

# Cloud Platform User Manual

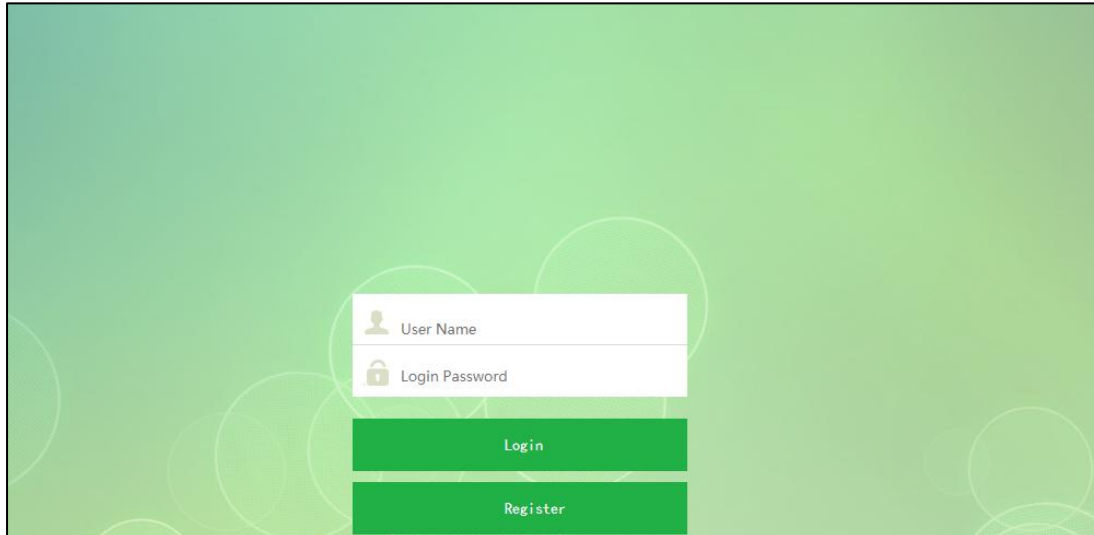


**TUDONIR 拓达**

# STEP 1

## 1. Register a new account

1.1 Visit the website of the Cloud platform at <http://47.88.54.22:8090>. Click Register to set up a new account.

A login and registration interface on a green background with faint circular patterns. It features two input fields: 'User Name' with a person icon and 'Login Password' with a lock icon. Below these are two green buttons: 'Login' and 'Register'.

1.2 Fill in the necessary information to finish the account registration.

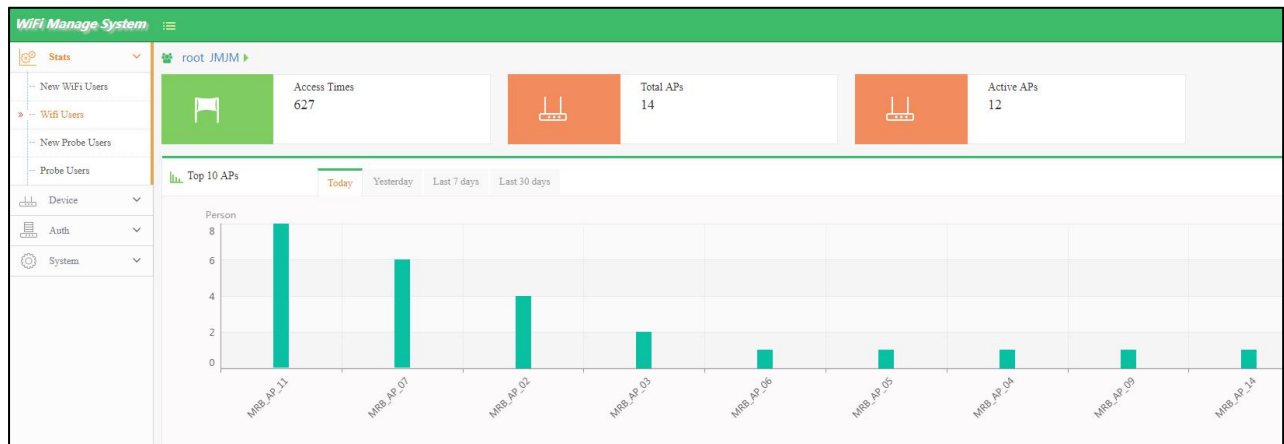
A registration form titled 'WiFi manage system - user registration'. The form is enclosed in a light green box and contains five required fields, each marked with a red asterisk: 'Group Name', 'User Name', 'E-mail', 'Password', and 'Confirm Password'. At the bottom of the form are two buttons: 'Submit' and 'Back Login'.

1.3 An confirmation e-mail will be sent to the register after presenting the information. Login the mailbox to activate the new account. Go back to the Cloud platform website and login with the new account.

# STEP 2

## 2. Status of the user and device

Click the Stats to check the statistic of the connecting terminals, MAC, AP devices, etc.



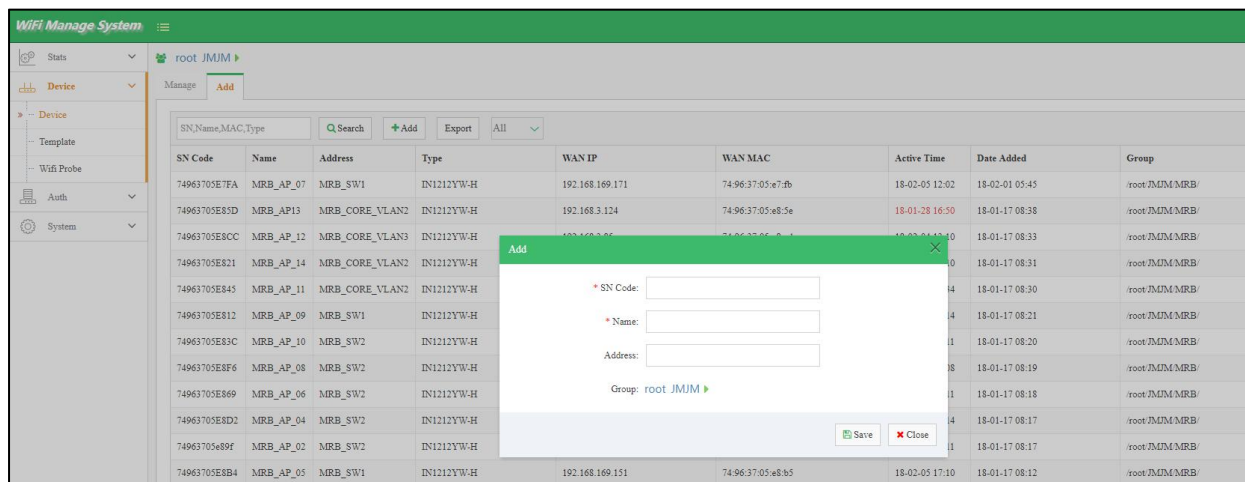
# STEP 3

3. Add a new AP device. Make sure the AP is connecting to the Internet in order to synchronize the data and setting with the Cloud platform.

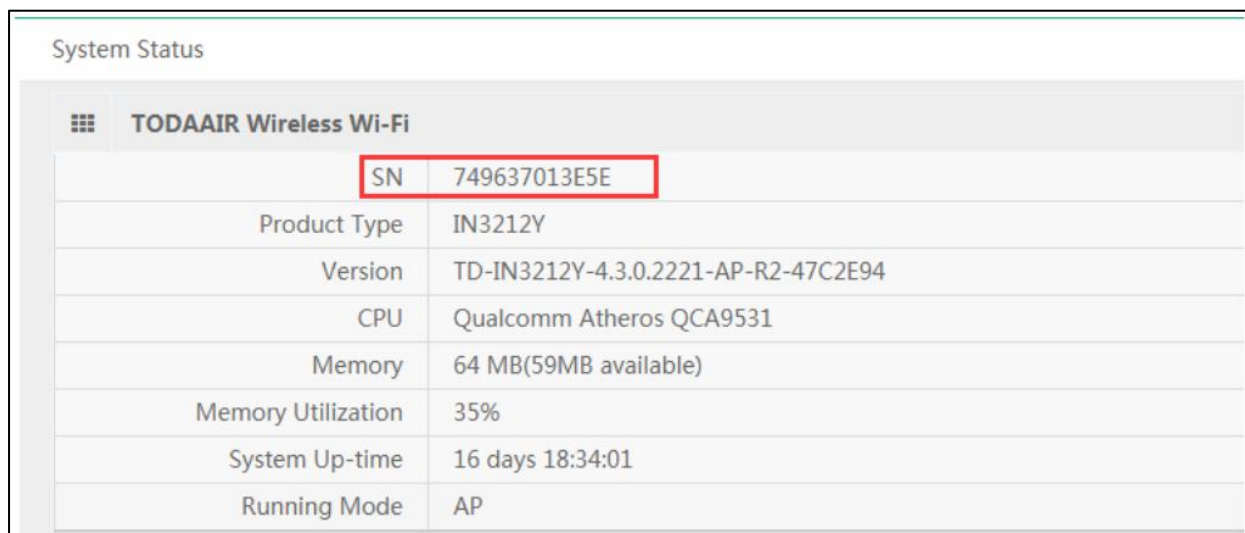
3.1 Click the Device to check the operating status of the AP which is linked to the Cloud platform.

SN Code	Name	Type	Version	Auth	Status	Last Online	Duration	Active Time	Group	Operation
74963705E7FA	MRB_AP_07	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-02-01 09:46:18	9 Hour55 Min	2018-02-05 17:13:34	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E83D	MRB_AP13	IN1212YW-H	4.3.0.2495	Enabled	Offline	-	3 Day10 Hour1 Min	2018-01-28 22:10:32	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E8CC	MRB_AP_12	IN1212YW-H	4.3.0.2495	Enabled	Offline	-	3 Day10 Hour54 Min	2018-02-04 15:15:46	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E821	MRB_AP_14	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-01-26 02:45:46	4 Day12 Hour53 Min	2018-02-05 17:14:17	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E845	MRB_AP_11	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-02-05 14:25:50	4 Day12 Hour52 Min	2018-02-05 17:13:37	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E812	MRB_AP_09	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-02-01 04:58:48	9 Hour54 Min	2018-02-05 17:13:10	/root/MJM/MRB/	Status Config Update Restart Operation Online
74963705E83C	MRB_AP_10	IN1212YW-H	4.3.0.2495	Enabled	Offline	-	6 Hour22 Min	2018-02-05 07:16:28	/root/MJM/MRB/	Status Config Update Restart Operation Online

3.2 Click the Device → Add, fill in the SN code, AP name, address and the Group information.



Remark: The SN code is in the product sticker. Or login the default IP address of the AP with 192.168.2.1. The SN code is showed in the system status. (The default account and the password is “admin”)



## STEP 4

### 4. AP Configuration

After the AP is added to the Cloud platform and it's online, the AP can be configured in the Ad authentication, SSID, encryption, transmitting power, etc.

#### 4. 1 Set the single AP

This method is suitable for setting different SSID among different APs. It's recommended to set groups for easier management (refer to the STEP 6) .

Click the Device → Device → Manage → Config

WiFi Management System

root JMJM

Manage Add

SN Code	Name	Type	Version	Auth	Status	Last Online	Duration	Active Time	Group	Operation
74963705E7FA	MRB_AP_07	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-02-01 09:46:18	2 Day4 Hour25 Min	2018-02-03 17:54:53	root/JMJM/MRB/	Status <b>Config</b> Update Restart Operation Online
74963705E8FA	MRB_AP_07	IN1212YW-H	4.3.0.2495	Enabled	Offline	-	-	-	root/JMJM/MRB/	Status Config Update Restart Operation Online
74963705E85D	MRB_AP13	IN1212YW-H	4.3.0.2495	Enabled	Offline	-	1 Day10 Hour1 Min	2018-01-28 22:10:32	root/JMJM/MRB/	Status Config Update Restart Operation Online
74963705E8CC	MRB_AP_12	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-01-26 02:55:54	2 Day13 Hour33 Min	2018-02-03 17:55:15	root/JMJM/MRB/	Status Config Update Restart Operation Online
74963705E821	MRB_AP_14	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-01-26 02:45:46	2 Day13 Hour33 Min	2018-02-03 17:54:44	root/JMJM/MRB/	Status Config Update Restart Operation Online
74963705E843	MRB_AP_11	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-01-26 02:45:04	2 Day13 Hour34 Min	2018-02-03 17:55:49	root/JMJM/MRB/	Status Config Update Restart Operation Online
74963705E812	MRB_AP_09	IN1212YW-H	4.3.0.2495	Enabled	Online	2018-02-01 04:58:48	2 Day12 Hour56 Min	2018-02-03 17:55:44	root/JMJM/MRB/	Status Config Update Restart Operation Online

Click the Config and make settings on below pages. The new setting will take effect in several minutes after the confirmation from the Cloud platform.

- \*Basic: set to use the AP template, the Ad Authentication, the schedule to reboot the AP
- \*SSID: set the WiFi SSID, add multiple SSID and set passwords, choose the VLAN value
- \*Frequency: set the wireless frequency and transmitting power
- \*Black White List: set the black and while list of the domains
- \*Advanced: WiFi probe setting and the WiFi connection parameters

Config-MRB\_AP\_07

✓ Templates: MRB\_APS\_TEMPLATE2 -- /root/JMJM/ ✓

**Basic** SSID(2.4G) SSID(5G) Radio Black White List Advanced

Auth: Enabled ✓

☐ IOS terminal does not automatically pop up the authentication page.

☐ Enable Escape

LAN IP: 192.168.100.10

Mode: AP ✓

Reboot: Disabled ✓

Last State:Downloaded Time:2018-02-03 17:57:46 User:system(AC sync to AP)

Save Cancel

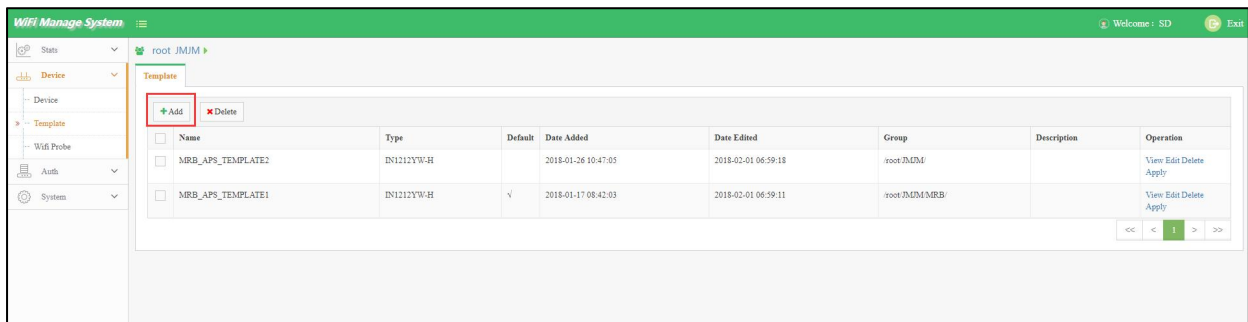


Remark:

1. In the Basic page, when the Auth is enabled, Ad will be showed when connecting the WiFi.
2. In the Advanced page, when the QoS is enabled, the function of traffic control will be available.
3. In the Advanced page, when the WiFi Probe is enabled, the terminal with week connection signal will be forced to be offline from the WiFi.
4. In the Advanced page, the Status Interval decides how often the AP will report its working status. The value is between 1-120.
5. In the Advanced page, the Duration decides how often the Cloud platform will check if the terminal is online or not. The value is between 5-60.

## 4.2 Template Modification (Suitable to modify the AP setting in batch)

### 4.2.1 Click the Device and then the Template, click Add button to add a new template.

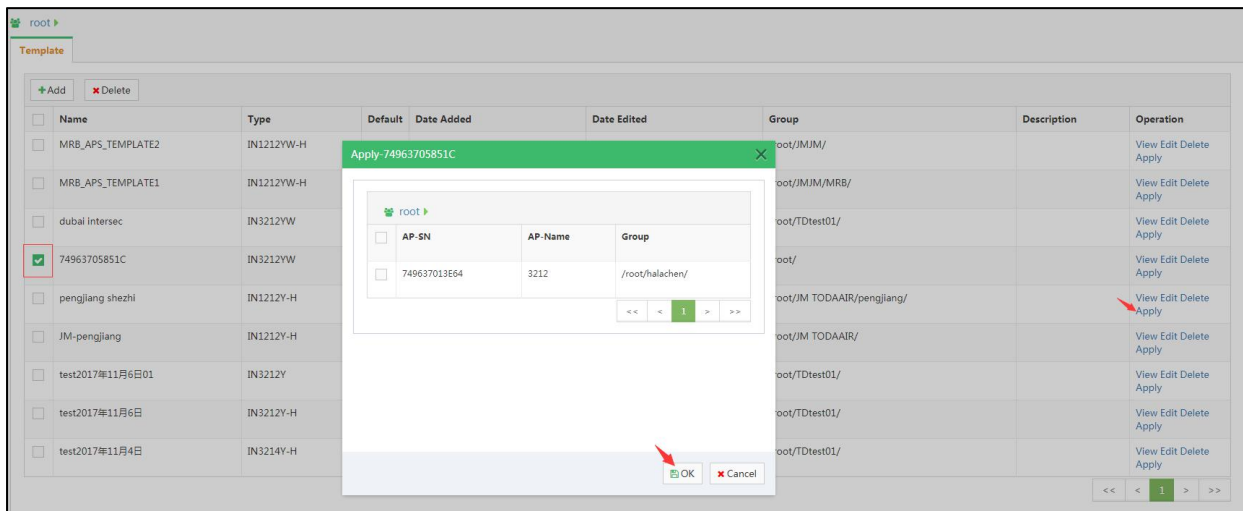


### 4.2.2 Fill the name of the template and choose the right AP model. Please note that the specific template is only available to the corresponding product model. The setting options in the template is the same to the single AP setting.

The 'Add' dialog box is shown with the following fields and options:

- Name:** Text input field (empty).
- Type:** Dropdown menu with 'IN1212Y-H' selected.
- Basic Tab:**
  - Auth:** Disabled (with a green checkmark icon).
  - LAN IP:** 192.168.2.1
  - Mode:** AP (with a green checkmark icon).
  - Reboot:** Disabled (with a green checkmark icon).
- Description:** Text area (empty).
- Footer:**
  - Checkbox: Set IN1212Y-H As Default Template
  - Buttons: OK, Cancel

4.2.3 After finishing the template setting, apply the template in the designated APs. Click the Template, choose the template and click the Apply, choose the corresponding AP and confirm. The newly settings will be updated in the Cloud platform and will be available in a few minutes.

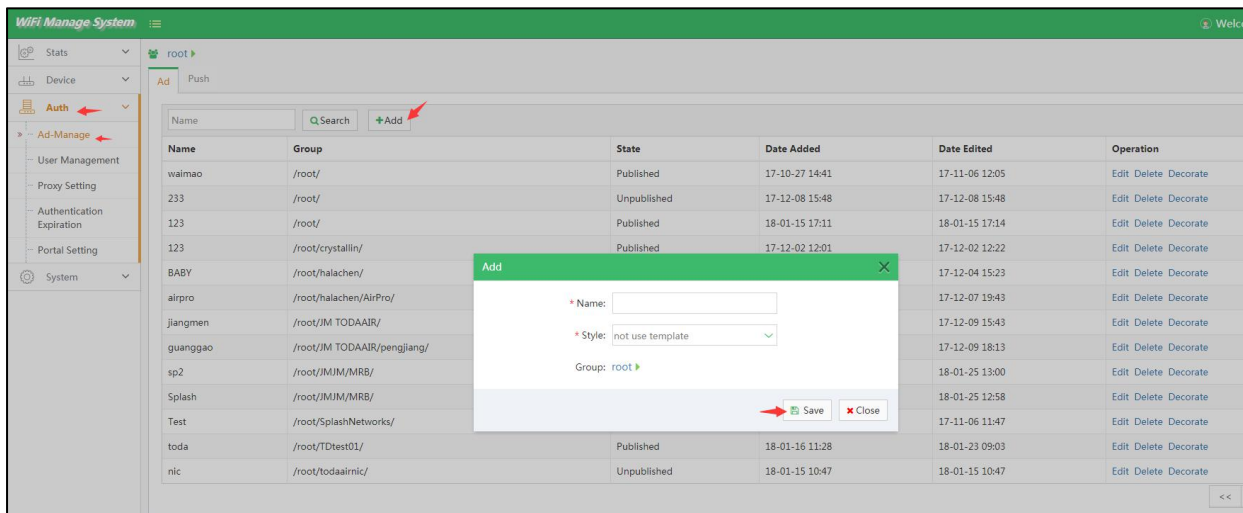


## STEP 5

### 5. Configuration of the Auth Function

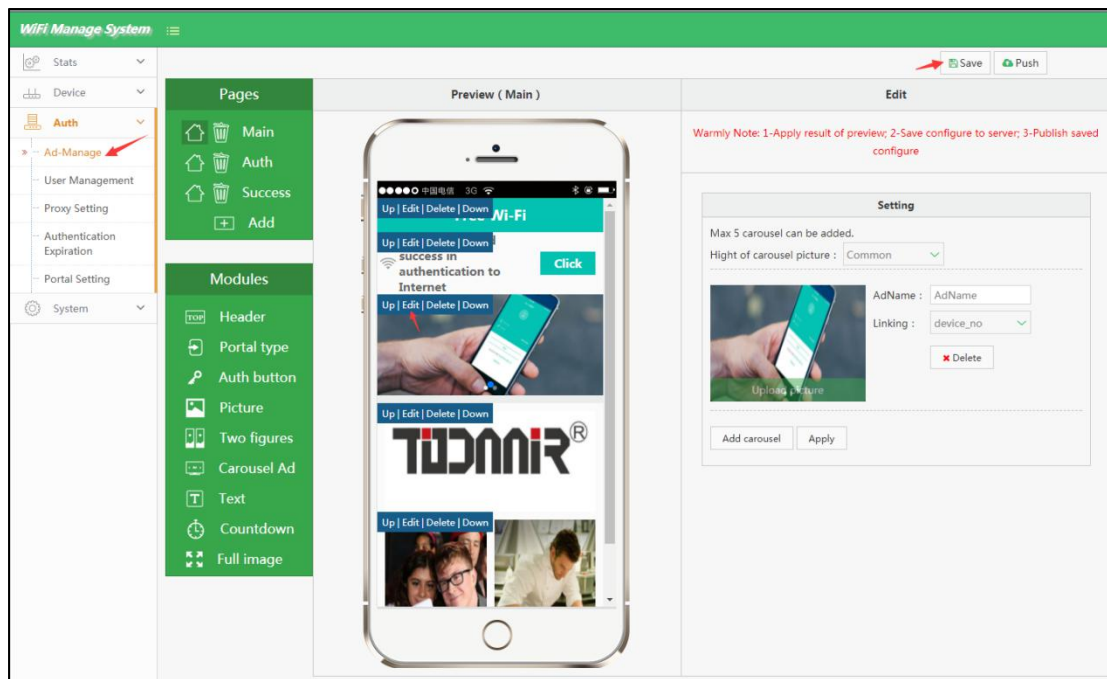
When the Auth is enabled, the terminals will receive a pop-up WiFi connecting page. If no connecting paged is preferred, the function can be disabled in the AP setting according to the Step 4.

5.1 Click Auth → Ad-Manager → Add, fill in the name of the Auth, choose the classic mode, and then choose the designated group to apply this function. Save the setting.

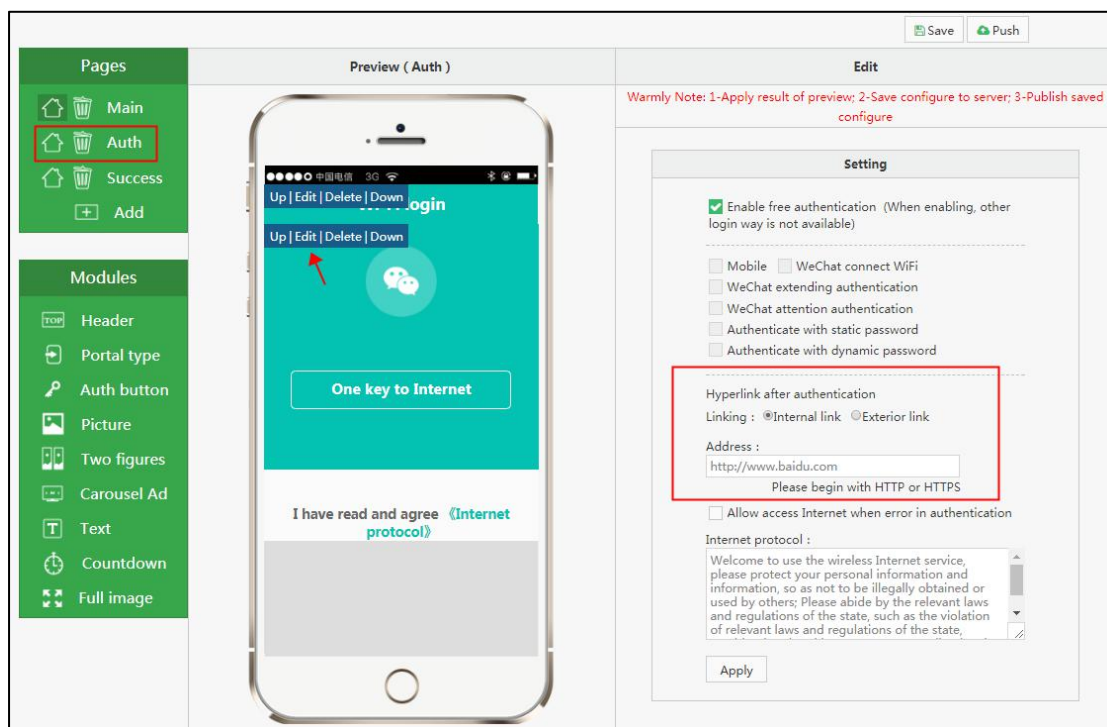




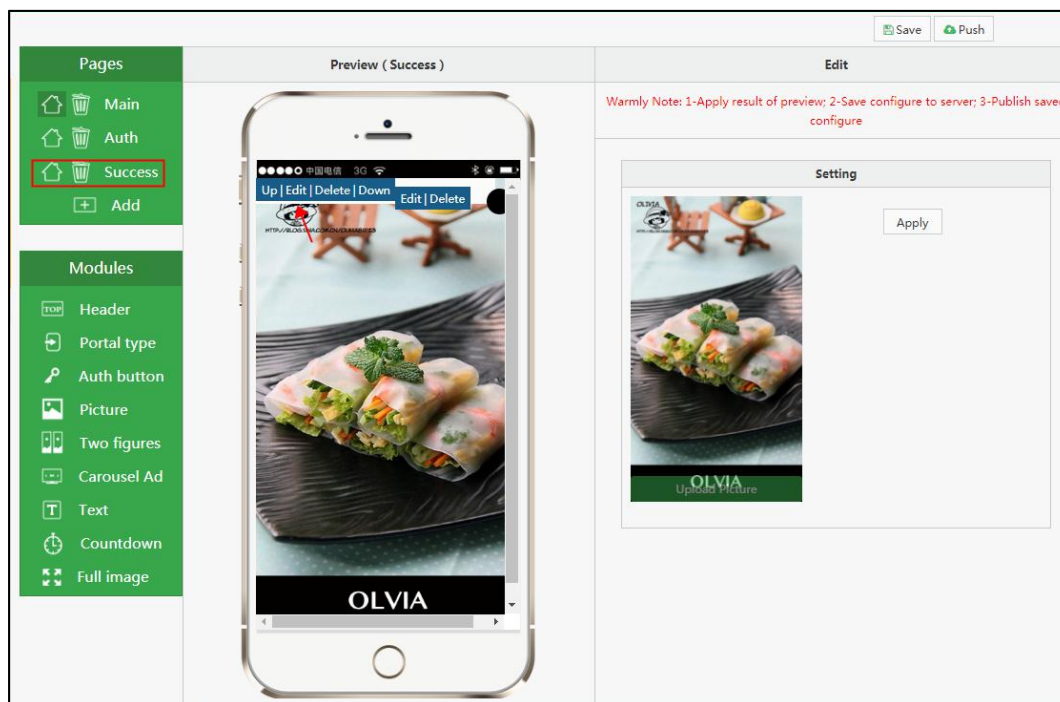




5.3.2 Auth page. The Auth page is after the main page. One-key authentication can be selected in this page. Click Auth → Edit, select the authentication method, fill in the intended Internal link, apply the settings.

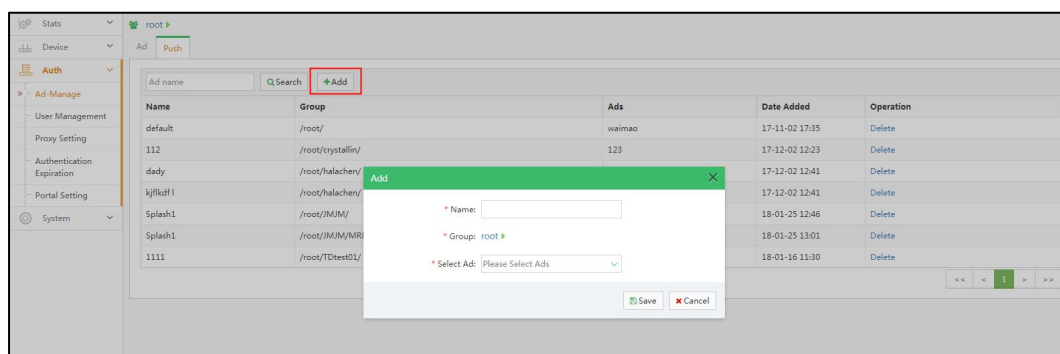


5.3.3 Success page. The final page of showing advertisement during the authentication process. Advertising picture, display duration, redirect URL, etc can be set in this page. Apply settings afterwards.

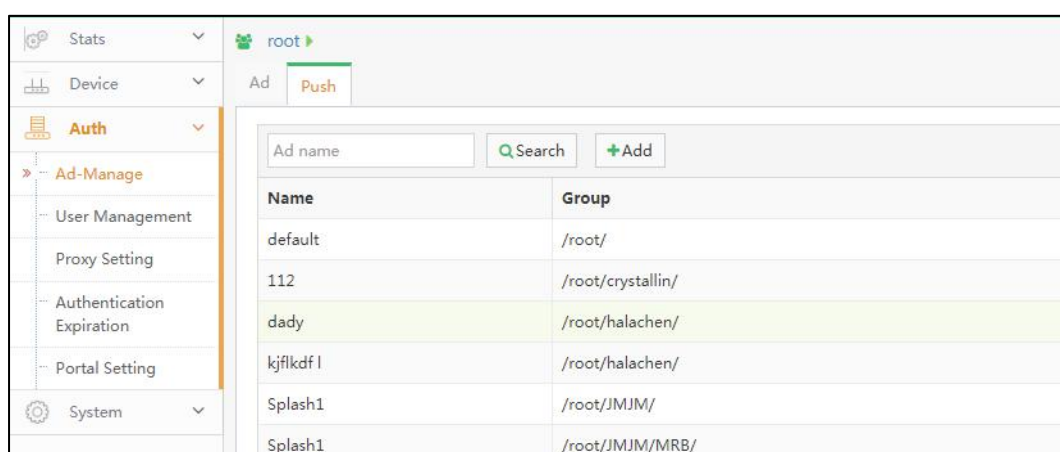


#### 5.3.4 Activate the advertisement.

After finishing the setting of all the three pages above, click Save on the top of the right side, and then click Push to activate the advertisement. Wait for three minutes and test the function with terminal devices. If failed to activate the Ad, please click Auth → Ad-Manage → Push. Click Add and fill in necessary info to activate the Ad in different groups.

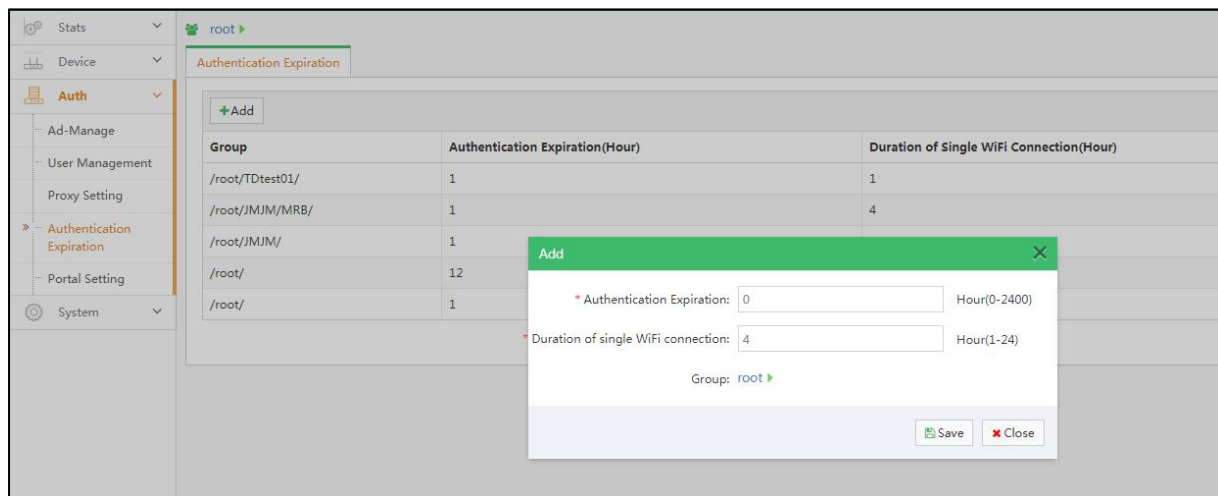


There is a list showing all the information of the Ads and the corresponding activated group.



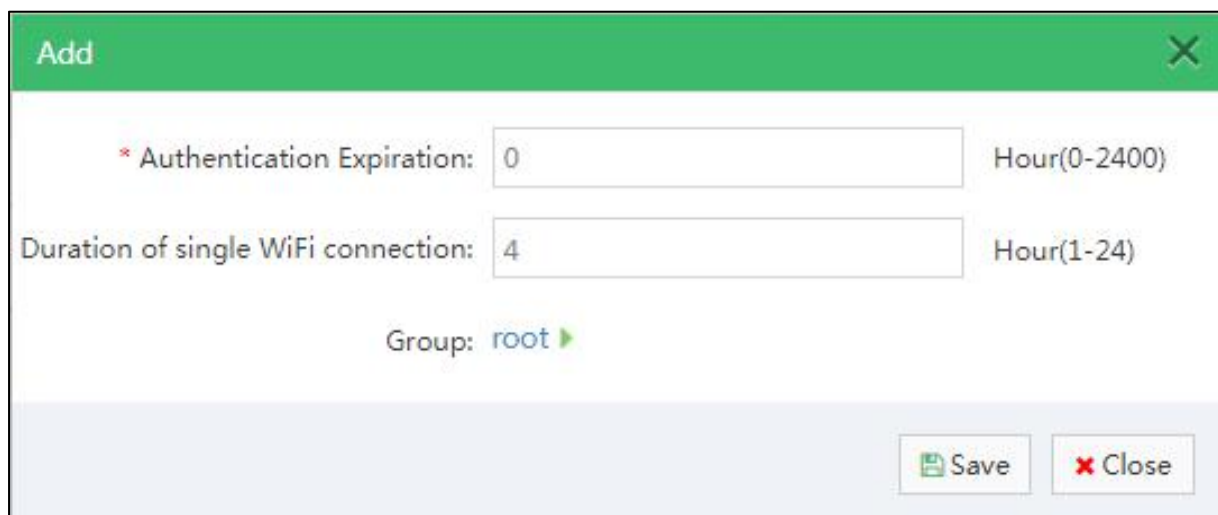
### 5.3.5 Set the authentication expiration for different groups.

Click Auth → Authentication Expiration → Add. Set the value of authentication expiration based on hours. And set the value of duration of single WiFi connection based on hours.



The screenshot shows the 'Authentication Expiration' configuration page. On the left, a sidebar menu includes 'Stats', 'Device', 'Auth', 'Ad-Manage', 'User Management', 'Proxy Setting', 'Authentication Expiration' (selected), 'Portal Setting', and 'System'. The main area displays a table with columns: 'Group', 'Authentication Expiration(Hour)', and 'Duration of Single WiFi Connection(Hour)'. The table contains five rows of data. An 'Add' dialog box is open in the foreground, allowing for a new entry. The dialog has fields for 'Authentication Expiration' (set to 0) and 'Duration of single WiFi connection' (set to 4), both with unit indicators. It also shows the 'Group' as 'root' and has 'Save' and 'Close' buttons.

Group	Authentication Expiration(Hour)	Duration of Single WiFi Connection(Hour)
/root/TDtest01/	1	1
/root/JM/JM/MRB/	1	4
/root/JM/JM/	1	
/root/	12	
/root/	1	



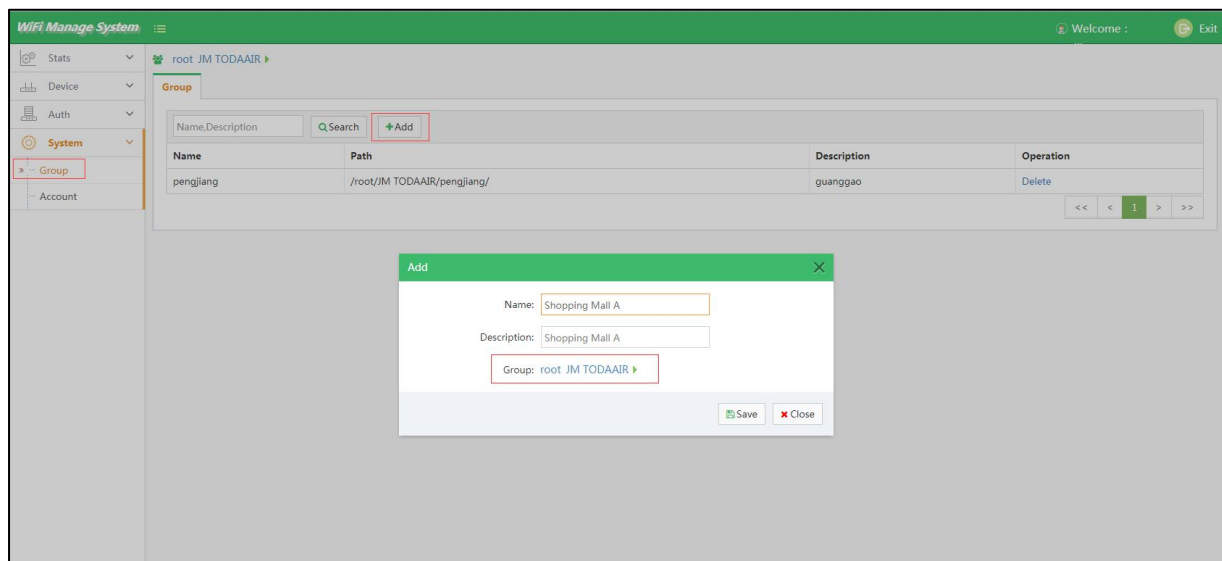
This is a close-up of the 'Add' dialog box. It features a green header with the title 'Add' and a close button. The form contains two main input sections: 'Authentication Expiration' with a value of '0' and a unit of 'Hour(0-2400)', and 'Duration of single WiFi connection' with a value of '4' and a unit of 'Hour(1-24)'. Below these is a 'Group' field showing 'root'. At the bottom right, there are 'Save' and 'Close' buttons.

## STEP 6

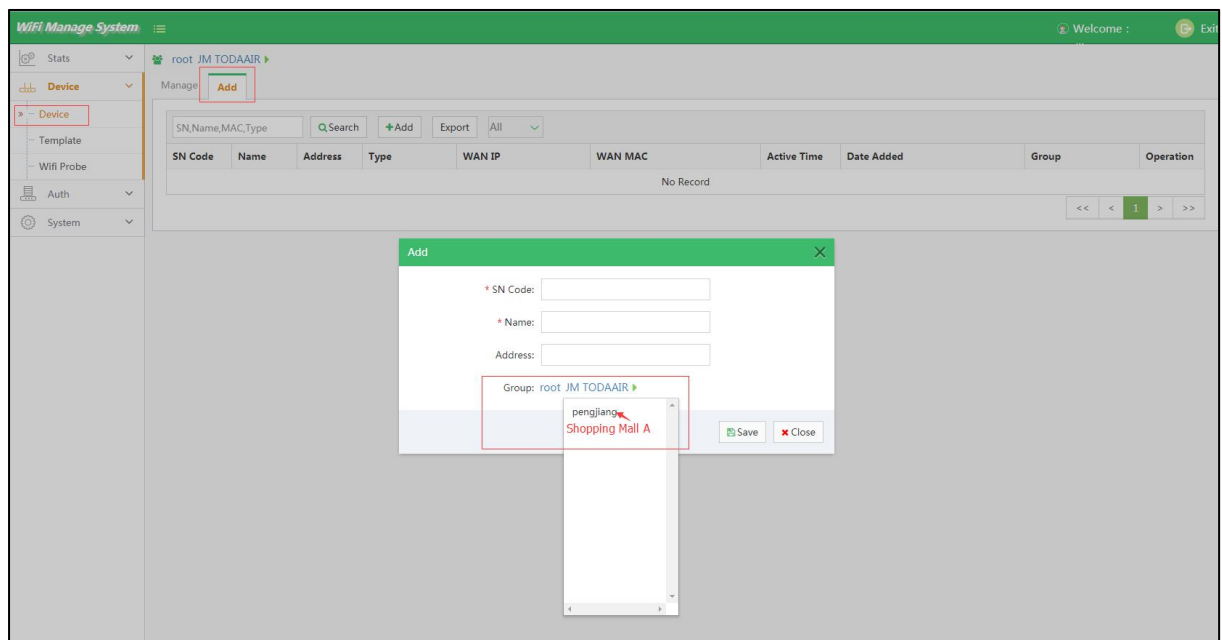
### 6. Group management

Through the group management, user can manage multiple APs in different area and choose different authentications. For example, if there are two projects in different areas, Shopping Mall A and Shopping Mall B. Both of the projects needs the AP installation and different authentication pages. In this case, user can create group for each of the project and set the AP and corresponding authentication into the designated group.

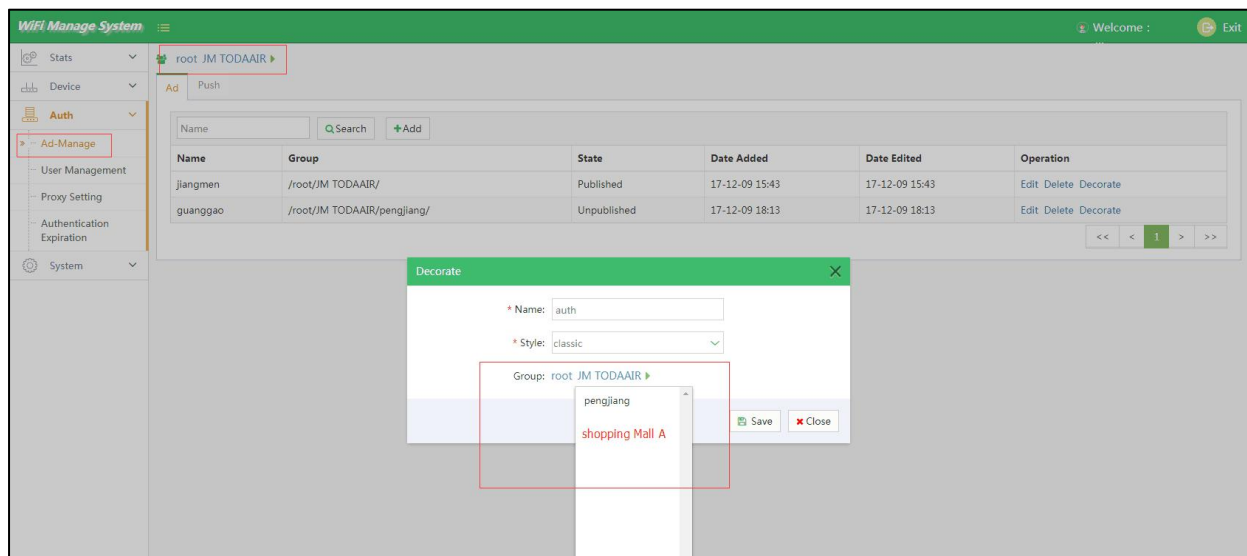
6.1 Click System → Group → Add, create a new group Shopping Mall A (The default account owns the highest authority group, any new established groups belongs to the highest authority group)



6.2 Set the specific AP in the corresponding group. Click the Device → Device → Add, click the Edit of the corresponding AP and set it in the designated group.



6.3 Set the Ad authentication. Click the Auth → Ad-Manage → Ad tab, choose the right Ad and click the Edit to apply the Ad in the specify group.



6.4 On the top of the tab, it shows the relationship of the groups. Click in to check the Ad content in different groups.

