

## XpressConnect Enrollment System

# Setting Up Third-Party Authentication Within the XpressConnect Enrollment System Using Google™

Software Release 4.2 December 2015

**Summary:** This document describes how to create a Google application for use with the Enrollment System, and how to configure the Enrollment System to use the Google application for authentication. **Document Type:** Configuration **Audience:** Network Administrator



## Setting Up Third-Party Authentication Within the XpressConnect Enrollment System Using Google™

Software Release 4.2 December 2015

Copyright © 2015 Cloudpath Networks, Inc. All rights reserved.

*Cloudpath Networks* and *XpressConnect* are trademarks of *Cloudpath Networks, Inc.* Other names may be trademarks of their respective owners.

## Setting Up Third-Party Authentication Within the XpressConnect Enrollment System Using Google™

## **Overview**

The XpressConnect Enrollment System (ES) automates WPA2-Enterprise configuration on any device that connects to the network and automatically connects the device to a secure SSID. This *Automated Device Enablement* means authorized devices onboard simply and securely, with the appropriate level of access. By using the ES with Automated Device Enablement, the user gets configured and connected, regardless of device type, ownership, or level of access.

The flexible workflow engine gives network administrators further control by blending traditional policies (Active Directory, RADIUS, and integration with Microsoft CA) with additional policy capabilities (LinkedIn, Facebook, and Google Gmail). When you combine third-party authentication with traditional authorization methods, the social media provides additional identity information during the onboarding process to deliver automated, self-service access for all devices.



#### FIGURE 1. XpressConnect Onboarding System

## Setting Up the Google Application

Before configuring the Enrollment System for third-party authentication, you must set up the Google application.

#### What You Need

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

### **Google App Configuration**

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

#### How to Set Up the Google App

- 1. Go to https://console.developers.google.com.
- 2. Sign in to your Google account.
- 3. On the *Developers Console*, create and name an API Project. A *Project ID* is automatically assigned. If you already have an API project for this web application, continue to the next step.
- 4. Open the API project.

#### Note >>

You may be asked to complete an SMS verification process.

5. Go to the left-menu APIs & auth > Credentials > OAuth and click Creat new Client ID. A Client *ID* is required for the Enrollment System web application.



Overview Permissions APIs & auth APIs Credentials Consent screen Push Monitoring	OAuth OAuth 2.0 allows users to share specific data with you (for example, contact lists) while keeping their usernames, passwords, and other information private. Learn more Create new Client ID	No client IDs found.
Source Code Deploy & Manage Compute Networking Storage Big Data	Public API access Use of this key does not require any user action or consent, does not grant access to any account information, and is not used for authorization. Learn more Create new Key	No keys found.

- 6. On the Create Client ID window, select Web application and Configure consent screen.
- 7. A consent screen is shown to users whenever you request access to their private data using your client ID.

3

#### FIGURE 3. Consent Screen

Overview	Consent screen	
Permissions	The consent screen will be shown to users whenever you request access to their	
APIs & auth APIs	private data using your client ID Note: This screen will be shown for all of your applications registered in this project	
Credentials	Email address 🛞	
Consent screen	anna@cloudpath.net 👻	
Push	Droduct name	
Monitoring	Product name	Logo
Source Code	Troduct name	
Deploy & Manage	Homepage URL (Optional)	- Project Name would like to:
Compute		roject name would like to.
Networking	Product logo (Optional)	
Storage		Know your basic profile info and list of people in your circles.
Big Data		
	This is how your logo will look to end users Max size: 120x120 px	Make your listen, app and comment activity available via Google, visible to: Your circles
	Privacy policy URL (Optional)	
		By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can
	Terms of service URL (Optional)	change this and other Account Permissions at any time.
		Cancel Accept
	Google+ page ID (Optional)	
	plus.google.com/ page ID	
	Save	

The example user prompt is displayed on the right side of the page.

8. Click Save to create the Client ID.

4

#### FIGURE 4. Create Client ID

Application type	
Web applicat Accessed by y	tion web browsers over a network.
Service acco     Calls Google /	unt APIs on behalf of your application instead of an end-user. Learn more
<ul> <li>Installed app Runs on a des</li> </ul>	lication iktop computer or handheld device (like Android or iPhone).
Authorized JavaS Cannot contain a	Script origins wildcard (http://*.example.com) or a path (http://example.com/subdir)
https://www.ex	kample.com
https://www.ex Authorized redire One URI per line. N be a public IP Add	kample.com et URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress.
https://www.ex Authorized redire One URI per line. N be a public IP Add	kample.com ket URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress. kemple.com (pauth?pallback
https://www.ex Authorized redire One URI per line. N be a public IP Add https://www.ex	cample.com ct URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress. cample.com/oauth2callback
https://www.ey Authorized redire One URI per line. N be a public IP Add https://www.ey	cample.com ct URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress. cample.com/oauth2callback
https://www.ex Authorized redire One URI per line. N be a public IP Add https://www.ex	cample.com ct URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress. cample.com/oauth2callback
https://www.ex Authorized redire One URI per line. N be a public IP Add https://www.ex	cample.com ect URIs leeds to have a protocol, no URL fragments, and no relative paths. Can ress. cample.com/oauth2callback

- 9. On the Create Client ID page, under Application Type, choose Web Application.
- 10. The Authorized Javascript origins field can be left blank.
- 11. In the *Authorized redirect URIs* field, the entry must be in this format *\${ENROLLER\_URL}/ enroll/google/*, where \${ENROLLER\_URL} is the external URL to which the user is redirected. For multiple redirect URLs, enter one path on each line.
- 12. Click Create Client ID.

The Google Developer page displays the Client ID for web application information.



Overview	OAuth	Client ID for web application	
Permissions	OAuth 2.0 allows users to share	Client ID	301727419082-ist72gi62rom6deq8u9oqv6vhnej3hpj.apps.googleusercontent.com
APIs & auth	specific data with you (for example, contact lists) while keeping their usernames, passwords, and other	Email address	301727419082-ist72gi62rom6deq8u9oqv6vhnej3hpj@developer.gserviceaccount.com
APIs		Client secret	IFOorBj_8nvdBwH2hX3FIW_K
Credentials	information private.	Redirect URIs	https://www.example.com/oauth2callback
Consent screen	Learn more	JavaScript origins	https://www.example.com
Push	Create new Client ID	Edit settings Reset secre	t Download ISON Delete
Monitoring		Luit settings	Delete
Source Code			
Deploy & Manage	Public API access	No keys found.	
Compute	Use of this key does not require any		
Networking	user action or consent, does not grant		
Storage	and is not used for authorization.		
Big Data	Learn more		
	Create new Key		

#### Tip >>

Make note of your *Client ID* and *Client Secret*. You need this information to set up Google authentication within the Enrollment System.

## Setting Up the Enrollment System

After the Google application is set up, you configure an authentication step in the Enrollment System to prompt the user for the Google credentials.

#### What You Need

- Google application Client ID
- Google application Client Secret

#### **Enrollment System Configuration**

This section describes how to add a step to the enrollment workflow to authenticate a user using the Google application.

#### How to Add Third-Party Authentication to the Workflow

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

The *Third-Party Authentication Setup* page allows you to specify which third-party sources are allowed as well as API information related to those sources.

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

FIGURE 6. Third-Party Authentication Setup - Google

Google Configuration				
Google Supported?				
Instructions:	The Google Developer's Console is available at <u>https://console.developers.google.com</u> .			
	Within the desir	ed project, locate API &	Auth->Crede	entials and create a client ID for a web
	application.			
	Google Developers Conso	× 🚬		
				piui/credential 😭 🗮
	< Test71	OAuth	Compute Engine and App	Engine Learn more
	Overview	OAuth 2.0 allows users to share specific data with you (for	Client ID	144443438384-betgw"mbd
	APIs & auth	example, contact lists) while keeping their usernames,	Email address	24444942828344-bet.ge*abil
	APIs	passwords, and other information private.	Download JSON	
	Credentials	Learn more		
	Push	Create new Client ID	Client ID for web applica	tion
	Damissions	(	Client ID	244449430334-betge"abd
	Settings		Client secret	
	Support		Redirect URIs	https://test71.cloudpa
	App Engine	•	Javascript Origins	none
	The client ID 'a	nonymous' has been der	preceted by G	coogle and should not be used
	The client ID a	nonymous nas been dep	precated by G	
Elient ID:	anonymous			
Elient Secret:	anonymous			
Redirect URIs:	Google will nee	d a list of acceptable Re	direct URIs. T	hese must be the full enrollment URL
	- + "/aooale", su	ch as https://test71.clou	dpath.net/enr	oll/Regression/Test/google, Multiple
	URIs may be sr	pecified, with one per lin	e.	
	Based on the c	urrent deployment locati	ons, the Redi	rect URIs should be:
	https://anna/	11.cloudpath.net/enr	oll/AnnaTes	t/Production/google
		rateroupputnited/enty		s, i i saaction, googla

- 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.



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

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

. 7

#### FIGURE 7. Enrollment System Workflow

Workflow New	Configuration View: Workflow Look & Feel Properties	×
A workflow defir of messages to Each item belov	es the sequence a user must go through to register and connect to the network. This includes the display the user, the acceptance of use policies, and authentication of the user and/or device. I represent a step within the process. To add additional steps, click the insert arrow on the left side of row.	
Step 1:	Require the user to accept the AUP Welcome Message and AUP $\mathscr{A}$ X Q.	
Step 2:	Split users by: Visitors Employees $\times \mathscr{J}$ Partners $\mathscr{I} \equiv \times Q$	
Step 3:	Authenticate the user via Gmail	
Step 4:	Split users by: Internet-Only X J Internal Access	
Step 5:	Prompt the user for a voucher from Partner Internal Access Vouchers	
Step 6:	Display the message Contractor Welcome Message	
Result:	End of process. No network or certificate assigned.	

#### **User Experience**

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

FIGURE 8. User Prompt for Google Authentication



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

8

## Terminology

The following table defines terminology for the Google authentication feature.

Term	Definition
Client ID	The ID that Google assigns to your application.
Client Secret	The secret key that allows your app to capture the Google request objects.
Enrollment	The process of a user becoming authenticated and ultimately gaining network access.
Enrollment workflow	The sequence a user must go through to register and connect to the network.
Google app	A web application directly within Google that allows you to add Google capabilities to an external website.
Onboarding Wireless Network	An open wireless network that provides access to the Enrollment System.
Secure Wireless Network	A WPA2-Enterprise wireless network.
Third-Party Authentication	Allow access to a network using a secure login through an outside application.

TABLE 1. Third-Party Authentication Terminology

## **About Cloudpath**

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the XpressConnect Enrollment System and how it can simplify your wireless environment, visit <u>www.cloudpath.net</u> or contact a Cloudpath representative.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

## **Contact Information**

General Inquiries: info@cloudpath.net

Support:support@cloudpath.net

Sales:sales@cloudpath.net

Media:media@cloudpath.net

Marketing:marketing@cloudpath.net

Phone:+1 303.647.1495 (US) +1 866.472.6053 (US) +44 (01) 161.261.1400 (UK) Fax:+1 760.462.4569 Address:1120 W 122nd Ave, Suite 302 Westminster, CO 80234 USA