



Grandstream Networks, Inc.

Captive Portal

Authentication with Vouchers



Table of Content

SUPPORTED DEVICES	4
INTRODUCTION	5
CAPTIVE PORTAL SETTINGS	6
Policy Configuration Page	6
Files Configuration Page	7
Clients Page	8
VOUCHERS SETTINGS	9
Print Vouchers	10
CONFIGURATION STEPS	11
Create Vouchers	11
Configure Captive Portal Policy with Vouchers Authentication	12
Assign Captive Portal to Network Groups and SSIDs	13
Connect to Network	14



Table of Figures

Figure 1: Captive Portal web GUI menu	6
Figure 2: Files Web Page.....	8
Figure 3: Client Web Page	8
Figure 4: Vouchers List	9
Figure 5: Vouchers List – Print button.....	10
Figure 6: Voucher Print Page	10
Figure 7: Add Voucher.....	11
Figure 8: Captive Portal with Voucher authentication	13
Figure 9: Enable Captive Portal on WiFi Settings.....	13
Figure 10 : Voucher Authentication	14

Table of Tables

Table 1: Supported Devices	4
Table 2: Policy Configuration Page	6
Table 3: Vouchers List Parameters	9
Table 4: Voucher Parameters.....	12



SUPPORTED DEVICES

Following table shows Grandstream networking products supporting Voucher feature:

Table 1: Supported Devices

Model	Supported	Firmware
GWN7610	Yes	1.0.5.12 or higher
GWN7600	Pending	Pending
GWN7600LR	Pending	Pending
GWN7000	Pending	Pending



INTRODUCTION

Voucher feature will allow clients to have internet access for a limited duration using a code that is randomly generated from GWN controller.

As an example, a coffee shop could offer internet access to customers via WIFI using voucher codes that can be delivered on each command. Once the voucher expires the client can no longer connect to the internet.

Note that multiple users can use a single voucher for connection with expiration duration of the voucher that starts counting after first successful connection from one of the users that are allowed.

Another interesting feature, is that the admin can set data bandwidth limitation on each created voucher depending on the current load on the network, users profile (VIP customers get more speed than regular ones etc....) and the internet connection available (fiber, DSL or cable etc....) to avoid connection congestion and slowness of the service.

Each created voucher can be printed and served to the customers for usage, and the limit is 1000 vouchers.

The usage of voucher feature needs to be combined with captive portal that is explained after this section, to have the portal page requesting clients to enter voucher code for authentication.



CAPTIVE PORTAL SETTINGS

The Captive Portal feature can be configured from the 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.

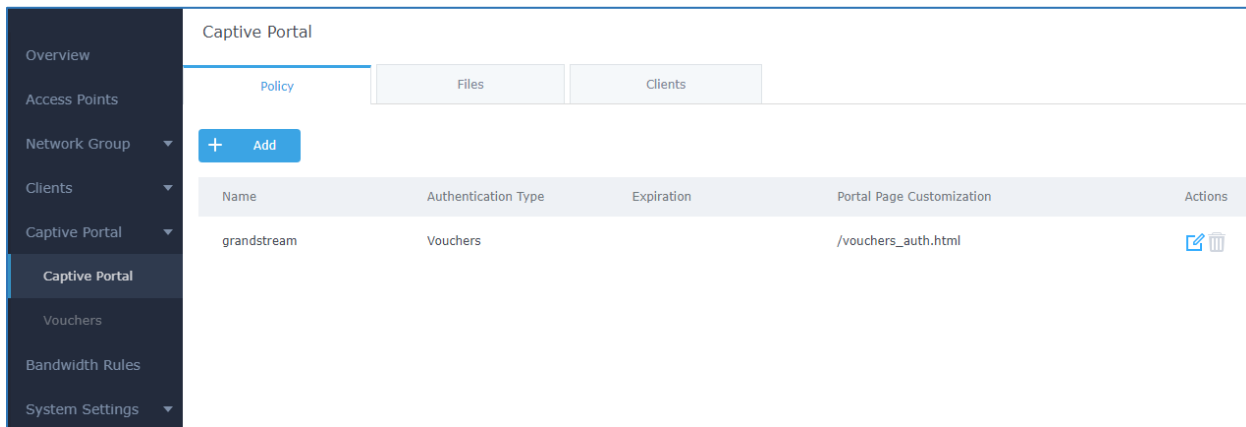


Figure 1: Captive Portal web GUI menu

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 (only parameters when setting “Authentication Type” to “Vouchers” are included in below table):

Table 2: Policy Configuration Page

Field	Description
Name	Enter a name to identify the created policy (ex: Guest Portal).
Authentication Type	Types of authentication are available: <ul style="list-style-type: none"> • 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.



	<ul style="list-style-type: none"> • 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/Facebook/Twitter. • Vouchers: Choosing this option will require a voucher code from users to get authenticated and connect to Internet. <i>This is the authentication type to use on this guide.</i> • Simple Password: Choosing this option will require to provide common password to get authenticated and connect to Internet.
Use Default Portal Page	If checked, GWN will use pre-configured default portal page which is " vouchers_auth.html " when using Vouchers as authentication Type.
Portal Page Customization	If not using default page, select custom portal page that will be shown to clients trying to connect to the WiFi.
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).

Files Configuration Page

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

The captive portal with voucher authentication uses **vouchers_auth.html** as default portal page.

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



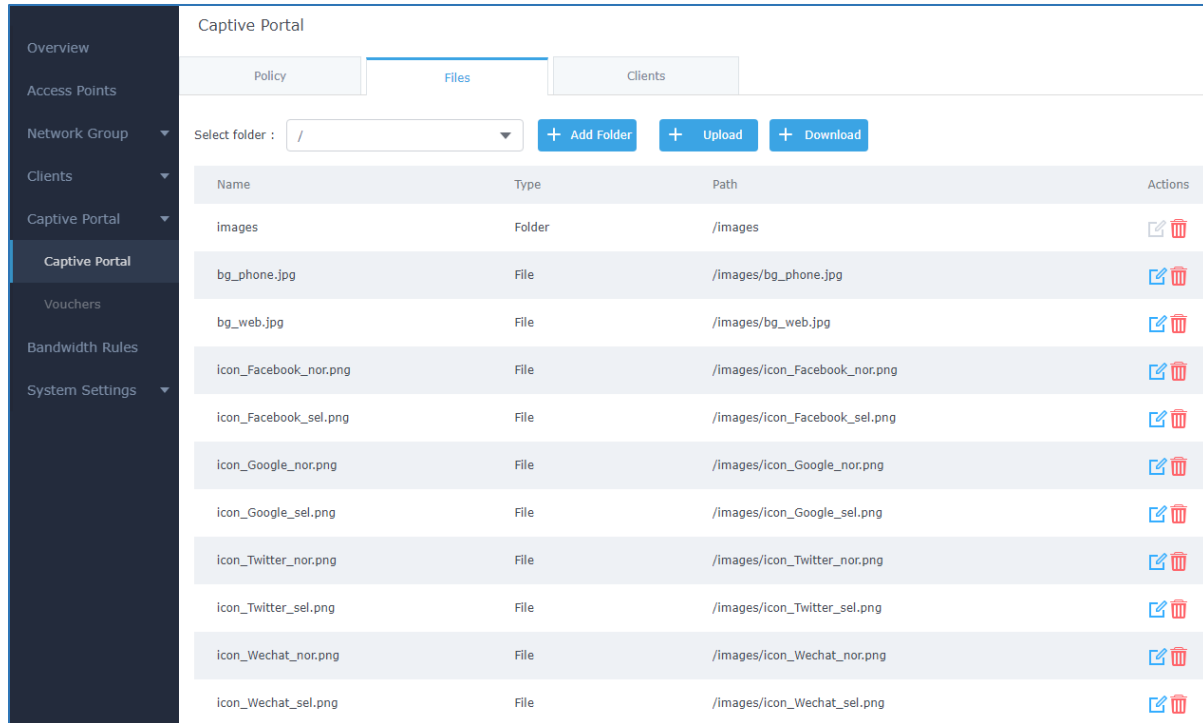


Figure 2: Files Web Page

- 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.

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 GWN:

- ✓ 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

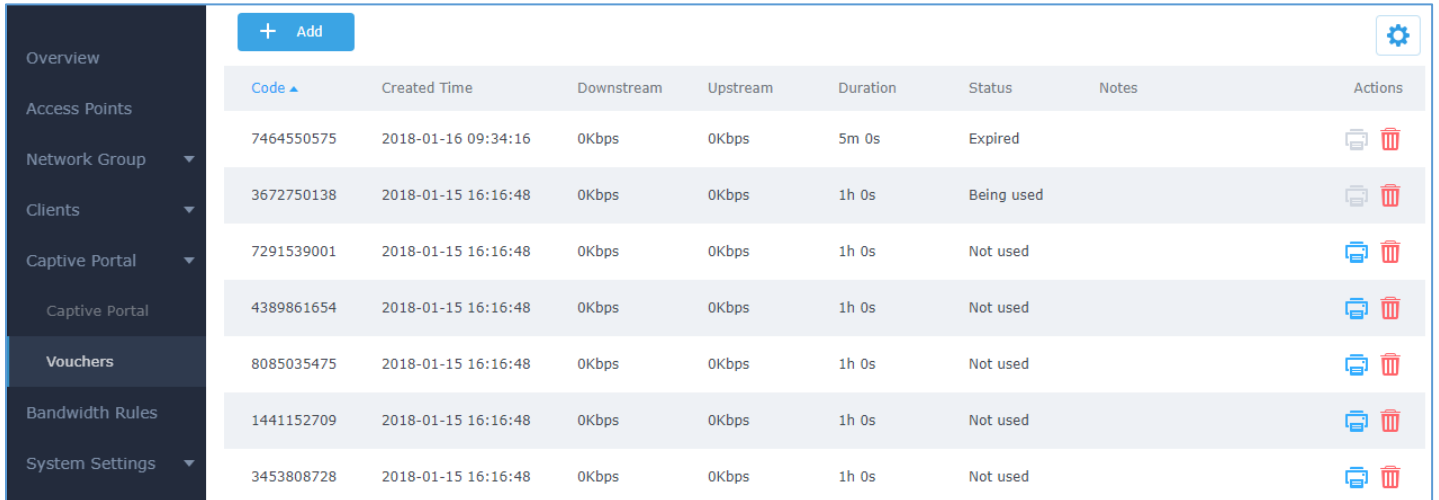
Figure 3: Client Web Page



VOUCHERS SETTINGS

The Vouchers parameters can be configured from the web page by navigating to “**Captive Portal → Vouchers**”.

- Press button  to create new voucher(s). For more details to generate vouchers, refer to **[Create Vouchers]** section.
- List of generated vouchers will be displayed with following details:




















Code ▲	Created Time	Downstream	Upstream	Duration	Status	Notes	Actions
7464550575	2018-01-16 09:34:16	0Kbps	0Kbps	5m 0s	Expired		 
3672750138	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Being used		 
7291539001	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
4389861654	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
8085035475	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
1441152709	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
3453808728	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 

Figure 4: Vouchers List

Table 3: Vouchers List Parameters

Code	Voucher code which needs to be entered by user during authentication.	
Created Time	The time when the voucher has been generated.	
Downstream	Configured downstream limit for the voucher. 0 means unlimited.	
Upstream	Configured downstream limit for the voucher. 0 means unlimited.	
Duration	Duration of validity of the voucher. It starts with first authentication.	
Status	<ul style="list-style-type: none"> • Not used: Voucher has been created but nobody gets authenticated with it yet. • Being used: At least one user got authenticated using this voucher. • Expired: The voucher has been used and duration timeout has been reached. Voucher with “Expired” status cannot be re-used. <p><u>Note:</u> Print button is deactivated with “Being used” or “Expired” status.</p>	
Notes	Notes entered during configuration.	
Actions		Print a voucher. Refer to [Print Vouchers] section for more details.
		Delete a voucher

Print Vouchers

To print a Voucher, access web UI → Captive Portal → Vouchers and press  button.

Important note: Only vouchers with status « Not Used » can be printed.















Code	Created Time	Downstream	Upstream	Duration	Status	Notes	Actions
7464550575	2018-01-16 09:34:16	0Kbps	0Kbps	5m 0s	Expired		 
3672750138	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Being used		 
7291539001	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
4389861654	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
8085035475	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
1441152709	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 
3453808728	2018-01-15 16:16:48	0Kbps	0Kbps	1h 0s	Not used		 

Figure 5: Vouchers List – Print button

Once print button pressed, a new page will be displayed to initiate the printing. Press **Print** to continue.

The following screenshot shows an example of voucher print page:

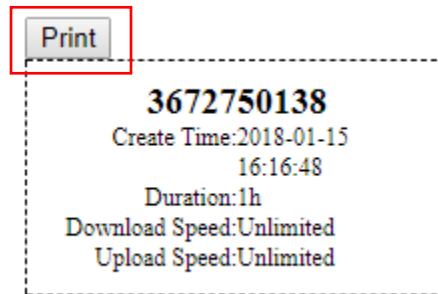



Figure 6: Voucher Print Page

CONFIGURATION STEPS

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

Create Vouchers

To configure/create vouchers for clients to use, follow below steps:

1. On controller web GUI, navigate under “**Captive Portal → Vouchers**”
2. Click on  button to add a new voucher.
3. Enter voucher details. Refer to [Table 4: Voucher Parameters] for details.
4. Press save to create the voucher(s).

CREATE VOUCHERS

Create Number One Time	<input style="width: 90%;" type="text" value="3"/>
Times can Use <small>?</small>	<input style="width: 90%;" type="text" value="2"/>
Duration	<input style="width: 80%;" type="text" value="1"/> hours ▼
Downstream	<input style="width: 80%;" type="text" value="1"/> Mbps ▼
Upstream	<input style="width: 80%;" type="text" value="250"/> Kbps ▼
Notes	<input style="width: 90%;" type="text" value="Tables 7, 9 & 12"/>

Save
Cancel

Figure 7: Add Voucher

The following table summarizes voucher configuration parameters:


Table 4: Voucher Parameters

Field	Description
Create Number One Time	Specify how many vouchers to generate which will have same profile/settings (duration, bandwidth and number of users). (Less or equal to 1000 – the minimum value is 1)
Times can Use	Specify how many users can use the voucher. If set to 1, the voucher can be used by a single user. (Valid range: 1 to 1000).
Duration	Specify the duration after which the voucher will expire, and clients will be disconnected from internet. Valid ranges: 1 to 10080 minutes 1 to 168 hours 1 to 7 days Note: In case of multiple users, the configured duration will be counted starting from the time when the first user is authenticated with the voucher.
Downstream	Set the downstream bandwidth speed limit (in Kbps or Mbps).
Upstream	Set the upstream bandwidth speed limit (in Kbps or Mbps).
Notes	Notes for the admin when checking the list of vouchers.

For more details, refer to [VOUCHERS SETTINGS] section.

Configure Captive Portal Policy with Vouchers Authentication

To successfully use the voucher feature, administrator will need to create a captive portal in order to request voucher authentication codes from users before allowing them access to internet. Follow below steps:

1. Go to “**Captive Portal → Captive portal**” menu.
2. Press  to add new captive portal policy.
3. Set the following parameters then save and apply.
 - Name: **Enter a name**
 - Authentication Type: **Vouchers**
 - Use Default Portal Page: **Checked**
 - Portal Page Customization: **/vouchers_auth.html**



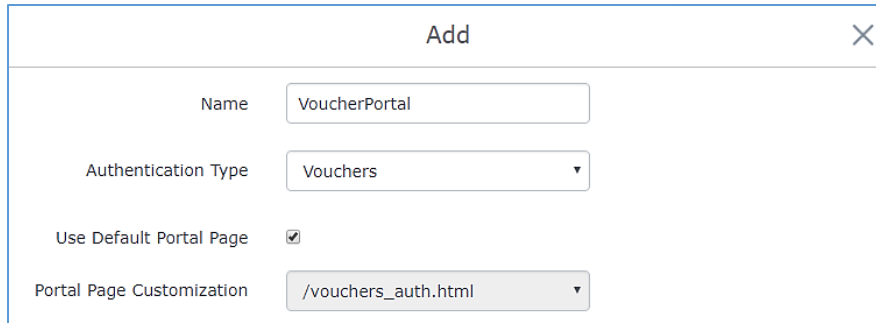


Figure 8: Captive Portal with Voucher authentication

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 to Network Groups and SSIDs

Once the captive portal policy has been configured with correct settings for Vouchers 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.

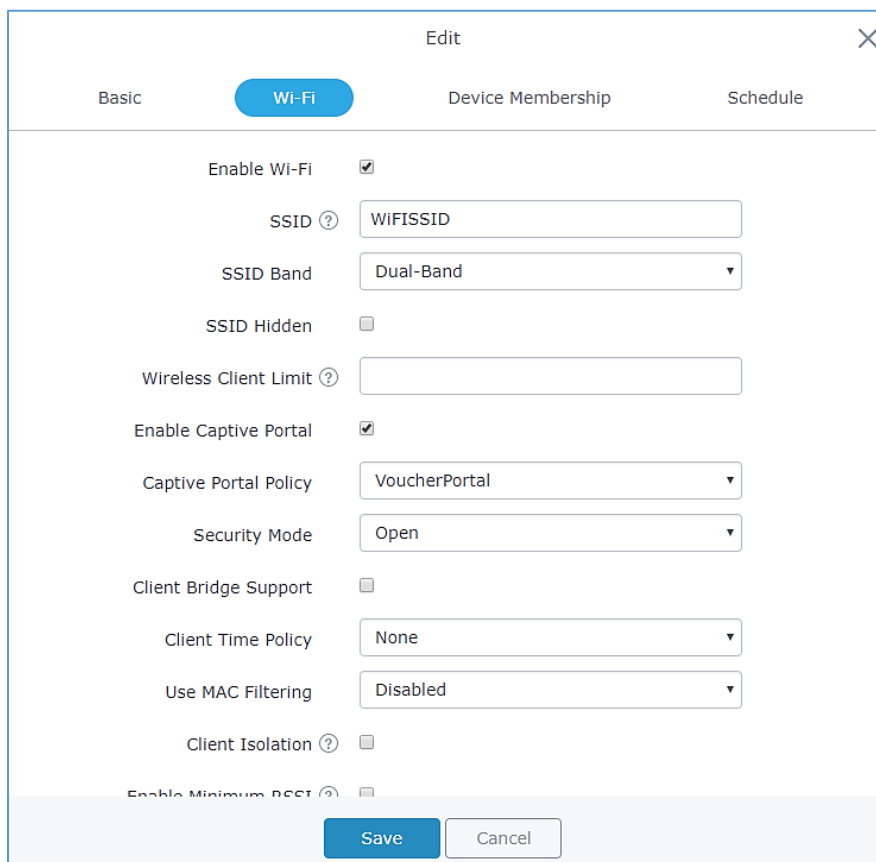


Figure 9: Enable Captive Portal on WiFi Settings

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 the Configuration done, guests can connect to the broadcasted WiFi SSID **CoffeeABC**, and will be automatically directed to below screen where they can enter their vouchers under the “Code” field:

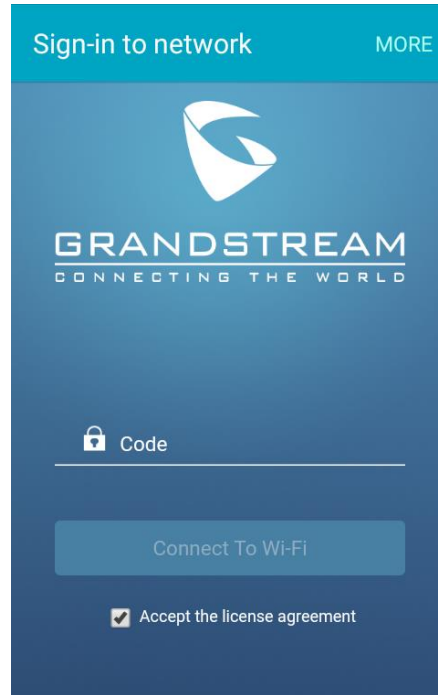


Figure 10 : Voucher Authentication

Important notes:

- After the Voucher duration is reached the user will be automatically disconnected from Internet and the voucher will expire.
- Same Voucher can be used by multiple users if [**Times can Use**] is higher than 1.
- In case of multiple users, the configured [**Duration**] will be counted starting from the time when the first user is authenticated with the voucher.
- When the duration of a voucher is reached, print button will be disabled for this voucher and it cannot be used again by another user.

