

Setting Up Third-Party Authentication Within Cloudpath Using Google[™]

Supporting Software Release 5.2

Copyright Notice and Proprietary Information

Copyright 2017 Brocade Communications Systems, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of or as expressly provided by under license from Brocade.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. BROCADE and RUCKUS WIRELESS, INC. AND THEIR LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. BROCADE and RUCKUS RESERVE THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL BROCADE or RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and in other countries. Brocade, the B-wing symbol, MyBrocade, and ICX are trademarks of Brocade Communications Systems, Inc. in the United States and in other countries. Other trademarks may belong to third parties.

Contents

- Setting Up the Google Application.....4**
 - What You Need.....4
 - Google App Configuration.....4
- Setting Up Cloudpath.....9**
 - What You Need.....9
 - Cloudpath Configuration..... 10
 - User Experience..... 12

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

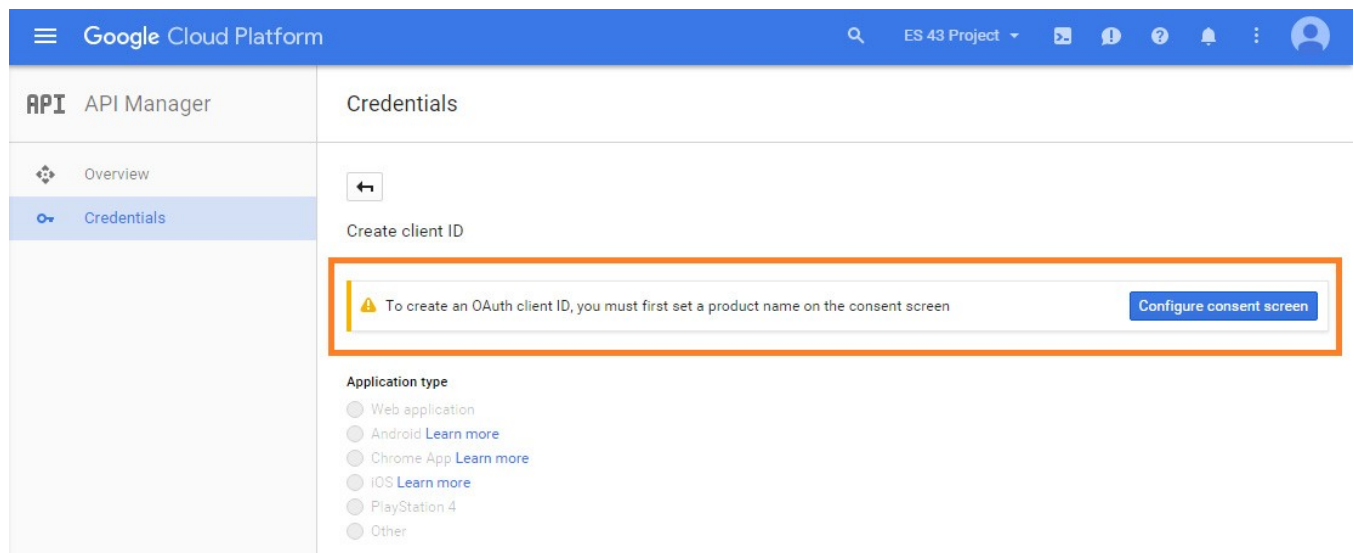
This section describes how to create the Google application to use with Cloudpath.

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 API Manager interface for the 'Cloudpath50' project. The left sidebar is titled 'API Manager' and has a 'Credentials' tab selected. The main content area is titled 'Credentials' and has three sub-tabs: 'Credentials', 'OAuth consent screen' (which is active), and 'Domain verification'. The 'OAuth consent screen' tab contains several form fields: 'Email address' (a dropdown menu with 'anna@cloudpath.net' selected), 'Product name shown to users' (a text input field with 'Cloudpath50'), 'Homepage URL (Optional)' (a text input field with 'https:// or http://'), 'Product logo URL (Optional)' (a text input field with 'http://www.example.com/logo.png'), a logo upload section with a placeholder image and the text 'This is how your logo will look to end users. Max size: 120x120 px', 'Privacy policy URL' (a text input field with 'https:// or http://'), and 'Terms of service URL (Optional)' (a text input field with 'https:// or http://'). At the bottom of the form are 'Save' and 'Cancel' buttons. On the right side 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.'

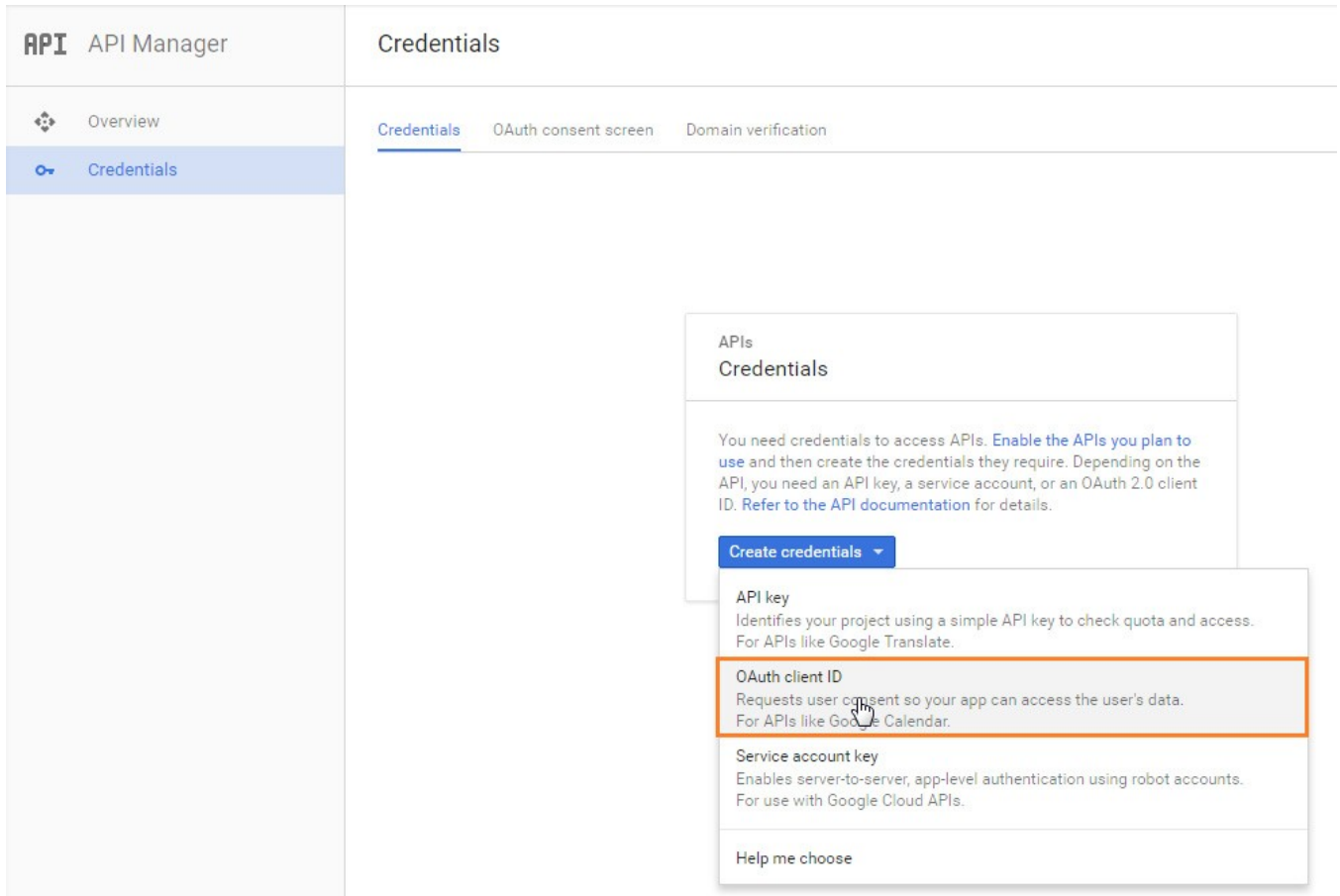
3. Save the **OAuth consent screen** page.

Create Client ID

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

- 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 'API Manager' interface for creating a client ID. On the left, there is a navigation menu with 'Overview' and 'Credentials' (selected). The main content area is titled 'Credentials' and 'Create client ID'. It features several input fields and 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 titled 'Enter JavaScript origins, redirect URIs, or both'.
 - Authorized JavaScript origins:** A text input field containing 'http://www.example.com'.
 - Authorized redirect URIs:** A list of text input fields. The first field contains 'https://testURI.cloudpath.net/enroll/Test/Production/google' and has a close button (X). The second field contains 'http://www.example.com/oauth2callback'.
- Buttons:** 'Create' (blue) and 'Cancel' (grey) buttons at the bottom.

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

37123249493-0s284eob1d0e8s6bovdp1thabi3e756b.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

The screenshot shows the Google API Manager interface. On the left is a navigation menu with 'API Manager' at the top, followed by 'Dashboard', 'Library', and 'Credentials' (which is selected). The main content area is titled 'Credentials' and has sub-tabs for 'Credentials', 'OAuth consent screen', and 'Domain verification'. Below the tabs are buttons for 'Create credentials' and 'Delete'. A message states: 'Create credentials to access your enabled APIs. Refer to the API documentation for details.' Below this is a section for 'OAuth 2.0 client IDs' with a table:

| <input type="checkbox"/> | Name | Creation date | Type | Client ID | |
|--------------------------|-------------|---------------|-----------------|---|--|
| <input type="checkbox"/> | Cloudpath50 | Oct 28, 2016 | Web application | 37123249493-0s284eob1d0e8s6bovdp1thabi3e756b.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

The screenshot shows the 'Credentials' page in the Google API Manager. On the left is a navigation menu with 'API Manager' at the top, and 'Dashboard', 'Library', and 'Credentials' below. The 'Credentials' page title is 'Credentials'. At the top right of the main content area are buttons for 'Download JSON', 'Reset secret', and 'Delete'. Below these is the title 'Client ID for Web application'. A table displays the following information:

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

Below the table is a 'Name' field containing 'Cloudpath50'. Underneath is the 'Restrictions' section, which includes instructions to 'Enter JavaScript origins, redirect URIs, or both'. It has two sub-sections: 'Authorized JavaScript origins' with a text input field containing 'http://www.example.com', and 'Authorized redirect URIs' with a list of URIs including 'https://anna40.cloudpath.net/enroll/Anna40TestBVT/Production/google' and 'http://www.example.com/oauth2callback'. At the bottom are 'Save' and 'Cancel' buttons.

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, 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.

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

FIGURE 8 Google Third-Party Authentication Setup

Third-Party Authentication Setup

Display Name:

Description:

Facebook Configuration

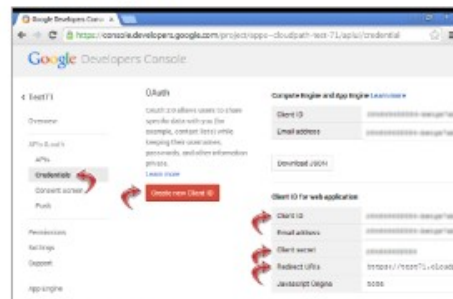
Facebook Supported?

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:

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

LinkedIn Supported?

Custom OAuth 2.0

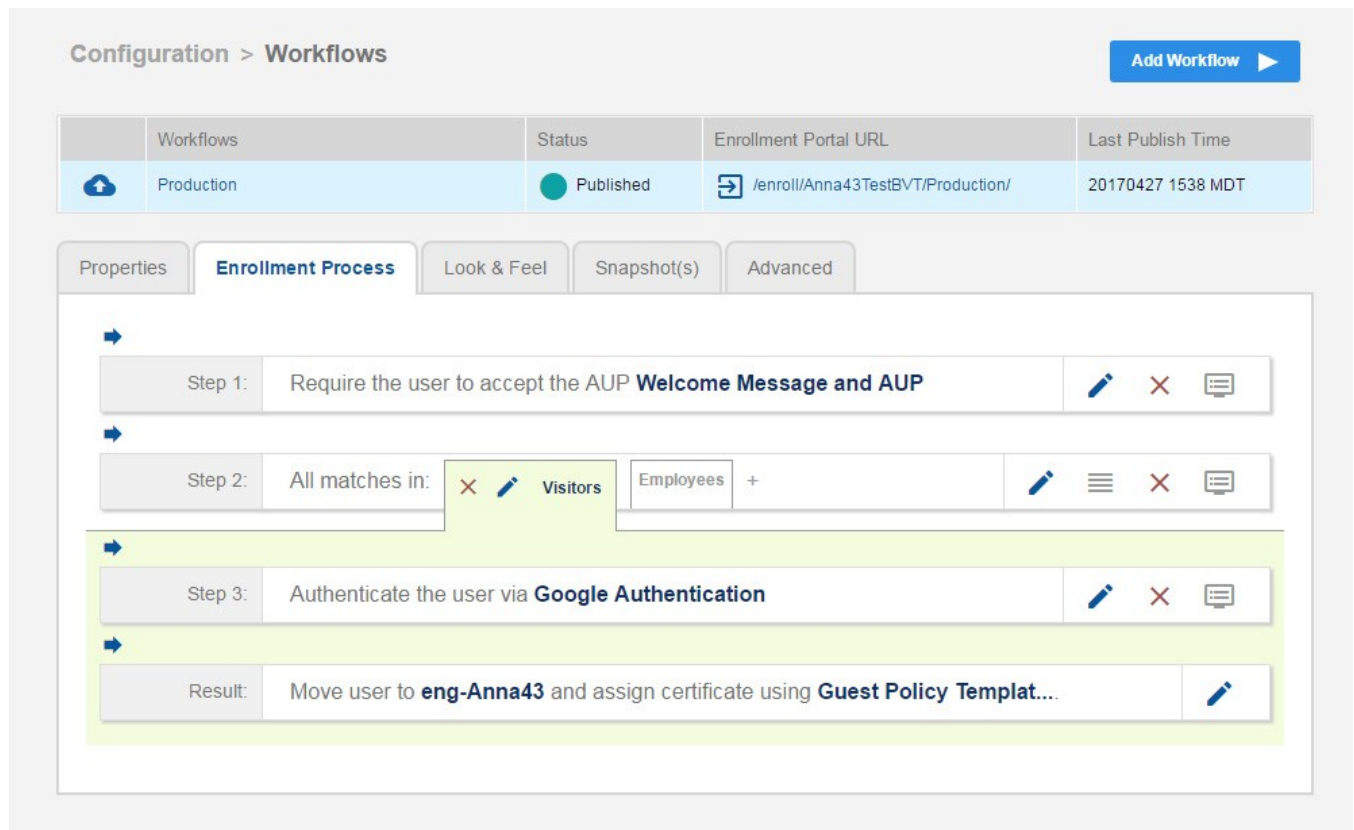
Custom OAuth 2.0 Configuration

- In the Google Configuration section, check the **Google Supported?** box.
- Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.

Setting Up Cloudpath User Experience

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



The screenshot displays the 'Configuration > Workflows' interface. At the top right, there is a blue 'Add Workflow' button with a play icon. Below this is a table with the following data:

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

Below the table are tabs for 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Enrollment Process' tab is active, showing a workflow with four steps:

- 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.



Copyright © 2006-2017. Ruckus Wireless, Inc.
350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com