Grandstream Networks, Inc.

Captive Portal Guide

Table of Content

Table of Figures

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 portals 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 deploy and setup the captive portal feature on the GWN76XX series.

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

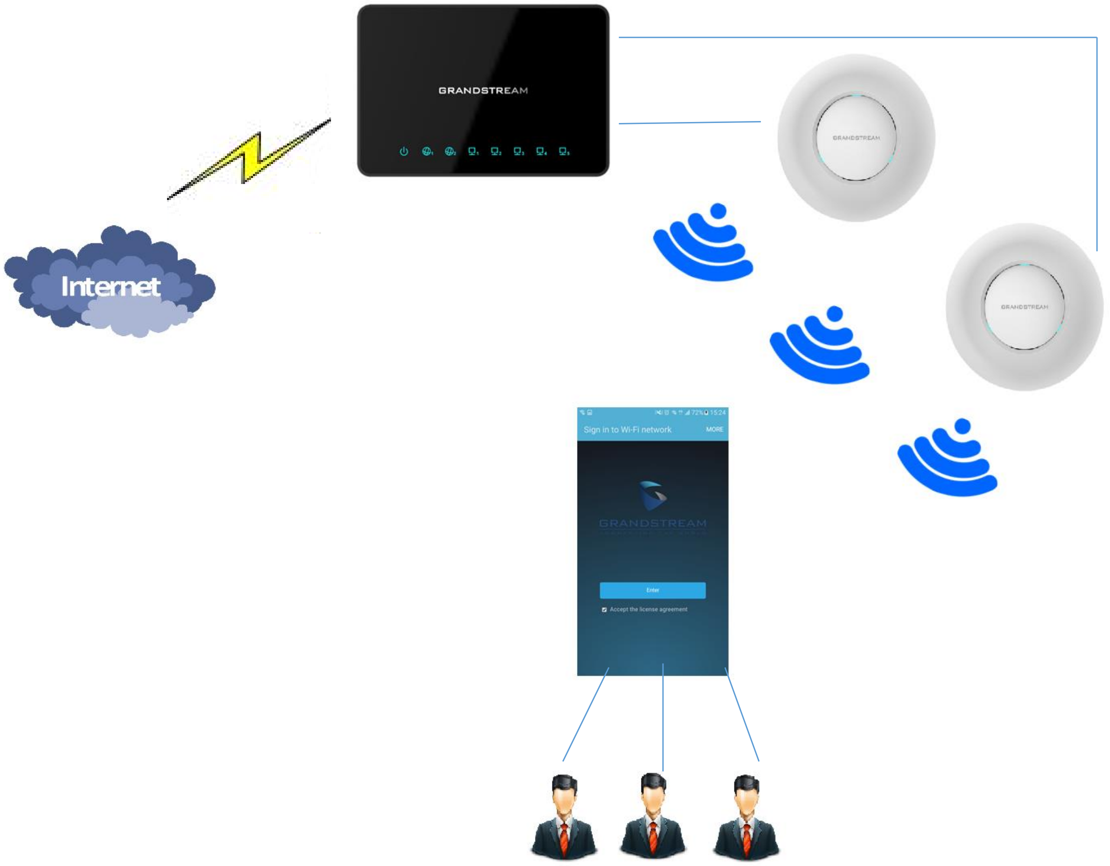


Figure 1: General Architecture

CAPTIVE PORTAL SETTINGS

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

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

Basic Configuration Page

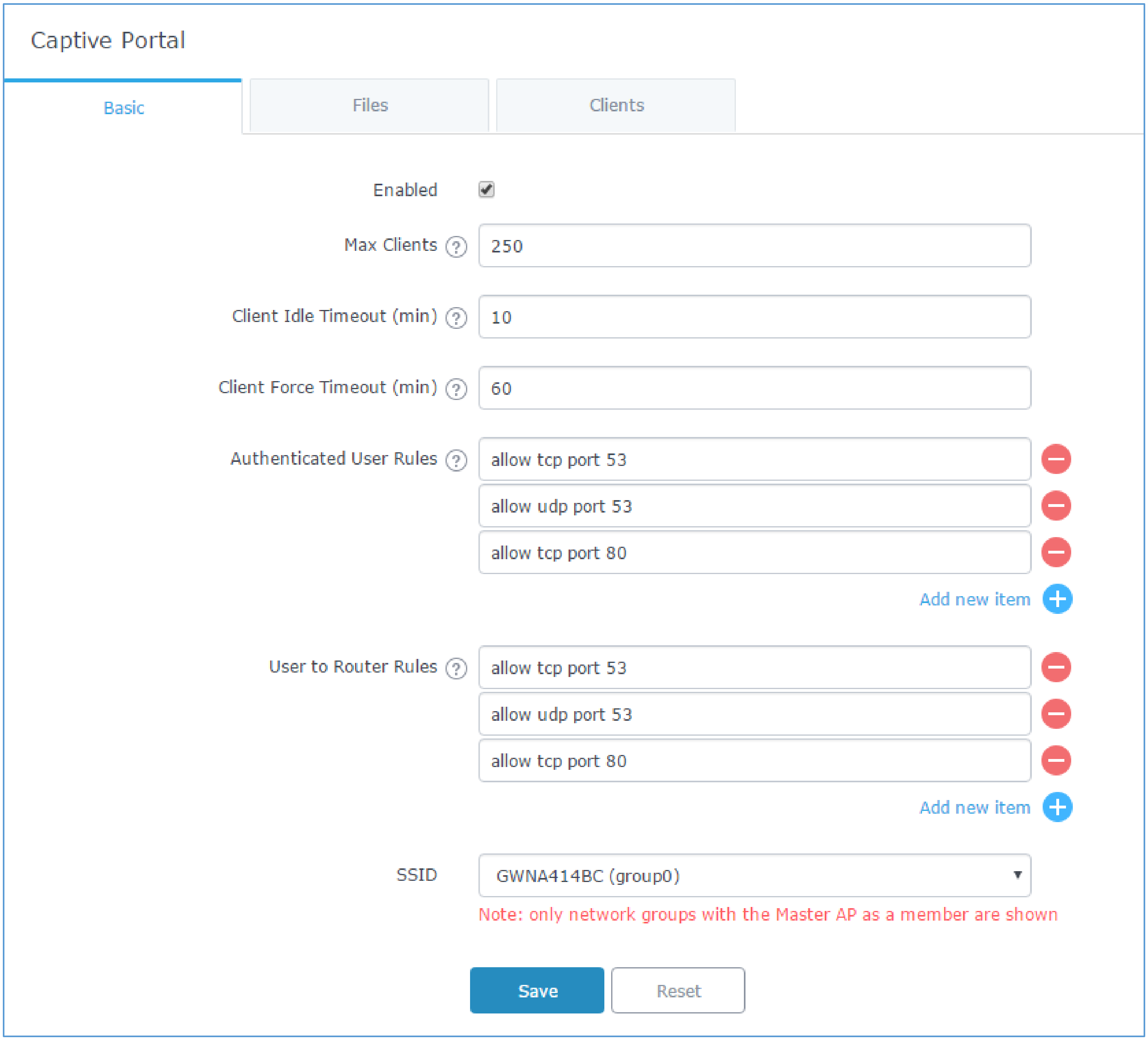
The basic configuration page contains options to enable/disable the captive portal feature, related firewall rules and timeout settings. The following table describes all the settings on this page:

Table 1: Basic Configuration Page

Field	Description
Enable	Check this option to enable/disable the captive portal feature. If disabled, configuration and uploaded files will not be lost. If enabled, WiFi users will be redirected to defined landing page before accessing Internet.
Max Clients	Specifies the maximum number of clients that can connect to the network via the captive portal feature.
Client Idle Timeout (min)	Configures the time of inactivity after which the client will be automatically de-authenticated. Valid range between 10 to 240. Default is **30** min.
Client Force Timeout (min)	Configures the time after which the client will be automatically de-authenticated without considering his status (active or idle). Valid range between 10 to 240. Default is **60** min.
Authenticated User Rules	Defines and manages rules for traffic from Router to Authenticated Users. Default/Typical Authenticated User Rules: • **allow tcp port 22** This rule allows traffic over TCP on port 22 (SSH) • **allow tcp port 53** This rule allows traffic over TCP on port 53 (DNS) • **allow udp port 53** This rule allows traffic over UDP on port 53 (DNS) • **allow tcp port 80** This rule allows traffic over TCP on port 80 (HTTP) • **allow tcp port 443** This rule allows traffic over TCP on port 443 (HTTPS) **Notes:** ▪ Not defined rules for specific ports are denied by default. ▪ These rules are applied in order. Rule syntax is the following: **allow/deny tcp/udp port <port number>**.

	Examples: The following rules will allow FTP access and deny TFTP. *allow tcp port 20* *allow tcp port 21* *deny udp port 69* **Note**: Users can Click on ⊖ to delete an existing rule or ⊕ to add a new rule.
User to Router Rules	Defines and manages rules for traffic from Users to Router. Default/Typical User to Router Rules: • **allow tcp port 22** This rule allows traffic over TCP on port 22 (SSH) • **allow tcp port 23** This rule allows traffic over TCP on port 23 (TELNET) • **allow tcp port 53** This rule allows traffic over TCP on port 53 (DNS) • **allow udp port 53** This rule allows traffic over UDP on port 53 (DNS) • **allow udp port 67** This rule allows traffic over UDP on port 67 (DHCP) • **allow tcp port 80** This rule allows traffic over TCP on port 80 (HTTP) • **allow tcp port 443** This rule allows traffic over TCP on port 443 (HTTPS) **Notes:** ▪ Not defined rules for specific ports are denied by default. ▪ These rules are applied in order. Rule syntax is the following: **allow/deny tcp/udp port <port number>**. **Note**: Users can Click on ⊖ to delete an existing rule or ⊕ to add a new rule.
Network Group	Selects the network group from the drop-down list where authenticated clients will belong to.

The following figure shows default Basic settings configuration:



Captive Portal

Enabled ☑

Max Clients: 250

Client Idle Timeout (min): 10

Client Force Timeout (min): 60

Authenticated User Rules:
- allow tcp port 53
- allow udp port 53
- allow tcp port 80

User to Router Rules:
- allow tcp port 53
- allow udp port 53
- allow tcp port 80

SSID: GWNA414BC (group0)

Note: only network groups with the Master AP as a member are shown

Figure 2: Basic Configuration Page

Files Configuration Page

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

The captive portal uses **splash.html** as landing page, WiFi clients will be redirected to this page before accessing Internet.

The following figure shows default **splash.html** page:

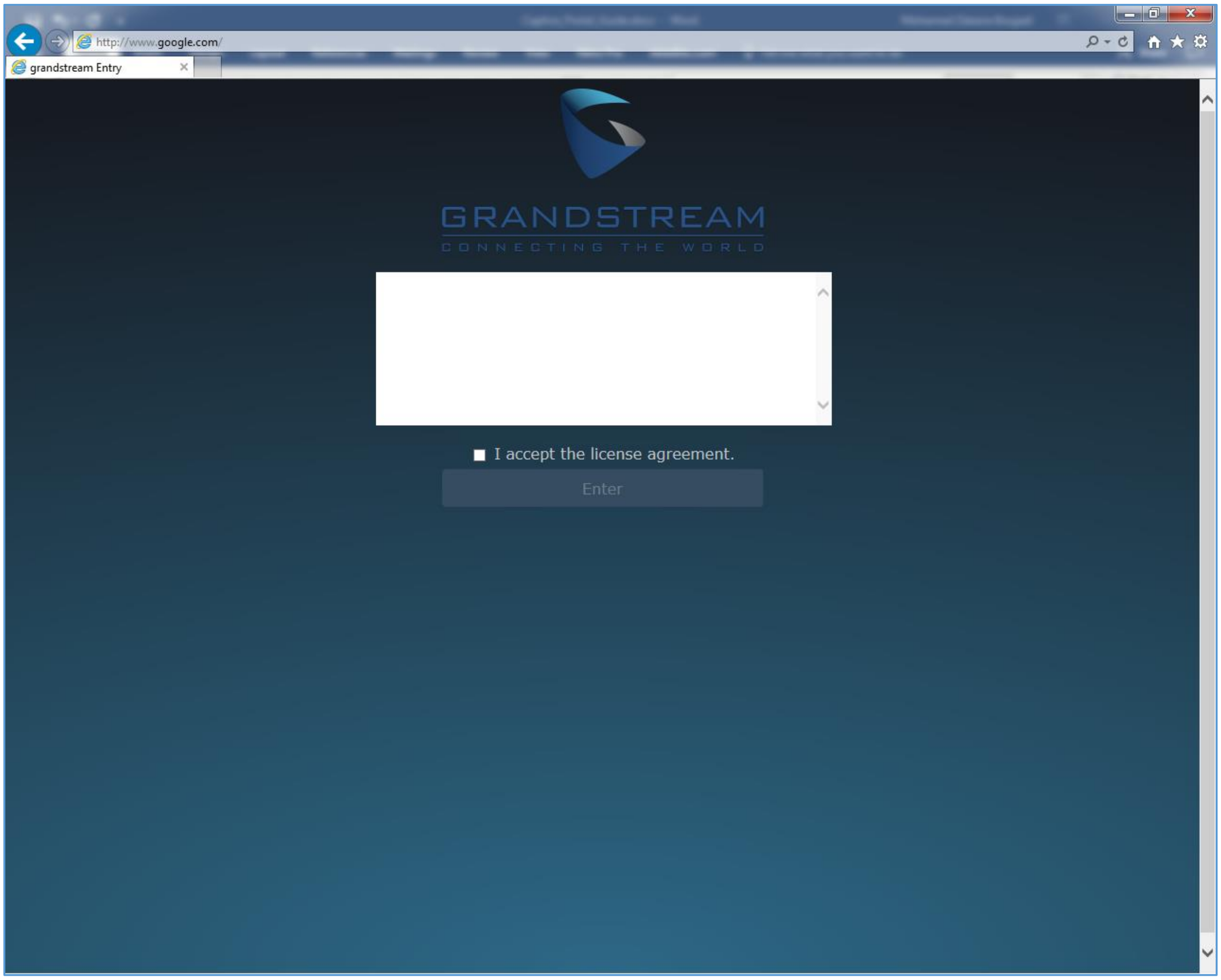
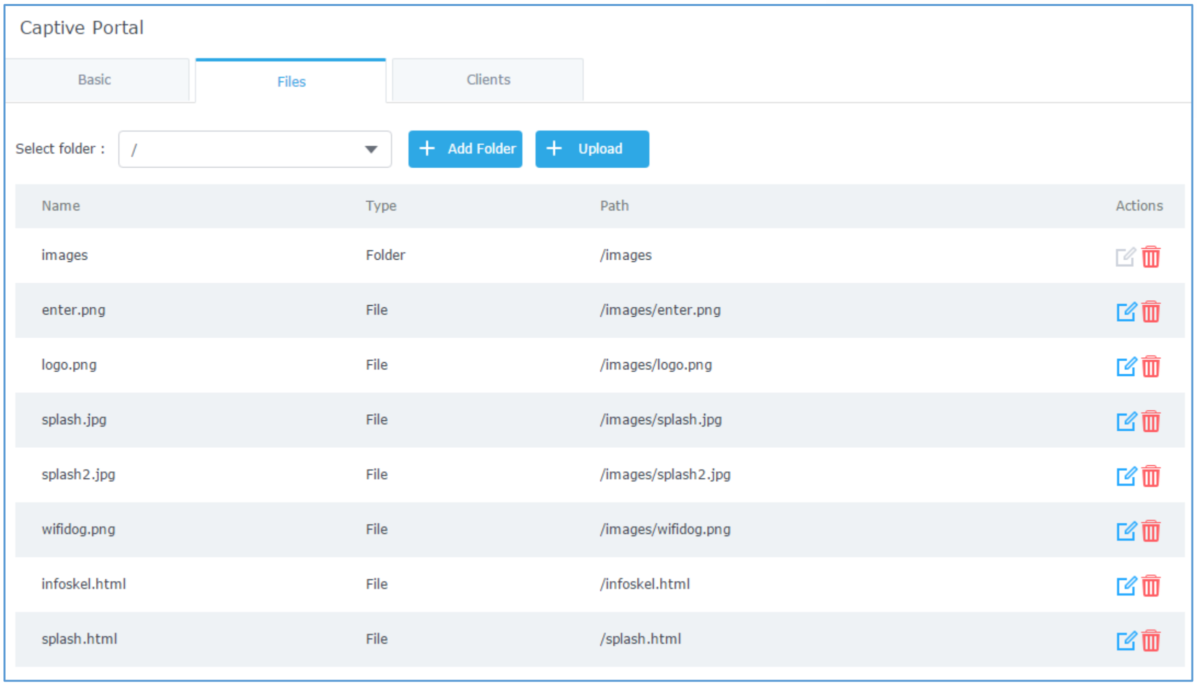


Figure 3: Default « splash.html » page

The following figure shows default files used for Captive Portal:



Captive Portal

Select folder : /

Name	Type	Path	Actions
images	Folder	/images	✎ 🗑
enter.png	File	/images/enter.png	✎ 🗑
logo.png	File	/images/logo.png	✎ 🗑
splash.jpg	File	/images/splash.jpg	✎ 🗑
splash2.jpg	File	/images/splash2.jpg	✎ 🗑
wifidog.png	File	/images/wifidog.png	✎ 🗑
infoskel.html	File	/infoskel.html	✎ 🗑
splash.html	File	/splash.html	✎ 🗑

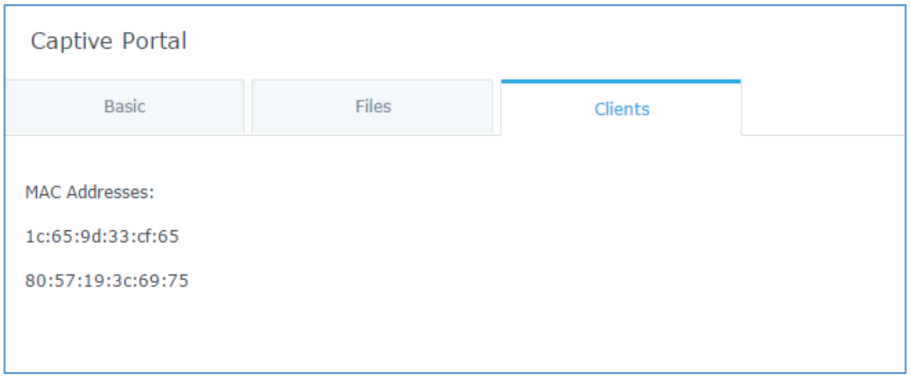
Figure 4: Files Web Page

- 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 ▾.

Landing page can be customized depending on customer's needs. Please refer to [CAPTIVE PORTAL CUSTOMIZATION] for more details and example.

Clients Page

Clients page lists MAC addresses of authenticated devices using captive portal.



Captive Portal

MAC Addresses:

1c:65:9d:33:cf:65

80:57:19:3c:69:75

Figure 5: Client Web Page

CAPTIVE PORTAL CUSTOMIZATION

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

Environment Setup Example

We consider that ABC company has deployed GWN76xx Access Points and wants to configure Captive Portal.

Below are ABC company requirements:

- The landing page should be customized with ABC company logo and “Terms of Use”.
- Users need to read and accept “Terms and Conditions” to get Internet access.
- Connected clients will be allowed to access websites using HTTP only.
- If a client is inactive for 10 min, he should be de-authenticated.
- All clients should be de-authenticated after 1 hour.

Customize splash.html Page

HTML code

The following is an example of splash.html code:

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<meta charset="utf-8" />
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel='shortcut icon' href='$imagesdir/abc.png' type='image/x-icon' />
<title>$gatewayname Entry</title>
<style>

Body { background-color:white;
color:black;
margin-left: 5%;
margin-right: 5%;
text-align: left; }
Img { width: 100%;
max-width: 500px;
margin-left: 5%;
margin-right: 5%; }
  .bordered {
    width: 800px;
    height: 200px;
    padding: 5px;
    border: 2px solid #AAAAAA;
      overflow: auto;
      text-align: justify;
      margin-left: 15%;
    margin-right: 15%;

  }
```

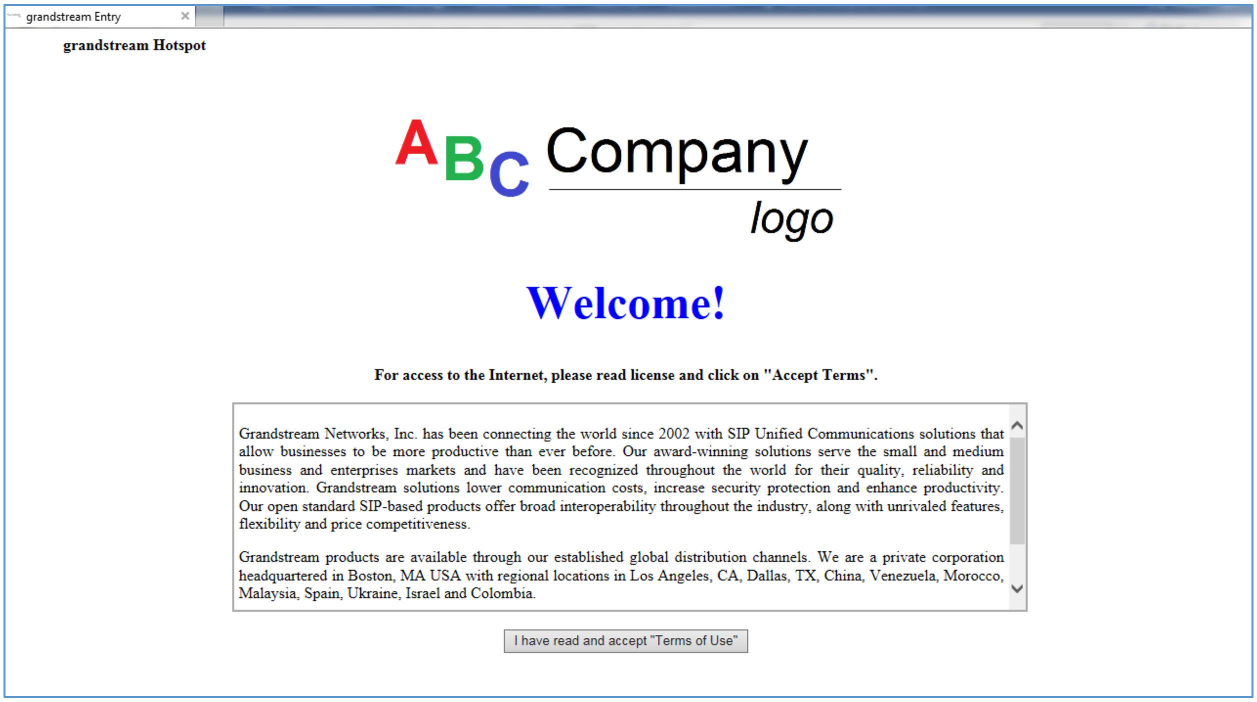
```
input [type=submit] {
color:black;
margin-left: 0%;
margin-right: 5%;
text-align:left;
font-size: 1.0em;
line-height: 2.5em;
font-weight: bold;
border: 1px solid; }
</style>
</head>
<body>
<b>$gatewayname Hotspot</b>
<div style="text-align: center;">
<br> <br> <b>
<img src="$imagesdir/abc.png" alt="Splash image" align="center">

<br> <br>
<span style="color:blue; font-style:normal; font-size: 300%;" align="center"> Welcome!
</span>
</b> <br> <br> <br>
<b>For access to the Internet, please read license and click on "Accept Terms"</b>
<br> <br>
<div class="bordered">
<p>Terms of Use conditions</p>
</div>
</br>
<form method='get' action='$authaction'>
<input type='hidden' name='tok' value='$tok'>
<input type='hidden' name='redir' value='$redir'>
<input type='submit' value='I have read and accept "Terms of Use"'>
</form>
</div>
</body>
</html>
```

Variables

"**$tok**", "**$redir**" and "**$authaction**" variables can be used with GET-method in HTML form to communicate with the server.

$tok	Token sent by the device trying to connect to the AP.
$authaction	URL of the gateway.
$redir	URL user typed initially. Once connected successfully users will be redirected to that URL.

HTML Page Display



grandstream Hotspot

Welcome!

For access to the Internet, please read license and click on "Accept Terms".

Grandstream Networks, Inc. has been connecting the world since 2002 with SIP Unified Communications solutions that allow businesses to be more productive than ever before. Our award-winning solutions serve the small and medium business and enterprises markets and have been recognized throughout the world for their quality, reliability and innovation. Grandstream solutions lower communication costs, increase security protection and enhance productivity. Our open standard SIP-based products offer broad interoperability throughout the industry, along with unrivaled features, flexibility and price competitiveness.

Grandstream products are available through our established global distribution channels. We are a private corporation headquartered in Boston, MA USA with regional locations in Los Angeles, CA, Dallas, TX, China, Venezuela, Morocco, Malaysia, Spain, Ukraine, Israel and Colombia.

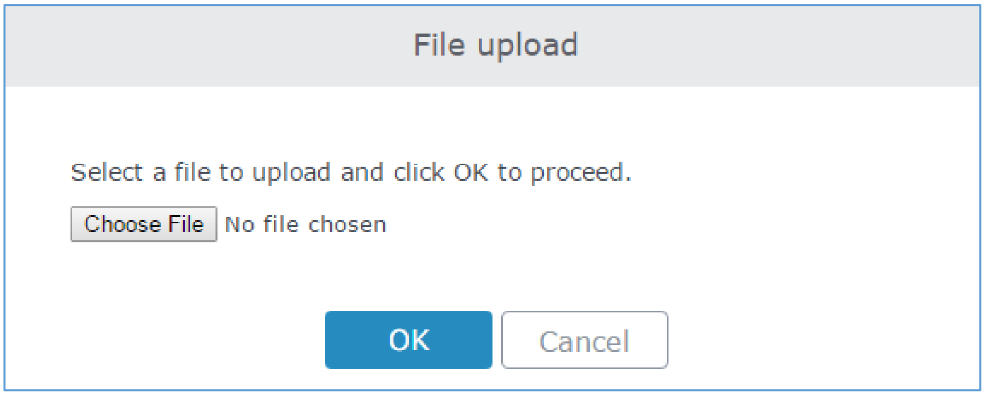
Figure 6: Custom splash.html Page

Configure Captive Portal Settings

Upload custom splash.html

To upload custom splash.html page, follow below steps:

1. Access GWN76xx web interface > System Settings > Captive Portal.
2. Go to **Files** tab.
    a. Locate splash.html row and press ✎ .
    b. In “File upload” popup window, press “Choose File” to browse customized “splash.html” file and press OK.



Select a file to upload and click OK to proceed.

No file chosen

Figure 7: File Upload window

c. In “Select Folder” drop-down list, select “Images”.

d. Press **+ Upload** button to upload related images (in this example, we need to upload “abc.png” file which is ABC company logo image).

Configure Captive Portal Settings

To configure captive portal with ABC company requirements, follow below steps:

1. Access GWN76xx web interface > System Settings > Captive Portal.
2. Go to **Basic** tab.

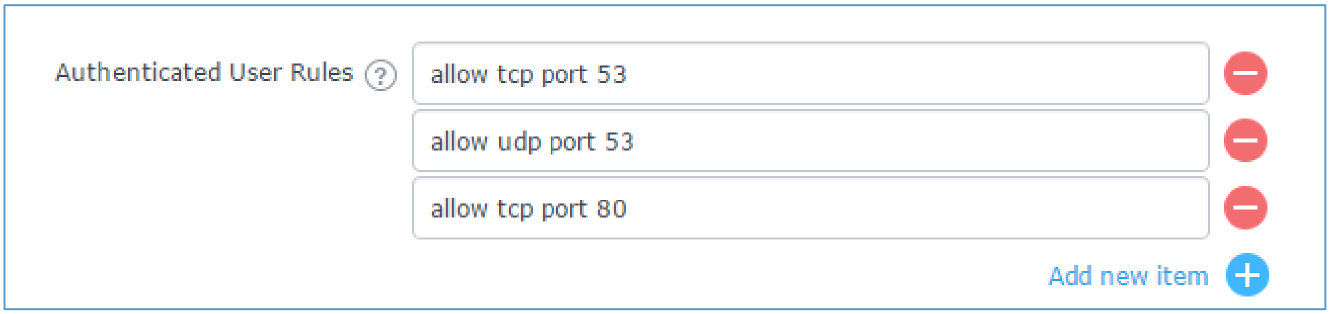
- Connected clients will be allowed to access websites using HTTP only.

a. In **Authenticated User Rules**, only following rules should be set:

Allow tcp port 53 => This rule to allow DNS queries over TCP.

Allow udp port 53 => This rule to allow DNS queries over UDP.

Allow tcp port 80 => This rule to allow HTTP queries over TCP.



Authenticated User Rules ?

allow tcp port 53 ⊖

allow udp port 53 ⊖

allow tcp port 80 ⊖

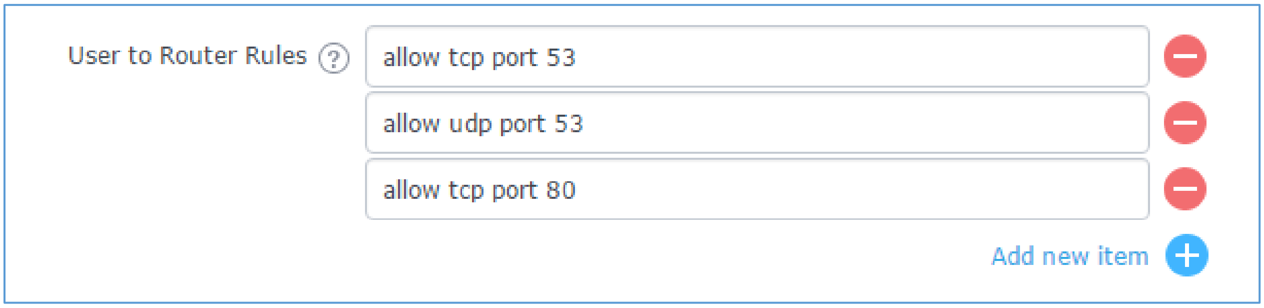
Figure 8: File Authenticated User Rules

b. In **User to Router Rules**, only following rules should be set:

Allow tcp port 53 => This rule to allow DNS queries over TCP.

Allow udp port 53 => This rule to allow DNS queries over UDP.

Allow tcp port 80 => This rule to allow HTTP queries over TCP.



User to Router Rules ?

allow tcp port 53 ⊖

allow udp port 53 ⊖

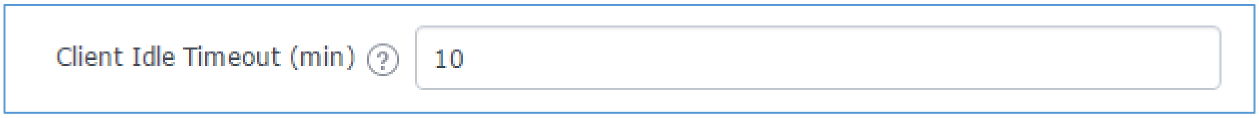
allow tcp port 80 ⊖

Figure 9: User to Router Rules

Note: Users can Click on ⊖ to delete an existing rule or ⊕ to add a new rule.

- <u>If a client is inactive for 10 min, he should be de-authenticated</u>.

  Set **Client Idle Timeout (min)** to 10.

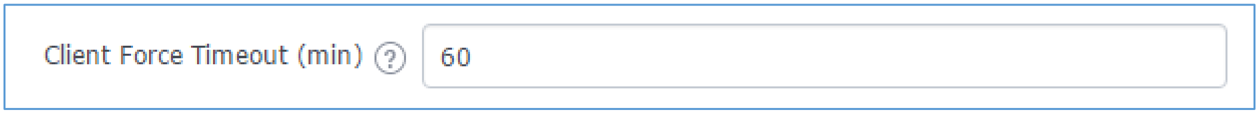


Client Idle Timeout (min) ? 10

Figure 10: Client Idle Timeout

- <u>All clients should be de-authenticated after 1 hour.</u>

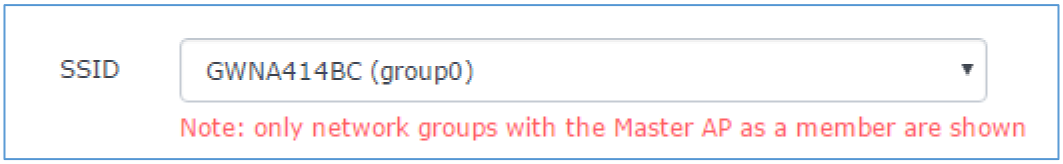
  Set **Client Force Timeout (min)** to 60.



Client Force Timeout (min) ? 60

Figure 11: Client Force Timeout

3. In **SSID** drop-down list, select the network group to use.

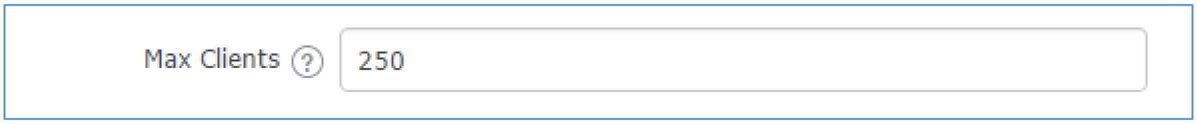


SSID GWNA414BC (group0) ▾

Note: only network groups with the Master AP as a member are shown

Figure 12: SSID

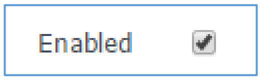
4. The maximum number of allowed users to connect can be configured using **Max Clients** field.



Max Clients ? 250

Figure 13: Max Clients

5. Enable captive portal by checking **Enabled.**



Enabled ☑

6. Press Save then Apply.

7. At this stage, WiFi clients trying to access Internet via GWN76xx access point will get customized “splash.html” landing page first, they will need to accept the terms of use to get Internet access.