COMMSCOPE" RUCKUS®

CONFIGURATION GUIDE

Cloudpath Enrollment System Third-Party Authentication Configuration Guide, 5.8

Supporting Cloudpath Software Release 5.8

Copyright, Trademark and Proprietary Rights Information

© 2021 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	
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

Trice-Party Authentication Servir () Dewryber: () Dewryber: Facebook Configuration Face		
Preserveix: Image:	Third-Party Authentication S	letup
Precesses Reporting Image:	(j) Display Name:	New Authentication Server
Precesses Reporting Image:	(i) Description:	
Image:	er. a contractor	
Image:		
Image:		
Instruction: The factorial because or statistics at they, size-edges to books any. When by App, Orabe a new app for a versite, and Create App D. Yall Instruction: Image: Ima	Facebook Configuration	
<pre>sheat be:</pre>	() Facebook Supported?	
Sector Configuration Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks Coople Configuration Interest National Streams TestBooks Interest National Streams TestBooks </td <td>Instructions:</td> <td>The Facebook Developer's Consule is available at https://developers.tocebook.com Within My Apps, oneste a new app for a website, and Create App ID. You</td>	Instructions:	The Facebook Developer's Consule is available at https://developers.tocebook.com Within My Apps, oneste a new app for a website, and Create App ID. You
Age D: Ag		will need the App ID and App Secret.
i App D: i App D: i Sord:		Research and Annual Contract Annual
App D: App D: Sort: Book: Rotext D: Coopsi https://doi.org/initiation.com/initiation.co		and the second s
i App D: i App D: i book:		An Cooljusti 5.0 Text App
App D: App D: Soopt: Soopt: Soopt: D: <pd:< p=""> <p< td=""><td></td><td></td></p<></pd:<></pd:<></pd:<></pd:<></pd:<></pd:<></pd:<>		
App D: App D: Soopt: Soopt: Soopt: D: <pd:< p=""> <p< td=""><td></td><td>e</td></p<></pd:<></pd:<></pd:<></pd:<></pd:<></pd:<></pd:<>		e
App D: App D: Scoret: Scor		
(i) App D: (i) App D: (i) Score: (i) Score: (i) Score: (i) Score: (i) Event D: (i) Linke Physic D: (i) Linke Physic D: (ii) Score: (iii) Score: (iii) Coorgin NetT and a Weestin "Dire Unit, in the full ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in "Scoreson", such as major interfull courganine ensitiened Unit, in the dure of the curve end ensitiened Unit, in the curve end ensitiened Unit, in the curve end ensitiened Unit, in the ensitiened Unit, in the ensite ensitiened Unit, in the ensite end Unit, in the ens		Name of Control of Con
(i) App D: (i) Score: (i) Score: (i) Score: (i) Score: (i) Score: (i) Event D: (i) Linke Physic D: (i) Linke Physic D: (ii) Score: (iii) Score: (iii) Score: (iii) Coore: (iii) Score: (iii) Coore: (iiii) Score: (iii) Coore: (iii) Score: (iii) Coore: (iiii) Score: (iiiii) Score: (iiii) Score		Receipter to
Image:		
i soort: i soort: i soort: i soort: i soort: i soort: i beet di: i Liked Page D: i Liked Page D: i Soort: i Soort: i Soort: i Soort: i Liked Page D: i Soort: i Soort: i Soort: i Liked Page D: i Soort: i Likedin Soportet? i Likedin Soportet? i Likedin Soportet? i Likedin Soportet?		Lee-
iii scort: iii scort: iii scort: iii scort: iii beet do: iii Liked Page D: iii Liked Page D: iii Addrect URL: Pacebook will need a Vestelle' Stie URL's to redirect Ib. This must alle buil enstiment URL + 'floatook', such alle iiii kited? Looudpath networktimasd? editory 17% reduction/tacebook Google Configuration iii LikedIn Configuration iii LikedIn Supported? iii LikedIn Supported?	App ID:	
i) stops: ii) stops: ii) Event I0: ii) Liked Page ID: iii) Addrect URL: rps:/sec11.couppet/neters/iftagression?estitoecoux. based on the current depayment tocations. The Sile URL: should be ove of https:/menual/Textby/T.feroduction/faceboook	(a) company)	
Image: Description Image: D	(i) Secret:	
(i) Liked Page ID: (i) Redirect URL: Processos will reed a Vestelle "Die URL" to redirect Is. This must alle full ensitivent URL + "Bostoox", such alle individual individ	() Scope:	
(i) Liked Page ID: (i) Redirect URL: Processos will reed a Vestelle "Die URL" to redirect Is. This must alle full ensitivent URL + "Bostoox", such alle individual individ	(D) Read (D)	
Redirect URL: Processor will need a Vressile "Site URL: to redirect Is. This must a the full ensitienent URL + "flootsoor", such as mps. Head on the current depolyment roadors, the Site URL: should be one of: https://mennekti.doustpath.netwenokti.neadOf extEv/T Procelyction/flootbook Google Configuration Configuration Linkedin Configuration Linkedin Supported? Custom CAuth 2.0	(I) Even of	
rtps:/test/1.couppath.netersoftingression/Testbootoox. Based on the current depreparent locations. the Sile Lift, should be one of https:/menuEcl.couppath.netersoftingression/Testbootook Google Configuration () Google Supported? LinkedIn Configuration () LinkedIn Supported? () LinkedIn Configuration () LinkedIn Configuration () LinkedIn Configuration () LinkedIn Configuration	(j) Liked Page ID:	
Siesed on the current depayment locations, the Sile URL should be one at https://www.scile.org/sile/scile.org/sile/scile.org/sile/scile.org/sile/scile/	Redirect URL:	Pacebook will need a Website "Dite URL," to redirect to. This must a the full enrollment URL + "facebook", such as
Mitpa Jannaki doudpila.ne/terroliti.neat/Teetti//T.Rhodudion%zoebook Google Configuration (i) Google Supporter? Linkedin Configuration (i) Linkedin Supporter? (i) Linkedin Supporter? (ii) Linkedin Supporter? (iii) Linkedin Supporter?		Mgs.steat71.cloudpath.netien/ofi/Regression/Teal/Booebook.
Mitpa Jannaki doudpila.ne/terroliti.neat/Teetti//T.Rhodudion%zoebook Google Configuration (i) Google Supporter? Linkedin Configuration (i) Linkedin Supporter? (i) Linkedin Supporter? (ii) Linkedin Supporter? (iii) Linkedin Supporter?		
Google Configuration (i) Google Supportiet? LinkedIn Configuration (i) LinkedIn Supportiet? (i) LinkedIn Supportiet? (i) LinkedIn Supportiet? (i) LinkedIn Supportiet?		
Googe Supported? LinkedIn Configuration LinkedIn Supported? Custom OAuth 2.0		https://annadl.courtpatn.net/enrol/LnnadTeeltSvT.Production/Tacebook
Googe Supported? LinkedIn Configuration LinkedIn Supported? Custom GAuth 2.0	Coopie Confermion	
Linkedin Configuration	Cooyle Connyarason	
Linkedin Supportez Custom OAuth 2.0	() Googie Supported?	
Linkedin Supportez Custom OAuth 2.0		
Custom OAuth 2.0	LinkedIn Configuration	
Custom OAuth 2.0	(i) Linkedin Supported?	
(j) Cuelon Gauth 2.8 Configuration	Custom OAuth 2.0	
W. Canadi Carlos Construction [7]	() Curles On the 16 Cart and Cart	
	 Communication Stational Consideration 	

- 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

	Workflo	ws		-	Status		Enrollment Porta	I URL		Last i	Publish	Time
0	Producti	on			Publi	shed	➔ /enroll/Anna	43TestBVT/Productio	on/	20170	427 15	37 MDT
Propert	ties	Enroll	ment Process	Look & Fee	t Sn	apshot(s)	Advanced					
+	Step	p 1:	Require the u	ser to accept	t the AU	P Welcon	ne Message a	nd AUP		1	×	
*	Ste	p 2:	All matches in	× /	Visitors	Employed	+		1	≣	×	
*	Ste	p 3:	Authenticate t	he user via F	aceboo	ok Auther	tication			/	×	
+												
	Res	sult:	Move user to	eng-Anna43	and as	sign certifi	cate using Gu	est Policy Ten	plat			1

Setting Up Cloudpath for 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

<u>Start Over</u>	Powered by Ruckus Networks
f	Login via Facebook Use your existing Facebook credentials to authenticate to the network.

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

		×
Create an app		Notes
App name CloudpathTestapp		When naming your app please provide a unique application name less than 50 characters.
I. App information	^	The privacy policy entered will be shown to each user when your app requests access to their Linkedin member data.
Company name		Depending on the products added, we may need to further review your request and we may
Ruckus Networks		require additional information after you create the app before we can provision API access. We
App description		will follow-up by email to the primary email
Test LinkedIn Authentication		address associated with your Linkedin member account if we need more information and to inform you of our decision.
Privacy policy URL https://jeff243.cloudpath.net/enroll/JackTest/Production		
https://jeff243.cloudpath.net/enroll/JackTest/Production		
Business email		
jeff@arris.com		
jeff@arris.com 2. Products	~	
	~	
2. Products	~	
2. Products 3. Legal terms When you develop on our platform, you are agreeing to be bound by our API Terms of Use.	~	
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 L ²	~	
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:	~	

- 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

inked in DEVELOPERS	Products Documentation Help
ettings Auth Products Usage & limits Team members	
CloudpathTestapp Client ID: 862fog4poe7w9n	Go to my apps Create app
Application credentials	Understanding authentication and OAuth At LinkedIn, we value the integrity and security
Client ID: 862fog4poe7w9n Hide client secret	of our members's data above all else. In order for your applications to access LinkedIn memb data and/or act on their behalf, they must be Authenticated. To make this process as easy as
Client Secret: TeOx52mvzcQeTMUX	possible, Linkedin relies on the industry standard OAuth 2.0 protocol for granting acce Learn more about how to authenticate.
	Learn more about now to authenticate.
Permissions	
r_emailaddress 3-legged member permission	
w_share 3-legged member permission	
r_liteprofile 3-legged member permission	
rw_company_admin 3-legged member permission	
w_member_social 3-legged member permission	
OAuth 2.0 settings	
Redirect URLs:	/
No redirect URLs added	

Setting Up Cloudpath for LinkedIn Authentication

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 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

OAuth 2.0 settings
Redirect URLs:
https://jeff243.cloudpath.net/enroll/JackTest/Production/linkedin

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 7 Cloudpath Third-Party Authentication Setup for LinkedIn

Lin	kedIn Configuration	
•	LinkedIn Supported?	\checkmark
	Instructions:	The LinkedIn Developer's Console is available at https://developer.linkedin.com. From My Apps, create a new app for a website. You will need the Client
		ID and Client Secret for the app.
		Linked R. Developers New Doo Support Polices Big Legit Mr New BSP Consis
		Cloudpath New App
		Antherstation AuthonoScation Keys Norm Over Combined International C
		In Annum Default Application Permissions
		OAuth 2.0
		Anthorized Balanci (R.). The Charlow Councept restronational function for the Charles of the Cha
1	API Key:	
1	Secret Key:	
1	Redirect URL:	LinkedIn will need a list of acceptable "Authorized Redirect URLs". These must be the full enrollment URL + "/linkedin", such as
		https://test71.cloudpath.net/enroll/Regression/Test/linkedin.
		Based on the current deployment locations, the Redirect URLs should be:
		https://jeff243.cloudpath.net/enroll/JackTest/Production/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.

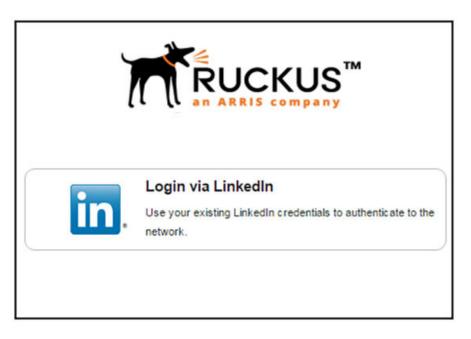
FIGURE 8 Cloudpath Workflow With LinkedIn Step Added

	Workflows		Stat	us	Enrollment Portal URL		Last I	Publish	Time
0	Production		•	Published	→ /enroll/Anna43TestBVT/Prod	luction/	20170	0427 15	40 MDT
Proper	ties Enrol	Iment Process	ok & Feel	Snapshot(s) Advanced				
+	Step 1:	Require the user to	o accept the	e AUP Welco	ome Message and AUP		1	×	
+	Step 2:	All matches in:	🗙 🧨 Visi	tors	ees +	1	≡	×	
•									
	Step 3:	Authenticate the u	ser via Lin	kedIn Authe	ntication		1	×	
+									
	Result:	Move user to eng-	Anna43 ar	nd assign cer	tificate using Guest Policy	Templat			1

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.

Setting Up Cloudpath for Google Authentication

- 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

OAuth client	
The client ID and secret can always be accessed from Credentials in APIs & Services	
OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is published. This may require a verification process that can take several days.	
screen is published. This may require a verification process that can take	
screen is published. This may require a verification process that can take several days.	m Г
screen is published. This may require a verification process that can take several days. Here is your client ID	m F

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 S	etup
(i) Display Name:	New Authentication Server
(i) Description:	
Facebook Configuration	
(i) 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.
	I and the second sec
() Client ID:	anonymous
(i) Client Secret:	anonymous
Redirect URIs:	Google will need a list of acceptable Redirect URIs. These must be the full enrollment URL + "google", such as https://test?1.cloudpath.neterroll.Regression/Testgoogle. Multiple URLs may be specified, with one per line.
	Based on the current deployment locations, the Redirect URIs should be: https://wnna43.cloudpath.net/enrow/Anna43TestBivTr/Production/google
LinkedIn Configuration	
(i) Linkedin Supported?	
Custom OAuth 2.0	
Custom Oauth 2.0 Configuration	

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

Note: These entries must match what is specified in the Google application.

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

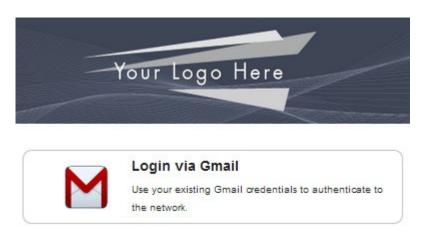
FIGURE 12 Cloudpath Workflow

	Workflows		Status		Enrollment Portal	URL		Last I	Publish	Time
0	Production		Pu	ublished	€ /enroll/Anna	3TestB∨T/Productio	n/	20170)427 15	38 MDT
Proper	ties Enrol	Ilment Process	k & Feel	Snapshot(s)	Advanced					
+										
	Step 1:	Require the user to	accept the A	UP Welcor	me Message a	nd AUP		1	×	
+										
	Step 2:	All matches in:	/ Visitor	s Employe	es +		1		×	
+										
	Step 3:	Authenticate the use	er via Goog	le Authenti	cation			1	×	
+										
	Result:	Move user to eng-A	nna43 and	assign certi	ficate using Gu	est Policy Tem	plat			1

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 a	authenticate via LDAP (or LDAPs).	
Required LDAP Information		
i LDAP Host	ldaps://ldap.google.com	*
i dn	dc=cloudpath,dc=net	*
(i) Bind Username:	[ex. uid=bob,cn=users,dc=test,dc=cloudpath,dc=local]	
i Bind Password:		
(i) Lookup Bind Credentials:	User ~	
(i) Search Filter:	(&(objectClass=person)(uid={0}))	

• Connect to LDAP: Idaps://Idap.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

		> Authentication Servers	Add Server
>	Server 1:	LDAP server Jack Test LDAP	•
>	Server 2:	SAML Identity Provider (IdP) Jack Test SAML	0 /
>	Server 3:	OAuth server LinkedIn, Facebook, or Gmail	1
>	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

Required LDAP Information		
Reference Name:	Jack Test LDAP	•
1 LDAP Host	ldaps://ldap.google.com	*
DN DN	dc=cloudpath,dc=net	*
() Bind Username:	[ex. uid=bob,cn=users,dc=test,dc=cloudpath,dc=local]	
() Bind Password:		
(i) Lookup Bind Credentials:	User ~	
(i) Search Filter:	(&(objectClass=person)(uid={0}))	
(i) TLS Client Certificate	×	

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

FIGURE 17 Selecting the Certificate Source

Configu	ration > Authentication Servers > Replace Certificate	Cancel	Next 🕨
Certific	ate Source		
Selec	t the source of the LDAP Service certificate below.		
	Upload a Certificate		
	Select this option if you have a LDAP Service certificate to upload.		
0	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 > Authentica	ation Servers > Replace Certificate Cancel Back Next
✓ Upload by PEM Files	
the second se	upload the individual components of the certificate. All files must be in PEM (Base64) format. If the private key is password- If the private key is not password-protected, leave the password blank.
(i) Public Key (PEM):	Choose File No file chosen
(i) Chain (PEM or P7b):	Choose File No file chosen
(i) Additional Chain (Optional):	Choose File No file chosen
(i) Additional Chain (Optional):	Choose File No file chosen
i Private Key (PEM):	Choose File No file chosen
(i) 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

 Vpload 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, leave the password blank. i Public Key (PEM): Choose File Google_202308_1523.crt i Chain (PEM or P7b): Choose File No file chosen i Additional Chain (Optional): Choose File No file chosen i Additional Chain (Optional): Choose File No file chosen 	Configuration > Authentic	cation Servers > Replace Certificate Cancel ABack Next >
i Public Key (PEM): Choose File Google_202308_1523.crt i Chain (PEM or P7b): Choose File No file chosen i Additional Chain (Optional): Choose File No file chosen	✓ Upload by PEM Files	
(i) Chain (PEM or P7b): Choose File No file chosen (i) Additional Chain (Optional): Choose File No file chosen		
Additional Chain (Optional): Choose File No file chosen	(i) Public Key (PEM):	Choose File Google_202308_1523.crt
	(i) Chain (PEM or P7b):	Choose File No file chosen
Additional Chain (Optional): Choose File No file chosen	(i) Additional Chain (Optional):	Choose File No file chosen
	(i) Additional Chain (Optional):	Choose File No file chosen
Private Key (PEM): Choose File Google_202308_1523.key	(i) Private Key (PEM):	Choose File Google_202308_1523.key
(i) Private Key Password:	(i) Private Key Password:	

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

Permised I DAD Information		
Required LDAP Information		
Reference Name:	Jack Test LDAP	•
(i) LDAP Host	ldaps://ldap.google.com	•
DN DN	dc=cloudpath,dc=net	•
(i) Bind Username:	jack@cloudpath.net	
(i) Bind Password:	••••	
(i) Lookup Bind Credentials:	User 🗸	
() Search Filter:	(&(objectClass=person)(uid={0}))	
(i) TLS Client Certificate	✓	
Common Name:	LDAP Client	
Issuer Name:	LDAP Client	
Thumbprint:	E55777EB27E70518C7250D8D9CF76FEAF6430F3D	
Serial Number:	00000000000000000000000000000000000000	
Algorithm (Bits):	SHA256WITHRSA (2048)	

FIGURE 20 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 21 Testing Server Connection

			Add Server
>	Server 1:	LDAP server Jack Test LDAP	•
>	Server 2:	SAML Identity Provider (IdP) Jack Test SAML	0 /
>	Server 3:	OAuth server LinkedIn, Facebook, or Gmail	1
>	Server 4:	Active Directory server Jack Test AD	0

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.



© 2021 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com