



Wireless Access Controller

User's Manual

V 1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Legal Statement


Copyrights

© 2018 ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.. All rights reserved.

Any or full contents of the user's manual cannot be copied, transmitted, distributed, partially or wholly, by any means, without the prior written notice of ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. (hereinafter "Dahua").

Dahua or the third party may reserve the right of the product described in this user's manual. Without the prior written approval of the corresponding party, any person cannot copy, distribute, amend, reverse compile, disassemble, decode, reverse engineering, rent, transfer or sub-license the software.

Trademark

-  and **HDCVI** are the trademarks or registered trademarks of the Dahua in various jurisdictions.
- HDMI logo, HDMI and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC. This product has been authorized by HDMI Licensing LLC to use HDMI technology.
- VGA is the trademark of IBM.
- Windows logo and Windows are trademarks or registered trademarks of Microsoft.
- Other trademarks and company names mentioned are the properties of their respective owners.

About this Document

- This document is for reference only. Please refer to the actual product for more details.
- This document serves as a reference for multiple types of products, whose specific operations won't be enumerated. Please operate according to actual products.
- The user shall undertake any losses resulting from violation of guidance in the document.
- In case that PDF document cannot be opened, please upgrade the reading tool to the latest version or use other mainstream reading tools.
- This company reserves rights to revise any info in the document anytime; and the revised contents will be added to the new version without prior announcement. Some functions of the products may be slightly different before and after revision.
- The document may include technically inaccurate contents, inconsistencies with product functions and operations, or misprint. Final explanations of the company shall prevail.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device’s IP address.

- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Overview





This document mainly introduces mounting and basic function of small wireless AC management platform.

Applicable Model

DH-PFM888S-AC

Symbol Definition

The following symbols may appear in the document. Please refer to the table below for the respective definition.

Symbol	Note
	It indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	It indicates a potential risk that, if ignored, could result in damage to device, loss of data, degraded performance, or unpredictable results.
	It means that it can help you to solve some problems or save your time.
	It means the additional info, which is to emphasize or supplement.

Revision Record

No.	Version No.	Revision Content	Release Date
1	V 1.0.0	First release	2018.3.20

Important Safeguards and Warnings

The following description is the correct application method of the device. Please read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

Suitable working environment is the foundation of normal operation. Please check whether it meets the following conditions before mounting.

- Please transport, use and store the device within allowed humidity and temperature range. For working humidity and temperature, please refer to technical parameters of the product.
- Please use and store the device on a stable foundation or in a fixed standard cabinet.
- Please pack the device with original package or equivalent material during transportation.
- Please don't block the vent of the device. Install it at well-ventilated places and keep at least 2 cm distance away from another device.
- Please don't put the device in explosive, damp, dusty, extremely hot, extremely cold, corrosive gas, strong electromagnetic radiation or instable lighting conditions.
- Please don't install the device in an area exposed to direct sunlight or near heat generating device, such as radiator, heater, furnace or other heating device, in order to prevent fire.
- Please prevent liquids from flowing into the device, in order to protect internal elements. In case that liquids flow into the device, please stop using at once, cut off power supply, pull out all cables and contact after-sales service.
- Please don't press, vibrate violently or immerse the device during transportation, storage and installation.
- Please don't dismantle the device unless the supplier's professionals are on the site or provide guidance.
- During deployment and use, please backup data timely, in order to prevent data loss due to abnormal operation.

Power Requirement

Safe and stable power supply is a precondition of normal work.

- Please conform to local electrical safety standard strictly; ensure that voltage is stable and meet power supply requirement of the device.
- Before operation, please check whether power supply is correct.
- Please use the power adapter or case power provided by the device manufacturer.
- Please don't connect the device after powering on power adapter. The power adapter and device shall be connected under power-off state.
- Please don't disconnect power cable of the device when power adapter is on.
- For permanently connected device, please install an obvious and easily identifiable all-pole disconnection device in external power circuit.
- In case that domestic or industrial plug is used and power is cut off by pulling out the plug, please mark the plug, for the purpose of emergency power-off when necessary.

- Please don't provide two or more power supply modes simultaneously, which may damage the device or lead to safety risks.
- It is suggested that overcurrent protection device (fuse or air switch) should be used in serial in device power circuit. Its overcurrent protection rated value shall not exceed 2 times as many as rated current of the device.
- Faulty power shall be replaced with a new power of the same specification.

Table of Contents

Legal Statement	I
Cybersecurity Recommendations.....	II
Preface.....	V
Important Safeguards and Warnings.....	VI
1 Product Overview	1
1.1 Product Profile	1
1.2 Features	1
1.3 Hardware Parameters	4
1.4 Performance Specification.....	5
2 Device Mounting	6
2.1 Interface.....	6
2.2 Device Mounting	7
3 Go Online	8
3.1 L2 Goes Online	8
3.1.1 Access Point Device Goes Online	8
3.1.2 Client Device Goes Online.....	9
3.2 L3 Goes Online	10
3.2.1 Access Point Device Goes Online	11
3.2.2 Client Device Goes Online.....	13
4 Functional Introduction.....	15
4.1 Login	15
4.2 State Statistics.....	16
4.3 Device Management.....	17
4.3.1 Device List.....	17
4.3.2 Delete Device	18
4.3.3 Edit Group	19
4.3.4 Issue Template.....	21
4.3.5 Device Upgrade.....	22
4.3.6 Retrieve the Client	23
4.4 Terminal Management.....	24
4.4.1 Terminal List.....	24
4.4.2 Info Statistics.....	25
4.5 Advanced Management	28
4.5.1 Template Management.....	28
4.5.2 Image Management.....	35
4.5.3 System Log	38
4.6 System Settings	39
4.6.1 Basic Settings	39
4.6.2 Upgrade Configuration Management.....	42
4.6.3 Access Control.....	43
4.7 Map Mode	51

4.7.1 Online Map.....	51
4.7.2 Offline Map.....	54
4.7.3 Map Management.....	55
4.8 Marketing Management	56
4.8.1 Advertising Management	57
4.8.2 Theme Management.....	58
4.8.3 Advertising Statistics.....	59
4.8.4 Message Management.....	60
4.8.5 Application Example	60
4.9 Logout.....	64



1 Product Overview

1.1 Product Profile

DH-PFM888S-AC is a wireless access control product independently researched, with a built-in Dahua wireless management platform. With this controller, realize centralized management and configuration of AP, and solve some management problems of traditional AP.

Without needs to change the structure, this controller integrates with existing network perfectly, simplifies network allocation and management greatly, and thus saves users' investment. It is able to manage 256 sets of equipment, so maximum amount of users reaches 8,192. It is able to upgrade automatically, issue the configuration automatically to access points and clients, realize real-time surveillance, and reduce network deployment cost and maintenance difficulty greatly. Wireless cloud platform is widely used in campus, large enterprise and city, to provide powerful WLAN hotspot coverage capability.

1.2 Features

Multi-device Management

DH-PFM888S-AC provides a friendly Web configuration interface, so as to help network administrator to complete device configuration and maintenance with the highest efficiency.

- Support CAPWAP protocol.
- Multi-level device management.
- Support manual and automatic upgrade of the device.

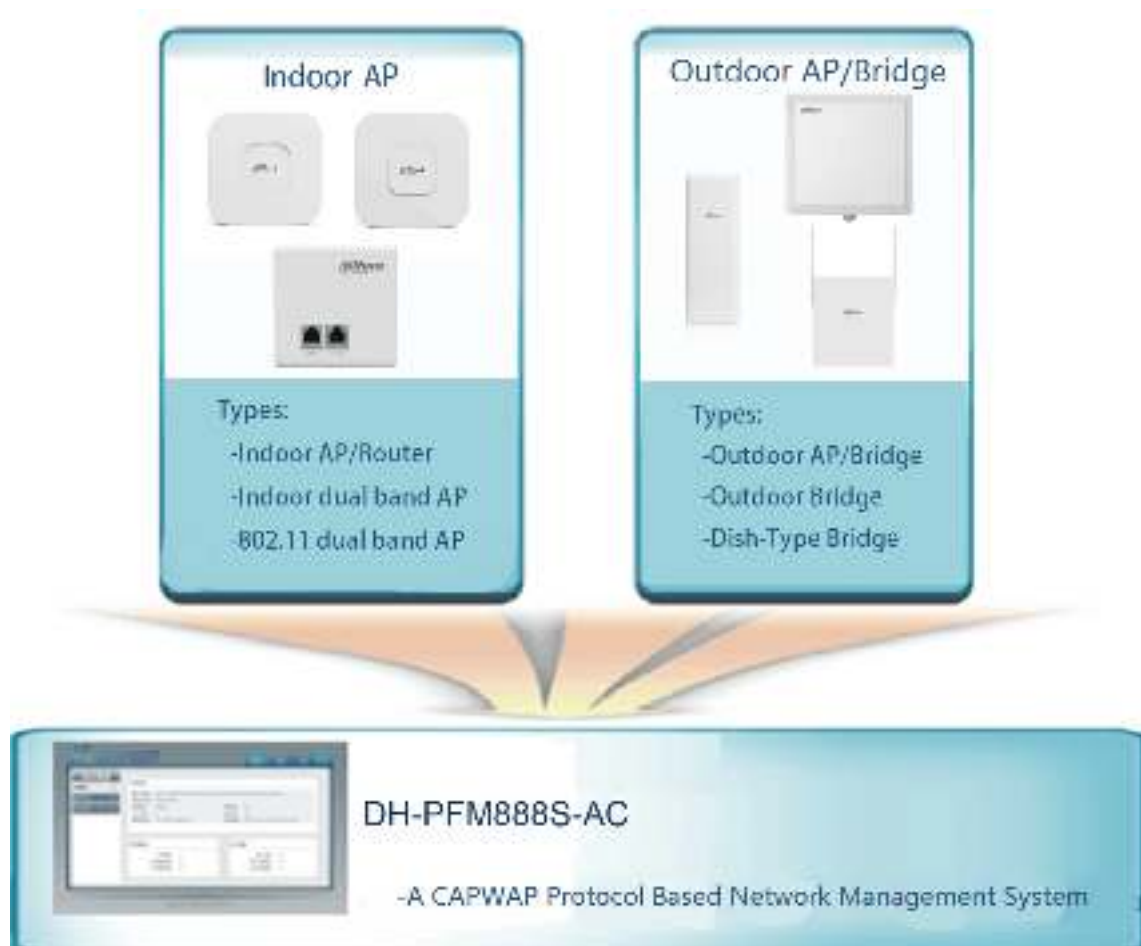


Figure 1-1

L2/L3 Network Configuration

DH-PFM888S-AC boasts functions such as user management, smart radio frequency (RF) management and restoration. In any existing L2/L3 network, this product can realize seamless and safe wireless network configuration, without needs to interrupt present network operation.

- Find the device through static IP or automatically
- Issue wireless configuration module.

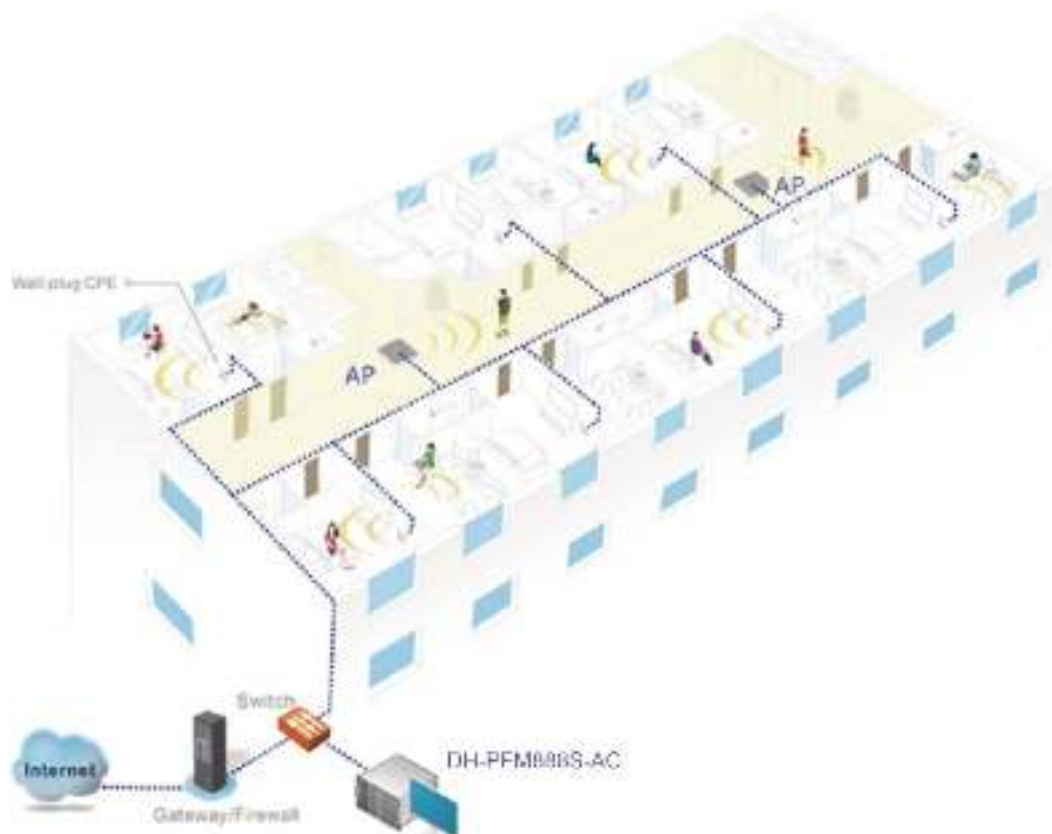


Figure 1-2

Real-time Surveillance System

With real-time surveillance function, DH-PFM888S-AC is able to monitor the operating state of network, and timely report connection, disconnection and abnormal alarm info. Meanwhile, all records can be uploaded to log server.

- Support many types of system info.
- Support many types of warning info.
- Support system log service.

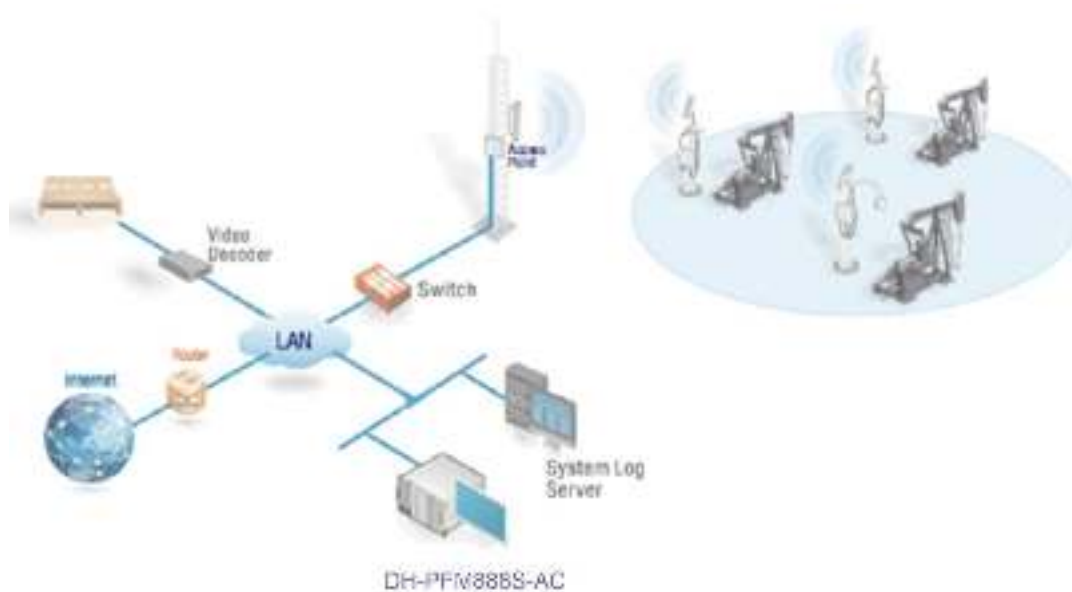


Figure 1-3

Map Display Device

With map display function, observe the distribution and operation conditions of the device.

- Support to display device location on Baidu/Google Map.
- Visually display the device info on the map.



Figure 1-4

1.3 Hardware Parameters

For relevant hardware parameters, please refer to Table 1-1.

No.	Feature	Specification
1	CPU	IPQ4028
2	Memory	256MB
3	Storage space	256MB
4	Physical interface	<ul style="list-style-type: none">• 5×10/100/1000M Base-TX• 1×USB• 1×Console
5	Dimension	170 mm×160 mm×34mm
6	Power supply	DC 12V 2A
7	Operating ambient temperature	-10℃～55℃
8	Operating ambient humidity	5%～95% (non-condensation)

Table 1-1

1.4 Performance Specification

For performance specification of DH-PFM888S-AC, please refer to Table 1-2.

No.	Features	Specification
1	Quantity of managed devices	256
2	Quantity of support modules	256
3	STA	8192

Table 1-2

2 Device Mounting

2.1 Interface

Schematic diagram of interfaces is shown in Figure 2-1. Please refer to Table 2-1 for descriptions.

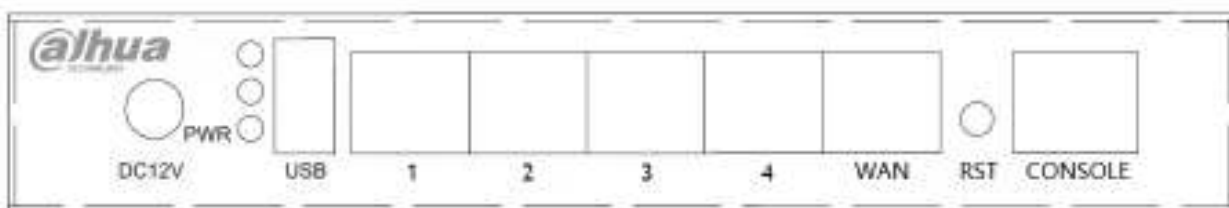


Figure 2-1

No.	Interface	Name	Connection and Function
1	DC12V	DC-JACK	DC power supply (12V 2A).
2	LED indicator	LED indicator	Power indicator, 2G/5G indicator.
3	USB	USB	Import license info to open authority of AP managed number. The largest managed number has been opened at present.
4	LAN1~LAN4	LAN interface	<ul style="list-style-type: none">Access point device can go on line after corresponding configuration and connection with this interface through network cable.After PC is connected with this interface through network cable, open the browser to input IP address of management interface, in order to visit and manage the device.Default address of LAN interface is 192.168.1.100.
5	WAN	Management interface	<ul style="list-style-type: none">After PC is connected with this interface through network cable, open the browser to input IP address of management interface, in order to visit and manage the device.Default address of WAN interface is 192.168.3.100.
6	RST	Reset key	Restore factory settings.
7	CONSOLE	Control interface	Use serial port line to connect this interface; view and manage the device at the background.

2.2 Device Mounting

DH-PFM888S-AC can be mounted on the wall or on desktop directly.

Step 1 Drill 8mm hole in the wall.

Step 2 Put in rivet bolt, and tighten screw.

Step 3 Install the device onto the screw.

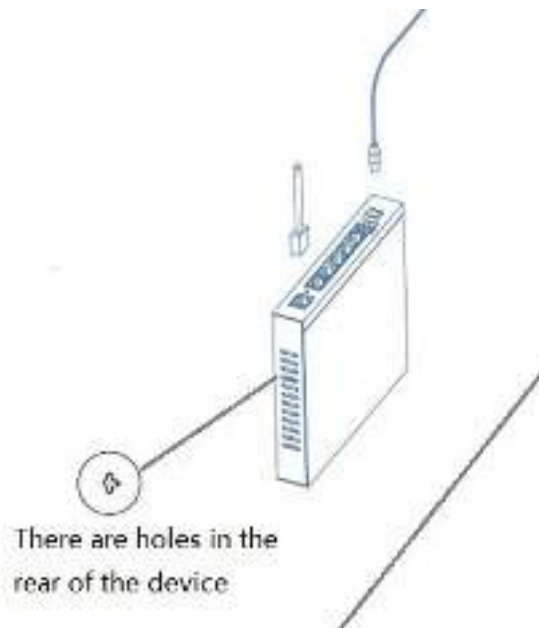


Figure 2-2

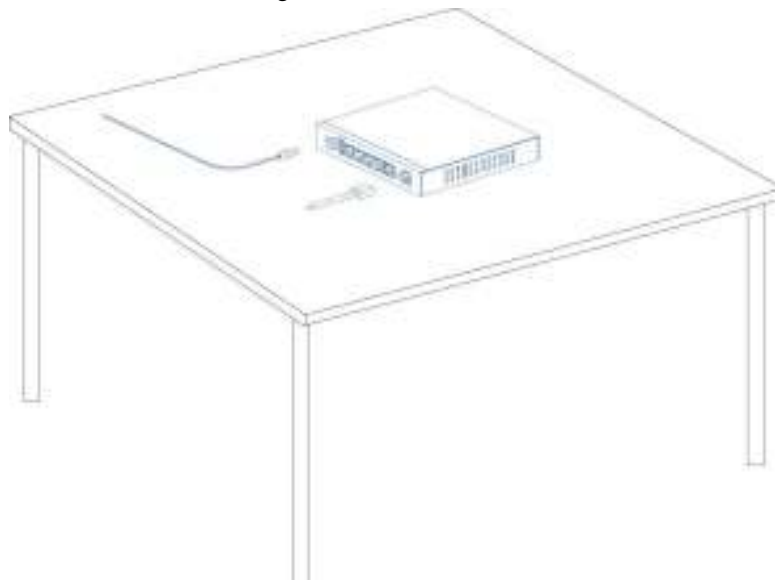


Figure 2-3

3.1 L2 Goes Online

Access points can directly connect LAN interface of DH-PFM888S-AC to go online. To join DH-PFM888S-AC, clients shall associate with access point device that has already joined DH-PFM888S-AC.

3.1.1 Access Point Device Goes Online

- Step 1 Open IP address page of the access point device to modify its IP address. For example, modify it to 192.168.1.36.
- Step 2 Set the following parameters in wireless setting page of access point device.
SSID is DaHua, channel is automatic, and default encryption is WPA2-PSK (secret key is 1234567890abc). After the access point device joins DH-PFM888S-AC, these parameters can be modified on DH-PFM888S-AC pages.

Basic Wireless Settings

Wireless Mode(?)	Access Point
SSID	DaHua
Frequency Mode	5GHz FHSS
Channel Power	20mW
IEEE 802.11 Mode	802.11n
Country Code	China (Mainland)
Channel Width	40MHz
WPA2 PSK Mode	WPA2 PSK

Wireless Security Settings

Security	WPA
Mode	WPA2
System	CCMP
Authentication Mode	PSK
WPA Key	1234567890abc

[Change](#)

Figure 3-1

- Step 3 At AC management page of AP wireless device, enable AC control function.

Controller Management

Controller ID:
 WTP Name:
 WTP Location:

Add IP Type:

IP Address	Action
Add IP: <input type="text" value="192.168.1.100"/>	<input type="button" value="Add"/>
IP: 192.168.1.100	<input type="button" value="Edit"/> <input type="button" value="Del"/>
IP: 192.168.1.100	<input type="button" value="Edit"/> <input type="button" value="Del"/>

Figure 3-2

Item	Description
WTP Name	Name of access point device on DH-PFM888S-AC, to be filled in according to needs.
WTP Location	Info about device location on DH-PFM888S-AC, to be filled in according to needs.
Add IP	<p>It consists of manual designation and automatic mode. Access point device IP and IP of DH-PFM888S-AC LAN interface shall be in the same network segment.</p> <ul style="list-style-type: none"> In case of manual designation, fill in IP address of DH-PFM888S-AC LAN interface manually; default address is 192.168.1.100. In case of automatic mode, search DH-PFM888S-AC address automatically and go online. After AC function is enabled, click Apply & Restart. Configuration of this function will take effect and the access point device will restart.

Table 3-1

Step 4 Connect access point device with one LAN interface of DH-PFM888S-AC, so the access point device will go online at DH-PFM888S-AC.

3.1.2 Client Device Goes Online



To join DH-PFM888S-AC, client devices shall wirelessly associate with access point device that has already joined DH-PFM888S-AC.

Step 1 Open IP address page of the client device to modify its IP address. For example, modify it to 192.168.1.37.

Step 2 Open wireless setting page of the client device, choose the access point whose SSID is DaHua; default encryption is WPA2-PSK (secret key is 1234567890abc).

Basic Wireless Settings

Wireless Mode(): Station ▼

SSID: Lohus Select

Frequency Scan Mode(): ☐ Enable

Output Power: 27 High

802.11 Mode: 11b, mixed ▼

Quality Code: Control Rate Test ▼ Select

Channel Width(): 20MHz ▼

Max TX Rate: Mbps(): MCS 15-300 ▼

Load AP Mac:

Wireless Security Settings

Security: WPA ▼

WPA: WPA2 ▼

Cipher: TKIP ▼

Authentication Mode: PSK ▼

WPA Key: Show

Change

Figure 3-3

Step 3 At AC management page of client device, enable AC control function.

Controller Management

Controller(): Bridge ▼

WTP Name: DH-PFM888S-STA WTP Location:

AP Mode Type: Master ▼

IP Address	Action
AP IP: 192.168.1.100	Add
IP: 192.168.1.20	File Del
IP: 192.168.1.101	Edit Del

Reboot

Figure 3-4

Up to now, setting of access point and client has been completed, ready to join DH-PFM888S-AC. Please check at DH-PFM888S-AC page.

3.2 L3 Goes Online

When DH-PFM888S-AC and the device to be managed are located in different network segments in relatively complicated network environment, online environment of access point and client is shown as follows.

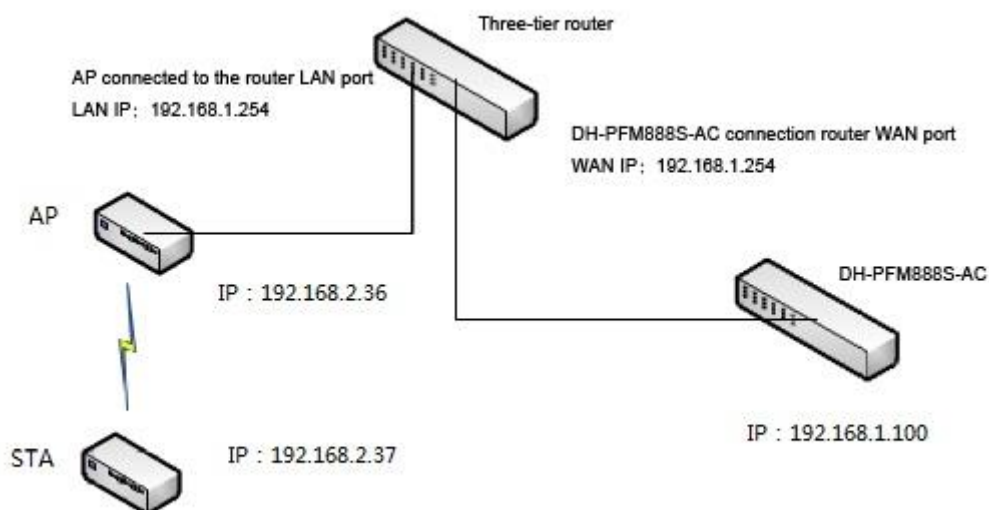


Figure 3-5

3.2.1 Access Point Device Goes Online

Step 1 Open IP address page of the access point device to modify its IP address. For example, modify it to 192.168.2.36. Gateway is the interface address of the connected upper router. For example, gateway in this example is set to be 192.168.2.254.

Management Interface:	<input type="text" value="br0"/>
IP Address:	<input type="text" value="192.168.2.36"/>
Netmask:	<input type="text" value="255.255.255.0"/>
Gateway IP:	<input type="text" value="192.168.2.254"/>
Primary DNS:	<input type="text" value="202.96.209.6"/>
Second DNS:	<input type="text" value="202.96.209.5"/>

Figure 3-6

Step 2 Set the following parameters in wireless setting page of access point device. SSID is DaHua, automatic channel; default encryption is WPA2-PSK (key is 1234567890abc). After the device joins DH-PFM888S-AC, these parameters can be modified on DH-PFM888S-AC pages.

Basic Wireless Settings

Wireless Mode(T):

SSID: ☐ Hide SSID

Frequency VHT:

Output Power:

802.11n Mode:

Channel Order:

Channel Width(T):

Max TX Rate (Mbps):

Wireless Security Settings

Security:

Mode:

Cipher:

Authentication Mode:

WPA Key:

Figure 3-7

Step 3 At AC management page of AP device, enable AC control function.

Controller Management

Controller(T):

WTP Name: WTP Location:

Add IP Type:

IP Address	Action
Add IP: <input type="text" value="192.168.1.101"/>	<input type="button" value="Add"/>
IP: 192.168.1.20	<input type="button" value="Edit"/> <input type="button" value="Del"/>
IP: 192.168.1.100	<input type="button" value="Edit"/> <input type="button" value="Del"/>

Figure 3-8

Item	Description
WTP Name	Name of access point device on DH-PFM888S-AC, to be filled in according to needs.
WTP Location	Info about device location on DH-PFM888S-AC, PFM888S to be filled in according to needs.
Add IP	<p>It consists of manual designation and automatic mode. Access point device IP and IP of DH-PFM888S-AC LAN interface shall be in the same network segment.</p> <ul style="list-style-type: none"> In case of manual designation, fill in IP address of DH-PFM888S-AC LAN interface manually; default address is 192.168.1.100. In case of automatic mode, search DH-PFM888S-AC address automatically and go online. After AC function is enabled, click Apply & Restart. Configuration of this function will take effect and the access point device will restart.

Table 3-2

Step 4 Connect access point device with one LAN interface of L3 router, whose IP address is 192.168.2.254. Access point device will go online at DH-PFM888S-AC.

3.2.2 Client Device Goes Online



To join DH-PFM888S-AC, client devices shall wirelessly associate with access point device that has already joined DH-PFM888S-AC.

- Step 1 Open IP address page of the client device to modify its IP address. For example, modify it to 192.168.2.37. Gateway is upper router LAN address of wireless associated access point device. In the example, gateway is set to be 192.168.2.254.
- Step 2 Open wireless setting page of the client device, choose the access point whose SSID is DaHua; default encryption is WPA2-PSK (secret key is 1234567890abc).

Basic Wireless Settings

Wireless Mode(1): Station ▾

SSID: DaHua Select

Frequency Scan List(1): ☐ Enable

Output Power: 27 High

802.11n Mode: Auto mode ▾

Country Code: China (Continent: Asia) Select

Channel Width(1): 40MHz ▾

Max TX Rate, Mode(1): 802.11n ▾

Lock AP Mac:

Wireless Security Settings

Security: WPA ▾

Mode: WPA2 ▾

Cipher: CCMP ▾

Authentication/Mode: PSK ▾

WPA Key: Show

Change

Figure 3-9

Step 3 At AC management page of client device, enable AC control function.

Controller Management

Controller:

WLAN Name: WLAN Location:

Add IP Type:

IP Address		Assign
Add IP:	<input type="text" value="100.108.1.100"/>	<input type="button" value="Add"/>
IP:	<input type="text" value="192.168.1.20"/>	<input type="button" value="Edit"/> <input type="button" value="Del"/>
IP:	<input type="text" value="192.168.1.100"/>	<input type="button" value="Edit"/> <input type="button" value="Del"/>

Figure 3-10

Up to now, setting of access point and client has been completed, ready to join DH-PFM888S-AC. Please check at DH-PFM888S-AC page.

4 Functional Introduction

4.1 Login

Precondition

- Please ensure that PC has been connected with LAN interface or management interface of DH-PFM888S-AC.
- IP address of PC and that of the device are in the same network segment. Please refer to Table 4-1 for IP planning.

Connection Mode	Default IP Address of Device	Planned IP Address of PC
Connection of PC and device management interface	<ul style="list-style-type: none">• IP address: 192.168.3.100• Subnet mask: 255.255.255.0	<ul style="list-style-type: none">• IP address: 192.168.3.145• Subnet mask: 255.255.255.0
Connection of PC and device LAN interface	<ul style="list-style-type: none">• IP address: 192.168.1.100• Subnet mask: 255.255.255.0	<ul style="list-style-type: none">• IP address: 192.168.1.145• Subnet mask: 255.255.255.0

Table 4-1

Operating Steps

- Step 1 Input DH-PFM888S-AC platform address in the browser, and press [Enter] key.
The system displays login interface, as shown in Figure 4-1.



Figure 4-1

- Step 2 Input username and password; click “Login”.



Default username is “root” and password is “admin”. It is suggested that a password

with high security should be set and modified regularly.

4.2 State Statistics

State statistics page is mainly used to display basic info about DH-PFM888S-AC, device and terminal state, as shown in Figure 4-2.



Figure 4-2

For meanings of every column, please refer to Table 4-2.

Parameter		Description
Basic Info	IP Address	IP address of LAN port of device
	Device Name	Device name. Select "System Setup > Basic Setup" to modify it.
	Soft Version	Software version of present device
	Available Memory	Available memory of the device at present.
	Run Time	Run time of device server
	CPU Usage	CPU usage rate of device
	Memory Usage	Memory usage rate of device
Device State	Online Device	Total number of online access points and client devices that are connected with device
	Offline Device	Total number of offline access points and client devices that are connected with device
Terminal State	Online Device	Total number of terminals (such as mobile phone, computer and pad etc.) of online access point devices, with wireless association with device

Parameter		Description
	Offline Device	Total number of terminals (such as mobile phone, computer and pad etc.) of online access point devices, without wireless association with device

Table 4-2

4.3 Device Management

4.3.1 Device List

Device list page displays info about all online/offline access point devices of DH-PFM888S-AC, as well as client devices under access point devices, as is shown in Figure 4-3 and Figure 4-4.



Figure 4-3



Figure 4-4

Parameter	Description
State	Display current state of the device, including online, offline, not configured, upgrade, configuring, upgrade fails and configuration fails.
Device	Name of access point or client device.
Model	Product model of access point or client device.
IP Address	IP address of access point or client device.



Parameter	Description
MAC Address	Wired MAC address of access point or client device.
Soft. Version	Software version of access point or client device.
Run Time	Run time after access point or client device goes online.
Group	Group name of access point device. On the right of the list, select “More > Edit” to modify configuration info.
Template	Template name simultaneously issued to access point and associated client. Configure the template in “Advanced > Template”.
Wireless Service	Radio frequency switch of access point device. If it is turned off, radio frequency of access point device will be turned off, subordinate client device will disconnect and go offline. It will enter client retrieval mode after 10 minutes.
Wireless Mode	Click “Display” on the right of access point or client, to display “Wireless Mode” column. <ul style="list-style-type: none"> Wireless mode of access point includes AP and AP+WDS. Wireless mode of client includes STA and STA+WDS.
Location	Location of access point or client
	Click  in the left of access point; display info about client device under access point device, including state, device name, IP address, MAC address, software version, run time, signal intensity, connection rate and location. Connection rate means sending and receiving rate of client device. Signal intensity means signal intensity of client device during connection with access point device.

Table 4-3

4.3.2 Delete Device

- To delete offline access point or client, select “More > Delete” after the device, to delete it.
- In case that many offline devices shall be deleted, click “Delete Offline Device” button directly, to delete all offline devices at the same time.



Caution

Only offline devices can be deleted. If there are clients under the offline access point device, delete the offline clients first, and then delete offline access point device.

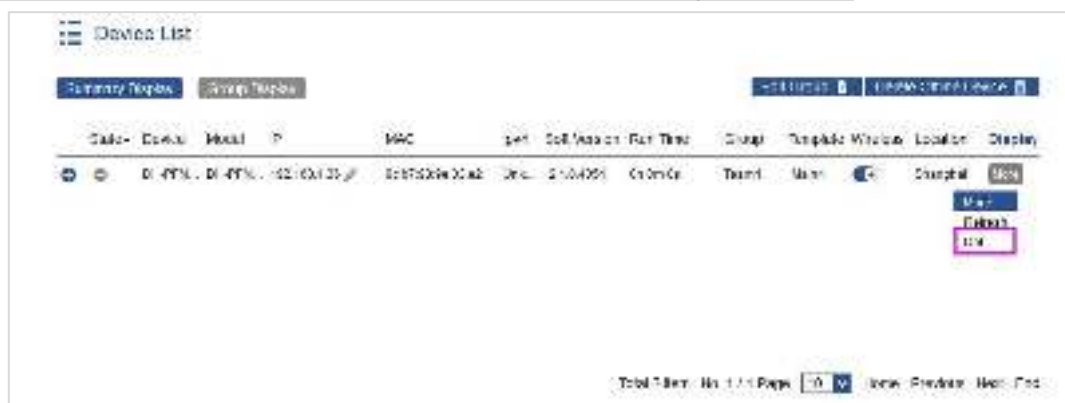


Figure 4-5

4.3.3 Edit Group

This part mainly introduces how to edit groups in batches and multiple levels.

Step 1 Click “”.

The system displays “Edit Group” interface, as shown in Figure 4-6.



Figure 4-6

Step 2 Click “New”, fill in name of root directory, such as “All”. Then, click “Finish”.
On completion, the interface is shown as Figure 4-7.

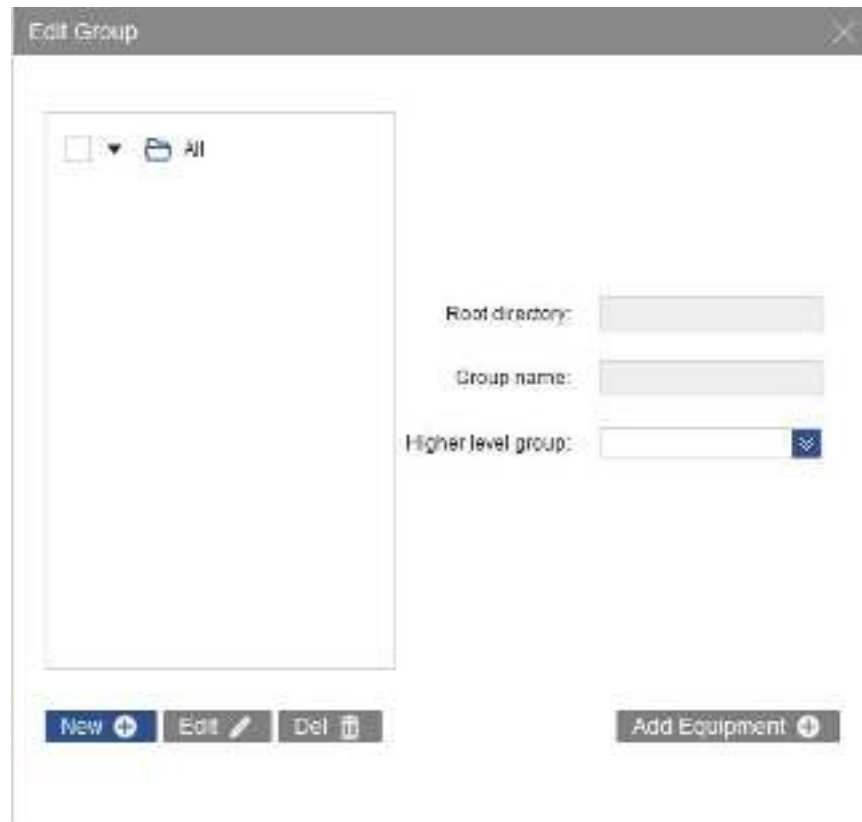


Figure 4-7

Step 3 Click “New” button again, fill in group name, choose higher level group, and click “Finish”.

Create multi-level group by reference to this step. The interface is shown in Figure 4-8.

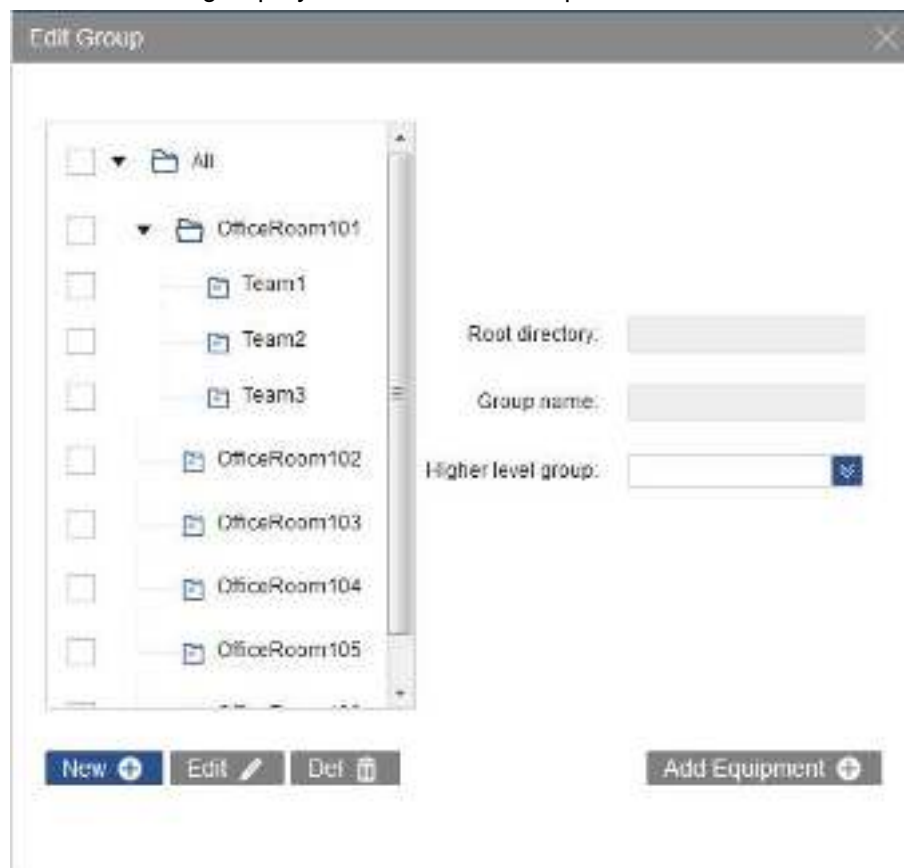


Figure 4-8

Step 4 Choose one group, click “Add Device”, and thus add devices to this group in batches.

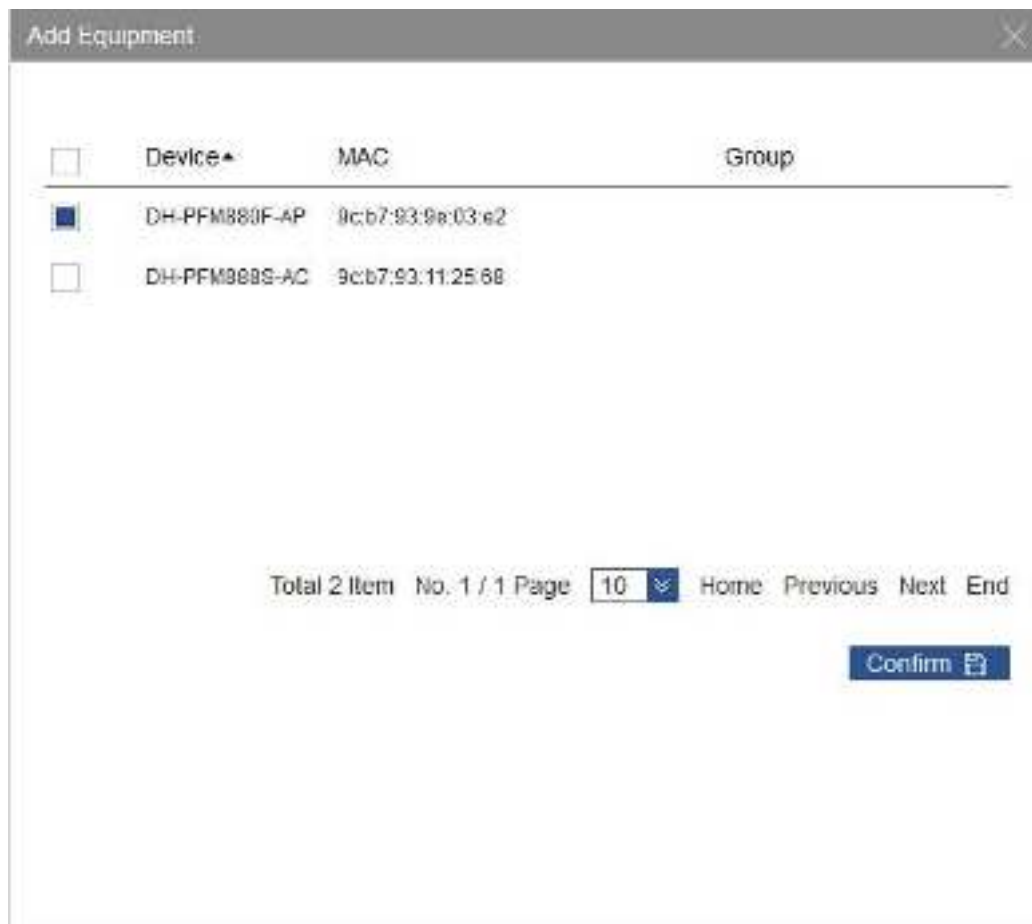


Figure 4-9

4.3.4 Issue Template

In the interface of device list, the added template can be issued to designated access point and client devices. Please refer to “4.5.1 Template Management” for details.



Device with state means that the device is not configured.

Step 1 Select “More > Edit” in the list of access point to be configured.

Step 2 Select the created template in template name.

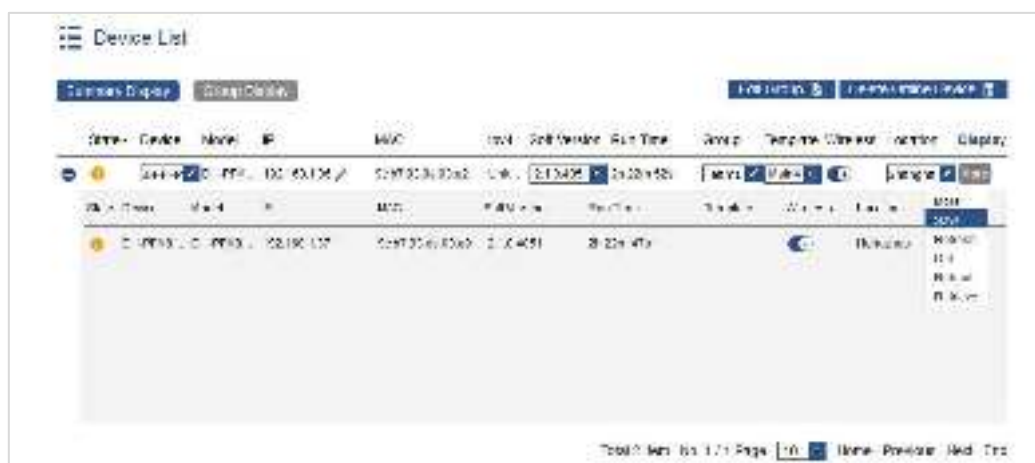



Figure 4-10

Step 3 After editing, select “More > Save”.

After issuing configuration, the state before device list changes into .



- If access point device owns client(s), client(s) will be issued at the same time. On DH-PFM888S-AC, templates cannot be directly issued to client(s). When the connected access point changes its configuration, the client will adapt to parameters of access point, so as to maintain normal communication with access point.

State	Device	Model	IP	MAC	IPv4	Soft Version	Run Time	Group	Template	Wireless	Location	Display
		DH-PFM888S-AC	192.168.1.25	98-73-23-2a-33-a2	192.168.1.25	2.1.0.4051	4h2m13s	Default	None		Shanghai	

Figure 4-11

When the mouse moves to “Wireless Service” in device list, display the template info of this device, including device type, country, mode, transmitting power, channel, band width and SSID.

State	Device	Model	IP	MAC	IPv4	Soft Version	Run Time	Group	Template	Wireless	Location	Display
		DH-PFM888S-AC	192.168.1.25	98-73-23-2a-33-a2	192.168.1.25	2.1.0.4051	4h2m13s	Default	None		Shanghai	

Figure 4-12

4.3.5 Device Upgrade

In the page of device list, device software can be upgraded. Upgrade method of terminal device is the same as that of access point. Take the upgrade of access point for example.

Precondition

New version file has been uploaded.

In the navigation bar, select “Advanced > Image” and upload the latest version file. Please refer to “4.5.2 Image Management” for details.

Operating Step

Step 1 In the list of access point to be upgraded, select “More > Edit”.

In pull-down list of upgrade version of every device, only versions of the same model of device will be displayed.






Figure 4-13

Step 2 In “Soft. Version”, select the desired version.

Step 3 After editing, select “More > Save” to start upgrade.



- The state changes into upgrading . The device disconnects  during upgrade. Its state becomes online  after upgrade, which means that upgrade has been successful
- If the selected version in device list is the current version of device, it won't be upgraded.

4.3.6 Retrieve the Client

Due to features of wireless transmission, client device may sometimes subject to unsuccessful configuration, and may fail to associate access point. At the time, associate the client again through client retrieval function of access point.



Caution

Only those clients that have been successfully associated with access point can be retrieved.

Step 1 In case that the client fails to associate with corresponding access point for more than 10 minutes, please select “More > Retrieve” on the right of access point.

The interface is shown in Figure 4-14.



Figure 4-14

Step 2 Wait for 5 minutes. All clients once associated with access point will be associated again. Meanwhile, wireless template of access point will be changed to null. The interface is shown in Figure 4-15.



Figure 4-15

Step 3 Select template name again and save.

4.4 Terminal Management

4.4.1 Terminal List

When mobile phones, notebooks and other terminals are connected with access point device, view detailed info about all terminals in terminal management list. The interface is shown in Figure 4-16. Please refer to Table 4-4 and Table 4-5 for operating descriptions.



Figure 4-16

Parameter	Description
State	Current state of terminal device, including online and offline.
IP Address	IP address of terminal device
MAC Address	Wireless MAC address of terminal device
Terminal	Reported terminal types after terminal device is associated with access point. Including UNKNOWN, Windows, Windows Phone, Android, iPhone, iPod, iPad and Macintosh.
Signal	Wireless signal intensity associated with terminal device

Parameter	Description
Wireless Mode	Wireless mode of access point associated with terminal
Rate	Connection rate of access point associated with terminal
SSID	SSID of access point associated with terminal
User	User name used by terminal for Web authentication
Flow	Upstream and downstream flow rate used by terminal after associated with access point
Run Time	Run time after terminal is associated with access point
Group	Group name of terminal. On the right of the list, select "More > Edit" to configure group name.
Connected AP	Name of access point device associated with terminal.
AP MAC	MAC address of the access point associated with terminal device.

Table 4-4











Operation	Description
 Details	Click "Details"  to display login time, offline time and registration time of the terminal; registration time means the time when the terminal carries out Web authentication, registration and going online.
 Delete	Click "Delete"  to delete offline terminals, whereas online terminals cannot be deleted.
 Edit	Click "Edit"  to add or edit group name of terminal.
 Offline	Click "Offline"  , terminals that have gone through Web authentication will be forced to go offline; terminals that haven't gone through Web authentication cannot go offline.
 Edit Group	Divide all terminals into groups. Please refer to "4.3.3 Edit Group".
 Group Display	Display terminal info in groups.

Table 4-5

4.4.2 Info Statistics

In the page of info statistics, view the online terminal type, online user group and time sharing info.

Information Statistics



Figure 4-17

- Display "Online Terminal Type" and "Online User Group" according to "Terminal Type" in terminal list and the edited "Group Name".

Information Statistics



Figure 4-18

- In the icon box of time sharing info, display the number of online users, number of registered users, upstream flow and downstream flow. Click the button to view data of today, yesterday, the last seven days and this month.
- Click to hide the data. Meanwhile, the icon turns gray.

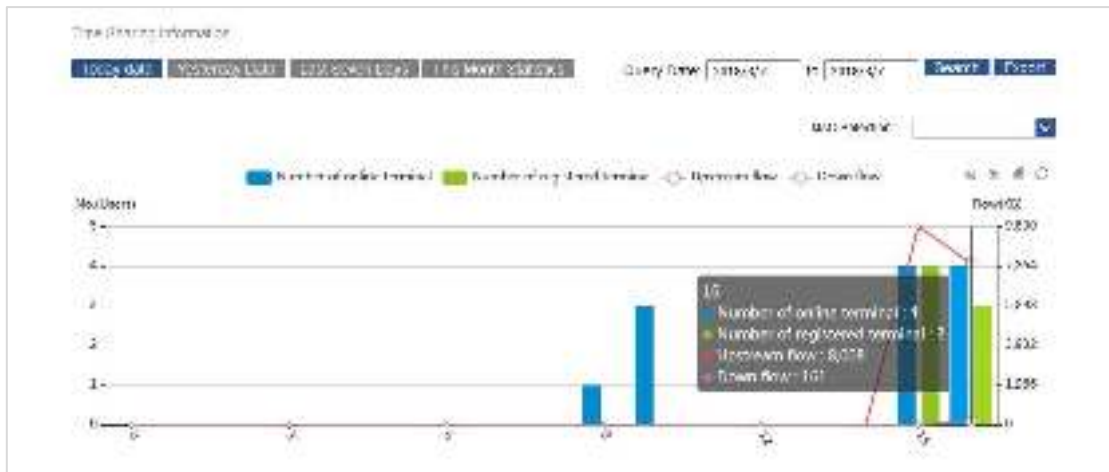


Figure 4-19

- Click "Download" to download the figure of present time sharing info.
- Click "Line Chart" or "Bar Chart" to modify display mode. Click "Restore" to restore display mode to default state.

In Figure 4-20, the data is displayed with bar chart.



Figure 4-20

- In "Query Date" column, click to choose starting date and ending date, query statistical info within a time period.

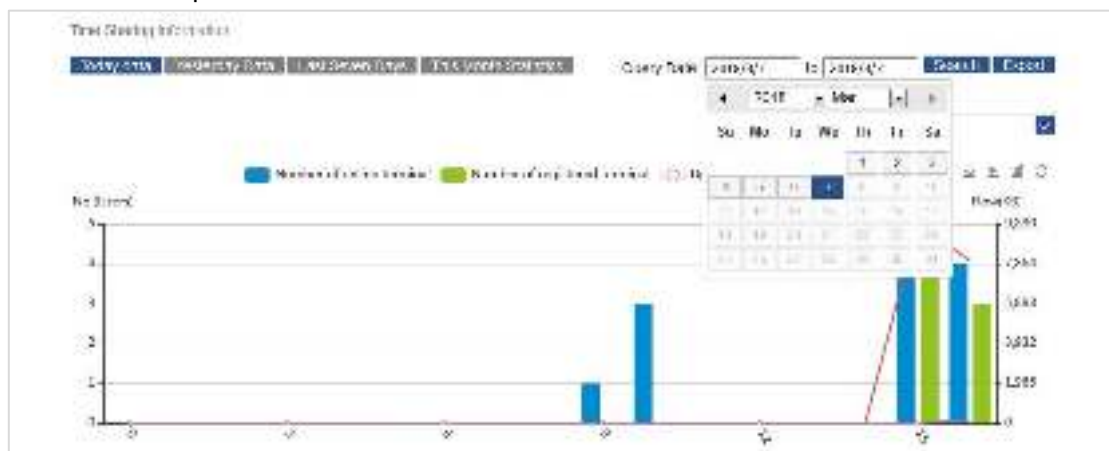


Figure 4-21

- Click "Export" button to export the selected data info in the format of Excel, as shown in Figure 4-22.

Time	Number of online users	Number of registered users	Up flow	Down flow
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	1	0	0	0
10	3	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	4	4	9028	0
16	4	3	8008	181

Figure 4-22

- Click MAC drop-down box to view time sharing info of every terminal according to MAC address, as shown in Figure 4-23.

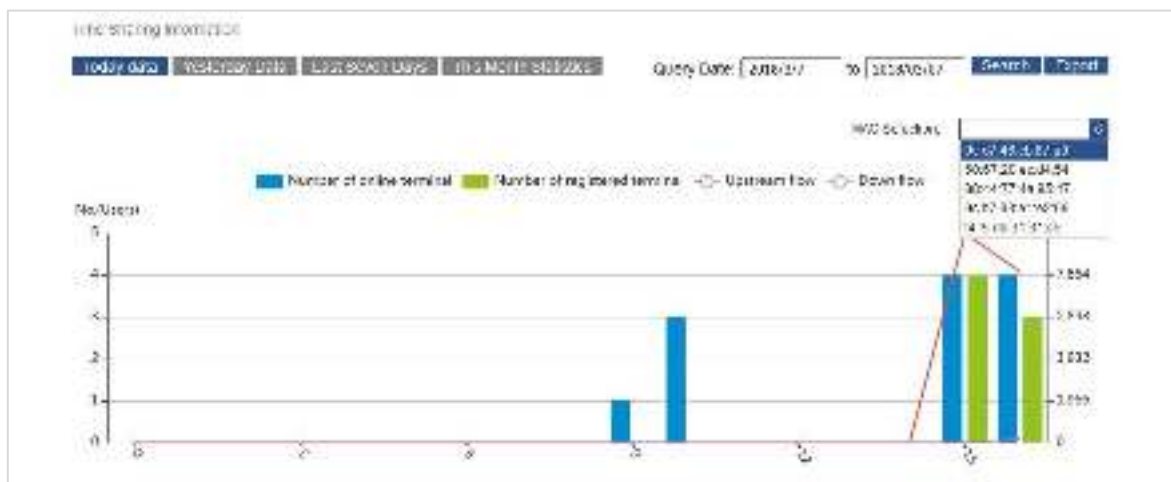


Figure 4-23

4.5 Advanced Management

4.5.1 Template Management

Template management page manages main template, basic template and VAP template.

For the first time, create basic template and VAP template first, and then the main template is able to associate with the created basic template and VAP template.

4.5.1.1 VAP Template

New



At most 128 VAP templates can be created.

Step 1 In the navigation bar, select “Advanced > Template”.

Step 2 Click “VAP Template” tab and click “New”.

Step 3 Fill in relevant info according to the user’s actual needs.


The interface is shown in Figure 4-24. Please refer to Table 4-6 for parameter descriptions.

The screenshot shows a web-based configuration interface for a new VAP template. The interface is titled "New" at the top. It contains various configuration options organized into sections. Key parameters include:

- Name:** A text input field.
- VAP Enable:** A checkbox labeled "Enable".
- SSID:** A text input field.
- Max Terminals:** A slider and a text input field set to "20".
- STA Isolation:** A checkbox labeled "Enable".
- SSID Hide:** A checkbox labeled "Enable".
- Encryption Type:** A dropdown menu showing "WPA Encryption".
- Authentication Type:** A dropdown menu showing "WPA-TKIP".
- Password:** A text input field with a toggle for visibility.
- User Speed Limit:** A checkbox labeled "Enable".
- Authentication Mode:** Three checkboxes for "Web Authentication", "WeChat Authentication", and "SMS Authentication", all of which are checked.
- Preferred Authentication Mode:** Three radio buttons for "Web Authentication", "WeChat Authentication", and "SMS Authentication", with "SMS Authentication" selected.
- WeChat Public Number:** A text input field.
- WeChat Public Appid:** A text input field.
- WeChat Connection WIFI ShopID:** A text input field.
- WeChat Connection WIFI SecretKey:** A text input field.
- Focus On Public No. To Unlimited Internet Access:** A checkbox labeled "Enable".
- WeChat Public Number Of Appsecret:** A text input field.
- SMS Account ID:** A text input field.
- Apply ID:** A text input field.
- Template ID:** A text input field.
- SMS Account Key:** A text input field with a toggle for visibility.
- Restrictive Options:** Two radio buttons for "Account Control" and "MAC Control".
- Universal Internet Length:** A checkbox labeled "Enable", followed by a text input field, the unit "Seconds", and a dropdown menu for "Unit".
- Flow Control:** A checkbox labeled "Enable", followed by a text input field, the unit "MB", and a dropdown menu for "Unit".
- Time Control:** A dropdown menu.
- Post-Certification Behavior:** Two radio buttons for "Jump to the specified page" and "Jump request page".
- Jump Specifies the URL:** A text input field.

Figure 4-24

Parameter	Description
Name	Name of this VAP template. The name can be 1 ~ 63 non-null characters, including number, letter or Chinese character.

Parameter	Description
VAP Enable	Choose to enable or disable this VAP. When it is enabled, the terminal can scan and connect with this VAP.
SSID	Name of wireless network.
Max Terminals	By setting it, limit the quantity of terminals that are connected with access point.
STA Isolation	By enabling this function, devices connected with the same access point cannot communicate with each other. Even IP of STA is repeated, it will not exert any effects on communication.
SSID Hide	Hide the name of wireless network (SSID). After this function is enabled, it will not be searched by clients, so as not to be connected by others and affect your own use.
Encryption Type	Encrypt the wireless connection. The user can choose corresponding encryption type according to security requirements. Wireless encryption of terminals to be associated shall be set as the same; otherwise, they cannot be associated.
WPA	As a standard interoperable WLAN security enhancement solution, WPA greatly increases data protection and access control level in the existing and future wireless local area network (WLAN).  Note When WPA-PSK (TKIP) and WPA2-PSK (TKIP) are used to encrypt, the product will only reach 802.11a/g handling capacity.
Authentication Mode	It consists of Web authentication, WeChat authentication and SMS authentication. Please refer to “4.6.3 Access Control” for details.
Preferred Authentication Mode	It consists of Web authentication, WeChat authentication and SMS authentication. After selecting the authentication mode, the terminal will jump to preferred authentication mode.
WeChat Public Number	WeChat Public Number used during WeChat authentication.
WeChat Public Appid, WeChat Connection WIFI ShopID, and WeChat Connection WIFI SecretKey	AppID, ShopID and secretKey of corresponding WeChat public number. Fill in them when WeChat authentication is selected.
Focus on Public No. to Unlimited Internet Access	After SMS authentication, it prompts whether you want to subscribe WeChat public number. After subscription, the terminal won't be limited by Internet length, but can go online all the time. It is configured when WeChat authentication is selected.
WeChat Public Number appsecret	Appsecret of corresponding WeChat public number. Fill in it when WeChat authentication is selected.
SMS Account ID	Account Sid of SMS authentication platform.
App ID	App Id of SMS authentication platform.
Template ID	Template ID of SMS authentication platform.
SMS Account Key	Auth token of SMS authentication platform.


Parameter	Description
Universal Internet Length	Internet time length allowed after authentication.  Note The terminal is not subject to length limit after enabling “Focus on Public No. to Unlimited Internet Access”.
Flow Control	Allowed traffic flow after authentication. The unit is day and month.
Time Control	Allowed time to surf the Internet after authentication.
Post-certification Behavior	Jump to the specified page and jump to the requested page. <ul style="list-style-type: none"> By ticking “Jump to the specified page”, jump to the specified URL after authentication. Fill in the specified URL first. When advertisement and authentication mode is enabled at the same time, advertisement image will jump out after authentication. No matter whether the image has a link, neglect the image link and jump to the specified URL. <ul style="list-style-type: none"> By ticking “Jump to the requested page”, after authentication, jump to the page requested by the user. When advertisement and authentication mode is enabled at the same time, advertisement image will jump out after authentication. If the clicked image has a link, jump to the linked page. Otherwise, jump to the page requested by the user.
Jump to Specified URL	It is used if post-authentication behavior is “Jump to the specified page”.

Table 4-6

Step 4 Click “Finish”.

The system displays “Summary Display” interface, as shown in Figure 4-25.



Figure 4-25

Other Operations

- Select the template; click “Edit” to edit the VAP template.
- Select the template; click “Del” to delete it. Multiple templates can be selected and deleted together, but the template under use cannot be deleted.
- Click title bar to rank them.

4.5.1.2 Basic Template

New



128 basic templates can be created at most.

- Step 1 In the navigation bar, select “Advanced > Template”.
- Step 2 Click “Basic Template” and then click “New”.
- Step 3 Fill in relevant info according to needs. The interface is shown in Figure 4-26. Please refer to Table 4-7 for parameter descriptions.

Figure 4-26

Parameter	Description
Mode	It consists of 2.4G-802.11n, 5G-802.11n and 5G-11ac. Choose corresponding mode according to the product. In device list, identify the template consistent with device mode.
Country	Standard channel varies in different countries or regions, which is distinguished with country code. In “Test” mode, 2G frequency will expand to 2312MHz-2732MHz, whereas 5G frequency will expand to 4920MHz~6100MHz.
Name	Name of this template. The name can be 1 ~ 63 non-null characters, including number, letter or Chinese character (one Chinese character occupies 3 digits).
Device Type	It consists of AP and Bridge type. <ul style="list-style-type: none">With AP type, 8 VAP can be chosen in main template.With Bridge type, only one VAP can be chosen in main template.


Parameter	Description
Channel	Channel of info transmission.  Note Before using non-standard frequency band, please check whether it conforms to local laws and regulations, as well as wireless management rules. To use non-standard frequency band, please change the country to test mode.
Channel Width	It refers to maximum data transmission rate of the channel.
Maximum Sending Rate	Maximum sending and receiving rate of the device. By setting it, limit the maximum sending and receiving rate of the device, so as to keep stability of device performance.

Table 4-7

Display

- Click “Summary Display” to display the info of all templates, as shown in Figure 4-27.



Figure 4-27

- Click “Mode Display” to display basic templates according to mode, as shown in Figure 4-28.

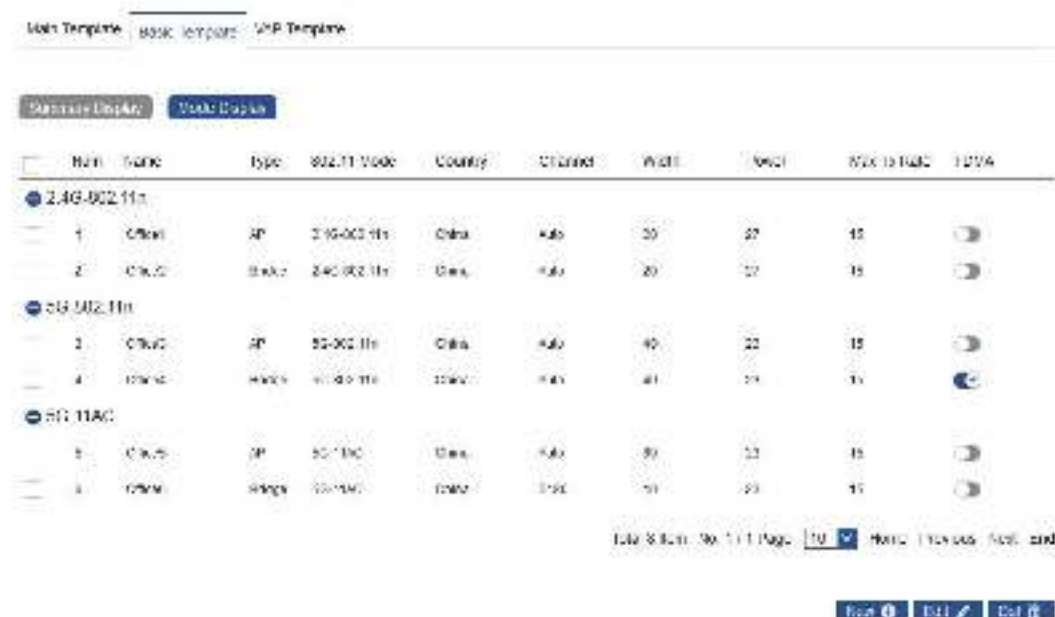


Figure 4-28

Other Operations

- Select the template; click “Edit” to edit the basic template.
- Select the template; click “Del” to delete it. Multiple templates can be selected and deleted together, but the template under use cannot be deleted.
- Click title bar to rank them.

4.5.1.3 Main Template

New



256 main templates can be created at most.

Step 1 In the navigation bar, select “Advanced > Template”.

Step 2 Click “Main Template” and then click “New”.



The name can be 1 ~ 63 non-null characters, including number, letter or Chinese character.

Step 3 Choose previously created basic template in drop-down box of basic template. After it is chosen, display the type and mode of this basic template automatically.

- When the type is AP, VAP1~VAP8 option box will appear, as shown in Figure 4-29.
- When the type is Bridge, only VAP1 choice box will appear, as shown in Figure 4-30.

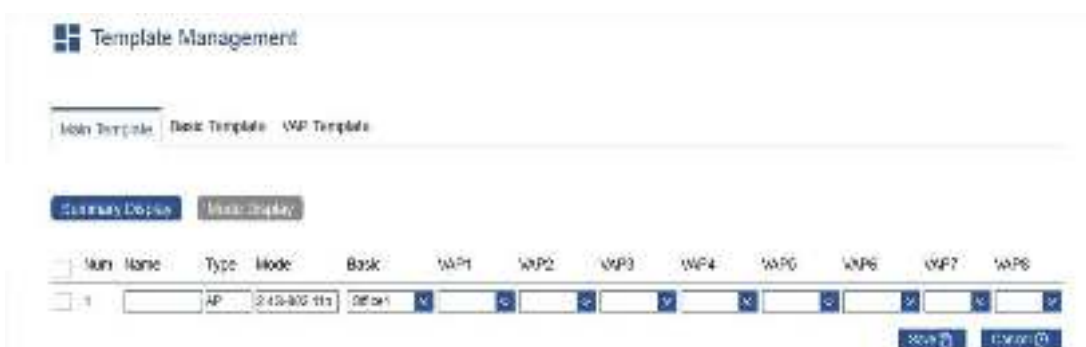


Figure 4-29



Figure 4-30

Display

- Click “Summary Display” to display the info of all basic templates.
- Click “Mode Display” to display main templates according to mode, as shown in Figure

4-31.

Name	Type	Mode	Radio	WPA1	WPA2	WPA3	WPA4	WPA5	WPA6	WPA7	WPA8
2.4G/5G/11n											
1	Main	W	2.4G/5G/11n	WPA1							
2	Main	WPA2	2.4G/5G/11n	WPA2							
5G/802.11n											
3	Main	W	5G/802.11n	WPA1	WPA2						
4	Main	WPA2	5G/802.11n	WPA2							
5G/11AC											
5	Main	W	5G/11AC	WPA2	WPA3	WPA8					
6	Main	WPA2	5G/11AC	WPA2							

Figure 4-31

Edit and Delete

- Select the template; click “Edit” to edit the main template.
- Select the template; click “Del” to delete it. Multiple templates can be selected and deleted together, but the template under use cannot be deleted.
- Click title bar to rank them.



- In case that modified wireless service configuration template has been applied to AP, modified configuration item will take effect on AP and associated client device immediately.
- In case that wireless service configuration template, which is planned to be deleted, has been applied to online device with DH-PFM888S-AC management, the template cannot be deleted.

4.5.2 Image Management

Image management is used to manage the software version, which can be upgraded manually or automatically through software in image management list.

View software program at “Advanced > Image Management” interface, as shown in Figure 4-32.

Figure 4-32

- Click “Manual Update” to select and update the selected devices that meet version requirements.
- Click “Upgrade All” to update all devices that meet version requirements.

Step 1 In the navigation bar, select “Advanced > Image Management”. The system displays “Image Management” interface.

1. Click "Select File" to select the file to be uploaded.
2. Click "Upload".

Product	Default Version	Auto Update	View
D-Link DSR-1000			
D-Link DSR-1000			
D-Link DSR-1000			
D-Link DSR-1000			

Step 4 Click  to save.

- When restarting the device, or restarting AC, or a new device joins AC, device upgrade will be completed automatically in accordance with version requirements.
- Click “Auto Upgrade” button again, and the button turns gray. Click “Save” to turn off automatic upgrade function.

4.5.2.2 Manual Update

Devices managed by DH-PFM888S-AC can be updated manually in two ways:

- Single device update: please refer to “4.3.5 Device Upgrade” for details.
- Multiple devices update: please refer to this section.

Step 1 In the navigation bar, select “Advanced > Image Management”.

The system displays “Image Management” interface.

Step 2 Upload image file.

1. Click “Select File” to select the file to be uploaded.
2. Click “Upload”.

Image List

File Name:

NO.	FILE NAME	VERSION	PRODUCT	FILE SIZE (KB)	UPLOAD TIME	ACTION
1	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
2	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
3	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
4	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
5	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
6	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
7	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>
8	TD421040310041_08-07-03_2.1.0.2681	2.1.0.2681	DH-PFM888S-AC	727.053 (94)	2016-01-26 22:52:02	<input type="button" value="Manual Update"/> <input type="button" value="Delete"/>

Figure 4-34

Step 3 In the image list, select “Manual Update” after the image file.

The system displays “Manual Update” interface, as shown in Figure 4-36.

Manual Update

<input type="checkbox"/>	State	Name	Model	MAC	Soft Version
<input checked="" type="checkbox"/>	✓	DH-PFM...	DH-PFM...	9c:b7:93:9e:03:e2	2.1.0.2681

Total 1 Item No. 1 / 1 Page

Figure 4-35

Step 4 Select the device which shall be upgraded, and click “Upgrade”.

View update status in “Device Update Status” interface, as shown in Figure 4-36.

- Search Alarm

Click “Alarm”, set the keyword, alarm module, alarm level or time frame, and click “Search” to search alarm info, as shown in Figure 4-38.

The screenshot shows the 'Log Management' interface with the 'Alarm' tab selected. The search section includes a 'Search' button and several filter fields: 'Key' (containing 'bin'), 'Alarm Module' (set to 'All'), 'Alarm Level' (set to 'All'), and 'Time Range' (set to 'All'). Below the filters, there is a table of search results with columns: 'Name', 'Module', 'Level', 'Content', and 'Time'.

Name	Module	Level	Content	Time
1	System	Normal	www.sony.jp/CD/Eat	2013-01-28 22:50:0
2	System	Normal	www.sony.jp/CD/Eat	2013-01-28 22:50:0
3	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
4	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
5	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
6	Web Service	Normal	login:00:00:00	2013-01-28 22:50:0
7	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
8	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
9	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0
10	System	Normal	authentication:PASSWD:00	2013-01-28 22:50:0

Figure 4-38

4.6 System Settings

Page of system settings includes basic settings, upgrade configuration management and access control. It is mainly used to manage the platform itself.

4.6.1 Basic Settings

4.6.1.1 General Settings

Set system properties at this interface, including host name and language.

Step 1 In the navigation bar, select “System Settings > Basic Settings”.

The system displays “General Settings” interface, as shown in Figure 4-39.



Figure 4-39

Parameter	Description
Host name	It is used to identify device host, to ensure its uniqueness in the network system. Host name consists of 1 ~ 63 non-null characters, including number, letter, Chinese character (one Chinese character occupies 3 digits) or special characters ("_", "~", "!", "@", "\$", "%", "^", ".", "*", and "-").
Language	Including Chinese and English.
Account Management	After ticking "Modify Login", input the old password, new password and confirm new password again.

Table 4-8

Step 2 Click "Save".

4.6.1.2 Time Synchronization

Set time synchronization between DH-PFM888S-AC and NTP server.

Step 1 In the navigation bar, select "System Settings > Basic Settings".

Step 2 Click "Time Sync" tab.

The system displays "Time Sync" interface, as shown in Figure 4-40.



Figure 4-40

Parameter	Description
Time Zone	Choose the stipulated time zone of your location.

Parameter	Description
Local Time	Display current system time of DH-PFM888S-AC.
NTP Client	Through network time protocol, DH-PFM888S-AC and time server realize time synchronization. After this function is enabled, please fill in address of proper time server according to needs, such as 118.103.146.184. At this time, LAN port of DH-PFM888S-AC shall be connected to public network, and configured with correct IP address and gateway.
NTP Server IP	IP address of designated NTP server.
NTP Server	Through network time protocol, network access point/client and DH-PFM888S-AC realize time synchronization.
Time Settings	System time is a very important parameter of DH-PFM888S-AC system, because NTP service of AP/STA, DHCP lease and system log need to use system time. It is suggested that time settings should be modified according to needs when logging in DH-PFM888S-AC for the first time.

Table 4-9

Step 3 Click “Save”.

4.6.1.3 Interface Settings

Set the interface of the device.

Step 1 In the navigation bar, select “System Settings > Basic Settings”.

Step 2 Click “Interface Settings” tab.

The system displays “Interface Settings” interface, as shown in Figure 4-41.



Figure 4-41

Parameter	Description
Network Mode	Select “Route Mode” or “Bridge Mode” according to needs.

Parameter	Description
WAN Interface	Default IP address of WAN interface is 192.168.3.100. PC connects management interface and visits the network management interface of the device through the browser.
LAN Interface	<ul style="list-style-type: none"> PC connects LAN interface, and visits the network management interface of the device through the browser. Access point device connects LAN interface, and then goes on line. Default IP address of LAN port is 192.168.1.100.

Table 4-10

Step 3 Click "Save".

4.6.2 Upgrade Configuration Management

At upgrade configuration management interface, backup or restore configuration file, restore factory settings and reboot the device. Please operate according to actual conditions.

In the navigation bar, select "System Settings > Upgrade Configuration Management". The system displays "Upgrade Configuration Management" interface, as shown in Figure 4-42.



Figure 4-42

Backup/Restore

- **Download Profile:** it saves current configuration of DH-PFM888S-AC, with default file name as config.db, in order to backup DH-PFM888S-AC configurations.
- **Upload Configuration:** upload config.db file to configure DH-PFM888S-AC. Click “Select File”, select “config.db”, and then click “Upload”. If image file on DH-PFM888S-AC server is inconsistent with image file info in the uploaded configuration file, at the end of waiting page, there will be hints to delete info.
- **Save Configuration:** click “Save” to save all operations on the page, so as not to lose configurations in case of shutdown or outage.
- **Restore Factory:** restore initial values of DH-PFM888S-AC.



“Restore Factory” will restore all configuration info to factory default values. Please be careful!

- **Device Reboot:** click “Reboot”, and DH-PFM888S-AC will be rebooted.



Please save configurations before reboot; otherwise, all configurations will be lost after DH-PFM888S-AC reboot.

- **All AP Reboots:** click “Reboot”, and all online AP will be rebooted.

Update

Update the latest firmware info of the device.

Step 1 Click “Select File” and select the latest firmware of the device.

Step 2 Click “Update” to update the device.

License

View the greatest number of AP managed by the device and number of Web authentication users.

- **Device Identification:** Generate the license.
- **AP Number:** the greatest number of AP to be managed by DH-PFM888S-AC.
- **Web Authentication User Number:** the greatest number of Web authentication user.
- **File Upload:** it is unnecessary to upload the license.
- **USB Automatic Import:** it is unnecessary to import the license.

4.6.3 Access Control

Access control is used to configure relevant parameters of authentication. After authentication is enabled, authentication system will redirect the client to authentication login interface. The user operates according to self-defined authentication mode. Authentication system will show successful login interface, and redirect to the designated URL.

4.6.3.1 Enable Web Authentication

After Web authentication is enabled, Web authentication system will redirect the client to authentication login interface. The user inputs valid username and password, and then submits. Web authentication system will show successful login interface, and redirect authenticated client to the designated URL.

Step 1 Enable Web authentication.

1. In the navigation bar, select “Advanced > Template Management”.
2. Click “VAP Template”.
3. Create VAP template or modify existing template, and enable Web authentication, as shown in Figure 4-43.

The screenshot shows a configuration window titled "Edit" for a VAP template named "VAP1". The settings are as follows:

- Name: VAP1
- VAP Enable: ☒ Enable
- SSID: Test1
- Max Terminals: 20
- STA Isolation: ☐ Enable
- SSID Hide: ☐ Enable
- Encryption Type: WPA Encryption
- Authentication Type: WPA-PSK
- Password: [masked]
- User Speed Limit: ☐ Enable
- Authentication Mode: ☒ Web Authentication, ☐ WeChat Authentication, ☐ SMS Authentication
- Preferred Authentication Mode: ☒ Web Authentication, ☐ WeChat Authentication, ☐ SMS Authentication
- Restrictive Options: ☒ Account Control, ☐ MAC Control
- Universal Internet Length: ☐ Enable, Seconds: [blank], Unit: [blank]
- Flow Control: ☐ Enable, MB: [blank], Unit: [blank]
- Time Control: [blank]
- Post-Certification Behavior: ☒ Jump to the specified page, ☐ Jump request page
- Jump Specifies the URL: [blank]

Buttons at the bottom right: Cancel, Finish.

Figure 4-43

4. Click “Finish”.

Step 2 In the navigation bar, select “System Settings > Access Control”.

Step 3 Configure Portal parameters and click “Save”.

Portal setting interface is shown in Figure 4-44. Please refer to Table 4-11 for parameter descriptions.

Figure 4-44

Parameter	Description
Portal Selection	Choose internal or external Portal.
URL	<ul style="list-style-type: none"> In case of external Portal, set external Portal server address, and ensure connection of LAN interface of DH-PFM888S-AC and Portal server. In case of internal Portal, Portal server is DH-PFM888S-AC itself.
Accounting Interval	During billing, billing server makes statistics of billing info about wireless client at set intervals.
Idle Time	If there is no operation within stipulated time, the user will be required to re-authenticate.
Secret Key	It shall be set in case that external Portal is selected and its protocol standard is V 2.0.
Exemption Authentication	After this function is enabled, some terminals can be set to exempt from authentication and can communicate directly. MAC addresses of terminals shall be added to the list of exemption from authentication.

Table 4-11

Step 4 Click “Radius” tab to configure Radius parameters and click “Save”.

“Radius” interface is shown in Figure 4-45. Please refer to Table 4-12 for parameter descriptions.

Figure 4-45

Parameter	Description
External Radius	<ul style="list-style-type: none"> Fill in Radius authentication and host info. Secret key is the shared key set on Radius server. Make sure that LAN port of DH-PFM888S-AC is connected with Radius server.
Internal Radius	Built-in Radius of DH-PFM888S-AC will be used to authenticate. That is to say, Radius server is DH-PFM888S-AC itself

Table 4-12

Step 5 Click “ACL Control Rules” tab to configure parameters.

- Click “New”.
- Add IP address and port of Portal server.
 - ◇ In case of internal Portal, add IP and 80 port of DH-PFM888S-AC.
 - ◇ In case of external Portal, add IP and corresponding http port (such as 80 or 8080) of Portal server.
- Click “Finish”.



Note

- Portal usually has multiple IP addresses, so it shall not be blocked with black list.
- Don't build a white list and black list for the same IP and corresponding port simultaneously.

Figure 4-46

Step 6 Click “Rule Configuration” tab to configure parameters and click “Save”.

Enable pre-authentication access control white list, and add the previous rules to white list, as shown in Figure 4-47. Please refer to Table 4-13 for parameter description.

Figure 4-47

Type	Parameter	Description
Pre Authentication Access Control	Pre Authentication Access Control	Set the access right before wireless terminal passes Web authentication.
	White List	Select the rule that has been added to “ACL Control Rules”.
Access Control	Access Control	It controls access right of terminals that have passed WEB authentication.
	Terminal MAC	Select rules that have been set at “ACL Control Rules” interface, and fill in MAC address to be controlled. This MAC address will take effect according to rules.
	WEB Authentication Account	<ul style="list-style-type: none"> In case of internal Radius, fill in account of account management page; choose rules that have been set at “ACL Control Rules” interface. Terminals that are logged in with this WEB authentication account will take effect according to rules. In case of external Radius, fill in the account on Radius server; choose rules that have been set at “ACL Control Rules” interface. Terminals that are logged in with this WEB authentication account will take effect according to rules.

Type	Parameter	Description
	SSID	Fill in SSID to be controlled; select rules that have been set at “ACL Control Rules” interface. Terminals associated with this SSID wirelessly will take effect according to rules.

Table 4-13

Step 7 Click “Authentication Account” tab to configure parameters.

- In case of internal Radius, terminals shall fill in account and password of this interface to be authenticated.
- In case of external Radius, terminals shall fill in account and password configured on Radius server

ID	Name	Account	Password	Mail
1	Web	admin	*****	1000000000
2	Web	admin	*****	1000000000

Figure 4-48

Step 8 Click “Authentication Statistics” tab to display details about the authenticated terminals. Click “Details Export” to export details about the authenticated terminals.

ID	IP	MAC	Terminal	Type	Risk	Access Time	Offline Time	Offline Reason	AP Name	AP MAC	AP Location
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai

Figure 4-49

ID	IP	MAC	Terminal	Type	Risk	Access Time	Offline Time	Offline Reason	AP Name	AP MAC	AP Location
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai
Web	192.168.20.100	00:0C:29:00:00:00	Android	Web	Low	2018-02-06 10:00:00	2018-02-06 10:00:00	Offline	Web	00:0C:29:00:00:00	Shanghai

Figure 4-50

Step 9 Click “Internet Time Control” tab to configure parameters.

Prohibit internet access according to week, day and week/day.



Figure 4-51



Figure 4-52

Step 10 Access point device issues template to enable Web authentication.

Step 11 Web authentication of wireless terminal.

1. Wireless terminal associates with SSID that has enabled Web authentication, and obtains IP address of public network.
2. Open the browser of terminal device, input any address and it will be forced to visit the address of Web authentication server.
3. Input the account and password (username and password of Radius server). Go online after passing authentication.

4.6.3.2 WeChat Authentication

Precondition

Before enabling WeChat authentication, ensure that the device has configured correct gateway and DNS, and it is able to access the internet.

Operating Step

- Step 1 VAP template issued by access point device shall enable WeChat authentication.
Enable WeChat authentication at “Advanced > Template > VAP Template”. Please refer to “4.5.1.1 VAP Template” for details.
- Step 2 In the navigation bar, select “System Settings > Access Control”.
- Step 3 Configure Portal parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 4 Click “ACL Control Rules” tab to configure parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 5 Click “Rule Configuration” tab to configure parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 6 Access point device issues template to enable WeChat authentication.
- Step 7 WeChat authentication of wireless terminal.
1. Wireless terminal associates with SSID that has enabled WeChat authentication, and obtains IP address of public network.
 2. Open the browser of terminal device, input any address and it will be forced to visit the address of WeChat authentication server.
 3. Click “Authenticate”, and the system jumps to WeChat interface.
Click “Subscribe Public Platform” to go online. The terminal is not subject to length limit after enabling “Subscribe Public Platform for Unlimited Internet Access”.


4.6.3.3 SMS authentication

- Step 1 VAP template issued by access point device shall enable SMS authentication.
Enable SMS authentication at “Advanced > Template > VAP Template”. Please refer to “4.5.1.1 VAP Template” for details.
- Step 2 Enable time synchronization.
In the navigation bar, select “System Settings > Basic Settings” and set time synchronization. Please refer to “4.6.1.2 Time Synchronization” for details.
- Step 3 Configure Portal parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 4 Click “ACL Control Rules” tab to configure parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 5 Click “Rule Configuration” tab to configure parameters. Please refer to “4.6.3.1 Enable Web Authentication” for details.
- Step 6 Access point device issues template to enable SMS authentication.
- Step 7 SMS authentication at mobile phone.
1. Mobile phone associates with SSID that has enabled SMS authentication.
 2. Visit any website, and it will jump to SMS authentication interface. Input mobile phone number to obtain verification code; input verification code and the terminal will be able to access the internet.

4.7 Map Mode

In map mode, all devices are displayed on the map. Import planar graphs of apartments, communities, malls and schools, and display the devices on planar graphs.

4.7.1 Online Map

When access point and client devices in the device list are  online, devices are displayed on the map normally, and they can be dragged and modified.

Configuration Step

Step 1 In the navigation bar, select “Map Mode > Online Map”.

Step 2 Edit the location of access point device.

1. Click “AP” and then click “Edit”.
2. Edit the AP name and device location.
 - ◇ AP device name is filled in according to your own needs.
 - ◇ Location shall be the address of the map.
3. Click “Save”.



Figure 4-53

Step 3 Edit client device location.

1. Click “STA” and then click “Edit”.
2. Edit the client device name and device location.
 - ◇ Client device name is filled in according to your own needs.
 - ◇ Location shall be the address of the map.
3. Click “Save”.



Figure 4-54

Configuration Result

- View configured device info on the map. AP and STA icons appear.
- Colored icon represents online device, whereas gray icon represents offline device.
- MAC address of the device is displayed on every icon.
- Green line between devices represents wireless connection at present; signal strength is equal or greater than -80dBm and it is relatively strong. Red line between devices represents wireless connection at present; signal strength is less than -80dBm, and it is relatively weak. Blue line between devices represents wired connection at present.
- Click the icon to view details, and edit the device name.



Figure 4-55

Other Operations

- Drag: if you are uncertain about specific address, drag online device icon to determine the location. For example, drag AP icon to Linjiang Park. Online device (whose configuration status is normal operation) supports drag operation, but offline device doesn't support.
- Delete offline device: click the right mouse button and select "Delete". After deletion, the device info won't appear in device list.

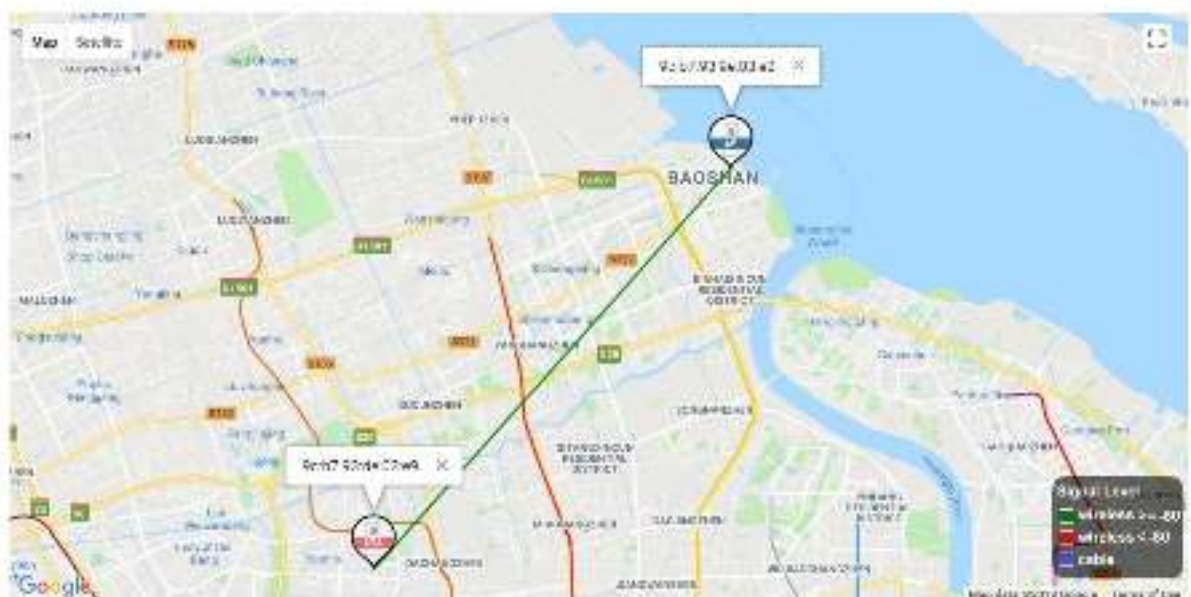


Figure 4-56

4.7.2 Offline Map

Step 1 Import offline map.

1. In the navigation bar, select “Map Mode > Map Management”.
2. Click “Offline Map” tab.
3. Click “Import” to import image info.



- Resolution ratio of uploaded image shall be larger than 600×600.
- Support “.png” and “.jpg” images.

Step 2 In the navigation bar, select “Map Mode > Offline Map”.

The system displays “Offline Map” interface, as shown in Figure 4-57.



Figure 4-57

Step 3 Click “Device Import” to select the device.



Figure 4-58

Step 4 Click “Confirm”, and the interface displays the added device.



Figure 4-59

4.7.3 Map Management

Online Map Management

Online map is “Baidu Map” by default, as shown in Figure 4-60.

- Map selection: online map selects “Baidu Map” by default.
- Center Point: modify longitude and latitude according to your needs, and determine center point.



Figure 4-60

Offline Map Management

The system supports to import offline map, such as planar graphs of apartments, communities, malls and schools, and display the devices on planar graphs.

Step 1 In the navigation bar, select “Map Mode > Map Management”.

Step 2 Click “Offline Map Management” tab.



Figure 4-61

Step 3 Click “Import” to select and import offline map.



- Resolution ratio of uploaded image shall be larger than 600×600.
- Support “.png” and “.jpg” images.

4.8 Marketing Management

Marketing management interface includes theme management and advertising management. It shall be used with Web authentication of access control interface (Please refer to “4.6.3.1 Enable Web Authentication” for details).

For the first time, upload advertising image to advertising management interface, and select

advertising theme at theme management interface. After selecting the theme, advertising image will be pushed when the terminal connects access point.

4.8.1 Advertising Management

Upload advertising image, which is imported by theme management interface.

Step 1 In the navigation bar, select “Marketing Management > Advertising Management”.

The system displays “Advertising Management” interface, as shown in Figure 4-62.



Figure 4-62

Step 2 Click “New”.

Step 3 Fill in advertising content and click “Finish”.

Figure 4-63

Parameter	Description
Ad Theme	It consists of theme 1 and theme 2. Create a theme at theme management interface, and select theme 1 or theme 2 image.

Parameter	Description
Ad Name	Ad image name. Ad name can be 1 ~ 63 non-null characters, including number, letter or Chinese character (one Chinese character occupies 3 digits).
Ad Position	The position of ad image on the terminal device. In theme 1, available position includes top image carousel and tail image. In theme 2, ad position is full screen image.
Ad Type	Ad type includes image ad and image ad link. <ul style="list-style-type: none"> Image ad: during ad authentication, click the image and go online directly to visit the requested website. Image ad link: during ad authentication, click the image and jump to the website link that is filled in here. For example, if image ad link is “www.baidu.com”, click the image ad and jump to the “www.baidu.com” website.
Ad Image	Image format: .png or .jpg. Recommended size: 768×1280 pixels for full screen image, 1000×600 pixels for top image carousel and 500×500 pixels for tail image.

Table 4-14

4.8.2 Theme Management

New

Step 1 In the navigation bar, select “Marketing Management > Theme Management”.

Step 2 Click “New”.

Step 3 Fill in theme name and click “Finish”.



Figure 4-64

Set Advertising

Theme 1 and theme 2 interfaces are shown in Figure 4-65.

Click **Select from the ad list** to select the ad.

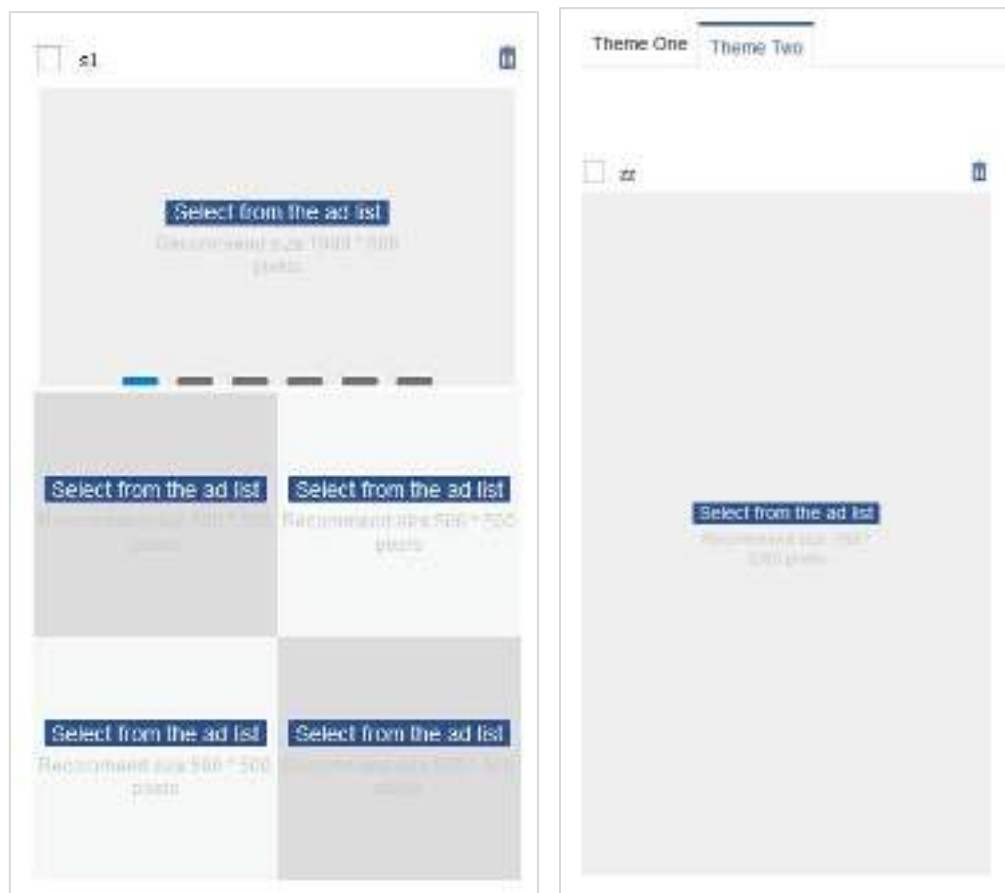



Figure 4-65



In theme 1, click  at top image carousel, in order to upload multiple images.

4.8.3 Advertising Statistics

Advertising statistics interface makes a statistics of the number of clicks of the advertising. View the data of today, yesterday, last seven days and this month; search according to date. The data can be exported with Excel.

In the navigation bar, select “Marketing Management > Advertising Statistics”. The system displays “Advertising Statistics” interface, as shown in Figure 4-66.

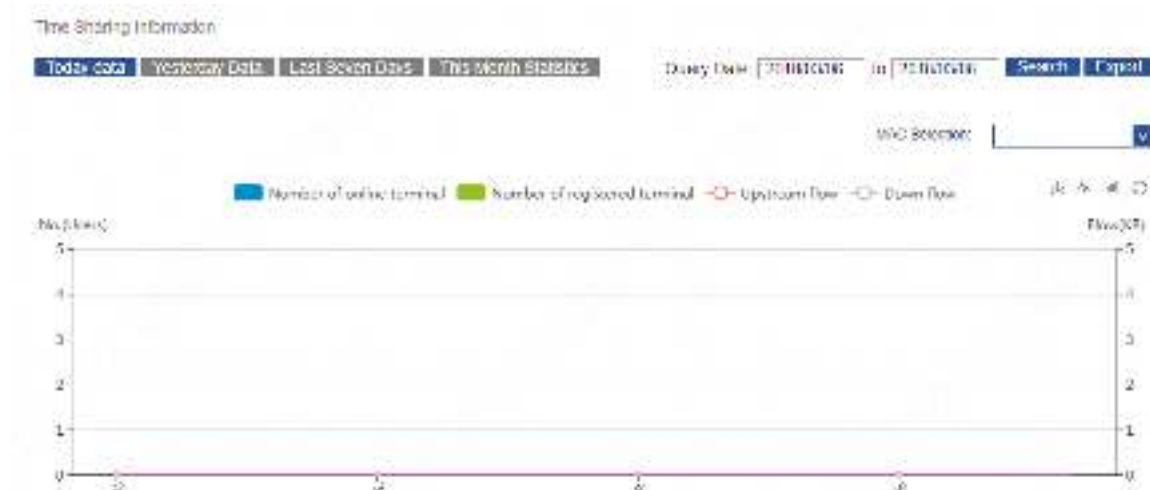


Figure 4-66

4.8.4 Message Management

Message management interface is used to view the user's message feedback info.

In the navigation bar, select “Marketing Management > Message Management”. The system displays “Message Management” interface, as shown in Figure 4-67.



Figure 4-67

4.8.5 Application Example

Before marketing management interface enables advertising authentication, please enable internal Web authentication (please refer to “4.6.3.1 Enable Web Authentication” for details). This chapter serves as a configuration example only.

Step 1 In the navigation bar, select “System Settings > Access Control”.

Step 2 In “Portal” tab, select “Internal Portal”, as shown in Figure 4-68.



Figure 4-68

Step 3 Click “Radius” tab to configure “Internal Radius”, as shown in Figure 4-69.

Figure 4-69

Step 4 Click “ACL Control Rules” tab to fill in AC IP address and 80 port number, and add to white list, as shown in Figure 4-70.

Figure 4-70

Step 5 Click “Rule Configuration” tab to enable white list; select the rule groups added in “ACL Control Rules”, as shown in Figure 4-71.

Figure 4-71

Step 6 In the navigation bar, select “Marketing Management > Advertising Management”; upload the advertising image to be played on the terminal, as shown in Figure 4-72.

Advertising Manage								
	Item	Ad Name	Ad Theme	Ad Position	Ad Type	Join Time	Update Time	View
	1	a1	Theme One	Top Image Database	Picture Advertising Link	2019-01-28 21:00:25	2019-01-28 21:00:25	⊞
	2	a2	Theme One	Left Image	Picture Advertising Link	2019-01-28 21:02:00	2019-01-28 21:02:00	⊞
	3	a3	Theme One	Left Image	Picture Advertising Link	2019-01-28 21:02:00	2019-01-28 21:02:00	⊞
	4	a4	Theme One	Left Image Database	Picture Advertising Link	2019-01-28 21:02:00	2019-01-28 21:02:00	⊞
	5	a5	Theme One	Left Image	Picture Advertising Link	2019-01-28 21:02:00	2019-01-28 21:02:00	⊞

Total 5 items, Max 7 / 1 Page: 15 / 50 items Previous Next End

New Add Edit Del

Figure 4-72

Step 7 In the navigation bar, select “Marketing Management > Theme Management”, create a theme and select advertising image, as shown in Figure 4-73.



Figure 4-73

Step 8 Select the box on the left of theme name, and click “Confirm”. Advertising images of this theme will be pushed in the terminal, as shown in Figure 4-74.



Figure 4-74

Step 9 Input any address in the browser of terminal (mobile phone and computer etc.), and it will be forced to visit the advertising image interface. Click any advertising image to go through Web authentication, and then go online.

Advertising viewing interface of the terminal is shown in Figure 4-75.




- LAN port of DH-PFM888S-AC shall be connected with public network.
- Wireless terminal, such as mobile phone and notebook computer, obtains IP address of public network, and associates with access point device.
- Apple iPhone doesn't need to open the browser, but jumps to advertising authentication interface automatically.



Figure 4-75

4.9 Logout

Click  button at the top right corner of the interface, and return to login interface.



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China

Postcode: 310053

Tel: +86-571-87688883

Fax: +86-571-87688815

Email: overseas@dahuatech.com

Website: www.dahuasecurity.com