

# 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<sup>™</sup>, BeamFlex<sup>™</sup>, MediaFlex<sup>™</sup>, ChannelFly<sup>™</sup>, 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

≡	Google Developers C	Console 🔍 Test Project 2 - 🖬 🗊 🤨 🌲 🗄 (	
♠	Home	Dashboard         Recently selected projects           My Project 3         proud-will-R83           Cloudpath Project         aglie-aplicer-784	
Dashboard           Image: Activity	Dashboard Activity	API Project     api-project-964831187091       Project: Test Project 2.979 (#301727419082)     Try App Enc.       ID: test-project-2.979 (#301727419082)     environmen	
		Use Google APIs Use Google API	
		Enable APIs, create credentials, and track your usage     Managed VM dc     My Project 1     auspicious-ite-syd     tutoriais L       Image: With the project 1     Managed VM dc     My Project 2     deft-beanbag-720     deft-beanbag-720       Image: With the project 3     proud-will-783     proud-will-783     proud-will-783	
		API     Enable and manage APIs       Image and manage APIs     Image all projects       Image all projects     worst e software packages       Image all projects     ud Platform with just a few       Image all projects     Create a project	
		Try Compute Engine     Try App Engine (sandbox environment)       Spin up virtual machines using Google Compute Engine, Node ja, and MongoDB to create a guestbook app in this guided walkthrough.     Try App Engine (sandbox environment)       Create and deploy a Hello World app withbout worrying about the underlying infrastructure in this guided walkthrough     Create and deploy a Hello World app	
		The started App Engine documentation L <sup>2</sup>	

#### FIGURE 3. Name API Project

Project na	me 🕜			
ES 43 P	roject			
Your proje	ct ID will be es	-43-project 🕜	Edit	

4. Click Create. The Project page displays.

#### FIGURE 4. Project Page

	Google Developers Co	nsole o	ર				Cloudpath ES Project 👻					0
₼	Home	Dashboar	d									
- 99	Dashboard		Proje	ect: Cloudnath ES Project		Docu	mentation					
≣	Activity		ID: clo	oudpath-es-project (#1075853920864)	~		Google Cloud Platform docu	imentat	ion 🖾			
							Cloud Platform solutions					
				Use Google APIs Enable APIs, create credentials, and track your usage	Cloud Platform tutorials 🖸							
			API	Enable and manage APIs		Try App Engine Create and deploy a Hello	World a	рр				
				Try Compute Engine		۰Ô۰	Get started			$\sim$		
				Spin up virtual machines using Google Compute Engine, Node ja, and MongoDB to create a guestbook app in this guided walkthrough. Get started			Create a Cloud Stor	<b>age b</b> i ita safe	ucket			
							with high availability using	Cloud	Storage			
							Get started					

#### **Access API Manager**

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

#### FIGURE 5. API Manager Page

API	API Manager	Credentials
¢*	Overview	Credentials OAuth consent screen Domain verification
0+	Credentials	Create credentials * Delete
		Create credentials to access your enabled APIs. Refer to the API documentation for details.

- 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

≡	Google Cloud Platform	n Q ES 43 Project 🗸	>.	ø	0			9
API	API Manager	Credentials						
<	Overview	<b>f</b>						
0+	Credentials	Create client ID						
		A To create an OAuth client ID, you must first set a product name on the consent screen			Config	ure con	sent so	reen
		Application type						
		Web application Android Learn more						
		Chrome App Learn more						
		It is Learn more PlayStation 4 Other						

#### **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.

	Google Cloud Platform		۹	ES 43 Project 👻	2.	ß	0	۰	:	9
API	API Manager	Credentials								
٠	Overview	Credentials OAuth consent screen Domain verification								
0.	Credentials	Email address  anna@cloudpath.net Product name shown to users Cloudpath ES Homepage URL (Optional) Product logo URL (Optional) Interp://www.example.com/logo.png This is how your logo will look to end users Max size: 120x120 px Privacy policy URL (Optional) Terms of service URL (Optional) Save Cancel		The consent scree users whenever yo to their private dal ID. It will be shown applications regist project. You must provide and product name work.	en will b bu reque a using n for all tered in an ema for OA	e shown est accee your cli il addrer uth to	ss ss			

#### FIGURE 7. OAuth Consent Screen

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

API	API Manager	Credentials
4Ç.>	Overview	Credentials OAuth consent screen Domain verification
0+	Credentials	
		APIs         Credentials         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 acrice account, or an OAuth 2.0 client ID. Refer to the API documentation for details.         Create credentials         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 complete to 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 9. Create Client ID

API	API Manager	Credentials
٠	Overview	•
0+	Credentials	Create client ID
		Application type  Web application  Android Learn more  Chrome App Learn more  Ols Learn more  PlayStation 4  Other
		Name Cloudpath ES web client
		Restrictions           Enter JavaScript origins, redirect URIs, or both:           Authorized JavaScript origins           For use with request 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 × https://www.example.com/oauth2callback
411		Create

- 4. Enter the Name for your web applciation 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

API	API Manager	Credentials
٠	Overview	Credentials OAuth consent screen Domain verification
0+	Credentials	Create credentials - Delete
		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
		Cloudpath Mar 18, 2016 Web 1075853920864- <u>ES web</u> application qm2vdmtpkrhumv7/0n6qfjj07es0e66c.apps.googleusercontent.com teliant

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

API	API Manager	Credentials
*** 0+	Overview Credentials	Image: Download JSON         Reset secret         Delete           Client ID for Web application         Image: Delete         Image: Delete         Image: Delete
		Client ID 1075853920864-qm2vdmtpkrhumv7i0n6qfjj07es0e66c.apps.googleusercontent.com
		Client secret ysedBJ1riP41w5eU79qgviDX
		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 floogle. 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
42		Save Cancel

#### FIGURE 12. Client ID for Web Application

#### 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?	<b>V</b>				
Instructions:	The Google Dev	eloper's Console is ava	ilable at <u>https</u>	://console.developers.go	ogle.com.
	Within the desire	ed project, locate API &	Auth->Crede	ntials and create a client	ID for a web
	application.				
	Concerto De referenza Concerto X			- 8 x	
	← → C A https://cor	sole.developers.google.com/project/ap	ps-cloudpath-test-71/a	ipiui/credential	
	Google Develo	opers Console			
	< Test71	OAuth	Compute Engine and Ap	Engine Learn more	
	Overview	OAuth 2.0 allows users to share specific data with you (for	Client ID	241412422224-betge"abil	
	APIs 8 auth	example, contact lists) while keeping their usernames,	Email address	244443433334-betpe*abil	
	APIs	passwords, and other information private.	Download JSON		
	Credentials	Learn more			
	Consent screen	Create new Client ID	Client ID for web applica	tion	
			Client ID	241413133314-betpe?ab4	
	Permissions		Email address	244449438384-betpe"abd	
	Support	(	Client secret	beneral (rear 21, c) and co	
		(	Javascript Origins	nttps://test/1.cloudpa	
	App Engine		< conscript origins	in the second se	
	The client ID 'an	onymous' has been de	precated by G	loogle and should not be i	used.
Client ID:	anonymous				
Client Secret	2000/000/00				
F chent Secret.	anonymous				
Redirect URIs:	Google will need	l a list of acceptable Re	direct URIs. T	hese must be the full enro	ollment URL
	+ "/google", suc	h as https://test71.clou	idpath.net/eni	oll/Regression/Test/goog	le. Multiple
	URLs may be sp	ecified, with one per lin	e.		
	Based on the cu	rrent deployment locati	ons, the Redi	rect URIs should be:	
	https://anna4	1.cloudpath.net/enr	oll/AnnaTes	t/Production/google	
	nttp3.//anna4	r.ciouupath.net/em	on/ Anna res	in Fronceion/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.



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

FIGURE 14. Cloudpath ES Workflow

Workflow New Configurat	ion View: Workflow Look & Feel Properties	×				
A workflow defines the sec of messages to the user, Each item below represent	quence a user must go through to register and connect to the network. This includes the display the acceptance of use policies, and authentication of the user and/or device. t a step within the process. To add additional steps, click the insert arrow on the left side of row.					
Step 1: Require	e the user to accept the AUP Welcome Message and AUP					
Step 2: Split us	sers by: Visitors Employees X Partners					
Step 3: Authen	ticate the user via Gmail					
Step 4: Split us	sers by: Internet-Only X I Internal Access					
Step 5: Promp	t the user for a voucher from Partner Internal Access Vouchers					
Step 6: Display	Display the message Contractor Welcome Message $\mathscr{I} \times Q$					
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 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-Part	y 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 <u>www.cloudpath.net</u> 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