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
GWN7610	Yes	1.0.5.11 or higher
GWN7600	Pending	Pending
GWN7600 LR	Pending	Pending
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 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.

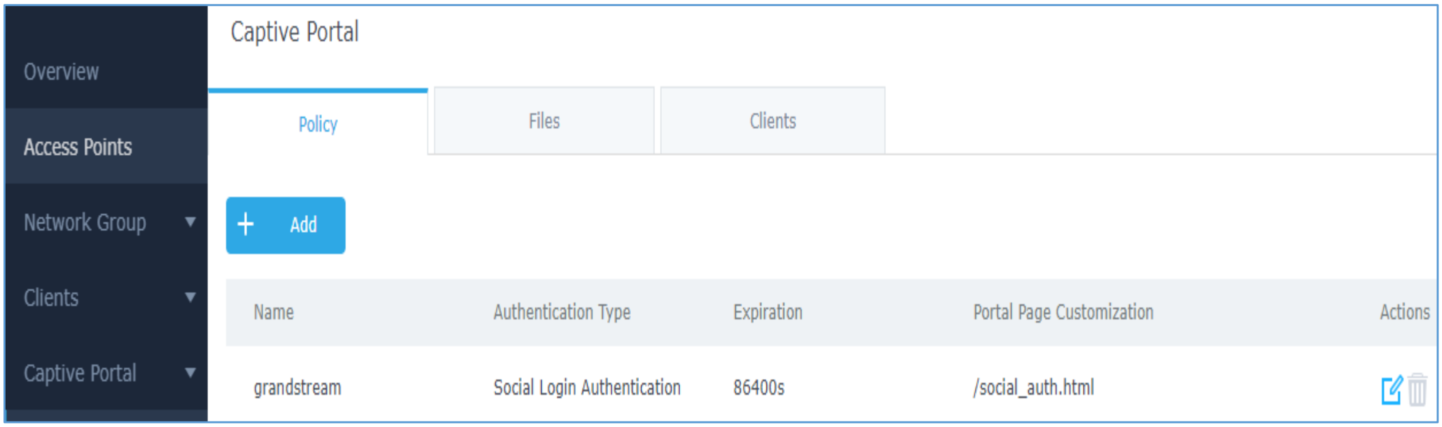
This guide describes how to setup the captive portal feature on the GWN76XX series using Twitter Authentication.

CAPTIVE PORTAL SETTINGS

The Captive Portal feature can be configured from the GWN76XX web page, by navigating to "**Captive Portal**".

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 specifc 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.



Name	Authentication Type	Expiration	Portal Page Customization	Actions
grandstream	Social Login Authentication	86400s	/social_auth.html	

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 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 the landing page, this field must contain an integer between 60 or 604800 in minutes. If this field is set to 0 the landing page will never expire.
Authentication Type	Three types of authentication are available: • **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. • **Social Login Authentication:** Choosing this option will allow users to log in using WeChat or Facebook or Twitter. We will be using this Twitter authentication type on this guide. • **Vouchers:** Choosing this option will allow users to log in using Vouchers. • **Simple Password:** Choosing this option will allow users to log in using simple password.
Twitter	Check this box to enable Twitter Authentication.
Owner	Enter the app Owner to use Twitter Login API.
Consumer key	Enter the app Key to use Twitter Login API.
Consumer Secret	Enter the app secret to use Twitter Login API.
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. • **Social Auth:** Choose this page when using authentication via WeChat or Facebook or Twitter. • **Vouchers Auth:** Choose this page when using authentication via Vouchers. • **Password Auth:** Choose this page when using authentication via Simple password.

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	When setting the landing page to (Redirect External Page), enter the URL where to send authenticated clients.
Enable HTTPS	Check this box to enable captive portal over HTTPS.
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.
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.

Post-Authentication Rules

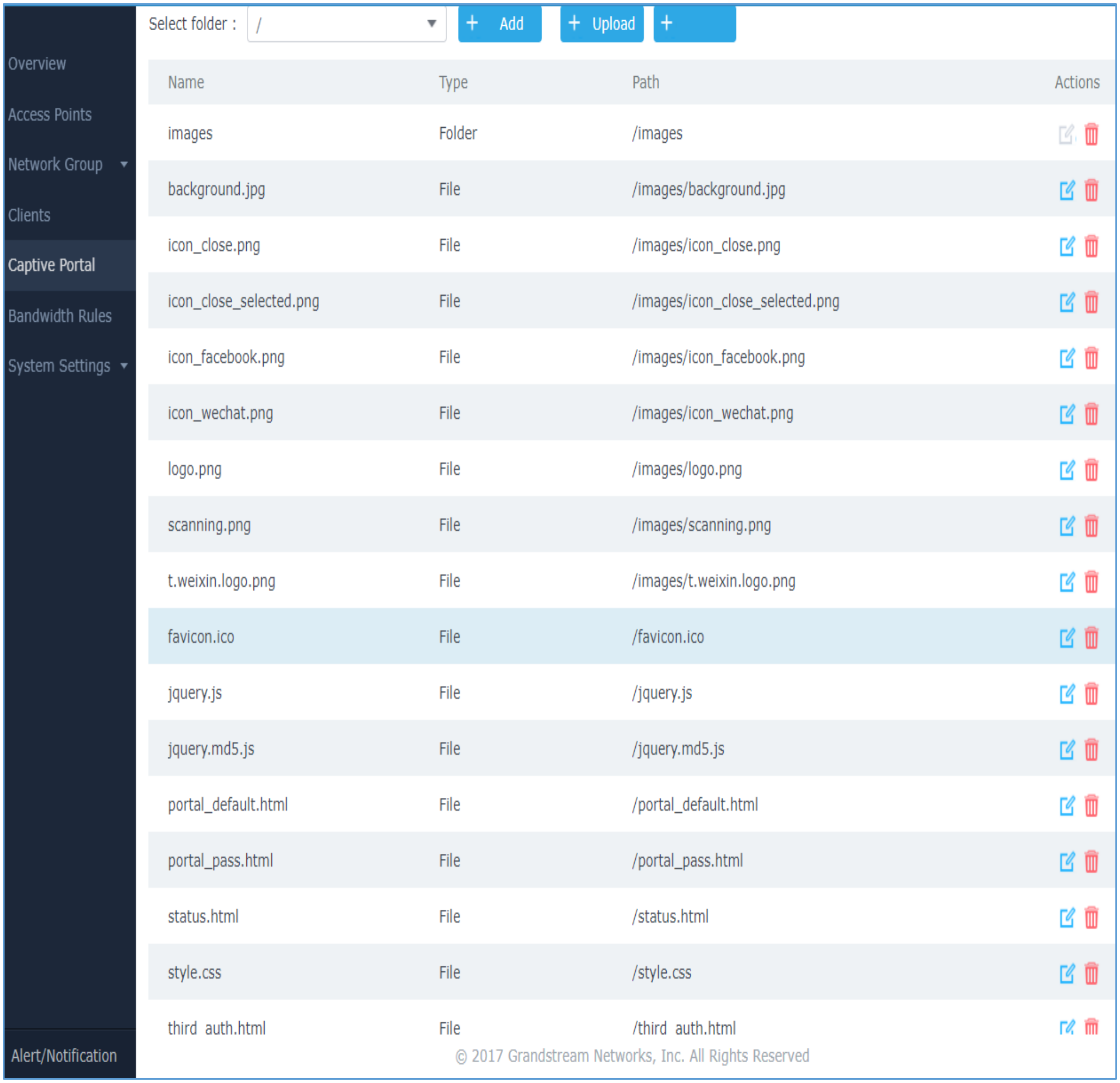
On the other hand, post authentication rules are used to match traffic that will be banned for WiFi clients after authentication. As an example, if you want to disallow connected WiFi clients to issue Telnet or SSH traffic after authentication then you can set post authentication rules to match that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

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 Twitter authentication, users need to select **Social_auth.html** as the portal page to let the user login via Twitter.

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



Name	Type	Path	Actions
images	Folder	/images	
background.jpg	File	/images/background.jpg	
icon_close.png	File	/images/icon_close.png	
icon_close_selected.png	File	/images/icon_close_selected.png	
icon_facebook.png	File	/images/icon_facebook.png	
icon_wechat.png	File	/images/icon_wechat.png	
logo.png	File	/images/logo.png	
scanning.png	File	/images/scanning.png	
t.weixin.logo.png	File	/images/t.weixin.logo.png	
favicon.ico	File	/favicon.ico	
jquery.js	File	/jquery.js	
jquery.md5.js	File	/jquery.md5.js	
portal_default.html	File	/portal_default.html	
portal_pass.html	File	/portal_pass.html	
status.html	File	/status.html	
style.css	File	/style.css	
third auth.html	File	/third auth.html	

© 2017 Grandstream Networks, Inc. All Rights Reserved

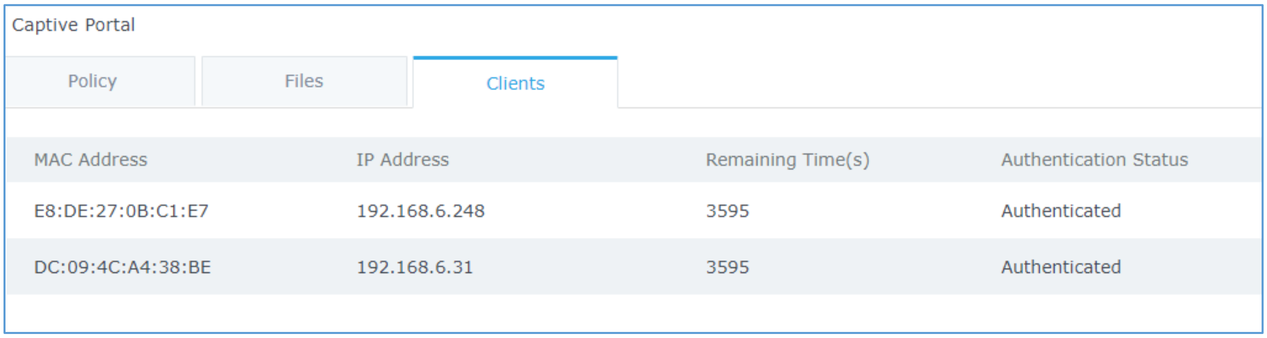
Figure 2: Files Web Page

- Click ✎ to upload a new web page.
- Click ⊕ Add Folder to add a new folder.
- Click ⊕ 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***



MAC Address	IP Address	Remaining Time(s)	Authentication Status
E8:DE:27:0B:C1:E7	192.168.6.248	3595	Authenticated
DC:09:4C:A4:38:BE	192.168.6.31	3595	Authenticated

Figure 3: Client Web Page

CONFIGURATION STEPS

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

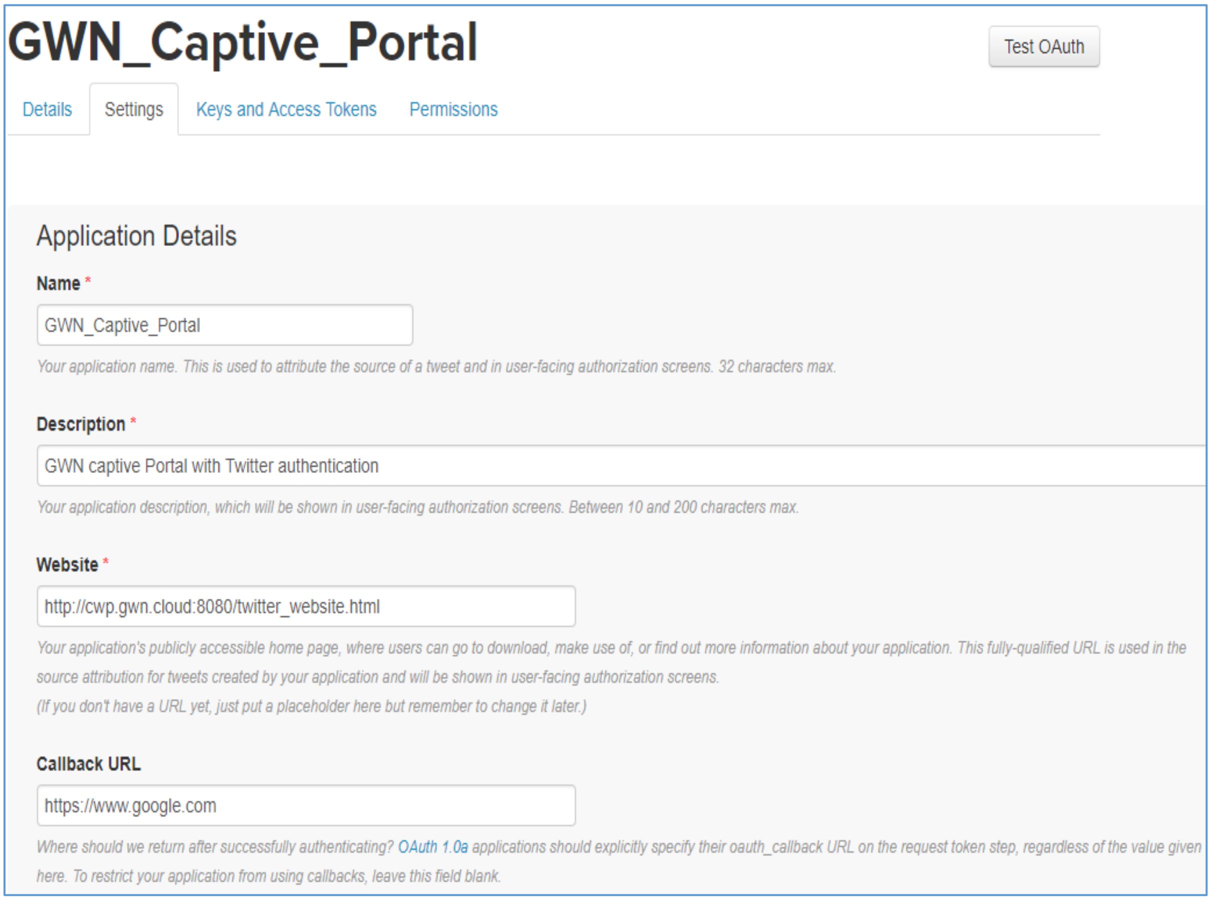
Create Twitter App

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://apps.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 "Website" field, enter **http://cwp.gwn.cloud:8080/twitter_website.html**



Application Details

Name *

GWN_Captive_Portal

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

Description *

GWN captive Portal with Twitter authentication

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

Website *

http://cwp.gwn.cloud:8080/twitter_website.html

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens.
(If you don't have a URL yet, just put a placeholder here but remember to change it later.)

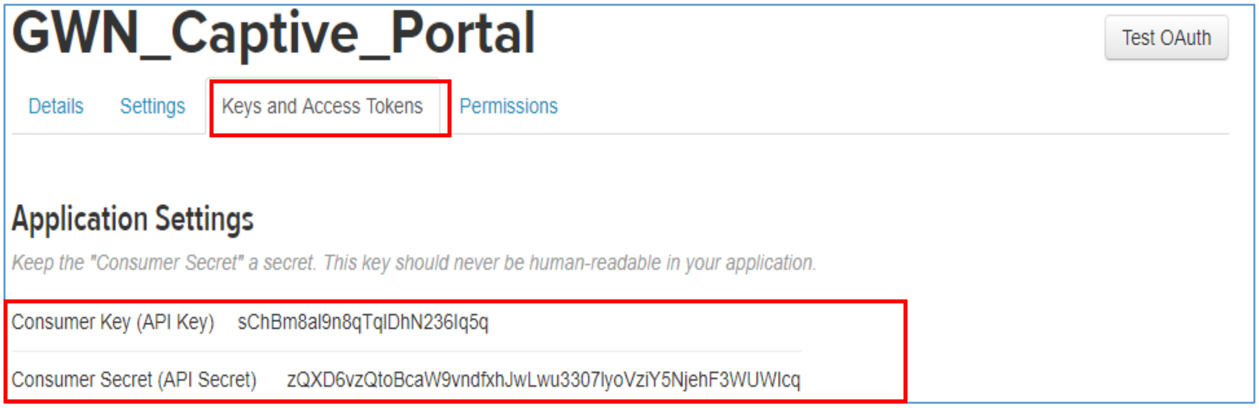
Callback URL

https://www.google.com

Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

Figure 4: Twitter Application details

5. 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.



GWN_Captive_Portal

Application Settings

Keep the "Consumer Secret" a secret. This key should never be human-readable in your application.

Consumer Key (API Key)	sChBm8al9n8qTqlDhN236lq5q
Consumer Secret (API Secret)	zQXD6vzQtoBcaW9vndfxhJwLwu3307lyoVziY5NjehF3WUWlcq

Figure 5: Twitter App keys and Access Tokens

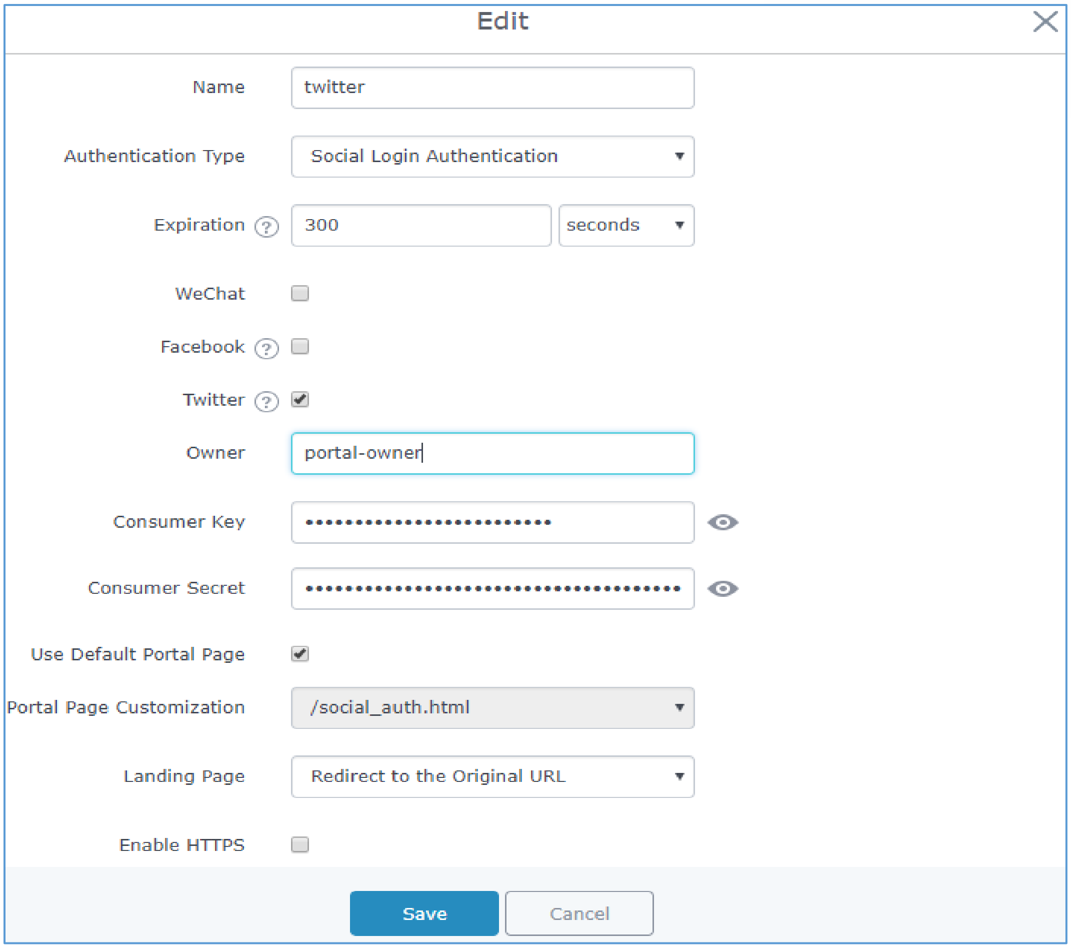
Configure Captive Portal Policy with Twitter Authentication

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**.
- Portal Page Customization: **/Social_auth.html**

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



Edit

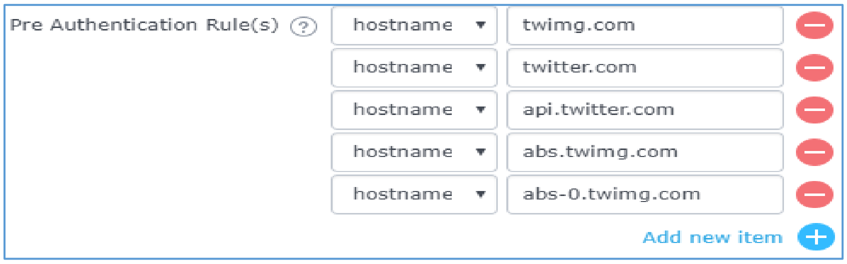
Name	twitter
Authentication Type	Social Login Authentication ▾
Expiration ?	300 seconds ▾
WeChat	□
Facebook ?	□
Twitter ?	☑
Owner	portal-owner
Consumer Key	••••••••••••••••••••••••
Consumer Secret	••••••••••••••••••••••••••••••••••••
Use Default Portal Page	☑
Portal Page Customization	/social_auth.html ▾
Landing Page	Redirect to the Original URL ▾
Enable HTTPS	□

Figure 6: Captive Portal Policy Sample Configuration

Pre-Authentication Rules

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

Following figure shows the hostnames that should be included.



Pre Authentication Rule(s) ?

hostname ▾	twimg.com
hostname ▾	twitter.com
hostname ▾	api.twitter.com
hostname ▾	abs.twimg.com
hostname ▾	abs-0.twimg.com

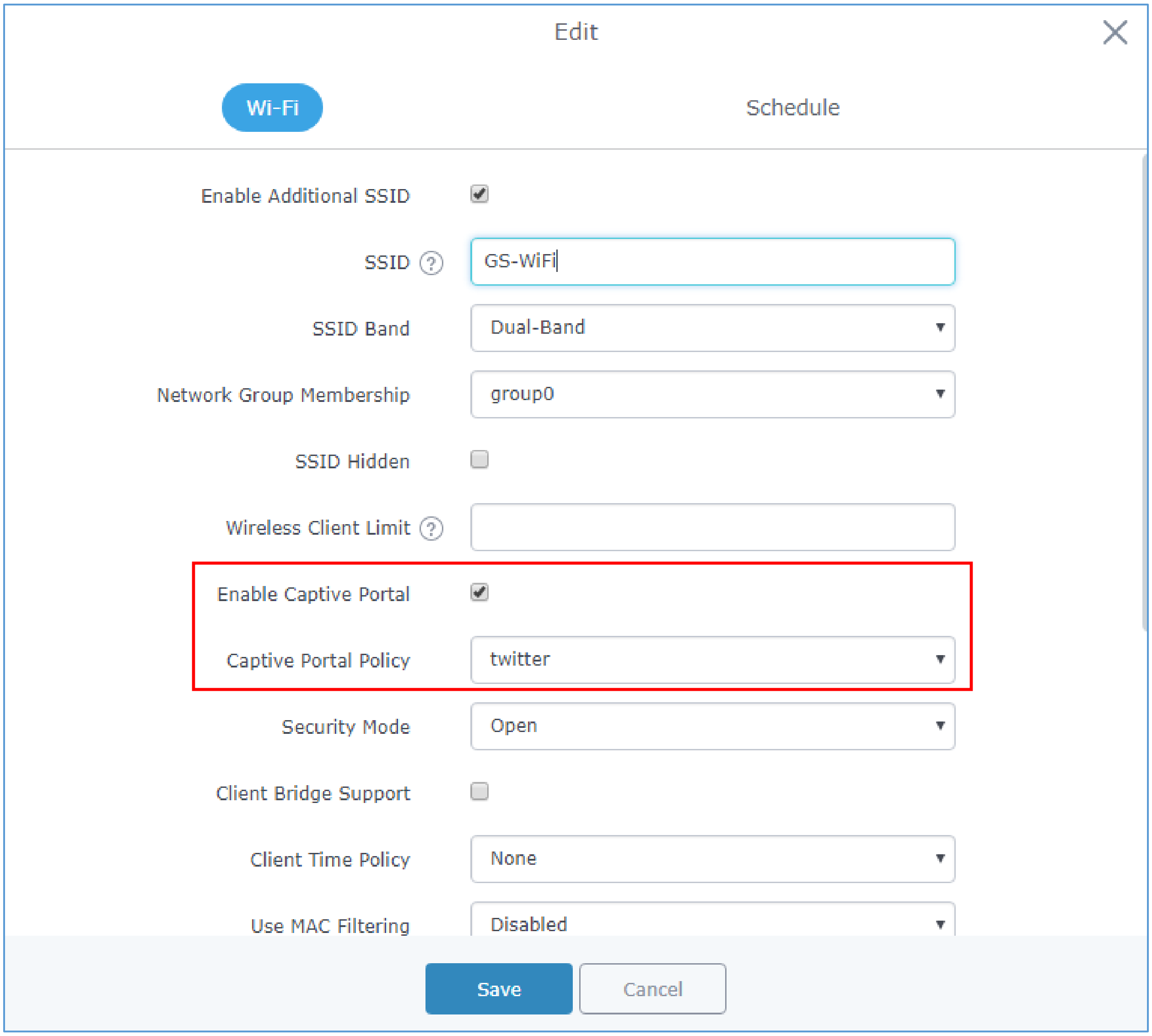
Figure 7: Pre-Authentication Rules for Twitter Authentication

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 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 Twitter 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 Captive Portal**", then select the configured policy from the drop-down policy as shown on the following figure.



Enable Additional SSID ☑

SSID: GS-WiFi

SSID Band: Dual-Band

Network Group Membership: group0

SSID Hidden □

Wireless Client Limit:

Enable Captive Portal ☑

Captive Portal Policy: twitter

Security Mode: Open

Client Bridge Support □

Client Time Policy: None

Use MAC Filtering: Disabled

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.

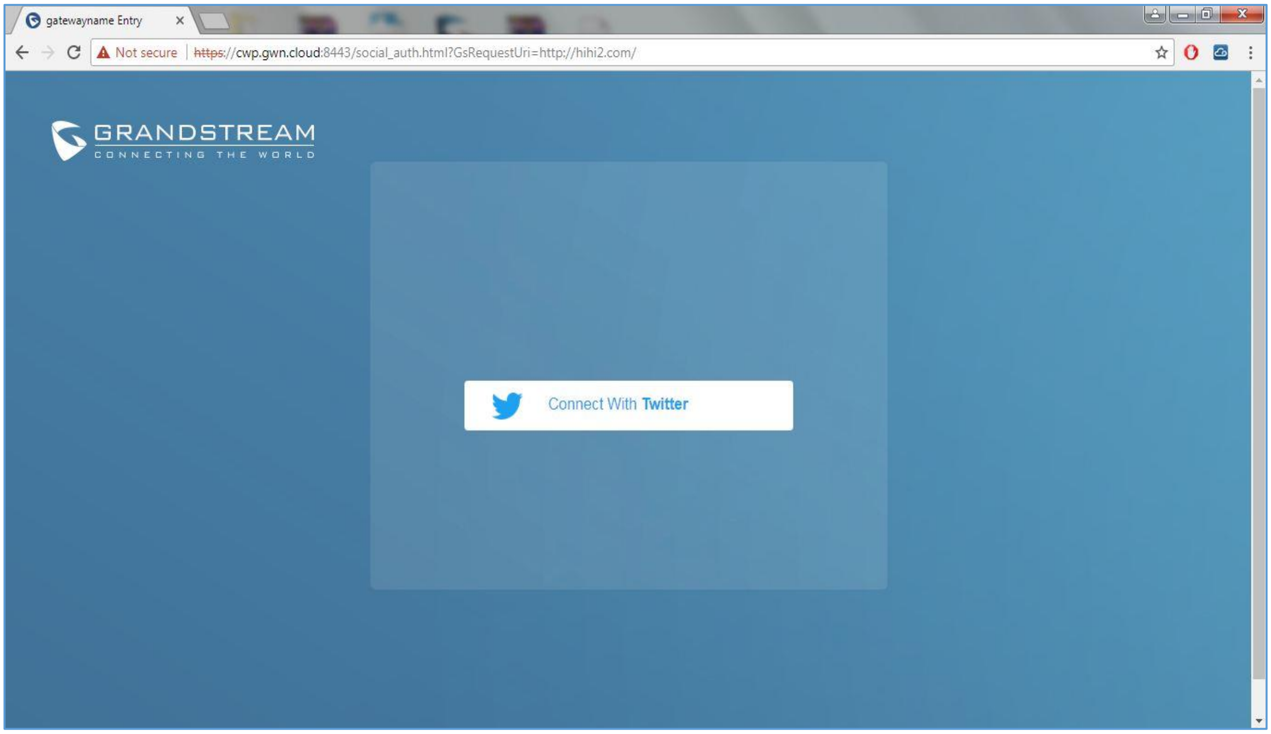
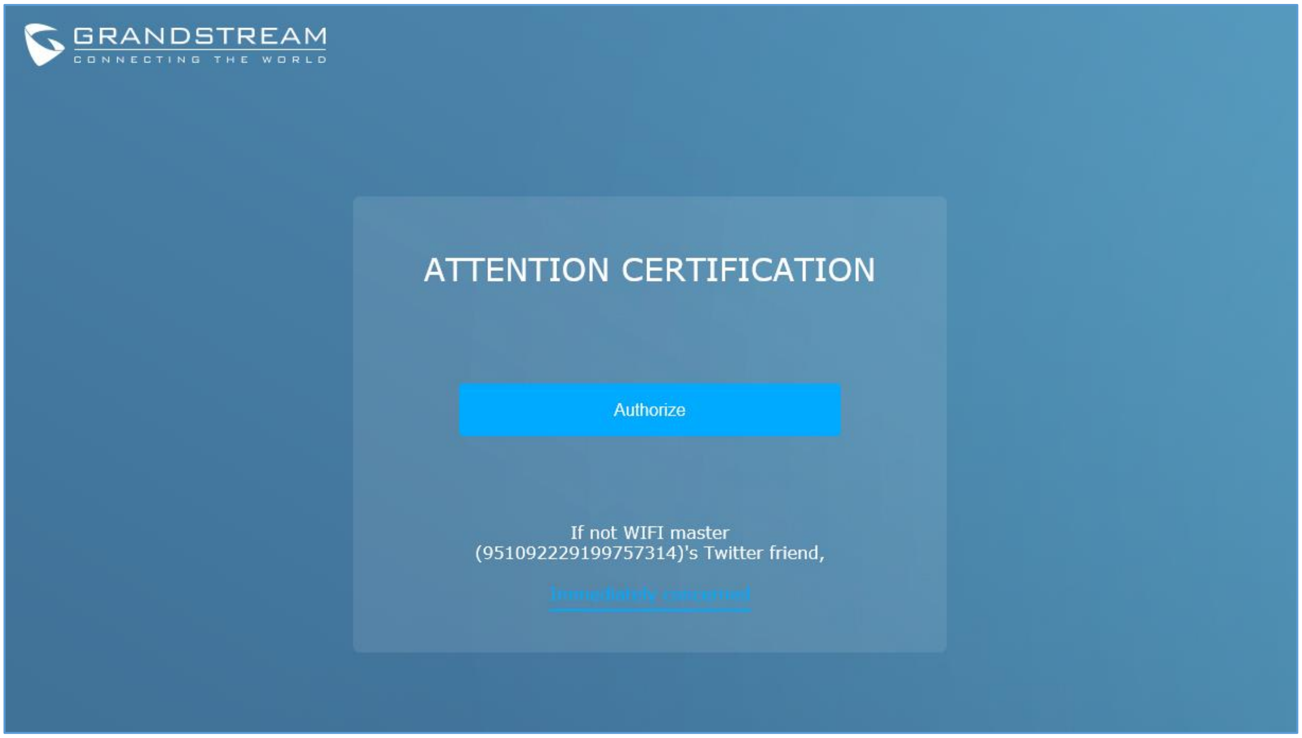


Figure 9: Login via Twitter Portal

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.

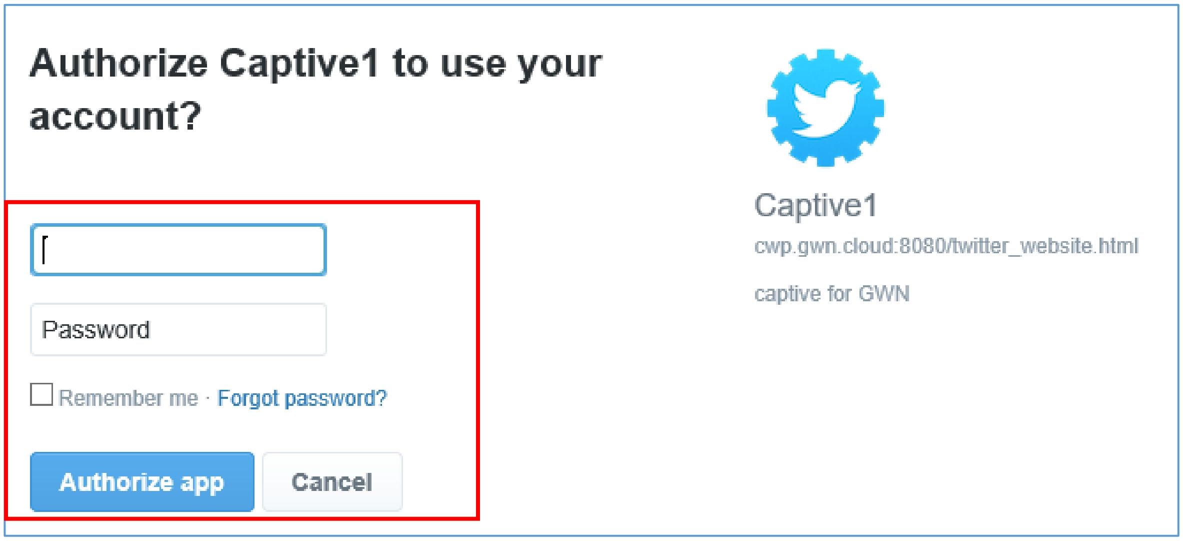

ATTENTION CERTIFICATION

If not WIFI master (951092229199757314)'s Twitter friend,

Figure 10: Twitter – Authorize

3. Enter your Twitter account credentials.

   Important note: The twitter account to login with needs to be a follower of the application owner.


Authorize Captive1 to use your account?

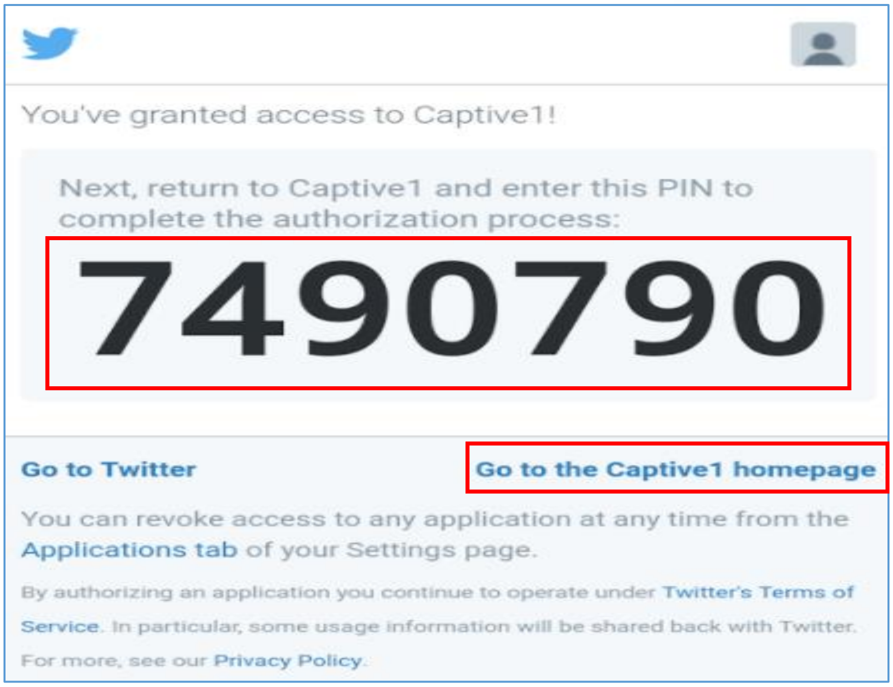
Captive1

cwp.gwn.cloud:8080/twitter_website.html

captive for GWN

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.



You've granted access to Captive1!

Next, return to Captive1 and enter this PIN to complete the authorization process:

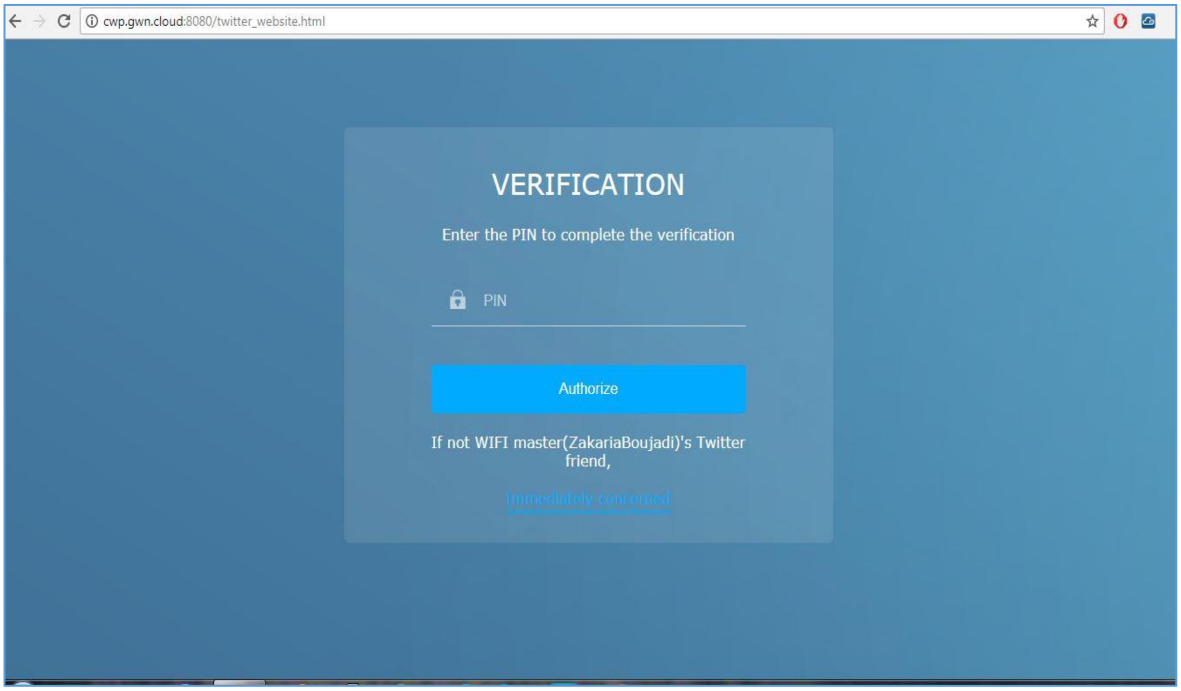
7490790

You can revoke access to any application at any time from the Applications tab of your Settings page.

By authorizing an application you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy.

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.



cwp.gwn.cloud:8080/twitter_website.html

VERIFICATION

Enter the PIN to complete the verification

If not WIFI master(ZakariaBoujadi)'s Twitter friend,

Figure 13 : PIN Verification Page

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