

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.

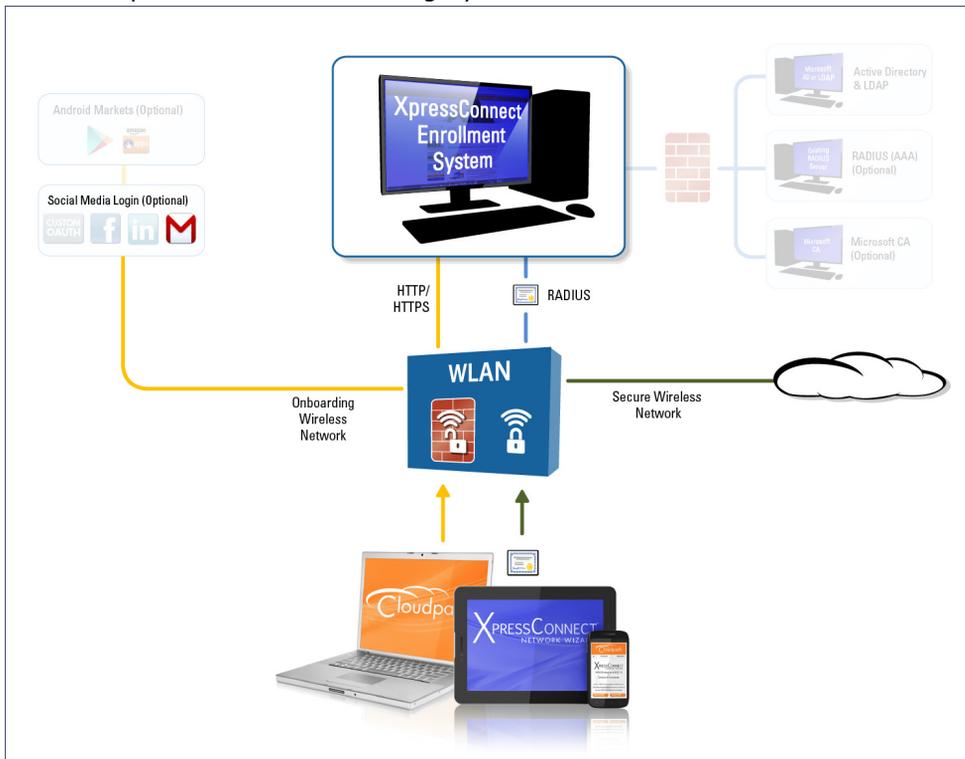
Setting Up Third-Party Authentication Within the XpressConnect Enrollment System Using Google™

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

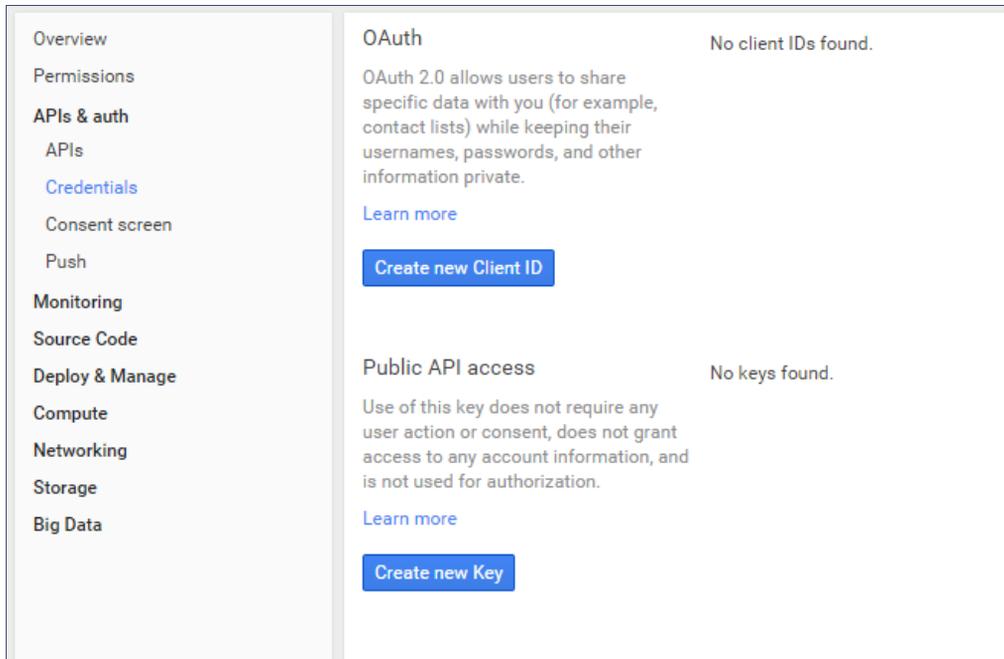
1. Go to <https://console.developers.google.com>.
2. Sign in to your Google account.
3. On the *Developers Console*, create and name an API Project. A *Project ID* is automatically assigned. If you already have an API project for this web application, continue to the next step.
4. Open the API project.

Note >>

You may be asked to complete an SMS verification process.

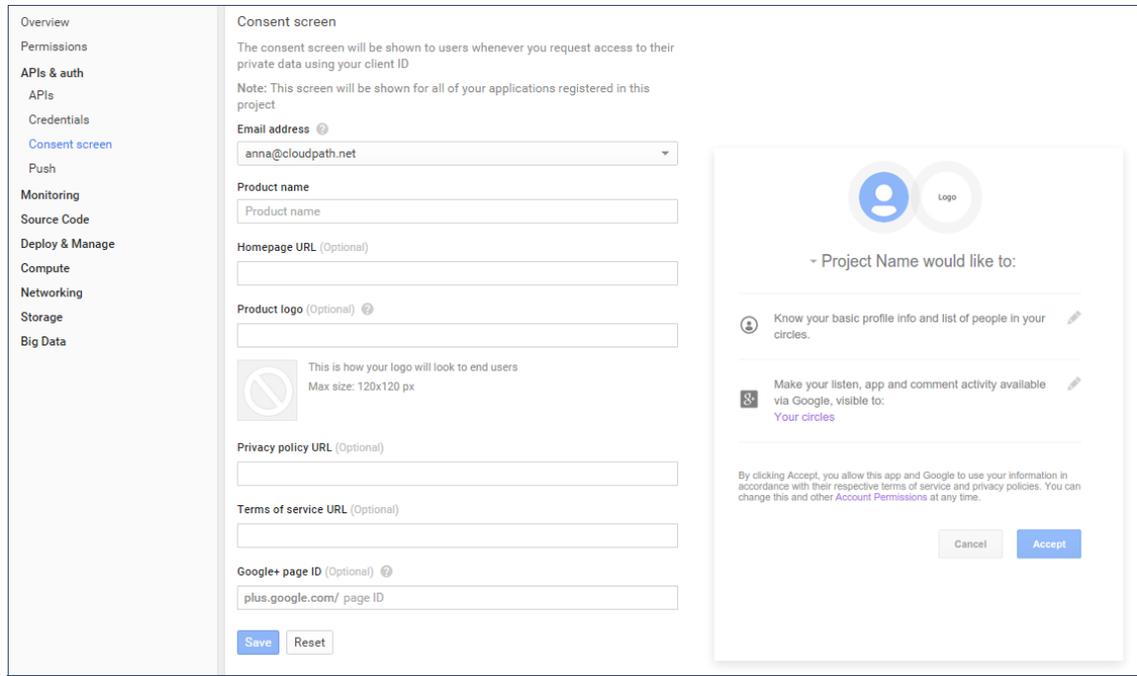
5. Go to the left-menu *APIs & auth > Credentials > OAuth* and click *Create new Client ID*. A *Client ID* is required for the Enrollment System web application.

FIGURE 2. Google Developers OAuth Create Client ID



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.

FIGURE 3. Consent Screen



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

8. Click *Save* to create the Client ID.

FIGURE 4. Create Client ID

Create Client ID

Application type

Web application
Accessed by web browsers over a network.

Service account
Calls Google APIs on behalf of your application instead of an end-user. [Learn more](#)

Installed application
Runs on a desktop computer or handheld device (like Android or iPhone).

Authorized JavaScript origins
Cannot contain a wildcard (`http://*.example.com`) or a path (`http://example.com/subdir`).

https://www.example.com

Authorized redirect URIs
One URI per line. Needs to have a protocol, no URL fragments, and no relative paths. Can't be a public IP Address.

https://www.example.com/oauth2callback

Create Client ID Cancel

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.

FIGURE 5. Client ID Information

The screenshot shows the Google Cloud Platform console interface for a web application. On the left is a navigation menu with options like Overview, Permissions, APIs & auth, and Credentials. The main content area is divided into three sections: OAuth, Client ID for web application, and Public API access. The OAuth section explains that OAuth 2.0 allows users to share data while keeping their information private. The Client ID for web application section displays a table with the following information:

Client ID for web application	
Client ID	301727419082-ist72gi62rom6deq8u9oqv6vhne3hpj.apps.googleusercontent.com
Email address	301727419082-ist72gi62rom6deq8u9oqv6vhne3hpj@developer.gserviceaccount.com
Client secret	IF0orBj_8nvdBwH2hX3FIW_K
Redirect URIs	https://www.example.com/oauth2callback
JavaScript origins	https://www.example.com

Below the table are buttons for 'Edit settings', 'Reset secret', 'Download JSON', and 'Delete'. The Public API access section indicates 'No keys found.' and includes a 'Create new Key' button.

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.

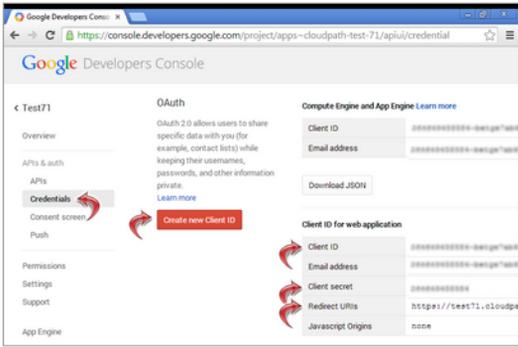
4. Enter the *Name* and *Description* of this configuration.

FIGURE 6. Third-Party Authentication Setup - Google

Google Configuration

Google Supported?

Instructions: The Google Developer's Console is available at <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://anna41.cloudpath.net/enroll/AnnaTest/Production/google>

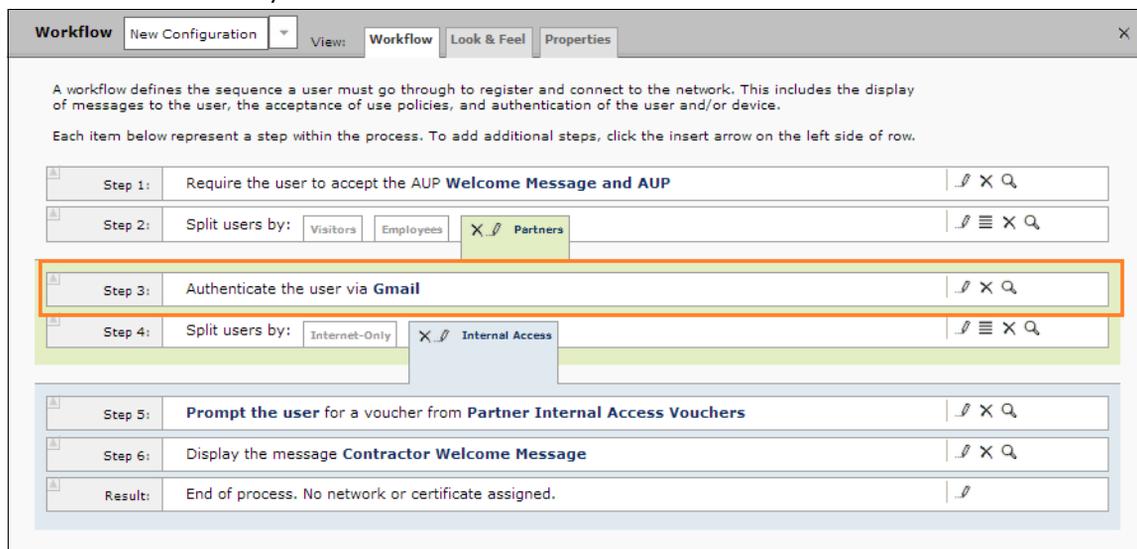
5. In the Google Configuration section, check the *Google Supported?* box.
6. Read the instructions for creating a client key. Be sure that the URI in the Google application matches the instructions on this page.
7. Enter the *Client ID* and *Client Secret* from the Google application.

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.

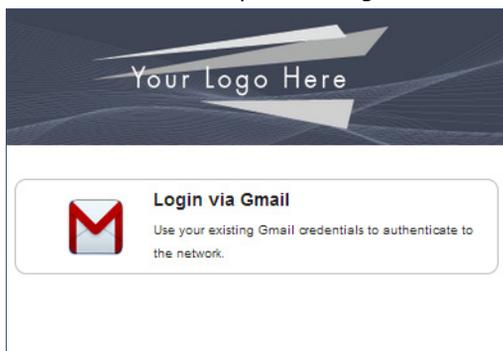
FIGURE 7. Enrollment System Workflow



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.

Terminology

The following table defines terminology for the Google authentication feature.

TABLE 1. Third-Party Authentication Terminology

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.

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 www.cloudpath.net 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