

Grandstream Networks, Inc.

Captive Portal Authentication via Facebook





Table of Content

SUPPORTED DEVICES	4
INTRODUCTION	5
CAPTIVE PORTAL SETTINGS	6
Policy Configuration Page	6
Landing Page Redirection	8
Pre-Authentication Rules	8
Post-Authentication Rules	8
Files Configuration Page	9
Clients Page	10
CONFIGURATION STEPS	11
Create Facebook App	11
Configure Captive Portal Policy with Facebook Authentication	13
Assign Captive Portal Policy to Network Groups and SSIDs	16
Facebook analytics	18





Table of Figures

Figure 1: General Architecture	5
Figure 2: Captive Portal web GUI menu	6
Figure 3: Files Web Page	9
Figure 4: Client Web Page	10
Figure 5: Facebook Dev - Add product	11
Figure 6: Facebook Login Settings	12
Figure 7: Make Facebook App Public	12
Figure 8: Facebook Developers Dashboard	13
Figure 9: Captive Portal Policy Sample Configuration	14
Figure 10: Pre-Authentication Rules for Facebook Authentication	15
Figure 11: Enable Captive Portal on WiFi Settings	16
Figure 12: Login via Facebook Portal	17
Figure 13: Facebook Login	17
Figure 14: Facebook Analytics	18

Table of Tables

Table 1: Supported Devices	.4
Table 2: Policy Configuration Page	.7
Table 3: Pre-Authentication Rules for Facebook Authentication1	14





SUPPORTED DEVICES

Following table shows Grandstream devices supporting Captive Portal with Facebook Authentication feature:

Table 1: Supported Devices				
Model	Supported	Firmware		
GWN7610	Pending	Pending		
GWN7600	Yes	1.0.3.19 or higher		
GWN7600 LR	Yes	1.0.4.12		
GWN7000	Pending	Pending		





INTRODUCTION

Captive Portal feature on GWN760X Access Points allows to define a Landing Page (Web page) that will be displayed on WiFi clients' browsers when attempting to access Internet.

Once connected to GWN760X AP, WiFi clients will be forced to view and interact with that landing page before Internet access is granted.

Captive portal can be used in different environments including airports, hotels, coffee shops, business centers and others offering free WiFi hotspots for Internet users.

This guide describes how to setup the captive portal feature on the GWN760X series using Facebook Authentication.

The following figure illustrates an example of the landing page feature using Facebook authentication.

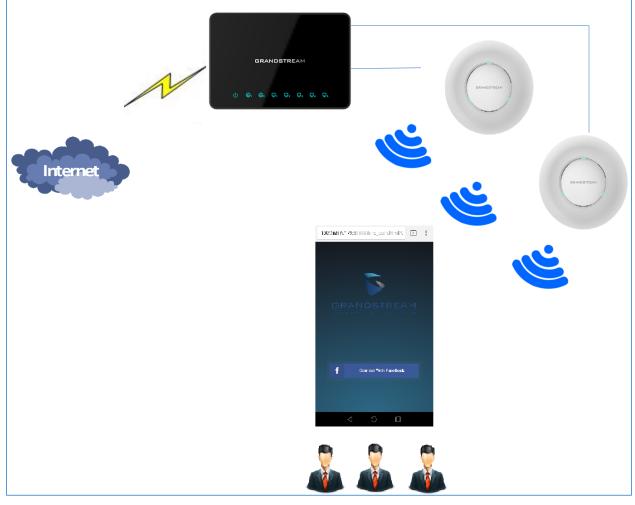


Figure 1: General Architecture





CAPTIVE PORTAL SETTINGS

The Captive Portal feature can be configured from the GWN760X web page, by navigating to "**Captive Portal**".

The page contains three tabs: **Policy**, **Files** and **Clients**.

- **Policy Tab**: In this page, users can configure multiple portal policies which then can be assigned to specific network groups under the menu "**Network Groups**". (For example having non-authentication based portal for temporary guests and setting up an authentication based portal policy for the internal staff).
- **Files Tab**: Under this tab, users could download and upload customized portal landing page to display to the users when they try to connect over the WiFi.
- Clients Tab: This tab lists the authenticated clients MAC addresses.

Overview	Captive Portal				
Access Points	Policy	Files	Clients		
Network Group 🔻	+ Add				
Clients	Name	Authentication Type	Expiration(s)	Portal Page Customization	Actions
Captive Portal	grandstream	Radius Server	3600	/portal_pass.html	
Bandwidth Rules					
System Settings 🔻					



Policy Configuration Page

The Policy configuration allows users to configure and customize different captive portal policies which then can be selected on network group configuration page, giving the admin the ability to set different captive portals for each network group.

The following table describes all the settings on this page:





	Table 2: Policy Configuration Page			
Field	Description			
Name	Enter a name to identify the created policy (ex: Guest Portal).			
Expiration	Enter the expiration time for user authentication, this field must contain an integer and set the unit to seconds, minutes, hours and days. If this field is set to 0 the landing page will never expire.			
	Three types of authentication are available:			
Authentication Type	• No Authentication: when choosing this option, the landing page feature will not provide any type of authentication, instead it will prompt users to accept the license agreement to gain access to internet.			
	• RADIUS Server: Choosing this option will allow users to set a RADIUS server to authenticate connecting clients.			
	• Third Authentication: Choosing this option will allow users to log in using WeChat or Facebook. We will be using this authentication type on this guide.			
Facebook Authentication	Check this box to enable Facebook Authentication.			
Facebook App ID	Enter the app ID to use Facebook Login API.			
Facebook App Secret	Enter the app secret to use Facebook Login API.			
Line Default Devial Devia	When enabled, the default portal page will be used, otherwise users			
Use Default Portal Page	can upload their custom page.			
Portal Page Customization	 This option allows users to choose the landing page that will be shown once a client tries to connect to the GWN, three pages are available: Portal Default: This page is used when no authentication is specified, users will have only to accept license agreement to gain access to internet. 			
	 Portal Pass: This option provides authentication textbox when using RADIUS authentication mode, to enter username and password stored in RADIUS database. 			
	• Third Auth: Choose this page when using authentication via WeChat or Facebook.			
	Select page where authenticated clients will be redirected to.			
Landing Page	• Redirect to the original URL: Sends the authenticated client to the original requested URL.			
	• Redirect External Page: Enter URL that you want to promote to connected clients (ex: company's website).			
Redirect External Page LIRI	When setting the landing page to (Redirect External Page), enter			
Redirect External Page URL	the URL where to send authenticated clients.			







Enable HTTPS	Check this box to enable captive portal over HTTPS.
	From this menu, users can set matching rules to allow certain types
Pre-Authentication Rules	of traffic before authentication happens or simply allow the traffic for non-authenticated end points.
Post Authentication Rules	This tool can be used to block certain type of traffic to authenticated
	clients, anything else is allowed by default.
	(Ex: Settings a rule that matches HTTP will ban all authenticated
	clients to not access web server that are based on HTTP).

Landing Page Redirection

This feature can be configured using the option "Redirect External Page URL" under the policy settings, and could be useful in the case the network admin wants to force all connected guest clients to be redirected to a certain URL (ex: company's website) for promotion and advertisement purposes.

Note: Supported on GWN7600 and GWN7600LR Access Points only.

Pre-Authentication Rules

Using this option, users can set rules to match traffic that will be allowed for connected WiFi users before authentication process. This can be needed for example to setup Facebook authentication where some traffic should be allowed to Facebook server(s) to process the user's authentication. Or simply to be used to allow some type of traffic for unauthenticated users.

Note: Supported on GWN7600 and GWN7600LR Access Points only.

Post-Authentication Rules

On the other hand, post authentication rules are used to match traffic that will be banned for WiFi clients after authentication. As an example, if you want to disallow connected WiFi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that traffic and once a connected client passes the authentication process they will be banned from issuing telnet and SSH connections.

Note: Supported on GWN7600 and GWN7600LR Access Points only.





Files Configuration Page

Files configuration page allows to view and upload HTML pages and related files (images...).

The captive portal uses portal_default.html as default portal page. When using Facebook authentication,

users need to select **third_auth.html** as the portal page to let the user login via Facebook.

The following figure shows default files used for Captive Portal in GWN Access point.

	Select folder : /	▼ + Add	+ Upload +	
Overview	Name	Туре	Path	Actions
Access Points	images	Folder	/images	1
Network Group 🔻	background.jpg	File	/images/background.jpg	1
Captive Portal	icon_close.png	File	/images/icon_close.png	<u>c</u>
Bandwidth Rules	icon_close_selected.png	File	/images/icon_close_selected.png	C
System Settings 🔻	icon_facebook.png	File	/images/icon_facebook.png	C
	icon_wechat.png	File	/images/icon_wechat.png	1
	logo.png	File	/images/logo.png	1
	scanning.png	File	/images/scanning.png	1
	t.weixin.logo.png	File	/images/t.weixin.logo.png	1
	favicon.ico	File	/favicon.ico	1
	jquery.js	File	/jquery.js	1
	jquery.md5.js	File	/jquery.md5.js	1
	portal_default.html	File	/portal_default.html	1
	portal_pass.html	File	/portal_pass.html	1
	status.html	File	/status.html	1
	style.css	File	/style.css	1
Alert/Notification	third auth.html	File © 2017 Grands	/third auth.html tream Networks, Inc. All Rights Reserved	۳% 🕅

Figure 3: Files Web Page

- Click 🗹 to upload a new web page.
- Click Add Folder to add a new folder.
- Click ^(D) Upload to upload files to the selected folder.
- Folder can be selected from the dropdown list.

Select folder : /images





Clients Page

For Information Purposes Clients page lists MAC addresses of authenticated devices using captive portal. As we can see on the below figure, two WiFi clients have been authenticated and granted internet access from the GWN7610 access points:

- ✓ Client 1 → *E8:DE:27:0B:C1:E7*
- ✓ Client 2 → *DC:09:4C:A4:38:BE*

aptive Portal				
Policy	Files	Clients		
MAC Address	IP Addres	S	Remaining Time(s)	Authentication St
E8:DE:27:0B:C1:E7	192.168.6	5.248	3595	Authenticated
DC:09:4C:A4:38:BE	192.168.6	5.31	3595	Authenticated

Figure 4: Client Web Page





CONFIGURATION STEPS

In this section, we will provide all steps needed to use Captive Portal with Facebook authentication.

Create Facebook App

To use Facebook Login API, users need first to create an APP under developers' platform and set some OAuth settings to allow login authentication between GWN Access Points and Facebook servers.

We summarize in the following section the required steps:

- 1. Go to Facebook developers' platform: <u>https://developers.facebook.com/apps</u>
- 2. Login using your account and enter your phone number to receive verification code.
- 3. Create a new APP and give it a name (ex: GWN_Captive_Portal).
- 4. On the left bar, click on **+Add Product** to add Facebook login feature:

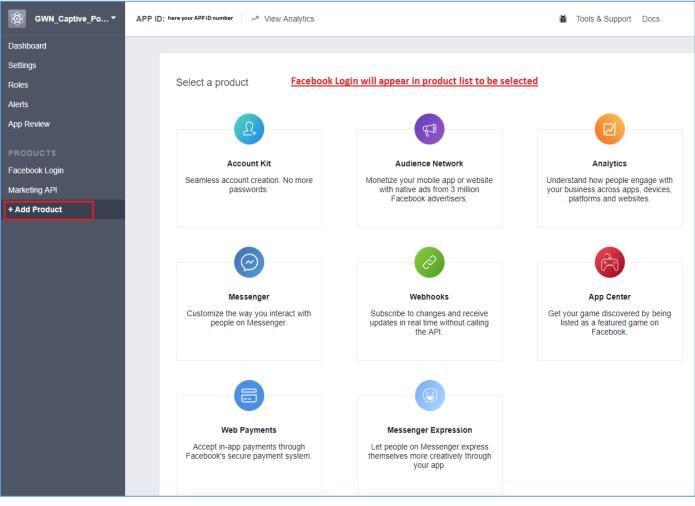


Figure 5: Facebook Dev - Add product





- Under Facebook Login settings, enter the valid OAuth redirect URIs to allow authentication requests from your access points. For each AP, note its IP address and make sure to enter two URIs per access point as following:
 - http://cwp.gwn.cloud:8080
 - https://cwp.gwn.cloud:8443

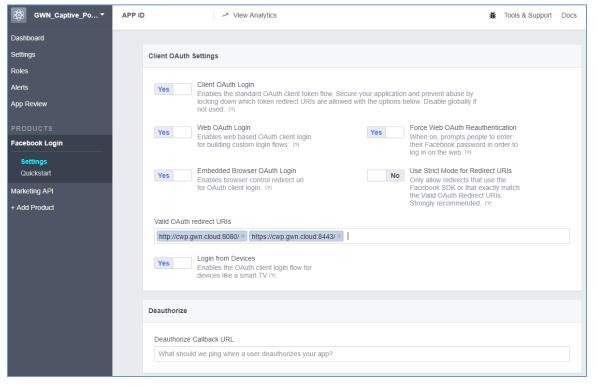


Figure 6: Facebook Login Settings

6. Press Save Changes.

facebook for developers	Disc	ard	Save Changes
<u> </u>			

7. Next, make sure to set the Facebook App public by going under **App Review** and settings it to Yes.

Dashboard	
Settings	Make GWN Captive Portal public?
Roles	
Alerts	Yes Your app is currently live and available to the public.
App Review	



 Finally, got to Dashboard page and take note of the APP ID and App Secret (press Show to display it) since these two credentials will be used on the GWN configuration as shown on the following sections.





🚳 GWN_Captive_Po ▼	APP ID: APP ID Number	View Analytics	¥ Tools & Support	rt Docs
Dashboard				
Settings	Dashboard			
Roles				
Alerts		GWN Ca	ptive_Portal ∘	
App Review			ent mode and can only be used by app admins, developers and testers (?) App ID	
PRODUCTS		v2.10	APP ID number will be shown here	
Facebook Login		App Secret		
Marketing API		•••••	Press Show Button to see the App Secret	show
+ Add Product				

Figure 8: Facebook Developers Dashboard

Configure Captive Portal Policy with Facebook Authentication

After configuring the basic settings for the Facebook app, make sur to take note of the APP ID and Secret ID to use them when configuring captive portal policy.

Users could navigate on the web GUI under Captive Portal menu and add new policy with Facebook authentication and configure the following required options.

- Authentication Type: Third Authentication.
- Enable Facebook Authentication.
- Enter the Facebook **App ID** and **Secret**.
- Portal Page Customization: /third_auth.html

Following figure shows a sample configuration for Facebook authentication based on portal policy.





	Add		\times
Name	grandstream		
Expiration (?)	60 se	econd 🔻	
Authentication Type	Social Login Authenticatio	on 🔻	
WeChat			
Facebook	₹		
Facebook App Id	Enter your APP ID here		
Facebook App Secret	Enter your APP secret h	nere 💿	
Use Default Portal Page	•		
Portal Page Customization	/social_auth.html	T	
Landing Page	Redirect to the original U	RL ▼	
Enable HTTPS			
Pre Authentication Rule(s)	subnet • 31.13.24.0		
	subnet • 31.13.64.0,	/18	
	Save Car	icel	

Figure 9: Captive Portal Policy Sample Configuration

Pre-Authentication Rules

When using Facebook authentication for captive portal policy, users need to make sure to setup the following subnets under pre-authentication rules to allow communication with Facebook server during the authentication process and before deciding to allow or deny the WiFi client the access to Internet.

The following table lists all subnets to be entered when using Facebook Authentication.

Table 3: Pre-Authentication Rules for Facebook Authentication				
Pre-Authentication Rule(s) Type	Value			
subnet	31.13.24.0/21			
subnet	31.13.64.0/18			
subnet	45.64.40.0/22			





subnet	66.220.144.0/20
subnet	69.63.176.0/20
subnet	69.171.224.0/19
subnet	74.119.7.0/22
subnet	103.4.96.0/22
subnet	129.134.0.0/16
subnet	157.240.0.0/16
subnet	173.252.64.0/18
subnet	179.60.192.0/22
subnet	185.60.216.0/22
subnet	204.15.20.0/22

Following figure shows the list of the subnets that should be included.

Pre Authentication Rule(s)	subnet 🔻	31.13.24.0/21		
	subnet 🔻	31.13.64.0/18		
	subnet 🔻	45.64.40.0/22		
	subnet 🔻	66.220.144.0/20 😑		
	subnet 🔻	69.63.176.0/20		
	subnet 🔻	69.171.224.0/19		
	subnet 🔻	74.119.7.0/22		
	subnet 🔻	103.4.96.0/22		
	subnet 🔻	129.134.0.0/16		
	subnet 🔻	157.240.0.0/16		
	subnet 🔻	173.252.64.0/18		
	subnet 🔻	179.60.192.0/22		
	subnet 🔻	185.60.216.0/22		
	subnet 🔻	204.15.20.0/22		
		Add new item 🕂		
Save				

Figure 10: Pre-Authentication Rules for Facebook Authentication





Once this is done, make sure to save and apply the configuration and we will check on the next steps how to assign the configured policy to network groups and SSIDs.

Assign Captive Portal Policy to Network Groups and SSIDs

Once the captive portal policy has been configured with correct settings and pre-authentication rules for Facebook Authentication, users can assign the created policy to a network group or additional SSID under WiFi settings tab.

Navigate to Network Groups menu and under WiFi settings click on "Enable Portal Policy", then select the configured policy from the drop-down policy as shown on the following figure.

	Wi-Fi	Schedule
	Enable Additional SSID	2
	SSID ?	FreeWiFi
	SSID Band	Dual-Band 🔻
Net	work Group Membership	group0 •
	SSID Hidden	
	Wireless Client Limit 🕐	1
	Enable Captive Portal	
	Captive Portal Policy	Facebook
	Security Mode	Open •
	Use MAC Filtering	Disabled •
	Client Isolation	
	Enable RSSI 🕐	
	Minimum RSSI (dBm) 💿	
	Enable 11K 🕐	
		Save Cancel

Figure 11: Enable Captive Portal on WiFi Settings

After this is done, save and apply the settings then the AP will broadcast the new WiFi settings for the users. Once a client tries to connect to the Internet via WiFi, they will be request to login using their Facebook account.





← → C ① 192.168.6.179:8080/third_auth.html?GsRequestUri=http://www.grandstream.com/	☆	0	M	• •
f Connect With Facebook				

Figure 12: Login via Facebook Portal

The user then clicks on the button **« Connect with Facebook »** and will be redirected to Facebook login page to enter his/her account credentials as shown on the following figure.

facebook				
Sign Up Connect and share with the people in your life.				
Facebook Login				
You must log in to see this page.				
Email or Phone:				
Password:				
Keep me logged in				
Log In or Sign up for Facebook				
Forgot your password?				
	J			
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية (夜न) 中文(管件) 日本語				

Figure 13: Facebook Login

If authentication credentials are correct, the user will be forwarded to the requested URL or redirected to a configured external URL depending on the setting of the option **Landing Page** on captive portal **policy**.





Facebook analytics

Users could benefit from Facebook analytics feature in order to get dashboard data and reports along with the ability to download reports in CSV files while customizing the date range.

To use Facebook analytics, go to the link: <u>https://www.facebook.com/analytics</u> Then you can gather, customize and download reports using Facebook developers platform.

f	∃ Analytics		🛱 Help 🚱
Ø 8	GWN_Captive_P →	Last 28 days 💌	
M	Overview	Last 24 hours Last 7 days	
	Dashboards >	Last 14 days 0 2 Last 28 days OGINS DAILY ACTIVE USERS MONTHLY ACTIV	VEUSERS
-Ą.,	Activity -	Last 90 days Custom	
	Active Users	Facebook Login Activity > Active Login Users -	* 0 *
	Revenue	Custom dashboards are in beta. added to a dashboard yet.	
	Funnels	-	 Monthly Active Us Weekly Active Us
	Retention		Daily Active Users
	Cohorts		
	Breakdowns		
	Percentiles		
	Events Event Debugging		
	Overlap	Oct 31 Nov 03 Nov 06 Nov 09 Nov 12 Nov 15 Nov 18 Nov 21 Nov 24	
	Lifetime Value		
*	People >	Login Dialog > Accept Rate -	* 0 *
•	Push Campaigns 🛛 🕨	100% o	SHOW BY
\$	Facebook Platform 👻		New Logins - Mobile Web
	Give Feedback	50%	_



