



# Grandstream Networks, Inc.

---

Captive Portal

Authentication via RADIUS



## Table of Content

<b>SUPPORTED DEVICES .....</b>	<b>4</b>
<b>INTRODUCTION .....</b>	<b>5</b>
<b>SYSTEM OVERVIEW .....</b>	<b>6</b>
<b>CAPTIVE PORTAL SETTINGS .....</b>	<b>7</b>
Policy Configuration Page .....	7
<i>Landing Page Redirection</i> .....	9
<i>Pre-Authentication Rules</i> .....	9
<i>Post-Authentication Rules</i> .....	9
Files Configuration Page .....	10
Clients Page .....	11
<b>CONFIGURATION STEPS .....</b>	<b>12</b>
Installing FreeRADIUS .....	12
Adding Clients (APs) .....	13
Adding WiFi Users .....	13
Configuring RADIUS Authentication for Captive Portal .....	14



## Table of Figures

Figure 1: General Architecture .....	5
Figure 2: RADIUS Authentication.....	6
Figure 3: Captive Portal web GUI menu .....	7
Figure 4: Files Web Page.....	10
Figure 5: Client Web Page.....	11
Figure 6: GWN7600 Captive Portal with RADIUS .....	15
Figure 7: Enable Captive Portal on Network Group.....	16
Figure 8: Captive Portal Authentication via RADIUS .....	17

## 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 RADIUS Authentication feature:

Table 1: Supported Devices

Model	Supported	Firmware
GWN7610	Yes	1.0.3.19 or higher
GWN7600	Yes	1.0.3.19 or higher
GWN7000	Yes	1.0.2.75 or higher



## INTRODUCTION

Captive Portal feature on GWN76XX Access Points and GWN7000 router allows to define a Portal Web Page that will be displayed on WiFi clients' browsers when attempting to access the Internet.

Once connected to GWN76XX AP, WiFi clients will be forced to view and interact with that landing page by providing authentication if required and accepting the use terms 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 RADIUS authentication.

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

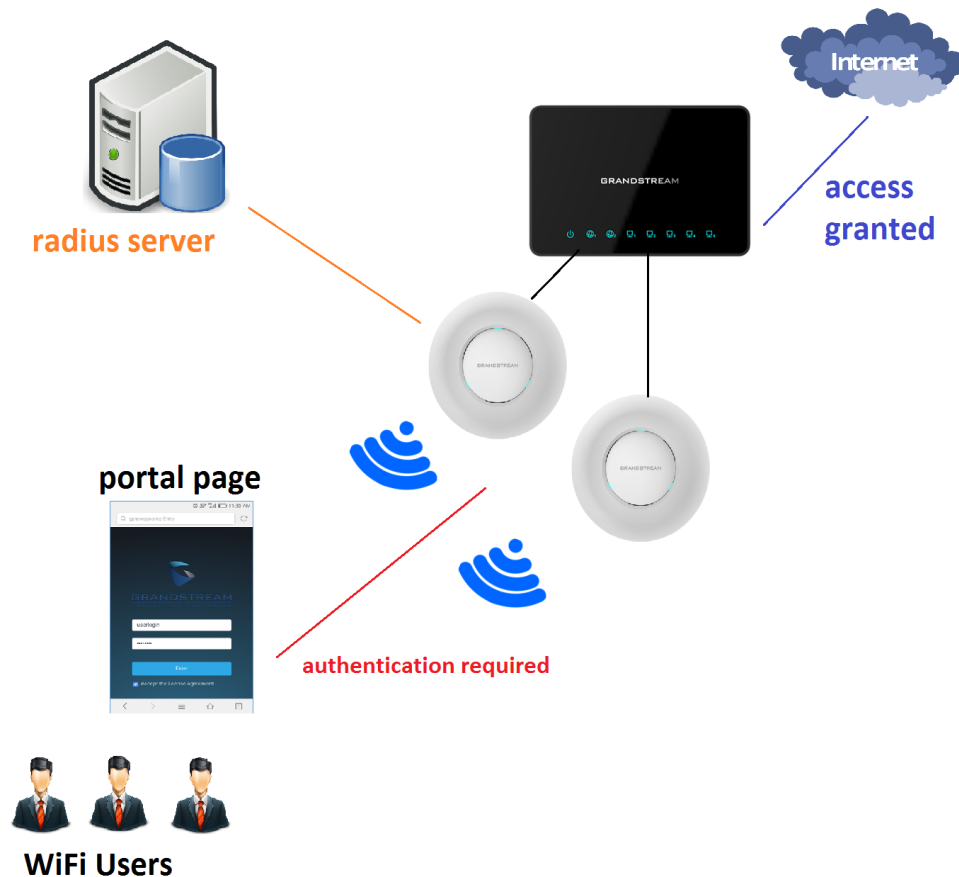


Figure 1: General Architecture

## SYSTEM OVERVIEW

In order to configure the captive portal feature on GWN76XX access points with RADIUS authentication, the following requirements should be applied:

- A fully setup and working RADIUS server for authentication (ex: FreeRADIUS).
- GWN76XX Access point with firmware supporting RADIUS. Refer to [SUPPORTED DEVICES].
- Network setup allowing GWN76XX access point and RADIUS server communication.

### RADIUS

Authentication via RADIUS server is commonly used on enterprise local networks, once this option selected the admin needs to configure the IP address and secret to connect the AP (RADIUS Client) to the RADIUS Server.



Figure 2: RADIUS Authentication

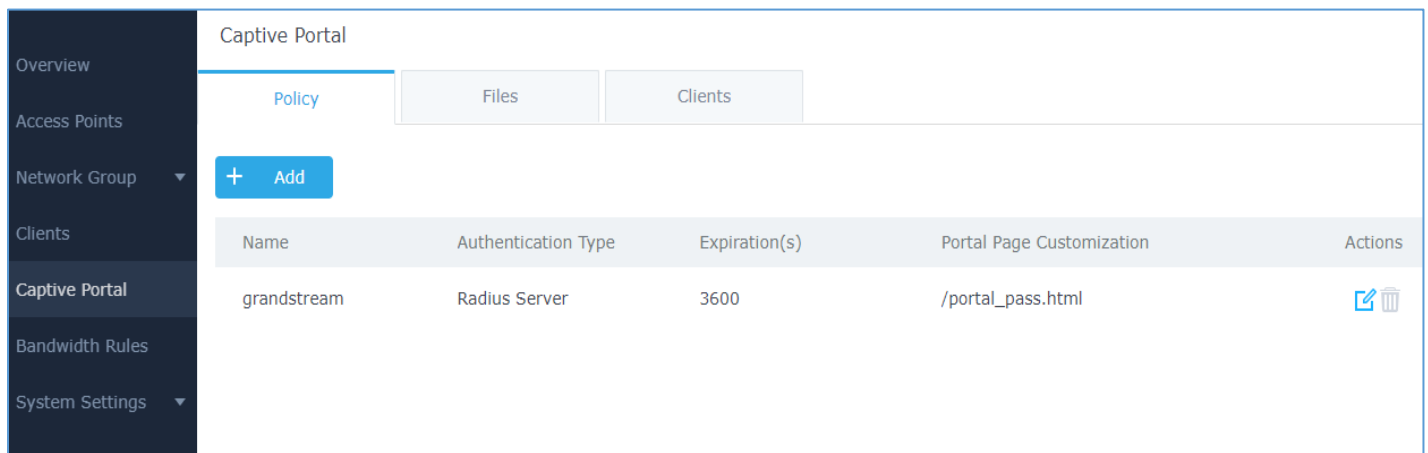
The supplicant will request to join an SSID, the authenticator will request an identity from the mobile device, the authenticator forwards the identity to the authentication server which will reply with a success or deny.

## CAPTIVE PORTAL SETTINGS

The Captive Portal feature can be configured from the GWN760X 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 specific 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.



The screenshot shows the Captive Portal configuration interface. On the left is a dark sidebar menu with options: Overview, Access Points, Network Group, Clients, Captive Portal (highlighted), Bandwidth Rules, and System Settings. The main content area is titled 'Captive Portal' and has three tabs: Policy (selected), Files, and Clients. Below the tabs is a blue '+ Add' button. A table lists the current policy configuration:



Name	Authentication Type	Expiration(s)	Portal Page Customization	Actions
grandstream	Radius Server	3600	/portal_pass.html	 

Figure 3: 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 the settings used for Captive Portal feature with RADIUS Authentication Basic:

Table 2: Policy Configuration Page

Field	Description
<b>Name</b>	Enter a name to identify the created policy (ex: Guest Portal).
<b>Expiration</b>	<p>Enter the expiration time for the landing page, The expiration time can be configured by days/hours/minutes or seconds.</p> <ul style="list-style-type: none"> <li>• <b>Days</b> : Set the number of days interval is [0-7]</li> <li>• <b>Hours</b> : Set the number of hours interval is [0-168]</li> <li>• <b>Minutes</b> : Set the number of minutes interval is [0-10080]</li> <li>• <b>Seconds</b> : Set the number of seconds interval is [60- 604800]</li> </ul> <p>If this field is set to 0 the landing page will never expire.</p>
<b>Authentication Type</b>	<p>Three types of authentication are available:</p> <ul style="list-style-type: none"> <li>• <b>No Authentication:</b> 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>• <b>RADIUS Server:</b> Choosing this option will allow users to set a RADIUS server to authenticate connecting clients. In this guide, we will use this Authentication Type.</li> <li>• <b>Social login Authentication:</b> Choosing this option will allow users to log in using WeChat or Facebook.</li> </ul>
<b>RADIUS Server Address</b>	Enter the IP address or the FQDN of the RADIUS server used to authenticate clients.
<b>RADIUS Server Port</b>	Enter the RADIUS server port, by default value is 1812.
<b>RADIUS Server Secret</b>	Enter the shared key between authenticator and RADIUS server.
<b>RADIUS Authentication Method</b>	Choose which method to use for RADIUS Authentication (PAP, CHAP or MS-CHAP).
<b>Use Default Portal Page</b>	If enabled the default page pre-loaded to the access point will be used to enter user's credentials.
<b>Portal Page Customization</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Portal Default:</b> This page is used when no authentication is specified, users will have only to accept license agreement to gain access to internet.</li> <li>• <b>Portal Pass:</b> This option provides authentication textbox when using RADIUS authentication mode, in order to enter username and password stored in RADIUS database. In this guide, we will use this option.</li> <li>• <b>Third Auth:</b> Choose this page when using authentication via WeChat or Facebook.</li> </ul>





<b>Landing Page</b>	Select page where authenticated clients will be redirected to. <ul style="list-style-type: none"> <li>• <b>Redirect to the original URL:</b> Sends the authenticated client to the original requested URL.</li> <li>• <b>Redirect External Page:</b> Enter URL that you want to promote to connected clients (ex: company's website).</li> </ul>
<b>Redirect External Page URL</b>	When setting the landing page to (Redirect External Page), enter the URL where to redirect authenticated clients.
<b>Enable HTTPS</b>	Check this box in order to enable captive portal over HTTPS.
<b>Pre Authentication Rules</b>	From this menu, users can set matching rules in order to allow certain types of traffic before authentication happens or simply allow the traffic for non authenticated end points.
<b>Post Authentication Rules</b>	This tool can be used to block certain type of traffic to authenticated clients, anything else is allowed by default. (Ex: Setting 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.

**Note:** Supported on GWN7600 Access Points only.

### 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 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.

**Note:** Supported on GWN7600 Access Points only.

### 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.

**Note:** Supported on GWN7600 Access Points only.

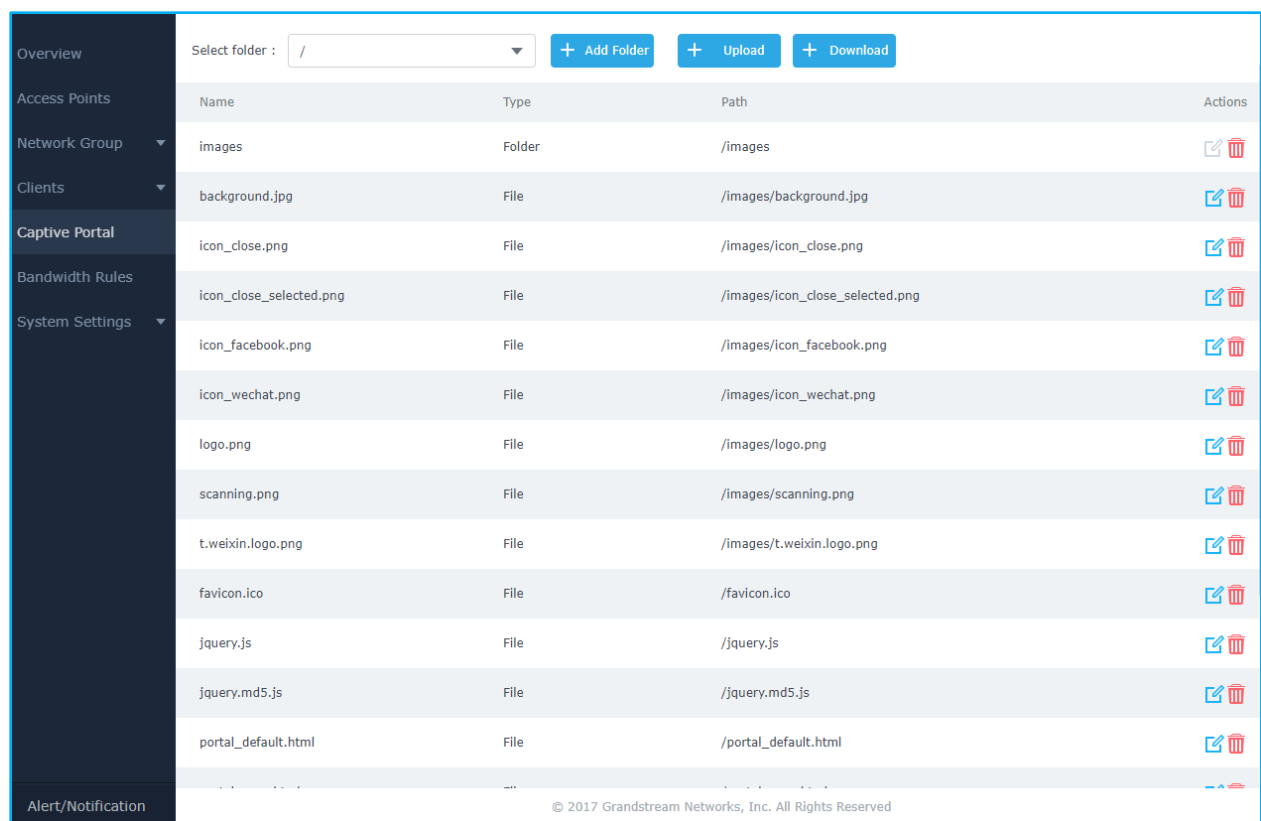


## Files Configuration Page

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 RADIUS authentication, users need to select **portal\_pass.html** as the portal page to let the user login via RADIUS.

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







The screenshot shows the 'Files Web Page' interface. On the left is a dark sidebar with navigation options: Overview, Access Points, Network Group, Clients, **Captive Portal**, Bandwidth Rules, and System Settings. The main area displays a file list with the following columns: Name, Type, Path, and Actions. At the top of the main area, there is a 'Select folder' dropdown menu set to '/', and three buttons: '+ Add Folder', '+ Upload', and '+ Download'. The file list contains the following entries:

Name	Type	Path	Actions
images	Folder	/images	[Edit] [Delete]
background.jpg	File	/images/background.jpg	[Edit] [Delete]
icon_close.png	File	/images/icon_close.png	[Edit] [Delete]
icon_close_selected.png	File	/images/icon_close_selected.png	[Edit] [Delete]
icon_facebook.png	File	/images/icon_facebook.png	[Edit] [Delete]
icon_wechat.png	File	/images/icon_wechat.png	[Edit] [Delete]
logo.png	File	/images/logo.png	[Edit] [Delete]
scanning.png	File	/images/scanning.png	[Edit] [Delete]
t.weixin.logo.png	File	/images/t.weixin.logo.png	[Edit] [Delete]
favicon.ico	File	/favicon.ico	[Edit] [Delete]
jquery.js	File	/jquery.js	[Edit] [Delete]
jquery.md5.js	File	/jquery.md5.js	[Edit] [Delete]
portal_default.html	File	/portal_default.html	[Edit] [Delete]

At the bottom of the interface, there is a footer with the text: © 2017 Grandstream Networks, Inc. All Rights Reserved.

Figure 4: Files Web Page

- Click  to upload a new web page.
- Click  to add a new folder.
- Click  to upload files to the selected folder.
- Folder can be selected from the dropdown list. Select folder :
- Click on  to download all the files/folders.



## 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**

Captive Portal				
Policy	Files	Clients		
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 5: Client Web Page

## CONFIGURATION STEPS

In this section, we will provide the steps needed to setup basic captive portal policy supporting RADIUS authentication with FreeRADIUS server.

### Installing FreeRADIUS

FreeRADIUS includes a RADIUS server, a BSD licensed client library, a PAM library, and an Apache module. In most cases, the word *FreeRADIUS* refers to the RADIUS server.

FreeRADIUS is the most widely deployed RADIUS server in the world. It is the basis for multiple commercial offerings. It supplies the AAA needs of many Fortune-500 companies and Tier 1 ISPs.

It is also widely used for Enterprise Wi-Fi and IEEE 802.1X network security, particularly in the academic community, including eduroam.

The following steps summarize simple installation procedure on Linux Debian based machines.

1. Run as root the command **#apt-get install freeradius** in order to install the server along with all its necessary dependencies.
2. After this is done you can verify successful installation by checking the version of the server using the command : **\$sudo freeradius -v** following screenshot shows that we are using version 2.2.8.

```
freeradius: FreeRADIUS Version 2.2.8, for host i686-pc-linux-gnu, built on Apr  5 2016 at 13:39:42
Copyright (C) 1999-2015 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License.
For more information about these matters, see the file named COPYRIGHT.
```

3. You can run the command **sudo \$freeradius -CX** in order to run a quick config check. The output should display **Configuration appears to be OK.**
4. All the configuration files are located at the directory **/etc/freeradius**. The following screenshot shows the list of the available files.

```
acct_users      clients.conf    modules         sites-enabled
attrs           dictionary      policy.conf     sql.conf
attrs.access_challenge eap.conf       policy.txt      sqlippool.conf
attrs.access_reject  experimental.conf preproxy_users  templates.conf
attrs.accounting_response hints           proxy.conf      users
attrs.pre-proxy     huntgroups     radiusd.conf
certs             ldap.attrmap   sites-available
```

5. The following files are the most important ones for the configuration:
  - **radiusd.conf:** This is the main configuration files of FreeRADIUS to tune the parameters of the running instance.



- **clients.conf:** On this file we can add the list of authorized clients (clients means the authenticators and should not be confused with WiFi clients, i.e. clients in FreeRADIUS configuration are your Access Points and Switches that are between the server and end devices).
- **eap.conf:** On this file we can choose the eap method used for authentication (defaults to eap-md5).

## Adding Clients (APs)

Next, we will include the list of authentication clients which are the access points relaying the requests back and forward between WiFi stations and the RADIUS server.

To do so, access to the file **clients.conf** and add each client as the following format:

```
client Client_IDENTIFIER {  
  ipaddr = IP_Address_of_AP  
  secret = Shared_Secret  
}
```

Following figure shows that we have added two GWN76XX access points as authenticators for the freeraiuds server.

```
client GWN7600 {  
  ipaddr = 192.168.6.189  
  secret = R@d!us7600  
}  
  
client GWN7610 {  
  ipaddr = 192.168.6.37  
  secret = R@d!us7610  
}
```

After this, save the file and let's add some users in the FreeRADIUS database.

## Adding WiFi Users

To add users, edit the file named users under the configuration folder **/etc/freeradius**. At the bottom of the file, create new WiFi users and assign usernames and passwords as the following examples show:

### Syntax:

```
USERNAME Cleartext-Password := "PASSWORD"
```

```
# On no match, the user is denied access.  
User1 Cleartext-Password := "admi132"  
User2 Cleartext-Password := "admin123"  
User3 Cleartext-Password := "admin123"
```



Once this is done, save the file and run the following command to check if the server is operational.

```
$radtest User1 admin123 127.0.0.1 0 testing123
```

The results should be something like following:

```
User-Name = "User1"  
User-Password = "admin123"  
NAS-IP-Address = 192.168.x.x  
NAS-Port = 0  
Message-Authenticator = 0x00000000000000000000000000000000  
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=156, length=20
```

Now that the server is configured, you can stop the server using the command **\$service freeradius stop** and run it again on debug mode in order to see the log messages when requests are handled by the server, to run the server in debug mode run the command **#freeradius -X**.

## Configuring RADIUS Authentication for Captive Portal

After setting up the RADIUS server and making sure that it is running properly, users could configure captive portal feature under the GWN76XX web GUI menu by following below steps:

1. First, access the web GUI menu **Captive Portal**.
2. Under the policy tab, click on Add button to create new portal policy.
3. Set the name of the policy (in our example we named it RadiusPortal).
4. Then on **Authentication type** choose "RADIUS Server" and set the IP and listening port of the configured server. (FreeRADIUS default listening port for authentication is 1812).
5. Enter the RADIUS shared secret which was configured for the Access point under **clients.conf** file (In this example, we set it to R@d!usPass).
6. Select **portal\_pass** as portal page to allow users to under their username and password.
7. From here you can leave the rest to default, following screenshot shows the configuration.



Add ✕

Name

Expiration ?  second ▼

Authentication Type ▼

RADIUS Server Address

RADIUS Server Port

RADIUS Server Secret  👁

Radius Authentication Method ▼

Use Default Portal Page

Portal Page Customization ▼

Landing Page ▼

Redirect External Page URL Address ?

Enable HTTPS

Pre Authentication Rule(s) ▼   -  
Add new item +

Post Authentication Rule(s) ▼  -  
Add new item +

**Figure 6: GWN7600 Captive Portal with RADIUS**

8. After this save and apply to complete the settings.

Now, the next step is to enable this portal on the network group.

For this, users should go to the menu **Network Groups** and edit the desired network group then go to **WiFi settings** tab and enable the captive portal Checkbox to select the created policy before saving and applying the new configuration.

**Edit**

BasicWi-FiDevice MembershipSchedule

Enable Wi-Fi

SSID

SSID Band

SSID Hidden

Wireless Client Limit

Enable Captive Portal

Captive Portal Policy

Security Mode

Use MAC Filtering

Client Isolation

Enable RSSI

Minimum RSSI (dBm)

Enable 11K

Enable 11V

Save Cancel

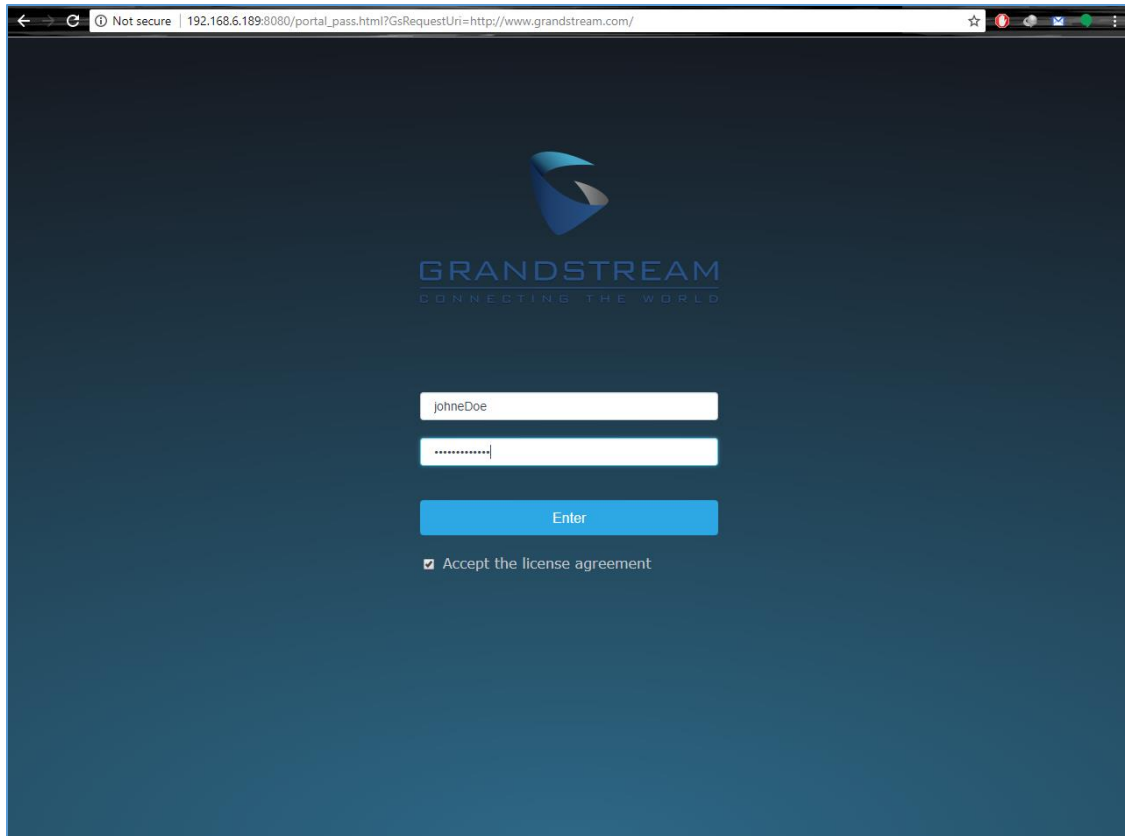
**Figure 7: Enable Captive Portal on Network Group**

At this stage, our GWN76XX access points is ready to receive authentication requests from WiFi clients and hand them over to the RADIUS server.

The default portal page is shown to provide his credentials as shown on the following figure:







**Figure 8: Captive Portal Authentication via RADIUS**

Authenticated clients will get access to the Internet and be listed on the Clients tab under Captive Portal menu.

After successful authentication, clients will be directed either to the original requested URL or a specific Configured URL depending on the option configured under **Captive Portal**→**Policy**→**Redirect External Page URL**.