



Grandstream Networks, Inc.

Captive Portal

Authentication via Twitter



Table of Content

SUPPORTED DEVICES	4
INTRODUCTION.....	5
CAPTIVE PORTAL SETTINGS	6
Policy Configuration Page	6
<i>Landing Page Redirection.....</i>	<i>10</i>
<i>Pre-Authentication Rules</i>	<i>10</i>
<i>Post-Authentication Rules.....</i>	<i>10</i>
Guest Page.....	10
CONFIGURATION STEPS.....	12
Create Twitter App.....	12
Configure Captive Portal Policy with Twitter Authentication	15
Assign Captive Portal Policy to SSIDs	18
Connect to Network.....	19



Table of Figures

Figure 1: Captive Portal web GUI menu	6
Figure 2: Policy Page Configuration	7
Figure 3: Client Web Page	11
Figure 4: Twitter Application details	13
Figure 5: Twitter App keys and Access Tokens	15
Figure 6: Captive Portal Policy Sample Configuration	16
Figure 7: Pre-Authentication Rules for Twitter Authentication.....	17
Figure 8: Enable Captive Portal on WiFi Settings	18
Figure 9: Login via Twitter Portal.....	19
Figure 10: Twitter – Authorize	20
Figure 11: Twitter Login.....	21
Figure 12 : PIN code.....	21
Figure 13 : PIN Verification Page	22

Table of Tables

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



SUPPORTED DEVICES

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

Table 1: Supported Devices

Model	Supported	Firmware
GWN7630	Yes	1.0.9.12 or higher
GWN7610	Yes	1.0.5.11 or higher
GWN7600	Yes	1.0.6.28 or higher
GWN7600LR	Yes	1.0.6.28 or higher
GWN7000	Yes	1.0.4.23 or higher



INTRODUCTION

Captive Portal feature on GWN76XX 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 GWN76XX 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 GWN76XX series using Twitter Authentication.



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 specific 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 WiFi.

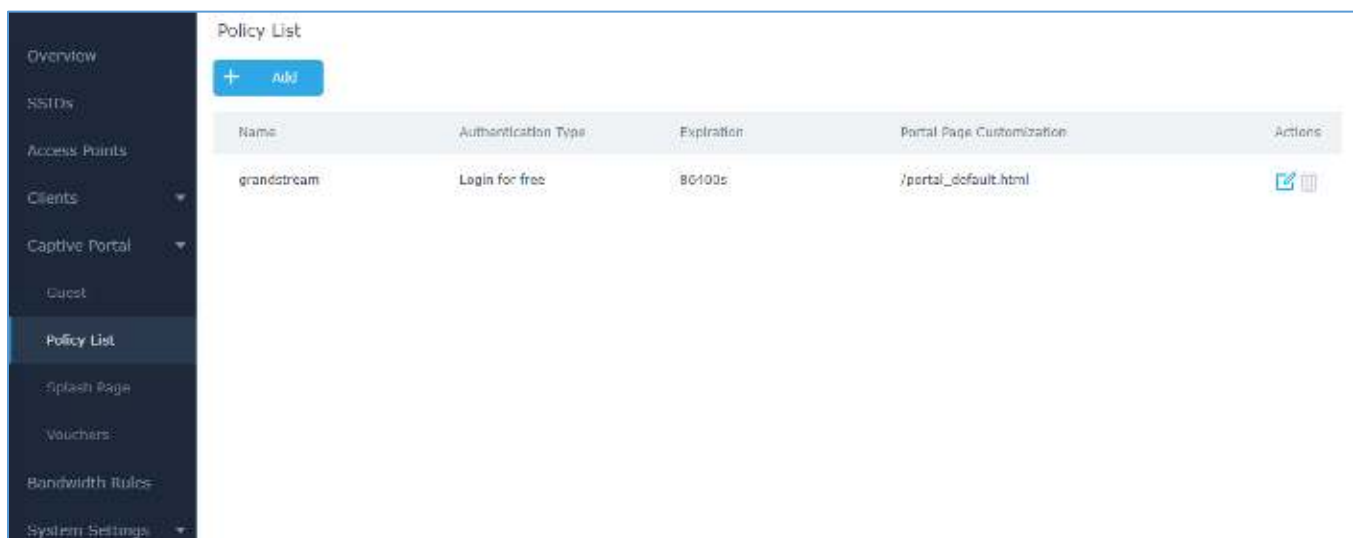


Figure 1: Captive Portal web GUI menu

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 Twitter Authentication.

Basic
Auth Rule

Name

Splash Page ▼

Authentication Type ▼

Expiration ? ▼

WeChat

Facebook ?

Twitter ?

Force to Follow

Consumer Key ?

Consumer Secret ?

Use Default Portal Page

Portal Page Customization ▼

Landing Page ▼

Enable Daily Limit

Enable HTTPS ?

Save
Cancel

Figure 2: Policy Page Configuration

The following table describes all the settings on this page:



Table 2: Policy Configuration Page

Field	Description
Basic	
Name	Enter a name to identify the created policy (ex: Guest Portal).
Splash Page	Select Splash Page type, Internal or External.
Authentication Type	<p>Following types of authentication are available:</p> <ul style="list-style-type: none"> • 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. • RADIUS Server: Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. • Social Login Authentication: Choosing this option will allow users to enable authentication Facebook or Twitter or WeChat. • Vouchers: Choose this page when using authentication via Vouchers. • Login with Password: Choose this page when using authentication via a password.
Expiration	Configures the period of validity, after the valid period, the client will be re-authenticated again.
Twitter	<p>Check this box to enable Twitter Authentication.</p> <p><i>This field appears only when “Authentication Type” option is set to “Social Login Authentication”.</i></p>
Force to Follow	If checked, users need to Follow owner before being authenticated.
Owner	<p>Enter the app Owner to use Twitter Login API.</p> <p><i>This field appears only when “Force to Follow” option is checked.</i></p>
Consumer Key	<p>Enter the app Key to use Twitter Login API.</p> <p><i>This field appears only when “Twitter” option is checked.</i></p>
Consumer Secret	<p>Enter the app secret to use Twitter Login API.</p> <p><i>This field appears only when “Twitter” option is checked.</i></p>
Use Default Portal Page	When enabled, the default portal page will be used, otherwise users can upload their custom page.



Portal Page Customization	<p>Select the customized portal page (if “Use Default Portal Page” is unchecked).</p> <ul style="list-style-type: none"> • <i>/terms_of_use/terms.html</i> • <i>/facebook.html</i> • <i>/password_auth.html</i> • <i>/portal_default.html</i> • <i>/portal_pass.html</i> • <i>/portal_tip.html</i> • <i>/social_auth.html</i> • <i>/status.html</i> • <i>/twitter.html</i> • <i>/twitter_website.html</i> • <i>/vouchers_auth.html</i> • <i>/wechat.html</i> 									
Landing Page	<p>Select page where authenticated clients will be redirected to.</p> <ul style="list-style-type: none"> • 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 URL Address	<p>Once the landing page is set to redirect to external page, user should set the URL address for redirecting.</p> <p><i>This field appears only when Landing Page is set to “Redirect to an External Page”.</i></p>									
Enable Daily Limit	<p>If enabled, captive portal will limit user connection by time of one day.</p>									
Enable HTTPS	<p>Check this box to enable captive portal over HTTPS.</p>									
Auth Rule										
Pre-Authentication Rules	<p>From this menu, users can set matching rules to allow certain types of traffic before authentication happens or simply allow the traffic for non-authenticated end points.</p> <p>When using Twitter, following rules will be added automatically and cannot be deleted:</p> <table border="1" data-bbox="634 1738 1409 1873"> <thead> <tr style="background-color: #cccccc;"> <th>Destination</th> <th>Hostname</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>Hostname</td> <td>twimg.com</td> <td>All</td> </tr> <tr> <td>Hostname</td> <td>twitter.com</td> <td>All</td> </tr> </tbody> </table>	Destination	Hostname	Service	Hostname	twimg.com	All	Hostname	twitter.com	All
Destination	Hostname	Service								
Hostname	twimg.com	All								
Hostname	twitter.com	All								



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 WiFi users before authentication process. This can be needed for example to setup Twitter authentication where some traffic should be allowed to Twitter server(s) to process the user’s authentication. Or simply to be used to allow some type of traffic for unauthenticated users.

When using Twitter, following mandatory rules will be automatically added:

Destination	Hostname	Service
Hostname	twimg.com	All
Hostname	twitter.com	All

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.

Guest Page

For Information purpose, Clients page lists MAC addresses of authenticated devices using captive portal. As we can see on the below figure, four WiFi 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**



GWN7610 Firmware 1.0.7.12 Time 2018-10-11 12:52				
Overview SSIDs Access Points Clients Captive Portal Guest	Guest			
	MAC Address	IP Address	Expire Time	Authentication Status
	B4:BF:F6:40:DF:38	192.168.5.149	2018-10-12 11:44:20	Authenticated
	24:18:1D:A1:27:3A	192.168.5.101	2018-10-12 11:42:56	Authenticated
	50:EA:D6:19:F9:AE	192.168.5.158	2018-10-12 11:47:15	Authenticated
D8:C4:6A:0F:6E:5F	192.168.5.137	2018-10-12 11:46:00	Authenticated	

Figure 3: Client Web Page



CONFIGURATION STEPS

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

Create Twitter App

To use Twitter 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 Twitter servers.

We summarize in the following section the required steps:

1. Go to Twitter's platform: <https://developer.twitter.com/>
2. Login using your account.
3. Create a new APP and give it a name (ex: GWN_Captive_Portal).
4. Enter Twitter Application Details:
 - Enter a description in "Description" field.
 - In "Callback URL" field, enter <http://cwp.gwn.cloud:8080/GsUserAuth.cgi>



Apps / Create an app

Understanding apps

[What is an app?](#) ▾

[Why register an app?](#) ▾

[Which products require an API key?](#) ▾

App details

The following app details will be visible to app users and are required to generate the API keys needed to authenticate Twitter developer products.

App name (required) ⓘ

Maximum characters: 32

Application description (required)

Share a description of your app. This description will be visible to users so this is a good place to tell them what your app does.

This is a Test GWN Captive Portal for Twitter Authentication with GWN76xx Grandstream Access Points

Between 10 and 200 characters

Website URL (required) ⓘ

Allow this application to be used to sign in with Twitter [Learn more](#)

Enable Sign in with Twitter

Callback URLs ⓘ

OAuth 1.0a applications should specify their oauth_callback URL on the request token step, which must match the URLs provided here. To restrict your application from using callbacks, leave these blank.

 ✕

[+ Add another](#)


Figure 4: Twitter Application details

- Once created, you can check the App details under “App details” section

App details Keys and tokens Permissions

App details

Details and URLs Edit

 **App icon**
App icon is default, click edit to upload.

App Name
GWN_Captive_Portall

Description
This is a Test GWN Captive Portal for Twitter Authentication with GWN76xx Grandstream Access Points

Website URL
<https://www.twitter.com>

Sign in with Twitter
Disabled

Callback URL
<http://cwp.gwn.cloud:8080/GsUserAuth.cgi>

Terms of service URL
None

Privacy policy URL
None

Organization name
None

Organization website URL
None

App usage
This Application is only for Documentation purposes to explain the integration of Captive Portal of GWN76XX with Twitter Authentication

6. Finally, go to “Keys and Access Tokens” tab and take note of the “**Consumer Key (API Key)**” and “**Consumer Secret (API Secret)**” since these two credentials will be used on the GWN configuration.



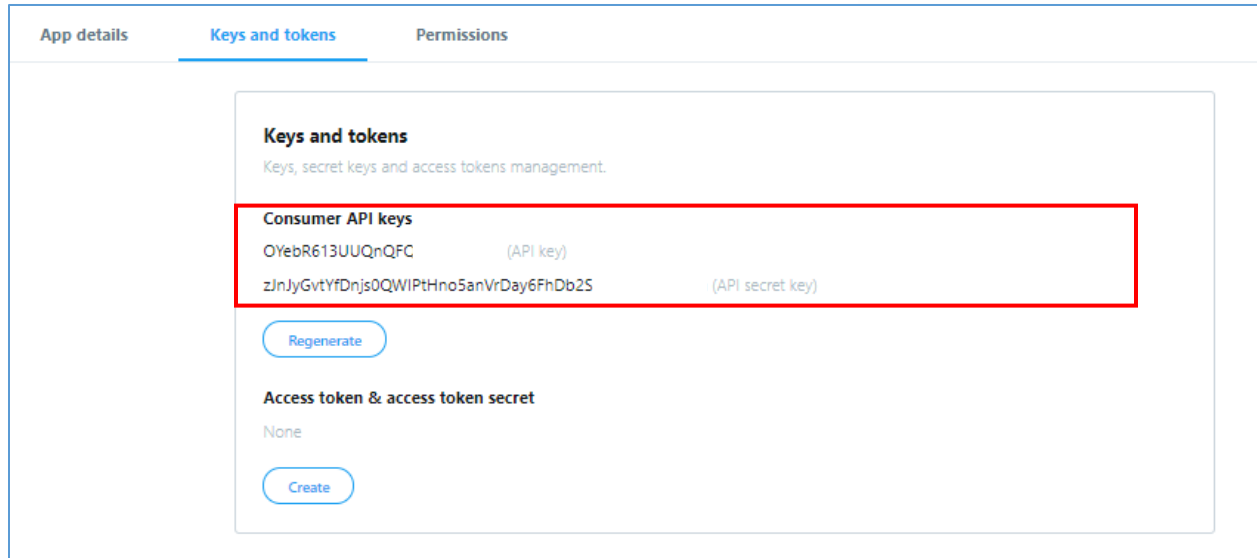


Figure 5: Twitter App keys and Access Tokens

Configure Captive Portal Policy with Twitter Authentication

After configuring the basic settings for the Twitter app, make sure to take note of the consumer key and Secret to use them when configuring captive portal policy.

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

- **Authentication Type:** Social login Authentication.
- Enable **Twitter Authentication**.
- Enter the Twitter **Owner** and **consumer Key** and **Secret**. (“**Owner**” field does only appear when “**Force to Follow**” option is enabled)
- Portal Page Customization: **/Social_auth.html**

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

Edit ✕

BasicAuth Rule

Name

Splash Page

Authentication Type

Expiration

WeChat

Facebook

Twitter

Force to Follow

Owner

Consumer Key

Consumer Secret

Use Default Portal Page

Portal Page Customization

Landing Page

Enable Daily Limit

Enable HTTPS

Save Cancel

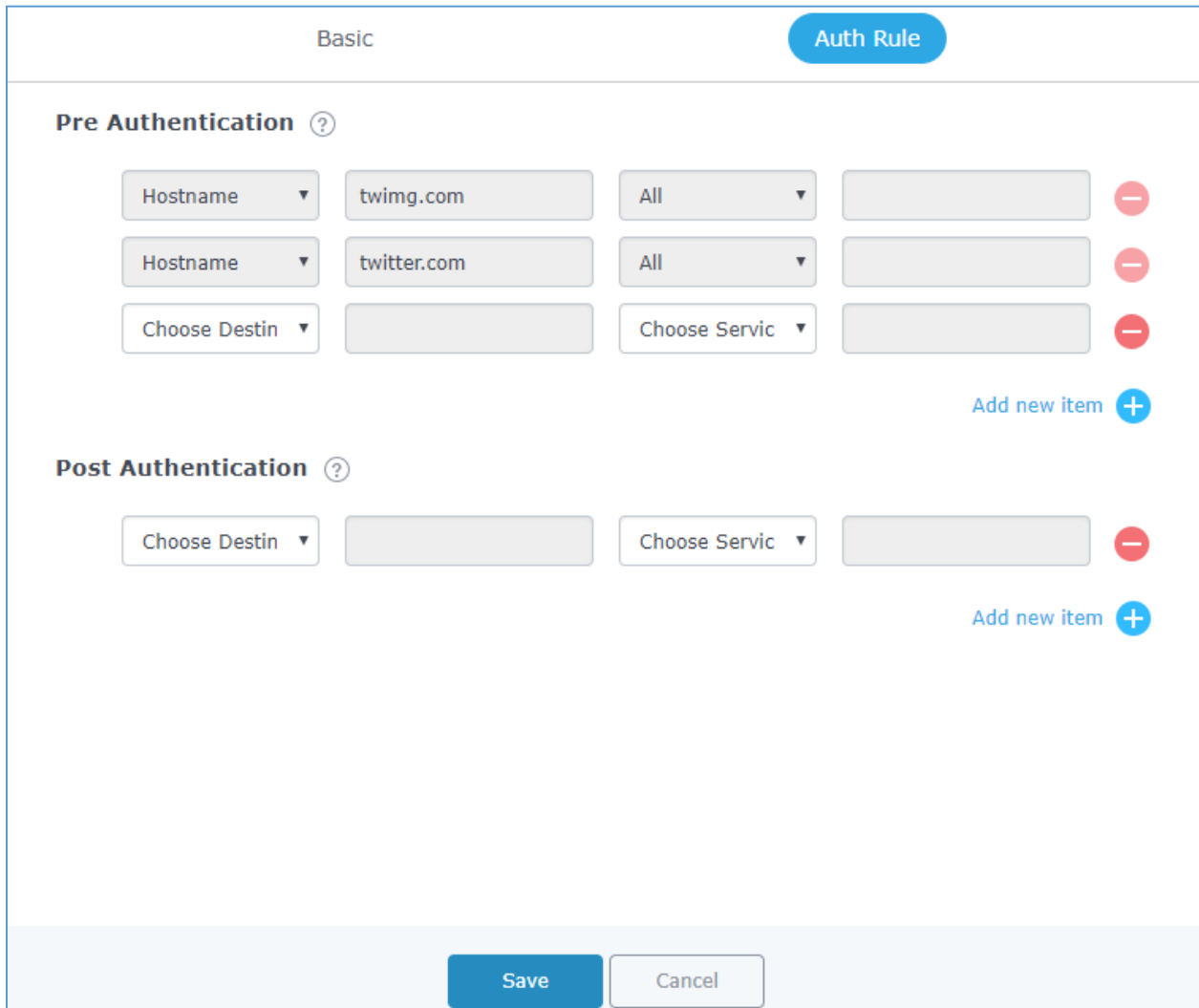
Figure 6: Captive Portal Policy Sample Configuration



Pre-Authentication Rules

When using Twitter authentication for captive portal policy, The GWN76XX Access point will automatically setup the needed domains 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.

Following figure shows the list of the included domains:



The screenshot displays the configuration page for Pre-Authentication Rules. It features a 'Basic' tab and an 'Auth Rule' button. The 'Pre Authentication' section contains three rows of configuration items. The first row has 'twimg.com' as the hostname and 'All' as the service. The second row has 'twitter.com' as the hostname and 'All' as the service. The third row is empty, with 'Choose Destin' and 'Choose Servic' as dropdown menus. Below the 'Pre Authentication' section is the 'Post Authentication' section, which contains one empty row with 'Choose Destin' and 'Choose Servic' dropdown menus. There are 'Add new item' buttons with plus signs next to each section. At the bottom of the page are 'Save' and 'Cancel' buttons.

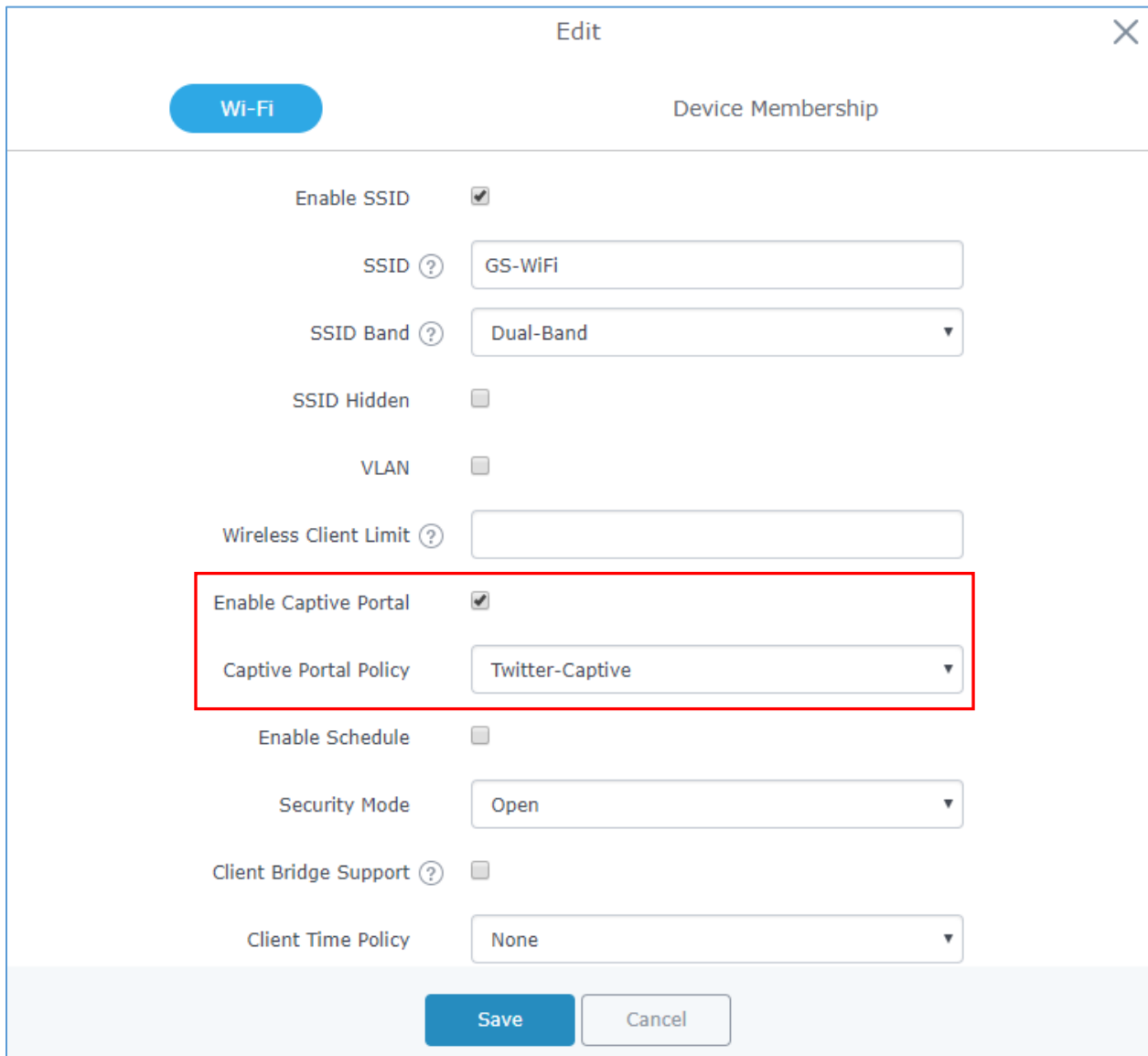
Figure 7: Pre-Authentication Rules for Twitter Authentication

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 SSIDs.

Assign Captive Portal Policy to SSIDs

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

Navigate to **SSIDs** menu and under WiFi settings click on **“Enable Captive Portal”**, then select the configured policy from the drop-down policy as shown on the following figure.



The screenshot shows the 'Edit' configuration window for a WiFi SSID. The 'Wi-Fi' tab is active. The 'Enable Captive Portal' checkbox is checked, and the 'Captive Portal Policy' dropdown menu is set to 'Twitter-Captive'. A red rectangular box highlights these two settings. Other visible settings include 'Enable SSID' (checked), 'SSID' (GS-WiFi), 'SSID Band' (Dual-Band), 'SSID Hidden' (unchecked), 'VLAN' (unchecked), 'Wireless Client Limit' (empty), 'Enable Schedule' (unchecked), 'Security Mode' (Open), 'Client Bridge Support' (unchecked), and 'Client Time Policy' (None). 'Save' and 'Cancel' buttons are at the bottom.

Figure 8: 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.



Connect to Network

Once a client tries to connect to the Internet via WiFi, they will be request to login using their Twitter account.

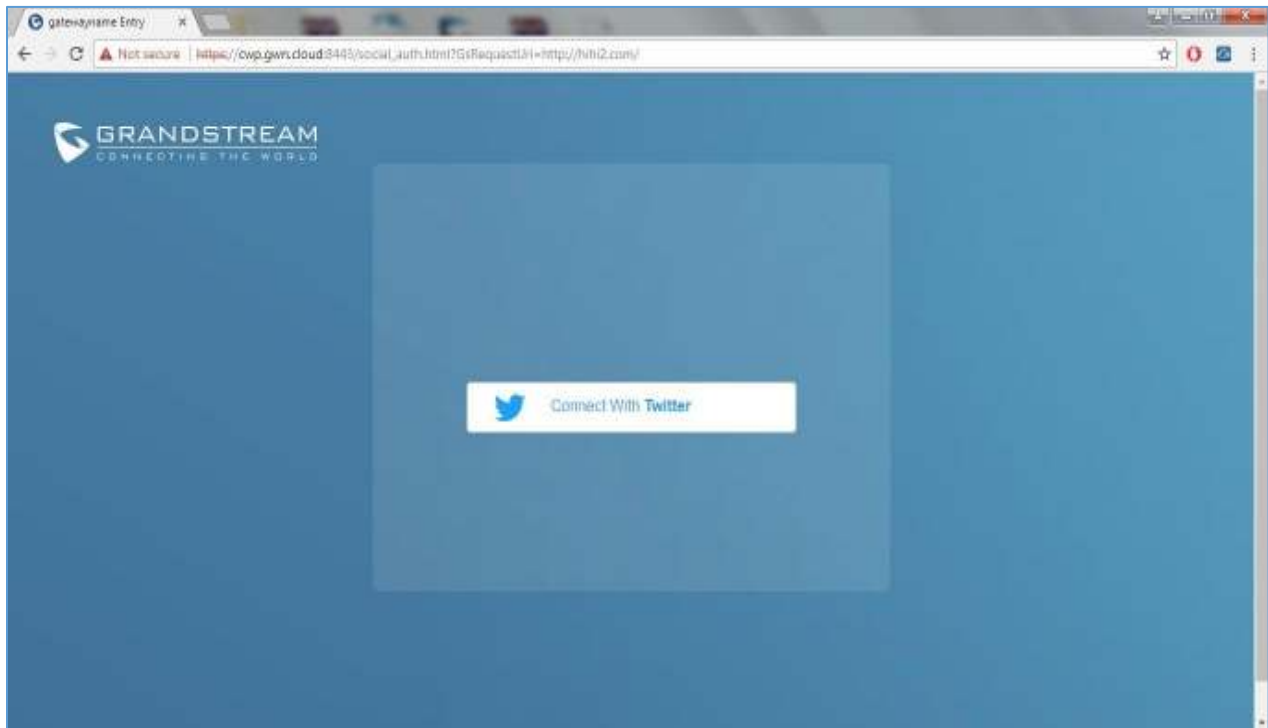


Figure 9: Login via Twitter Portal

1. Click on **Connect with Twitter** button. You will be re will be redirected to Twitter login page.
2. Click on **Authorize** button to access twitter login page.





Figure 10: Twitter – Authorize

3. Enter your Twitter account credentials.

Authorize GWN_Captive_Portal to use your account?


Remember me · [Forgot password?](#)

This application will be able to:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

Will not be able to:

- Access your direct messages.
- See your email address.
- See your Twitter password.



GWN_Captive_Portal
www.twitter.com

This is a Test GWN Captive Portal for
Twitter Authentication with GWN76xx
Grandstream Access Points

Figure 11: Twitter Login

4. Press **Authorize app** button. A page with PIN code to complete the verification will be displayed as shown in below figure.

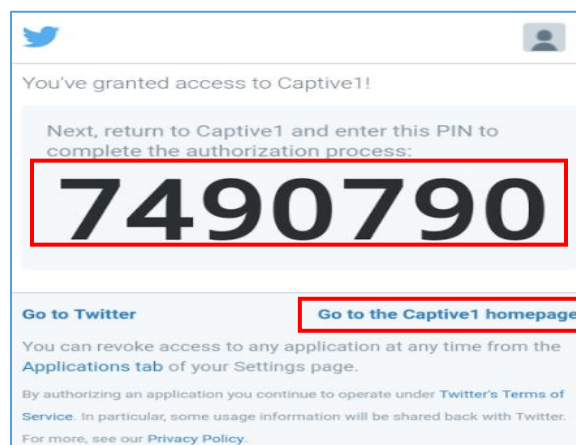


Figure 12 : PIN code



5. Take note of the PIN code and click on **Go to the <app> homepage**.
6. On the verification page, enter the saved PIN code to get authenticated.

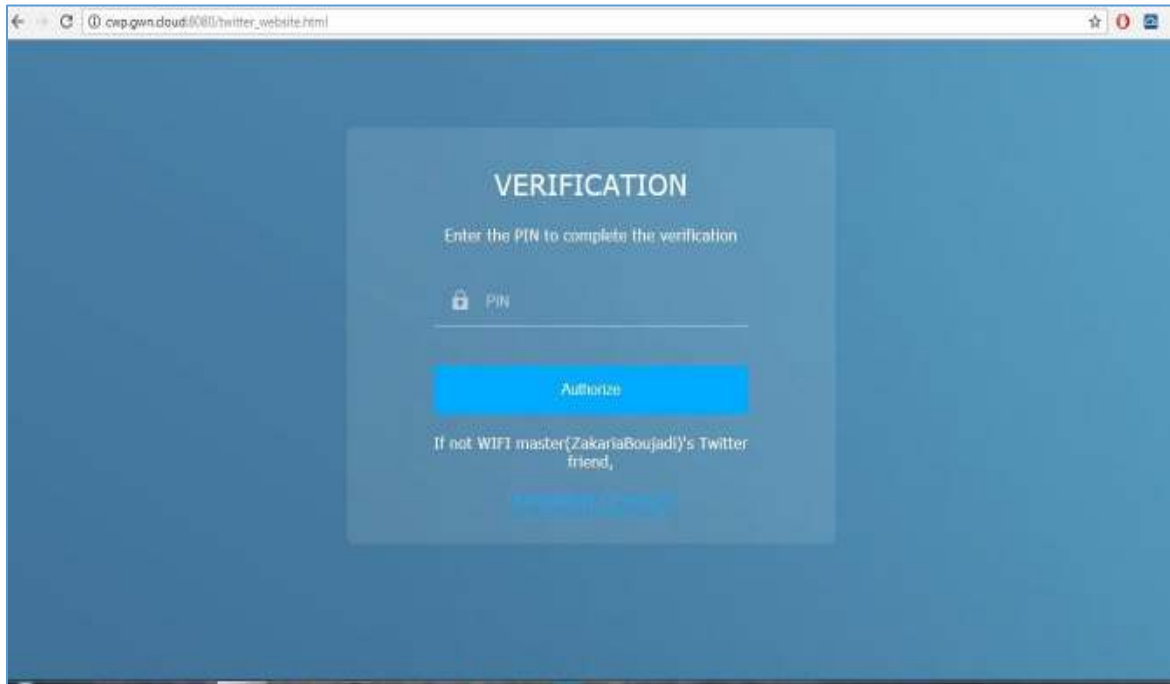


Figure 13 : PIN Verification Page

7. If code is valid, you will be authorized to use Internet.

Important Note:

- If **“Force To Follow”** option is enabled, clients will need to Follow Owner Twitter account before granting access to Internet.

