CONFIGURATION GUIDE

Cloudpath Enrollment System Third-Party Authentication Using Google™ Configuration Guide, 5.4

Supporting Cloudpath Software Release 5.4

Part Number: 800-72199-001 Rev A
Publication Date: 08 March 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Setting Up the Google Application... 4
What You Need.. 4
Create Web Application Project.. 4

Setting Up Cloudpath...5
What You Need.. 5
Cloudpath Configuration.. 5
User Experience... 7

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

Create Web Application Project

The steps given here are only very high-level to inform you what information you will need to collect from your Google project that is needed on the Cloudpath UI-side configuration. You need to refer to your Google developer's documentation for all the information about creating your application.

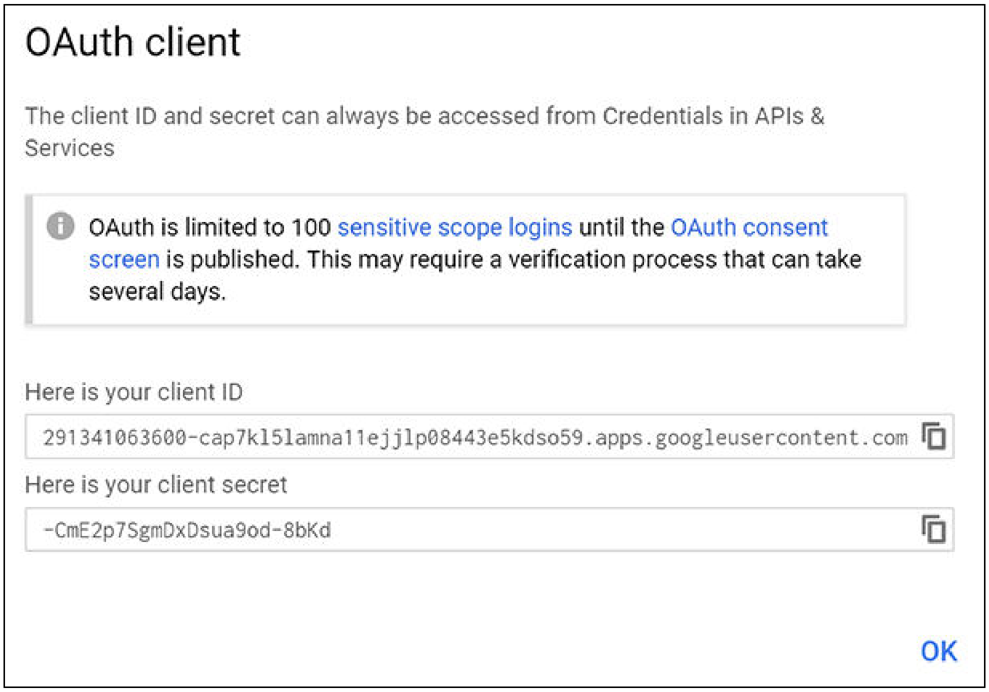
1. Go to https://console.developers.google.com.
2. Sign in to your Google account.
3. Create and name your API web-application project.
4. During creation of your application, you may see a field called "Authorized Javascript origins." Leave this field blank.
5. When you get to the "Authorized redirect 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
    To obtain the Redirect URI, when you are creating a workflow and you choose the "Authenticate to a third party" step and click **Next**, scroll down to the "Google" section and click the "Google Supported ?" checkbox. The redirect URI appears.

6. At some point during the process, you will be notified of the following information that you need to take note of because you will need this information for Cloudpath configuration:
   - client ID
   - client Secret

   An example of one screen that provides you with this information is the following:

FIGURE 1 **Client ID and Client Secret for Google Application**



OAuth client

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is published. This may require a verification process that can take several days.

Here is your client ID

291341063600-cap7kl5lamna11ejjlp08443e5kdso59.apps.googleusercontent.com

Here is your client secret

-CmE2p7SgmDxDsua9od-8bKd

Setting Up Cloudpath

After the Google application is set up, you 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

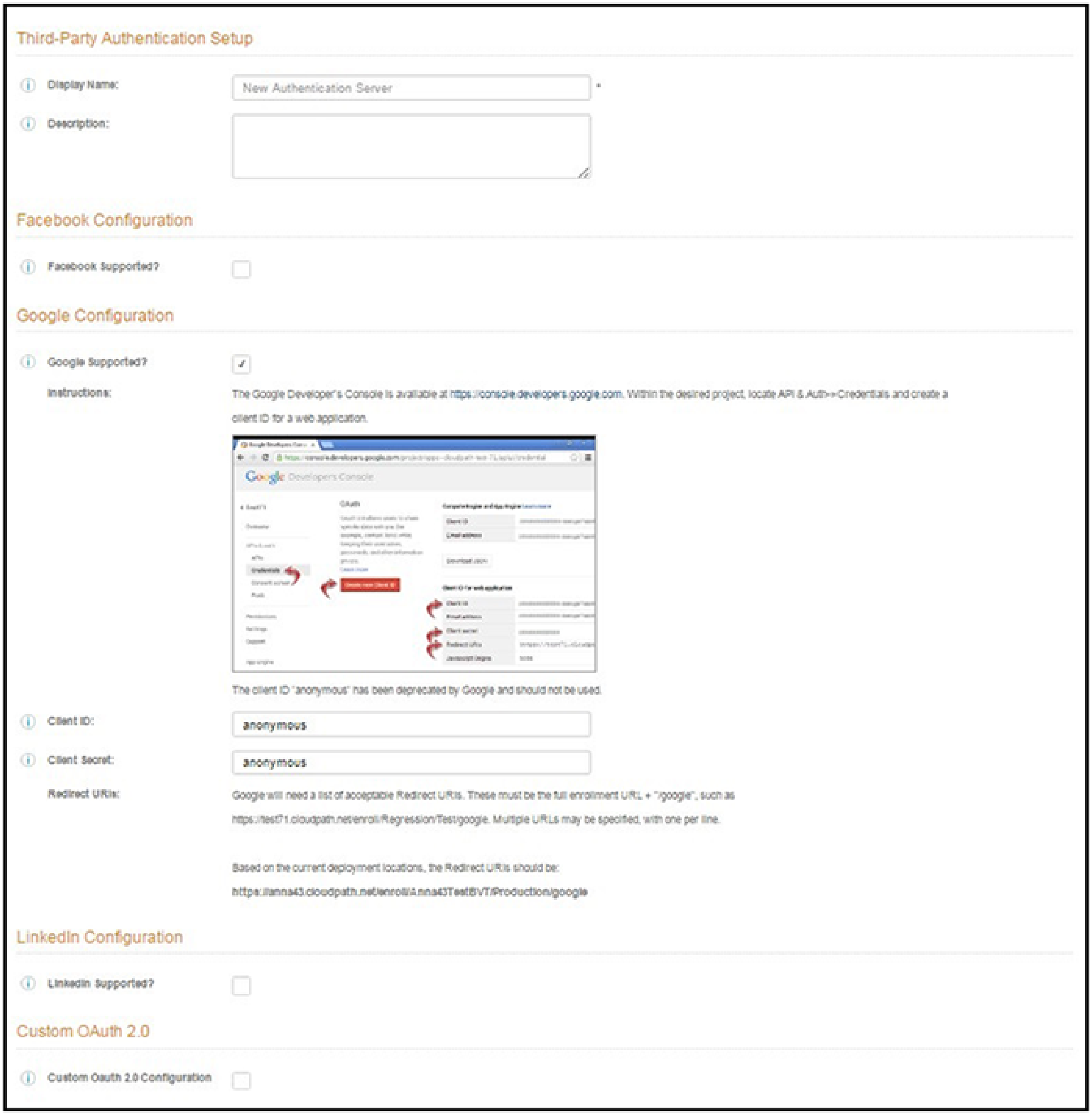
This section describes how to add a step to the enrollment workflow to authenticate a user using the Google application.

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 2 Google Third-Party Authentication Setup



Third-Party Authentication Setup

Display Name: New Authentication Server *

Description:

Facebook Configuration

Facebook Supported? □

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: 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://anna43.cloudpath.net/enroll/Anna43TestBVT/Production/google

LinkedIn Configuration

LinkedIn Supported? □

Custom OAuth 2.0

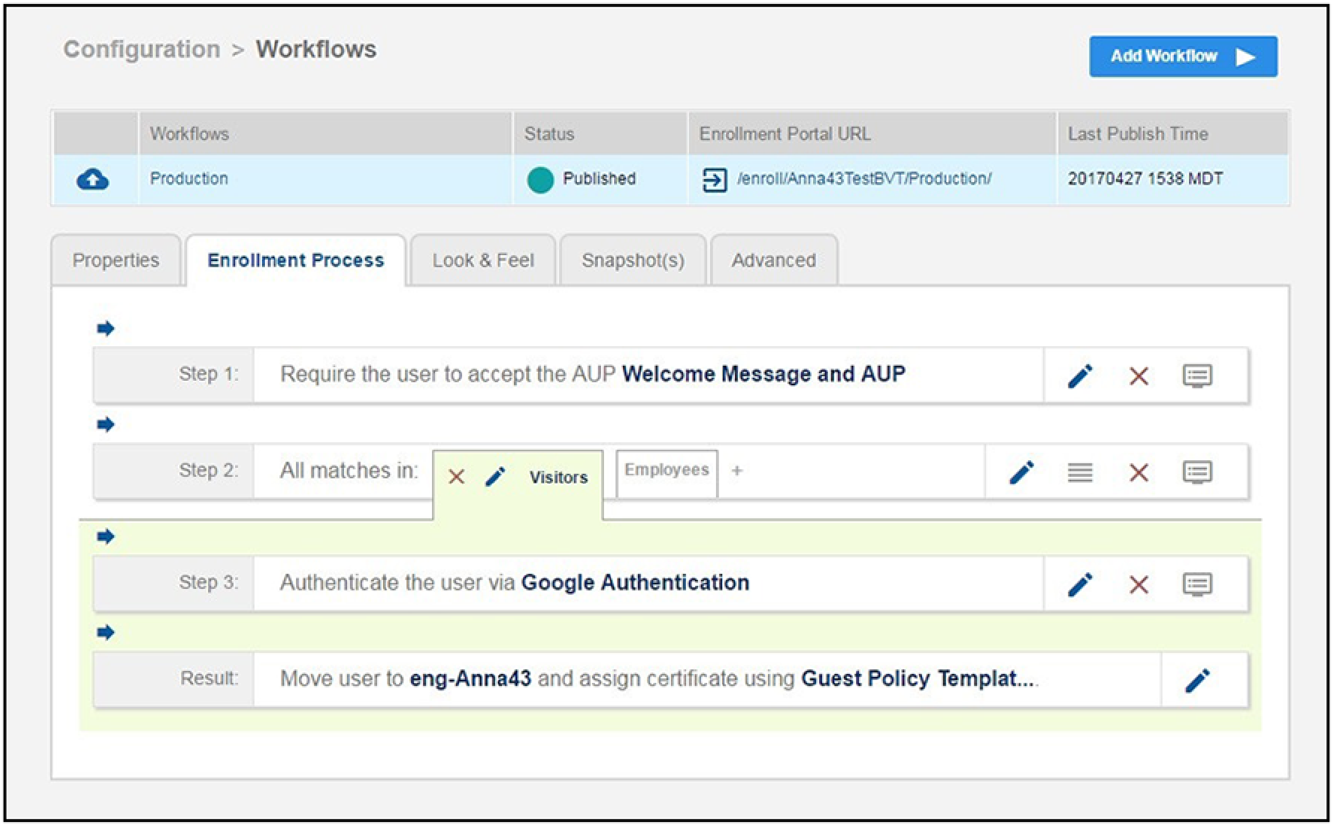
Custom Oauth 2.0 Configuration □

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 3 Cloudpath Workflow



Configuration > Workflows

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

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

Step 2: All matches in: Visitors | Employees +

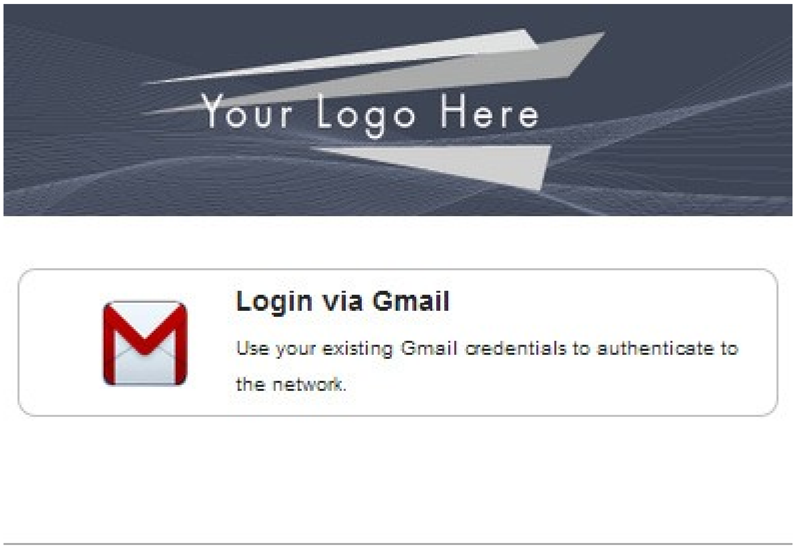
Step 3: Authenticate the user via **Google Authentication**

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 4 User Prompt for Google Authentication



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.

RUCKUS™
an ARRIS company

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com