE 1. Cloudpath ES Onboarding System



Setting Up the Google Application

Before configuring the Cloudpath ES 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 the Cloudpath ES.

Create Web Application Project

1. Go to <https://console.developers.google.com>.
2. Sign in to your Google account.
3. On the *Developers Console*, create and name an API Project. A *Project ID* is automatically assigned.

FIGURE 2. Create API Project

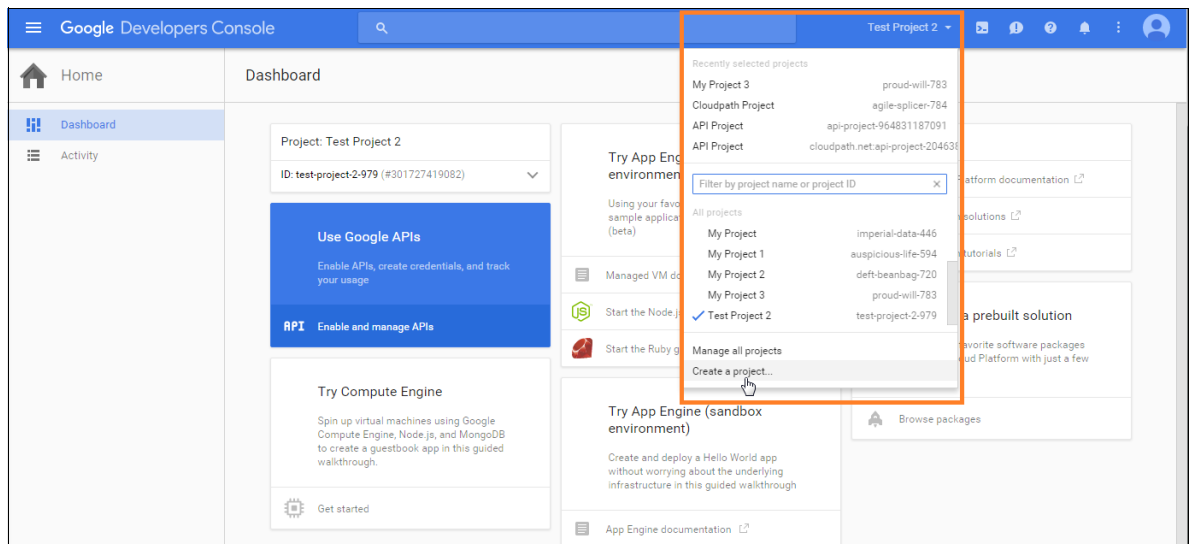
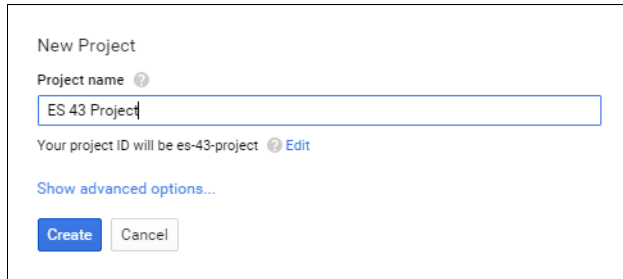
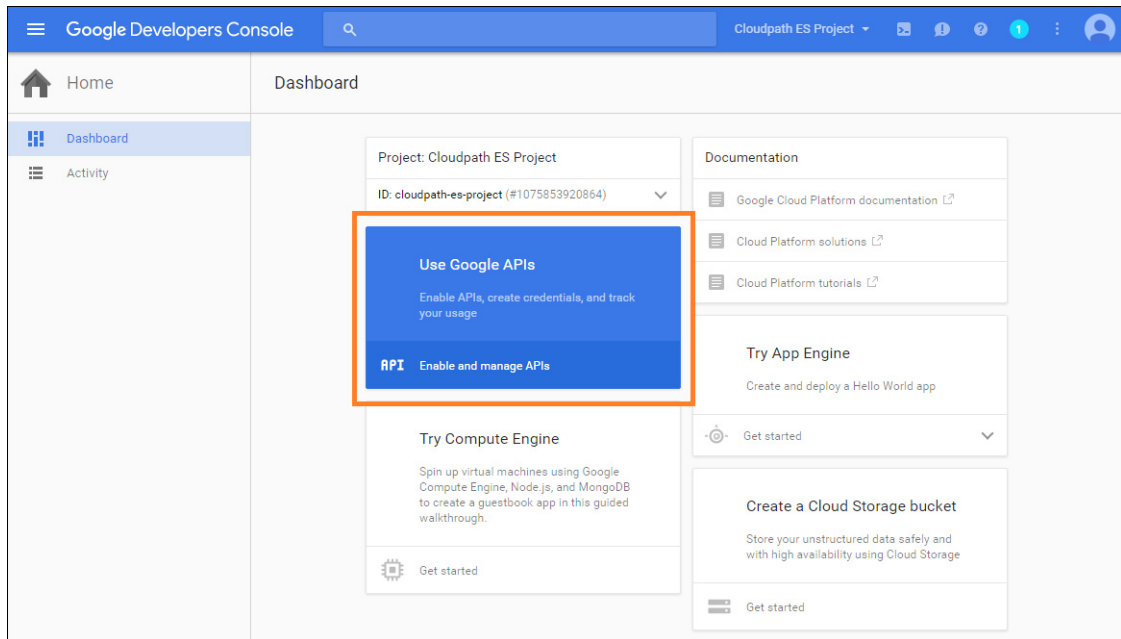


FIGURE 3. Name API Project



4. Click *Create*. The Project page displays.

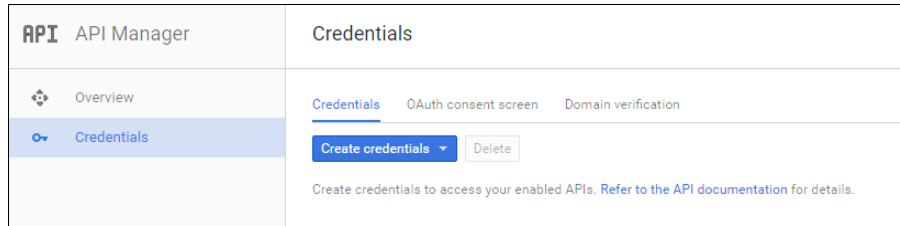
FIGURE 4. Project Page



Access API Manager

1. From your Project page, select *Use Google APIs*. The Google API Manager page displays.

FIGURE 5. API Manager Page

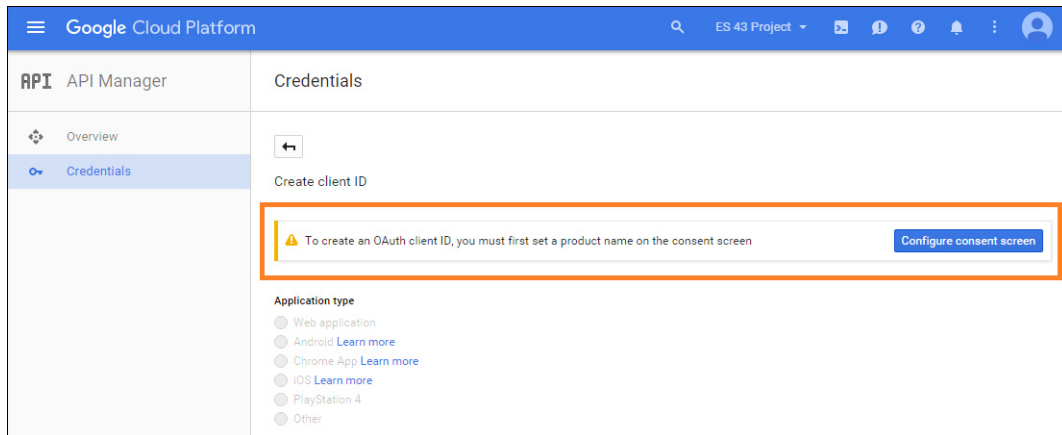


2. On the API Manager page, select the *Credentials* tab on the left-menu.
3. On the left-menu *Credentials*, tab, there are 3 tabs across the top, *Credentials*, *OAuth consent screen*, and *Domain verification*.

Note >>

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

FIGURE 6. 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.

FIGURE 7. OAuth Consent Screen

The screenshot shows the Google Cloud Platform API Manager interface. The left sidebar is titled "API Manager" and has a "Credentials" tab selected. The main content area is titled "Credentials" and has a sub-tab "OAuth consent screen" selected. The form contains the following fields:

- Email address**: A dropdown menu with "anna@cloudpath.net" selected. This field is highlighted with an orange border.
- Product name shown to users**: A text input field containing "Cloudpath ES". This field is also highlighted with an orange border.
- Homepage URL (Optional)**: An empty text input field.
- Product logo URL (Optional)**: A text input field containing "http://www.example.com/logo.png".
- Privacy policy URL (Optional)**: An empty text input field.
- Terms of service URL (Optional)**: An empty text input field.

At the bottom of the form are "Save" and "Cancel" buttons. To the right of the form is a graphic of a laptop and a smartphone, and a text block explaining the 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. You must provide an email address and product name for OAuth to work."

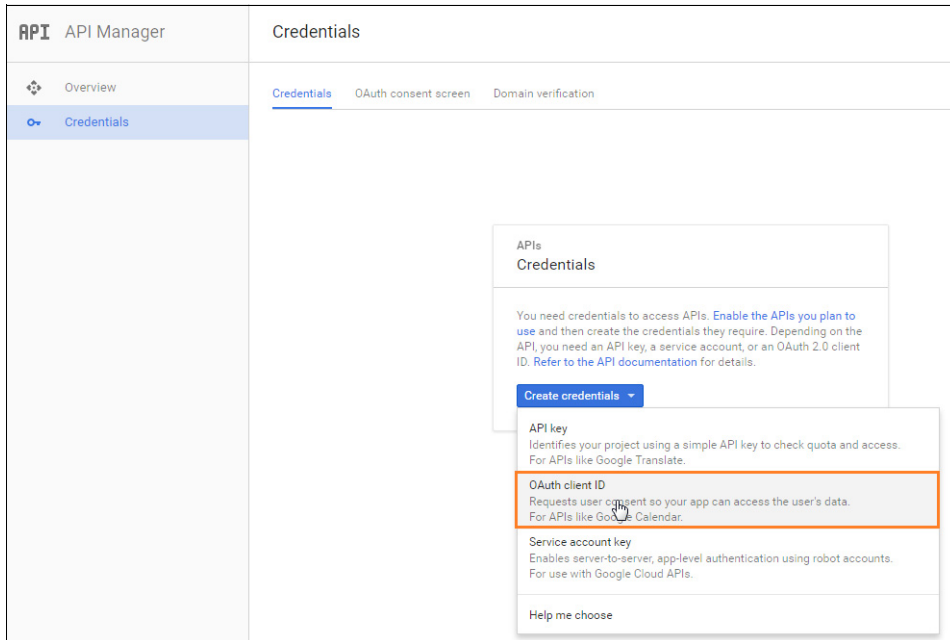
3. Save the OAuth consent screen page.

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 8. Create OAuth Client ID



3. Select *Application Type - Web application*.

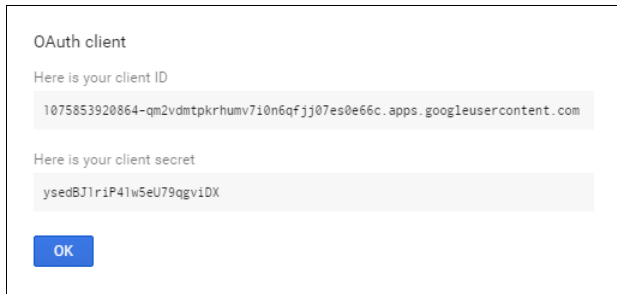
FIGURE 9. Create Client ID

The screenshot shows the 'API Manager' interface for creating a client ID. The left sidebar has 'Overview' and 'Credentials' (selected). The main content area is titled 'Credentials' and 'Create client ID'. There is a back arrow icon. The 'Application type' section has radio buttons for 'Web application' (selected), 'Android Learn more', 'Chrome App Learn more', 'iOS Learn more', 'PlayStation 4', and 'Other'. The 'Name' field contains 'Cloudpath ES web client'. The 'Restrictions' section has a sub-section 'Authorized JavaScript origins' with a blank input field. Below it is the 'Authorized redirect URIs' section with a text input field containing 'https://testURL.cloudpath.net/enroll/Test/Production/google' and a close button (X). At the bottom 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.
7. Click *Create*.

The Google Developer page displays the OAuth client ID and client secret for your web application.

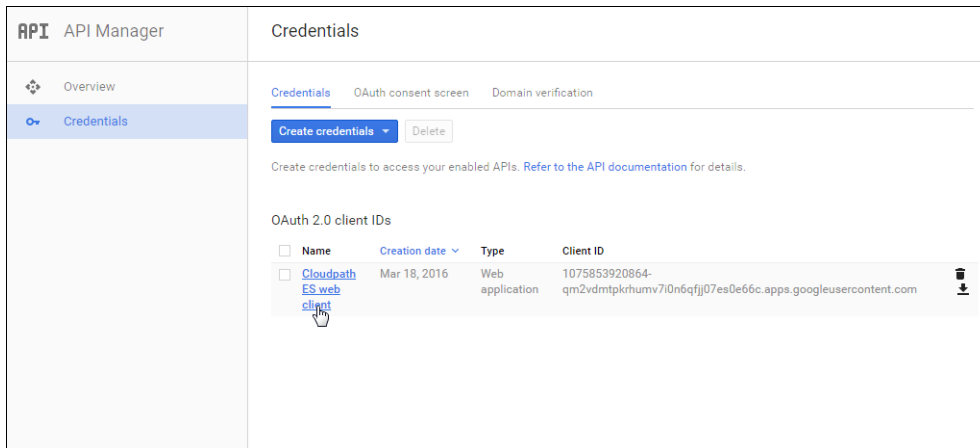
FIGURE 10. OAuth Client Information



View Client ID Details

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

FIGURE 11. OAuth Client IDs



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

FIGURE 12. Client ID for Web Application

API API Manager

Credentials

← Download JSON Reset secret Delete

Client ID for Web application

Client ID	1075853920864-qm2vdmtpkrhmv7i0n6qfj07es0e66c:apps.googleusercontent.com
Client secret	yse dB J 1 r i P 4 1 w 5 e U 7 9 q g v i D X
Creation date	Mar 18, 2016, 9:52:06 AM

Name

Cloudpath ES web client

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

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://testURI.cloudpath.net/enroll/Test/Production/google x

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 the Cloudpath ES.

Setting Up the Cloudpath ES

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

What You Need

- Google application Client ID
- Google application Client Secret

Cloudpath ES 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.

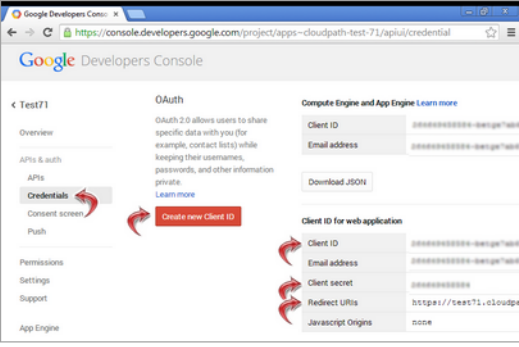
4. Enter the *Name* and *Description* of this configuration.

FIGURE 13. Third-Party Authentication Setup - Google

Google Configuration

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.



The client ID 'anonymous' has been deprecated by Google and should not be used.

Client ID:

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 URLs may be specified, with one per line.

Based on the current deployment locations, the Redirect URIs should be:
<https://anna41.cloudpath.net/enroll/AnnaTest/Production/google>

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

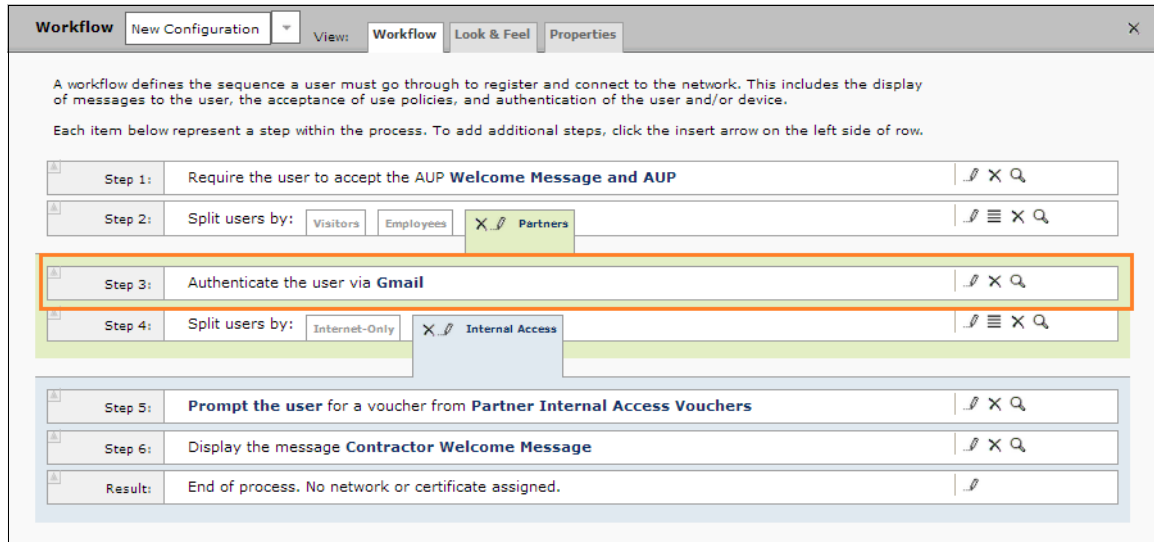
6. Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.
7. Enter the *Client ID* and *Client Secret* from the Google application.

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.

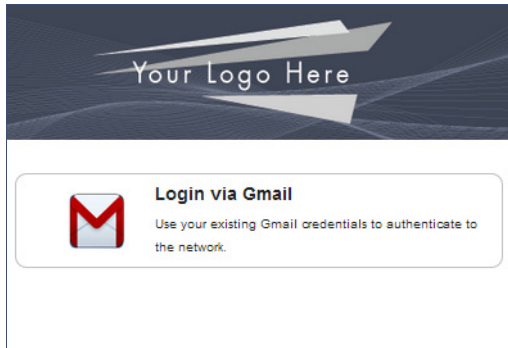
FIGURE 14. Cloudpath ES Workflow



User Experience

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

FIGURE 15. User Prompt for Google Authentication



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

Terminology

The following table defines terminology for the Google authentication feature.

TABLE 1. Third-Party Authentication Terminology

Term	Definition
Client ID	The ID that Google assigns to your application.
Client Secret	The secret key that allows your app to capture the Google request objects.
Enrollment	The process of a user becoming authenticated and ultimately gaining network access.
Enrollment workflow	The sequence a user must go through to register and connect to the network.
Google app	A web application directly within Google that allows you to add Google capabilities to an external website.
Onboarding Wireless Network	An open wireless network that provides access to the Cloudpath ES.
Secure Wireless Network	A WPA2-Enterprise wireless network.
Third-Party Authentication	Allow access to a network using a secure login through an outside application.

About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the Cloudpath ES and how it can simplify your wireless environment, visit www.cloudpath.net or contact a Cloudpath representative.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

Contact Information

General Inquiries: info@cloudpath.net

Support: support@cloudpath.net

Sales: sales@cloudpath.net

Media:media@cloudpath.net

Marketing:marketing@cloudpath.net

Phone:+1 303.647.1495 (US)

+1 866.472.6053 (US)

+44 (01) 161.261.1400 (UK)

Fax:+1 760.462.4569

Address:1120 W 122nd Ave, Suite 302

Westminster, CO 80234 USA