

# **WAPI Wireless Security Router RAK5422AC User Manual**

Version V2.0 | July 2019

**[www.RAKwireless.com](http://www.RAKwireless.com)**

*Visit our website for more document.*

15 PAGES

## Table of Contents

1. Hardware and Installation.....	3
1.1 Interface.....	3
1.2 Product List.....	5
1.3 Environmental Requirements.....	6
1.4 Installation.....	6
1.5 Location Selection.....	6
2. Quick Configuration Guide.....	7
2.1 Connecting the Router.....	7
2.2 Built in AS Initialization.....	7
2.3 Certificate Issued.....	8
2.4 Router Login.....	9
2.5 Installation Certificate.....	10
2.6 Network Configuration.....	11
3. Restore Factory Setting.....	14
4. Revision History.....	15
5. Document Summary.....	15

# 1. Hardware and Installation

## 1.1 Interface

The interface of the front side of RAK5422AC device is shown in the following figure.

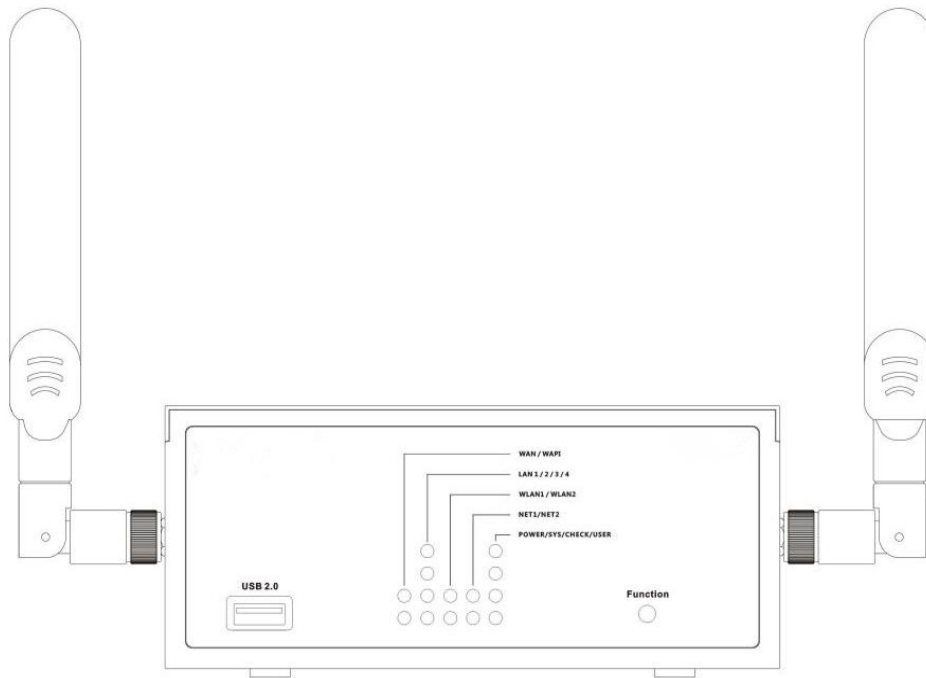


Figure 1-1 Front side of RAK5422AC

LED indicator at the front side of the device is described below.

	LED Name	Description
1	POWER	Power indicator, after power-up, the LED is always red on.
2	SYS	System indicator, after the system is fully started, the LED is in blue flashing state.
3	CHECK	Self-check indicator, it is orange on when power-up, after self-check is completed, the LED is off.
4	USR	Reserved
5	NET1/NET2	Reserved

6	WLAN1/WLAN2	<p>Wireless status indicator;</p> <p>WLAN1 for Radio1;</p> <p>The LED is always green on when system start up, flickering when data transmission.</p> <p>WLAN 2 for Radio 2;</p> <p>The LED is always orange on when system start up, flickering when data transmission.</p>
7	LAN1/2/3/4	<p>LAN port status indicator;</p> <p>Corresponding to the LAN ports 1, 2, 3, 4, after the LAN port is connected, the LED is always green on, and flickering when data transmission.</p>
8	WAN	<p>WAN port status indicator;</p> <p>Corresponding to the WAN port, after the WAN port is connected, the LED is always green on, and flickering when data transmission.</p>
9	WAPI	<p>WAPI security start LED indicator, when the WAPI security mechanism is enabled, the LED is always orange on.</p>

Note: Function button at the front side is used for WAPI-EC mechanism, which can quickly establish a WAPI secure connection with the WAPI terminal. The USB 2.0 interface at the front side has not been developed yet, it is reserved.

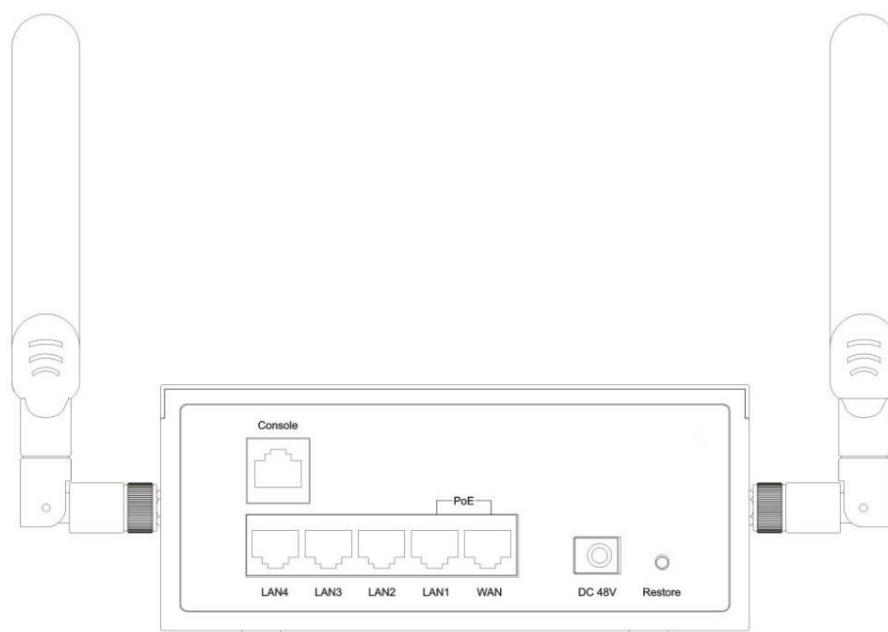


Figure 1-2 Back side of RAK5422AC

Interfaces at the back side of the device is described below.

	<b>Interfaces Name</b>	<b>Description</b>
1	DC 48V	DC 48V power supply interface.
2	WAN	Wired WAN port, supports PoE power supply.
3	LAN1	Wired LAN1 port, supports PoE power supply.
4	LAN2	Wired LAN2 port.
5	LAN3	Wired LAN3 port.
6	LAN4	Wired LAN4 port.
7	Console	Reserved
8	Restore	Restore or restart keys;  Press the key within 3 seconds : restart the device.  Press the key more than 6 seconds : restore the factory settings.

## 1.2 Product List

	<b>Name</b>	<b>Number</b>
1	Wireless Security Router RAK5422AC	1
2	Antenna	6
3	48V power adapter	1
4	Ethernet cable	1
5	Installation package	1

## 1.3 Environmental Requirements

1. There must be an AC 100V-240V, 50Hz-60Hz power interface to supply power to Wireless Secure Routers through power adapters or with PoE switches, and through ethernet cable to supply power.
2. At least one 10Mbps/100Mbps/1000Mbps adaptive Ethernet interface for connecting the wired networks.

## 1.4 Installation

Basic Principles of Hardware Installation:

The signals of RAK5422AC wireless security router can reach 400 meters outdoors and 100 meters indoors. Within this range, wireless access to the network can be used anywhere. Please note that walls, ceilings or other obstacles and the number, thickness and location of the obstacles will affect the transmission of wireless signals, which will limit the coverage of wireless signals. The coverage of device will vary with the type of obstacles and the size of radio frequency noise.

The key to maximizing the range of wireless signals is to follow the following basic principles:

1. Minimize barriers between wireless secure routers and receiving devices. Each wall or ceiling will reduce the signal range of the wireless security router by 1-30 meters, and properly place the wireless security router and terminal devices so as to minimize the number of walls and ceilings between them.
2. Make sure that the distance between the wireless security router and the terminal device is a straight line as far as possible. When a wall with a thickness of 0.5 meters is 45 degrees, it is equivalent to a wall with a thickness of 1 meter. The wireless security router and terminal equipment should be properly installed so that the signal can be vertically passed through the wall or ceiling to achieve the best reception effect.
3. Signal range varies with building materials. Strong metal doors will attenuate the signal range. Wireless security routers and terminal devices should be properly positioned so that the signal can directly pass through the wall or open the door.
4. Keep the RAK5422AC device away from electronic devices or devices that may generate RF noise for at least 1-2 meters.

## 1.5 Location Selection

Before installing the wireless security router, it is necessary to select an appropriate location for it. To ensure the effect of wireless connection, you should make sure that

there is no overlap with the channels used by adjacent wireless devices in the same frequency band.

## 2. Quick Configuration Guide

### 2.1 Connecting the Router

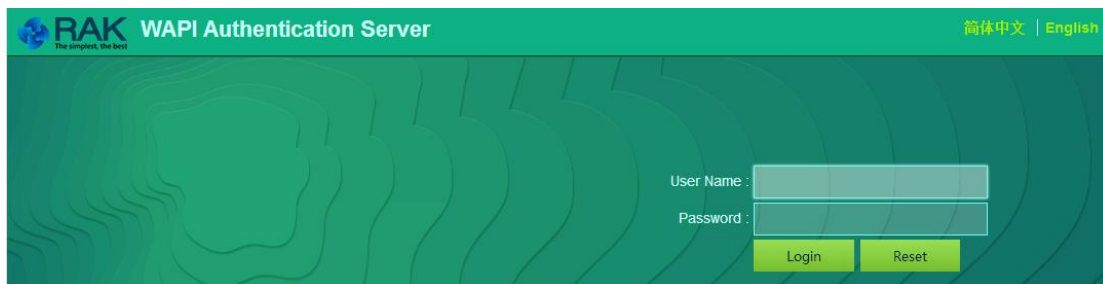
The default IP address of the device is 192.168.1.1 (LAN port). It is necessary to configure the IP address of your PC and the LAN port of the RAK5422AC wireless security router in the same network segment, such as 192.168.1.10.

**Note: The browsers that you use to login to the RAK5422AC router recommend IE10 and above, Chrome 62 and above, Firefox 55 and above.**

### 2.2 Built in AS Initialization

The device has a built-in identification server (AS) function, which can issue certificates to terminal devices through built-in AS.

You need to initialize the device before the certificate. Enter <https://192.168.1.1:8758> in the browser's address bar. The default account name: **hufuas**, and default password: **hufu.as4138**. As shown in the following figure.



Then enter AS Initialization, input the administrator's key (default is **hufu.seroot4138**), click <OK> to initialize. The local certificate will be emptied after initialization. As shown in the following figure.

AS Initialization

*Note : Initialization will lead all certificates invalid.*

Base configuration

Common Name(CN): @ASU Note:The part before '@' of Common Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

Authentication Server Port:

Organization Name

Domain Component(DC):

Country Name (C):  Note:Country Name can only be capital.

Organization Name (O):  Note:Organization Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

Organizational Unit Name(OU):  Note:Organizational Unit Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

System administrator

Administrator password :

Initialization successful, as shown in the following figure.

AS Initialization

*Note : Initialization will lead all certificates invalid.*

Base configuration

Common Name(CN): @ASU Note:The part before '@' of Common Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

Authentication Server Port:

Organization Name

Domain Component(DC):

Country Name (C):  Note:Country Name can only be capital.

Organization Name (O):  Note:Organization Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

Organizational Unit Name(OU):  Note:Organizational Unit Name must consist of one or more kinds of Chinese characters,digits,letters,underscores,dots.

System administrator

Administrator password :

**Initialization**

initialization successful

## 2.3 Certificate Issued

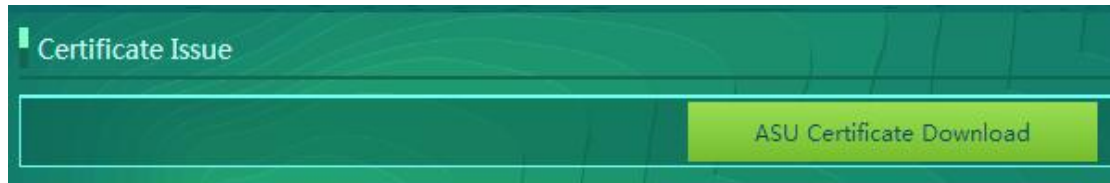
After the completion of the initialization, certificate issue settings are required.

### 1) ASUE certificate download



Enter the Certificate Issue page, click <ASUE Certificate Download>. ASUE certificate and user certificate are installed in the user's device.

As shown in the following figure.

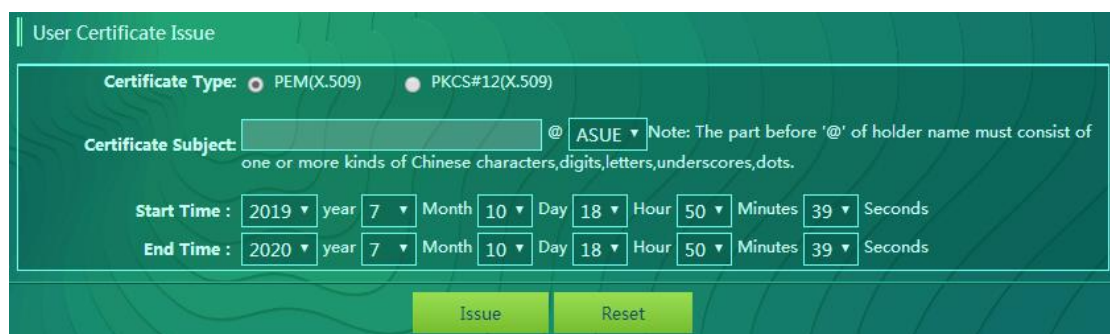


## 2) user certificate issued

User certificate issued is divided into "PKCS#12" type(password certificate) certificate and "PEM" type certificate, as shown in the following figure.

Then you can select the certificate type, certificate password, holder name, type and certificate validity period.

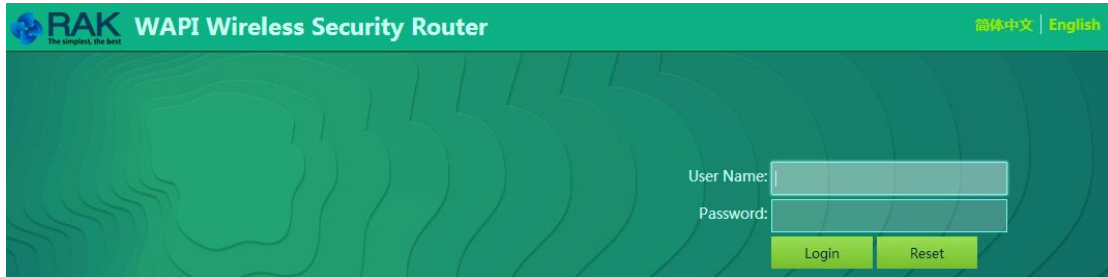
Then Click <Issue> download and save the certificate. As shown in the following figure.



## 2.4 Router Login

Firstly you need connect the LAN port of wireless security router. And also make sure that the IP address of the RAK5422AC router and your PC is in the same network segment. Then enter <https://192.168.1.1:8759> (default address of wireless security router) in browser, and enter the Wireless security router login interface.

User Name is : **hufuap**, and default Password is: **hufu.ap4138**, then click <Login> enter the router configuration page. As shown in the following figure.

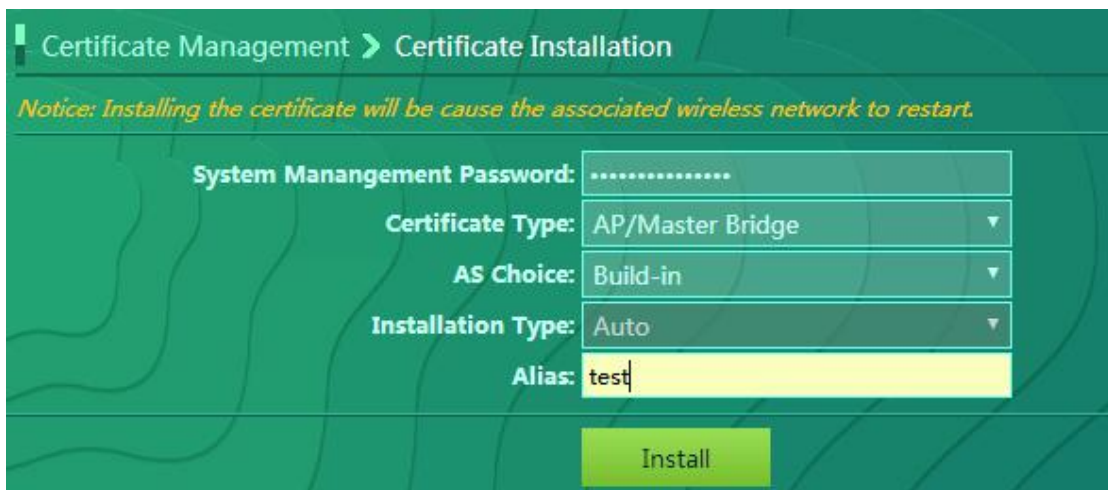


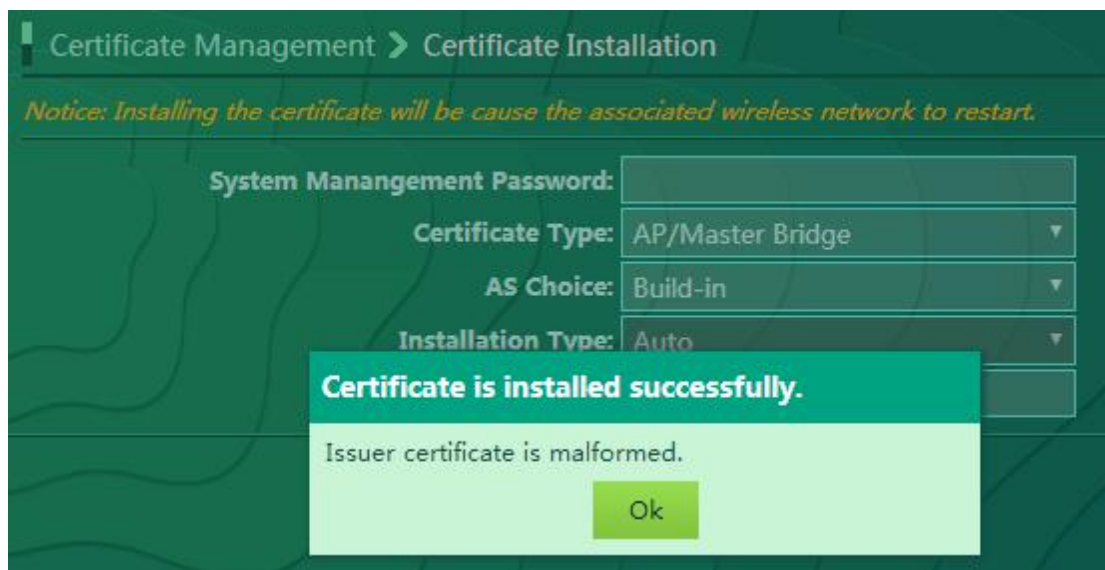
## 2.5 Installation Certificate

After initialization, you need install the certificate according to the operation mode of the device. Select <Certificate Management> <Install>. As shown in the following figure.



Then we can input the management password **hufu.seroot4138**, choice AP/Master Certificate Type, Auto Installation Type, Build-in AS Choice, then input a certificate Alias. As shown in the following figure.





Users can modify the already installed certificate alias and trusted AS's IP. As shown in the following figure.



Note:

- I. The default system management password: **hufu.seroot4138**;
- ii. Certificate types are divided into AP/Master certificate and Client/Slave certificate.
- III. AS Choice can be selected as an independent AS and a built-in AS. If built-in AS is selected, the default installation mode is automatic and you need to input the certificate alias.
- IV. Installation mode can be selected as "manual" or "automatic".
- V. If AS is selected for external location and installation is automatic, external AS is required to support this function before it can be used.

## 2.6 Network Configuration

Enter the <Network Configuration>, select WLAN Configuration, as shown in the following figure.

Network Configuration > WLAN Configuration

*Notice: Modify or add a wireless network may cause all network terminals connected to the network is interrupted.*

Wireless Overview

Radio0	Modify	Add
<b>Mode:</b> AP   <b>SSID:</b> WAPI1 <b>Channel:</b> 149 (5.745 GHz)   <b>Quality:</b> 0%   <b>BSSID:</b> 60:C5:A8:74:D1:B1   <b>Encryption:</b> WAPI-PSK		
Radio1	Modify	Add
<b>Mode:</b> AP   <b>SSID:</b> WAPI2 <b>Channel:</b> 1 (2.412 GHz)   <b>Quality:</b> 0%   <b>BSSID:</b> 60:C5:A8:74:D1:B2   <b>Encryption:</b> WAPI-PSK		

Radio0 Connection information

No.	SSID	MAC Address	IPv4 Address	Signal	Noise	Receiving rate	Sending rate
No information available							

Radio1 Connection information

No.	SSID	MAC Address	IPv4 Address	Signal	Noise	Receiving rate	Sending rate
No information available							

On this page you can view wireless network information, including wireless mode of operation, SSID information, channels, security classes etc. Also you can add remove and modify the wireless configuration, radio frequency enabled and disabled etc. As shown in the following figure.

### 1) Enable or Disable wireless networks

Select the configured wireless network, click <enable> or <disable> to turn on or turn off the wireless network.

### 2) Add wireless network (SSID)

On this page, you can configure SSID name, mode, WMM, security type, certificate, Password and so on. For example as shown in the following figure.

Network Configuration > WLAN > Wireless Configuration

*Notice: Modify or add a wireless network may cause all network terminals connected to the network is interrupted.*

SSID Configuration

Basic Settings | **Advanced Settings**

SSID: ssid0

UTF-8  GB2312

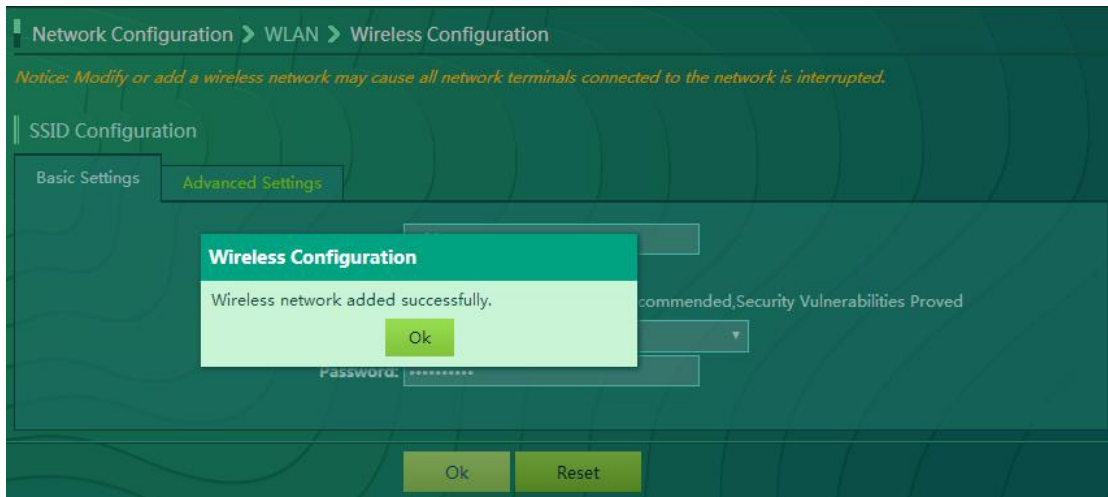
Security Type: WPA/WPA2-PSK NOT Recommended, Security Vulnerabilities Proved

Algorithm: Auto

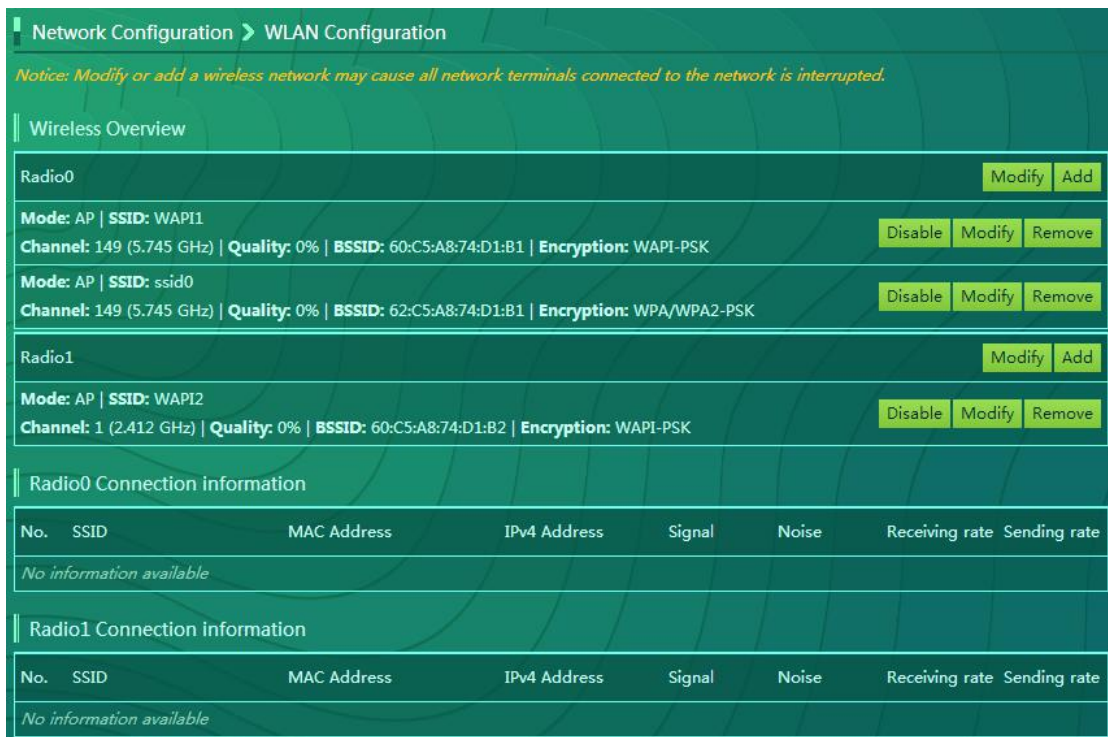
Password: .....

Ok Reset

Wireless network added successful.



ssid0 AP added successful, as shown in the following figure.



### 3) Modifying wireless network (SSID)

Select the SSID you want to modify and click <Modify> to change the content in the next step on the SSID Configuration page.

### 4) Remove wireless network (SSID)

Select the SSID you want to delete and click <Remove> to delete this wireless network.

### 3. Restore Factory Setting

Restore Factory Setting for RAK5422AC hardware: press the restore key for more than 6 seconds, then wait the WAPI LED to flicker, which indicating starting to restore factory settings. Until the WAPI LED does not flicker, and the system LED starts to flicker, which indicating that system has completed the restoring factory settings

**Note: After upgrading the firmware or restoring the factory default configuration, you need to reinstall the AP certificate in the certificate management page.**

**Please contact us if you need technical support or want to know more information.**

**Support center:** <https://forum.rakwireless.com/>

**Email us:** [info@rakwireless.com](mailto:info@rakwireless.com)

## 4. Revision History

Revision	Description	Date
1.0	Initial version	2018-08-21
2.0	Modify login account and web page	2019-07-10

## 5. Document Summary

Prepared by	Checked by	Approved by
Fomi	Penn&Fomi	



### About RAKwireless:

RAKwireless is the pioneer in providing innovative and diverse cellular and LoRa connectivity solutions for IoT edge devices. It's easy and modular design can be used in different IoT applications and accelerate time-to-market.

For more information, please visit RAKwireless website at [www.rakwireless.com](http://www.rakwireless.com).