CONFIGURATION GUIDE

Cloudpath Enrollment System Third-Party Authentication Configuration Guide, 5.6

Supporting Cloudpath Software Release 5.6

Part Number: 800-72518-001 Rev A
Publication Date: 15 December 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

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

Contents

Using Facebook for Third-Party Authentication....5
Setting Up the Facebook Application....5
What You Need To Set Up the Facebook Application....5
Creating the New Facebook App....5
Setting Up Cloudpath for Facebook Authentication....5
What You Need to Configure Cloudpath for Facebook....6
How to Add Facebook Authentication to the Workflow....6
User Experience for Facebook Authentication....9

Using Google for Third-Party Authentication....11
Setting Up the Google Application....11
What You Need To Set Up The Google Application....11
Creating the Google Web Application Project....11
Setting Up Cloudpath for Google Authentication....12
What You Need to Configure Cloudpath for Google....12
How to Add Google Authentication to the Workflow....12
User Experience for Google Authentication....14

Using LinkedIn for Third-Party Authentication....17
Setting Up the LinkedIn Application....17
What You Need To Set Up The LinkedIn Application....17
How to Set Up the LinkedIn App....17
Setting Up Cloudpath for LinkedIn Authentication....20
What You Need to Configure Cloudpath for LinkedIn....20
How to Add LinkedIn Authentication to the Workflow....20
User Experience for LinkedIn Authentication....22

Using Facebook for Third-Party Authentication

- Setting Up the Facebook Application..... 5
- Setting Up Cloudpath for Facebook Authentication..... 5

Setting Up the Facebook Application

Before configuring Cloudpath for Facebook authentication, you must set up the Facebook application.

What You Need To Set Up the Facebook Application

- Facebook login credentials
- Name and Namespace for your application
- Display Name for your application
- Domain and Website URL for your application

Creating the New Facebook App

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

1. Go to http://developer.facebook.com
2. Log in using your Facebook credentials.
3. Follow the instructions in the developer's manuals on how to create a website application.
4. During the process, you need to create an App ID.
5. Later in the process, you can go to the dashboard, where both the App ID and the App Secret are shown. Be sure to write down these values because you will need them during the Cloudpath configuration process.
6. Continue the configuration process in the Basic Settings area. You will need to add a Website platform.
7. For site URL and Valid OAuth Redirect URI, obtain this information from the Cloudpath workflow process in the Cloudpath UI. When you choose the "Authenticate to a third party" step and click **Next**, scroll down to the "Facebook" section and click the "Facebook Supported ?" checkbox.

Setting Up Cloudpath for Facebook Authentication

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

What You Need to Configure Cloudpath for Facebook

- Facebook App ID
- Facebook App Secret
- (Optional) Scope parameters, Event ID, and Liked Page ID for your Facebook application

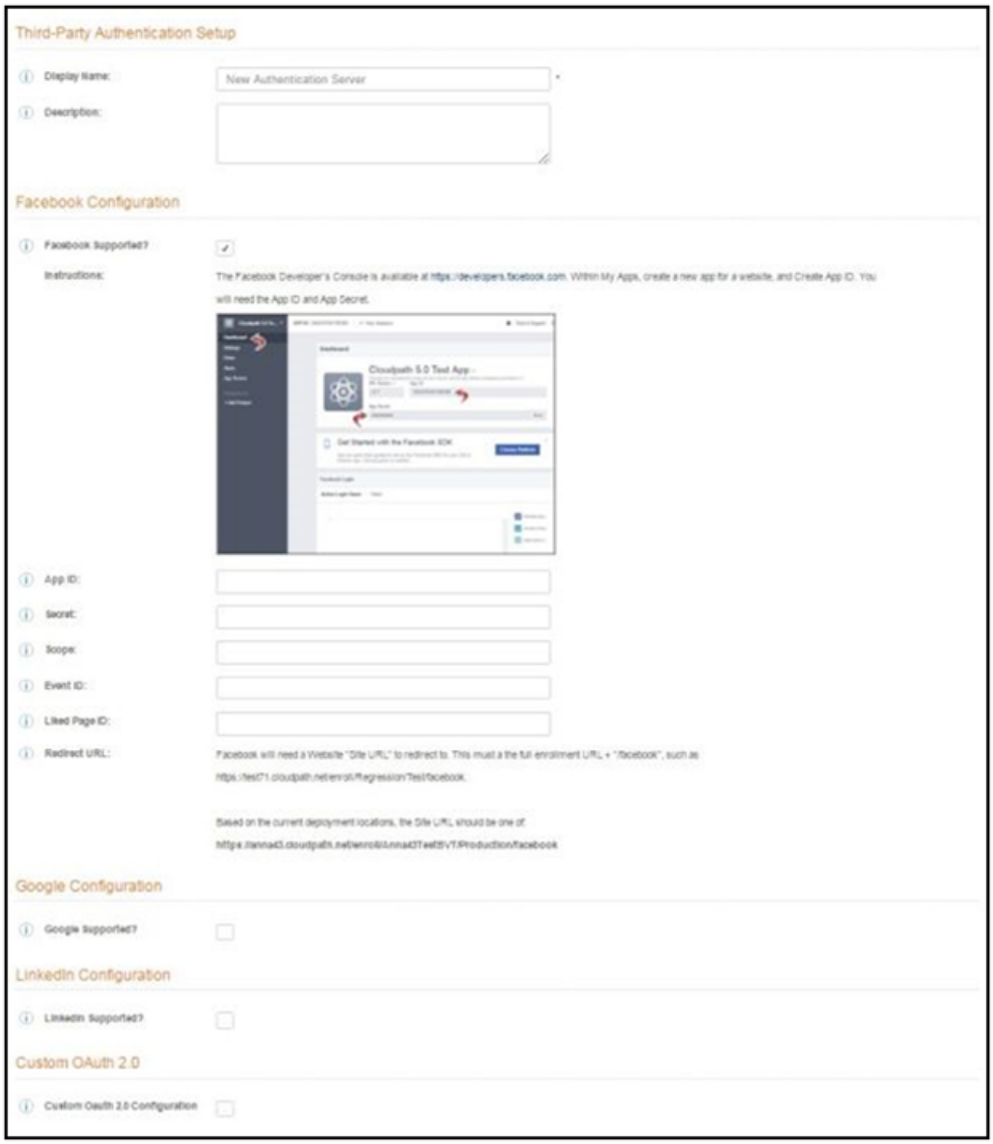
How to Add Facebook Authentication to the Workflow

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 1 Cloudpath Third-Party Authentication Setup

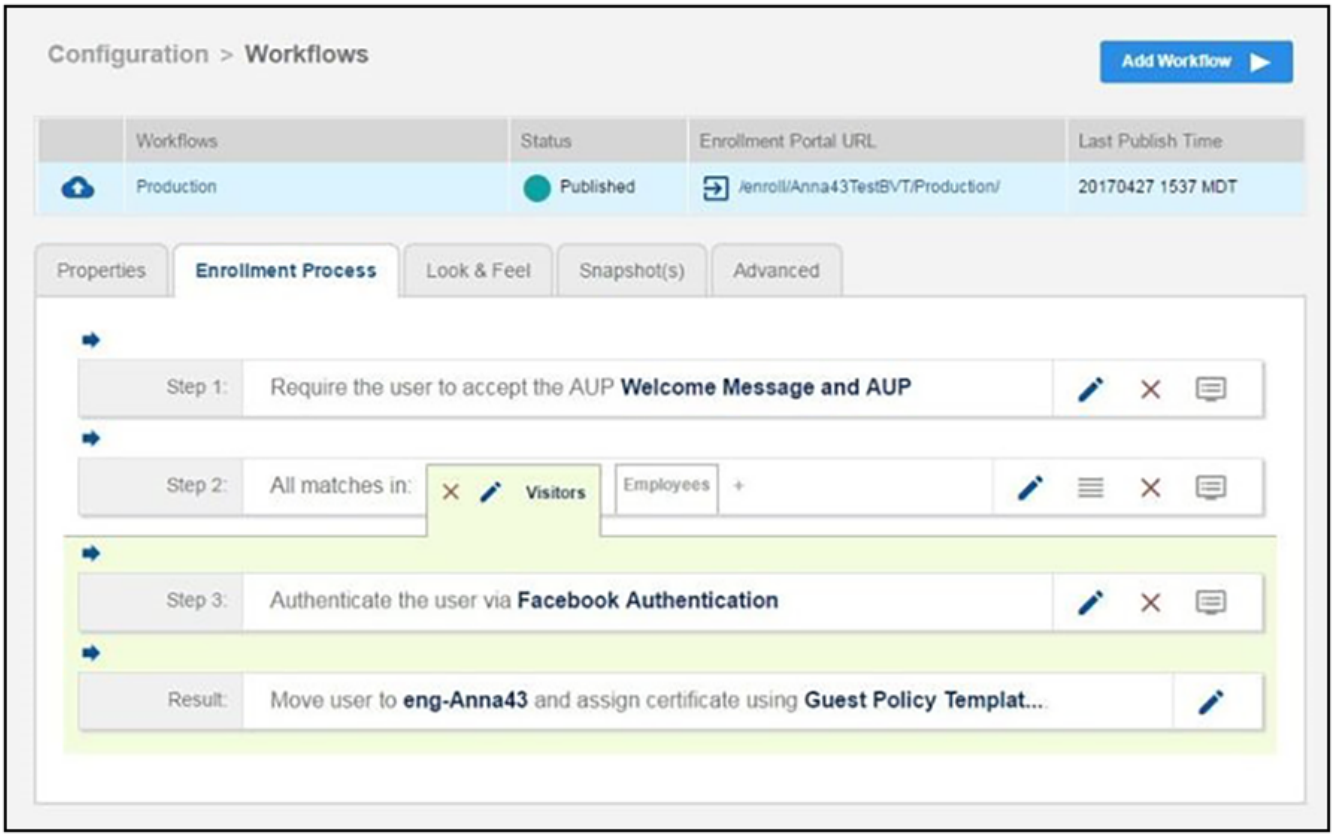


5. In the Facebook Configuration section, check the **Facebook Supported?** box and complete the following fields:
   - **App ID** - The **App ID** from the Facebook application you just created.
   - **Secret** - The **App Secret** from the Facebook application you just created.
   - Optional settings:
     - **Scope** - A comma separated list of permission names that allows the application to read or write additional data (such as email or user_group) from the Facebook application. If scope is left blank, you can only obtain the **Facebook profile ID**, **URL**, and **Name**.
     - **Event ID** and **Liked Page ID** - Allows the application to provide additional information about the user. The **Scope** must include **user_likes** to use **Liked Page ID**, and **user_events** to use **Event ID**. Adding a user_event (or user_likes) in the Scope allows you to create a filter in the workflow based on whether a user is in the user_event (or user_likes) group. See the Identity Information in the Enrollment Record to view the User Groups.

       NOTE
       To obtain the **Event ID** or **Page ID**, right-click on the FB page or event and **View Page Source**, then search for the string **event_id** or **page_id**.

6. Click **Save**. The Facebook authentication step is added to your enrollment workflow.

FIGURE 2 Workflow with Facebook Authentication



User Experience for Facebook Authentication

During the enrollment process, the user is prompted to authenticate using their Facebook credentials.

- If the user is logged into Facebook, the enrollment continues.
- If the user is not logged into Facebook, they are prompted to log in, and after a successful authentication, redirected back to Cloudpath to continue with the enrollment process.

FIGURE 3 Authenticate Using Facebook

Using Google for Third-Party Authentication

- Setting Up the Google Application..... 11
- Setting Up Cloudpath for Google Authentication.....12

Setting Up the Google Application

Before configuring Cloudpath for Google authentication, you must set up the Google application.

What You Need To Set Up The Google Application

- Google login credentials
- Branding information for your application
- Redirect URL for your application

Creating the Google 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.

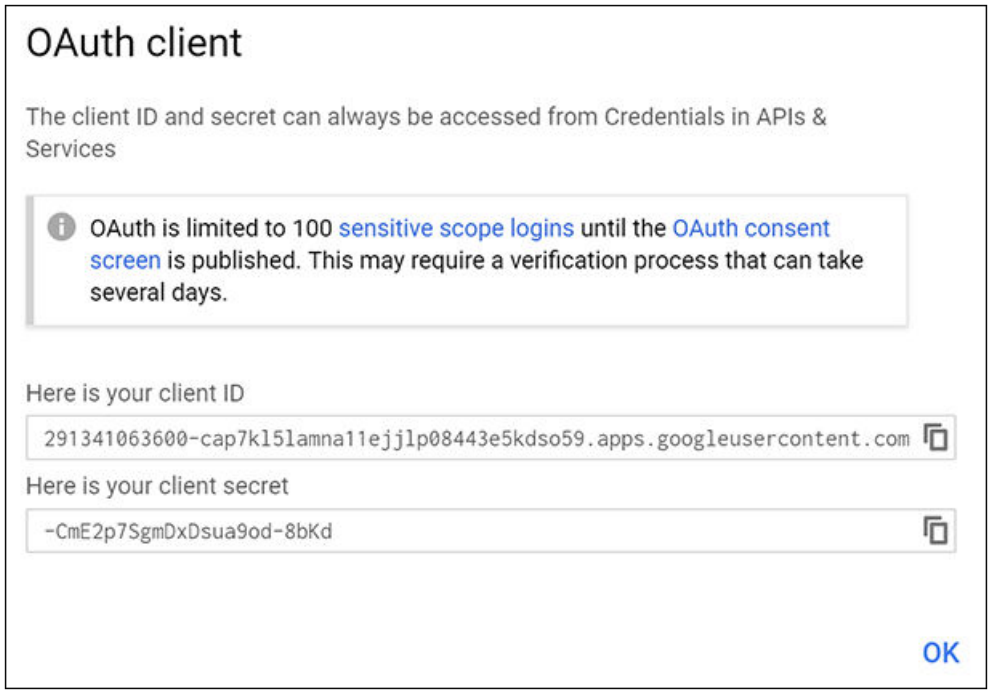
1. Go to https://console.developers.google.com.
2. Sign in to your Google account.
3. Create and name your API web-application project.
4. During creation of your application, you may see a field called "Authorized Javascript origins." Leave this field blank.
5. When you get to the "Authorized redirect 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 4 Client ID and Client Secret for Google Application



Setting Up Cloudpath for Google Authentication

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 to Configure Cloudpath for Google

- Google application Client ID
- Google application Client Secret

How to Add Google Authentication to the Workflow

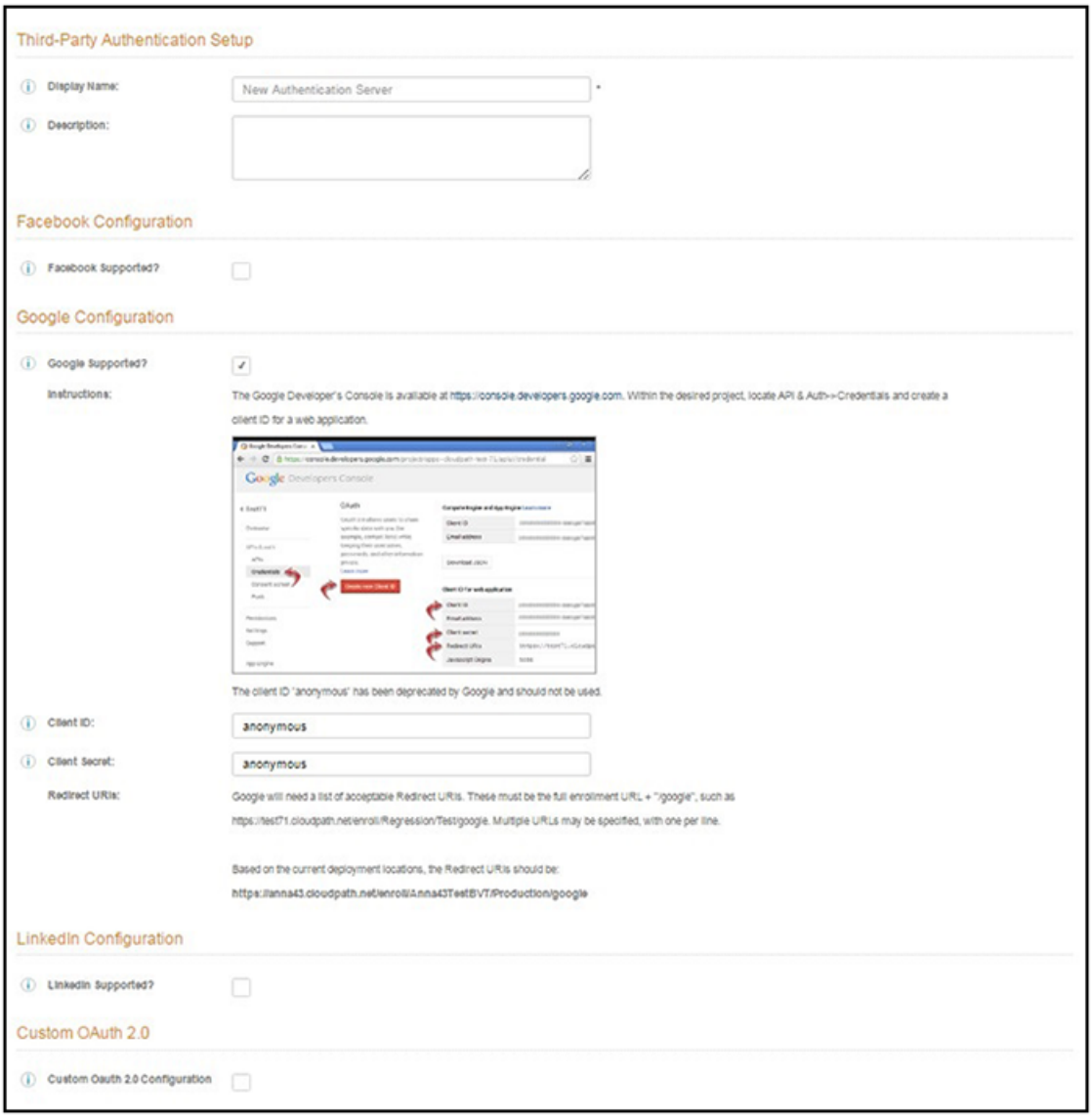
1. Create an enrollment workflow for third-party authentication.
2. Add an enrollment step that prompts the user to authenticate through a third-party source.

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 5 Google Third-Party Authentication Setup

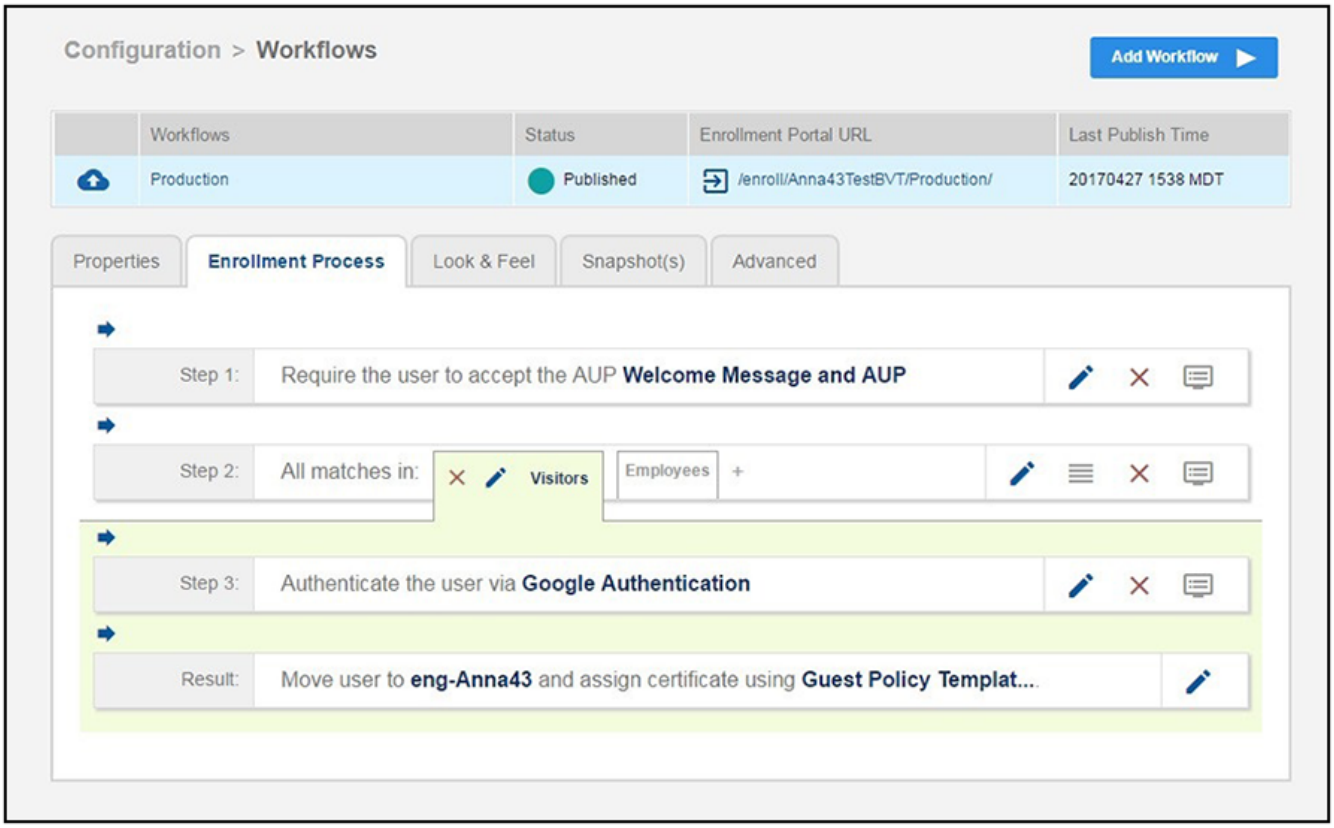


5. In the Google Configuration section, check the **Google Supported?** box.
6. Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.
7. Enter the **Client ID** and **Client Secret** from the Google application.

   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.

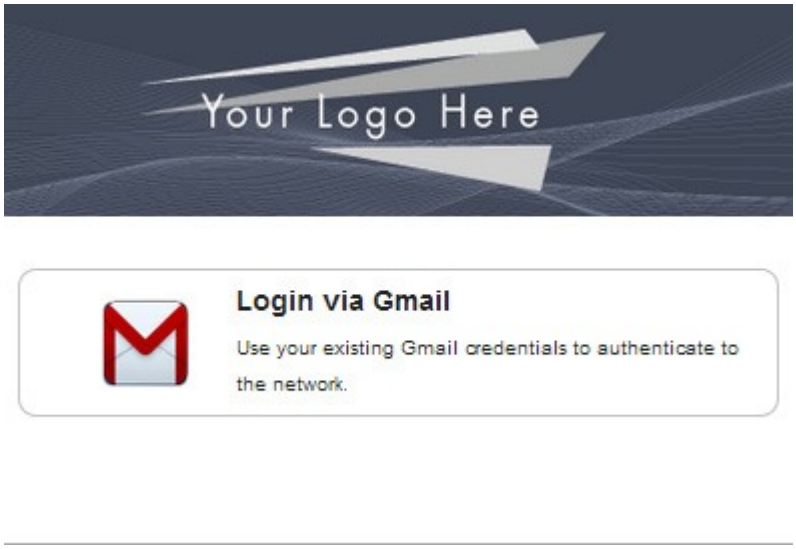
FIGURE 6 Cloudpath Workflow



User Experience for Google Authentication

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

FIGURE 7 **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.

Using LinkedIn for Third-Party Authentication

- Setting Up the LinkedIn Application....17
- Setting Up Cloudpath for LinkedIn Authentication....20

Setting Up the LinkedIn Application

Before configuring Cloudpath for LinkedIn authentication, you must set up the LinkedIn application.

What You Need To Set Up The LinkedIn Application

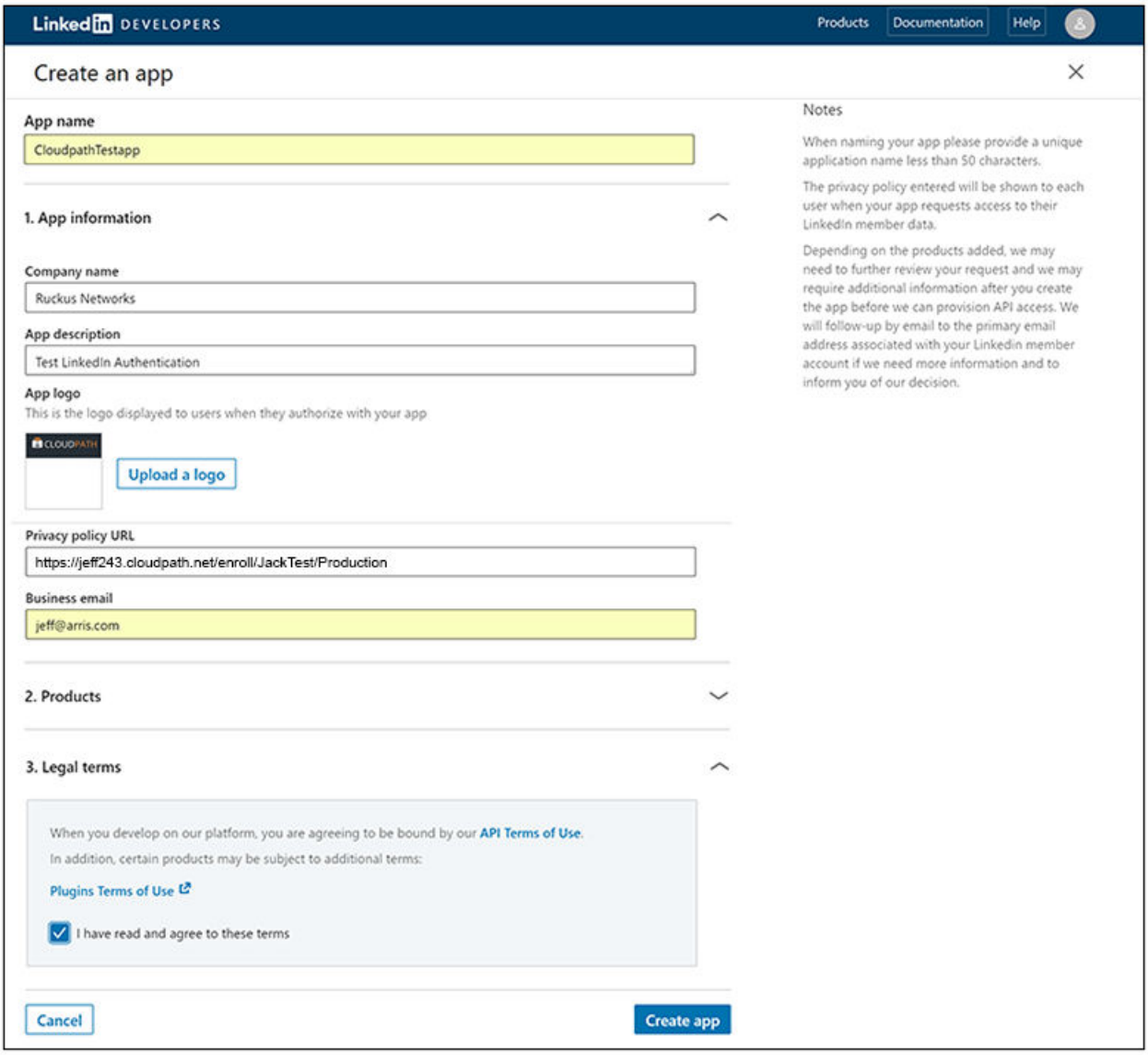
- LinkedIn login credentials
- Name and Description for your application
- Privacy policy URL for your company
- JavaScript API Domain

How to Set Up the LinkedIn App

1. Navigate to `http://developer.LinkedIn.com`.
2. Sign in to your LinkedIn account.
3. Click **Create app**.

4. The **Create an app** page displays.

FIGURE 8 Create an app Screen on LinkedIn Developers Site



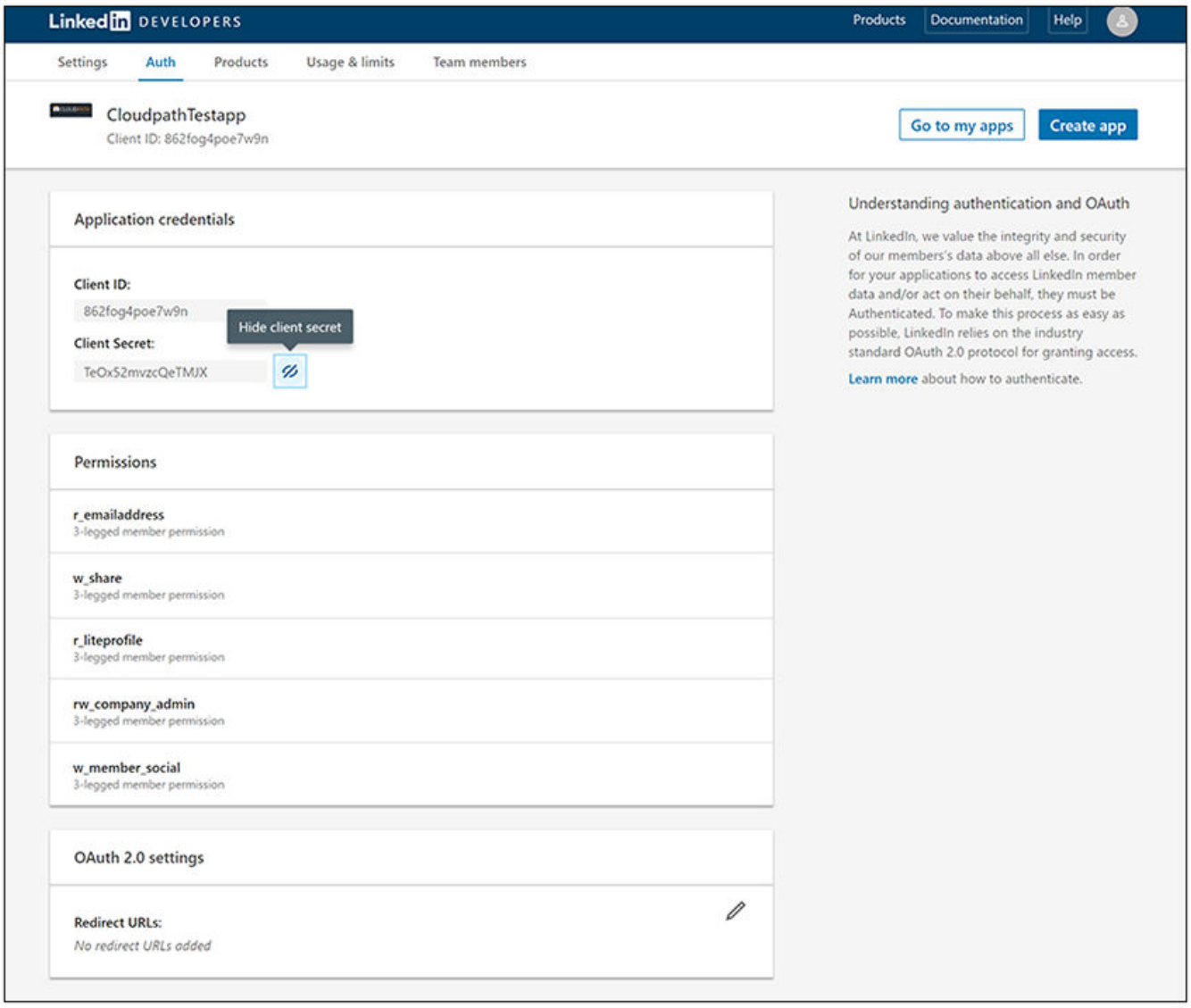
5. Enter the following information for your application:
   - App name (name of your application)
   - Company name
   - App description
   - Upload an application logo
   - Private policy URL (of your company)
   - Business Email

6. Agree to the **Terms of Service** and click **Create app**.

   The application is created, and you are returned to a screen that provides the information you just configured.

7. Click the **Auth** tab of your application screen. An example figure is shown below:

FIGURE 9 Auth Tab Settings of Newly Created Application



8. In the OAuth 2.0 settings section, use the pencil icon to enter the Redirect URLs.

   NOTE
   These must be acceptable Redirect URLs and must include the full enrollment URL + "/linkedin". An example is: `https://jeff243.cloudpath.net/enroll/JackTest/Production/linkedin`.
   You obtain the "Redirect URL" during workflow creation when you add a step to "Authenticate to a third party." For more information, refer to How to Add LinkedIn Authentication to the Workflow on page 20. (Figure 11 on page 21 shows the Redirect URL, which appears once you have checked the "LinkedIn Supported?" box when adding the third-party authentication step.)
   You can add multiple URLs.

   The following figure shows the Redirect URL section after adding a URL:

   FIGURE 10 Redirect URL Added to LinkedIn Configuration

9. Click **Update** to save configuration changes to your application.

Make a note of your **Client ID** and **Client Secret**. You need this information to set up the LinkedIn authentication within Cloudpath.

Setting Up Cloudpath for LinkedIn Authentication

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

What You Need to Configure Cloudpath for LinkedIn

- LinkedIn application Client ID (API Key in previous versions)
- LinkedIn application Client Secret (Secret Key in previous versions)

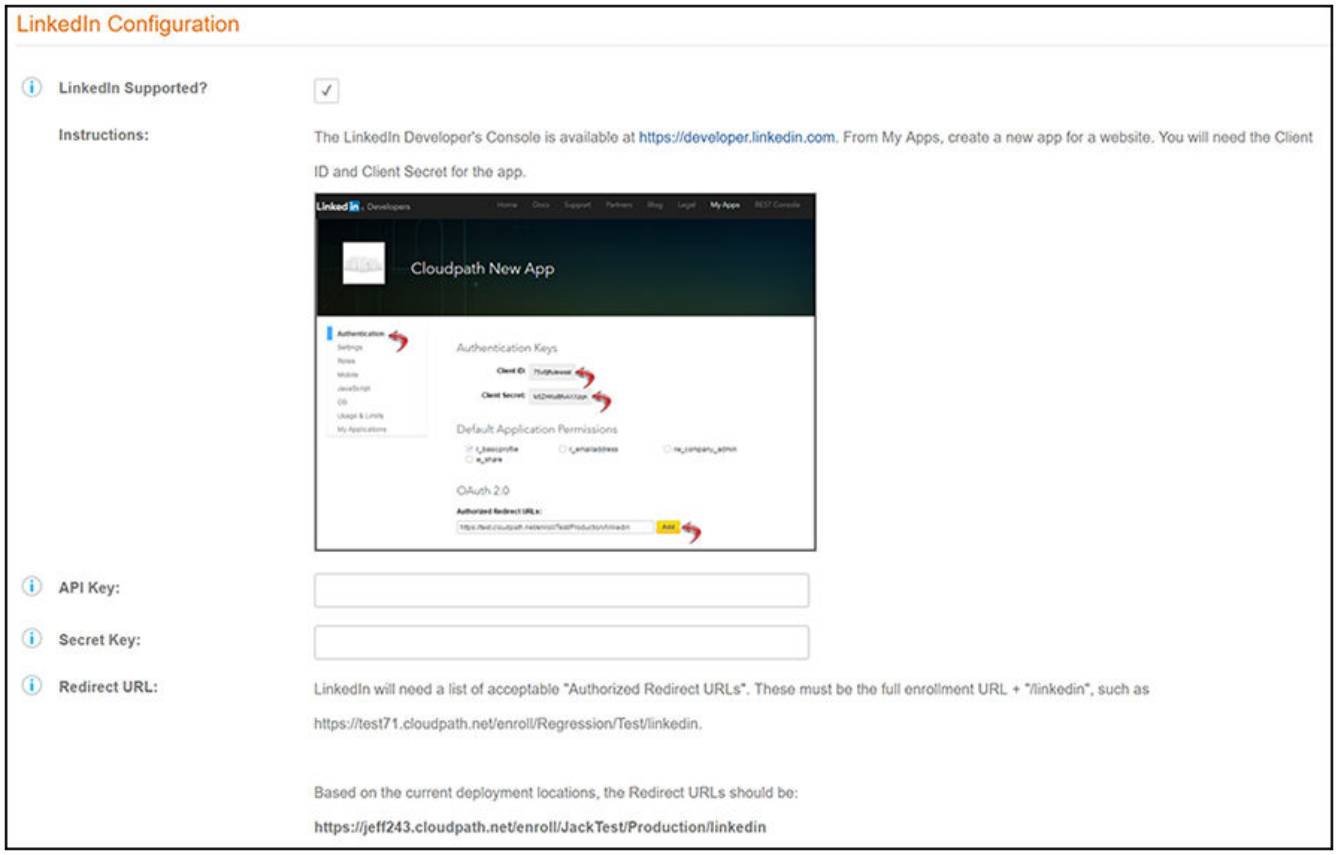
How to Add LinkedIn Authentication to the Workflow

You can add a step to the enrollment workflow to authenticate a user by using the LinkedIn application.

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. 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.
3. Place the authentication step after the **User Type** option.

4. Enter the **Name** and **Description** of this configuration.
5. Scroll down to the **LinkedIn Configuration** section, and check the **LinkedIn Supported**? box.

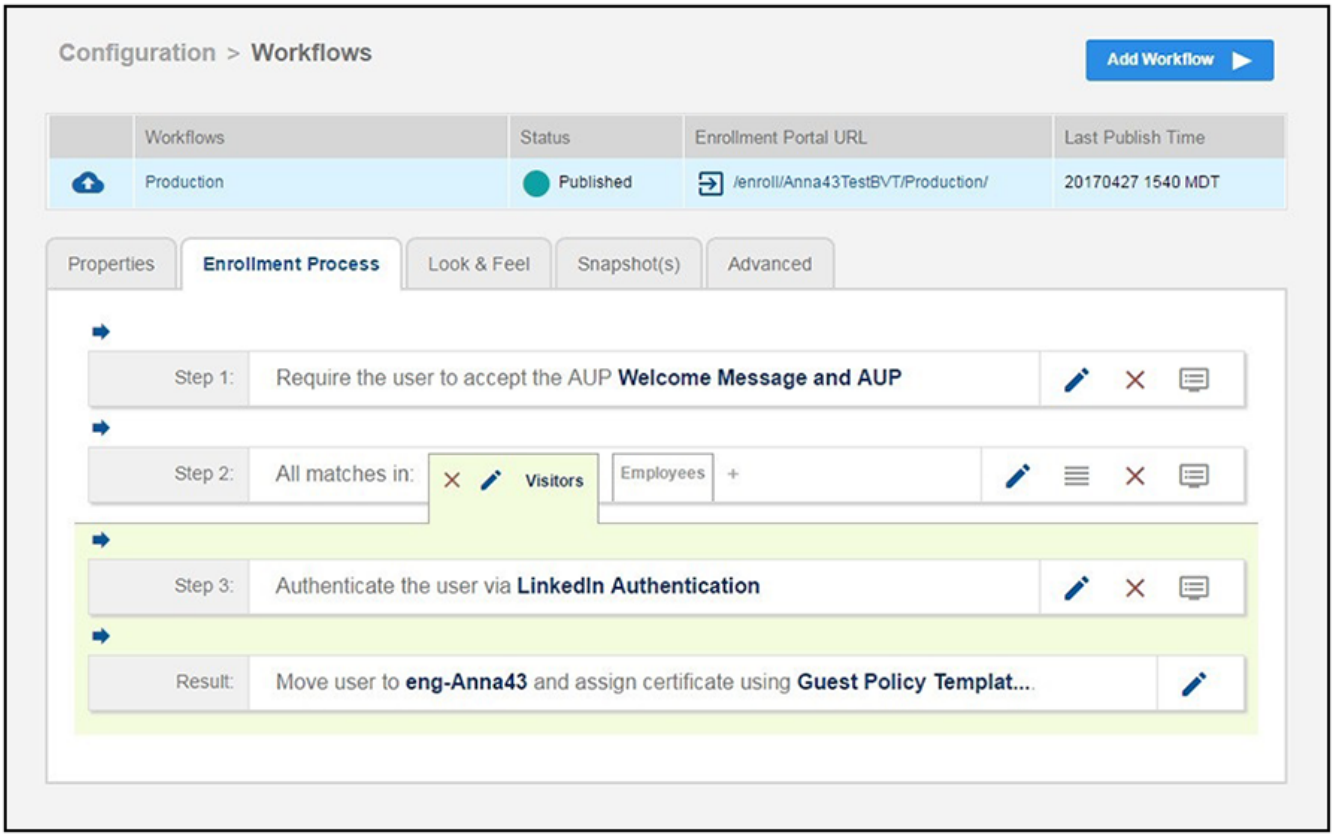
FIGURE 11 Cloudpath Third-Party Authentication Setup for LinkedIn



6. In the API Key field, enter the Client ID from the LinkedIn Auth Tab Settings of Newly Created Application screen (refer to Figure 9 on page 19).
7. In the Secret Key field, enter the Client Secret from the LinkedIn Auth Tab Settings of Newly Created Application screen(refer to Figure 9 on page 19).

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

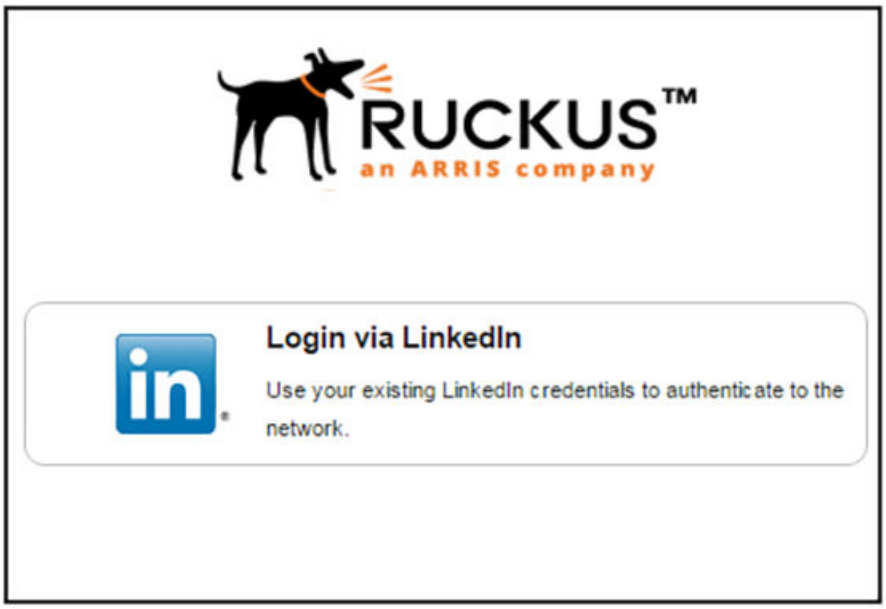
FIGURE 12 Cloudpath Workflow With LinkedIn Step Added



User Experience for LinkedIn Authentication

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

FIGURE 13 User Prompt for LinkedIn Authentication



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

© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com