

# Grandstream Networks, Inc.

**Captive Portal** 

Authentication via Facebook



### **Table of Content**

SUPPORTED DEVICES	4
INTRODUCTION	5
CAPTIVE PORTAL SETTINGS	6
Policy Configuration Page	7
Landing Page Redirection	
Pre-Authentication Rules	
Post-Authentication Rules	
Guest Page	11
CONFIGURATION STEPS	12
Create Facebook App	12
Configure Captive Portal Policy with Facebook Authentication	17
Using GWN Master GUI (Standalone mode)	17
Using GWN Management Platform	20
Wi-Fi Client	23
Facebook analytics	25



# **Table of Figures**

Figure 1: General Architecture	5
Figure 2: Captive Portal GWN76XX web GUI menu	6
Figure 3: GWN76XX Web GUI Policy Page Configuration	7
Figure 4: GWN76XX Guest Web Page	.11
Figure 5: Create new APP	12
Figure 6: App options	12
Figure 7: Create an App ID	13
Figure 8: Security check	13
Figure 10: Add "Facebook login" product to your App	14
Figure 11: Facebook Login - Settings	14
Figure 12: Facebook Login Settings - Valid OAuth redirect URIs	15
Figure 13: Facebook Developers Parameters - General	15
Figure 14: Make Facebook App Public	16
Figure 15: Switch Mode to LIVE	16
Figure 16:Facebook Login App - Live	16
Figure 17: GWN Master - Captive Portal Policy Sample Configuration	17
Figure 18: GWN Master – Pre Authentication Rules for Facebook Authentication	18
Figure 19: GWN Master - Enable Captive Portal on Wi-Fi Settings	19
Figure 20: GWN Platform - Splash Page Configuration	20
Figure 21: GWN Platform - Captive Portal Policy Sample Configuration	21
Figure 22: GWN Platform - Enable Captive Portal on Wi-Fi Settings	22
Figure 23: Connect to the SSID	23
Figure 24: Login with Facebook	23
Figure 25: Facebook Login page	24
Figure 26: Authentication succeed	24
Figure 27: Facebook Tools	25
Figure 28: Facebook Analytics	25

# **Table of Tables**

Table 1: Supported Devices	4
Table 2: GWN76XX Policy Configuration Page	8



### **SUPPORTED DEVICES**

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

Table 1: Supported Devices					
Model	Supported	Firmware			
GWN7610	Yes	1.0.5.14 or higher			
GWN7615	Yes	1.0.15.18 or higher			
GWN7605	Yes	1.0.15.18 or higher			
GWN7605LR	Yes	1.0.15.18 or higher			
GWN7600	Yes	1.0.3.19 or higher			
GWN7600LR	Yes	1.0.4.12 or higher			
GWN7630	Yes	1.0.9.12 or higher			
GWN7630LR	Yes	1.0.15.18 or higher			
GWN7000	Yes	1.0.4.23 or higher			

G

### **INTRODUCTION**

Captive Portal feature on GWN76XX Access Points allows to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access Internet.

Once connected to GWN76XX AP, Wi-Fi 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 Wi-Fi hotspots for Internet users.

This guide describes how to setup the captive portal feature on the GWN76XX 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 GWN76XX web page, by navigating to "**Captive Portal**" section.

This section contains four subsections: Guest, Policy List, Splash Page and Vouchers.

- **Guest**: This section lists the authenticated clients MAC addresses.
- **Policy List** : In this section, users can configure multiple portal policies which then can be assigned to specifc SSIDs under the menu "**SSIDs**". (For example having non-authentication based portal for temporary guests and setting up an authentication based portal policy for the internal staff).
- **Splash Page**: Under this tab, users could download and upload customized portal landing page to display to the users when they try to connect over the Wi-Fi.

	Policy List				
Overview	+ Add				
SSIDs					
Access Points	Name	Authentication Type	Expiration	Portal Page Customization	Actions
Clients 🔻	grandstream	Login for free	86400s	/portal_default.html	
Captive Portal 🔹					
Guest					
Policy List					
Splash Page					
Vouchers					
Bandwidth Rules					
System Settings 🔻					

#### Figure 2: Captive Portal GWN76XX web GUI menu



### **Policy Configuration Page**

The Policy configuration allows users to configure and customize different captive portal policies which then can be selected on SSID configuration page, giving the admin the ability to set different captive portals for each SSID, in this guide, we will be using **Internal Splash Page** for Facebook Authentication.

Basic		Auth Rule
Name	grandstream	
Splash Page	Internal <b>v</b>	
Authentication Type	Social Login Authentication	
Expiration 🥐	86400 Second(s) 🔻	
WeChat		
Facebook 🥐	•	
Facebook App Id	Enter your APP ID here	
Facebook App Secret	Enter your APP Secret here	•
Twitter 🕐		
Use Default Portal Page	<ul> <li>Image: A start of the start of</li></ul>	
Portal Page Customization	/social_auth.html	
Landing Page	Redirect to the Original URL	
Enable Daily Limit		
Enable HTTPS 흿 🖲	0	
	Save	

Figure 3: GWN76XX Web GUI Policy Page Configuration



The following table describes all the settings on this page:

### Table 2: GWN76XX Policy Configuration Page

Field	Description			
Name	Enter a name to identify the created policy (ex: Guest Portal).			
Splash Page	Select Splash Page type, Internal or External.			
Authentication Type	<ul> <li>Following types of authentication are available:</li> <li>Login for free: 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.</li> <li>RADIUS Server: Choosing this option will allow users to set a RADIUS server to authenticate connecting clients.</li> <li>Social Login Authentication: Choosing this option will allow users to enable authentication Facebook or Twitter or WeChat.</li> <li>Vouchers: Choose this page when using authentication via Vouchers.</li> <li>Login with Password: Choose this page when using authentication via a password.</li> </ul>			
Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.			
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.			
Use Default Portal Page	When enabled, the default portal page will be used, otherwise users can upload their custom page.			



	Select the customized portal page (if "Use Default Portal Page" is
	unchecked).
	• /facebook.html
	• /password_auth.html
	• /portal_default.html
	• /portal_pass.html
Portal Page Customization	• /portal_tip.html
	• /social_auth.html
	• /status.html
	• /twitter.html
	• /twitter_website.html
	• /vouchers auth.html
	<ul> <li>/wechat.html</li> </ul>
	Select page where authenticated clients will be redirected to
	Redirect to the original LIRI : Sends the authenticated
	client to the original requested LIRI
Landing Page	client to the original requested ONE.
	• Redirect External Page: Enter URL that you want to
	promote to connected clients (ex: company's website).
	Once the landing page is set to redirect to external page, user
Podiroct Extornal Page LIPI	should set the URL address for redirecting.
Redirect External Page ORL	This field appears only when Landing Page is set to "Redirect to
	an External Page".
	If enabled, captive portal will limit user connection by times of one
Enable Daily Limit	day.
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.

#### **Pre-Authentication Rules**

Using this option, users can set rules to match traffic that will be allowed for connected Wi-Fi 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.

#### **Post-Authentication Rules**

On the other hand, post authentication rules are used to match traffic that will be banned for Wi-Fi clients after authentication. As an example, if you want to disallow connected Wi-Fi 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.



### **Guest Page**

For Information Purposes Guest section lists MAC addresses of authenticated devices using captive portal. As we can see on the below figure, four Wi-Fi clients have been authenticated and granted internet access from the GWN7610 access points:

- ✓ Client 1 → 24:18:1D:A1:27:3A
- ✓ Client 2 → 50:EA:D6:19:F9:AE
- ✓ Client 3 → B4:BF:F6:40:DF:3B
- ✓ Client 3 → D8:C4:6A:9F:6E:5F

Overview		Guest			۵
SSIDs		MAC Address	IP Address	Expire Time	Authentication Status
Access Points		B4:BF:F6:40:DF:3B	192.168.5.149	2018-10-12 11:44:20	Authenticated
Clients	▼	24:18:1D:A1:27:3A	192.168.5.101	2018-10-12 11:42:56	Authenticated
Captive Portal	•	50:EA:D6:19:F9:AE	192.168.5.158	2018-10-12 11:47:15	Authenticated
Guest		D8:C4:6A:9F:6E:5F	192.168.5.137	2018-10-12 11:46:09	Authenticated

Figure 4: GWN76XX Guest 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.

FACEBOOK for Developers	Docs	Tools	Support	My Apps	Q Search developer documentation	,
		Ð				
	No	Apps C	reated			
	You curren	tly have n	o apps create	ed.		
		Create A	р			

Figure 5: Create new APP

- Click "Create APP" and choose the first option.

Create an	App ID	×
How are yo	ou using your app? Learn More	
	Manage Business Integrations	
	Create or manage Pages, Groups, Events, Ads, Messenger, Instagram or other types of business integrations.	
	Integrate a Third-Party Gaming App	
đ	Create an app to let people play mobile games that are off the Facebook platform. <b>Note:</b> Select <b>For Everything Else</b> option to build Instant Games or Canvas Games.	
	For Everything Else	
•	Select if you're integrating Facebook Login, building an Instant Game or app that will access user data on Facebook or Instagram.	C

Figure 6: App options



3. Create an App ID:

This step prompts you to choose a display name for your application. Choose a name that will represent your Wi-Fi portal. Users will see this when authenticating. For this example, we'll use the name "GWN\_Captive\_Portal" and keep the default email, which is the email linked to your Facebook account. For who can use this App, we'll use "Other business".

Create an App ID X
App Display Name
This is the app name associated with your app ID.
GWN_Captive_Portal
App Contact Email
This email address is used to contact you about potential policy violations, app restrictions or steps to recover the app if it's been deleted or compromised.
ysoukrat@grandstream.com
Just me, people in my business or developers who have role on my app Select if your app will manage just your own business or personal data
Other business     Select if your app needs to access customer data, or will manage assets on behalf of a business
Do you have a Business Manager account? · Optional
Your app may need to be connected to a verified Business Manager account to access different levels of data. If you do not have a Business Manager account, you can create one later in the process.
No Business Manager Account selected
Cancel By proceeding, you agree to the Facebook Platform Policies Create App ID

Figure 7: Create an App ID

Then, Submit the security check

Security Check				
Please complete the security check.				
I'm not a robot	reCAPTCHA Privacy - Terms			
Why am I seeing this? If you think this doesn't go against our Commu	nity Standards let us	know.		
			Su	ibmit Cancel

Figure 8: Security check



-

- 4. Add "Facebook login" product to your App:
- Facebook for Developers will display all the available products
- Click to set up "Facebook login" feature, as shown below:



Figure 9: Add "Facebook login" product to your App

5. Locate the left barre and click on Facebook Login > Settings:

FACEBOOK for	Deve	elopers
GWN_Captive_Portal	•	Арр
		C
👚 Dashboard		_
Settings	•	
Roles	Þ	
🜲 Alerts	•	
App Review	Þ	
PRODUCTS (+)		
Facebook Login	-	
Settings		
Quickstart		
i≣ Activity Log		

Figure 10: Facebook Login - Settings

6. Add Controller Redirect URI and Port:

Under Facebook Login settings, include the following URL under "Valid OAuth redirect URIs".

#### https://cwp.gwnportal.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3



- Enable option "Login from Devices"

Use the toggle options as shown in the below image:

A Dathard		Client OAuth Settings
Dashboard		
Settings	Þ	Client OAuth Login
Roles	Þ	Yes Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [7]
Alerts	•	
App Review	Þ	Yes         Endoles web-based Client OAuth Login. [?]         Yes         Enforce HTTPS           Enables web-based Client OAuth Login. [?]         Yes         Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]
PRODUCTS 🕂		
Facebook Login	*	No         Force Web OAuth Reauthentication         Embedded Browser OAuth Login           No         When on, prompts people to enter their         No         Enable webview Redirect URIs for Client
Settings		Facebook password in order to log in on the OAuth Login. [?] web. [?]
Quickstart		Yes Only allow redirect URIs Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [7]
		Valid OAuth Redirect URIs
		https://cwp.gwnportal.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3 👾
		Yes         Login from Devices           Enables the QAuth client login flow for devices like a smart TV (?)

Figure 11: Facebook Login Settings - Valid OAuth redirect URIs

- 7. App ID and App Secret:
- Navigate to Settings → Basic: App ID and App Secret will be automatically assigned to your app. Choose a Display Name and Namespace for your app these can be anything, but users will see them when authenticating. For Category, we'll use Business and pages. Category isn't critical here, so feel free to use a different category if it better represents your business.

FACEBOOK fo	r Deve	lopers	Documentation	Outils	Assistance	Mes applications	Q. Rechercher dans la docum	nentation développeur	Ļ
GWN_Captive_Portal	•	ID d'app: 3036724229780831	En développeme	ent	Type d'app : Int	tégration professionnelle		✓ Voir Analytics	0
ord Tableau de bord		Arr 10				Are Creet			
Paramètres	*	App ID				App Secret		Chau	
Général		3030724229780831				•••••		SHOW	
Avancé		Display Name				Namespace			
FJ Rôles	Þ	GWN_Captive_Ports	al			gwn_fb_login			
🌲 Alertes	Þ								
🥏 Contrôle app	Þ	App Domains				Contact Email 🚯			
						ysoukrat@grandstrea	im.com		
PRODUITS 🕀		Privacy Policy URL				Terms of Service URL			
Facebook Login	Þ	http://www.grandstre	am com/			http://www.grandstrea	am.com/		
		inip				inip			
Journal des activités		App Icon (1024 x 1024	4)			Category			
						Business and Pages 🔻			
		+7				Find out more informat	tion about app categories her	e	

Figure 12: Facebook Developers Parameters - General

- Under both "Privacy Policy URL" and "Terms of Service URL", enter the domain : <u>http://www.grandstream.com/</u> as shown on the figure above.



- 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.
- Press "Save Changes".
- 8. Publish App:

Finally, publish the app to live, by clicking the switch at the top of the "Facebook for developers" page to change status from "In development" to "live".

FACEBOOK for Dev	Docs	Tools	Support	My Apps		
GWN_Captive_Portal     ▼	App ID: 3036724229780831	In development	App	Type: Busine	ess Integration	



- Confirm to Switch Mode



Figure 14: Switch Mode to LIVE

Your Facebook Login App is now Live



Figure 15: Facebook Login App - Live



### **Configure Captive Portal Policy with Facebook Authentication**

### Using GWN Master GUI (Standalone mode)

#### 1. Captive Portal

This includes both cases: If the master is the GWN7000 router or a GWN76XX Access Point. First, users need to take note of the APP ID and Secret ID from Facebook app  $\rightarrow$  basic settings, to use them when configuring captive portal policy. Then, navigate on the GWNXXXX master web GUI under Captive Portal menu  $\rightarrow$  Policy List and add new policy with Facebook authentication and configure the following required options.

- Authentication Type: Social Login Authentication
- Enable Facebook Authentication.
- Enter the Facebook App ID and Secret.
- Portal Page Customization: /social\_auth.html
- Enable HTTPS

Basic			Auth Rule
Name	grandstream		]
Splash Page	Internal	•	•
Authentication Type	Social Login Authentication	1	•
Expiration 🥎	86400	Second(s)	•
WeChat			
Facebook 🤅	•		
Facebook App Id	Enter your APP ID here	e	
Facebook App Secret	Enter your APP Secre	t here	•
Twitter 🤉			
Use Default Portal Page	٢		
Portal Page Customization	/social_auth.html	,	•
Landing Page	Redirect to the Original URL	•	
Enable Daily Limit			
Enable HTTPS 🤅	•		





 Pre-Authentication Rules: When using Facebook authentication for captive portal policy, The GWN76XX Access point will automatically setup the needed domains under preauthentication rules to allow communication with Facebook server during the authentication process and before deciding to allow or deny the Wi-Fi client the access to Internet.

	Edit						×
		Ba	sic		A	auth Rule	
Pre A	uthentication	?					
	Hostname	•	facebook.com	All	•		0
	Hostname	•	facebook.net	All	•		•
	Hostname	•	akamaihd.net	All	Ŧ		•
	Hostname	•	akamai.net	All	Ŧ		•
	Hostname	•	fbcdn.net	All	Ŧ		•
	Choose Destin	•		Choose Servic	•		•
						Add new item	Ð
Post	Authenticatio	<b>n</b> (?	)				
	Choose Destin	•		Choose Servic	T		•
						Add new item	•

Following figure shows the list of the included domains:

Figure 17: GWN Master – Pre Authentication Rules for Facebook Authentication

We will check on the next steps how to assign the configured policy to SSIDs.



#### 2. Assign Captive Portal Policy to SSIDs:

Once the captive portal policy has been configured with correct settings for Facebook Authentication, users can assign the created policy to a SSID under Wi-Fi settings tab.

Navigate to **SSIDs** menu and under Wi-Fi settings click on "Enable Portal Policy", then select the configured policy from the drop-down policy as shown on the following figure.

Overview	+		Edit	×	
SSIDs	Name	Wi-Fi	Device Membership		
Access Points	GWNC	Enable SSID			^
Clients 🔹		SSID 🧿	GWN8B4DD8		
Captive Portal 🔻		SSID Band (?)	Dual-Band v		
Bandwidth Rules		SSID Hidden			
System Settings 🔻		VLAN			
		Wireless Client Limit ?			
		Enable Captive Portal			
		Captive Portal Policy	grandstream •		
		Security Mode	Open <b>v</b>		
		Client Bridge Support (?)			
		Client Time Policy	None •		
			Save Cancel		

Figure 18: GWN Master - Enable Captive Portal on Wi-Fi Settings

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



### **Using GWN Management Platform**

This includes both Grandstream management platforms: GWN.Cloud and GWN Manager.

First, users must configure the basic settings for the Facebook app and make sur to take notes of the APP ID and Secret ID to use them when configuring the splash page before moving on the captive portal policy settings.

- 1. Splash Page:
  - Enable Facebook Login.
  - Enter the Facebook App ID and Secret.

II Overview	Page Advertisement	GS_Splash_Page Save Cancel
🗢 Access Points 🛛 🗸	Basic Components	
🗟 SSIDs 🗸 🗸	🗹 Image	8 Facebook ^
🖵 Clients 🗸 🗸	Text	Facebook App Id @ 3036724229780831
: Captive Portal ㅅ	I Terms of Use	* Facebook App Secret 📀
Summary	Logging Components	<b>GRANDSTREAM</b> (b69a2d2897a384caad0420a74131a)
Guest	For Free	Welcome 😣
Policy List	Simple Password	
Splash Page	Radius Server	8
Vouchers	Custom Field	
፰ Access Control →	Z Facebook	
🗐 Insight 🗸 🗸	Twitter	T Login with Facebook

Figure 19: GWN Platform - Splash Page Configuration

#### 2. <u>Captive Portal Policy</u>

- Name the Policy and decide the Client expiration time
- Set Splash Page to Internal
- Select your splash page (including the Facebook Login)
- Choose the landing page: Redirect to the original URL
- Enable HTTPS
- Default Pre-Authentication Rules



n Dashboard		Add	Delete			
default	-	GS_PC	A Eolach agus	Edit Portal Po	olicy	lach Branc Carloon
ili Overview		D POL	* Name 🔘	GS_Policy		
🐨 Access Points	~		Splash page	Internal	-	
🕆 SSIDs	~		* Client Expiration 💿	0 day(s) 0 ho	ur(s) 1 minute(s)	
🕤 Clients	~		Fallsafe Mode 😡			
i≡ Captive Portal	^		Daily Limit 🕥			
Summary			Splash Page Customization	GS_Splash_Page	~	
Guest			Landing Page 🕥	Redirect to the origin	nai URL 👻	
Policy List			Enable HTTPS 🔘	<b>U</b>		
Splash Page			Pre Authentication Rule(s) 💿	Hostname 👻	facebook.com	
Vouchers	_			Ali 👻		
	~			Hostname 💌	facebook.net	
🔛 Insight	~					
() System	~			All -	akamaind.net	
Global				Hostname 👻	fbcdn.net	
illi. Report				All		
📋 Change Log				Hostname 🚽	akamal.net	
				All		
			Post Authentication Bule/s)	Select Destina	cation Rule	
					Can	cel Save

Figure 20: GWN Platform - Captive Portal Policy Sample Configuration

#### 3. Assign the Captive Portal Policy to SSIDs

Once the captive portal policy has been configured with correct settings for Facebook Authentication, users can assign the created policy to a SSID under Wi-Fi settings tab.

Navigate to **SSIDs** menu and under Wi-Fi settings click on "Enable Portal Policy", then select the configured policy from the drop-down policy as shown on the following figure:



🛧 Network 🔹	Edit SSID	:
default	Wi-Fi Settings Device Membership	
II Overview	* SSID 📀 WiFi_FB_Login	
👄 Access Points 🔍 🗸	Enabled 🗹	
≎ SSIDs ^	VLAN	
Summary	SSID Band Uual-Band 💌	
Configuration	Access Security	^
🖫 Clients 🗸 🗸	Security Mode WPA2 💌	
$\equiv$ Captive Portal $\sim$	WPA Key Mode PSK 👻	
킄 Access Control 🗸	WPA Encryption Type AES 💌	
🗐 Insight 🗸 🗸	* WPA Pre-Shared Key 💿	
🗘 System 🗸 🗸	Enable Captive Portal	
🌐 Global	* Captive Portal Policy GS_Policy 🔷	
uli Report	MAC Filter Disabled 👻	
📋 Change Log	Client Isolation	
	Cancel	Save

Figure 21: GWN Platform - Enable Captive Portal on Wi-Fi Settings

After this is done, save and apply the settings then the AP will broadcast the new Wi-Fi settings for the users.



# Wi-Fi Client

Once a client tries to connect to the Internet via our previously configured Wi-Fi SSID, they will be request to login using their Facebook account. (In this example we will be using Win10 Laptop as a Wi-Fi client):

1. Select the related SSID and enter the correct password



Figure 22: Connect to the SSID

- 2. The following page will popup asking for Facebook Login before allowing access to the network:
- Accept the Terms of use The, click on Login with Facebook



Figure 23: Login with Facebook



3. You will be redirected to Facebook login page to enter your account credentials as shown on the following figure:

I Log in to Facebook   Facebook x +			-	٥	×
$\leftarrow$ $\rightarrow$ $\circlearrowright$ $\land$ https://www.faceboo	c.com/login.php?skip_api_login=1&api_key=3036724229780831&kid_directed_site=0&app_id=30367 🖈	∿≡	Ē	۲	
facebook	Create New Account				
	Log in to Facebook				
	Email address or phone number				
	Password				
	Log In				
	Forgotten account? - Sign up for Facebook Not now				

Figure 24: Facebook Login page

4. If authentication credentials are correct, a prompt will announce Authentication succeed then the

user will be forwarded according to the Landing Page configuration on the captive portal policy:



Figure 25: Authentication succeed



### **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: https://www.facebook.com/analytics

• Same as FACEBOOK for Developers GUI → Tools → Analytics

FACEBOOK for Developers	Docs	Tools	Support	My Apps	Q Search developer documentation	. 🔺 🔣
Developer Tools						
(8)	2			S		
Graph API Explorer	Sharing Debugger			Access T	oken Debugger	
Test, create, and authenticate API calls and debug responses.	Preview how your conten shared to Facebook.	t will look w	hen it's	See detailed	l info for an access token.	
Other Developer Tools				Business T	ools	
Access Token Tool				📶 Analytic	s	
Generate user and app access tokens for testing.				💷 Ads Man	ager	
JS SDK Console				🔘 Monetiza	ation Manager	
A testing environment for the Facebook SDK for Javascript				🖻 Business	Manager	
API Upgrade Tool See which API calls are affected by changes in newer versi make to upgrade.	ons of the API and learn what c	hanges you n	eed to			

Figure 26: Facebook Tools

Then you can gather, customize and download reports using Facebook developers' platform. Refer to the figure bellow:

🌉 Yahia 🔻 🏟 ? f ≡ Analytics GWN\_Captive\_Portal Last 28 days 100% of people + Add a filter Synthesis Starting July 1, 2020, businesses who create analytics reports that include individuals in California will see impact to reporting in Facebook Analytics. We've released a Limited Data Use feature to give businesses more control over how their data is used in our systems and better support them with their California Consumer Privacy Act (SCPA) compliance efforts. × Learn More E Dashboards Create a dashboard ും Activity 23 People S Facebook platform {ô} Settings Set up Facebook Analytics des you with a summary of how people use your app or website. You'll have access to data such ns, the number of active users, the number of purchases, and more. you start recording events, this overview provides as the number of sessions, Facebook @ 2020 | Privacy Terms of Service Cookies Advertising Jobs Developers About

Figure 27: Facebook Analytics

