



How to social login with Aruba controller

Bo Nielsen, CCIE #53075 (Sec)

December 2016, V1.00

Overview

This short document describes the basic setup for social login using Aruba ClearPass and Aruba wireless LAN controller.

- Aruba ClearPass, version 6.6.2.86786
- Aruba wireless LAN controller 7005, version 6.4.4.8

The Aruba ClearPass (CP) offers guest login with or without MAC caching and self-provisioning where the end user is allowed to create a guest account with a time limit. Another solution is to offer guest access using a social login.

A screenshot of the Aruba login page. At the top, the Aruba logo is displayed in orange. Below it, a light blue banner contains the text "Please login to the network using your username and password." In the center, there is a "Login" form with a blue header. The form contains two input fields: "Username:" and "Password:", each followed by a text box. Below these fields is a "Log In" button. At the bottom of the form, there is a link that says "Contact the master of Infoblox if it does not work." Below the link is a red button with the Google+ logo and the text "Google+".

This is how it goes:

1. The user connects to an open wireless network.
2. The initial role on the Aruba wireless controller is set to use captive portal and the settings for this captive portal points to an URL. This URL uses a dedicated web page on the CP.
3. The web page on the CP is configured to use social login.
4. The webpage can also use guest accounts on the CP or users from an external database like Windows AD (option).
5. If the user clicks on the social login button (in this example Google+), the user is instructed to enter the username and password for the Google account.
6. The user is authenticated and the MAC address for the user's endpoint is updated to status *Known* and some extra attributes for the Google login are added.
7. The user can then use the wireless network until the session expires, then a new login from the social network is required.

The easy part is the wizard for social login and guest access role.

The difficult part is the Google API...

The web page for social login

Login to ClearPass Guest.

ClearPass Guest -> Configuration -> Pages-> Web Logins -> Create a new web login page

1. Enter a name for the web page in the *Name* field.
2. Enter the page name (use for captive portal configuration) in the *Page Name* field.
3. Enter a short description in the *Description* field (option).
4. Use the default setting for Aruba wireless LAN controller.

Web Login Editor	
* Name:	<input type="text" value="Social-login"/> <small>Enter a name for this web login page.</small>
Page Name:	<input type="text" value="google"/> <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	<input type="text" value="Google+ authentication"/> <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	<input type="text" value="Aruba Networks"/> <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	<input type="text" value="Controller-initiated — Guest browser performs HTTP form submit"/> <small>Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.</small>
* Address:	<input type="text" value="securelogin.arubanetworks.com"/> <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	<input type="text" value="Use vendor default"/> <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small>

5. Enable *Set Prevent CNA* in order to avoid an error from Google API saying that "This user-agent is not permitted to make OAuth authorization request to Google..."

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:	<input type="text" value="Credentials — Require a username and password"/> <small>Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.</small>
Prevent CNA:	<input checked="" type="checkbox"/> Enable bypassing the Apple Captive Network Assistant <small>The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.</small>
Custom Form:	<input type="checkbox"/> Provide a custom login form <small>If selected, you must supply your own HTML login form in the Header or Footer HTML areas.</small>
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages <small>If selected, you will be able to alter labels and error messages for the current login form.</small>
* Pre-Auth Check:	<input type="text" value="None — no extra checks will be made"/> <small>Select how the username and password should be checked before proceeding to the NAS authentication.</small>
Terms:	<input type="checkbox"/> Require a Terms and Conditions confirmation <small>If checked, the user will be forced to accept a Terms and Conditions checkbox.</small>

6. Set the *Pre-Auth Check* to **None - no extra checks will be made**.

How to social login with Aruba controller

7. Under *Social Logins*, select **Enable login with social network credentials**.
8. Click on **Add new authentication provider**.
9. Select *Google* from the list.
10. Enter a short random number in *Client ID* and *Client Secret* (we come back to that later).
11. Click on **Add**.
12. Copy the text for *Buttons*, here `{nwa_social_logins}`

Social Logins					
Optionally present guests with various social login options.					
Social Login:	<input checked="" type="checkbox"/> Enable login with social network credentials				
Authentication Providers:	<div> Add new authentication provider </div> <table border="1"> <thead> <tr> <th>Provider</th> <th>Client ID</th> </tr> </thead> <tbody> <tr> <td>✓ Google</td> <td>823710716977 [REDACTED]</td> </tr> </tbody> </table>	Provider	Client ID	✓ Google	823710716977 [REDACTED]
Provider	Client ID				
✓ Google	823710716977 [REDACTED]				
Buttons:	<p>To display social network login buttons, add the following to the Header HTML or Footer HTML area.</p> <div><code>{nwa_social_logins}</code></div> <p>Refer to the help for more details.</p>				
Debug:	<input type="checkbox"/> Log debugging data				

13. Paste the text in the Header HTML or Footer HTML (here the footer part)

Footer HTML:	<pre> {nwa_text id=7979}<p> Contact the prophet of Infoblox if it does not work. </p>{/nwa_text} {nwa_social_logins}
 </pre> <div>Insert...</div>
--------------	---

HTML template code displayed after the login form.

14. Click the **Save Changes**.

Next is the configuration on the Aruba wireless LAN controller.

Configure the Aruba controller

The this example the wizard for campus WLAN is completed. We have a SSID, "Guest", and no use of MAC authentication. The first part is to create a captive portal and a new user role. This role will use captive portal and allow access to Google before the final authentication takes places. The end user must have access to Google in order to be authenticated externally.

In this example I have used the role *social-login*.

First it is important, that the Aruba LAN controller can do DNS lookup.

Configuration -> NETWORK -> IP -> IP Routes & DNS

Enter the IP address(es) for DNS.

The screenshot shows the Aruba Cloud Services Controller configuration interface for an Aruba7005. The left sidebar contains a navigation menu with categories: WIZARDS, NETWORK, SECURITY, WIRELESS, and MANAGEMENT. The 'IP' option under NETWORK is selected. The main content area is titled 'Network > IP > IP Routing' and has tabs for 'IP Interfaces', 'IP Routes & DNS' (which is active), 'IPv6 Neighbors', 'GRE Tunnels', 'NAT Pools', and 'DHCP Server'. Under 'IP Routes & DNS', there are sections for 'Default Gateway' and 'Domain Name Servers'. The 'Default Gateway' section has a 'Static' tab with an 'IP Address' field containing '10.100.200.1' and an 'Add' button. Below it is a 'Dynamic' section with checkboxes for 'DHCP, cost: 10', 'PPPoE, cost: 10', and 'Cellular, cost: 10'. The 'Domain Name Servers' section is highlighted with a red box and contains an 'IP Address' field with '10.100.100.36' and a 'New' button.

The good thing is that there is already an alias for *Auth-Google* under:

Configuration -> ADVANCED SERVICES -> Stateful Firewall -> Destination

This alias is used for access to Google authentication for the initial role **social-login**.

Create the captive portal

The captive portal configuration uses the Aruba ClearPass web page, that you just created.

Configuration -> SECURITY -> Authentication -> L3 Authentication

Click on (+) for *Captive Portal Authentication*, enter a name and click **Add**.

The essential part is to:

- De-select use for *Logout popup window*
- De-select *Show Welcome Page*
- Enter the full URL in *Login page*, here "https://clearpass.credocom.dk/guest/google.php"

User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>
Logout popup window	<input type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>
Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec
logon wait CPU utilization threshold	60 %
Max Authentication failures	0
Show FQDN	<input type="checkbox"/>
Authentication Protocol	PAP
Login page	ocom.dk/guest/google.php
Welcome page	/auth/welcome.html
Show Welcome Page	<input type="checkbox"/>
Add switch IP address in the redirection URL	<input type="checkbox"/>

Click on **Apply**.

Remember to select the RADIUS server group under *Server Group* for captive portal setting.

Security > Authentication > L3 Authentication

Servers	AAA Profiles	L2 Authentication	L3 Authentication	User Rules	Advanced				
<div> <div> <div>Captive Portal Authentication</div> <div> <div>CPPM_CaptivePortal</div> <div> <div>Server Group</div> <div>Clearpass</div> </div> </div> </div> <div> <div>default</div> <div>Guest-cp_prof</div> <div>OnBoarding</div> <div>OnGuard</div> </div> </div>									
<div> <div>Server Group > Clearpass</div> <div> <div>Fail Through</div> <div>Load Balance</div> </div> <div> <div>Servers</div> <table border="1"> <thead> <tr> <th>Name</th> <th>Server-Type</th> </tr> </thead> <tbody> <tr> <td>CP78</td> <td>Radius</td> </tr> </tbody> </table> <div> <div>New</div> <div>▲</div> <div>▼</div> <div>Delete</div> </div> </div> </div>						Name	Server-Type	CP78	Radius
Name	Server-Type								
CP78	Radius								

If no RADIUS server group can be selected, you have to create a RADIUS under:

Configuration -> SECURITY -> Servers

How to social login with Aruba controller

Create the init role for social login

Configuration -> SECURITY -> Access Control -> User Roles -> Add

Enter name for the user role, here *social-logon*.

Select the captive portal under Captive Portal Profile.

Misc. Configuration

Re-authentication Interval	0 minutes (0 disables re-authentication. A positive value enables authentication 0-4096)
Role VLAN ID	Not Assigned
VPN Dialer	Not Assigned
L2TP Pool	Not Assigned (default-l2tp-pool)
PPTP Pool	Not Assigned (default-pptp-pool)
Captive Portal Profile	CPPM_CaptivePortal
Captive Portal Check for Accounting	<input checked="" type="checkbox"/>
Max Sessions	65535 (0 - 65535)
idp profile name	none
Stateful NTLM Profile	Not Assigned
Stateful Kerberos Profile	Not Assigned
WISPr Profile	Not Assigned
Enable Deep Packet Inspection	<input checked="" type="checkbox"/>
Enable Web Content Classification	<input checked="" type="checkbox"/>

Add 4x access rules for this role (social-logon):

- HTTP and HTTPS access to the Aruba ClearPass server
- Access to Google, the default alias under stateful firewall destination
- *Logon-control* for DHCP and DNS
- *Captiveportal* (must be the last rule)

Firewall Policies Bandwidth Contracts

Name	Rule Count	Location
global-sacl	0	
apprf-social-logon-sacl	0	
Clearpass server	2	
Google-Auth	1	
logon-control	7	
captiveportal	6	

Add [Up] [Down] Delete

Next you have to modify the AAA profile to use this user role for initial access.

How to social login with Aruba controller

Modify the AAA profile

The final step on the Aruba wireless LAN controller is to use the newly created role for initial access.

Configuration -> SECURITY -> Authentication -> AAA profiles

Click on (+) for the guest ssid, here *Guest-aaa_prof*.

The most part of the configuration on the authentication can be seen or verified under:

1. Select the newly created role as *Initial role*.
2. No use of *MAC Authentication*
3. Select or verify the server group name for *RADIUS Accounting Server Group* (option).

Security > Authentication > Profiles

The screenshot shows the 'AAA Profiles' configuration page. On the left, a list of profiles includes 'default', 'default-dot1x', 'default-dot1x-psk', 'default-mac-auth', 'default-open', 'default-smi-api', and 'Guest-aaa_prof'. The 'Guest-aaa_prof' profile is selected and highlighted with a red box. Below it, the 'MAC Authentication' checkbox is unchecked. The 'RADIUS Accounting Server Group' is set to 'Guest_srvgrp-rt51'. On the right, the 'AAA Profile > Guest-aaa_prof' configuration is shown. The 'Initial role' is set to 'social-logout'. The 'MAC Authentication Default Role' is set to 'guest'. The '802.1X Authentication Default Role' is set to 'guest'. The 'Download Role from CPPM' checkbox is unchecked. The 'L2 Authentication Fail Through' checkbox is unchecked. The 'Multiple Server Accounting' checkbox is unchecked. The 'User idle timeout' is set to 2 seconds. The 'Max IPv4 for wireless user' is set to 2. The 'RADIUS Interim Accounting' checkbox is unchecked. The 'User derivation rules' are set to '--NONE--'.

That's it!

Next step is the wizard on Aruba ClearPass for social authentication.

Configure the ClearPass

Login to ClearPass Policy Manager.

ClearPass Policy Manager -> Configuration -> Start Here

UseGuest Social Media Authentication



Guest Social Media Authentication

To authenticate guest users logging in via captive portal with their social media accounts. Guests must re-authenticate after their session ends.

Enter the few parameters for the step-by-step wizard, and in this example only Google is used.

Service Templates - Guest Social Media Authentication

General	Wireless Network Settings	Guest Access Restrictions
Enable the days on which the guest users are allowed network access; enter the maximum bandwidth allowed per user		
Social login Provider*:	<input checked="" type="checkbox"/> Google <input type="checkbox"/> Facebook <input type="checkbox"/> LinkedIn <input type="checkbox"/> Twitter	
Days allowed for access*:	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday	
Maximum bandwidth allowed per user*:	<input type="text" value="0"/> MB (For unlimited bandwidth, set value to 0)	

The wizard creates:

- 1x Service
- 1x Enforcement policy
- 6x Enforcement profiles

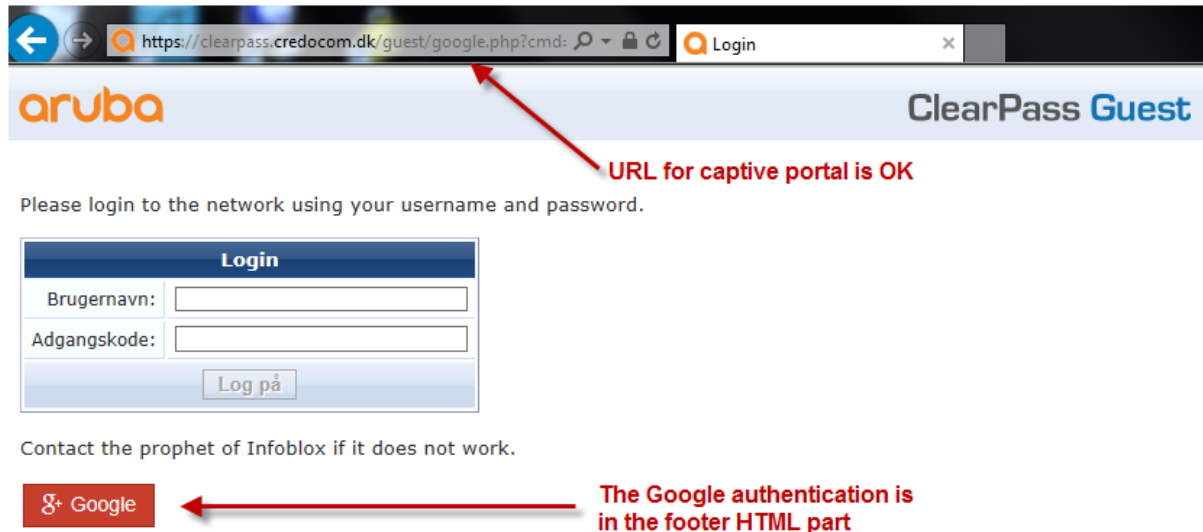
The essential part of the profiles is the session-timeout.

Filter:

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	Google Guest Bandwidth Limit	Post_Authentication	System-defined profile to set Guest bandwidth limits
2.	<input type="checkbox"/>	Google Guest Do Expire	Post_Authentication	Enforcement profile for Guest do expire functionality
3.	<input type="checkbox"/>	Google Guest Expire Post Login	Post_Authentication	Enforcement profile for Guest expire post login functionality
4.	<input type="checkbox"/>	Google Guest MAC Caching	Post_Authentication	System-defined profile to update the endpoint with Guest user details
5.	<input type="checkbox"/>	Google Guest Session Limit	Post_Authentication	System-defined profile to set concurrent Guest session count
6.	<input type="checkbox"/>	Google Guest Session Timeout	RADIUS	

Short verification before Google API

Before going on to the Google API you may verify that redirection takes place.



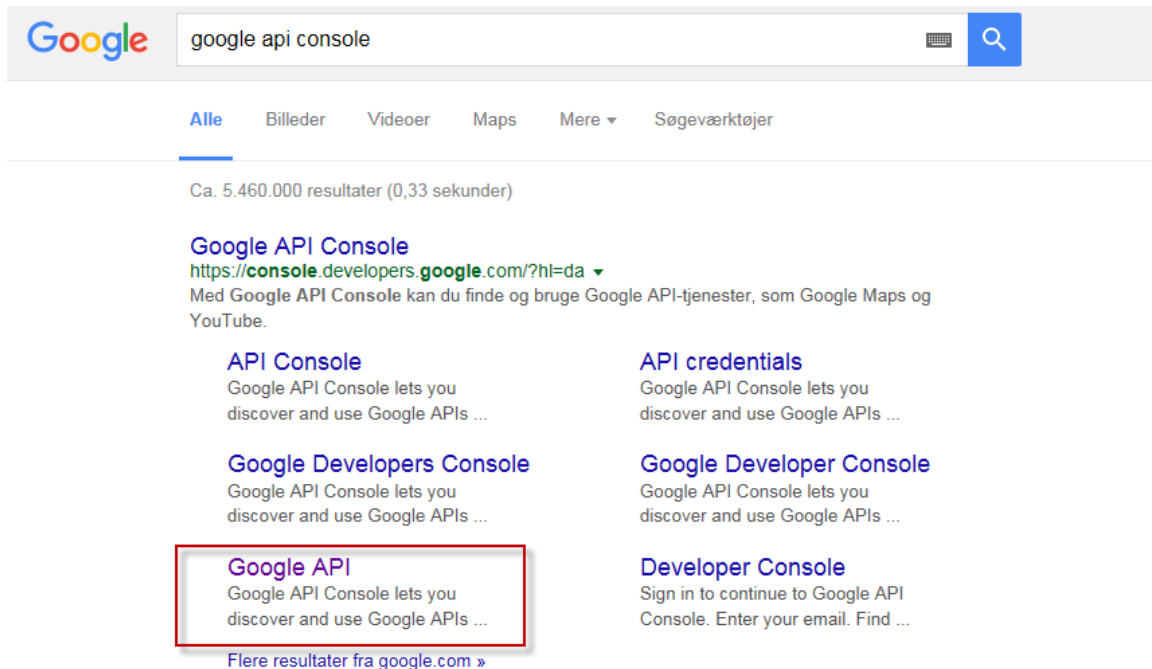
Right, you got it!

Google API configuration

The goal is to create a Client ID and a Client Secret using the Google API.

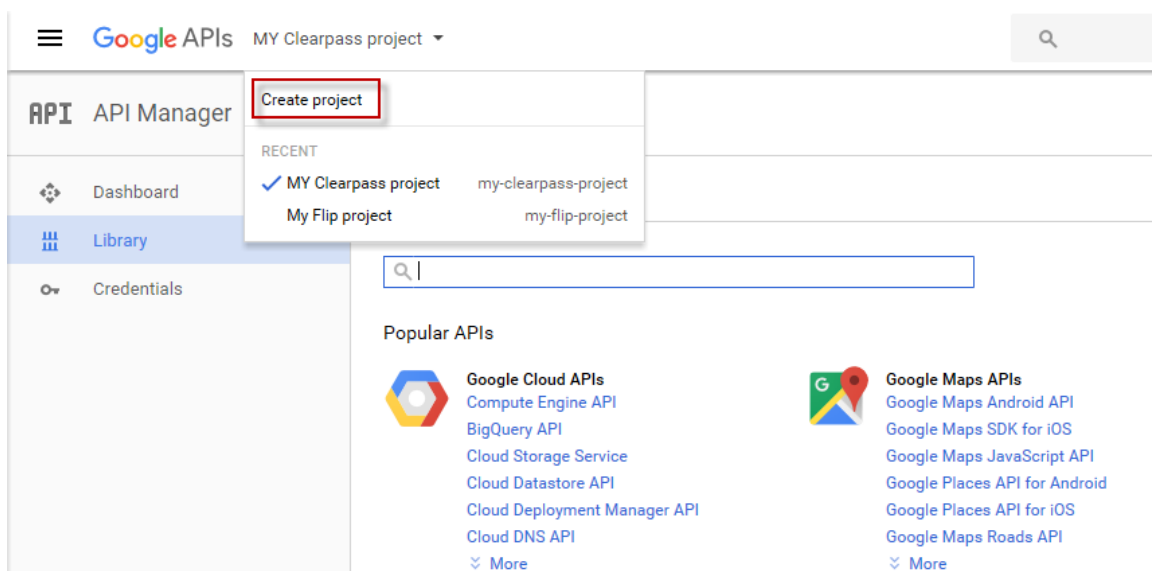
First you must have a Google account.

Start the web browser and the easiest way is to search for "Google api console".



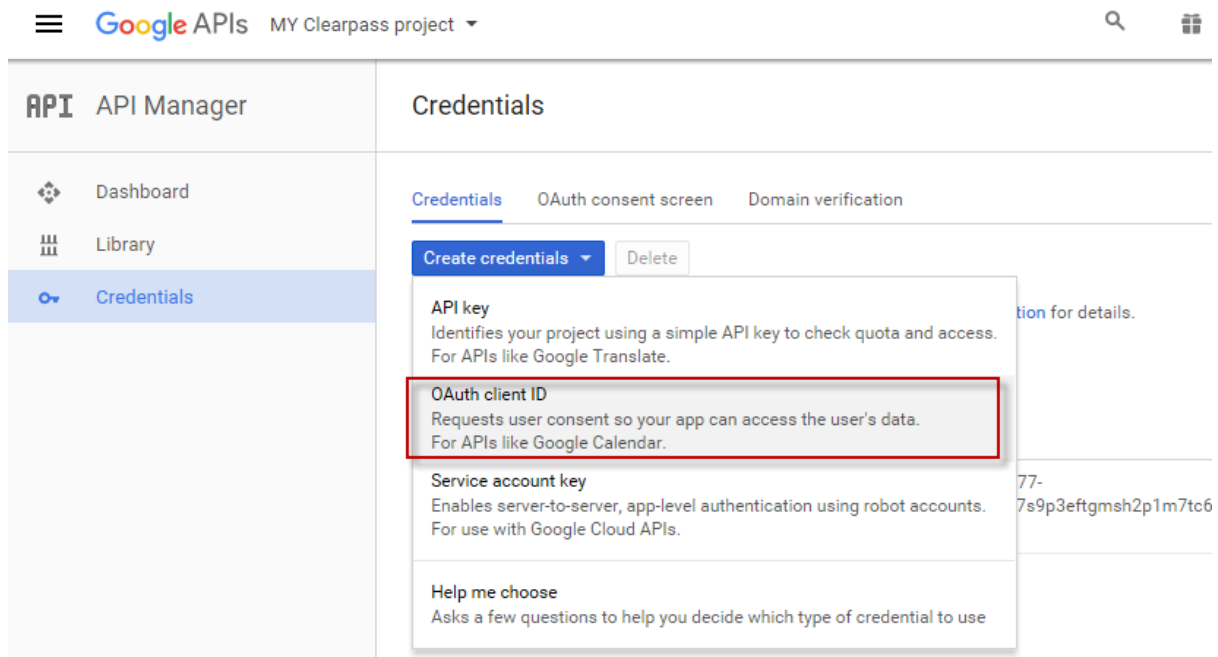
Click on **Google API**.

Login using your own Google account. Create a project, and here I have created "MY Clearpass project".



1. Click on **Credentials**.
2. Click on **Create credentials**.

3. Select **OAuth client ID**.



4. Select **Web application** from the list.

5. Enter a name for the credentials.

- Enter the URL for the web page that is used for captive portal.

Google APIs MY Clearpass project

API Manager

Dashboard
Library
Credentials

Credentials

←

Create client ID

Application type

☒ Web application
☐ Android [Learn more](#)
☐ Chrome App [Learn more](#)
☐ iOS [Learn more](#)
☐ PlayStation 4
☐ Other

Name

Clearpass

Restrictions
Enter JavaScript origins, redirect URIs, or both

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (http://*.example.com) or a path (http://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

http://www.example.com

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://clearpass.credocom.dk/guest/google.php

Create Cancel

- Click **Create**.

A new window pops up with the Client ID and Client secret.

OAuth client

Here is your client ID

823710716977-jsphbjqmik6mukp

Here is your client secret

x9vE

OK

Copy these string values into notepad or a text editor. Save the file for later use, if required.

Logout from the Google API.

How to social login with Aruba controller

Finally you must add the *Client ID* and *Client secret* to the web page on ClearPass.

Login to ClearPass Guest.

ClearPass Guest -> Configuration -> Pages-> Web Logins

Edit the web page for social login.

Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for





Use this list view to define new web login pages, and to make changes to existing web login pages.

➔ Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

△ Name	Page Title	Page Name	Page Skin
 login Captive Portal for Aruba Instant AP		login	(Default)
 OnGuard Portal		OnGuard	(Default)
 Social-login Google+ authentication		google	(Default)
3 web logins 			Show all rows ▾

Under *Social Logins*, click on *Google* and select **Edit**.

Copy-and-paste the *Client ID* and *Client Secret*, click on **Update**.

Provider	Client ID
 Google	823710716977-ruobkfvc14a7s9p3eftgmsh2p1m7tc6d.apps.googleusercontent.com
 Edit  Disable  Delete	
Use the form below to modify the authentication provider.	
Properties	
* Provider:	Google ▾
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	823710716977-ruobkfvc14a7s9p3eftgmsh2p1m7tc6d.apps.googleusercontent.com The Client ID associated to your provider. They may use a different label.
* Client Secret:	x9vEF-ruobkfvc14a7s9p3eftgmsh2p1m7tc6d.apps.googleusercontent.com The Client Secret associated to your provider. They may use a different label.

Click on **Save Changes**.

Well done!

Verification using Tracker

Bring a device on the wireless guest network.

Redirecting should happen due to the initial role on the Aruba wireless LAN controller.

Click on the Google+ button.


Enter the Google credentials, and you are done.

Server	Source	Username	Service	Login S
10.100.200.78	RADIUS	Regnar Ingversen	Google Guest Social Media Authentication	ACCEPT

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000498-10-5842abbe		
Date and Time:	Dec 03, 2016 12:25:50 CET		
End-Host Identifier:	0013E880F5C5 (Computer / Windows / Windows)		
Username:	Regnar Ingversen		
Access Device IP/Port:	10.100.200.102:0 (WLC7005 / Aruba)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	Google Guest Social Media Authentication		
Authentication Method:	PAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Social Login Repository]		
Roles:	[Employee], [Machine Authenticated], [User Authenticated], google		
Enforcement Profiles:	Google Guest Bandwidth Limit, Google Guest Session Limit, Google Guest MAC Caching, [Update Endpoint Known], Google Guest Do Expire, Google Guest Expire Post Login, [Allow Access Profile], Google Guest Session Timeout		

Take a look for the endpoint under *Configuration -> Identity -> Endpoints*

Status is set to *Known* (if you want to use MAC authentication).

Endpoint	Attributes	Fingerprints	Policy Cache
MAC Address	0013e880f5c5	IP Address	10.100.200.178
Description		Static IP	FALSE
Status	<input checked="" type="radio"/> Known client <input type="radio"/> Unknown client <input type="radio"/> Disabled client	Hostname	oem
MAC Vendor	Intel Corporate	Device Category	Computer
Added by	Policy Manager	Device OS Family	Windows
Online Status	 Online	Device Name	Windows
Connection Type	Wireless	Added At	Nov 25, 2016 15:05:31 CET
		Updated At	Dec 03, 2016 12:20:57 CET

The attributes are also set:

Endpoint		Attributes	Fingerprints	Policy Cache
Attribute		Value		
1.	Guest Role ID	= %{GuestUser:Role ID}		
2.	Username	= Regnar Ingversen		
3.	social_args	= { "page_name": "google", "oauth": "google", "state": "1480764348-f94c6d", "code": "4V65djil31lEr7CRObIF8xLNahSQinwcnZJyzuEbsjrxI" }		
4.	social_json	= { "kind": "plus#person", "etag": "\"FT7X6cYw9BSnPtiywEFNNGVVdioVMTzIC7QmhXs2twf-7ft0jWVB\\\"", "objectType": "person", "id": "111762725469942756632", "displayName": "Regnar Ingversen", "name": { "familyName": "Ingversen", "givenName": "Regnar" }, "url": "https://plus.google.com/V/111762725469942756632", "image": { "url": "https://lh5.googleusercontent.com/V-9PZgNd8hD2VAAAAAAAAAAI/AAAAAAAAAHwV819H1v-tT_A/photo.jpg?sz=50", "isDefault": false }, "isPlusUser": true, "language": "da", "circledByCount": 0, "..." }		
5.	social_method	= google		
6.	social_password	= [REDACTED]		
7.	social_timestamp	= 1480764349		
8.	social_username	= Regnar Ingversen		
9.	social_vip	=		
10.	Click to add...			

Note: The social_password and social_username can be use for login, but the end user have no clue about the random password here in clear text.

On the Aruba wireless LAN controller the user role switch from *social-login* to *guest*.

Before login

Controller > Clients

Clients							
Search Results							
Clients							
	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
C		Win 7	00:13:e8:80:f5:c5	10.100.200.178	social-login		Guest

After login

Controller > Clients

Clients							
Search Results							
Clients							
	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
C	Regnar Ingversen	Win 7	00:13:e8:80:f5:c5	10.100.200.178	guest	Captive Portal	Guest

The role guest is set by the Aruba controller under the AAA profile, because the RADIUS profile on ClearPass does not return a role.

You can add a user role on the Aruba wireless LAN controller when authenticated, and add the attribute Aruba-user-role to the RADIUS profile for social login.

Add-on to the setup

If you also wants guest access, I have used this:

Add the Guest User Repository to the authentication service.

Services - Google Guest Social Media Authentication

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods:				
		[PAP] [MSCHAP] [CHAP]	Move Up Move Down Remove View Details Modify	
		--Select to Add--		
Authentication Sources:				
		[Guest User Repository] [Local SQL DB] [Social Login Repository] [Local SQL DB]	Move Up Move Down Remove View Details Modify	

Create a RADIUS profile with an Aruba role used for guest users created on ClearPass. The role must also exist on the Aruba wireless LAN controller.

Enforcement Profiles - Guest access profile

Summary	Profile	Attributes
Profile:		
Name:	Guest access profile	
Description:	Return "MYROLE"	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= MYROLE

Finally, modify the enforcement policy from the wizard.

Summary	Enforcement	Rules
Enforcement:		
Name:	Google Guest Social Media Authentication Enforcement Policy	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
Rules:		
Rules Evaluation Algorithm: First applicable		
Conditions	Actions	
1. (Authorization:[Guest User Repository]:AccountEnabled EQUALS true) AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false)	Guest access profile	
2. (Authorization:[Social Login Repository]:SocialSP EQUALS google)	[Allow Access Profile]	
3. (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	Google Guest Session Guest MAC Caching, [Login]	