Grandstream Networks, Inc.

Captive Portal

Authentication via Twitter

Table of Content

Table of Figures

Table of Tables

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 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 WiFi.

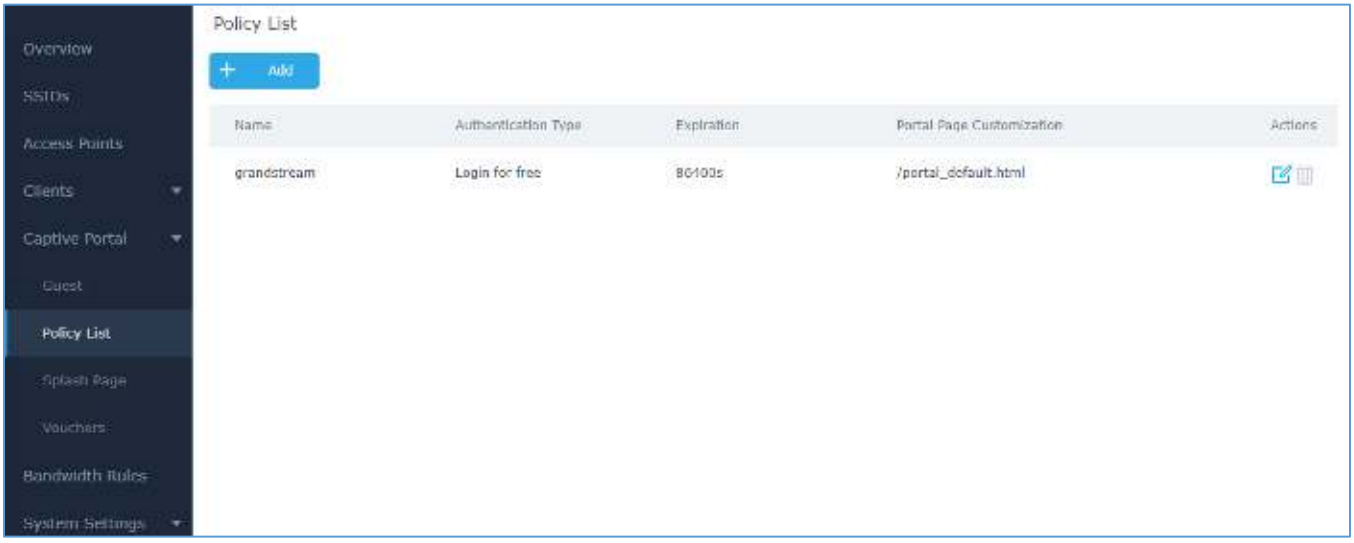


Figure 1: Captive Portal web GUI menu

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.

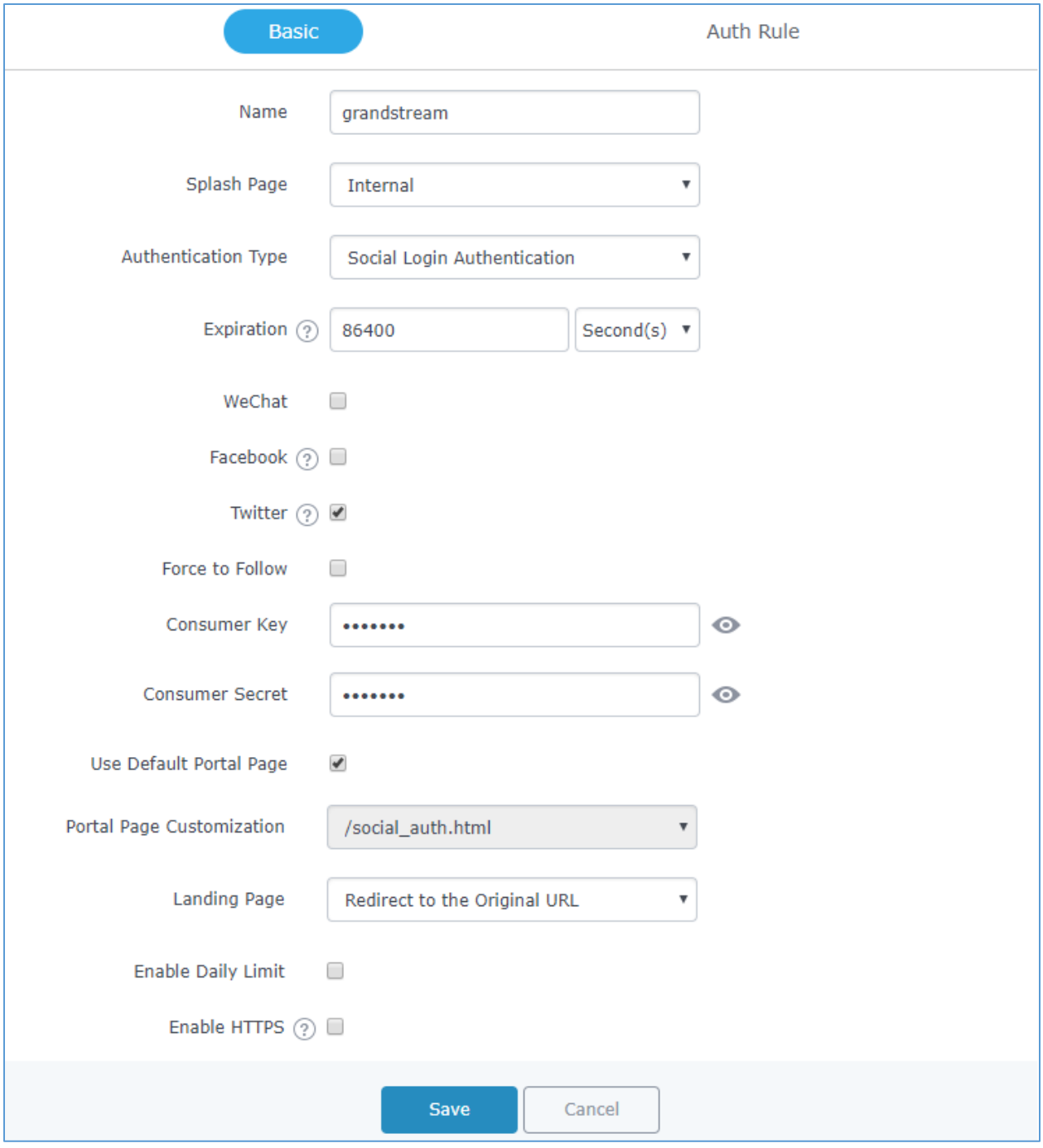


Figure 2: Policy Page Configuration

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	Following types of authentication are available: • **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	Check this box to enable Twitter Authentication. *This field appears only when **"Authentication Type"** option is set to "**Social Login Authentication**".*
Force to Follow	If checked, users need to Follow owner before being authenticated.
Owner	Enter the app Owner to use Twitter Login API. *This field appears only when **"Force to Follow"** option is checked.*
Consumer Key	Enter the app Key to use Twitter Login API. *This field appears only when **"Twitter"** option is checked.*
Consumer Secret	Enter the app secret to use Twitter Login API. *This field appears only when **"Twitter"** option is checked.*
Use Default Portal Page	When enabled, the default portal page will be used, otherwise users can upload their custom page.

Portal Page Customization	Select the customized portal page (if "Use Default Portal Page" is unchecked). • */terms_of_use/terms.html* • */facebook.html* • */password_auth.html* • */portal_default.html* • */portal_pass.html* • */portal_tip.html* • */social_auth.html* • */status.html* • */twitter.html* • */twitter_website.html* • */vouchers_auth.html* • */wechat.html*
Landing Page	Select page where authenticated clients will be redirected to. • **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	Once the landing page is set to redirect to external page, user should set the URL address for redirecting. *This field appears only when **Landing Page** is set to "Redirect to an External Page".*
Enable Daily Limit	If enabled, captive portal will limit user connection by time of one day.
Enable HTTPS	Check this box to enable captive portal over HTTPS.
Auth Rule	
Pre-Authentication Rules	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. When using Twitter, following rules will be added automatically and cannot be deleted:

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***

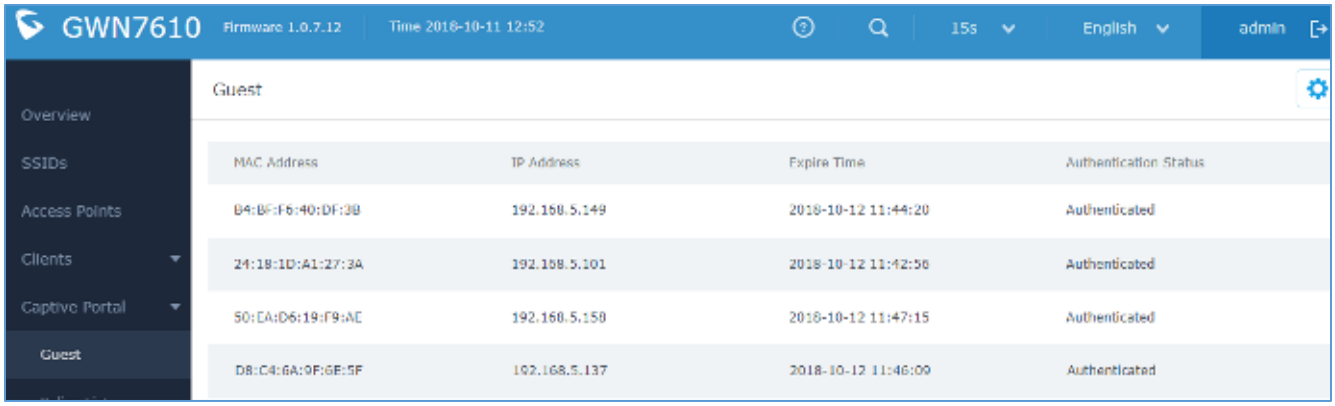


Figure 3: Client Web Page

CONFIGURATION STEPS

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

Create Twitter App

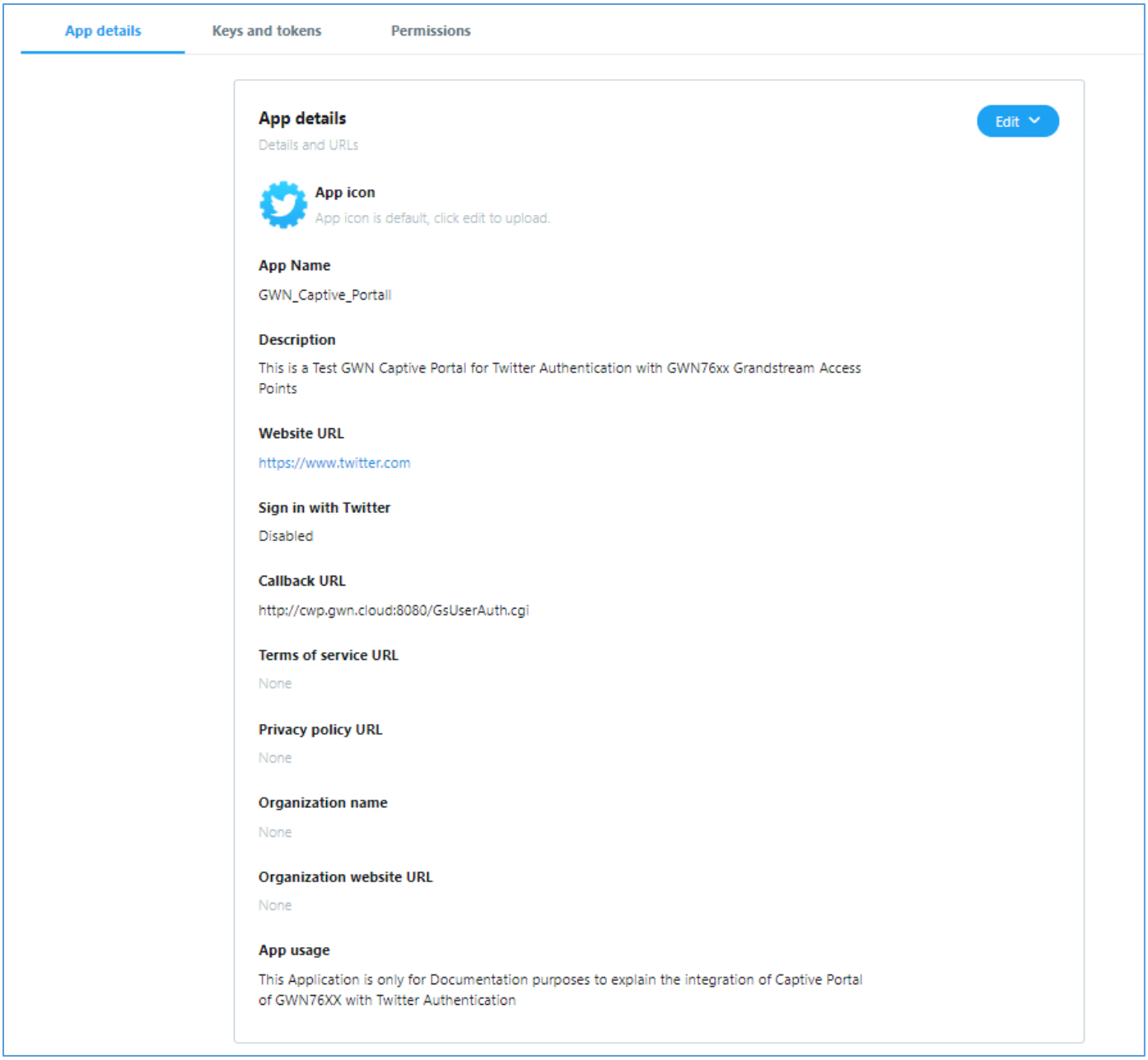
To use Twitter Login API, users need first to create an APP under developers' platform and set some OAuth settings to allow login authentication between GWN Access Points and Twitter servers.

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**

Figure 4: Twitter Application details

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



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.

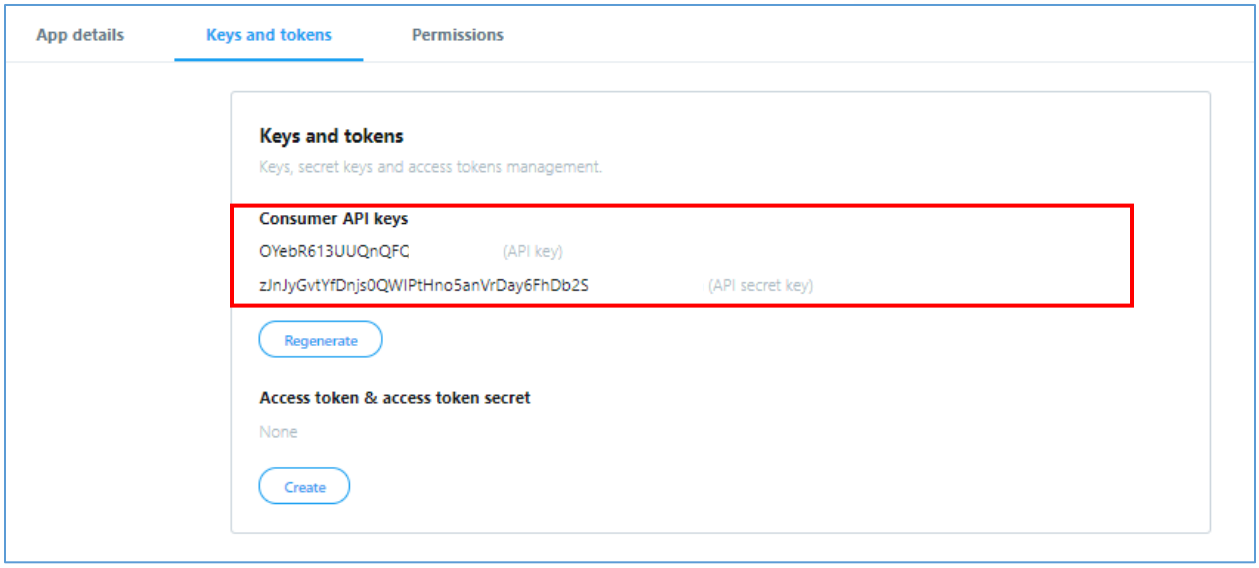


Figure 5: Twitter App keys and Access Tokens

Configure Captive Portal Policy with Twitter Authentication

After configuring the basic settings for the Twitter app, make sur 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.

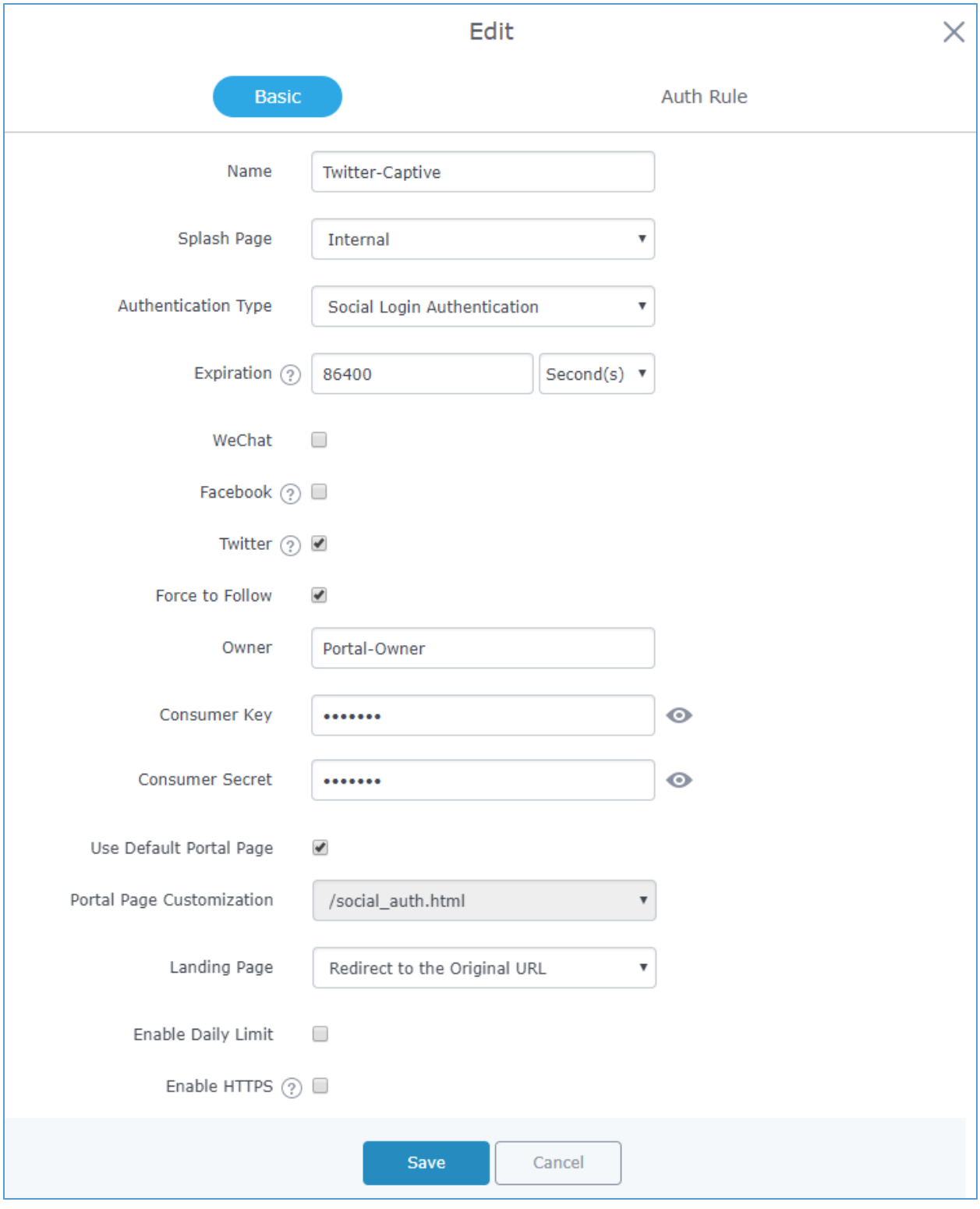


Figure 6: Captive Portal Policy Sample Configuration

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:

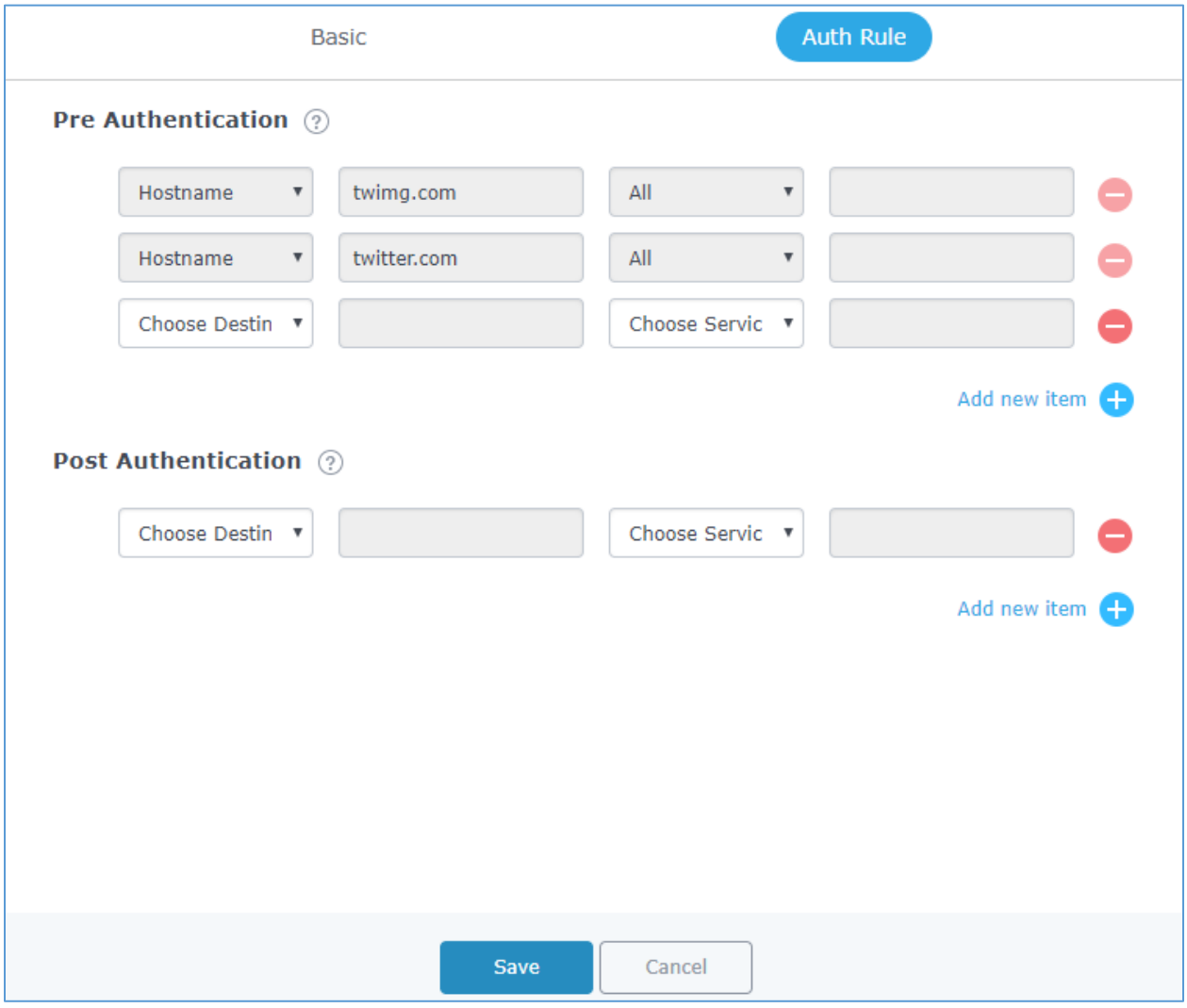


Figure 7: Pre-Authentication Rules for Twitter Authentication

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.

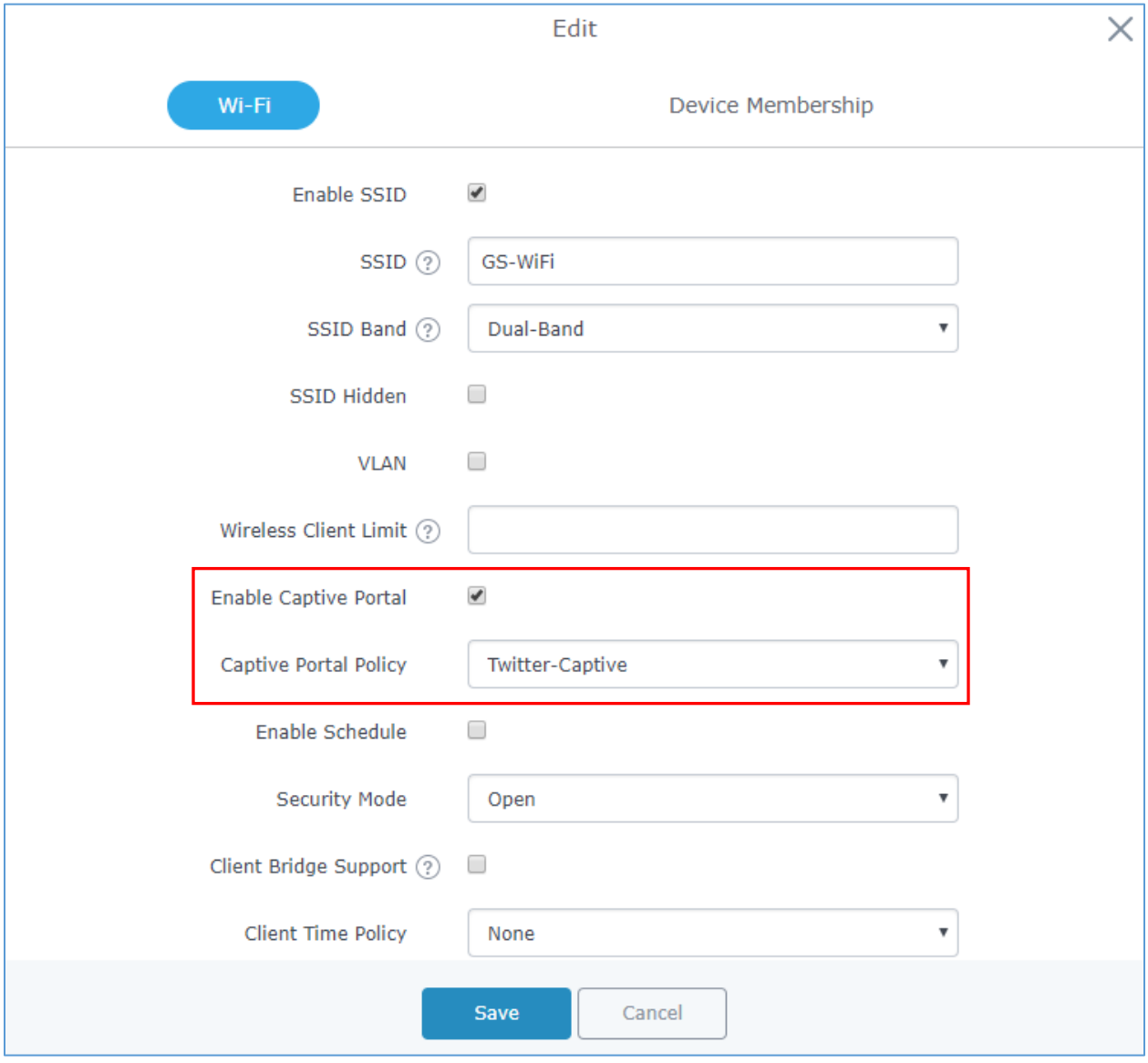


Figure 8: Enable Captive Portal on WiFi Settings

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.

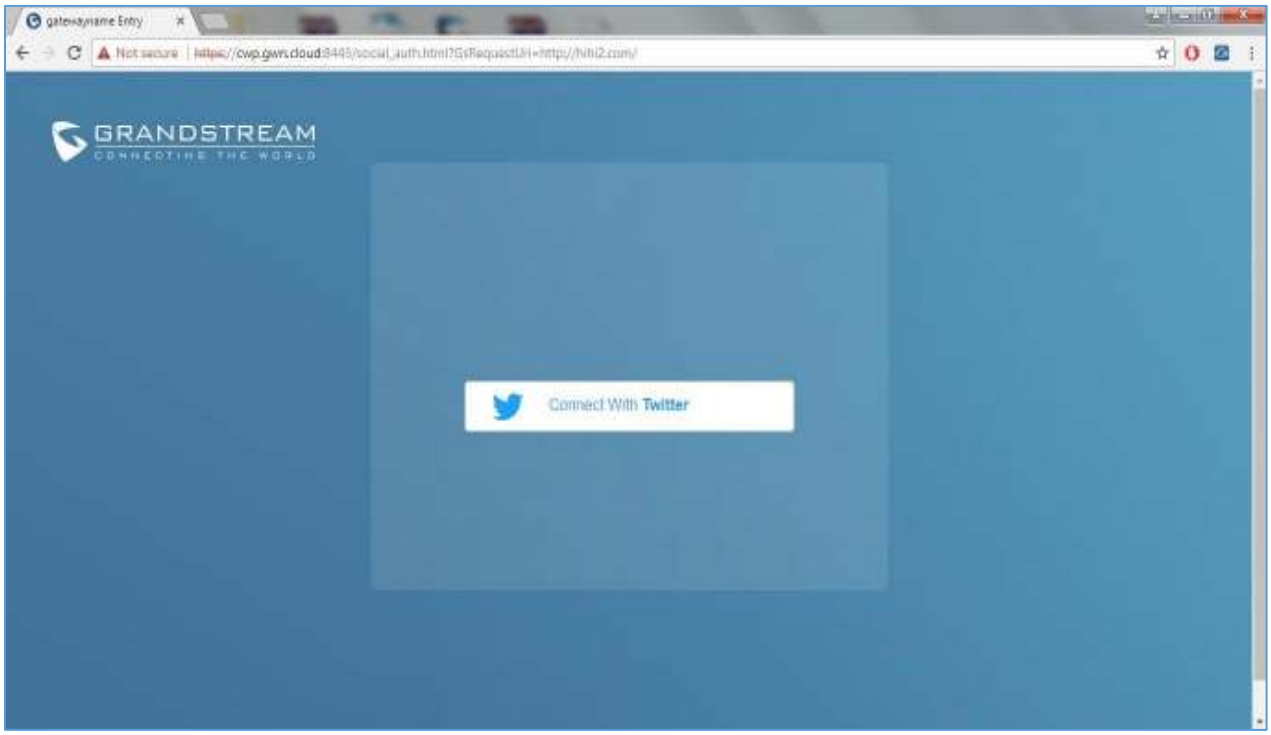


Figure 9: Login via Twitter Portal

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.

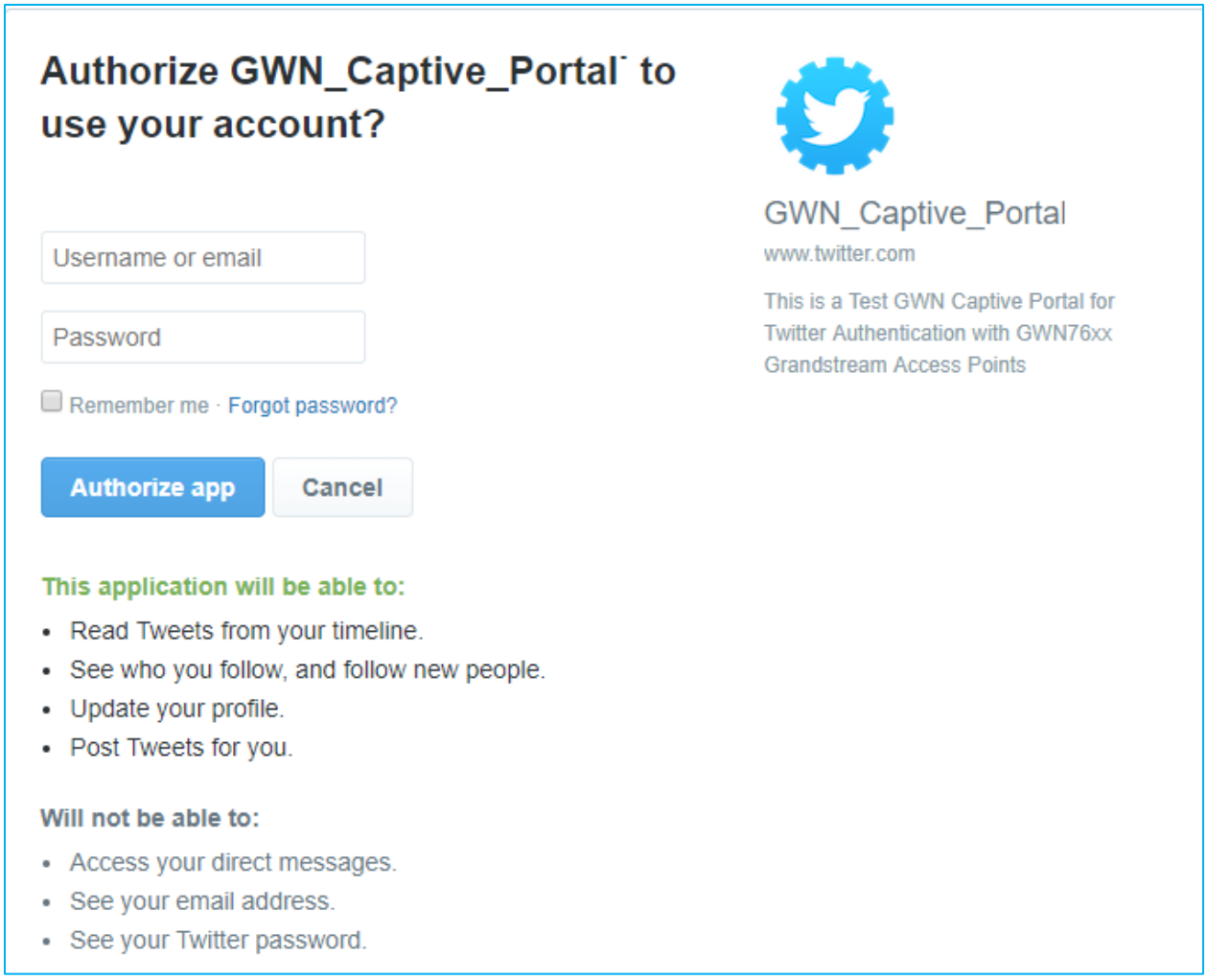


Figure 11: Twitter Login

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

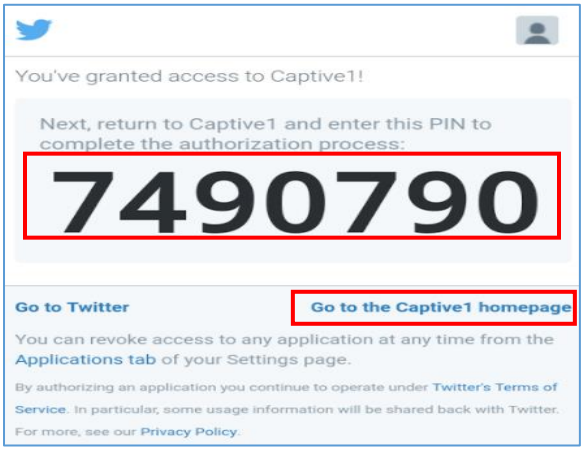


Figure 12 : PIN code

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.

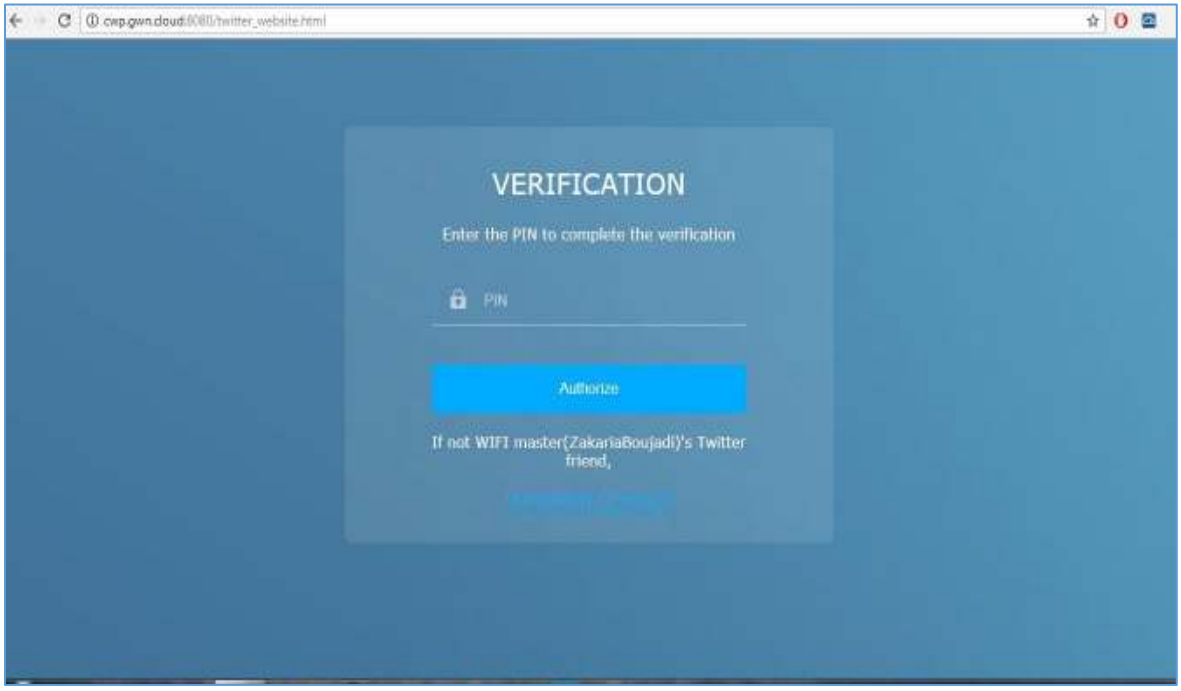


Figure 13 : PIN Verification Page

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.