TECHNICAL DOCUMENTATION

Cloudpath
Enrollment System

Setting Up Third-Party Authentication Within Cloudpath Using Google™

Software Release 5.0
December 2016

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 5.0

December 2016

Setting Up Third-Party Authentication Within CloudpathES Using Google™

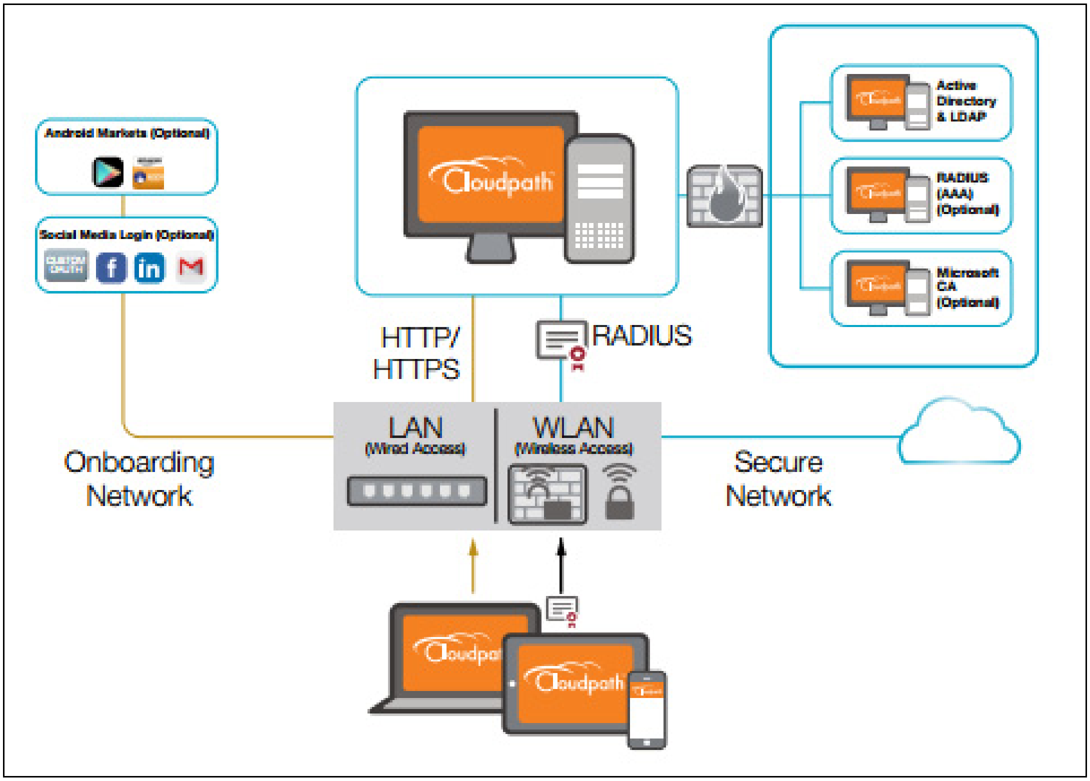
Cloudpath Security and Policy Management

Cloudpath Enrollment System (ES) software is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords.

Cloudpath software lets IT do with one system what usually requires many, while easily and automatically integrating with existing access and network security infrastructure..

The flexible workflow engine gives network administrators further control by blending traditional policies (AD, RADIUS, and 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 Security and Policy Management Platform



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

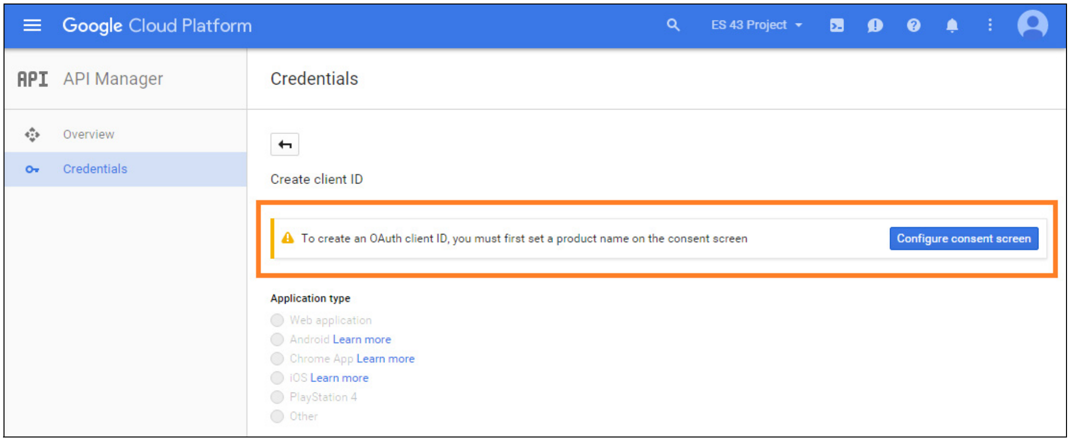
This section describes how to create the Google application to use with Cloudpath.

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 2. Warning Message



To create an OAuth client ID, you must first set a product name on the consent screen

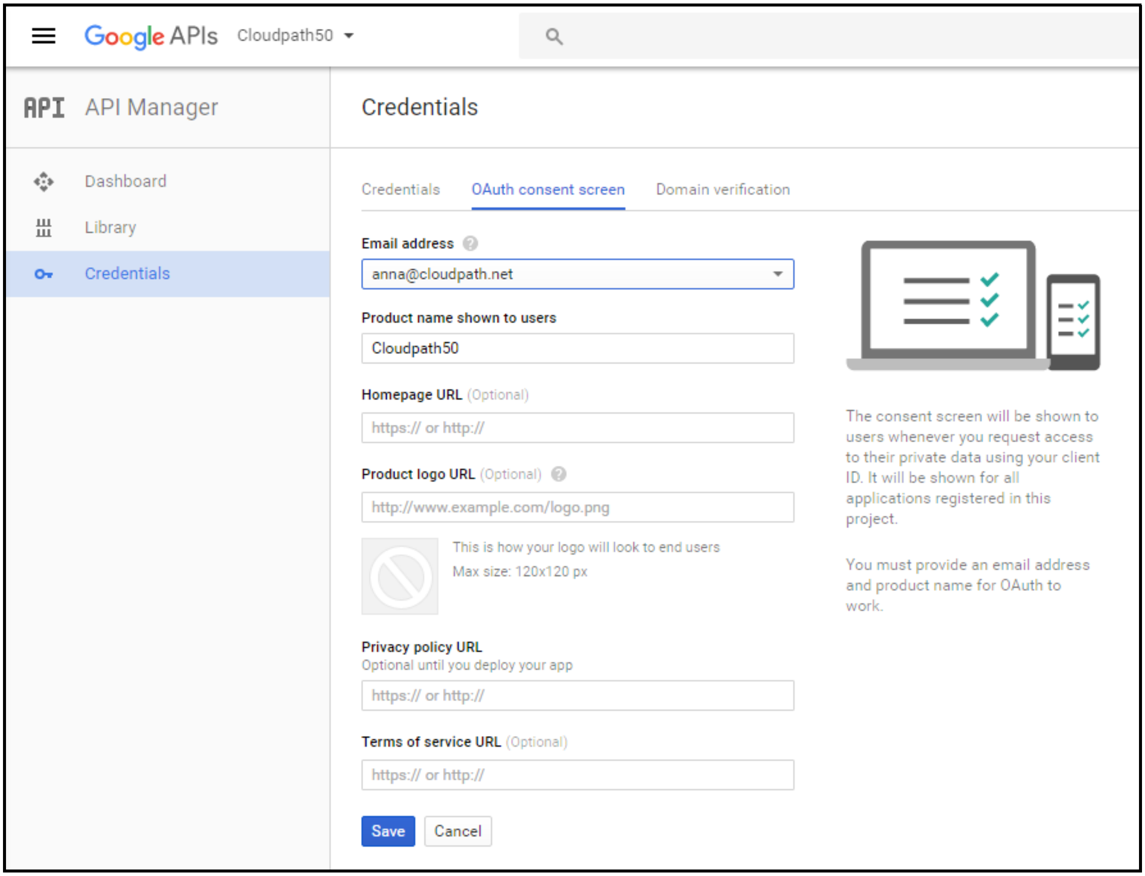
Configure OAuth Consent Screen

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 3. OAuth Consent Screen



Email address
anna@cloudpath.net

Product name shown to users
Cloudpath50

Homepage URL (Optional)
https:// or http://

Product logo URL (Optional)
http://www.example.com/logo.png

This is how your logo will look to end users
Max size: 120x120 px

Privacy policy URL
Optional until you deploy your app
https:// or http://

Terms of service URL (Optional)
https:// or http://

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.

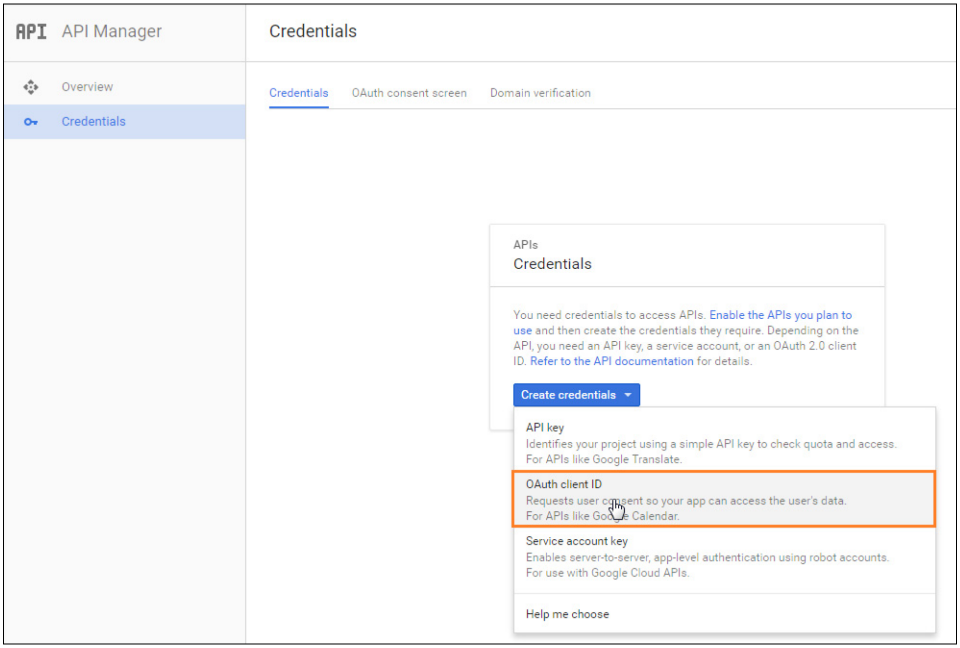
3. *Save* the OAuth consent screen page.

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 4. Create OAuth Client ID



You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. Refer to the API documentation for details.

API key
Identifies your project using a simple API key to check quota and access.
For APIs like Google Translate.

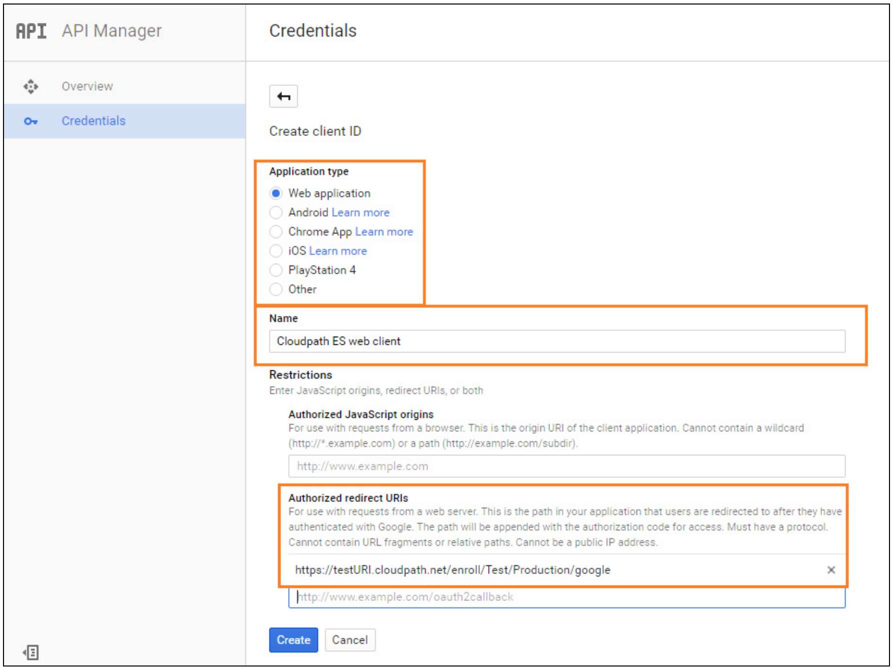
OAuth client ID
Requests user consent so your app can access the user's data.
For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts.
For use with Google Cloud APIs.

Help me choose

3. Select *Application Type - Web application*.

FIGURE 5. Create Client ID



Create client ID

Application type

● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ PlayStation 4
○ Other

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 ×

http://www.example.com/oauth2callback

Create Cancel

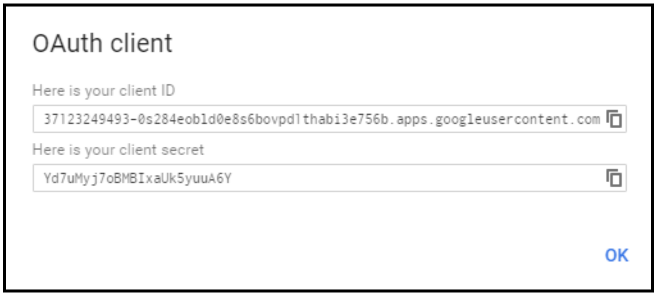
4. Enter the Name for your web application client.
5. On the *Create Client ID* page, leave the *Authorized Javascript origins* field blank.
6. In the *Authorized redirect URIs* field, the entry must be in this format *${ENROLLER_URL}/enroll/google/*, where ${ENROLLER_URL} is the external URL to which 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 6. OAuth Client Information



OAuth client

Here is your client ID

37123249493-0s284eobld0e8s6bovpdlthabi3e756b.apps.googleusercontent.com

Here is your client secret

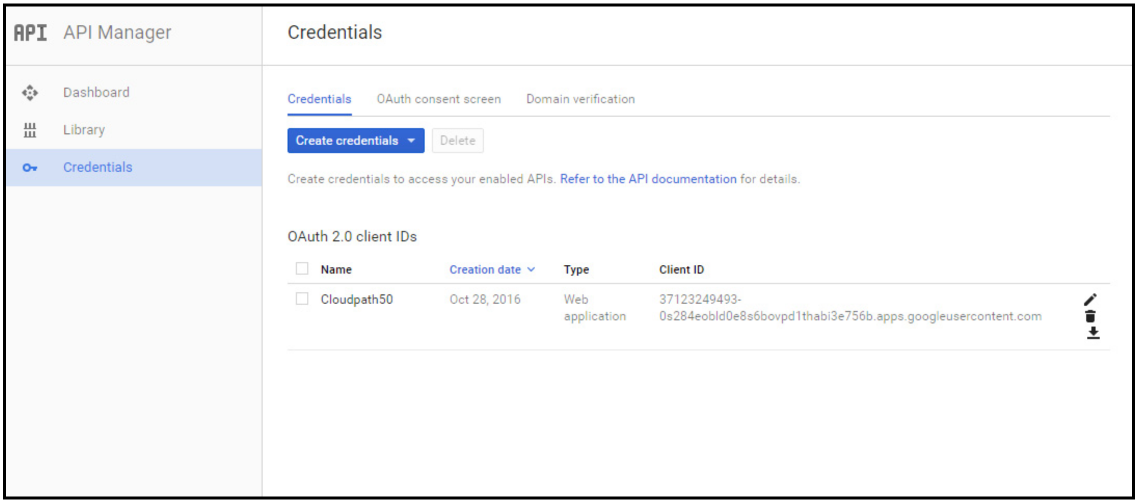
Yd7uMyj7oBMBIxaUk5yuuA6Y

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 7. OAuth Client IDs



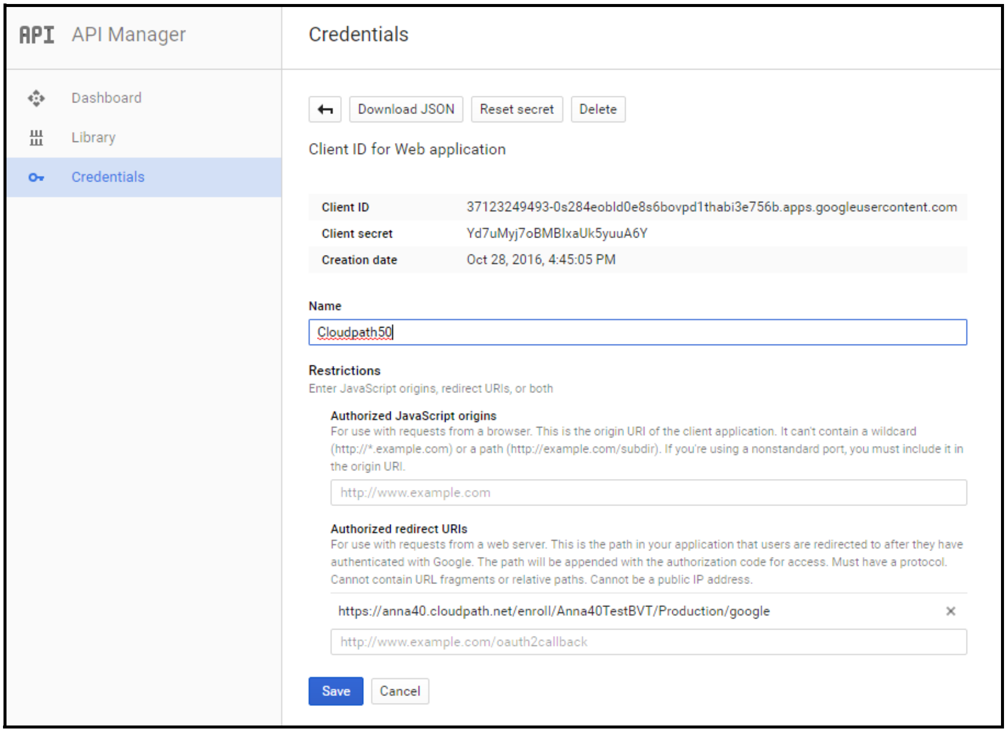
Create credentials to access your enabled APIs. Refer to the API documentation for details.

OAuth 2.0 client IDs

□	Name	Creation date	Type	Client ID
□	Cloudpath50	Oct 28, 2016	Web application	37123249493-0s284eobld0e8s6bovpd1thabi3e756b.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 8. Client ID for Web Application



Client ID for Web application

Client ID	37123249493-0s284eobld0e8s6bovpd1thabi3e756b.apps.googleusercontent.com
Client secret	Yd7uMyj7oBMBlxaUk5yuuA6Y
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

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.

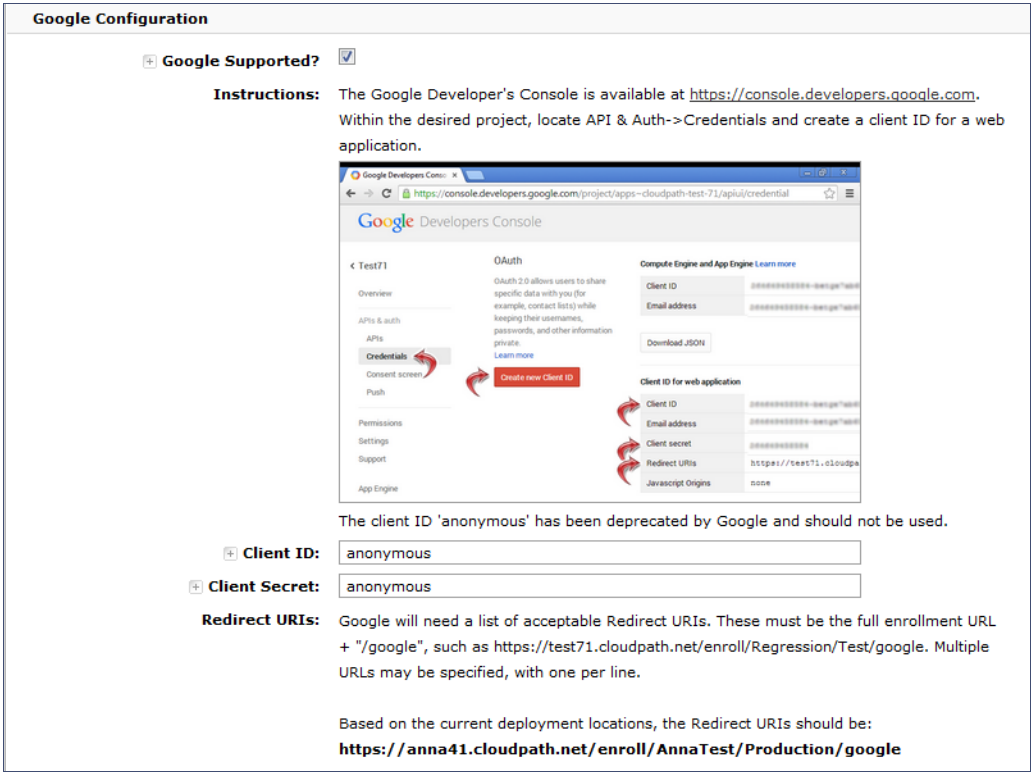
How to Add Third-Party Authentication to the Workflow

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 9. 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.

OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private.

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

⊞ **Client ID:** anonymous

⊞ **Client Secret:** anonymous

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

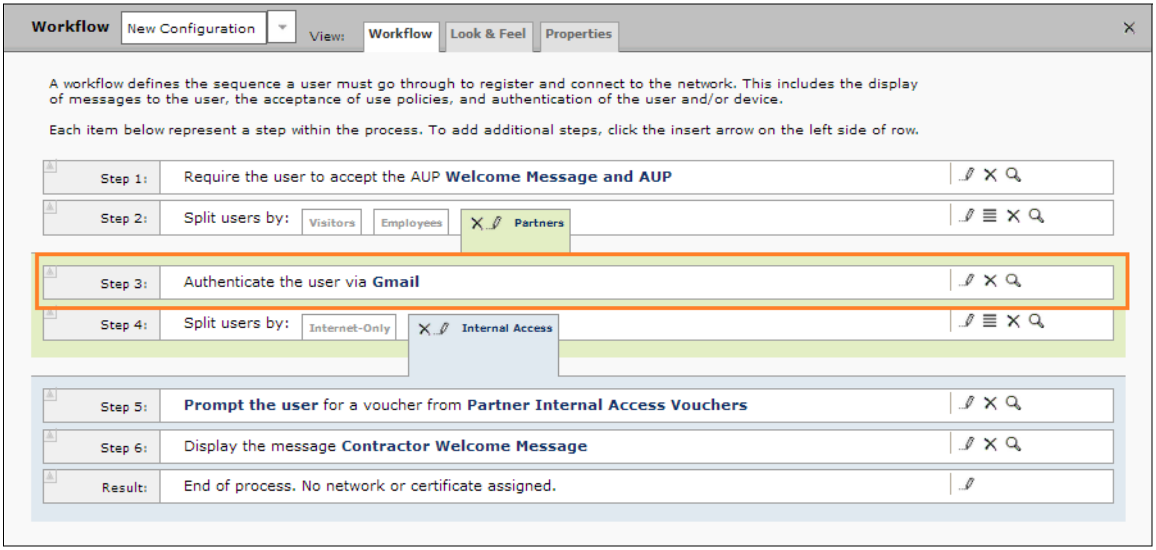
5. In the Google Configuration section, check the *Google Supported?* box.

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 10. Cloudpath Workflow



A workflow defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click the insert arrow on the left side of row.

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

Step 2: Split users by: Visitors | Employees | Partners

Step 3: Authenticate the user via **Gmail**

Step 4: Split users by: Internet-Only | Internal Access

Step 5: **Prompt the user** for a voucher from **Partner Internal Access Vouchers**

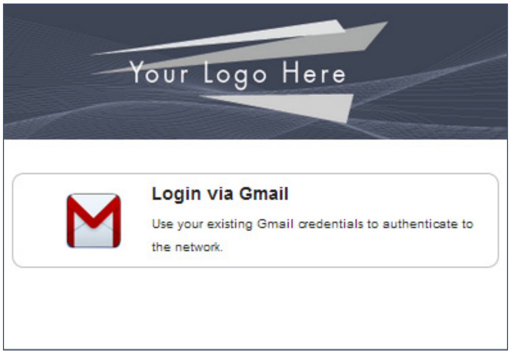
Step 6: Display the message **Contractor Welcome Message**

Result: End of process. No network or certificate assigned.

User Experience

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

FIGURE 11. User Prompt for Google Authentication



Login via Gmail

Use your existing Gmail credentials to authenticate to the network.

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