

Cloudpath Enrollment System Third-Party Authentication Configuration Guide, 5.7

Supporting Cloudpath Software Release 5.7

Copyright, Trademark and Proprietary Rights Information

© 2020 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, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED 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.....	5
How to Add Facebook Authentication to the Workflow.....	6
User Experience for Facebook Authentication	8
Using LinkedIn for Third-Party Authentication.....	9
Setting Up the LinkedIn Application.....	9
What You Need To Set Up The LinkedIn Application.....	9
How to Set Up the LinkedIn App.....	9
Setting Up Cloudpath for LinkedIn Authentication.....	12
What You Need to Configure Cloudpath for LinkedIn.....	12
How to Add LinkedIn Authentication to the Workflow.....	12
User Experience for LinkedIn Authentication.....	14
Using Google for Third-Party Authentication.....	17
Setting Up the Google Application.....	17
What You Need To Set Up The Google Application.....	17
Creating the Google Web Application Project.....	17
Setting Up Cloudpath for Google Authentication.....	18
What You Need to Configure Cloudpath for Google.....	18
How to Add Google Authentication to the Workflow.....	18
User Experience for Google Authentication.....	20
Using Google LDAP Client as an Authentication Server.....	23
Prerequisites.....	23
Configuration Steps.....	23
Testing.....	28
Next Steps.....	29

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

Third-Party Authentication Setup


1 Display Name:

1 Description:

Facebook Configuration

1 Facebook Supported?

Instructions: The Facebook Developer's Console is available at <https://developers.facebook.com>. Within My Apps, create a new app for a website, and Create App ID. You will need the App ID and App Secret.



1 App ID:

1 Secret:

1 Scope:

1 Event ID:

1 Liked Page ID:

1 Redirect URL: Facebook will need a Website "Site URL," to redirect to. This must be the full enrollment URL, + "facebook", such as <https://test01.cloudpath.net/enroll/RegistrationTest?facebook>.

Based on the current deployment locations, the Site URL should be one of <https://test01.cloudpath.net/enroll/RegistrationTest?ProductionFacebook>

Google Configuration

1 Google Supported?

LinkedIn Configuration

1 LinkedIn Supported?

Custom OAuth 2.0

1 Custom OAuth 2.0 Configuration

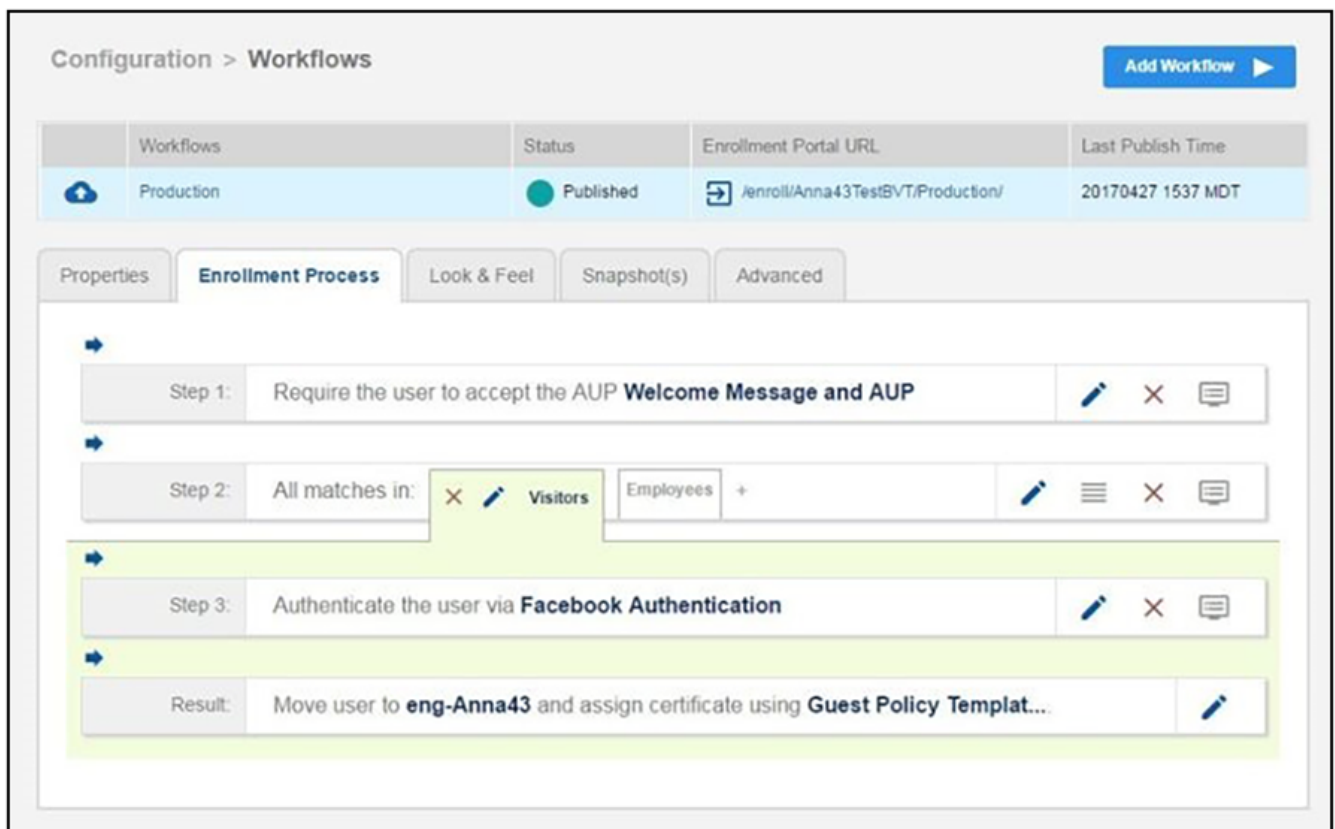
5. In the Facebook Configuration section, check the **Facebook Supported?** box and complete the following fields:
 - **App ID** - The **App ID** from the Facebook application you just created.
 - **Secret** - The **App Secret** from the Facebook application you just created.
 - Optional settings:
 - **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.....](#) 9
- [Setting Up Cloudpath for LinkedIn Authentication.....](#) 12

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 4 Create an app Screen on LinkedIn Developers Site

LinkedIn DEVELOPERS Products Documentation Help

Create an app

App name
CloudpathTestapp

1. App information

Company name
Ruckus Networks

App description
Test LinkedIn Authentication

App logo
This is the logo displayed to users when they authorize with your app.
Upload a logo

Privacy policy URL
https://jeff243.cloudpath.net/enroll/JackTest/Production

Business email
jeff@arris.com

2. Products

3. Legal terms

When you develop on our platform, you are agreeing to be bound by our [API Terms of Use](#).
In addition, certain products may be subject to additional terms:
[Plugins Terms of Use](#)

I have read and agree to these terms

Cancel Create app

Notes
When naming your app please provide a unique application name less than 50 characters.
The privacy policy entered will be shown to each user when your app requests access to their LinkedIn member data.
Depending on the products added, we may need to further review your request and we may require additional information after you create the app before we can provision API access. We will follow-up by email to the primary email address associated with your LinkedIn member account if we need more information and to inform you of our decision.

5. Enter the following information for your application:

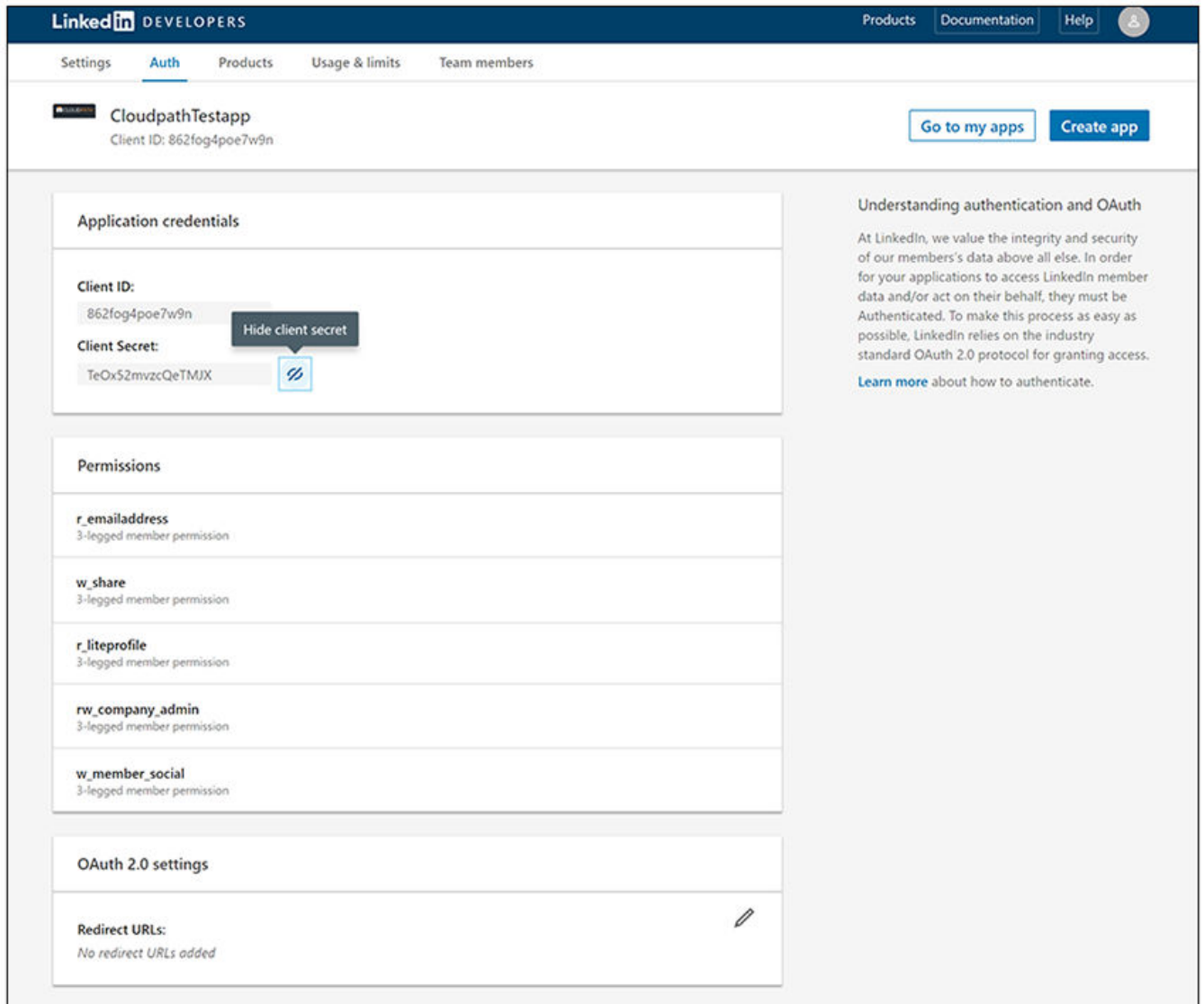
- App name (name of your application)
- Company name
- App description
- Upload an application logo
- Private policy URL (of your company)
- Business Email

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 5 Auth Tab Settings of Newly Created Application



- 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 12. (Figure 7 on page 13 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 6 Redirect URL Added to LinkedIn Configuration



- 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)

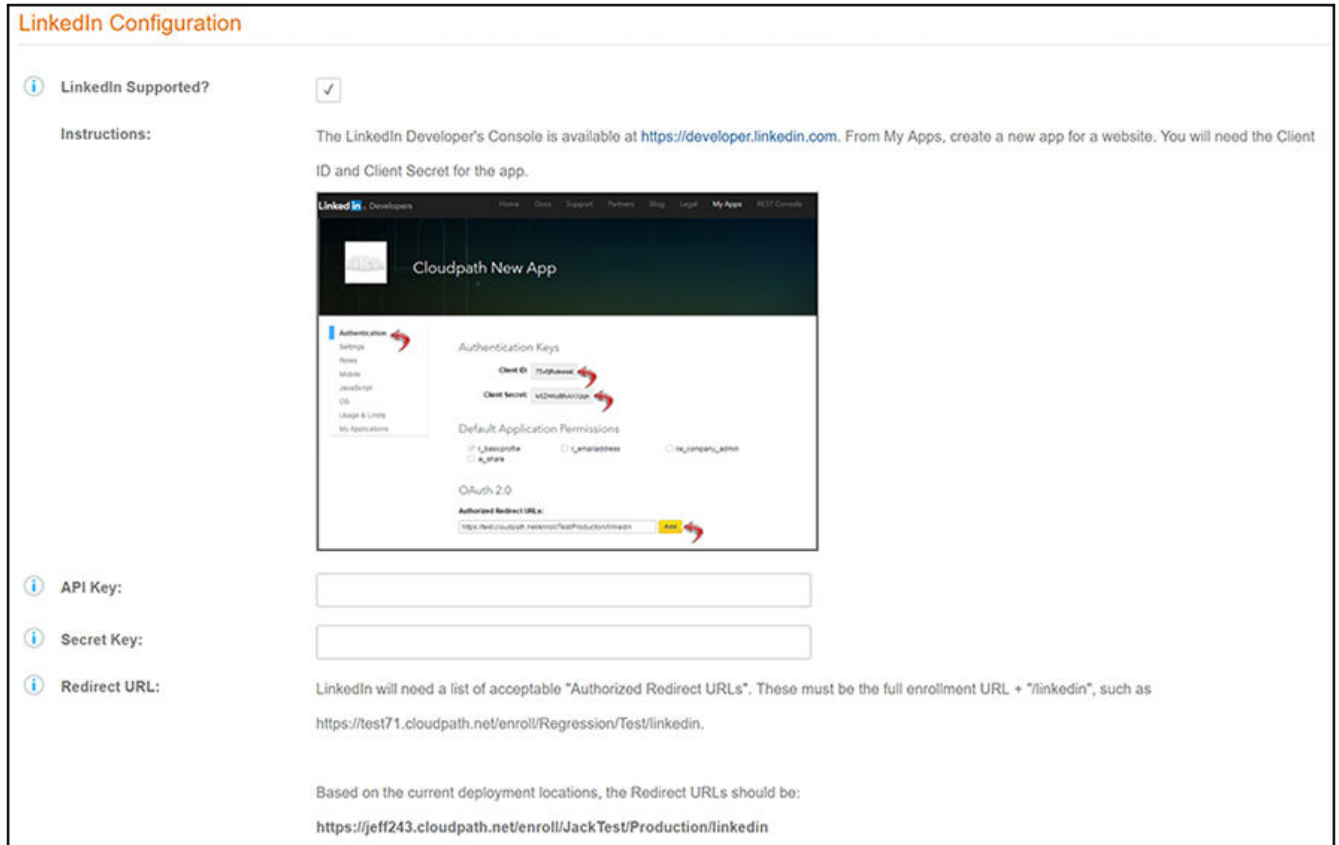
How to Add LinkedIn Authentication to the Workflow

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

- Create an enrollment workflow for third-party authentication.
- 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.
- Place the authentication step after the **User Type** option.
- Enter the **Name** and **Description** of this configuration.

5. Scroll down to the **LinkedIn Configuration** section, and check the **LinkedIn Supported?** box.

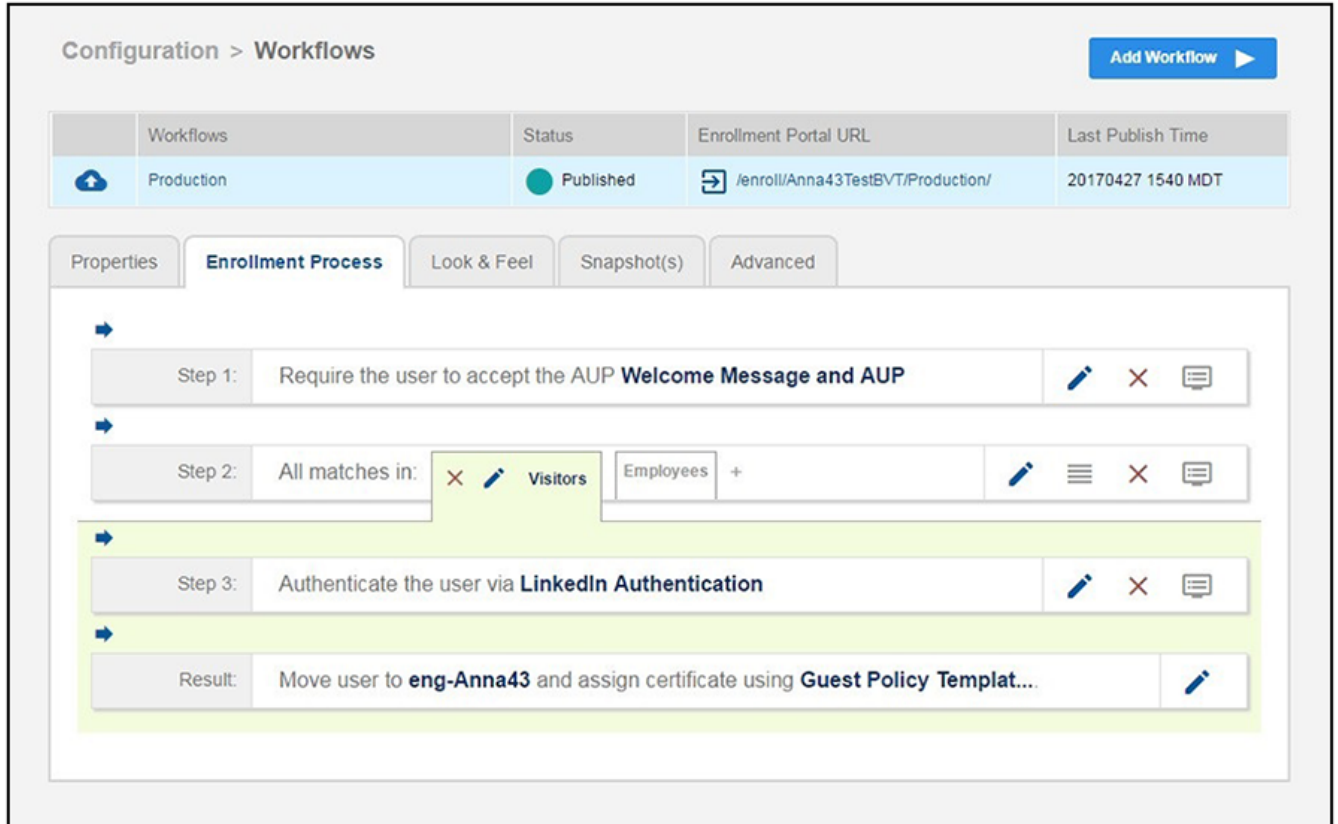
FIGURE 7 Cloudpath Third-Party Authentication Setup for LinkedIn



6. In the API Key field, enter the Client ID from the LinkedIn Auth Tab Settings of Newly Created Application screen (refer to [Figure 5](#) on page 11).
7. In the Secret Key field, enter the Client Secret from the LinkedIn Auth Tab Settings of Newly Created Application screen (refer to [Figure 5](#) on page 11).

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

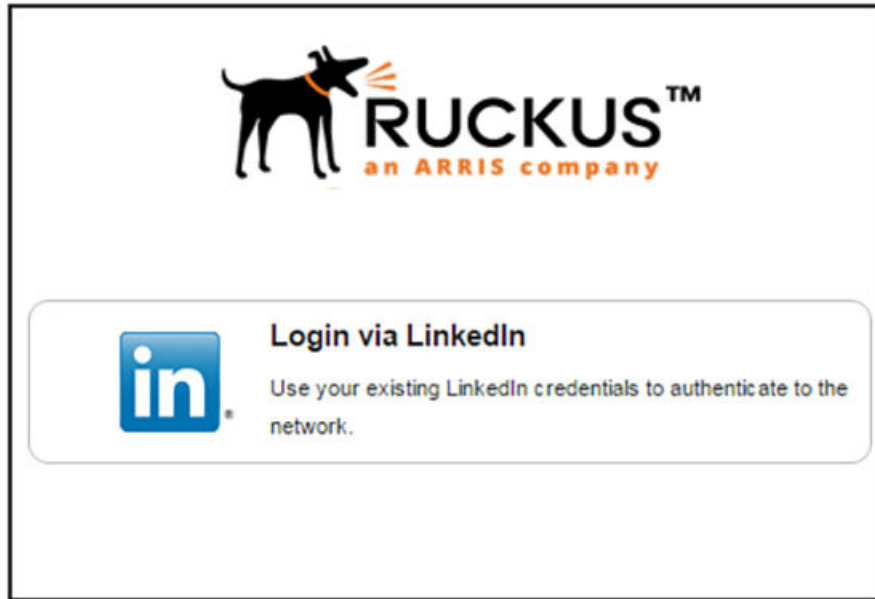
FIGURE 8 Cloudpath Workflow With LinkedIn Step Added



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 9 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.....](#) 17
- [Setting Up Cloudpath for Google Authentication.....](#) 18

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.

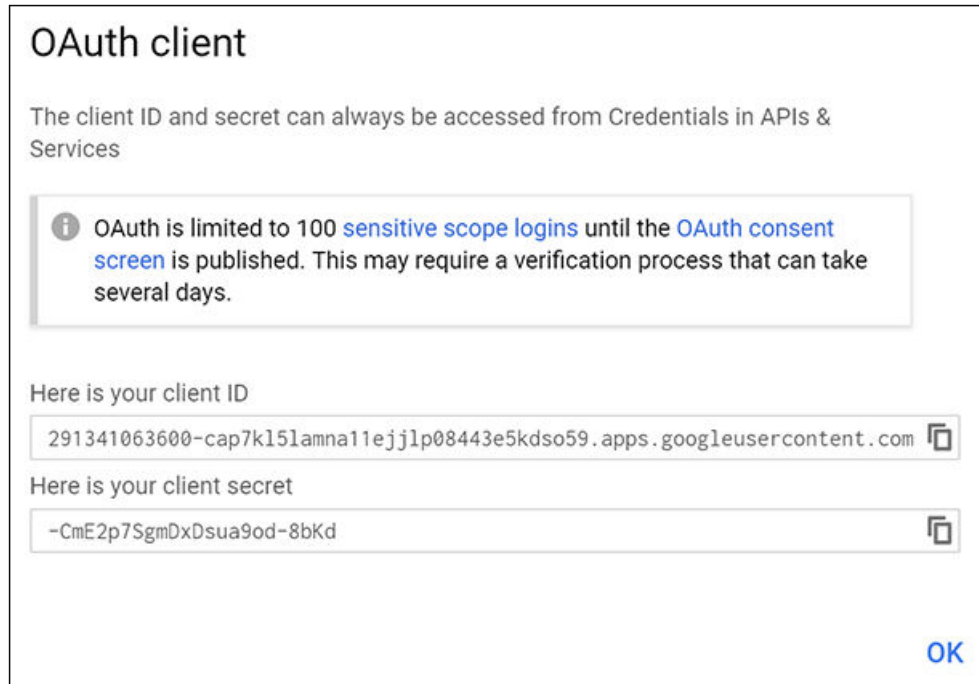
NOTE

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 10 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 11 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 Configuration

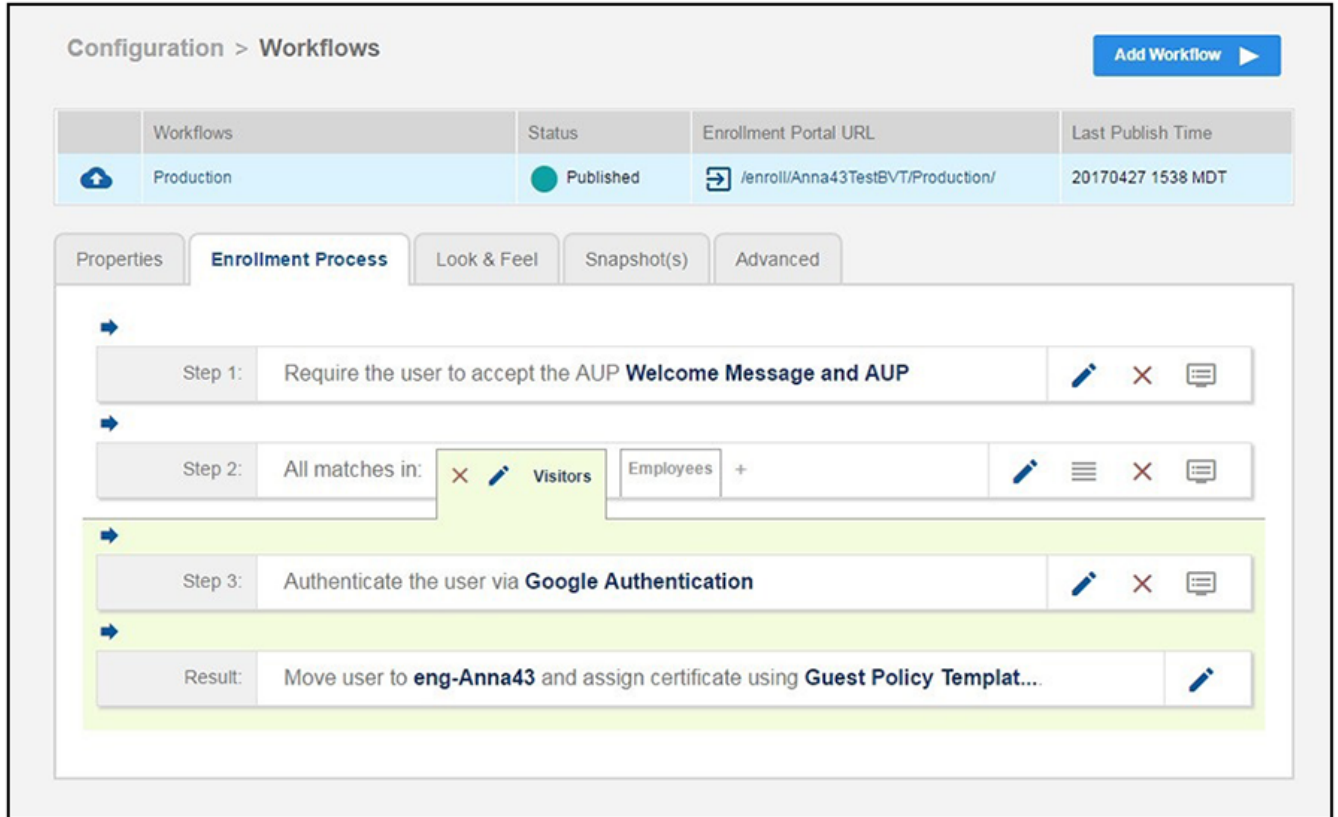
Custom OAuth 2.0 Configuration

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.

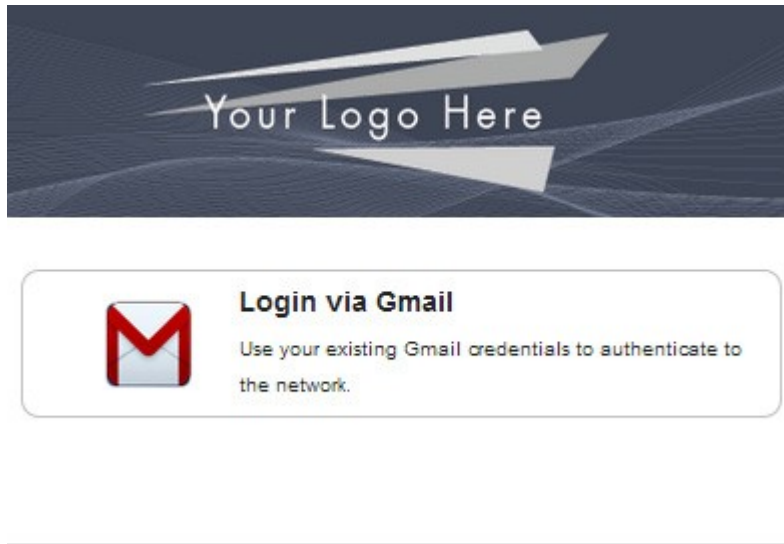
FIGURE 12 Cloudpath Workflow



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 13 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 14](#)) 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 14 Connect to LDAP Selection

Connect to LDAP
Select this option to enable end-users to authenticate via LDAP (or LDAPs).

Required LDAP Information

- LDAP Host:** ldaps://ldap.google.com *
- DN:** dc=cloudpath,dc=net *
- Bind Username:** [ex. uid=bob,cn=users,dc=test,dc=cloudpath,dc=local]
- Bind Password:**
- Lookup Bind Credentials:** User
- Search Filter:** (&(objectClass=person)(uid={0}))

- 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 15 LDAP Authentication Server Added

Configuration > Authentication Servers Add Server

>	Server 1:	LDAP server Jack Test LDAP		
>	Server 2:	SAML Identity Provider (IdP) Jack Test SAML		
>	Server 3:	OAuth server LinkedIn, Facebook, or Gmail		
>	Server 4:	Active Directory server Jack Test AD		

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 16 Checking the TLS Client Certificate Button

Connect to LDAP
Select this option to enable end-users to authenticate via LDAP (or LDAPs).

Required LDAP Information

Reference Name:	Jack Test LDAP *
<i>i</i> LDAP Host	ldaps://ldap.google.com *
<i>i</i> DN	dc=cloudpath,dc=net *
<i>i</i> Bind Username:	[ex. uid=bob,cn=users,dc=test,dc=cloudpath,dc=local]
<i>i</i> Bind Password:	
<i>i</i> Lookup Bind Credentials:	User ▾
<i>i</i> Search Filter:	{&(objectClass=person)(uid={0})}
<i>i</i> TLS Client Certificate	<input checked="" type="checkbox"/>

No certificate defined - Press 'Define Certificate' button below.

Actions: [Define Certificate](#)

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

FIGURE 17 Selecting the Certificate Source

Configuration > Authentication Servers > Replace Certificate

Cancel Next

Certificate Source

Select the source of the LDAP Service certificate below.

Upload a Certificate
Select this option if you have a LDAP Service certificate to upload.

Generate New Certificate Automatically
Select this option to generate a Ldap Service certificate automatically using the onboard certificate authority.

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

FIGURE 18 Screen for Uploading Certificates

Configuration > Authentication Servers > Replace Certificate

Cancel Back Next

Upload by PEM Files

If a p12 file is not available, you may upload the individual components of the certificate. All files must be in PEM (Base64) format. If the private key is password-protected, specify the password too. If the private key is not password-protected, leave the password blank.

Public Key (PEM): Choose File No file chosen

Chain (PEM or P7b): Choose File No file chosen

Additional Chain (Optional): Choose File No file chosen

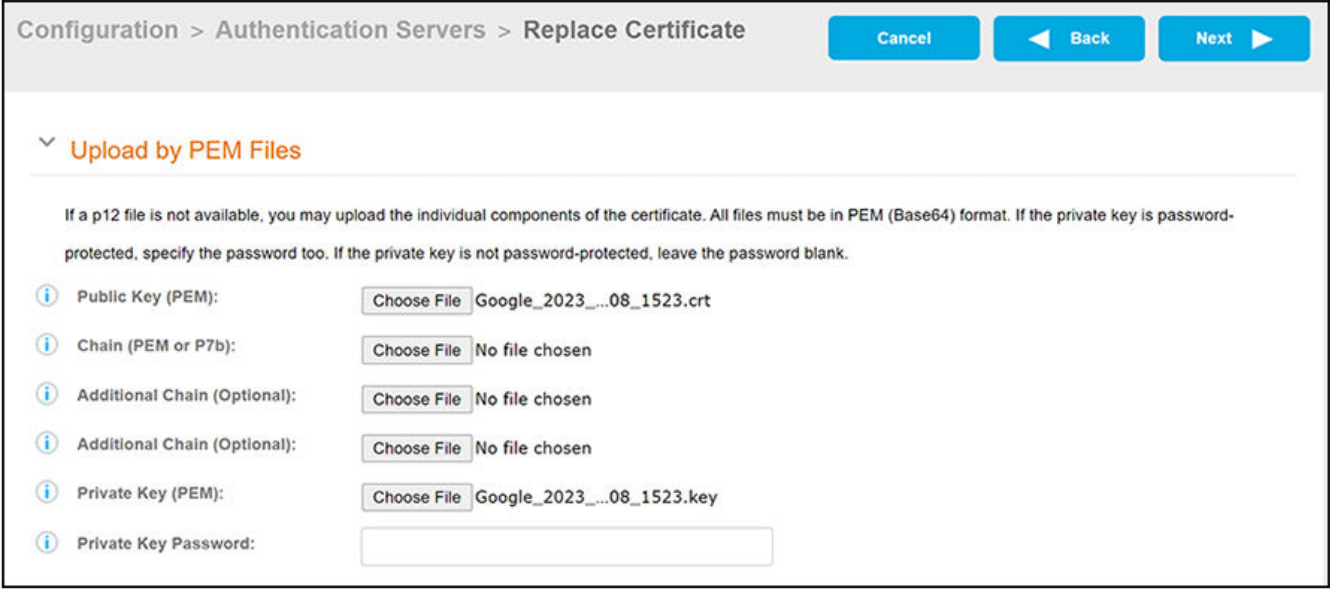
Additional Chain (Optional): Choose File No file chosen

Private Key (PEM): Choose File No file chosen

Private Key Password:

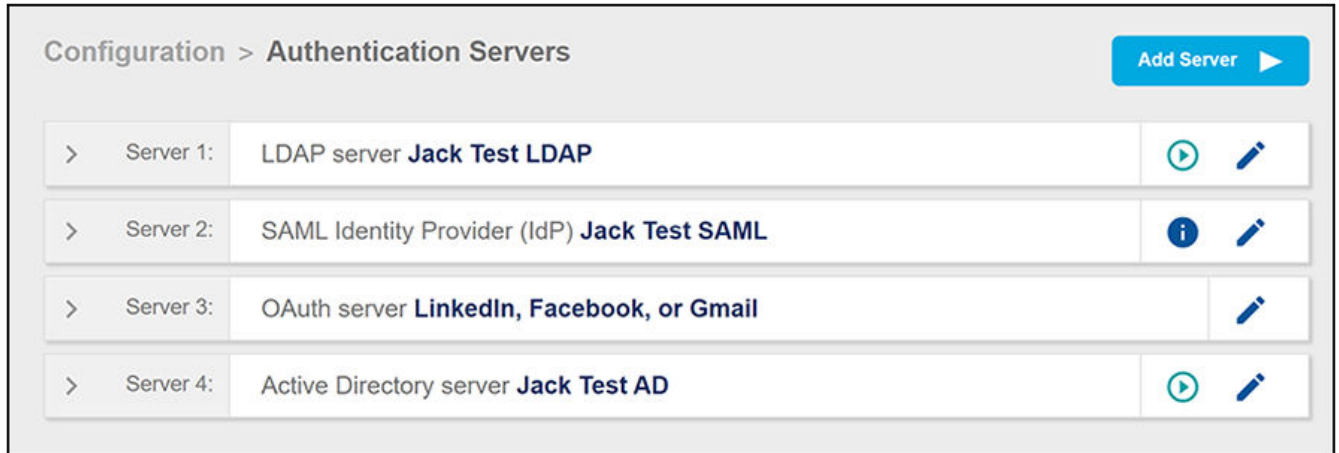
8. Using the Public Key (PEM) field, click **Choose File** to upload your certificate (a .crt file).
9. Using the Private Key (PEM) field, click **Choose File** to upload your private key (a .key file). The screen should now appear as follows:

FIGURE 19 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 21 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*.

