CONFIGURATION GUIDE

Cloudpath Enrollment System Third-Party Authentication Configuration Guide, 6.0

Supporting Cloudpath Software Release 6.0

Part Number: 800-73661-001 Rev A
Publication Date: 26 August 2024

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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Using Facebook for Third-Party Authentication

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

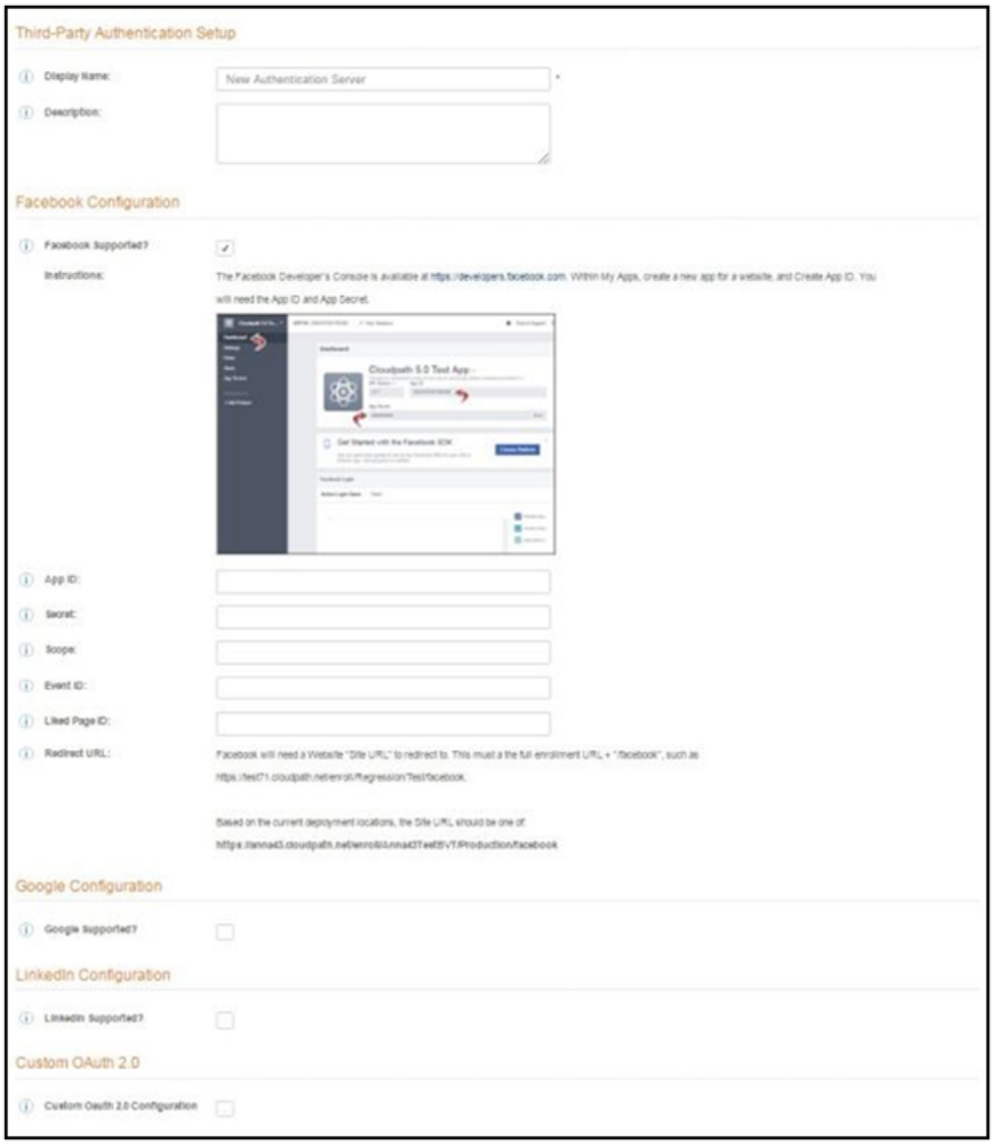
- Facebook App ID
- Facebook App Secret
- (Optional) Scope parameters, Event ID, and Liked Page ID for your Facebook application

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

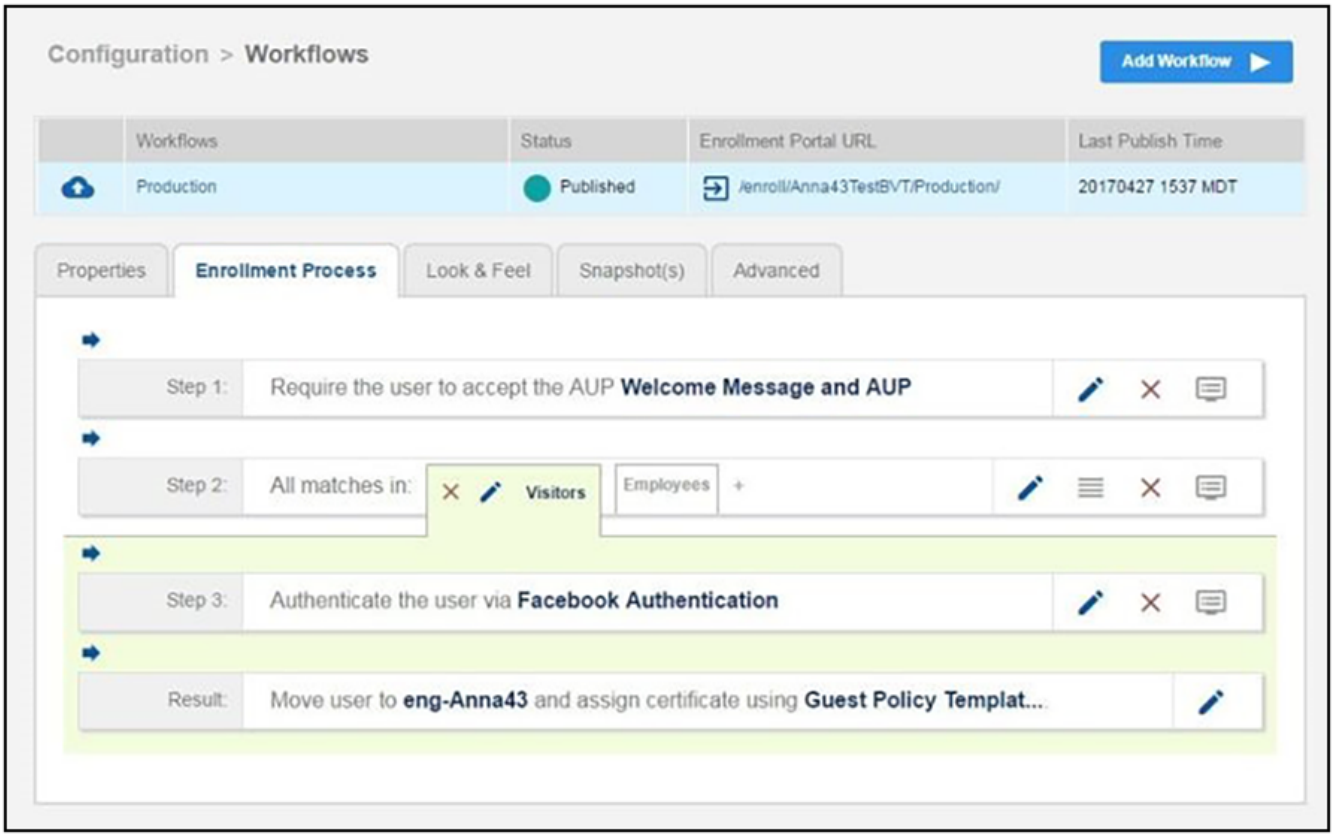


5. In the Facebook Configuration section, check the **Facebook Supported?** box and complete the following fields:
   - **App ID** - The **App ID** from the Facebook application you just created.
   - **Secret** - The **App Secret** from the Facebook application you just created.
   - Optional settings:
     - **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 LinkedIn for Third-Party Authentication

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

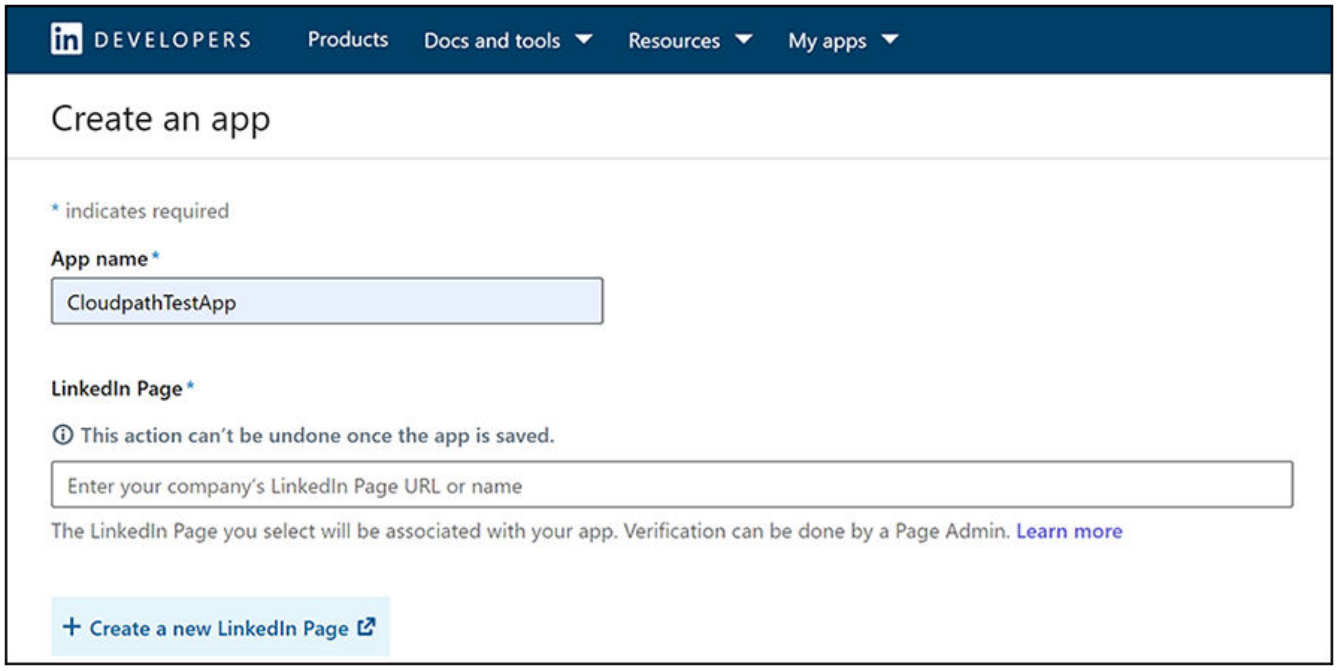
- LinkedIn login credentials
- Name and Description for your application
- Verification of company URL with your application. This is required to create Oauth 2.0 "scopes," which define what your application can do on a user's behalf. This process is described in How to Set Up the LinkedIn App on page 9.
- 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**.

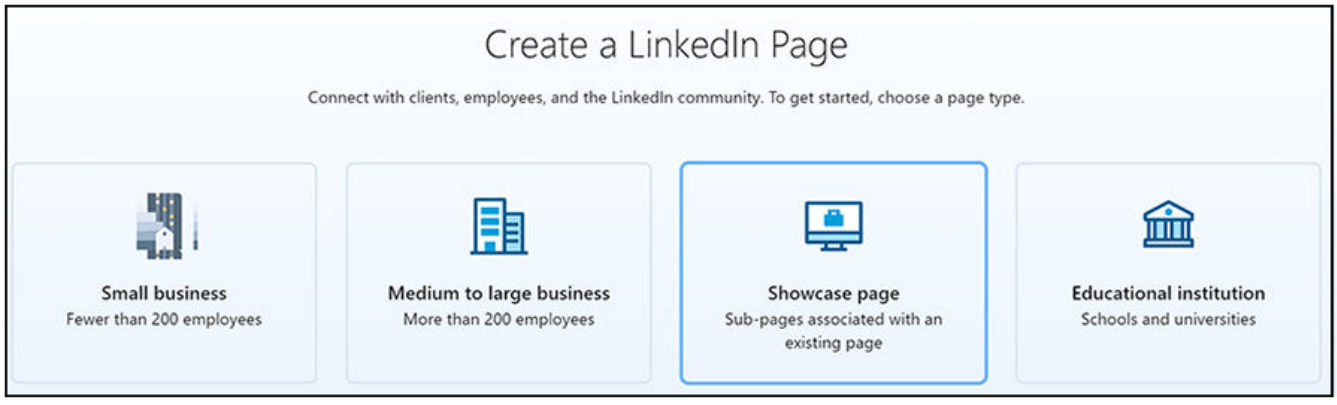
4. The **Create an app** page displays. The top part of that page is shown below:

   FIGURE 4 "Create an app" Screen on LinkedIn Developers Site



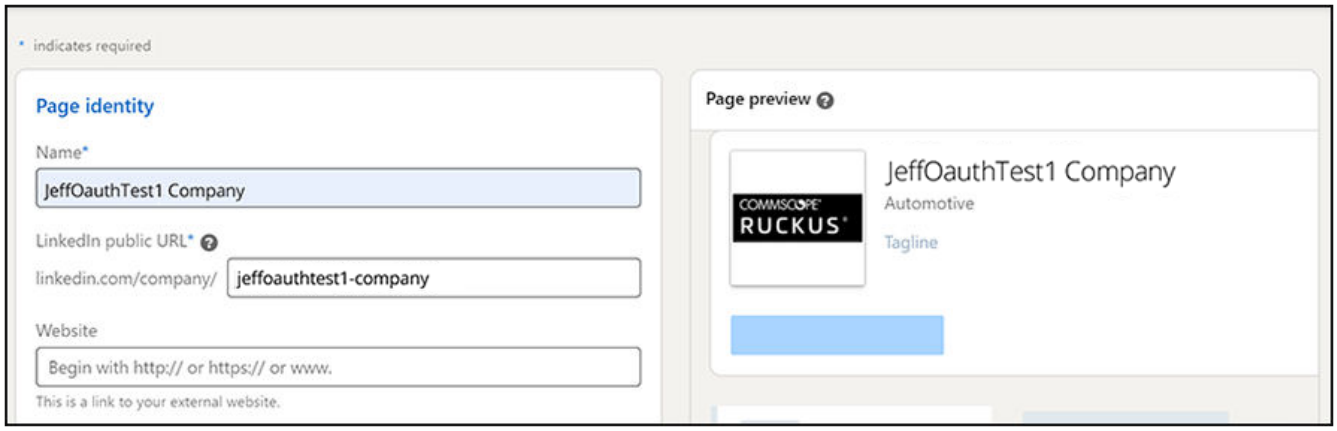
5. Enter the name of your application, then click **+ Create a new LinkedIn Page** to enter information about your company. The following screen is displayed.

   FIGURE 5 Creating a LinkedIn Page for Your Company



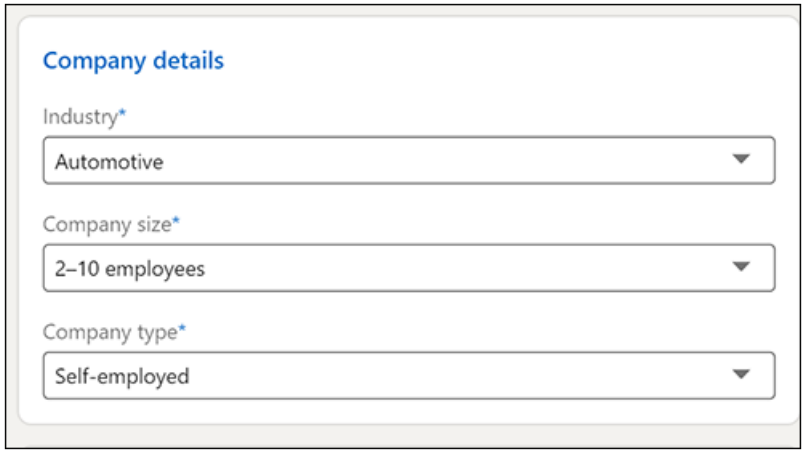
6. Click on the applicable button for your business; the example below shows the screens for a "Small business."

FIGURE 6 Identity Information for Your Company: Top Portion of Screen



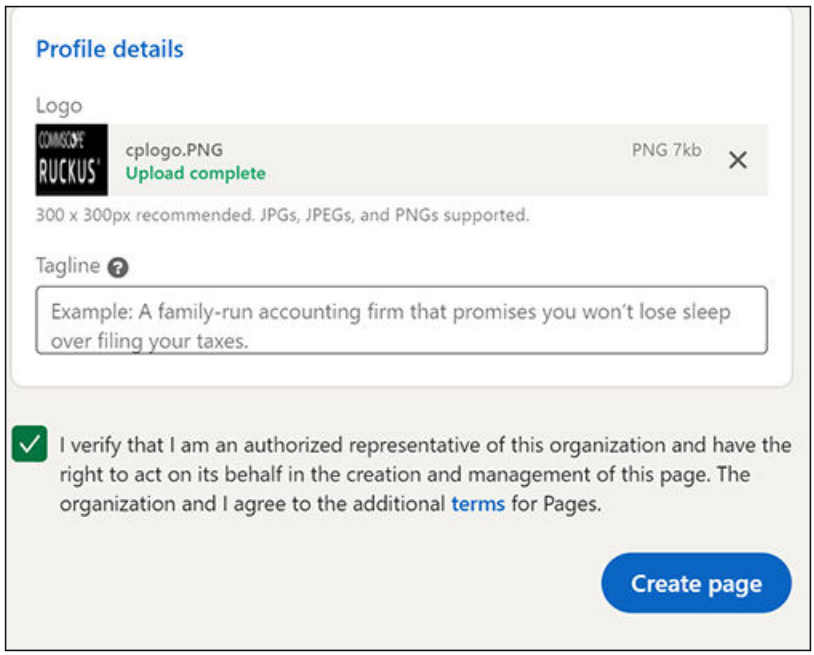
- Name: Enter the name of your company.
- LinkedIn public URL: This field will be generated based on what you enter in the "Name" field.
- Website: This field is optional.

FIGURE 7 Identity Information for Your Company: Middle Portion of Screen



Select the appicable options from the drop-down lists.

FIGURE 8 Identity Information for Your Company: Bottom Portion of Screen

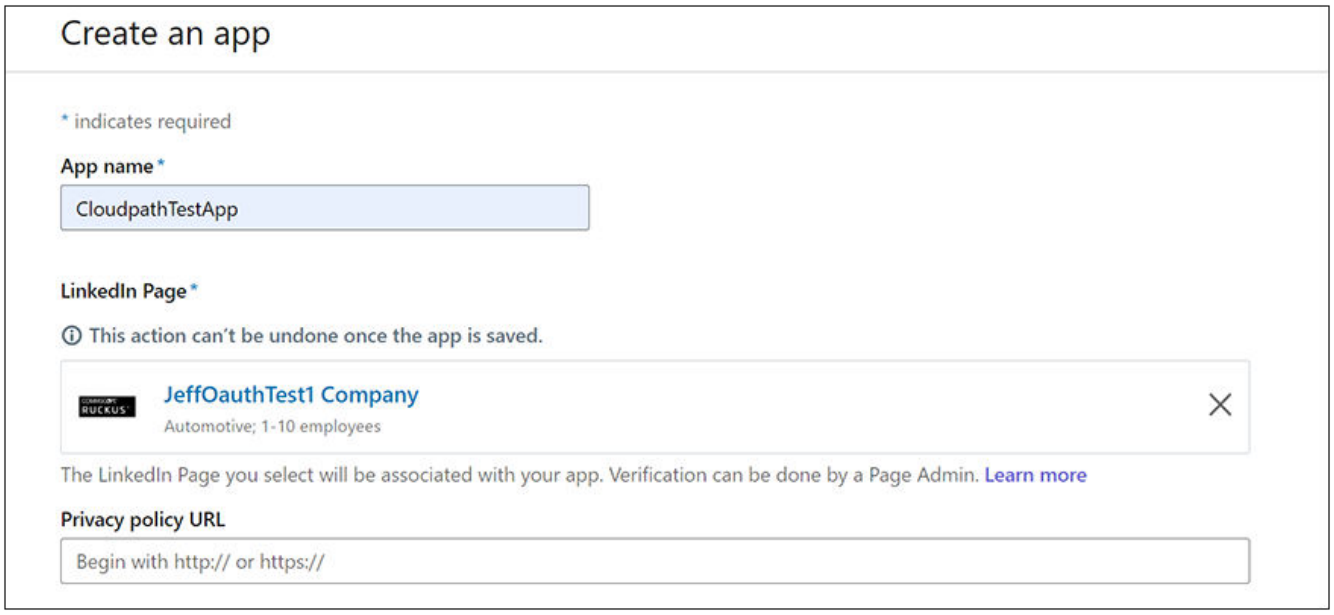


- Logo: Upload a logo if desired.
- Tagline: Enter a tagline if desired.
- Verification checkbox: Read and check this box in order to proceed.

Click **Create page**.

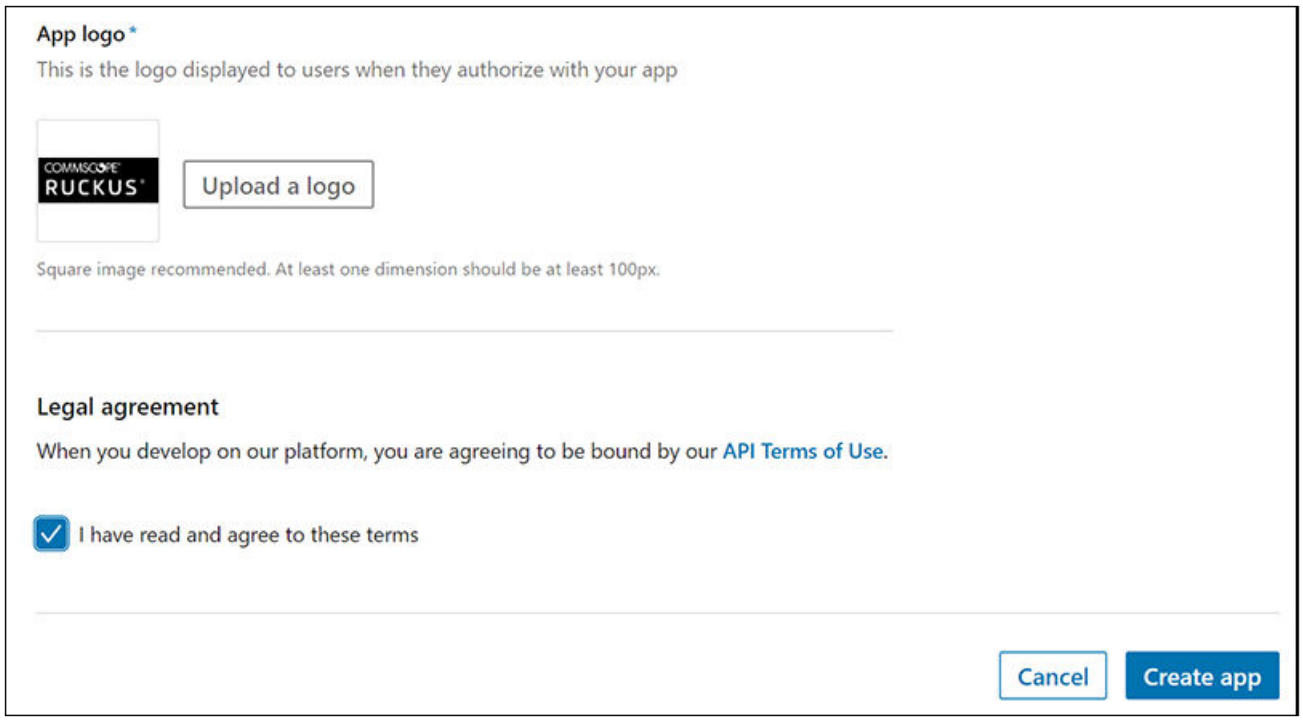
7. Click on the tab in your browser that has the original "Create an app" page that you already started.

FIGURE 9 Returning to "Create an App" Page: Top Portion of Screen



- App name: The name of the application you created is displayed.
- LinkedIn Page: Start typing the name of your application, then select it.
- Privacy policy URL: Optional field.

FIGURE 10 Returning to "Create an App" Page: Bottom Portion of Screen



Upload your logo, check the legal agreement, then click **Create app**.

The application is created, and you are returned to a screen that provides the information you just configured. The screen that is displayed is shown below in two parts:

FIGURE 11 Application Created: Top Portion of Screen

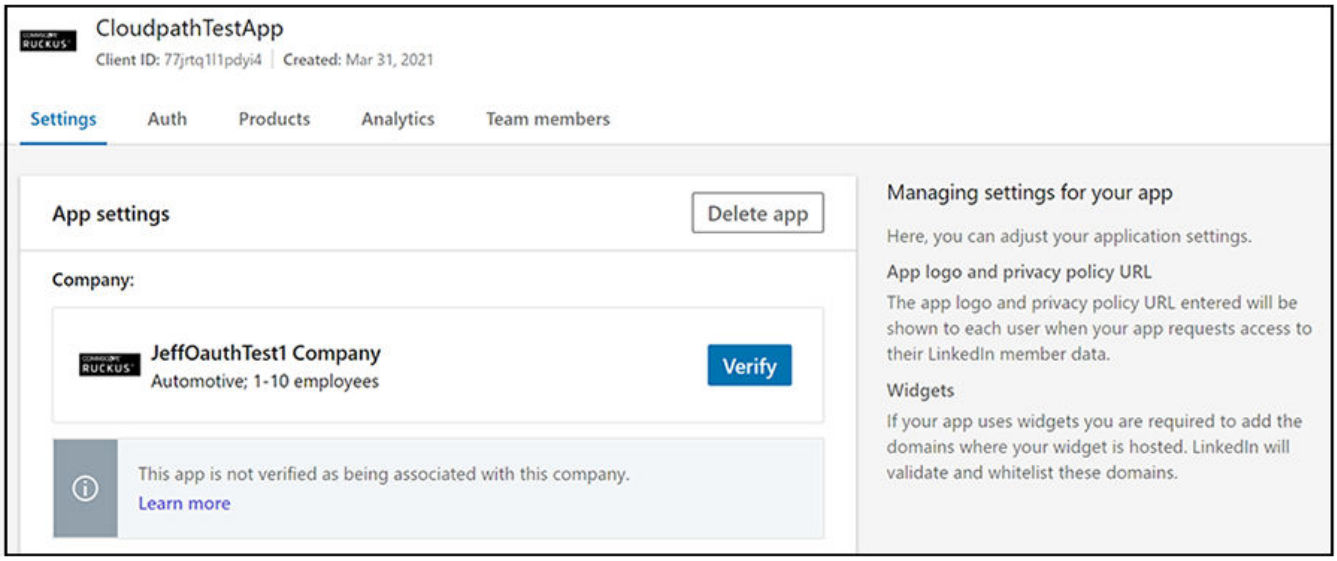
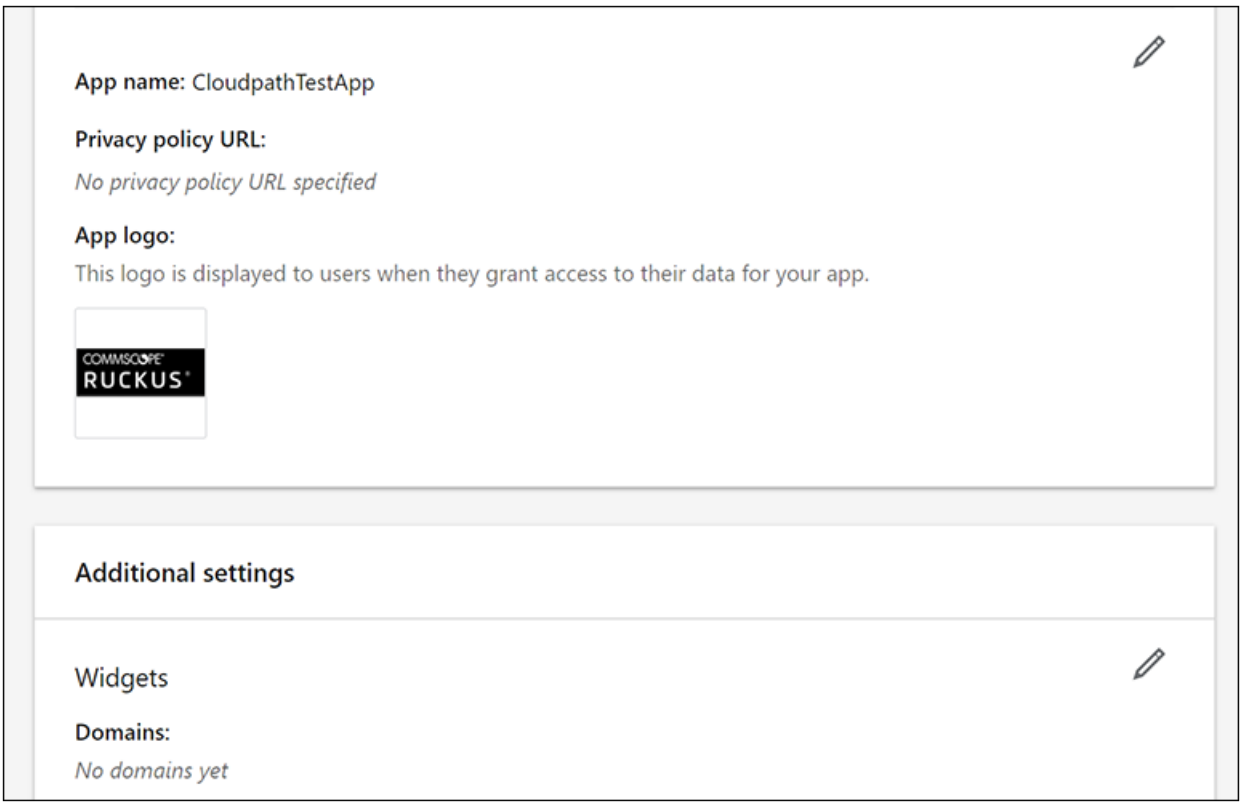
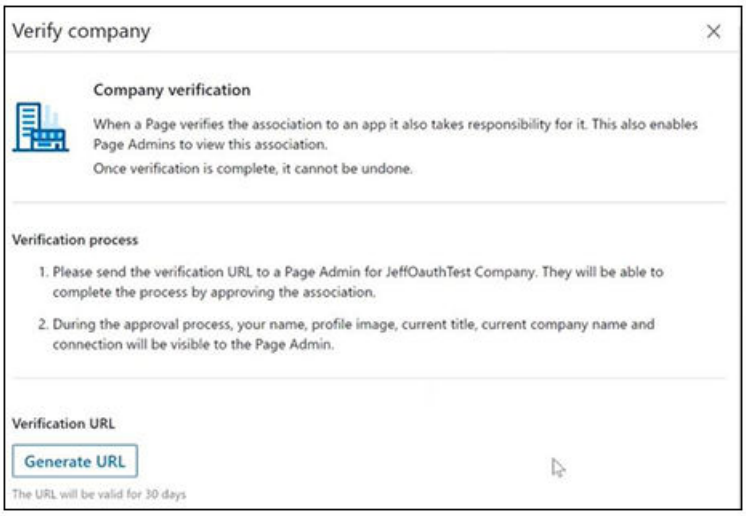


FIGURE 12 Application Created: Bottom Portion of Screen



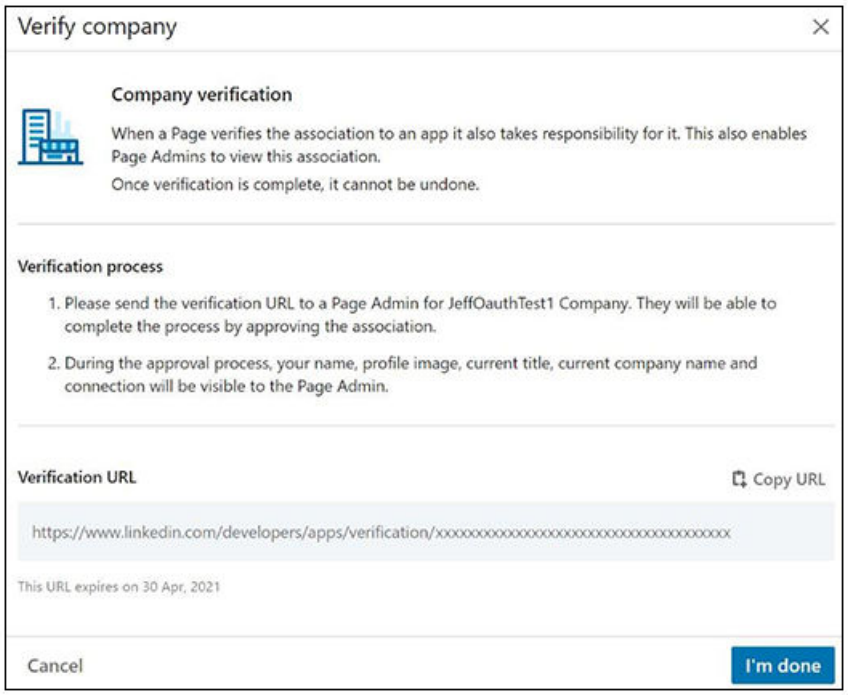
8. To verify your company with your application, click the **Verify** button (see Figure 11). The following screen is displayed.

FIGURE 13 Verifying Your Company



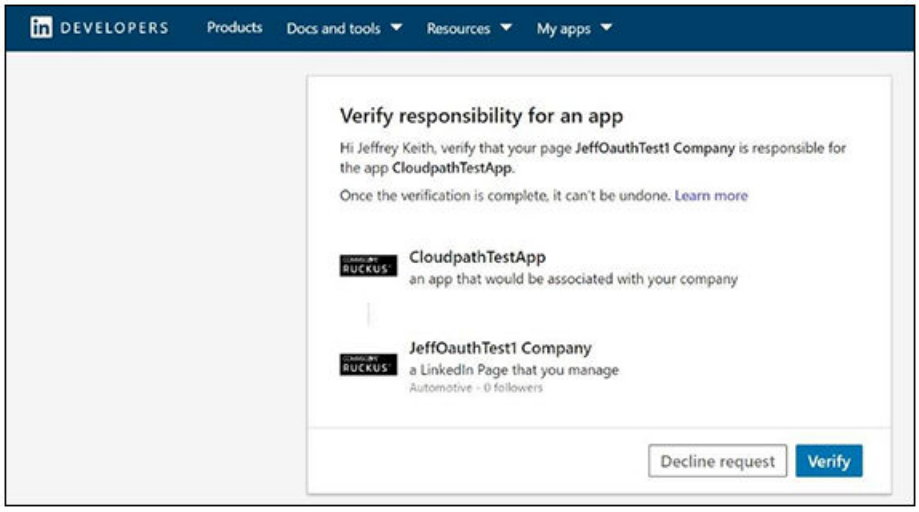
9. Click the **Generate URL** button. The URL is generated, as shown in the following screen.

   FIGURE 14 Using the Verification URL



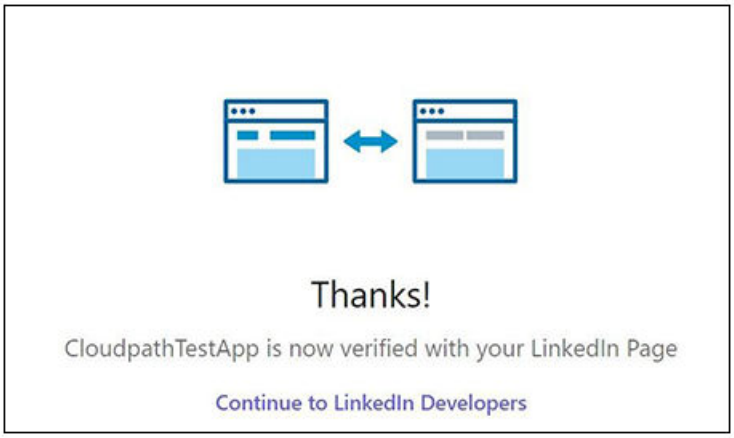
10. Copy the URL (and click **I'm done**.)
11. Paste the URL into a new tab on your browser (and click on the highlighted link as you paste it into the browser). You will receive the following screen, which shows the example company "JeffOauthTest1 Company" created earlier.

    FIGURE 15 Pasting the URL Into a Browser to Verify the Company



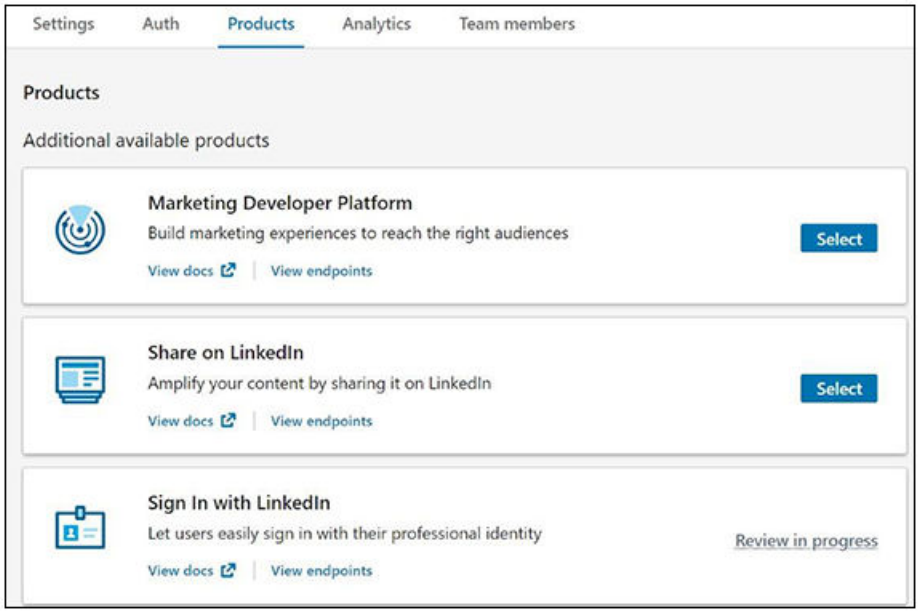
12. Click **Verify**. A successful verifcation will yield the following screen.

FIGURE 16 Verification Successful



13. From the Developer's page, click on the **Products** tab, then sign in with LinkedIn.

FIGURE 17 Signing in With LinkedIn from the Products Tab of Developer's Page



NOTE

You can refresh the page after a few minutes to check if the review has completed. You will also receive an email notification once you application has been verified as being associated with your company. Once verification is successful, the "Sign in with Linked In" step adds the "r_emailaddress" and "r_liteprofile" scopes to the OAuth 2.0 scopes (as shown in Figure 20). These scopes allow the Oauth integration to use the primary e-mail address associated with the LinkedIn account as well as the person's name and photo. Without these scopes being successfully added, the Oauth integration fails.

14. On the Developer's page, go to the **Settings** tab, then scroll down to the "Widgets" area, use the pencil icon to add your domain, and click **Update**.

    FIGURE 18 Adding Your Domain to Widgets

15. Click the **Auth** tab of the Developer's screen. An example figure is shown below in two parts:

FIGURE 19 Auth Tab Settings of Newly Created Application - Top Part of Screen

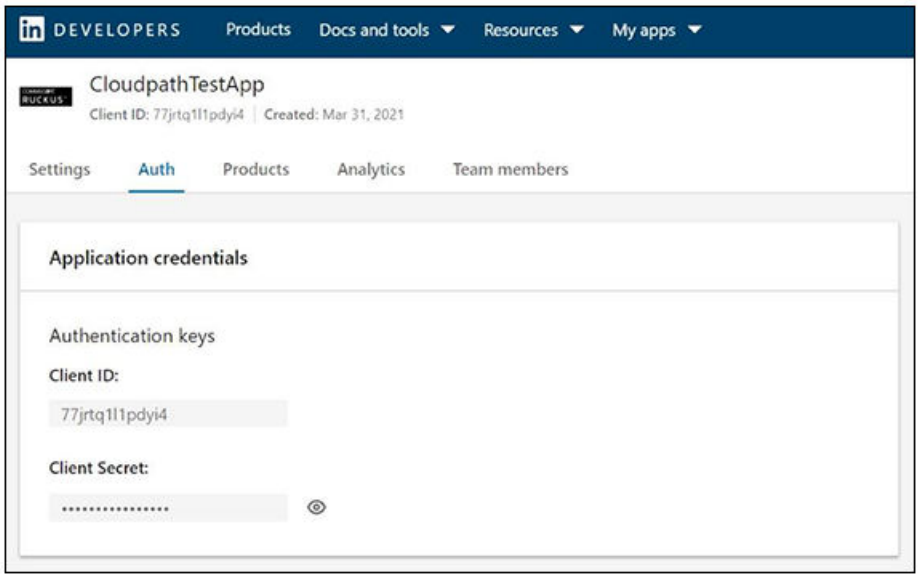
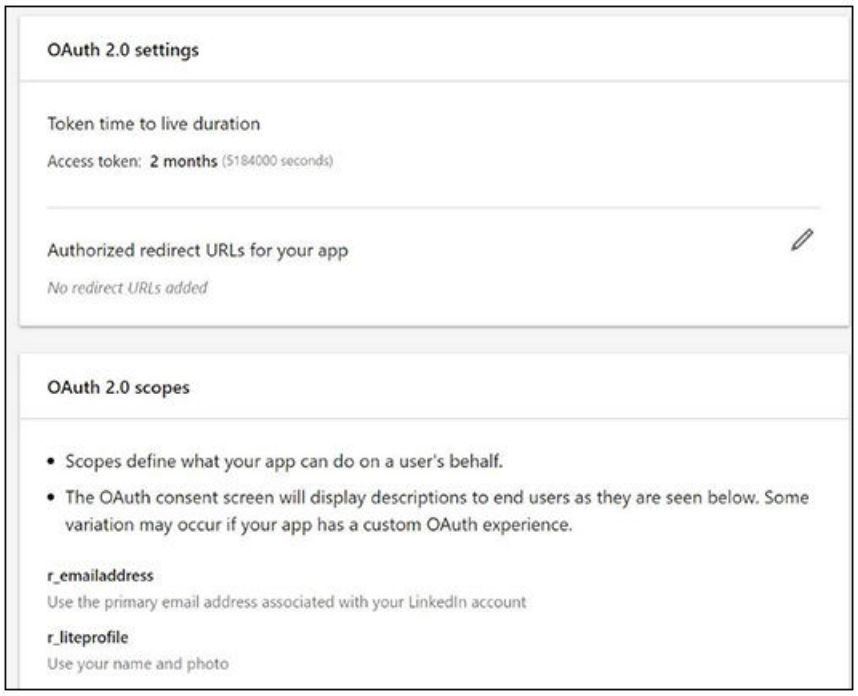


FIGURE 20 Auth Tab Settings of Newly Created Application - Bottom Part of Screen



16. 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 22 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 21 Redirect URL Added to LinkedIn Configuration

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

Make a note of your **Client ID** and **Client Secret** from Figure 19. 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)

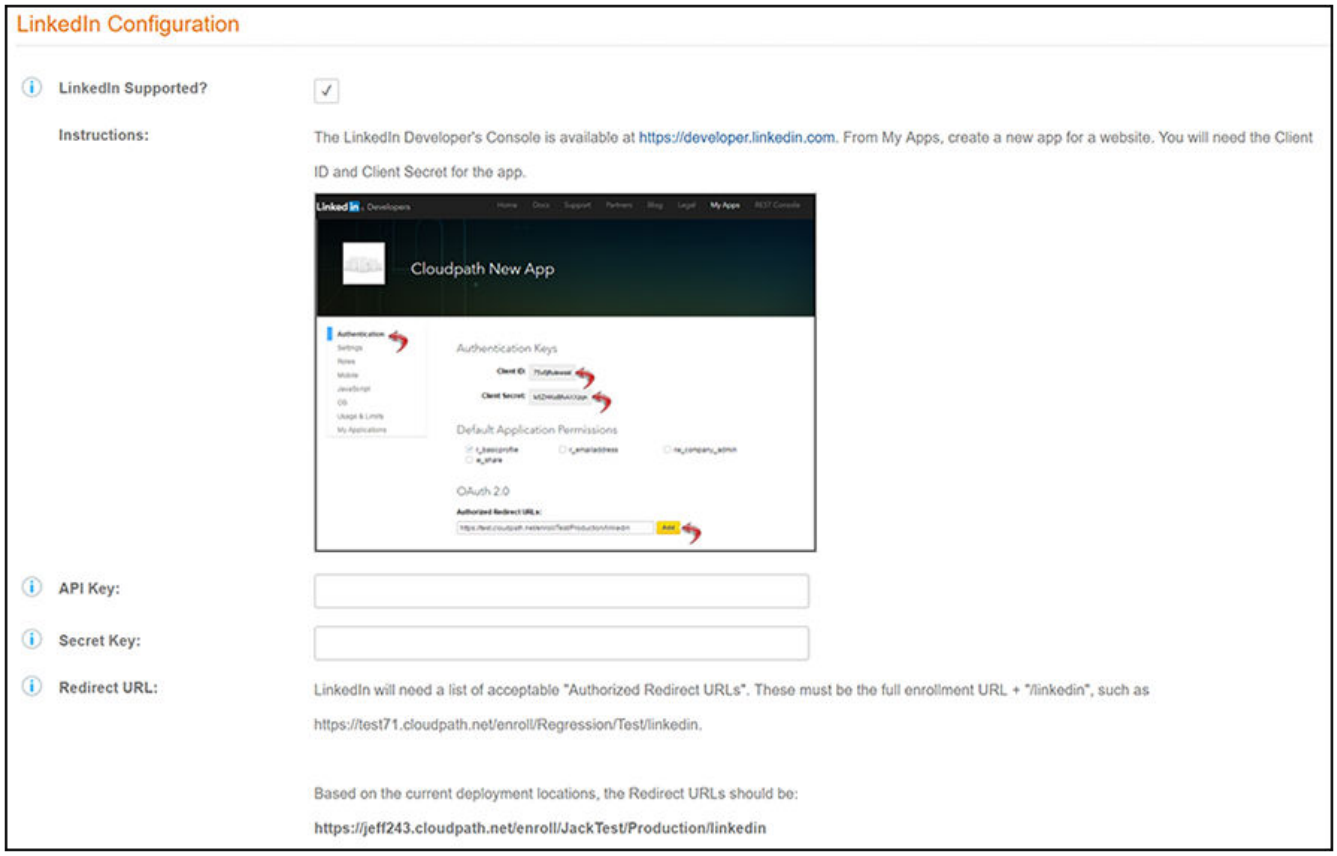
How to Add LinkedIn Authentication to the Workflow

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.

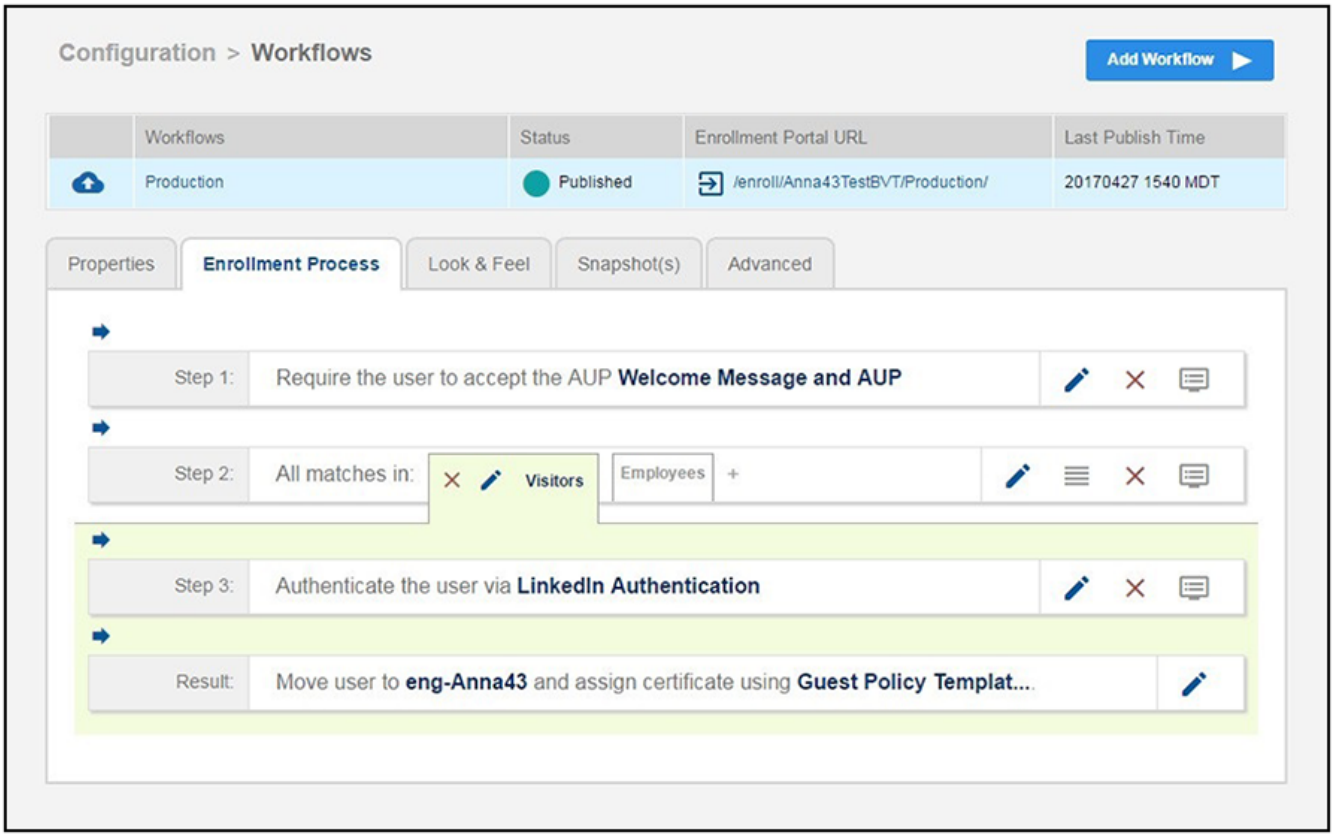
FIGURE 22 Cloudpath Third-Party Authentication Setup for LinkedIn



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

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

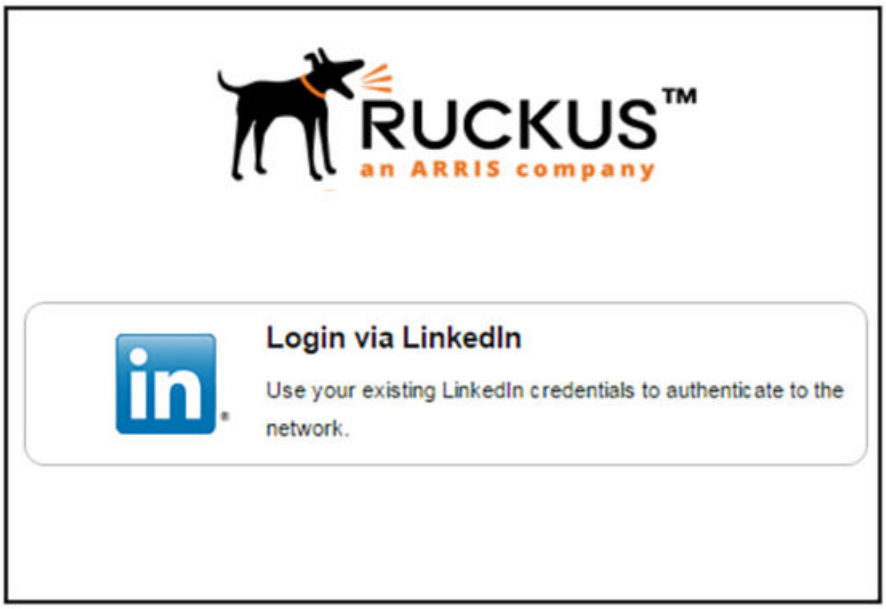
FIGURE 23 Cloudpath Workflow With LinkedIn Step Added



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 24 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.

Using Google for Third-Party Authentication

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.

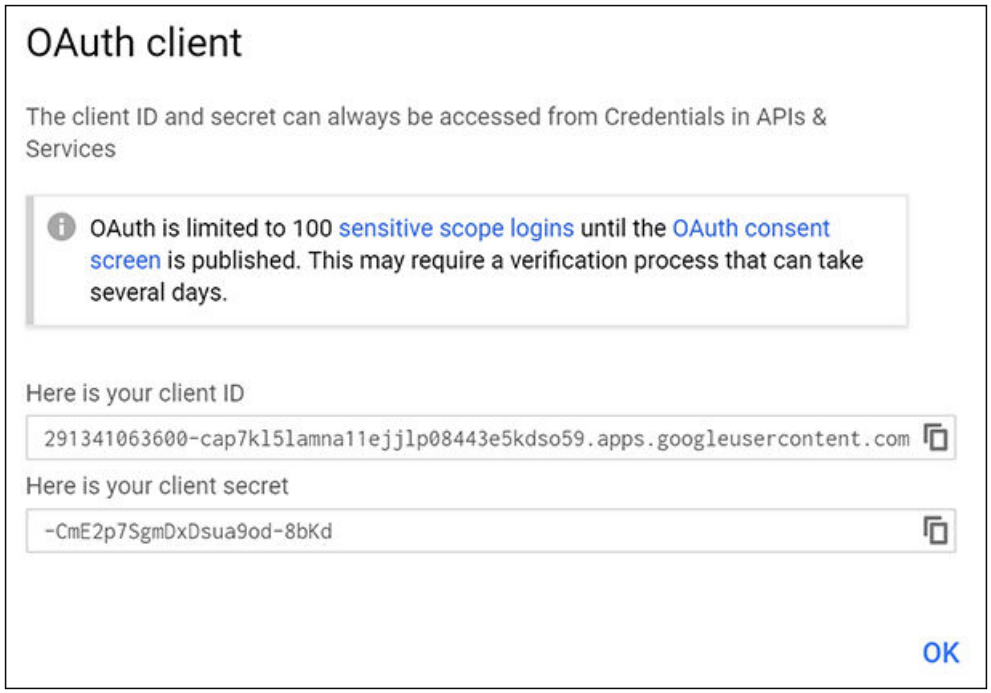
1. Go to https://console.developers.google.com.
2. Sign in to your Google account.
3. Create and name your API web-application project.
4. During creation of your application, you may see a field called "Authorized Javascript origins." Leave this field blank.
5. When you get to the "Authorized redirect 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 25 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

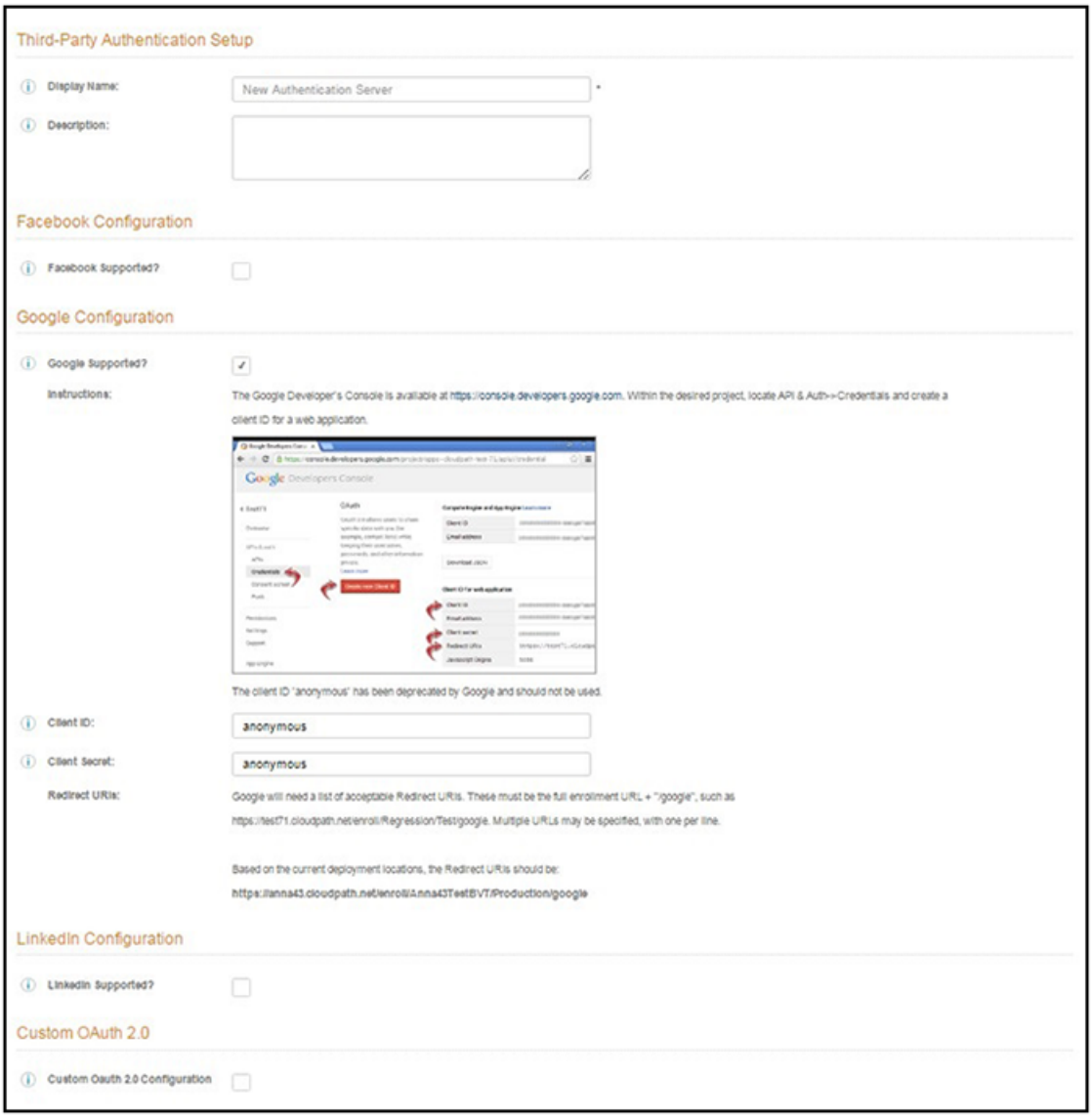
1. Create an enrollment workflow for third-party authentication.
2. Add an enrollment step that prompts the user to authenticate through a third-party source.

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 26 Google Third-Party Authentication Setup

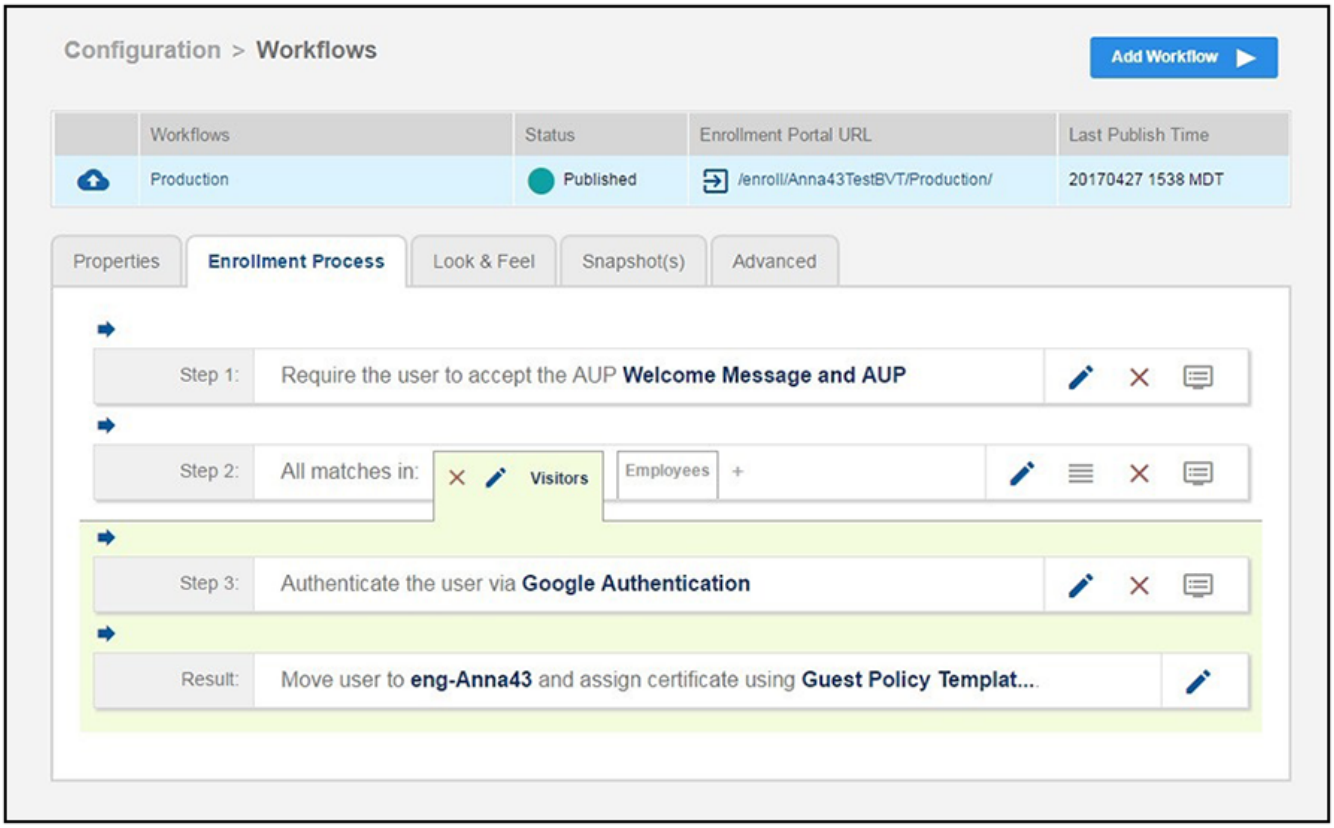


5. In the Google Configuration section, check the **Google Supported?** box.
6. Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.
7. Enter the **Client ID** and **Client Secret** from the Google application.

   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.

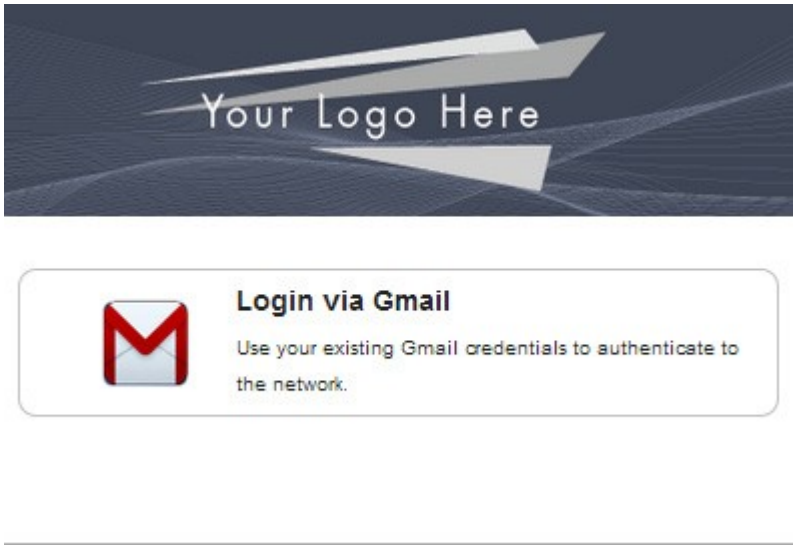
FIGURE 27 Cloudpath Workflow



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 28 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 Google LDAP Client as an Authentication Server

If you use G Suite to manage your users with Google Directory, you can use Google LDAP as an authentication server for onboarding users to your Cloudpath Enrollment System.

Prerequisites

Before you begin any configuration on the Cloudpath UI, be sure you have the following:

- Google LDAP client with access permissions as follows:
  - Specify the LDAP client access level for verifying user credentials. When a user tries to sign in to the application, this setting specifies which organizational units the LDAP client can access to verify a user's credentials. Users who not part of one of the selected organizational units cannot sign in to the application.
  - Specify the LDAP client access level for reading user information. This setting specifies the organizational units that the LDAP client can access to retrieve additional user information.
  - Specify whether the LDAP client can read group information. This setting specifies whether the LDAP client can read group details and check a user's group memberships for purposes such as a user's role in the application.
- Google LDAP client certificate zip file (which contains both the public and private keys). The certificate is used for encryption by the LDAP service provider.
- (Optional) Access credentials from Google LDAP client: If you will require Cloudpath to use the "Binding Username" and "Binding Password" fields (Figure 29) in addition to the certificate to connect to the secure LDAP service you must generate access credentials.

  NOTE
  Refer to your G Suite LDAP documentation for information about setting up Google LDAP clients.

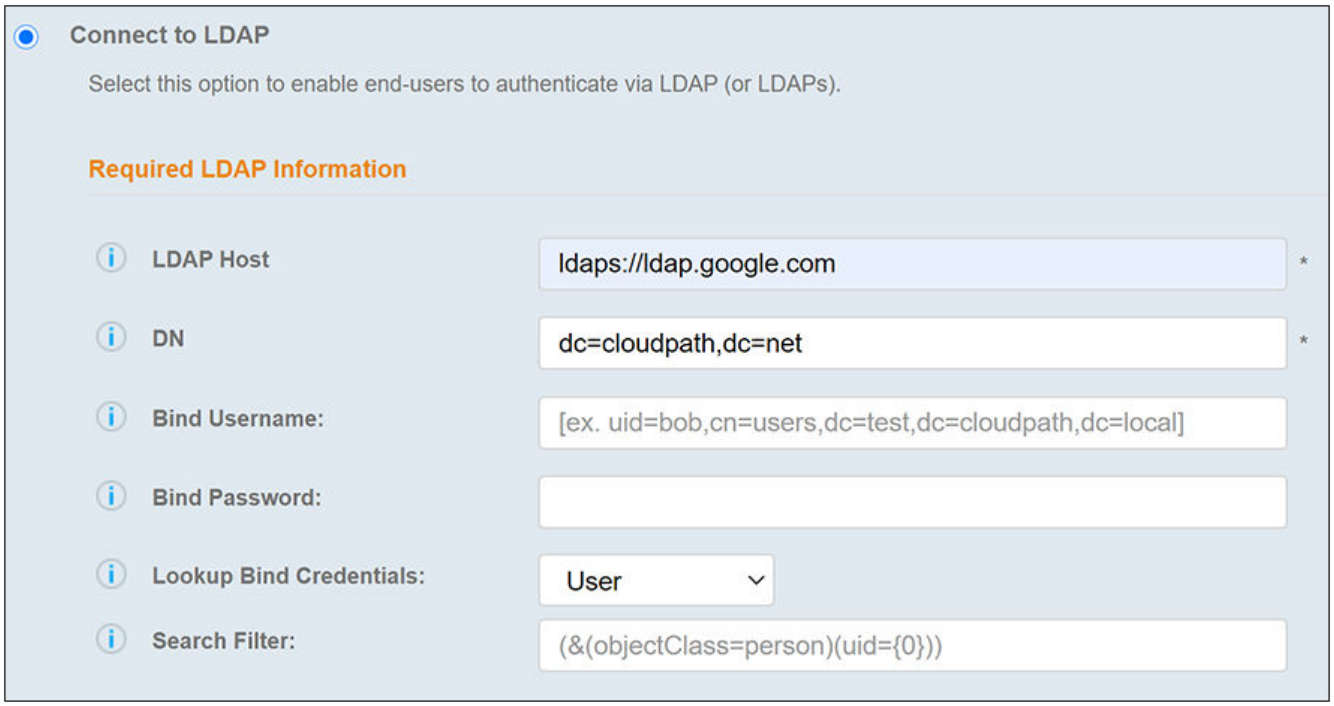
Configuration Steps

Follow these steps to configure the Google LDAP authentication server in the Cloudpath UI:

NOTE
Because access credentials are optional, the configuration steps below do not include using the applicable fields: Binding Username, Binding Password, and Lookup Bind Credentials.

1. Go to **Configuration > Authentication Servers**, and click **Add Server**.
2. In the next screen, where you select the type of Authentication server, scroll down and select the " Connect to LDAP" button, then fill in the LDAP Host and DN fields as shown in the example below:

FIGURE 29 Connect to LDAP Selection



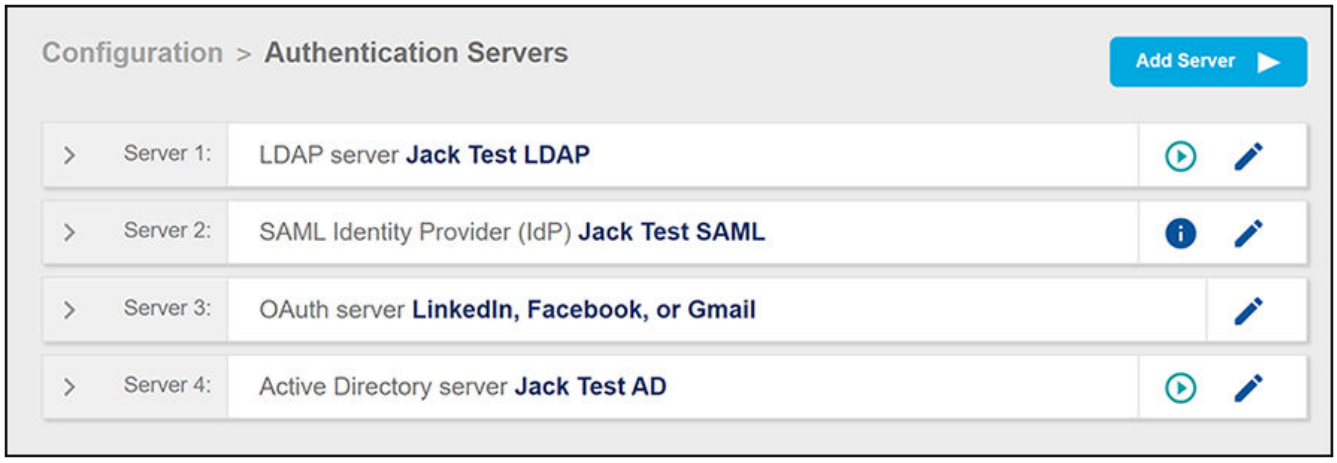
- Connect to LDAP: ldaps://ldap.google.com

  NOTE
  ldaps://ldap.google.com is always the LDAP host name for G Suite LDAP client

- DN: The distinguished name of the domain

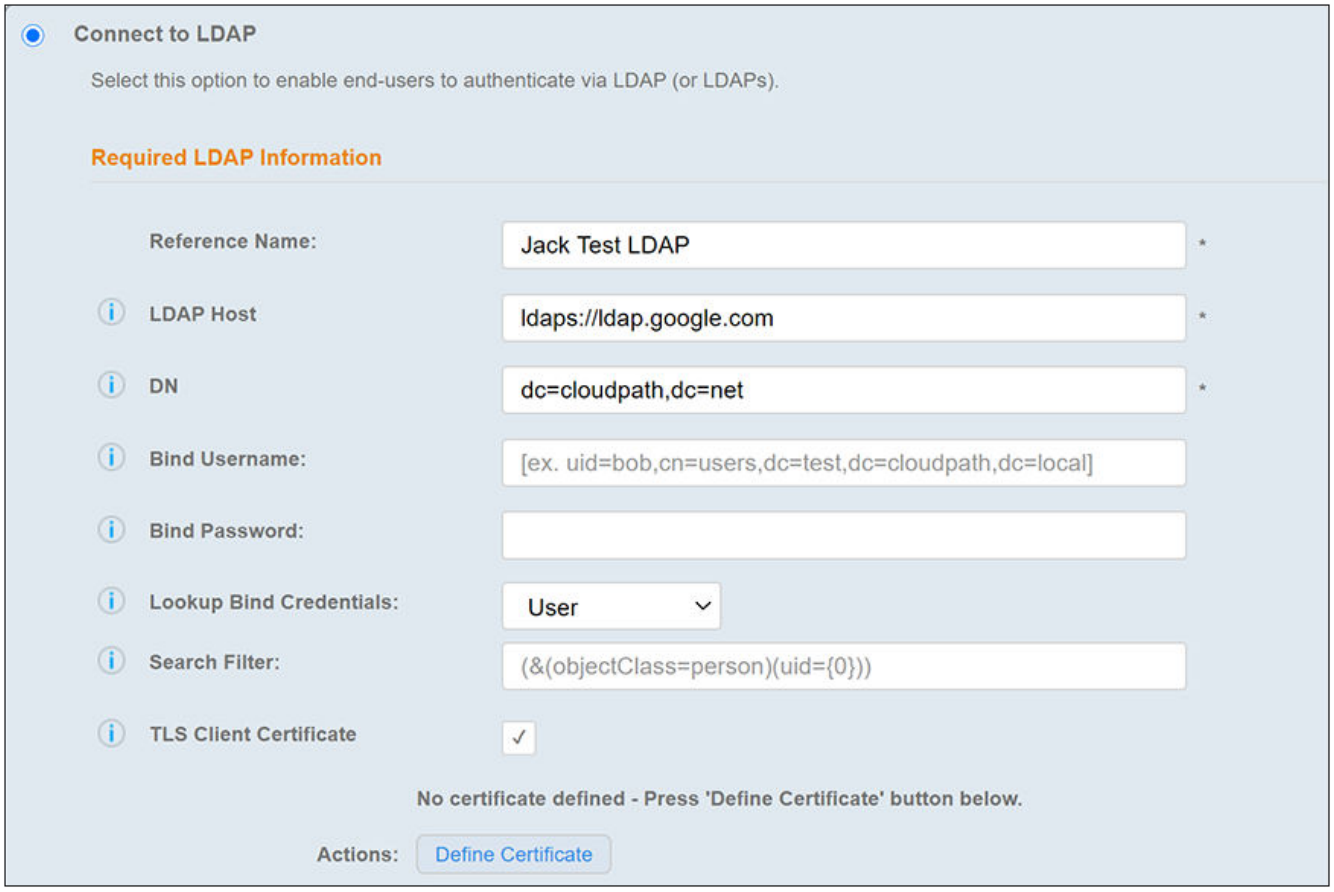
3. If you are not using binding, leave the Bind Username and Bind Password fields empty, then click **Save**. The new LDAP server ("Jack Test LDAP") is now added to the list of authorization servers, as shown in the example below:

FIGURE 30 LDAP Authentication Server Added



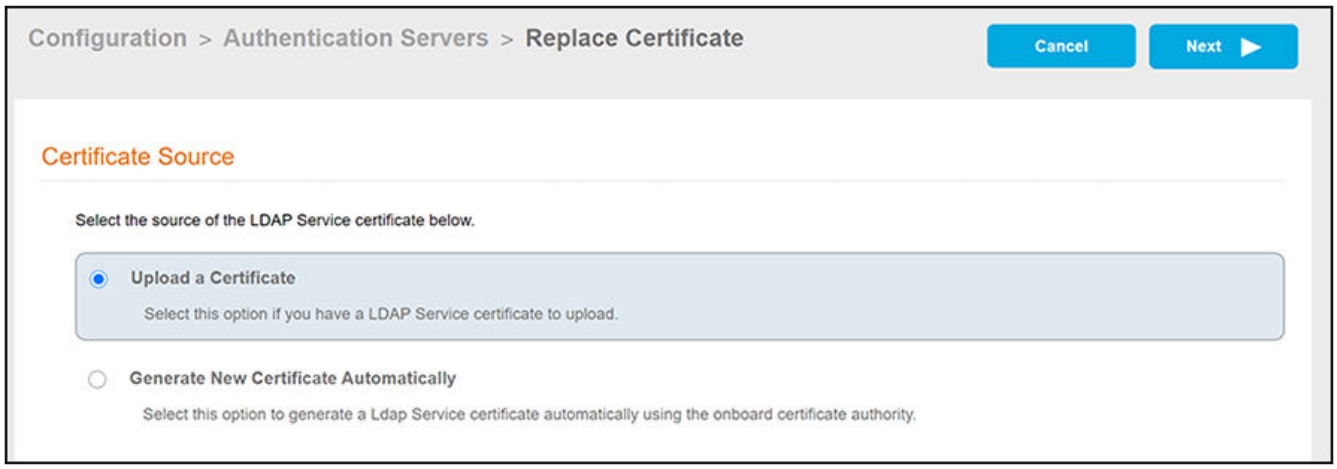
4. Enter edit mode for the newly created LDAP server by clicking the pencil icon to the right of the server name.
5. In the ensuing Modify Authentication Servers screen, check the TLS Client Certificate box. When you check this box, the screen allows you to upload the certificate using the "Define Certificate" button, as shown at the bottom of the following illustration:

FIGURE 31 Checking the TLS Client Certificate Button



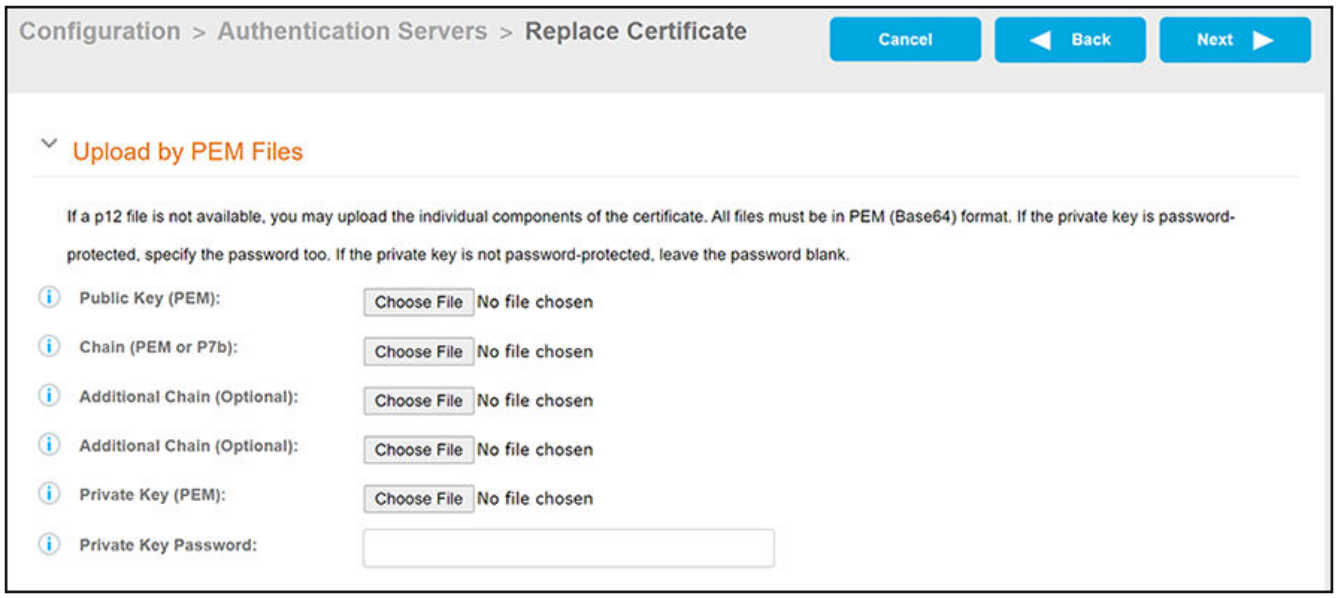
6. Click "Define Certificate" to invoke the following screen, where you select the source of your certificate:

FIGURE 32 Selecting the Certificate Source



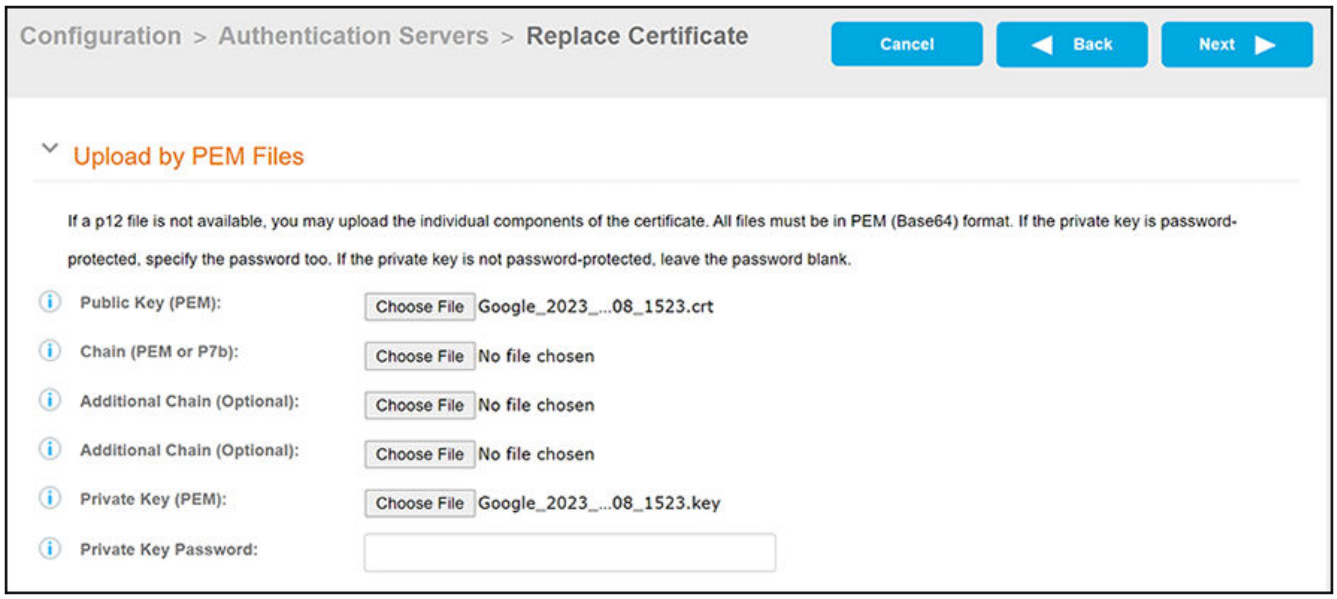
7. With the "Upload a Certificate" button selected, click **Next**. The following screen appears:

FIGURE 33 Screen for Uploading Certificates



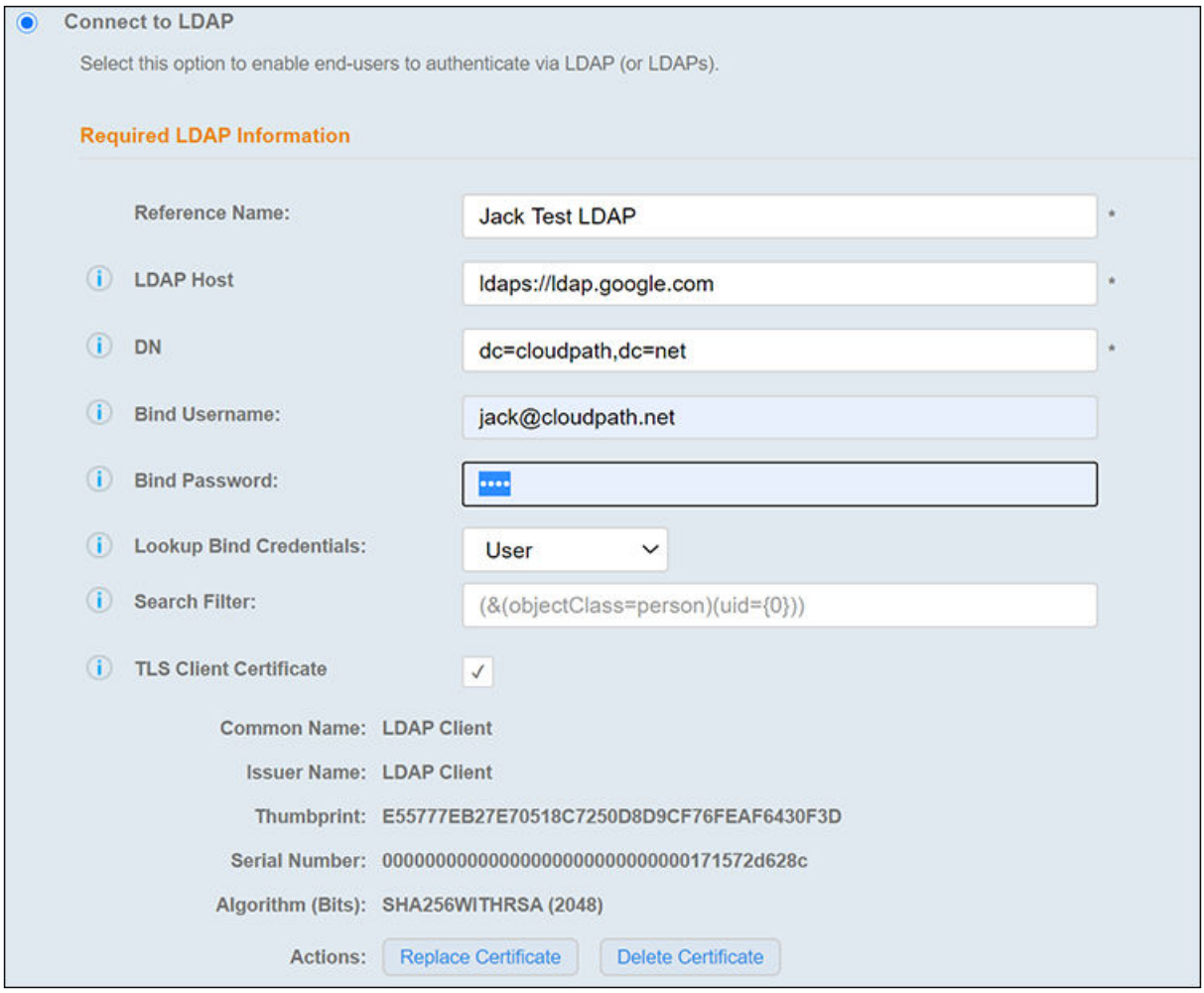
8. Using the Public Key (PEM) field, click **Choose File** to upload your certificate (a .crt file).
9. Using the Private Key (PEM) field, click **Choose File** to upload your private key (a .key file). The screen should now appear as follows:

FIGURE 34 Screen After Certificate Files Are Added



10. Click **Next**. A message indicating success of the certificate upload briefly appears, and you are returned to the LDAP Configuration screen.

FIGURE 35 LDAP Configuration Screen After Certificates Are Successfully Added



11. If you are not using binding, you should remove any values that may have been placed into the Bind Username and Bind Password fields, then click **Save**.

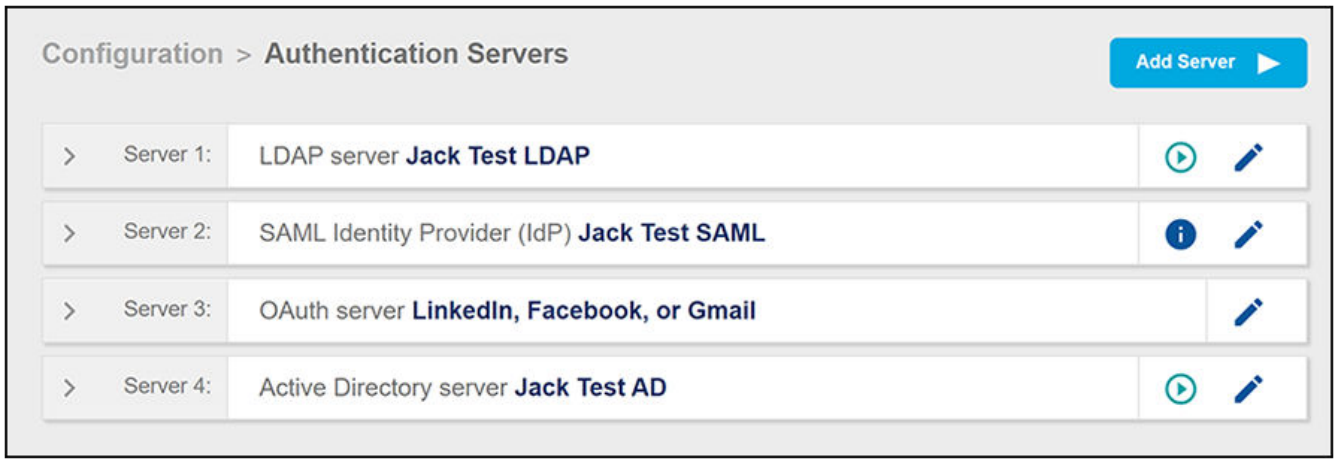
    NOTE
    As shown in the screen above, you can now view details such as thumbprint and serial number of the certificate, and you can also replace or delete the certificate from this screen. To return to this screen later, go to **Configuration > Authentication Servers** and click the pencil icon next to the sever to go into edit mode, then follow the instructions.

Testing

To test the connection to the LDAP server, do the following:

1. Go to **Configuration > Authentication Servers** and click the arrow to the right of the server name, as shown below:

FIGURE 36 Testing Server Connection



2. Enter a valid Google G Suite LDAP client username and password, then click **Continue**. If the connection is good, a message will indicate successful authentication.

   NOTE
   If the connection test fails, be sure that the Binding Username and Binding Password fields are empty (if you are not using binding) in the LDAP configuration screen.

Next Steps

You can include the LDAP authentication server in a workflow. For more information about workflows, refer to the *Cloudpath ES Deployment Administration Guide*.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com