KEDACOM

User Manual for Face Recognition Access Control System of KSCA121 Series

V1.1 (September, 2021)

Trademarks

KEDACOM®, Kedacom®, TrueSens®, 摩云视讯®, and NexVision® are registered trademarks of Suzhou Keda Technology Co., Ltd. in China and various other countries. All other trademarks mentioned in this document are the property of their respective holders.

Suzhou Keda Technology Co., Ltd.
131 Jinshan Road
New District, Suzhou, 215011
People's Republic of China
https://www.kedacom.com
Tel: +86-512-68418188
Fax: +86-512-68412699

Notice

The information in this document is subject to change without notice. Every effort has been made to prepare this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. Suzhou Keda Technology Co., Ltd. is not responsible for printing or clerical errors.

Target Audience

Administrators and Operators of Video Surveillance Products

Document Version

V1.1

Software Version

7.3.3

Applicable Models

KSCA121 series

Related Document

Quick Start Guide

Convention

Icon	Convention
ⓘ	Notes and warnings: necessary supplements to operations
BOLD	Menu, e.g. Drag to Zoom
>	Connector between menus of different levels, e.g. Settings > System

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss. Please read this Guide carefully before using the product, and keep it properly for future reference. If the product cannot work normally or is damaged because the user does not follow the safety instructions, we shall not assume any responsibility.

Working Conditions

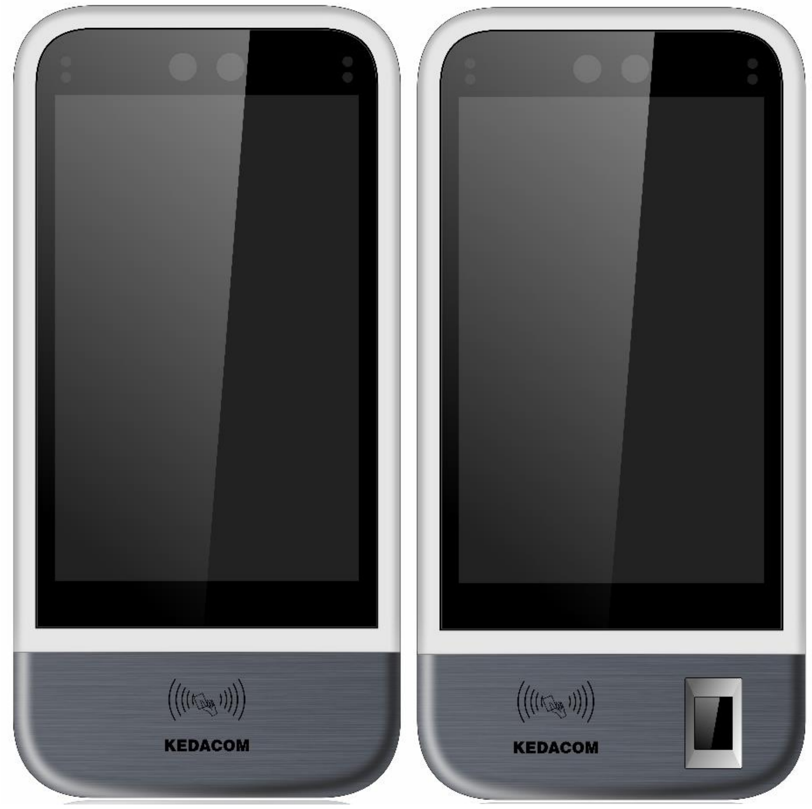
Please make sure the device is stored or working under the following environment.

Model	Working Voltage (Please use standard power adaptor)	Temperature	Relative Humidity	Altitude	Pressure
KSCA121 Series	DC12V±10% Power consumption: Max 25W	-40°C~+60°C	10%~95%	-60m~+3000m	86kPa~106kPa

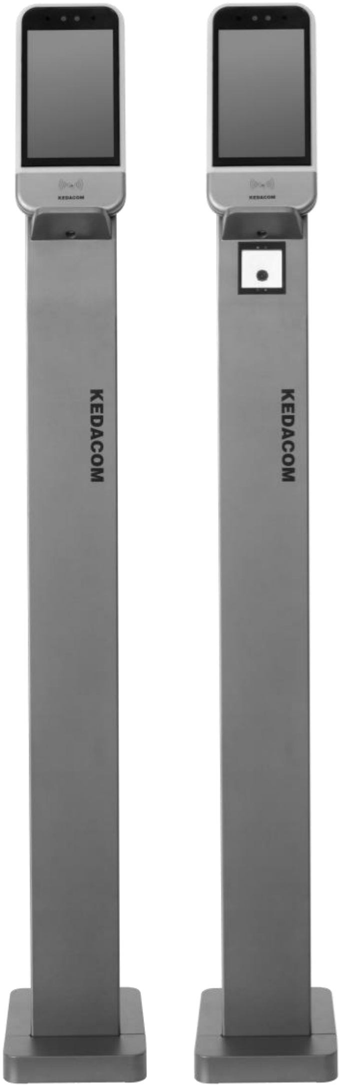
Contents

1. Product Brief

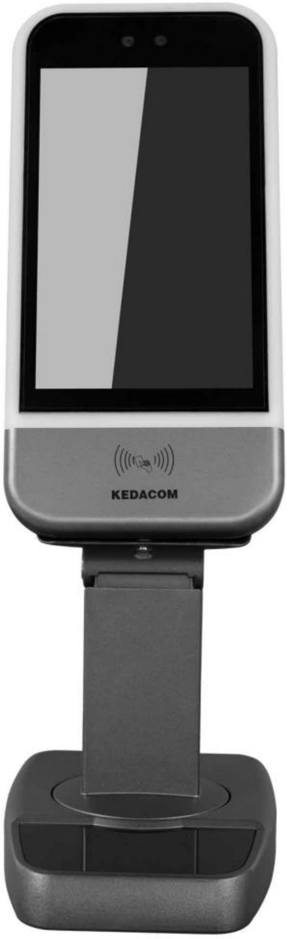
KSCA121 series are a kind of face recognition access control and attendance system. It supports multiple opening modes, including face/card/fingerprint, face & card & fingerprint, full match of face and ID photo, and remote help. It manages access electric lock and checks on work attendance through face recognition. Usually, it is applied to communities, financial places, enterprises, governments, schools, public security bureaus, judiciary authorities and buildings where personnel access needs to be controlled.



Picture 1-1 Product appearance (series with and without fingerprint)



Picture 1-2 Product appearance (Vertical type)



Picture 1-3 Product appearance (Desk type)

Features:

- 2.0MP 1/2.8” high-performance image sensor;
- H.264 encoding, 1080P@25fps HD live video;
- 8-inch LCD touch screen, show face comparison information and provide good man-machine interaction;
- Binocular UHD wide-angle lens, face recognition distance at 0.3~2m, suitable for height range of 1.2 to 1.9m;
- Deep-learning algorithm, fast recognition speed and high accuracy rate;
- Liveness detection, prevent photo-fraud and video-fraud effectively;
- Intelligent facial fill light, enable fill light automatically according to the light condition to suit outdoor backlight;
- Support multiple opening modes, including face/card/fingerprint, face & card & fingerprint, full match of face and ID photo, and remote help;

- Support stand-alone off-line operation, input card and face information locally to manage without platform or command center;
- Real-time uploading data to the command center to manage the blacklist at real time;
- Direct control over electric lock, door switch and door magnetism so as to manage access control;
- Support tamper alarm and door magnetic detection;
- Support Wiegand and RS485 port, to connect to access control system;
- Built-in MIC and speaker, support two-way audio and voice broadcast;
- Support Wi-Fi for convenient internet service;
- Support extended card reader, support people and card verification and registration;
- TF card local storage (maximum 256 G), support ANR;
- IP65-rated water-proof and dust-proof, -40°C~+60°C wide temperature range, to suit outdoor severe environment;
- Applied to communities, financial places, enterprises, governments, schools, public security bureaus, judiciary authorities and buildings where personnel access needs to be controlled.

2. Device Touch Screen

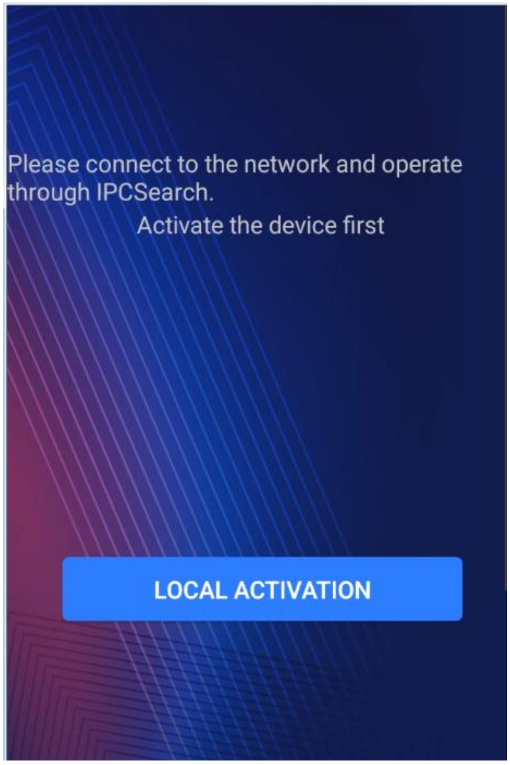
2.1 Startup

Please refer to the *Quick Start Guide* for device installation and wire connection.

For first-use of the device, user should activate it by any of the three methods: local activation, web client activation and IPCSearch activation. This chapter will introduce local activation and other methods will be introduced in chapter *3.1.1 Activation.*

2.1.1 Local Activation

Electrify and start the device. If the device is not activated before use, it will come to the activation interface automatically.



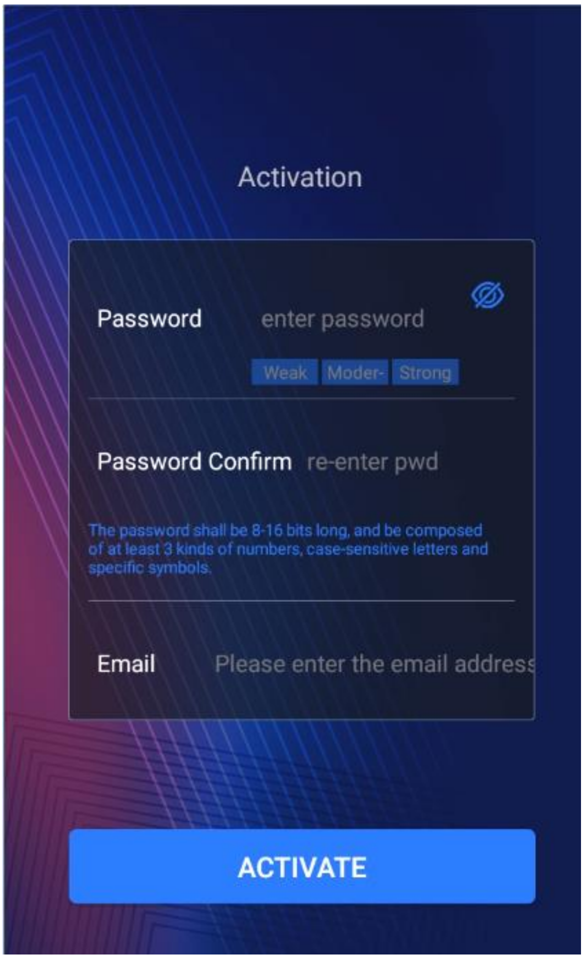
Please connect to the network and operate through IPCSearch.

Activate the device first

Picture 2-1 Activation prompt

Operation steps are as follows:

1) Tap “Local Activation” on the interface;



Activation

Password: enter password

Weak | Moder- | Strong

Password Confirm: re-enter pwd

The password shall be 8-16 bits long, and be composed of at least 3 kinds of numbers, case-sensitive letters and specific symbols.

Email: Please enter the email address

Picture 2-2 Local activation

2) Enter password, confirm password, and the email address for claiming password;

3) Tap “Activate” to activate the device.

Note:

- To ensure the safety of device on internet, it is strongly recommended that you set a strong password composed of at least 2 kinds of the following, numbers, upper-case letters, lower-case letters or specific symbols with length of 8 to 16 characters.
- Please modify the password periodically such as once every 3 months. If the device is used in highly risky environment, suggest modifying the password monthly or weekly.
- Please keep your username and password safe.

2.1.2 Stand-By Interface

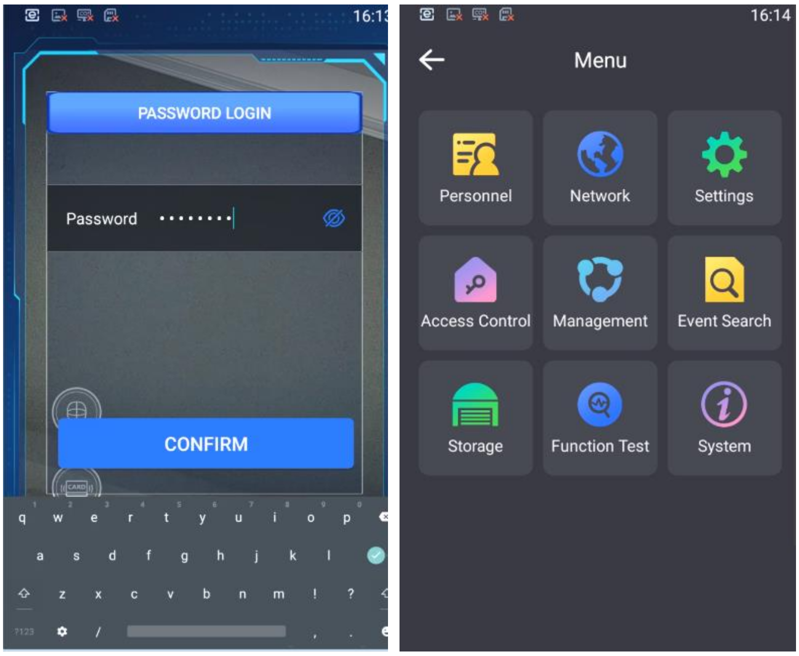
After being activated, the device enters stand-by mode. Face toward the screen to activate face verification and display the live-view image.

Picture 2-3 Stand-by interface

- If the person to be recognized is in the database (registered or imported) and the face recognition score reaches the threshold, it will show verification succeeded and display the person’s name at the bottom of the screen.
- If the person to be recognized is out of the database, it will show verification failed.

2.2 Login

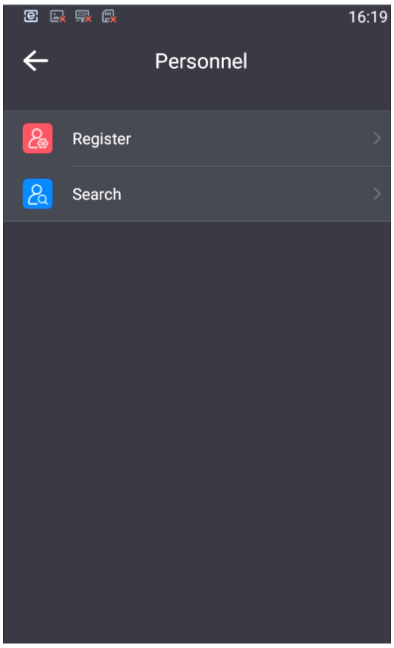
Touch the screen for 3 seconds to pop up the login interface. Enter the password set during activation to log into the device, and perform operations such as personnel management, access control configuration, event search and etc. Click ⇦ at top left corner of the interface to return to standby interface.



Picture 2-4 Menu

2.3 Personnel

Tap **Menu>Personnel** to register and search personnels.

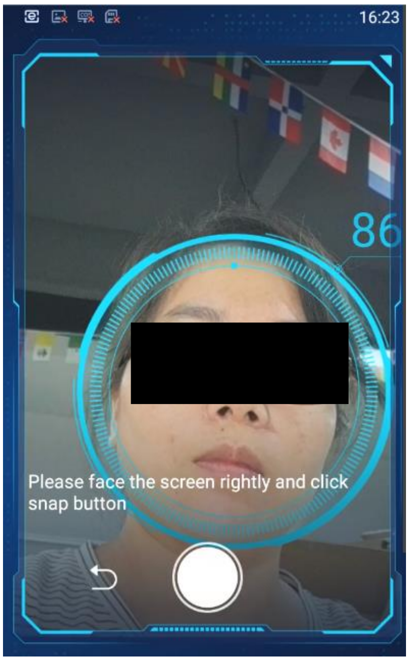


Picture 2-5 Personnel management

2.3.1 Register

Tap **Menu > Personnel > Register** to add new user and register information such as name, certificate type, certificate No. and etc.

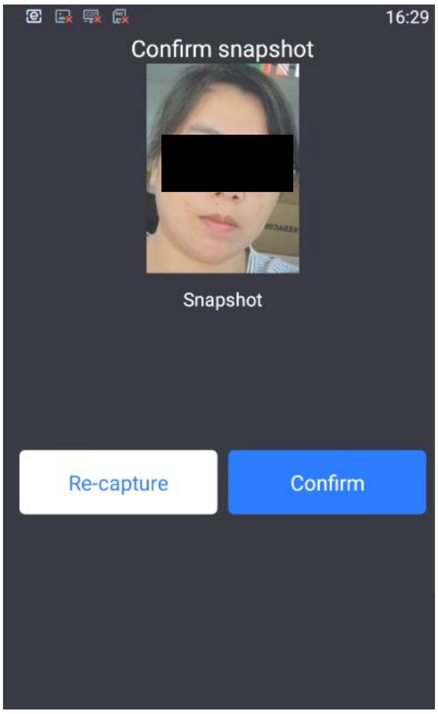
1) Tap **Menu > Personnel > Register**, face toward the camera with optimum distance of 1 m, tap the button at the bottom to capture a snapshot.


[redacted]

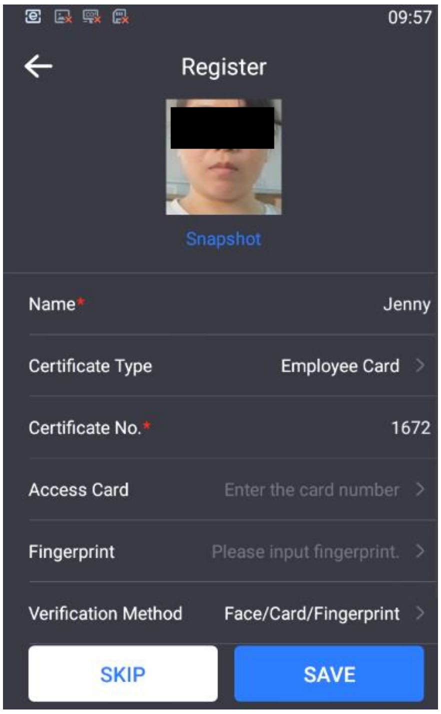
Please face the screen rightly and click snap button

Picture 2-6 Personnel registration

2) Tap “Confirm” to enter the information registration interface and input name, certificate type, certificate No. and etc.



Picture 2-7 Registration information



Name* Jenny

Certificate Type Employee Card

Certificate No.* 1672

Access Card Enter the card number

Fingerprint Please input fingerprint.

Verification Method Face/Card/Fingerprint

Picture 2-8 Registration information

3) When there is an access card, tap “Access Card” to select a card and put the access card on the card area to register access card number;

Note:

♦ Only some models support access card. Please subject to actual device;

- ♦ When one access card is shared by several people, please make sure the verification method is the same, otherwise there will be a mess.

4) Tap “Save” to complete personnel registration;

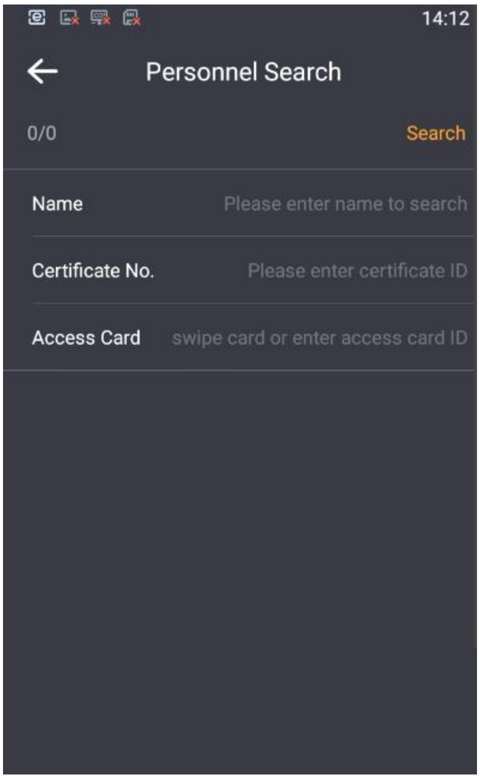
ⓘNote: If the certificate number of the same type already exists when saving the information, it will pop up “The ertificate number already exists, please confirm if you would like to save anyway.” Tap “Confirm” to overwrite the former number.

5) After finishing registration, it will skip to the personnel registration interface. Tap “<” at top left corner and input the login password to exit.

ⓘNote: The snapshot may fail when people fail to face the camera rightly or the distance to the camera is too close or too far. When it occurs, tap “Re-capture”.

2.3.2 Search

Tap **Menu > Personnel > Search**, and view, edit or delete the information of registered personnel.



14:12

Personnel Search

0/0 Search

Name: Please enter name to search

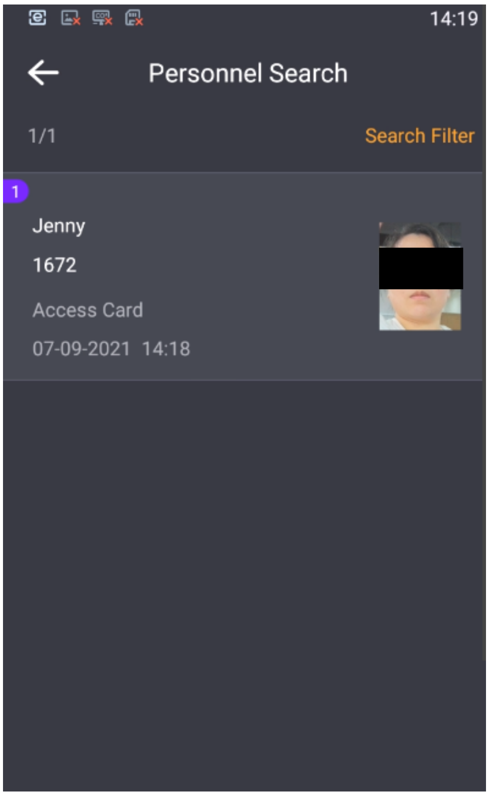
Certificate No.: Please enter certificate ID

Access Card: swipe card or enter access card ID

Picture 2-9 Personnel search

Input any one or more of the information such as name, certificate No. and access card number, tap “Search” to enter the interface of personnel information, and the relevent information will show on the list below.

Tap “Search Filter” to return to the search interface and re-input the search condition.



1/1

1

Jenny

1672

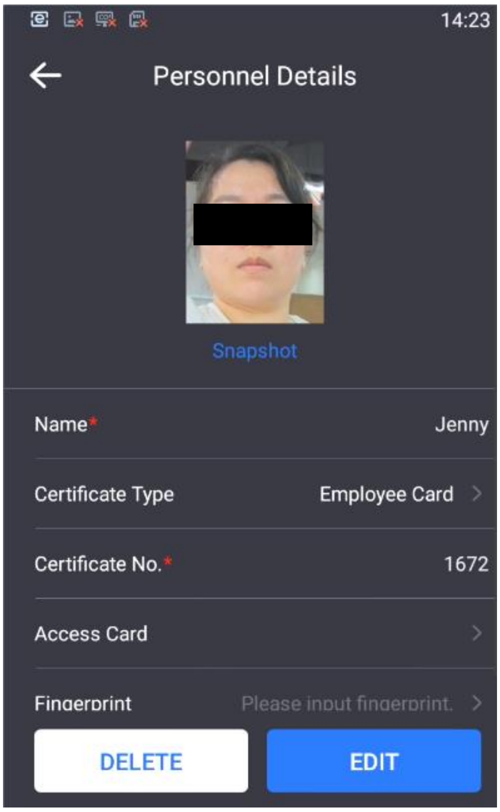
Access Card

07-09-2021 14:18

[redacted]

Picture 2-10 Search result

Select the expected one and tap to view the personnel detail.



[redacted]

Name* Jenny

Certificate Type Employee Card >

Certificate No.* 1672

Access Card >

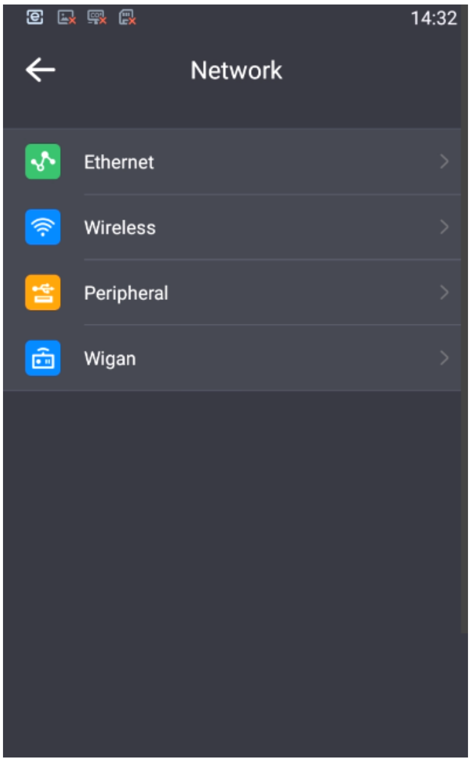
Fingerprint Please input fingerprint. >

Picture 2-11 Personnel detail

- Edit: Tap “Edit” to edit the information, but the certificate type and certificate No. are non-editable; tap “Save” to finish.
- Delete: Tap “Delete” and select “Confirm” to delete the personnel information.

2.4 Network

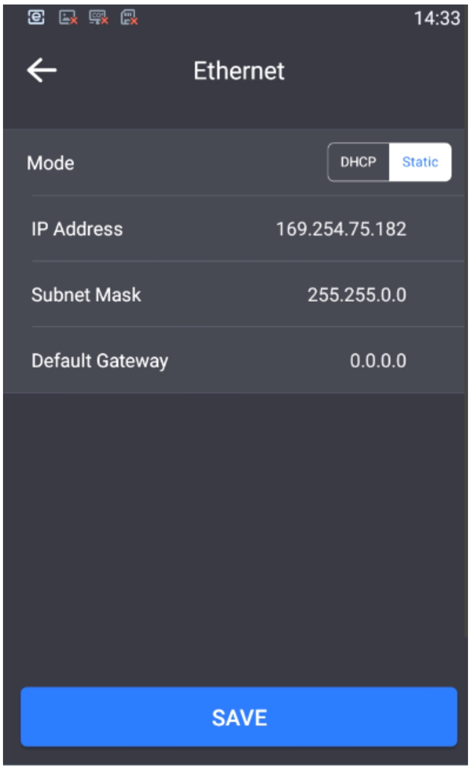
Tap **Menu > Network** and configure Ethernet, Wireless, Peripheral and Wigan.



Picture 2-12 Network

2.4.1 Ethernet

Tap **Menu > Network > Ethernet** and configure Ethernet parameters.



14:33

Ethernet

Mode: DHCP / Static

IP Address: 169.254.75.182

Subnet Mask: 255.255.0.0

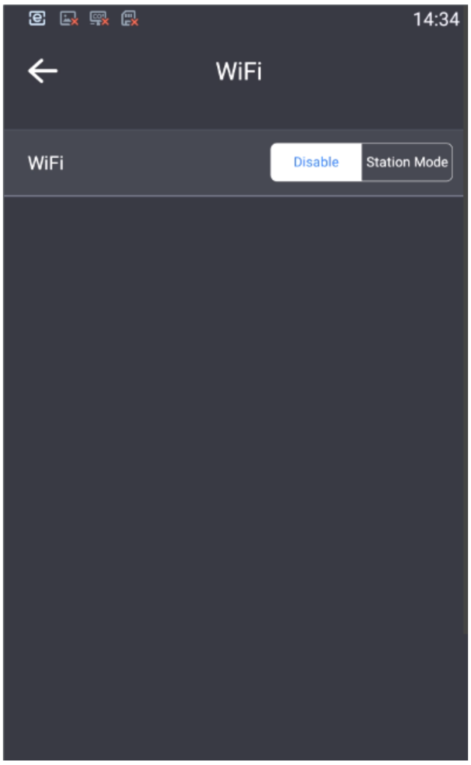
Default Gateway: 0.0.0.0

Picture 2-13 Ethernet

Select “Mode”. If selecting “DHCP”, it will assign IP address automatically; if selecting “Static”, input “IP Address”, “Subnet Mask” and “Default Gateway” manually; tap “Save” to finish configuration.

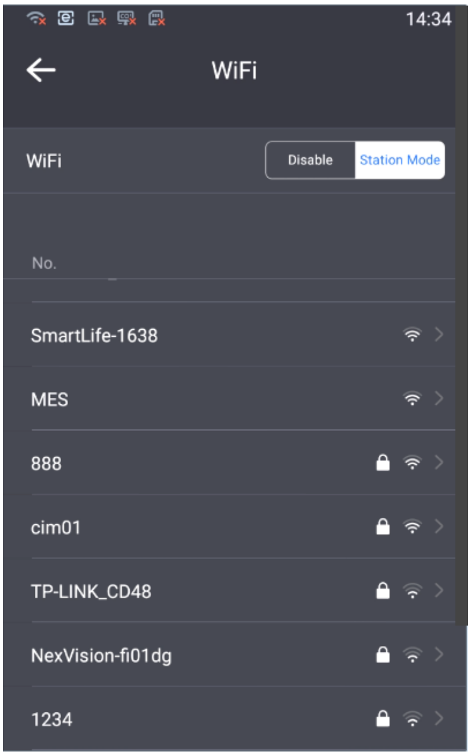
2.4.2 Wireless

Tap **Menu > Network > Wireless** and configure WiFi parameters. WiFi mode options include “Disable” and “Station Mode”.



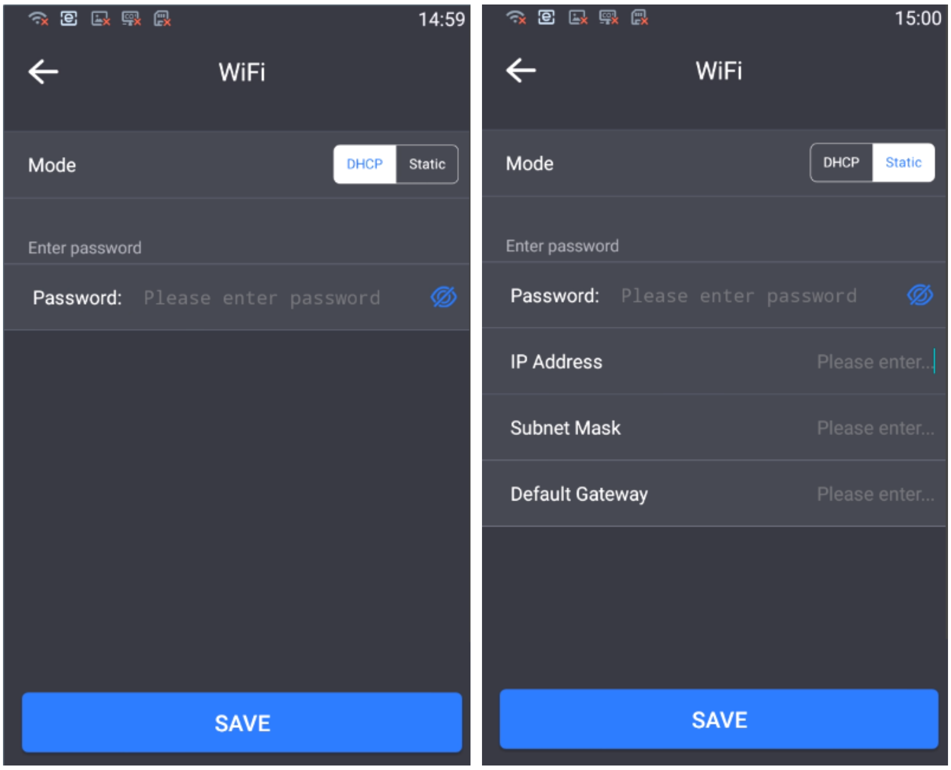
Picture 2-14 WiFi

When it’s necessary to access to wireless network, enable “Station Mode”, and select AP hotspot from the list for the device to connect to.



Picture 2-15 Station mode

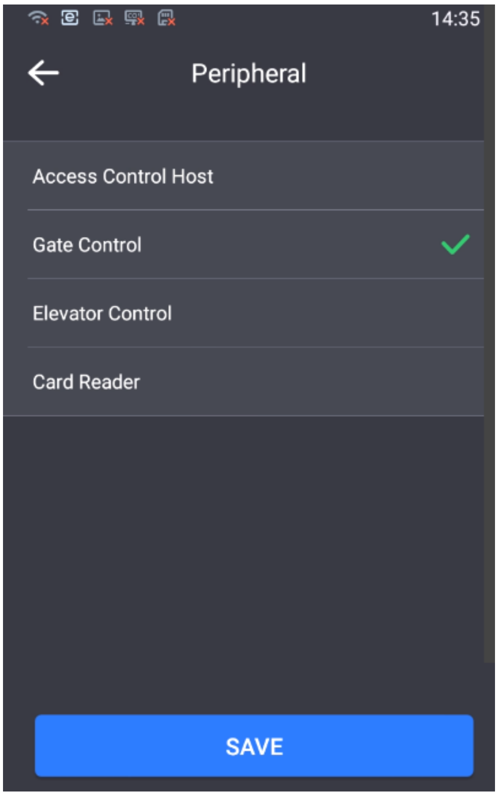
Select a hotspot from the list and enter the “WiFi” setting interface; select mode according to actual request, including “Static” and “DHCP”. When selecting “DHCP”, enter the password; when selecting “Static”, configure IP address, subnet mask and default gateway manually.After finishing, tap “Save” to connect to the selected WiFi network.


14:59
WiFi
Mode
DHCP
Static
Enter password
Password: Please enter password
SAVE
15:00
WiFi
Mode
DHCP
Static
Enter password
Password: Please enter password
IP Address Please enter...
Subnet Mask Please enter...
Default Gateway Please enter...
SAVE

Picture 2-16 Wifi- DHCP and Static

2.4.3 Peripheral

Tap **Menu > Network > Peripheral** and select a peripheral for the access control device.



14:35

Peripheral

Access Control Host

Gate Control ✓

Elevator Control

Card Reader

SAVE

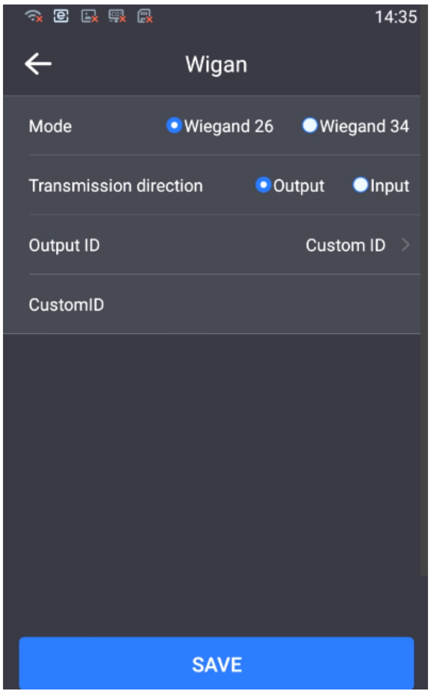
Picture 2-17 Peripheral

Select a peripheral device, options including “Access Control Host”, “Gate Control”, “Elevator Control” and “Card Reader”. Tap “Save” to finish.

2.4.4 Wigan

Tap **Menu > Network > Wigan**, and configure parameters by actual request.

When connecting to the access control host through Wigan port, the WG0 wire of the buttcock line connects to the D0 wire of access control host, the WG1 wire to the D1 wire of access control host, and the GND wire to the earth wire of access control host.



14:35

Wigan

Mode ● Wiegand 26 ○ Wiegand 34

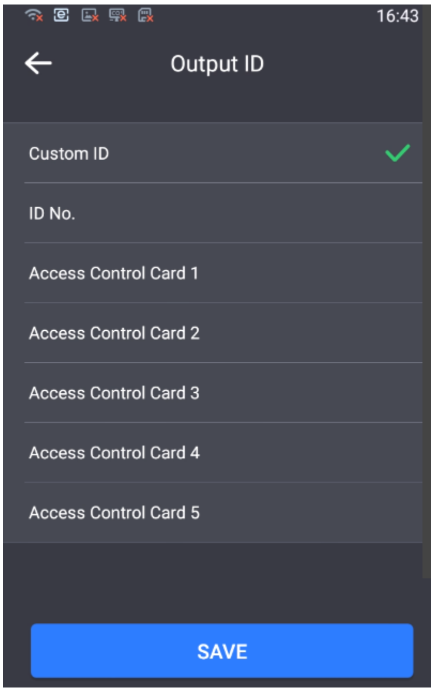
Transmission direction ● Output ○ Input

Output ID Custom ID >

CustomID

Picture 2-18 Wigan

- Mode: Options include Wiegand 26 and Wiegand 34. The data transmission rules are as follows:
  - It transmits 10-bit “Int” type data and the limit value is 4294967295. When the data is over the limit value, it will turn the first bit to 0. For example, when transmitting 5165214521, it will turn it to 0165214521. For data shorter than 10-bit, it will add “0” as the prefix. For example, when transmitting 23000000, it will turn it to 0023000000. For data longer than 10-bit, it will pick the last 10 bits and make sure it is smaller than the limit value. For example, when transmitting 999998888899999, it will turn it to 0888899999.
- Transmission direction: Currently it supports “Output” only.
- Output ID: Options include “Custom ID”, “ID No.” and “Access Control Card”. When selecting “Custom ID”, enter custom ID number. The device recognizes the human face and will transmit the ID number to the access control host. When selecting “ID No.” or “Access Control Card”, the device recognizes the human face and will transmit the ID No. or access control card No. to the access control host. The transmission of custom ID, ID No. and access control card also follows the data transmission rules illustrated above.


16:43

Output ID

Custom ID ✓

ID No.

Access Control Card 1

Access Control Card 2

Access Control Card 3

Access Control Card 4

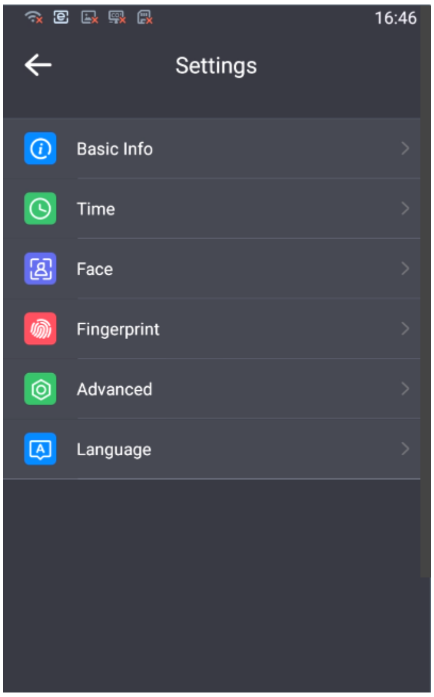
Access Control Card 5

SAVE

Picture 2-19 Output ID

2.5 Settings

Tap **Menu > Settings** and configure “Basic Info”, “Time”, “Face” “Fingerprint” (some models support), “Advanced” and “Language”.


16:46

Settings

Basic Info

Time

Face

Fingerprint

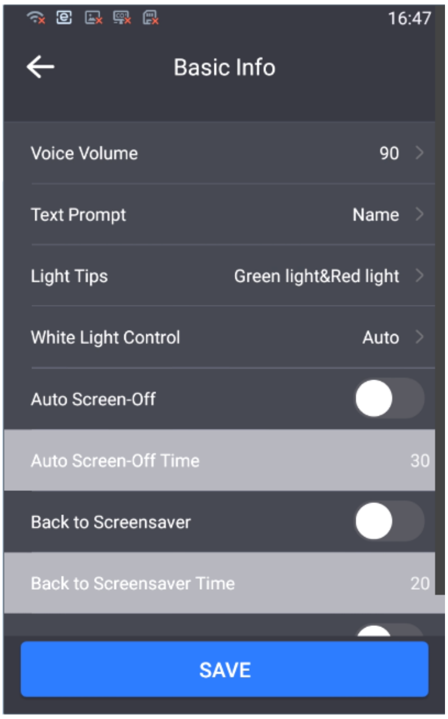
Advanced

Language

Picture 2-20 Settings

2.5.1 Basic

Tap **Menu > Settings > Basic Info** and configure parameters such as voice volume, text prompt, light tips, white light control, auto screen-off, auto screen-off time and etc.



16:47

Basic Info

Voice Volume 90

Text Prompt Name

Light Tips Green light&Red light

White Light Control Auto

Auto Screen-Off

Auto Screen-Off Time 30

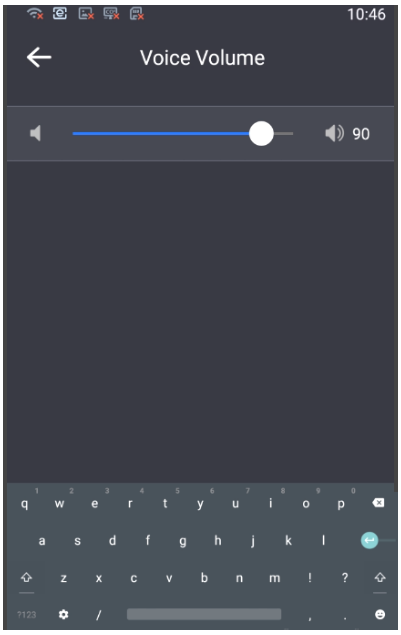
Back to Screensaver

Back to Screensaver Time 20

Picture 2-21 Basic info

- ➢ Voice Volume

  Tap “Voice Volume” and drag the slide bar to adjust device volume, the range being 0~100 and the default being 90.



10:46

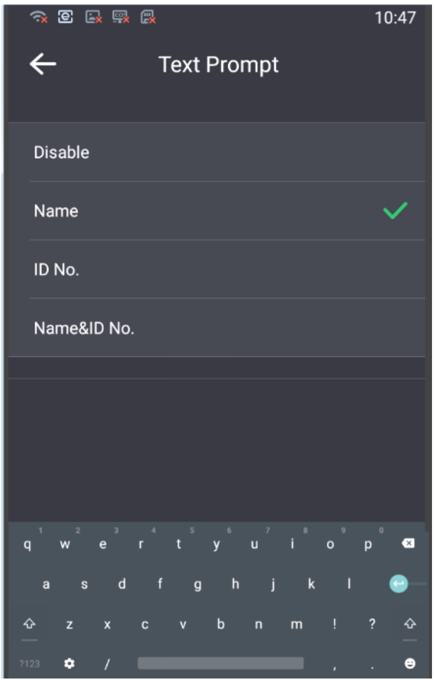
Voice Volume

90

Picture 2-22 Voice volume

- Text Prompt

Tap “Text Prompt” to enter the text prompt interface; select the prompt text displayed on the main interface when the device recognizes a user, options including “Name”, “ID No.”, “Name& ID No.” and “Disable”; if selecting “Disable”, when the device recognizes a user, there will be no text prompt; tap “Save” to validate setting.



10:47

Text Prompt

Disable

Name ✓

ID No.

Name&ID No.

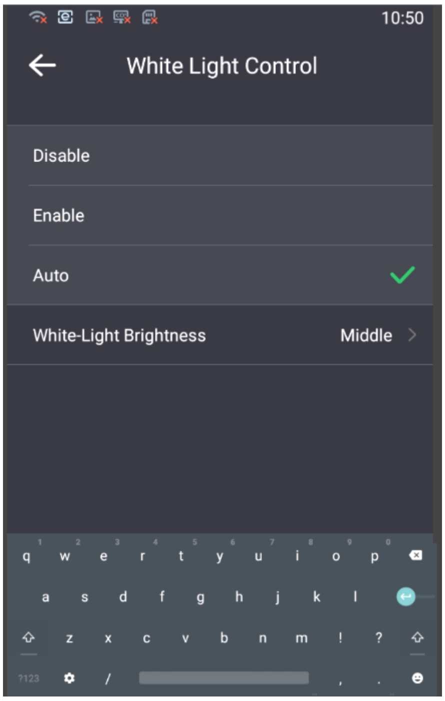
Picture 2-23 Text prompt

- Light Tips

Select light tips type according to actual requirements, options including “Close”, “Green light”, “Red Light” and “Green light&Red light”.

- White Light Control

Tap “White Light Control” and select “Enable” or “Disable” or “Auto”; select “Middle”, “Low” or “High” for white light brightness; tap “Save” to validate setting.



White Light Control

Disable

Enable

Auto ✓

White-Light Brightness Middle >

Picture 2-24 White light control

- Auto Screen-Off

  Enable or disable auto screen-off function. If enabled, user can configure the auto screen-off time (unit: second). If no operation is done to the device in the configured duration, the device will skip to the stand-by interface. If disabled, the device will not screen-off automatically.

- Back to Screensaver

  Enable or disable back to screensaver function. If enabled, user can configure the back to screensaver time (unit: second). If no operation is done to the device in the configured duration, the device will skip to the stand-by interface.

- Screen-Off Test

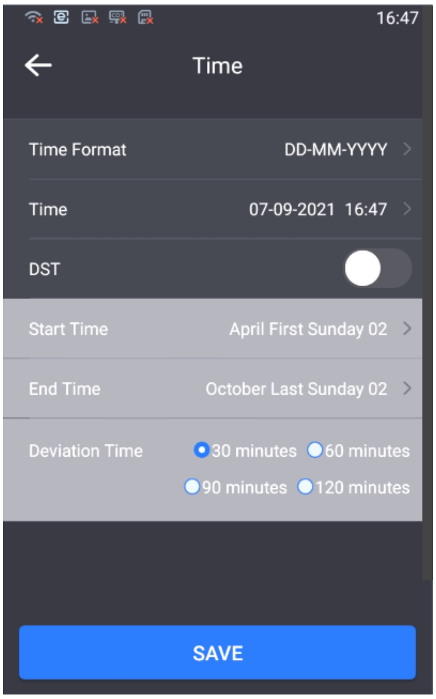
  Enable or disable back to screen-off test function. If enabled, it allows screen-on and face detection under screen-off mode.

- Select screensaver

  Tap “Select screensaver” to enter the interface and select screensaver; tap “Save” to validate setting.

2.5.2 Time

Tap **Menu > System > Time** and configure “Time Format”, “Time”, “DST”, “Start Time”, “End Time” and “Deviation Time”.



Time Format DD-MM-YYYY

Time 07-09-2021 16:47

DST

Start Time April First Sunday 02

End Time October Last Sunday 02

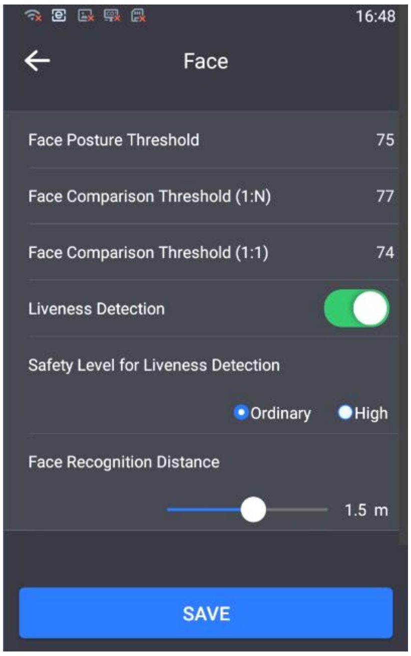
Deviation Time ● 30 minutes ○ 60 minutes ○ 90 minutes ○ 120 minutes

Picture 2-25 Time

- Time Format: Tap “Time Format” and select a displaying format of time, options including “MM-DD-YYYY”, “DD-MM-YYYY” and “YYYY-MM-DD”. Tap “Save” to validate setting.
- Time: Tap “Time” to enter time setting interface and configure date and time manually; tap “Save” to validate setting.
- DST: Enable or disable DST; if enabled, configure “Start Time”, “End Time” and “Deviation Time”.
    - Start Time: Tap “Start Time” to enter time setting interface and configure DST start time manually, the default being 2:00 on the first Sunday of April; tap “Save” to validate setting.
    - End Time: Tap “End Time” to enter time setting interface and configure DST end time manually, the default being 2:00 on the last Sunday of October; tap “Save” to validate setting.
    - Deviation Time: Select an option for deviation time, including “30 minutes”, “60 minutes”, “90 minutes” or “120 minutes”, the default being “30 minutes”. Tap “Save” to validate setting.

2.5.3 Face

Tap **Menu > System > Face** and configure “Face Posture Threshold”, “Face Comparison Threshold (1:N)”, “Face Comparison Threshold (1:1)”, “Liveness Detection”, “Safety Level for Liveness Detection” and “Face Recognition Distance”.



Face Posture Threshold 75

Face Comparison Threshold (1:N) 77

Face Comparison Threshold (1:1) 74

Liveness Detection

Safety Level for Liveness Detection

● Ordinary ○ High

Face Recognition Distance

1.5 m

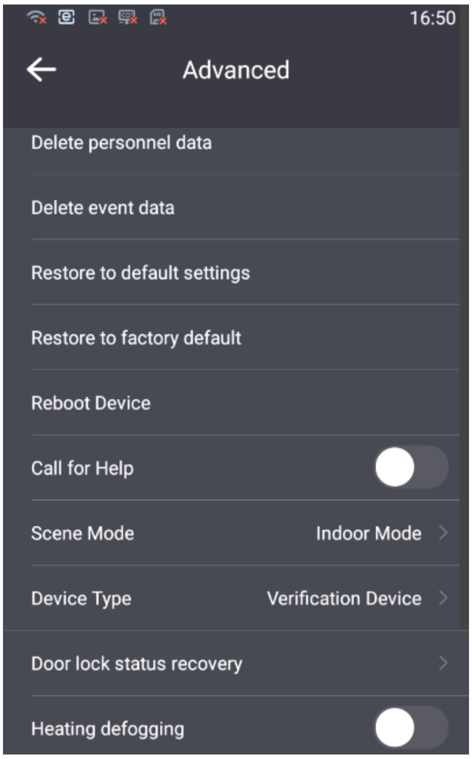
Picture 2-26 Face

- Face Posture Threshold: Configure the threshold score for face recognition, the range being 0~100 points. The device will assess face posture from the perspective of vertical pitching angle, horizontal level angle and interorbital distance; if the score is lower than the preset value, the face recognition will fail, and face comparison or face registration will fail.
- Face Comparison Threshold (1:N): Configure the threshold score for face comparison by 1:N, the range being 0~100 points. The higher the preset value is, the lower the false recognition rate will be but the higher the rejection rate will be.
- Face Comparison Threshold (1:1): Configure the threshold score for face comparison by 1:1, the range being 0~100 points. The higher the preset value is, the lower the false recognition rate will be but the higher the rejection rate will be.
- Liveness Detection: Enable or disable liveness detection function. After enabling the function, the device will judge if the recognized object is truly a human face; if the object is not a real human face, the verification will fail. After enabling the function, the maximum recognition distance is 1.8m.
- Safety Level for Liveness Detection: After enabling “Liveness Detection”, select a safety level for liveness detection, “Ordinary” or “High”.
- Face Recognition Distance: Drag the slide bar to configure face recognition distance, the range being 0.3~2.5 m and the default being 1.5 m. The value is a rough one, and there will be some deviation in actual practice according to the sizes of human faces.

Tap “Save” to validate setting.

2.5.4 Advanced

Tap **Menu > Settings > Advanced** to delete personnel data and event data, restore to default settings, restore to factory default and etc.



16:50

Advanced

Delete personnel data

Delete event data

Restore to default settings

Restore to factory default

Reboot Device

Call for Help ○

Scene Mode Indoor Mode >

Device Type Verification Device >

Door lock status recovery >

Heating defogging ○

Picture 2-27 Advanced

- Delete personnel data

  Tap “Delete personnel data” and it will pop up a prompt dialogue box. Tap “Confirm” and the device will clear all personnel data.

- Delete event data

  Tap “Delete event data” and it will pop up a prompt dialogue box. Tap “Confirm” and the device will clear all event data.

- Restore to default settings

  Tap “Restore to default settings” and it will pop up a prompt dialogue box. Tap “Confirm” and the device will reboot automatically and restore to default settings.

- Restore to factory default

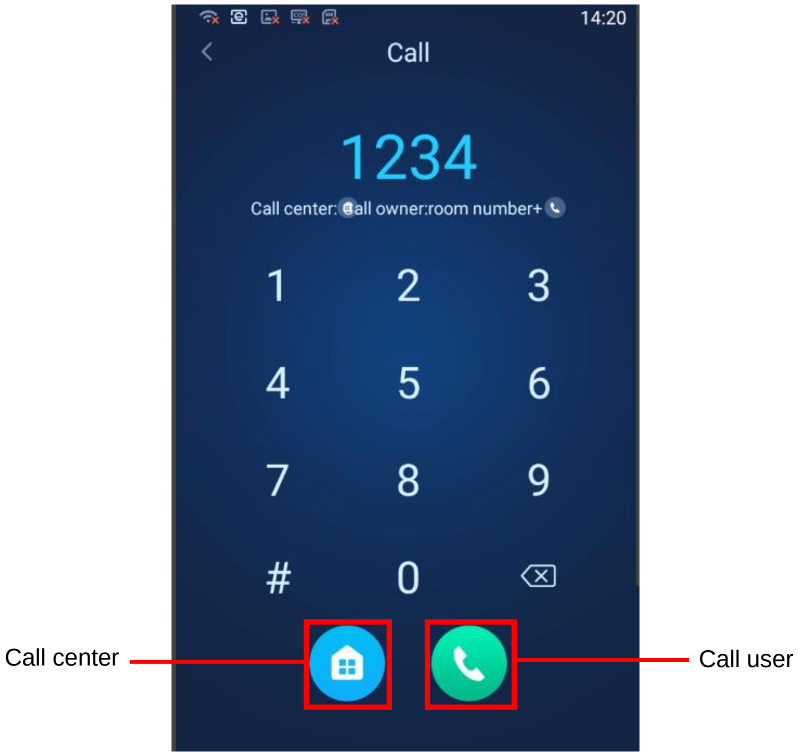
  Tap “Restore to factory default” and it will pop up a prompt dialogue box. Tap “Confirm” and the device will reboot automatically and restore to factory default.

- Reboot Device

  Tap “Reboot Device” and it will pop up a prompt dialogue box. Tap “Confirm” and the device will reboot.

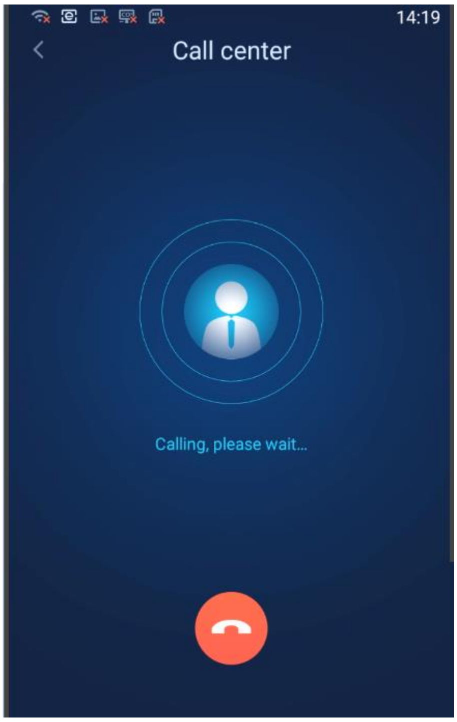
- Call for Help

Tap “Call for Help” to enable or disable the function; after enabling, there will be 2 icons showing on the standby interface, call center and call user.



Picture 2-28 Call for help

- Call center



Picture 2-29 Call center

Tap to enter call center interface and have conversations with the back-end platform when it connects.

- Call user

  This function is unavailable now.

Note: The “Call for Help” function is available only when the device accesses to the specific back-end platforms. Some custom versions may have different variants of the function. Please subject to the actual interfaces of the devices.

- Scene Mode

  Select a mode according to actual installation situation, options including “Ourdoor Mode” and “Indoor Mode”.

- Device Type

  Select device type according to actual condition, options including “Verification Device”, “Collection Device-JG”, “Collection Device-YL” and “Verification Device –SD”.

- Door lock status recovery

  Tap “Door lock status recovery” and it will pop up a prompt dialogue box. Tap “Confirm” to recover door lock status.

- Heating defogging

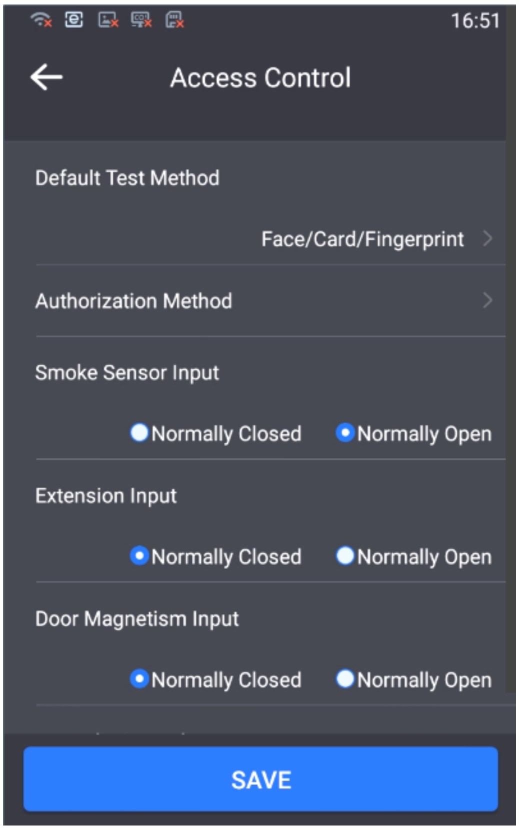
  Enable or disable heating defogging function according to actual requirements.

2.5.5 Language

Tap **Menu > Settings > Language,** and select language for the interface, options including simplified Chinese and English.

2.6 Access Control

Tap **Menu > Access Control**, and configure default test method, authorization method, smoke sensor input and etc. Tap “Save” to finish configuration.



Access Control

Default Test Method: Face/Card/Fingerprint

Authorization Method

Smoke Sensor Input: ○ Normally Closed ● Normally Open

Extension Input: ● Normally Closed ○ Normally Open

Door Magnetism Input: ● Normally Closed ○ Normally Open

Picture 2-30 Access control

- Default Test Method: Tap "Default Test Method" to pop up a dialogue box; select a test method, options including "Face", "Card", "Face & Card", "Face/Card" and etc.

Note:

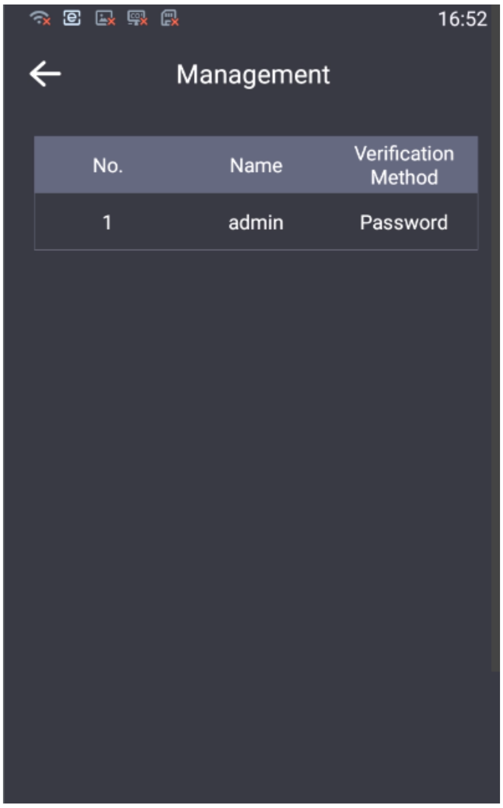
- As different devices support different test methods, please subject to actual devices.
- If the default test method of the device includes "Face & Card", it is the default test method for actual verification; if the device does not contain "Face & Card", the actual verification is subject to the method selected during personnel registration, and the default test method is only for personnel registration.

- Authorization Method: Configure the authorization methods for different verification modes. Tap "Authorization Method" and select the method on the popup interface, options including "Face", "Card" and "Face & Card". Tap "Save" to validate setting.
- Smoke Sensor Input: Options include "Normally Closed" and "Normally Open". When the device connects to low frequency electric smoke sensor, select "Normally Open"; when it connects to high frequency electric smoke sensor, select "Normally Closed".
- Extension Input: This function is used in building intercom system to open and close the door. Options include "Normally Closed" and "Normally Open", and the former is the default.

- Door Magnetism Input: This function is used to feedback access control status to the platform. Options include “Normally Closed” and “Normally Open”, and the former is the default. When selecting “Normally Closed”, the door magnetism port SENS connects to the door magnetism switch NC port, and GND to door magnetism COM port; when selecting “Normally Open”, the door magnetism port SENS connects to the door magnetism switch NO port, and GND to door magnetism COM port.
- Door-closing Delay Time: Configure the delay time from door opening to door closing, the range being 1~255 s, the default being 5 s.
- Test Time of Door-opening Exception: Configure the alarm threshold for door opening timeout, the range being 0~3600 s, the default being 30 s; when the door opening exceeds the threshold, an alarm will be triggered.
- Identification Alarm Times: Configure the maximum times of identification failures, the range being 1~255 times, the default being 5 times; if the identification failure exceeds the maximum value, an alarm will be triggered.
- Tamper Alarm: Enable “Tamper Alarm” to enable tamperproof button alarming. After enabling this function, when the tamperproof button on the back of the device is triggered, the device will alarm.
- Card Type: Configure the supported card types for card reading, options including “Citizen Card”, “CPU Card”, “M1 Card” and “Physical ID”.
- Card-reader Type: Select card-reader type according to actual condition.
- Remove repetition of door-opening signal: It’s enabled by default. When it’s enabled, one cannot send door-opening signal or upload to back-end repeatedly in 5s.
- Door Lock Type: Select door lock type according to actual condition.

2.7 Management

Tap **Menu > Management**, and change admin user password, add/edit face and add/edit card number.

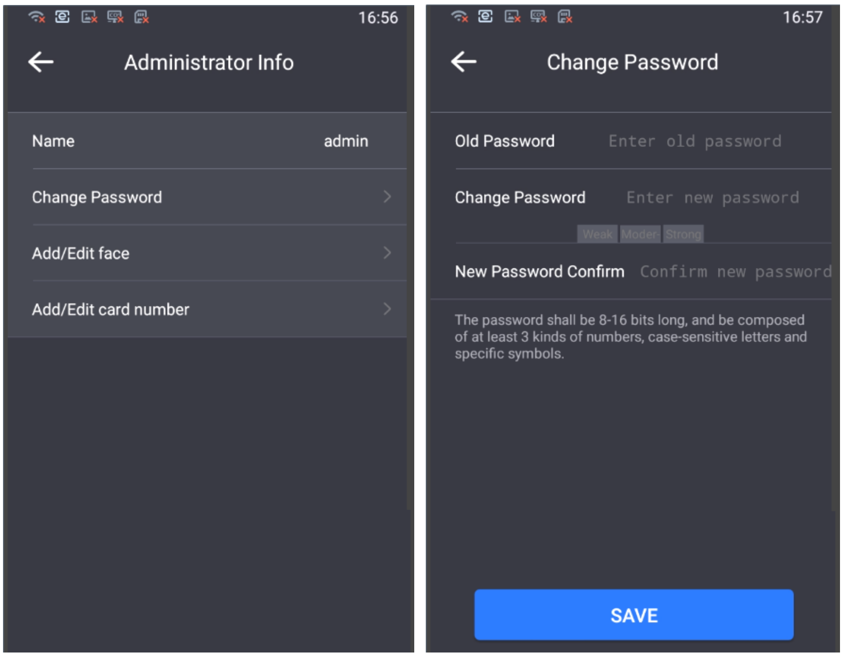


No.	Name	Verification Method
1	admin	Password

Picture 2-31 Management

- Change Password

Tap to select user and enter the “Administrator Info” interface; tap “Change Password” to enter “Change Password” interface; input the “Old Password”, “Change Password”, and “New Password Confirm”; tap “Save” to finish.



Name admin

Change Password

Add/Edit face

Add/Edit card number

Old Password Enter old password

Change Password Enter new password

New Password Confirm Confirm new password

The password shall be 8-16 bits long, and be composed of at least 3 kinds of numbers, case-sensitive letters and specific symbols.

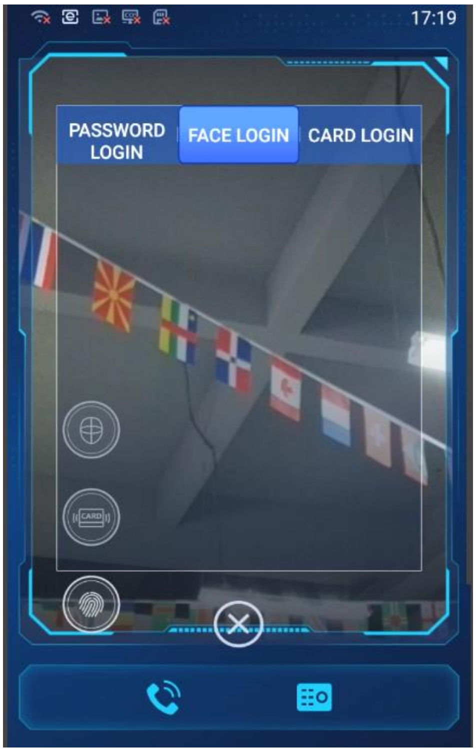
Picture 2-32 Change password

Note:

- To ensure the safety of device on internet, it is strongly recommended that you set a strong password composed of at least 2 kinds of the following, numbers, upper-case letters, lower-case letters or specific symbols with length of 8 to 16 characters.
- Please modify the password periodically such as once every 3 months. If the device is used in highly risky environment, suggest modifying the password monthly or weekly.
- Please keep your username and password safe.

➢ Add/Edit face

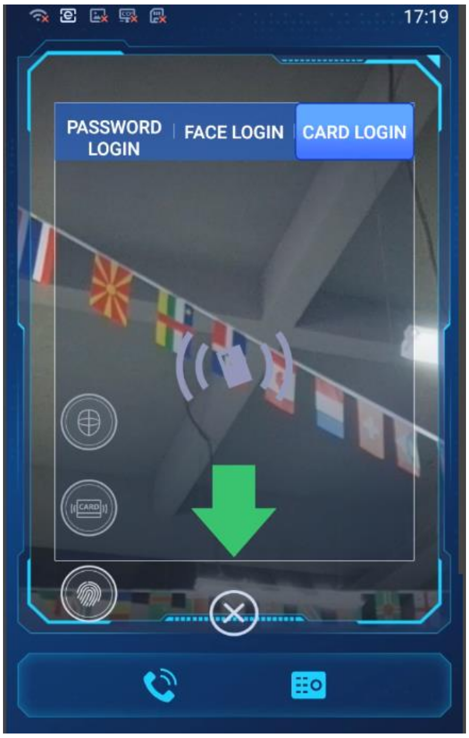
If the face of the user has been registered, tap it to delete or re-capture; if the user hasn’t registered the face, tap it to enter the interface of capture and register. After finishing face registration, user can select face recognition to login and enter the menu on the login interface.



Picture 2-33 Face login

➢ Add/Edit card number

Add or edit the card number of the user. After finishing, user can swipe card to login and enter the menu on the login interface.

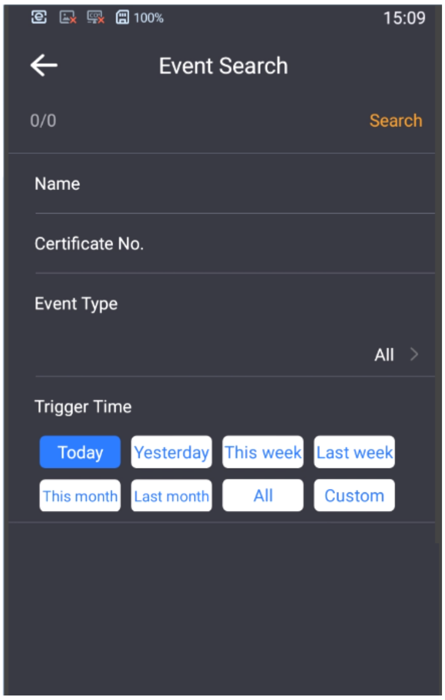


Picture 2-34 Card login

2.8 Event Search

The function of event search requires a TF card, so make sure the TF card has been inserted and works normally.

Tap **Menu > Event Search,** and search event records.

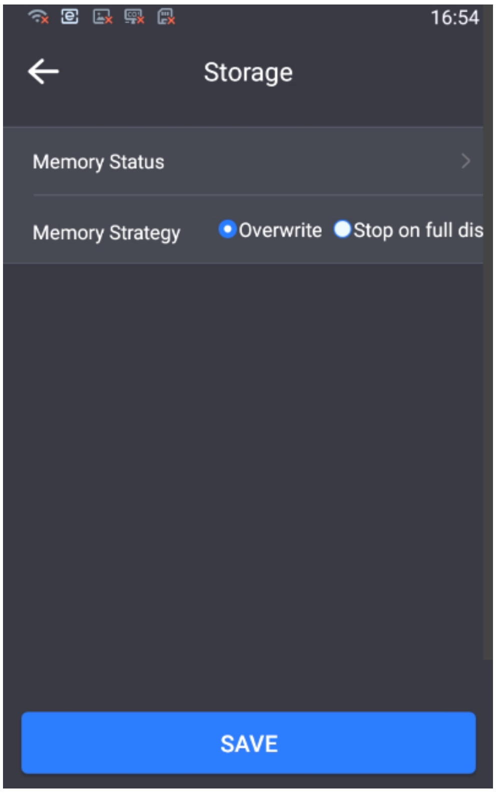


Picture 2-35 Search events

Input one or more of the conditions such as name, certificate No., event type and trigger time and tap “Search” to search expected event records.

2.9 Storage

Tap **Menu > Storage** and view the “Memory Status” and “Memory Strategy”.



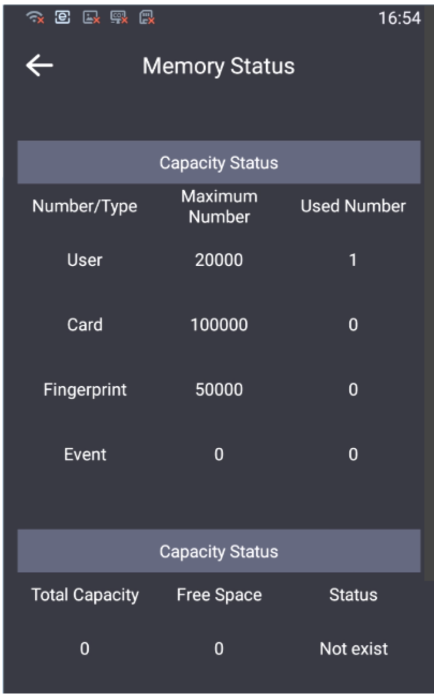
Memory Status

Memory Strategy ● Overwrite ○ Stop on full dis

Picture 2-36 Storage

- Memory Status

  Tap “Memory Status” to enter “Memory Status” interface and view capacity status of the device and external storage.



Memory Status

Capacity Status

Number/Type	Maximum Number	Used Number
User	20000	1
Card	100000	0
Fingerprint	50000	0
Event	0	0

Capacity Status

Total Capacity	Free Space	Status
0	0	Not exist

Picture 2-37 Storage status

- Capacity status: This table shows the “Maximum Number” and “Used Number” of “User”, “Card” and “Event”.
- External storage: This table shows the “Total Capacity”, “Free Space” and “Status” of external storage.

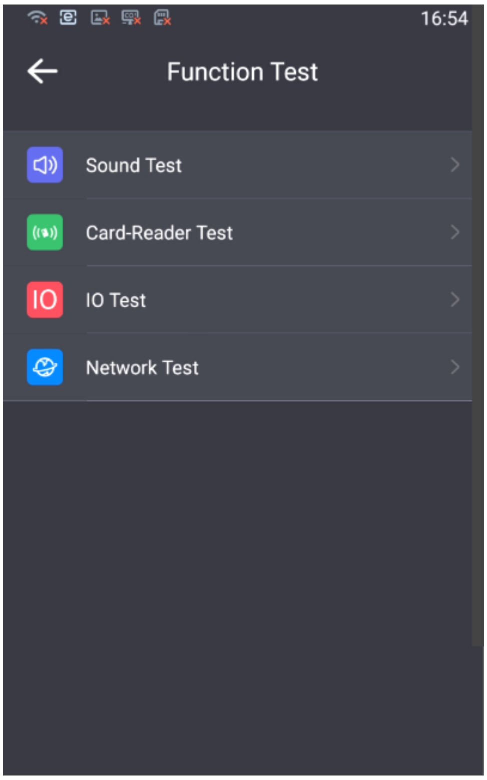
- Memory Strategy

Tap to select the memory strategy, options including “Overwrite” and “Stop on full disk”. If selecting “Overwrite”, when the memory is full, the device will overwrite the earliest data automatically; if selecting “Stop on full disk”, when the memory is full, the device will stop storing data.

After finishing configuration, tap “Save”.

2.10 Function Test

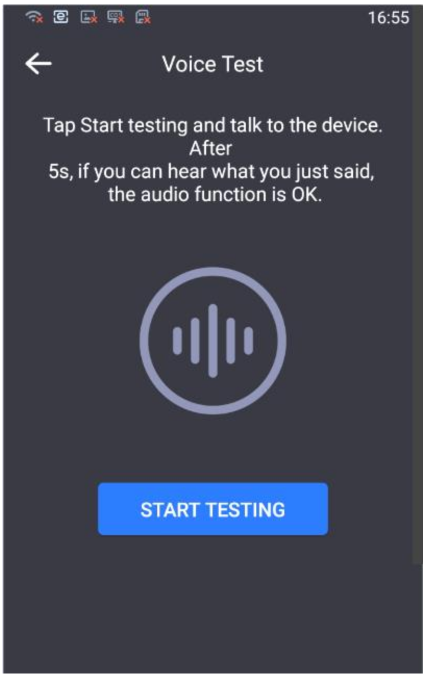
Tap **Menu > Function Test** and perform “Sound Test”, “Card-Reader Test”, “IO Test” and “Network Test”.



Picture 2-38 Function test

2.10.1 Sound Test

Tap **Menu > Function Test > Sound Test,** and test if the sound function of the device is OK.



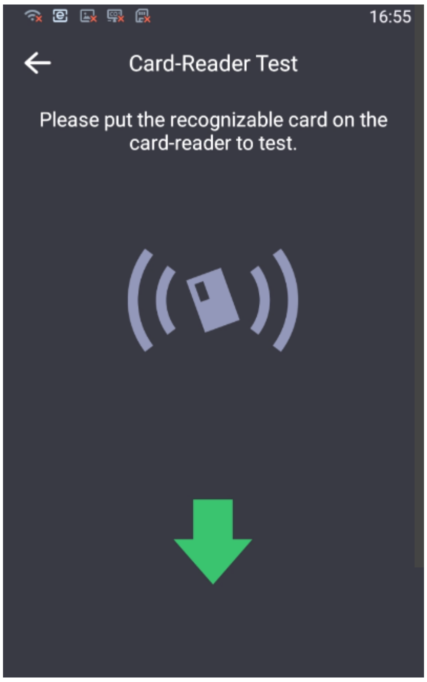
Tap Start testing and talk to the device. After 5s, if you can hear what you just said, the audio function is OK.

Picture 2-39 Sound test

Tap “Start Testing” and talk to the device. If you can hear what you said in 5 s normally, the sound function of the device is OK.

2.10.2 Card-Reader Test

Tap **Menu > Function Test > Card-Reader Test** and test if the card reader works normally.


16:55

Card-Reader Test

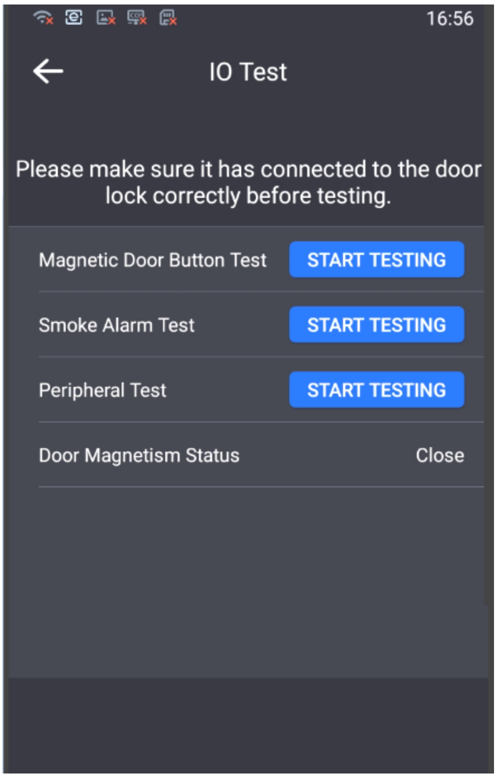
Please put the recognizable card on the card-reader to test.

Picture 2-40 Card reader test

Put a readable card at the card-reader area at the bottom of the device to test the card reading function. If the device reads the card normally, the card reading function is OK.

2.10.3 IO Test

Tap **Menu > Function Test > IO Test** and test if the door magnetism status is normal when door magnetic button, smoke sensor and peripheral device are triggered.



Please make sure it has connected to the door lock correctly before testing.

Magnetic Door Button Test	START TESTING
Smoke Alarm Test	START TESTING
Peripheral Test	START TESTING
Door Magnetism Status	Close

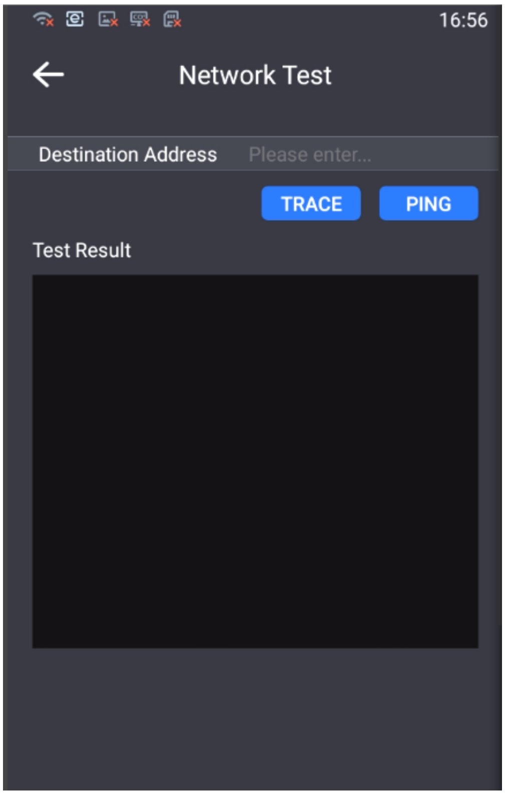
Picture 2-41 IO test

- Magnetic Door Button Test: Confirm the device is connected to the door lock correctly. Tap “Start Testing” and if the door lock is normal, the door magnetic button triggers normally.
- Smoke Alarm Test: Confirm the device is connected to the door lock correctly. Tap “Start Testing” and if the door lock is normal, the smoke sensor triggers normally.
- Peripheral Test: Confirm the device is connected to the door lock correctly. Tap “Start Testing” and if the door lock is normal, the peripheral device triggers normally.

The 3 tests can be performed simultaneously. After finishing, tap ← at the top left corner to return to “Function Test” interface.

2.10.4 Network Test

Tap **Menu > Function Test > Network Test** and test if the device is connected to the network successfully.

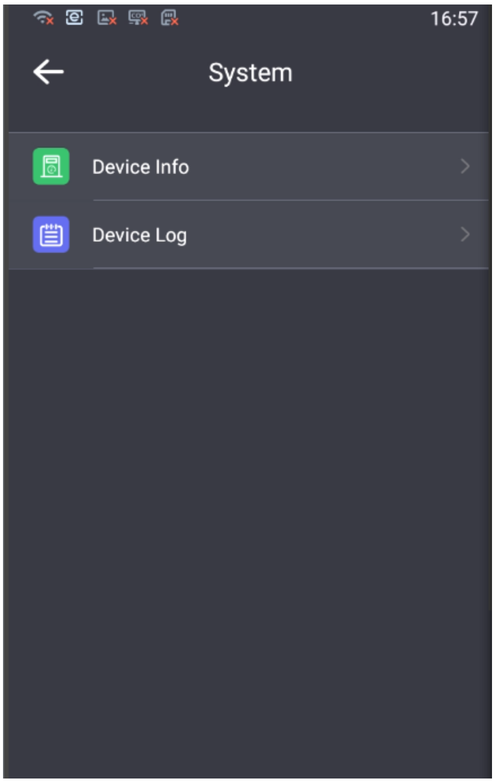


Picture 2-42 Network test

- In “Destination Address”, input the IP address of the destination device and tap “Ping” to display the result of accessing the destination IP address. It is used to test if the network between the device and the destination device is connected.
- In “Destination Address”, input the IP address of the destination device and tap “Trace” to display the routing entries of accessing the destination IP address. It is used to test the routing information of the network between the device and the destination device.

2.11 System

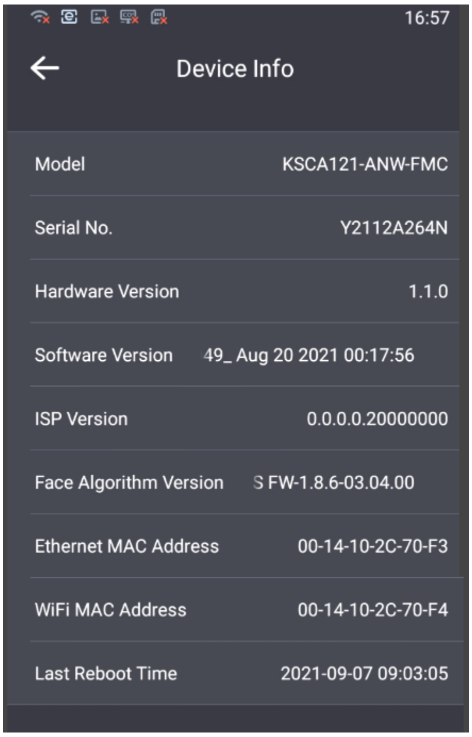
Tap **Menu > System,** and view device info and device log.



Picture 2-43 System

2.11.1 Device Info

Tap **Menu > System > Device Info** and view information such as “Model”, “Serial No.”, “Hardware Version”, “Software Version”, “ISP Version” and etc.

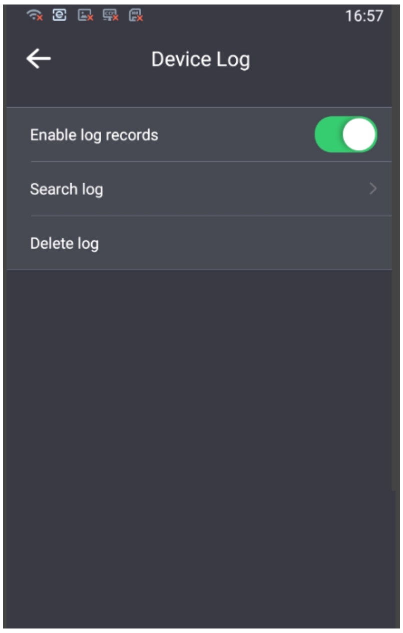


Model	KSCA121-ANW-FMC
Serial No.	Y2112A264N
Hardware Version	1.1.0
Software Version	49_ Aug 20 2021 00:17:56
ISP Version	0.0.0.0.20000000
Face Algorithm Version	S FW-1.8.6-03.04.00
Ethernet MAC Address	00-14-10-2C-70-F3
WiFi MAC Address	00-14-10-2C-70-F4
Last Reboot Time	2021-09-07 09:03:05

Picture 2-44 Device information

2.11.2 Device Log

Tap **Menu > System > Device Log** and configure device log.



16:57

Device Log

Enable log records

Search log

Delete log

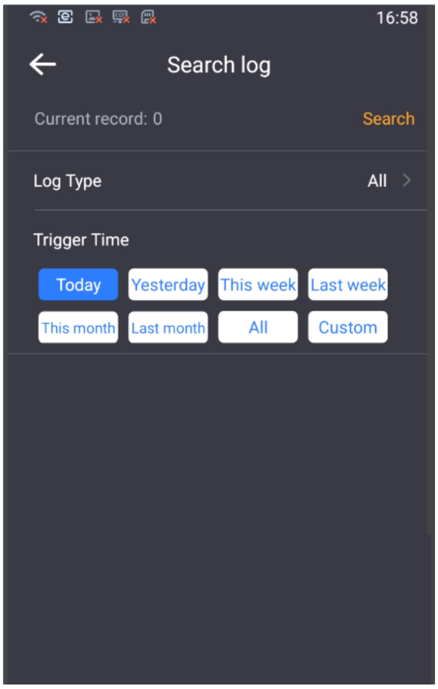
Picture 2-45 Device log

- ➢ Enable Log Records

Tap “Enable Log Records” and the device will record user operations, alarm messages, system tasks and system exception logs.

- ➢ Search Log

Tap “Search Log” to enter the log searching interface.



16:58

Search log

Current record: 0

Search

Log Type All

Trigger Time

Today Yesterday This week Last week

This month Last month All Custom

Picture 2-46 Search log

Tap “Log Type” and select a type, options including “All”, “User Operation”, “Alarm Message”, “System Task” and “System Exception”; select “Trigger Time”, options including “Today”, “Yesterday”, “This Week”, “Last Week”, “This Month”, “Last Month”, “All” and “Custom”. When selecting “Custom”, user needs to input “Start Time” and “End Time” manually; tap “Search” and view log information such as username, user IP address, log trogger time” amd log content.

- Delete Log

Tap “Delete Log” and select "Confirm" on the popup interface to delete device logs.

3. Web Client

3.1 Startup

For device installation and wiring, please refer to the *Quick Start Guide*.

After the device is installed, configure parameters and functions through the web client. Please ensure the mutual network communication between the device and the PC before configuring.

Note: User should be responsible for all risks of accessing the device to the Internet, including but not limited to possible cyber-attack, hacking attack, virus infection and etc. This company is not responsible for product failures and information disclosure caused thereby, but will provide timely technical support for the device.

Requirements of PC for installing the client:

- Processor: 3.3 GHz Intel CORE®i3 series and later version or other equivalent processors
- RAM Memory: 4GB or above
- Operating System: Windows 7 or later
- Browser: Suggest using IE Kernel browser, otherwise it will affect some functions of the client
- DirectX：9.0c

3.1.1 Activate

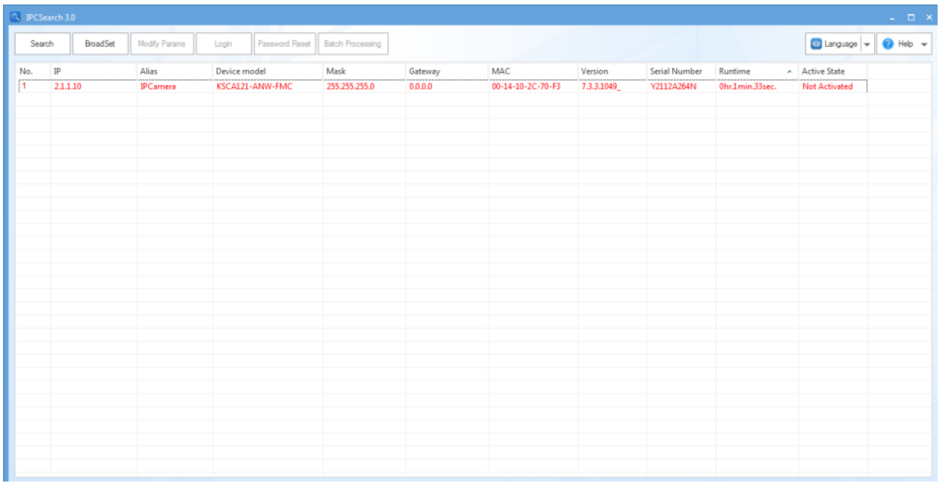
When the camera is first used, user should activate it and set the login password for normal use.

There are 3 methods to activate the device: though IPCSearch, through browser and through device.

- Activate through IPCSearch

1) Get IPCSearch from our website and install it according to the prompts (address: https://www.kedacom.com/cn/softtools/index.jhtml);

2) After finishing installation, run IPCsearch and the system will search the cameras in LAN and display the list as shown below.



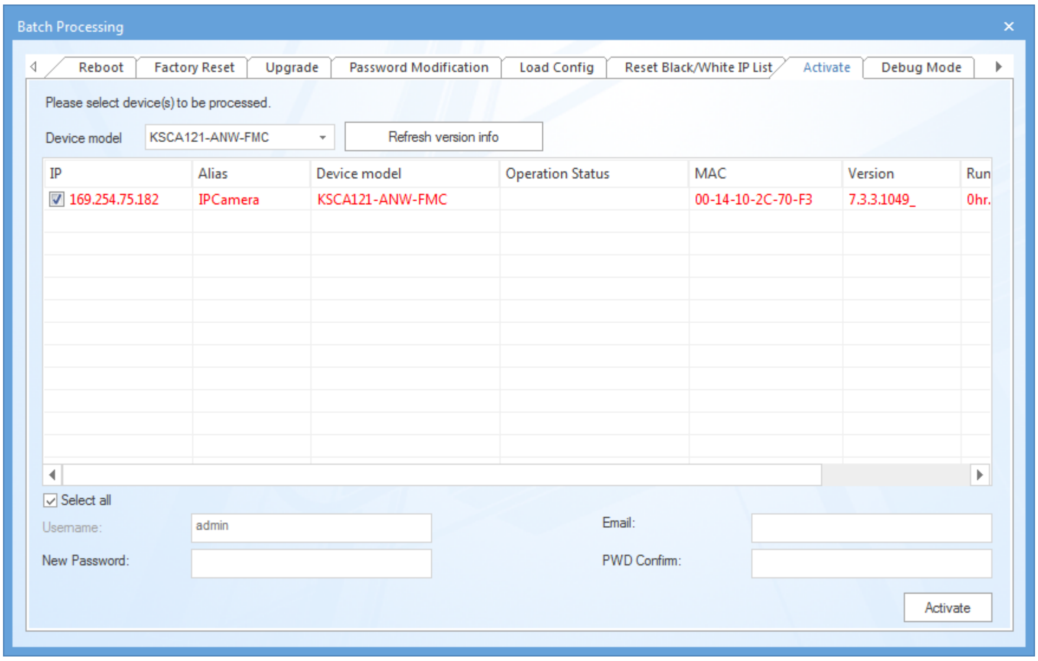
No.	IP	Alias	Device model	Mask	Gateway	MAC	Version	Serial Number	Runtime	Active State
1	2.1.1.10	IPCamera	KSCA121-ANW-FMC	255.255.255.0	0.0.0.0	00-14-10-2C-70-F3	7.3.3.1049_	Y2112A264N	0hr.1min.33sec.	Not Activated

Picture 3-1 IPCSearch

Note: Alias is subject to the actual search result.

3) Select the device to be activated, right click and select “Activate”. On the popup interface, configure admin user password and email for claiming password. Click “Activate” to activate the device.

Note: When there are more than one non-activated devices, select the device and click “**Batch processing**”. On the popup interface, set admin user’s password and the email address to claiming password. Click “**Activate**” and wait for rebooting.



Please select device(s) to be processed.

Device model: KSCA121-ANW-FMC

IP	Alias	Device model	Operation Status	MAC	Version	Run
☑ 169.254.75.182	IPCamera	KSCA121-ANW-FMC		00-14-10-2C-70-F3	7.3.3.1049_	0hr.

☑ Select all

Username: admin

Email:

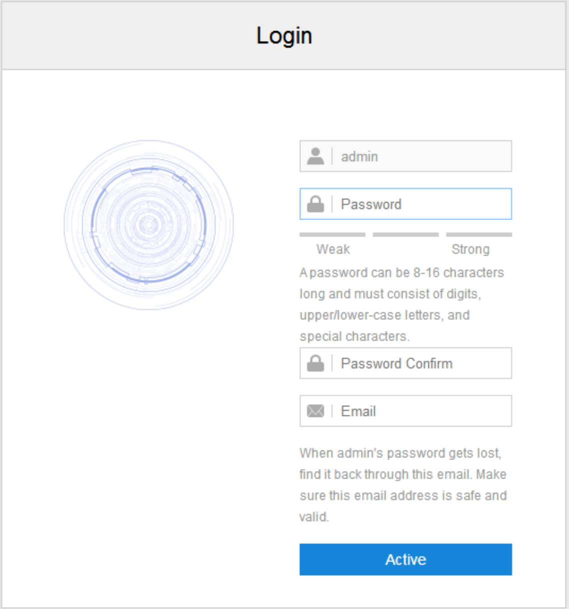
New Password:

PWD Confirm:

Picture 3-2 Batch Processing

- Activate through browser

1) Configure the IP address of PC in the same network segment as that of the camera and input the camera address http://device IP address:8080 in browser. The device activation interface will pop up, as shown below:



A password can be 8-16 characters long and must consist of digits, upper/lower-case letters, and special characters.

When admin's password gets lost, find it back through this email. Make sure this email address is safe and valid.

Picture 3-3 Activate through browser

2) Configure admin user password and email for claiming password. Click "Activate" to activate the device.

- Activate through device

  Start the device and it will prompt "Local Activation" automatically. Operate according to the prompts to finish activation. Please refer to chapter *2.1.1 Local Activation* for details.

Note:

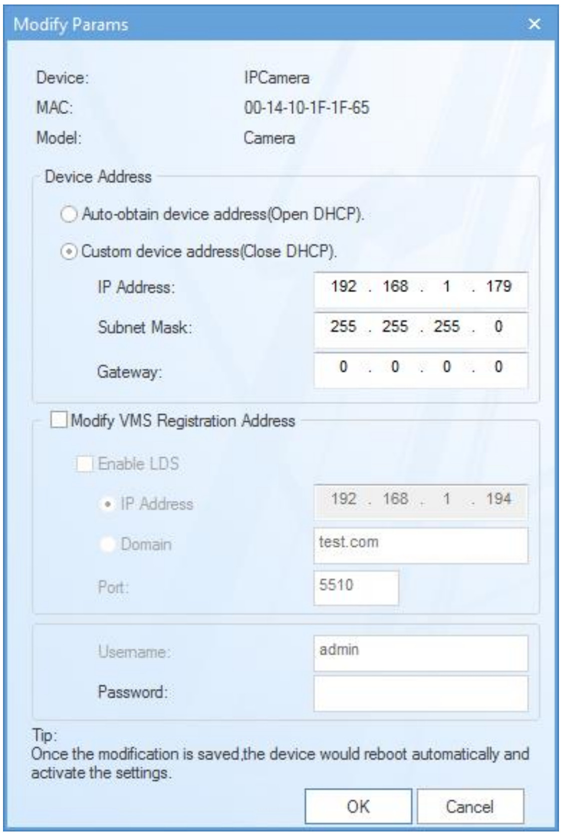
- To ensure the safety of device on internet, it is strongly recommended that you set a strong password composed of at least 2 kinds of the following, numbers, upper-case letters, lower-case letters or specific symbols with length of 8 to 16 characters.
- Please modify the password periodically such as once every 3 months. If the device is used in highly risky environment, suggest modifying the password monthly or weekly.
- Please keep your username and password safe.

3.1.2 Configure Network Parameters

After activating the camera, modify camera network parameters through IPCSearch, such as IP address, subnet mask and gateway.

1) Run IPCSearch and the system will search the cameras in LAN automatically and display the result on the list;

2) Select a device whose network parameters should be modified. Click “**Modify Params**” or right click the mouse. Modify parameters and fill admin user name (admin) and the password set when activating the device.



Modify Params

Device: IPCamera
MAC: 00-14-10-1F-1F-65
Model: Camera

Device Address

○ Auto-obtain device address(Open DHCP).
● Custom device address(Close DHCP).

IP Address: 192 . 168 . 1 . 179
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 0 . 0 . 0 . 0

□ Modify VMS Registration Address

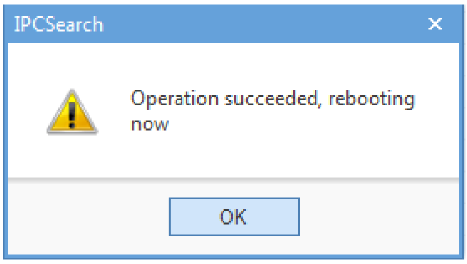
□ Enable LDS
● IP Address 192 . 168 . 1 . 194
○ Domain test.com
Port: 5510

Username: admin
Password:

Tip:
Once the modification is saved,the device would reboot automatically and activate the settings.

Picture 3-4 Modify Parameter

3) Click “OK” and the following window will pop up. Click “OK” and wait for the camera rebooting.



IPCSearch

Operation succeeded, rebooting now

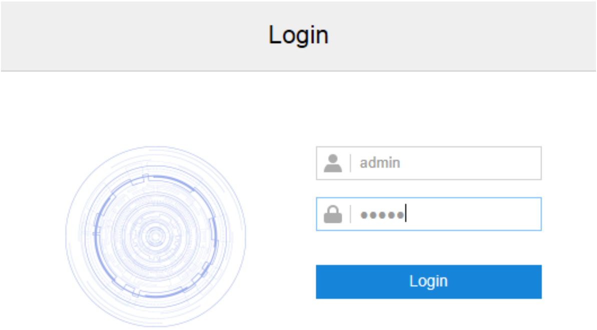
Picture 3-5 Camera Reboot

Note: For more network parameters of the device, login to the web client and configure. Please refer to chapter *3.3 Network* for details.

3.1.3 Log In and Log Out of the Web Client

- Log In to the Web Client

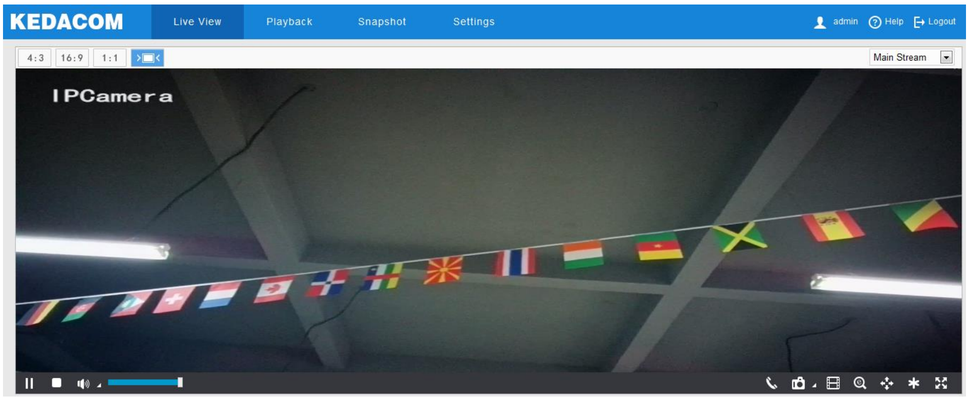
After activating the camera and modifying its network parameters, the camera will reboot automatically. After rebooting, input camera IP address “http://device IP address:8080" in the browser to enter the login interface. Input username and the password set during activation and click "**Login**".



Picture 3-6 Web Client Login Interface

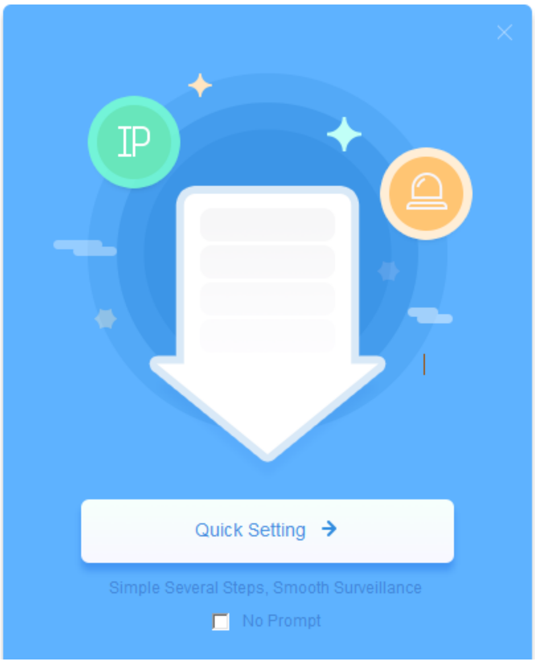
After login successfully for the first time, download and install the plug-in according to the prompts. Close the browser when installing the plug-in. After finishing, re-login and enter the following interface.

Note: Suggest using IE Kernel browser, otherwise it might affect some functions of the web client.

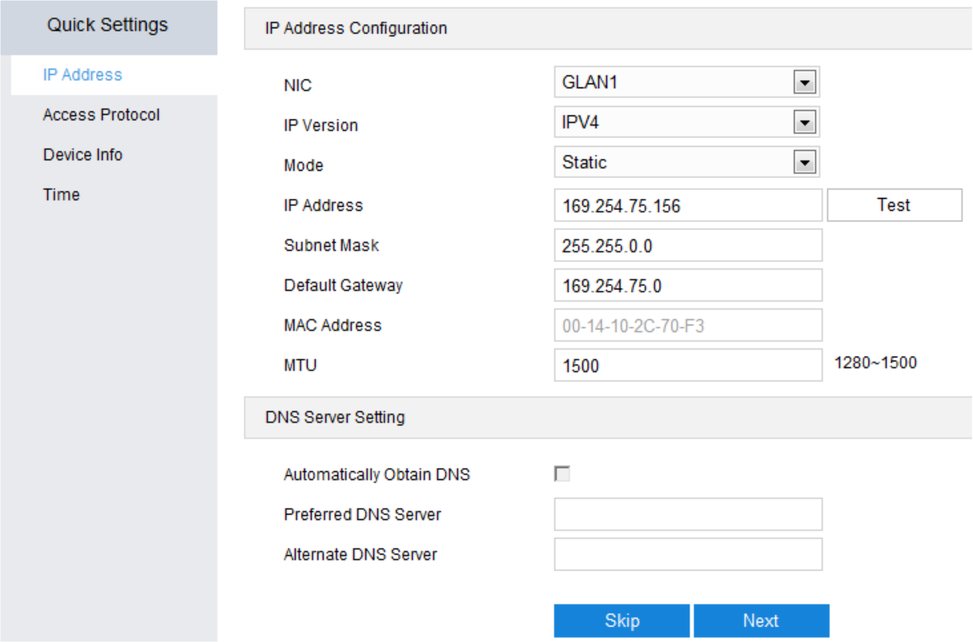


Picture 3-7 Web Client Interface

Note: After login to the web client successfully for the first time, it will pop up the quick setting interface. Click "Quick Setting" to perform simple settings to the camera. User can go to **Settings > Local Setting** and unselect "Enable Configuration Guide", or select "No Prompt" to cancel the prompt window.



Picture 3-8 Quick Setting



IP Address Configuration

NIC	GLAN1
IP Version	IPV4
Mode	Static
IP Address	169.254.75.156
Subnet Mask	255.255.0.0
Default Gateway	169.254.75.0
MAC Address	00-14-10-2C-70-F3
MTU	1500 1280~1500

DNS Server Setting

Automatically Obtain DNS	□
Preferred DNS Server	
Alternate DNS Server	

Picture 3-9 Unselect Configuration Guide

- Log Out of the Web Client

Click the icon Logout at the top right corner of the interface to log out of the web client.

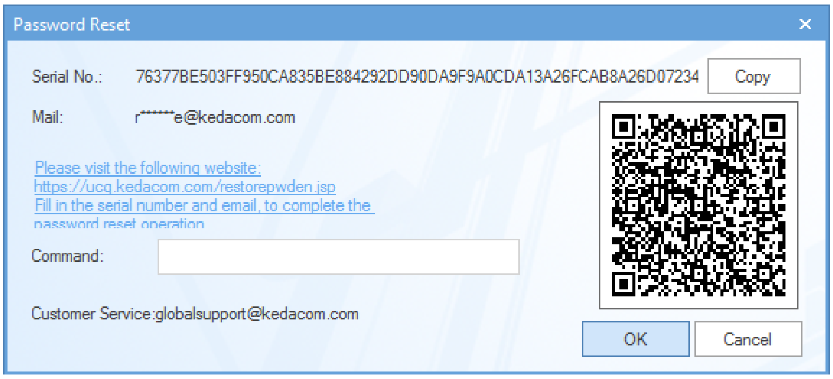
- Help

Click the icon Help at the top right corner of the interface to view the help file.

3.1.4 Reset Password

If user enters a wrong username or password for 6 times, the camera IP will be locked up for 10 minutes, during which user cannot login to this camera. If user forgets the password, reset the password.

1) Run IPCSearch and select the device whose password should be reset. Click "**Password Reset**" and a window will pop up, as shown below:



Password Reset

Serial No.: 76377BE503FF950CA835BE884292DD90DA9F9A0CDA13A26FCAB8A26D07234

Mail: r******e@kedacom.com

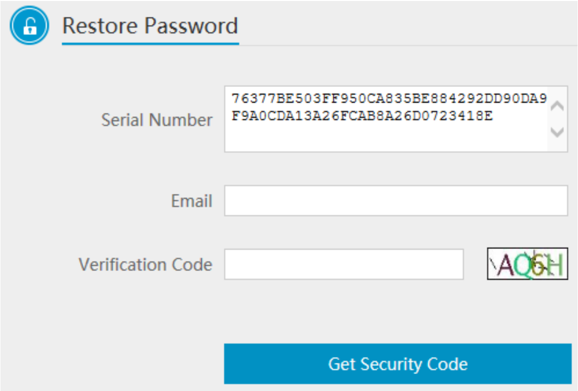
Please visit the following website:
https://ucq.kedacom.com/restorepwden.jsp
Fill in the serial number and email, to complete the password reset operation

Command:

Customer Service:globalsupport@kedacom.com

Picture 3-10 Password Reset

2) Click the password reset link or scan the QR code in Picture 3-10 with a mobile device and fill in the "Serial Number" and "Email" address set during activation. Click "Get Security Code" in the following picture;



Restore Password

Serial Number 76377BE503FF950CA835BE884292DD90DA9
F9A0CDA13A26FCAB8A26D0723418E

Email

Verification Code

Picture 3-11 Password Reset

3) Login to the email address to get a security code and fill in "**Command**" blank in Picture 3-10 and click "**OK**". Please remember the new password on the popup window and click "OK". The device will reboot.

3.1.5 Main Interface

On the main interface of the client, you can view live video, playback video records, manage snapshots and configure system settings.

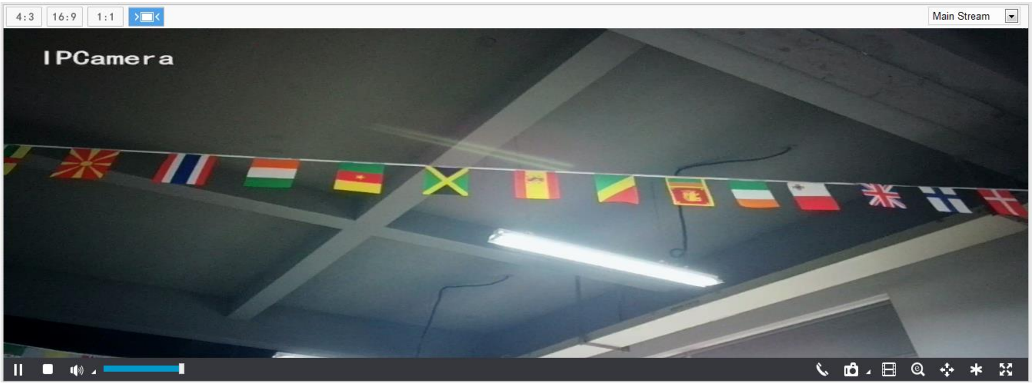
- Live View: preview camera live video and adjust parameters;
- Playback: search, playback and download video records by timeline or record types;
- Snapshot: search, view and download snapshots by picture type;

- Settings: configure camera functions and system parameters.

3.2 Basic Functions

3.2.1 Live View

Click “Live View” to enter the preview interface.



Picture 3-12 Live View

- Aspect Ratio

Icon	Function
4:3	The live view window displays image in standard screen ratio 4:3.
16:9	The live view window displays image in wide screen ratio of 16:9.
1:1	The live view window displays image in actual size 1:1.
>■<	The image window adaptive to your PC resolution.

- Stream Selection

Menu	Function
Main Stream	Display HD images.

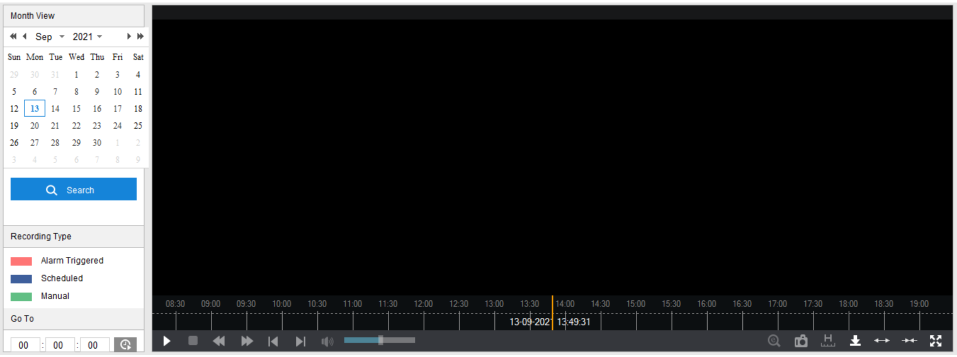
- Toolbar

Icon	Function
▶/⏸	Play/ Pause, click this button to play or pause a viewing.
■	Stop, click this button to stop live view.
🔊 ◢	Volume, the local decoding volume. Click 🔊 to enable to

	disable audio. Click ◢ to select audio channel.
▬	Drag the slide bar to adjust volume
☎	Click this button to call and talk to camera. Click again to stop talking.
📷 ◢	Snapshot, click 📷 to capture current image. Click ◢ to select camera snapshot or local snapshot. The former means the camera captures an image and sends it to local client; the latter means the web client captures an image and saves it locally.
🎞	Start/ Stop recording, click this button to start recording and click again to stop recording.
🔍	Click this icon to enable the e-PTZ function. Left click and drag toward lower right to draw an area. The pixels of this area will be amplified and will cover the whole screen. Left click and drag toward upper left to draw an area, then image will recover.
✥	PTZ, click the icon to zoom. Left click and drag toward lower right to draw an area. The pixels of this area will be amplified and will cover the whole screen. Left click and drag toward upper left to draw an area, then the image will recover. Double click a point in the image and the point will be centered.
📈	Status, click this button to display the frame rate and bitrate of the live video, and click again to hide. This button is hidden by default. To enable this function, go to Settings > Local Setting > Play, select “Display Status Info” and click “Save”.
✱	Video freeze, click this button and the image will freeze at the last frame before clicking. Click again to recover image.
⛶	Full screen, click this button to display in full screen. Double click in full screen or press Esc to exit.

3.2.2 Playback

Click “Playback” to enter the interface of recording management. User can search, view and download video records in TF card.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Picture 3-13 Playback

Operation steps:

1) Select recording duration from the calendar. If there is background color on a date, it means there is recording on that day;

2) Click "Search" and the video will be displayed directly in the timeline on the right (the highlight parts on the timeline);

ⓘ Note: Red means alarm video recordings, blue meaning scheduled video recordings and green meaning manual video recordings.

- Alarm recording: Enable video recording when an alarm event occurs such as motion detection triggered video recording. Go to **Settings > Event > Intelligent Function > Motion Detection**, and select linkage method(s).
- Scheduled recording: Enable video recording automatically during certain durations. Configure on the interface of **Settings > Storage > Recording**.
- Manual recording: When the network is disconnected from the platform, video recording will be enabled by default.

3) Click the "Play" button on the interface to playback the video recording. During the playback, user can perform operations such as clipping, accelerating and downloading the video recording;

4) Put the cursor of the mouse on the timeline to show the time of the video. Double-click or press the left button of the mouse and drag the timeline to the backward or forward to skip. Alternatively, enter a time under “Go To” and click ◷.

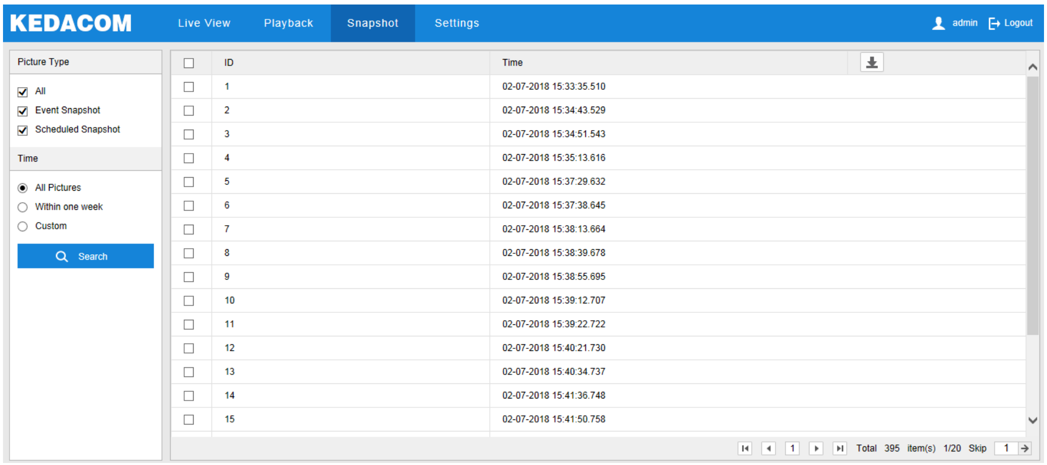
Buttons on the playback interface:

Icon	Function
▶/⏸	Play/ Pause, click the icon to play the video and click again to pause.
⏹	Stop, click the icon to stop playing the video.

⏪	Decelerate playing speed; click the icon to decelerate the speed of playing the video, one-click to decelerate by 1/2x and one more click by 1/4x, max by 1/8x.
⏩	Accelerate playing speed; click the icon to accelerate the speed of playing the video, one-click to accelerate by one time, max 8 times.
⏮	Previous video section, click the icon to play the previous video section and user can click it continuously. The default skipping time in a continuous video is 1 hour.
⏭	Next video section, click the icon to play the next video section and user can click it continuously. The default skipping time in a continuous video is 1 hour.
🔊	Volume, click the button to enable sound and click again to disable sound. Drag the slide bar to adjust volume.
🔍	ePTZ, click this icon to enable the ePTZ function. Left click and drag toward lower right to draw an area. The pixels of this area will be amplified and will cover the whole screen. Left click and drag toward upper left to draw an area, then image will recover.
📷	Snapshot, click the icon to capture current playback image. Save path for playback snapshots can be set in Settings > Local Setting.
H	Clip, click this icon to start clipping current video and click again to stop clipping. Save path for clipped playback videos can be set in Settings > Local Setting.
⬇	Download, click the icon to pop up the download interface. On the popup interface, configure the start time, end time and select video type(s) to download. Click "Search" to display expected videos on the list below. Select the files to be downloaded and click “Download”. User can view the download progress on the list. Save path for downloaded videos can be set in Settings > Local Setting.
↔/→←	Zoom in/ Zoom out timeline, adjust the scale interval on the timeline. Click the icons to zoom in or zoom out the timeline. The scale intervals on the timeline include 5 min, 10 min, 30 min, 1 hour and 2 hours. Zooming of the timeline will not affect the playback of current video.
⛶	Full screen, click this button to display the video in full screen. Double-click on the screen or press Esc to exit.

3.2.3 Snapshot

Click “Snapshot” to enter the interface of snapshot management. User can view or download snapshots in TF card.



Picture Type

☑ All
☑ Event Snapshot
☑ Scheduled Snapshot

Time

● All Pictures
○ Within one week
○ Custom

□	ID	Time
□	1	02-07-2018 15:33:35.510
□	2	02-07-2018 15:34:43.529
□	3	02-07-2018 15:34:51.543
□	4	02-07-2018 15:35:13.616
□	5	02-07-2018 15:37:29.632
□	6	02-07-2018 15:37:38.645
□	7	02-07-2018 15:38:13.664
□	8	02-07-2018 15:38:39.678
□	9	02-07-2018 15:38:55.695
□	10	02-07-2018 15:39:12.707
□	11	02-07-2018 15:39:22.722
□	12	02-07-2018 15:40:21.730
□	13	02-07-2018 15:40:34.737
□	14	02-07-2018 15:41:36.748
□	15	02-07-2018 15:41:50.758

1 Total 395 item(s) 1/20 Skip 1

Picture 3-14 Snapshot

Snapshot search and download steps:

1) Select required picture type(s) on the left checkboxes;

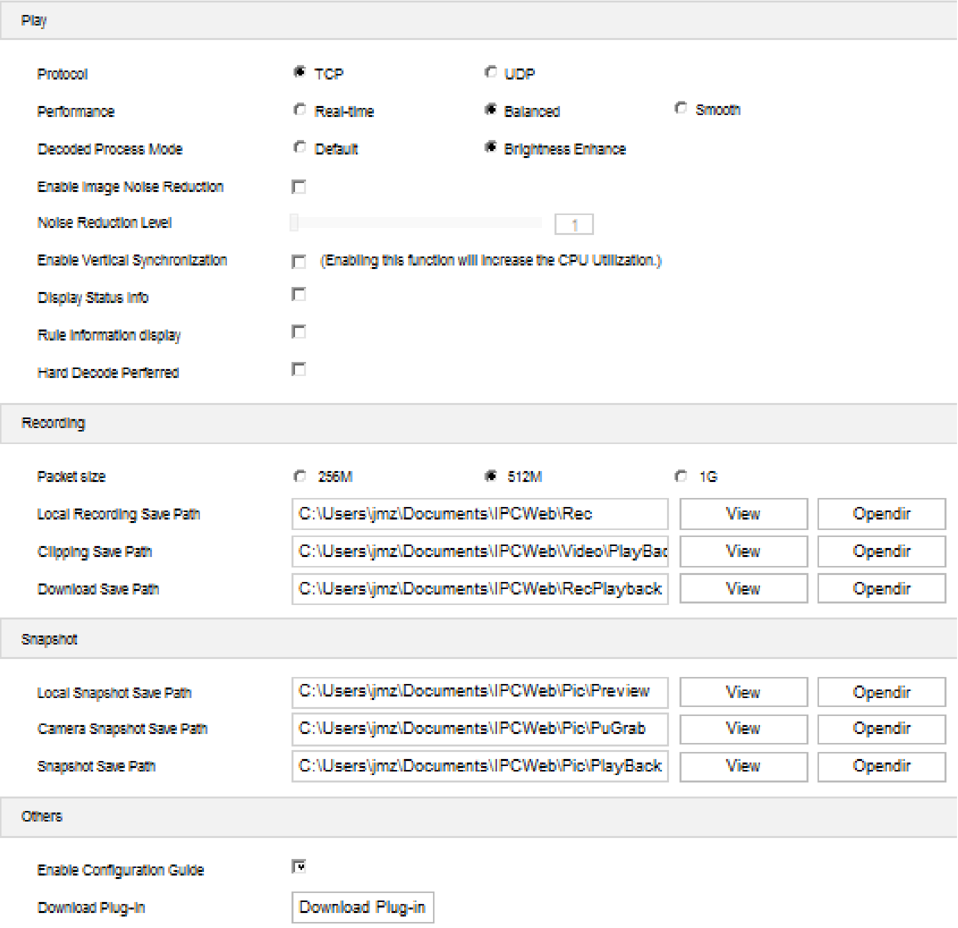
2) Select duration of snapshots from "Time". If selecting "Custom", specify the start time and end time;

3) Click "Search" and the search result will show on the right list, from which you can see picture ID and snapshot time;

4) Select pictures and click ⬇ to download the selected pictures. Snapshot save path can be set in **Local Setting > Camera Snapshot Save Path**.

3.2.4 Local Setting

Go to **Settings > Local Setting**, and configure parameters of video playing, the size and save path of video records and snapshots on local PC, as shown in the following picture.



Play

Protocol	● TCP	○ UDP	
Performance	○ Real-time	● Balanced	○ Smooth
Decoded Process Mode	○ Default	● Brightness Enhance	
Enable Image Noise Reduction	□		
Noise Reduction Level	1		
Enable Vertical Synchronization	□ (Enabling this function will increase the CPU Utilization.)		
Display Status Info	□		
Rule Information display	□		
Hard Decode Perferred	□		

Recording

Packet size	○ 256M	● 512M	○ 1G
Local Recording Save Path	C:\Users\jmz\Documents\IPCWeb\Rec	View	Opendir
Clipping Save Path	C:\Users\jmz\Documents\IPCWeb\Video\PlayBac	View	Opendir
Download Save Path	C:\Users\jmz\Documents\IPCWeb\RecPlayback	View	Opendir

Snapshot

Local Snapshot Save Path	C:\Users\jmz\Documents\IPCWeb\Pic\Preview	View	Opendir
Camera Snapshot Save Path	C:\Users\jmz\Documents\IPCWeb\Pic\PuGrab	View	Opendir
Snapshot Save Path	C:\Users\jmz\Documents\IPCWeb\Pic\PlayBack	View	Opendir

Others

Enable Configuration Guide	☑
Download Plug-in	Download Plug-in

Picture 3-15 Local setting

- Play

  - Protocol: Select the stream output protocol, options including UDP and TCP, default being TCP; UDP is applicable when the request for image quality is not high and the network is unstable.

  - Performance: Select playing level from "Real-time", "Balanced" and "Smooth", default being "Balanced". “Balanced” mode gives consideration of both real-time playing and smooth playing; “real-time” ensures the shortest latency of video playing but affects the smoothness of the video; “smooth” ensures smooth playing of the video but affects the real-time performance of the video.

  - Decoded Process Mode: Select the process mode after decoding, options including "Default" and "Brightness Enhance".

  - Enable Image Noise Reduction: Image noise reduction is decoding noise reduction. Select this option to enable image noise reduction and it only changes the viewing effect of current user. After selecting it, drag the slide bar below to adjust the noise reduction level, including 4 levels. The higher the level is, the more obvious the noise reduction will be. Usually it’s unnecessary to enable this option as it will cause streaking on moving objects.

  - Enable Vertical Synchronization: When there is image tearing, enable vertical synchronization to improve image quality. Usually it's unnecessary to enable this option as it will increase CPU utilization.
  - Display Status Info: After enabling this function, there will be a status icon in the menu bar at the bottom of the live view window. Click it to view frame rate, bitrate and packet loss rate.
  - Rule Information Display: If a device supports intelligent functions, when this option is selected, the settings on **Settings > Event > Intelligent Function** interfaces and on **Settings > Camera >Video > Video Info Overlay** interface will be shown in the intelligent zone on live view window such as the rule box and target box of guard line alarming, on which user can perform operations if necessary.

- Recording
  - Packet Size: Configure the size of single video recording saved locally, options including 256M, 512M and 1G.
  - Local Recording Save Path: Configure the local save path for recordings recorded during live viewing. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the recordings are saved currently.
  - Clipping Save Path: Configure the local save path for video clippings clipped during playback. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the clippings are saved currently.
  - Download Save Path: Configure the local save path for recordings downloaded during playback. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the recordings are saved currently.

- Snapshot
  - Local Snapshot Save Path: Configure the local save path for snapshots captured during live viewing. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the recordings are saved currently.
  - Camera Snapshot Save Path: Configure the local save path for snapshots downloaded from "Snapshot" interface. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the recordings are saved currently.

ⓘ Note:

- ♦ Camera Snapshot: Camera captures an image and sends it to local client. The image quality is good, but there is some time delay caused by network.

- ♦ Local Snapshot: Client captures an image and saves it locally. The image quality is ordinary, but there is no time delay.

- ■ Snapshot Save Path: Configure the local save path for snapshots captured during playback. Click the button of "View" to customize the save path. Click “Opendir” to open the folder where the recordings are saved currently.

➢ Others

- ■ Enable Configuration Guide: When it is selected, the configuration guide will pop up during login to lead the user to the quick settings interface. It is selected by default.

- ■ Download Plug-in: Log into the client through IE Kernel browser and click "Download Plug-in" to download the video plug-in. When logging into the web client for the first time, download and install the plug-in to view the live video normally.

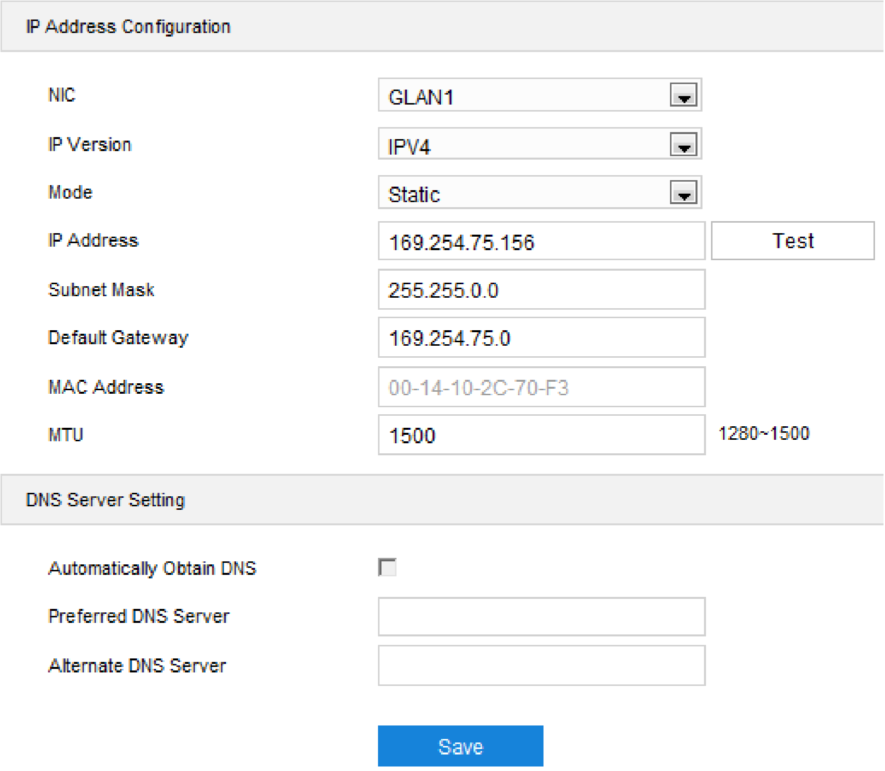
3.3 Network

Go to **Settings > Network** to configure IP and Port, Access Protocol and Other Protocols.

3.3.1 IP and Port

3.3.1.1 LAN

Go to **Settings > IP and Port > LAN**, and configure network parameters such as IP address, subnet mask, default gateway and etc.



IP Address Configuration

NIC	GLAN1	
IP Version	IPV4	
Mode	Static	
IP Address	169.254.75.156	Test
Subnet Mask	255.255.0.0	
Default Gateway	169.254.75.0	
MAC Address	00-14-10-2C-70-F3	
MTU	1500	1280~1500

DNS Server Setting

Automatically Obtain DNS	□
Preferred DNS Server	
Alternate DNS Server	

Picture 3-16 LAN

- IP Address Configuration

When the IP version is IPV4, select “Static” or “DHCP” mode. When selecting static mode, configure IP address, subnet mask and default gateway manually; when selecting DHCP mode, the system obtains IP address automatically;

When the IP version is IPV6, select “Manual” or “Automatically Obtain” mode. Under “Automatically Obtain” mode, the IPV6 IP address is distributed by network server, gateway or router; under manual mode, input the actual IP address, subnet mask and default gateway.

MTU: Maximum transmission unit, the maximum size of data packet transmitted through TCP/UDP protocol, ranging 500 ~ 1500 (unit: byte), by default 1500.

Note: The larger the MTU is, the higher communication efficiency and the longer transmission latency there will be. Please enter according to actual request.

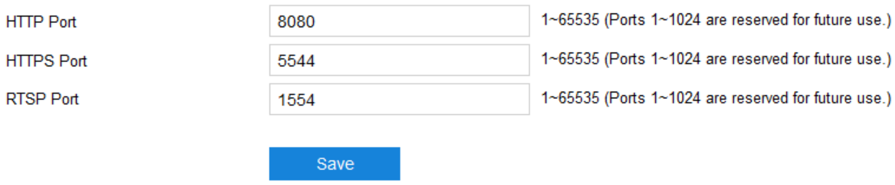
- DNS Server Setting

When the device needs to access by domain name, user needs to configure the correct DNS server address, options including “Automatically Obtain DNS” and entering DNS server address manually. If selecting “Automatically Obtain DNS”, the device will obtain DNS server parameters automatically from the gateway.

Click “Save” to validate settings.

3.3.1.2 Port

Go to **Settings > Network > IP and Port > Port**, and configure HTTP Port, HTTPS Port and RTSP Port. Please configure corresponding ports by request.



HTTP Port	8080	1~65535 (Ports 1~1024 are reserved for future use.)
HTTPS Port	5544	1~65535 (Ports 1~1024 are reserved for future use.)
RTSP Port	1554	1~65535 (Ports 1~1024 are reserved for future use.)

Picture 3-17 Port

- **HTTP Port:** Hypertext Transport Protocol Port. When login through browser, you need to add a port number behind camera IP address. For example, if HTTP port is edited as 83, when you login through browser, you need to input "http://camera IP address:83. The number is 8080 by default, ranging 1 ~ 65535.
- **HTTPS Port:** Hypertext Transport Protocol Secure Port based on SSL. When login through browser, you need to add a port number behind

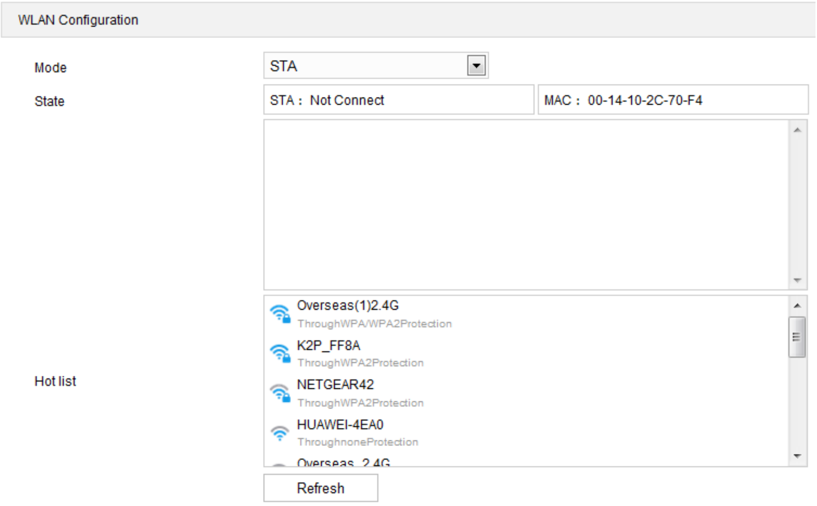
camera IP address. For example, if HTTPS port is edited as 5545, when you login through browser, you need to input "http://camera IP address:5545. The number is 5544 by default, ranging 1 ~ 65535.

- **RTSP Port:** Real Time Streaming Protocol Port. Make sure that the port you are editing is available. When the RTSP port number is edited as 1555, enter “rtsp://camera IP address:1555/id=0 (id=0 play main stream, id=1 play secondary stream)” in the browser. RTSP port number is 1554 by default, ranging 1 ~ 65535.

Click “Save” to validate settings.

3.3.1.3 Wireless

Go to **Settings > Network > IP and Port > Wireless**, and view wireless network status and configure wireless connection.



WLAN Configuration

Mode: STA

State: STA : Not Connect | MAC : 00-14-10-2C-70-F4

Hot list:
- Overseas(1)2.4G ThroughWPA/WPA2Protection
- K2P_FF8A ThroughWPA2Protection
- NETGEAR42 ThroughWPA2Protection
- HUAWEI-4EA0 ThroughnoneProtection
- Overseas_2.4G

Picture 3-18 Wireless

WLAN mode includes “Close” and “STA”. When it’s necessary to enable wireless network, select “STA” mode.

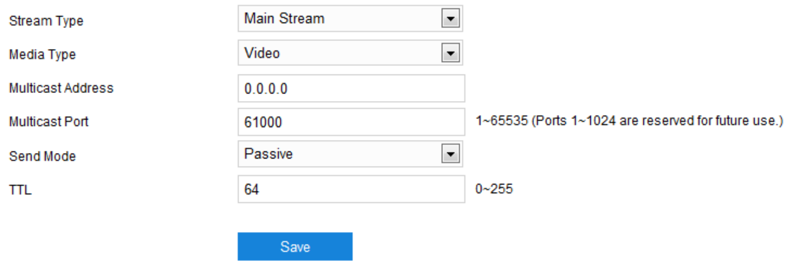
Operation steps are as follows:

1) Select “STA” mode and click “Refresh” to refresh hot list;
2) On the hot list, select the expected hotspot name and click the add icon + on the right;
3) Enter password on the popup window and select “Show advanced options”;
4) The IP address mode is by default “DHCP”. If selecting static IP, enter IP address, subnet mask and default gateway manually;
5) Click “Save” to connect to the specific hotspot.

3.3.1.4 Multicast

Go to **Settings > Network > IP and Port > Multicast**, and configure parameters such as stream type, media type, multicast address.

ⓘNote: Multicast is a method of data packet transmission. The source host can send the data packets to every host in the group by sending a datagram only. It also depends on the group relationship maintenance and selection by the router.



Stream Type	Main Stream	
Media Type	Video	
Multicast Address	0.0.0.0	
Multicast Port	61000	1~65535 (Ports 1~1024 are reserved for future use.)
Send Mode	Passive	
TTL	64	0~255

Picture 3-19 Multicast

- Stream Type: the stream to be sent, the default being “Main Stream”.
- Media Type: the media type of the stream to be sent, the default being “Video”.
- Multicast Address: the address to send the stream, fill it according to the actual conditions.
- Multicast Port: the multicast port of the multicast address, the default being 61000, ranging 1 ~ 65535.
- Send Mode: options include “Passive” and “Initiative”. Under “Initiative” mode, if the multicast addres is normal and valid, the default setting is to send stream to this multicast address; under “Passive” mode, only when receiving the request of multicast can the system send stream to the multicast address. If the address is set 0.0.0.0, the system will send stream to 239.2.2.2 by default.
- TTL: Time to Live, ranging 0~255.

ⓘNote: TTL means the maximum number of network segments allowed to pass through IP data packet before it is discarded by the router. It is used to avoid endless loop of sending and receiving the data packet in the network so as to save network resources.

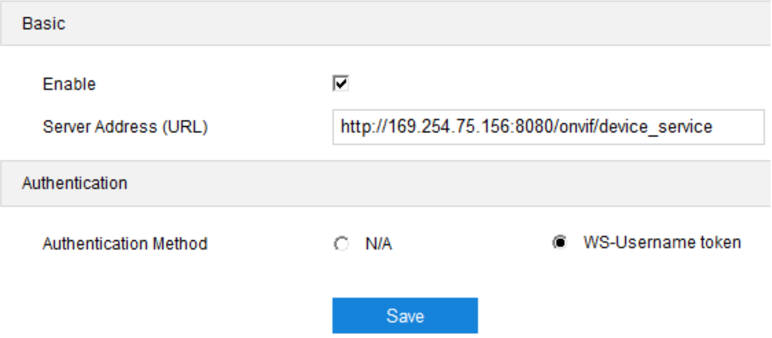
3.3.2 Access Protocol

Go to **Settings > Network > Access Protocol**, and configure protocols such as VSIP, ONVIP and SIP to access the device to the platforms.

3.3.2.1 ONVIF

The client supports adding device to the back-end platform through ONVIF protocol, which enables different network video products such as cameras and recorders from different manufacturers to communicate with each other. Configuration steps are as follows:

1) Go to **Settings > Network > Access Protocol > ONVIF**;



Basic

Enable ☑

Server Address (URL) http://169.254.75.156:8080/onvif/device_service

Authentication

Authentication Method ○ N/A ● WS-Username token

Picture 3-20 ONVIF

2) Select “Enable”. Afterwards, the device will generate a server address (URL) automatically, default port number being 80;

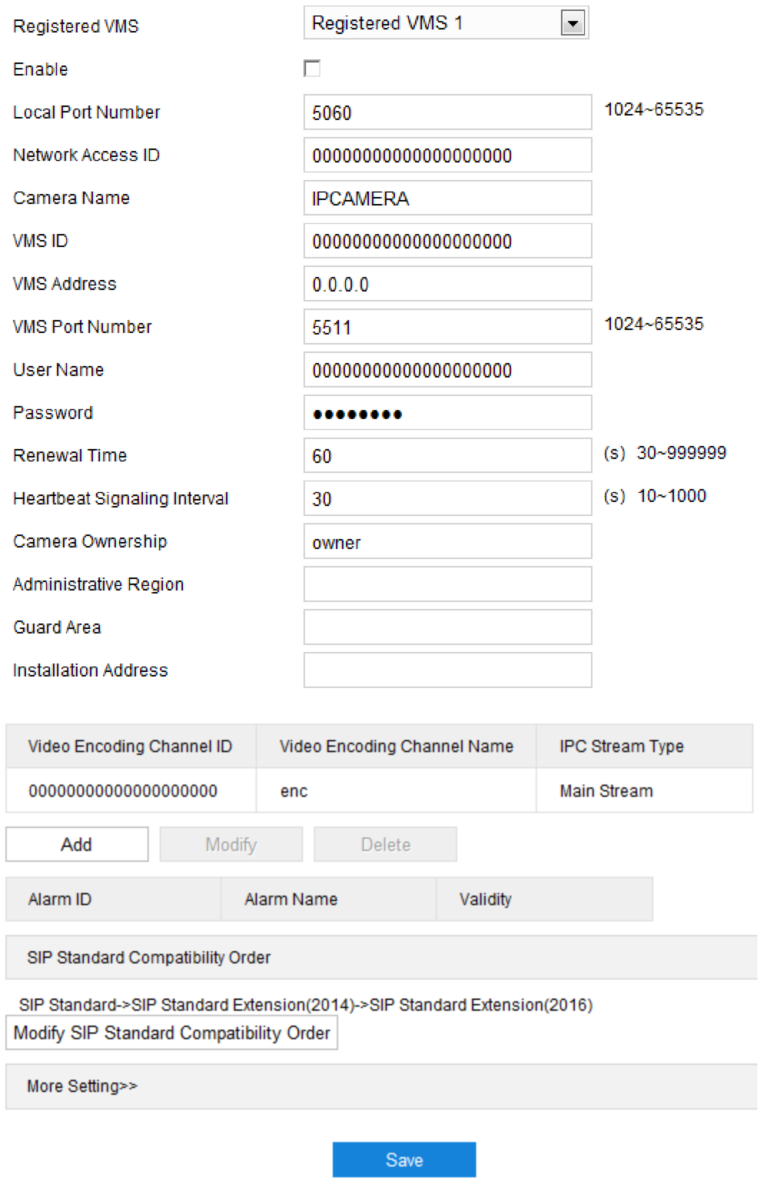
3) Set authentication method for ONVIF login. When selecting "N/A", user can login freely; when selecting "WS-Username token", user needs to verify username and password before login;

4) Click “Save” to validate settings.

3.3.2.2 SIP

The device can be registered to GB platform through web client. Configuration steps:

1) Go to **Settings > Network > Access Protocol > SIP**;



Registered VMS	Registered VMS 1	
Enable	□	
Local Port Number	5060	1024~65535
Network Access ID	00000000000000000000	
Camera Name	IPCAMERA	
VMS ID	00000000000000000000	
VMS Address	0.0.0.0	
VMS Port Number	5511	1024~65535
User Name	00000000000000000000	
Password	●●●●●●●●	
Renewal Time	60	(s) 30~999999
Heartbeat Signaling Interval	30	(s) 10~1000
Camera Ownership	owner	
Administrative Region		
Guard Area		
Installation Address		

Video Encoding Channel ID	Video Encoding Channel Name	IPC Stream Type
00000000000000000000	enc	Main Stream

Alarm ID	Alarm Name	Validity

SIP Standard Compatibility Order

SIP Standard->SIP Standard Extension(2014)->SIP Standard Extension(2016)

Picture 3-21 SIP

2) Select the “Registered VMS”;

3) Select “Enable”;

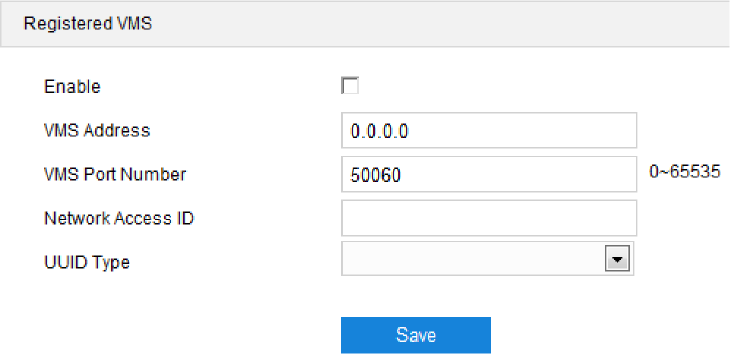
4) Enter parameters such as network access ID, VMS ID, VMS address, VMS port number, user name/password and video encoding channel ID, which are all provided by VMS;

5) Click “Save” to validate settings.

3.3.2.3 DPSS

When access the device to DPSS platform, configure DPSS parameters.

1) Go to **Settings > Network > Access Protocol > DPSS**;



Registered VMS

Enable	□	
VMS Address	0.0.0.0	
VMS Port Number	50060	0~65535
Network Access ID		
UUID Type		

Picture 3-22 DPSS

2) Select "Enable";

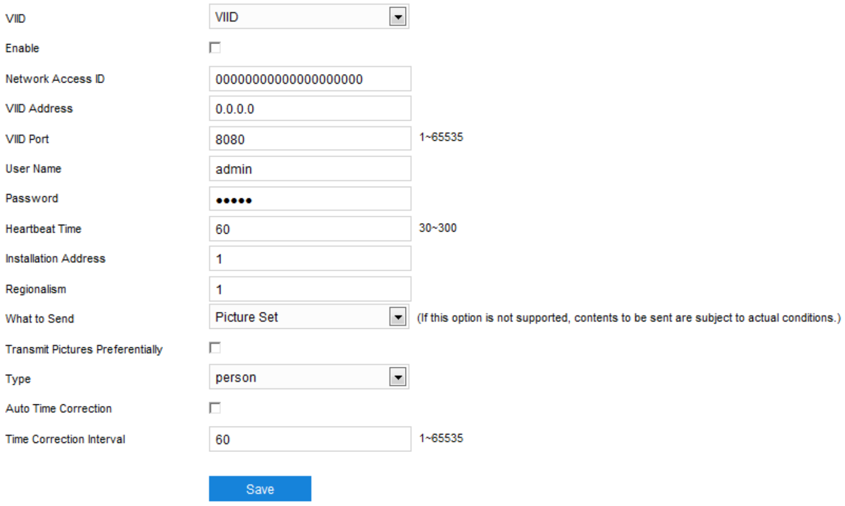
3) Enter VMS address, port number and network access ID, and select UUID type from the dropdown list;

4) Click "Save" to validate settings.

3.3.2.4 VIID

The device can upload the captured snapshots to VIID platform for future data analysis and comparison. Configuration steps are as follows:

1) Go to **Settings > Network > Access Protocol > VIID**;



VIID	VIID	
Enable	□	
Network Access ID	00000000000000000000	
VIID Address	0.0.0.0	
VIID Port	8080	1~65535
User Name	admin	
Password	●●●●●	
Heartbeat Time	60	30~300
Installation Address	1	
Regionalism	1	
What to Send	Picture Set	(If this option is not supported, contents to be sent are subject to actual conditions.)
Transmit Pictures Preferentially	□	
Type	person	
Auto Time Correction	□	
Time Correction Interval	60	1~65535

Picture 3-23 VIID

2) Select "Enable" to enable VIID access;

3) Enter VIID platform ID in "Network Access ID";

4) Enter VIID IP address and port number in "VIID Address" and "VIID Port";

5) Enter VIID user name and password in "User Name" and "Password";

6) Heartbeat interval is used to detect abnormal disconnection of TCP. Usually it sends simple communication packets periodically. If the system does not receive any response from the other side in the configured

interval, it will judge the other side has been disconnected. For example, if the parameter is set 30, the system will send the packet once every 30 s;

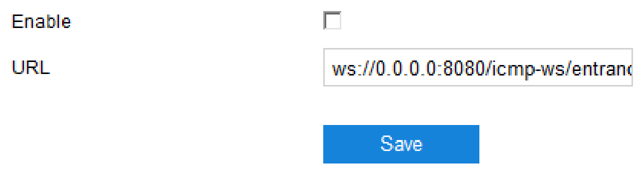
7) Enter installation address and regionalism if necessary for device positioning;

8) Click “Save” to validate settings.

3.3.2.5 COI

The device can be connected to the COI platform server and be managed by the platform. Configuration steps are as follows:

1) Go to **Settings > Network > Access Protocol > COI**;



Enable	□
URL	ws://0.0.0.0:8080/icmp-ws/entranc

Picture 3-24 COI

2) Select “Enable”;

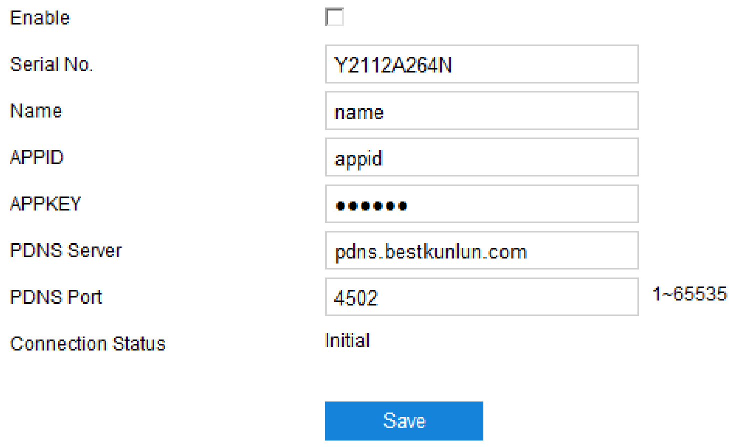
3) Enter URL;

4) Click “Save” to validate settings.

3.3.2.6 PDNS

When the device is registered to PDNS platform, user can login to the web client through PDNS platform. Configuration steps are as follows:

1) Go to **Settings > Network > Access Protocol > PDNS**;



Enable	□	
Serial No.	Y2112A264N	
Name	name	
APPID	appid	
APPKEY	••••••	
PDNS Server	pdns.bestkunlun.com	
PDNS Port	4502	1~65535
Connection Status	Initial	

Picture 3-25 PDNS

2) Select “Enable” to enable PDNS access;

3) Enter device SN and name in “Serial No.” and “Name”;

4) Enter APP ID and password in “APPID” and “APPKEY”;

5) Enter PDNS IP address and port number in “PDNS Server” and “PDNS Port”;

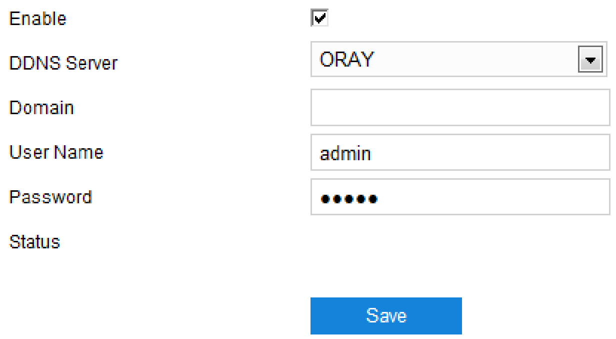
6) Click “Save” to finish setting and show connection status.

3.3.3 Other Protocols

3.3.3.1 DDNS

DDNS (Dynamic Domain Name Server) is to connect the device to various servers so that user can login to the device through servers. Apply domain names at different server websites and then visit the device by domain names directly even if the IP address has been modified, which solves the problem of visiting the device through public network. Configuration steps are as follows:

1) Go to **Settings > Network > Other Protocols > DDNS**;



Enable ☑

DDNS Server: ORAY

Domain:

User Name: admin

Password: ●●●●●

Status

Picture 3-26 DDNS

2) Select "Enable";

3) Select DDNS server type, options including “ORAY”, “DYNDNS” and “NOIP”. When selecting “DYNDNS” or “NOIP”, enter device domain name;

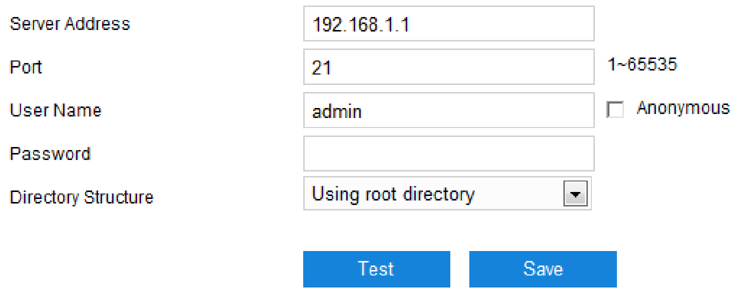
4) Enter user name and password according to the selected DDNS server;

5) Click "Save" to validate setting and show connection status.

3.3.3.2 FTP

The web client supports FTP protocol and user can upload snapshots of the device to specific FTP server. Configuration steps are as follows:

1) Go to **Settings > Network > Other Protocols > FTP;**



Server Address	192.168.1.1	
Port	21	1~65535
User Name	admin	□ Anonymous
Password		
Directory Structure	Using root directory	

Picture 3-27 FTP

2) Input FTP “Server Address” and “Port”;

3) Input “User Name” and “Password” of users who have the authority to upload. If an anonymous user also has the authority to upload, select "Anonymous" to visit FTP server anonymously;

4) Configure directory structure, i.e. the file save path. Select from the dropdown list by actual request, options including “Using root directory”, “Use level one directory” and “Use level two directory”;

- Options for level-one directory include “Use device name”, “Using device IP” and “Custom”;
- Options for level-two directory include “Use channel number” and “Custom”.

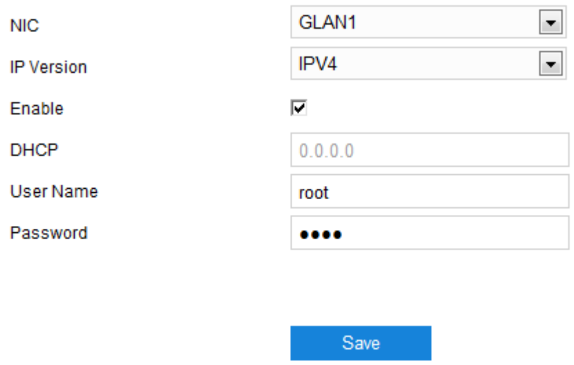
5) Click "Test" to verify if current FTP is available, and the result will show on the popup dialogue box;

6) Click "Save" to validate setting.

3.3.3.3 PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) function is to access camera to the internet by dialing the account provided by ISP (Telecom, Unicom and CMCC). Configuration steps are as follows:

1) Go to **Settings > Network > Other Protocols > PPPoE**;



NIC	GLAN1
IP Version	IPV4
Enable	☑
DHCP	0.0.0.0
User Name	root
Password	••••

Picture 3-28 PPPoE

2) Select NIC and IP version;

3) Select "Enable" to enable PPPoE dialing function;

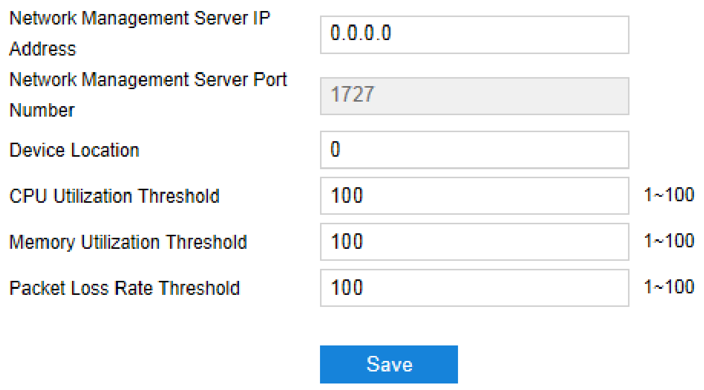
4) Input user name and password provided by ISP;

5) Click "Save" to validate setting. It will show dynamic IP after dialing succeeds.

3.3.3.4 K-SNMP

K-SNMP is KEDACOM private network management protocol. Configuration steps are as follows:

1) Go to **Settings > Network > Other Protocols > K-SNMP**;



Network Management Server IP Address	0.0.0.0	
Network Management Server Port Number	1727	
Device Location	0	
CPU Utilization Threshold	100	1~100
Memory Utilization Threshold	100	1~100
Packet Loss Rate Threshold	100	1~100

Picture 3-29 K-SNMP

2) Input "Network Management Server IP Address" and "Device Location";

3) Configure "CPU Utilization Threshold", "Memory Utilization Threshold" and "Packet Loss Rate Threshold". The default values are all 100, ranging 1 ~ 100;

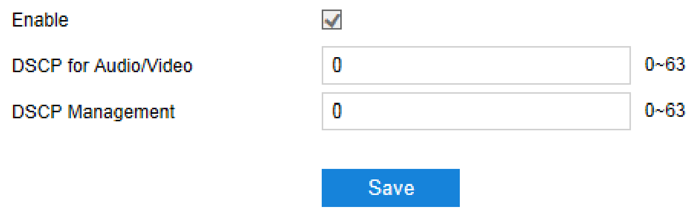
4) Click "Save" to validate setting.

3.3.3.5 QoS

QoS stands for Quality of Service, which can solve the problem of network latency and network congestion efficiently. Configuration steps are as follows:

Note: QoS function needs support of network device on the transmission path such as router or switch.

1) Go to **Settings > Network > Other Protocols > QoS**;



Enable	☑	
DSCP for Audio/Video	0	0~63
DSCP Management	0	0~63

Picture 3-30 QoS

2) Select “Enable” to enable QoS function;

3) Configure "DSCP for Audio/Video" and “DSCP Management”, ranging 0 ~ 63;

Note: There are 64 DSCP priority levels (0-63), which identify different priority levels of packets, 0 with the lowest priority and 63 with the highest. Select and keep packets according to their priority levels. Different levels occupy different bandwidths with different packet loss rates during network congestion, thus the quality of service is ensured.

Attention: During configuration, the same parameters should be set at router end.

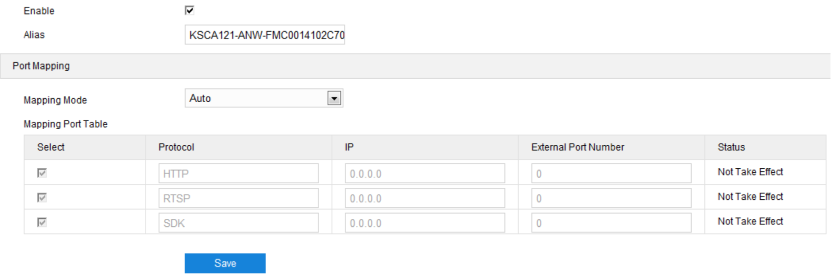
4) Click "Save" to validate setting.

3.3.3.6 UPnP

By UPnP protocol, it's able to set up mapping relation between private network and the internet. Internal port is camera port while external port is router port. User can visit camera when accessing to the external port. Configuration steps are as follows:

Note: For a camera in an Ethernet, UPnP function can make gateway or router perform auto-port-mapping which maps the camera monitor port from gateway or router to the Ethernet device, thus the firewall module on the gateway or router starts to open this port to other PCs on the internet.

1) Go to **Settings > Network > Other Protocols > UPnP**;



Enable ☑

Alias KSCA121-ANW-FMC0014102C70

Port Mapping

Mapping Mode Auto

Mapping Port Table

Select	Protocol	IP	External Port Number	Status
☑	HTTP	0.0.0.0	0	Not Take Effect
☑	RTSP	0.0.0.0	0	Not Take Effect
☑	SDK	0.0.0.0	0	Not Take Effect

Picture 3-31 UPnP

2) Select “Enable” to enable UPnP function;

3) Set alias, then user can search the alias directly from the network on PCs which have enabled UPnP protocol in the broadcast domain of the same Ethernet. Double-click the icon and the system will pop up a page automatically for user to visit current IP address;

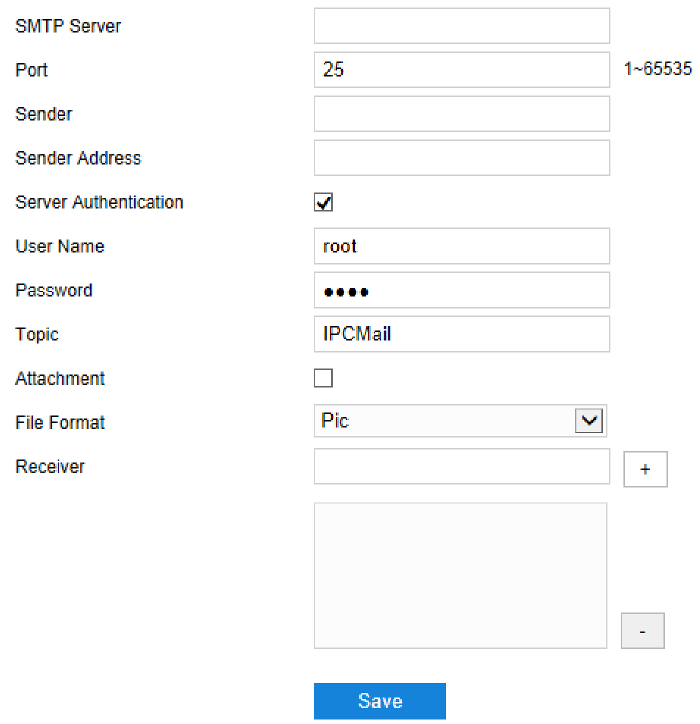
4) Select "Auto" or "Manual" for mapping mode. When selecting “Manual”, enter “External Port Number” manually;

5) Click "Save" to validate setting.

3.3.3.7 SMTP

SMTP stands for Simple Message Transfer Protocol. When an alarm is triggered, the system will send email notification automatically through SMTP protocol. Configuration steps are as follows:

1) Go to **Settings > Network > Other Protocols > SMTP**;



SMTP Server		
Port	25	1~65535
Sender		
Sender Address		
Server Authentication	☑	
User Name	root	
Password	••••	
Topic	IPCMail	
Attachment	□	
File Format	Pic	
Receiver		+
		-

Picture 3-32 SMTP

2) Input SMTP server IP address and port number, which ranges 1 ~ 65535, 25 by default;

3) Input "Sender" and "Sender Address"; optionally select "Server Authentication" and input correct user name and password;

4) Input email topic; optionally select "Attachment" and choose attached file format, then the email sent will attach the relative file;

5) Add receiver email address. Input the receiver's email address and click the symbol "+" behind it and the address will be saved to the list below. Select an address from the list and click the symbol "-" to remove the email address;

6) Click "Save" to validate setting.

ⓘ Note: This function is available only when email notification is enabled.

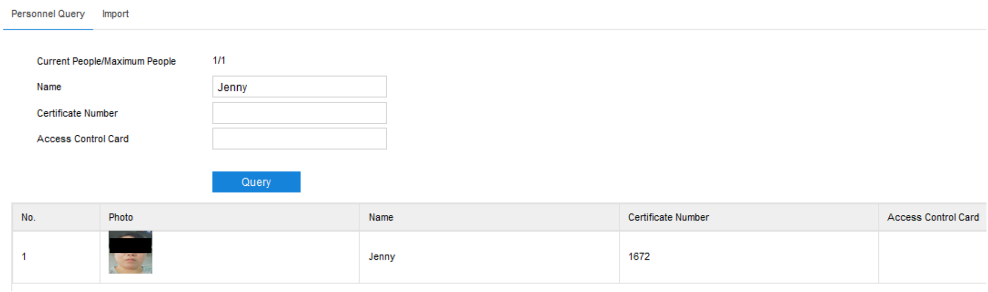
3.4 Access Control

3.4.1 Personnel

- Personnel Query

Go to **Settings > Access Control > Personnel > Personnel Query**, and query personnel info.

Enter anyone or more of the information such as name, certificate number and access control card, and click “Query” to search the expected personnel info.



Current People/Maximum People 1/1

Name Jenny

Certificate Number

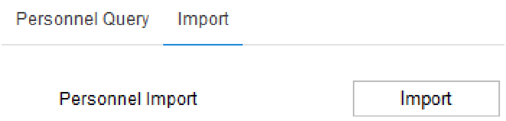
Access Control Card

No.	Photo	Name	Certificate Number	Access Control Card
1	[redacted]	Jenny	1672	

Picture 3-33 Personnel query

- Import

Go to **Settings > Access Control > Personnel > Import,** and import personnel info.



Picture 3-34 Personnel import

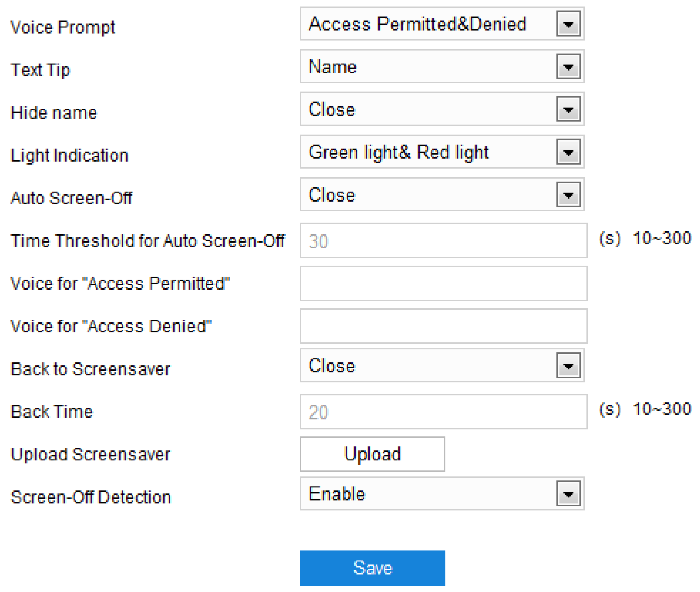
Click “Import” to pop up the prompt box “Would you like to import personnel info?” Click “Confirm” and browse and open the compressed file of personnel info to finish. Please refer to chapter *Appendix: Personnel Import Through Web Client* for details.

Note:

- If there is a person in the imported file with the same certificate number as that of a registered person, the info of the registered person will be updated by the imported info.
- If the total number of registered personnel after importing exceeds the maximum capacity of the device, the importing will fail.

3.4.2 Settings

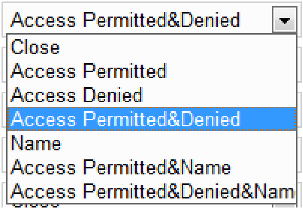
- Basic



Voice Prompt	Access Permitted&Denied	
Text Tip	Name	
Hide name	Close	
Light Indication	Green light& Red light	
Auto Screen-Off	Close	
Time Threshold for Auto Screen-Off	30	(s) 10~300
Voice for "Access Permitted"		
Voice for "Access Denied"		
Back to Screensaver	Close	
Back Time	20	(s) 10~300
Upload Screensaver	Upload	
Screen-Off Detection	Enable	

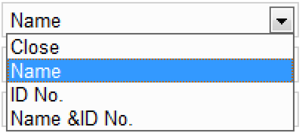
Picture 3-35 Basic setting

- Voice Prompt: Select the voice prompt for user recognition. If selecting “Close”, there will be no voice prompt during recognition.



Picture 3-36 Voice prompt

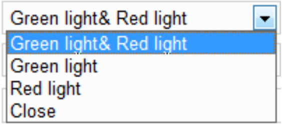
- Text Tip: Select the text tip for user recognition. If selecting “Close”, there will be no text tip during recognition.



Picture 3-37 Text tip

- Hide name: Select hiding or showing device name.

- Light Indication: Select light indication type.



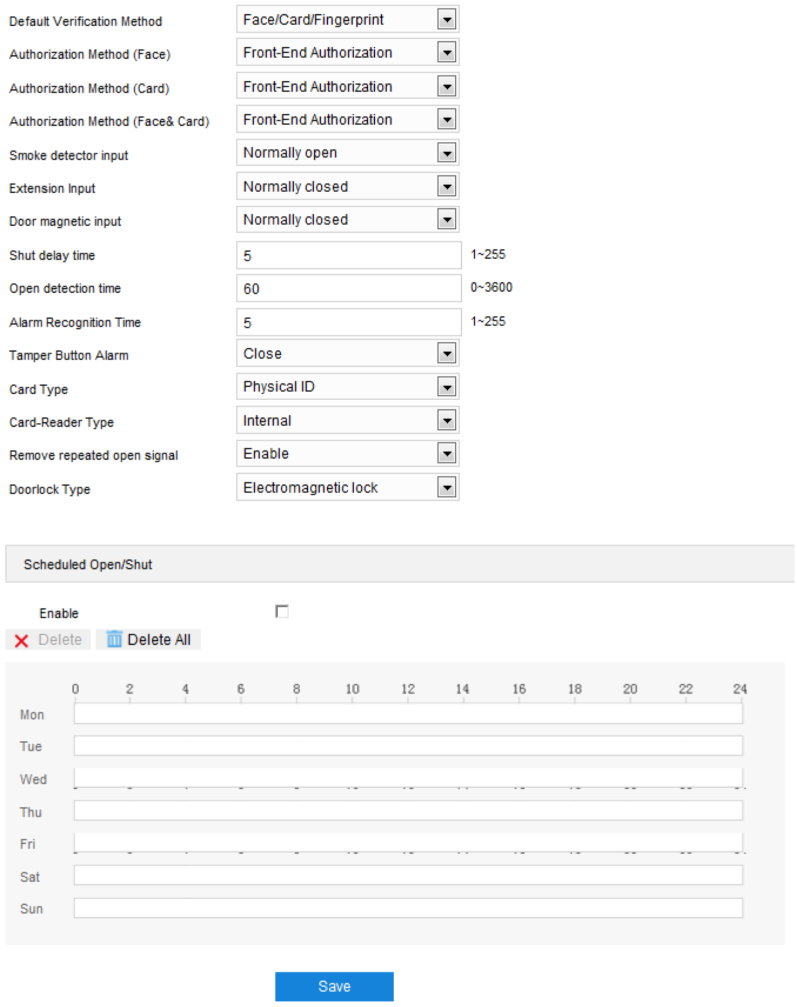
Picture 3-38 Light indication

- Auto Screen-Off: Enable or disable auto screen-off function. If enabled, user can configure the auto screen-off time (unit: second). If no operation is done to the device in the configured duration, the device will skip to the stand-by interface. If disabled, the device will not screen-off automatically.

- Voice for "Access Permitted": Configure the prompt voice when verification succeeds.
- Voice for "Access Denied": Configure the prompt voice when verification fails.
- Back to Screensaver: Enable or disable back to screensaver function. If enabled, user can configure the back to screensaver time (unit: second). If no operation is done to the device in the configured duration, the device will skip to the stand-by interface.
- Upload Screensaver: Click "Upload" to select local picture as screensaver.
- Screen-Off Detection: Enable or disable screen-off detection. After being enabled, it allows face recognition and screen-on under screen-off status.

➢ Access Control

Go to **Settings > Access Control > Settings > Access Control**, and configure parameters such as verification method, authorization method and scheduled open/shut.



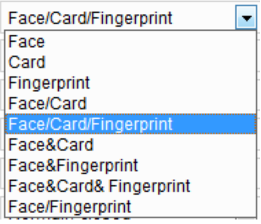
Default Verification Method	Face/Card/Fingerprint	
Authorization Method (Face)	Front-End Authorization	
Authorization Method (Card)	Front-End Authorization	
Authorization Method (Face& Card)	Front-End Authorization	
Smoke detector input	Normally open	
Extension Input	Normally closed	
Door magnetic input	Normally closed	
Shut delay time	5	1~255
Open detection time	60	0~3600
Alarm Recognition Time	5	1~255
Tamper Button Alarm	Close	
Card Type	Physical ID	
Card-Reader Type	Internal	
Remove repeated open signal	Enable	
Doorlock Type	Electromagnetic lock	

Scheduled Open/Shut

Enable □

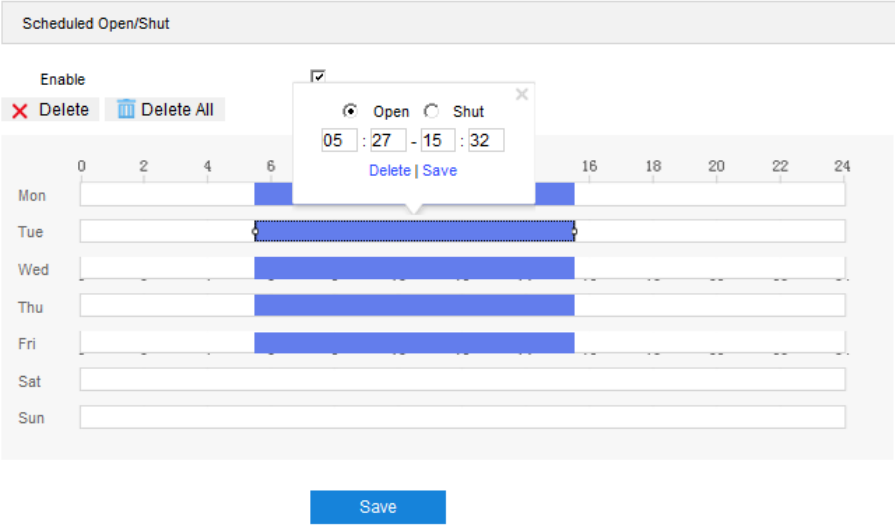
Picture 3-39 Access control setting

- Default Verification Method: Select default verification method, options as shown below.



Picture 3-40 Verification method

- Authorization Method: Select the authorization method for different verification method, options including “Front-End Authorization” and “Networking Authorization”.
- Smoke detector/Extension/Door magnetic input: Select “Normally closed” or “Normally open” according to actual requirements for smoke detector input, extension input and door magnetic input.
- Shut delay time: Configure the shut delay time after verification succeeds.
- Open detection time: Configure the detection time for door opening exception.
- Alarm Recognition Time: Configure the times of recognition alarm.
- Tamper Button Alarm: Enable or disable tamper button alarm.
- Card Type: Select card type according to actual request (some models support).
- Card-Reader Type: Select card-reader type according to actual request (some models support).
- Remove repeated open signal: Enable or disable repeated open signal.
- Scheduled Open/Shut: Configure scheduled door opening/shut durations. Select “Enable” and configure the scheduled durations on the timeline for door opening/shut. Click the duration to pop up a window and select “Open” or “Shut” for the duration. Click “Save” to finish.



Enable ☑

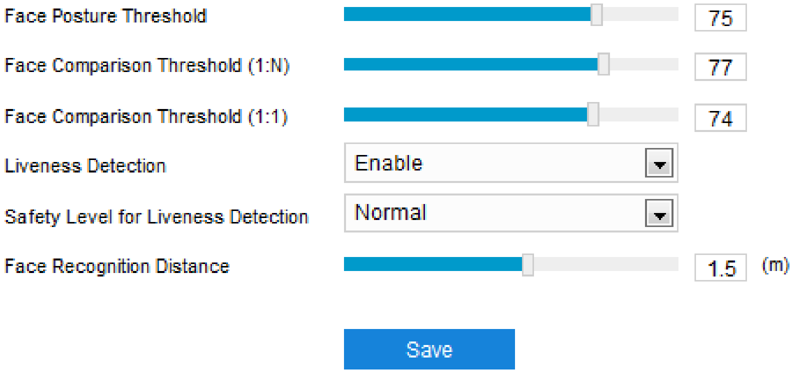
● Open ○ Shut

05 : 27 - 15 : 32

Picture 3-41 Scheduled open/shut

➢ Face

Go to **Settings > Access Control > Settings > Face**, and configure face recognition parameters.



Face Posture Threshold 75

Face Comparison Threshold (1:N) 77

Face Comparison Threshold (1:1) 74

Liveness Detection Enable

Safety Level for Liveness Detection Normal

Face Recognition Distance 1.5 (m)

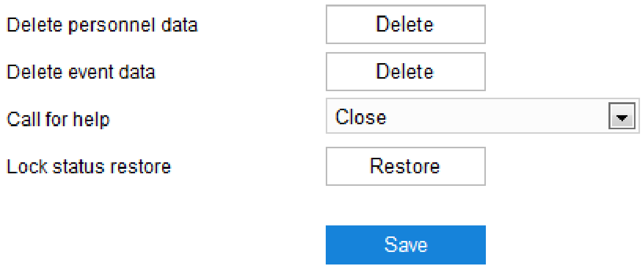
Picture 3-42 Face parameters

- Face Posture Threshold: Configure the threshold score for face recognition, the range being 0~100 points. The device will assess face posture from the perspective of vertical pitching angle, horizontal level angle and interorbital distance; if the score is lower than the preset value, the face recognition will fail, and face comparison or face registration will fail.
- Face Comparison Threshold (1:N): Configure the threshold score for face comparison between captured face and face photo in database, the range being 0~100 points. The higher the preset value is, the lower the false recognition rate will be but the higher the rejection rate will be.
- Face Comparison Threshold (1:1): Configure the threshold score for face comparison between captured face and face photo on the certificate, the range being 0~100 points. The higher the preset value is, the lower the false recognition rate will be but the higher the rejection rate will be.

- Liveness Detection: Enable or disable liveness detection function. After enabling the function, the device will judge if the recognized object is truly a human face; if the object is not a real human face, the verification will fail. After enabling the function, the maximum recognition distance is 1.8m.
- Safety Level for Liveness Detection: After enabling “Liveness Detection”, select a safety level for liveness detection, “Normal” or “High”.
- Face Recognition Distance: Drag the slide bar to configure face recognition distance, the range being 0.3~2.5 m and the default being 1.5 m. The value is a rough one, and there will be some deviation in actual practice according to the sizes of human faces

➢ Advanced

Go to **Settings > Access Control > Settings > Advanced**, and configure the parameters.



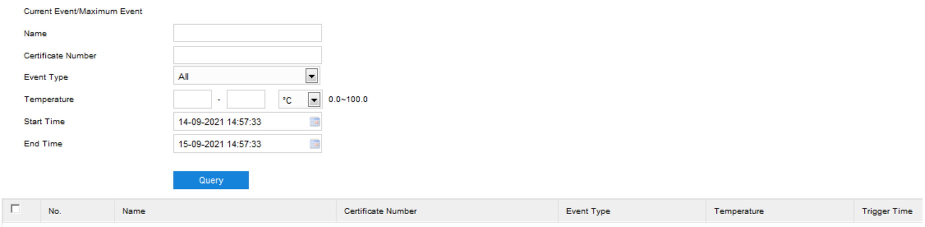
Delete personnel data	Delete
Delete event data	Delete
Call for help	Close
Lock status restore	Restore

Picture 3-43 Advanced setting

- Delete personnel data: Click “Delete” to pop up a prompt dialogue box, and click “Confirm” to delete all personnel data.
- Delete event data: Click “Delete” to pop up a prompt dialogue box, and click “Confirm” to delete all event data.
- Call for help: Select “Close” or “Enable” the function of call for help.
- Lock status restore: Click “Restore” to pop up a prompt dialogue box, and click “Confirm” to restore door lock status.

3.4.3 Event

Go to **Settings > Access Control > Event > Event Query**, and query relevant events.



Current Event/Maximum Event

Name	
Certificate Number	
Event Type	All
Temperature	- °C 0.0~100.0
Start Time	14-09-2021 14:57:33
End Time	15-09-2021 14:57:33

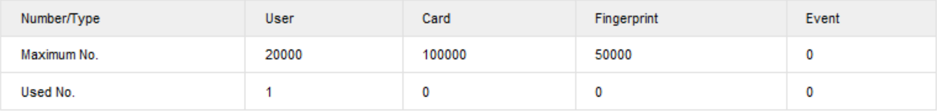
□	No.	Name	Certificate Number	Event Type	Temperature	Trigger Time

Picture 3-44 Event query

Enter anyone or more of the information such as name, certificate number and event type, configure event start time and end time, and click “Query” to display the expected events on the list below.

3.4.4 Storage

Go to **Settings > Access Control > Storage**, and view the storage status of device.



Number/Type	User	Card	Fingerprint	Event
Maximum No.	20000	100000	50000	0
Used No.	1	0	0	0

Picture 3-45 Storage status

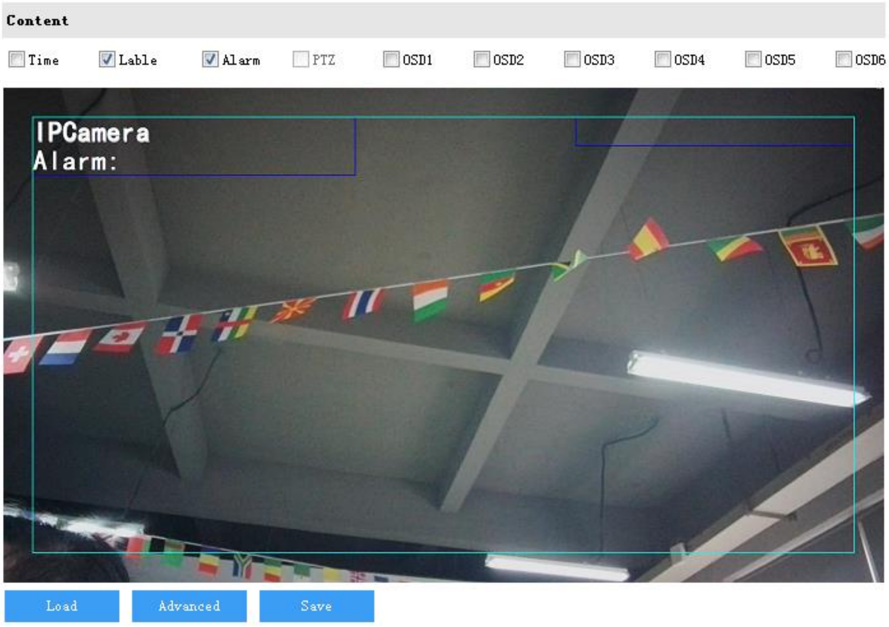
3.5 Camera

Go to **Settings > Camera** to configure camera parameters such as OSD, video and audio.

3.5.1 OSD

OSD (On Screen Display) is the information displayed on live view image. User can configure time, label, alarm, PTZ and other video info. Configuration steps are as follows:

1) Go to **Settings > Camera > OSD**;



Content

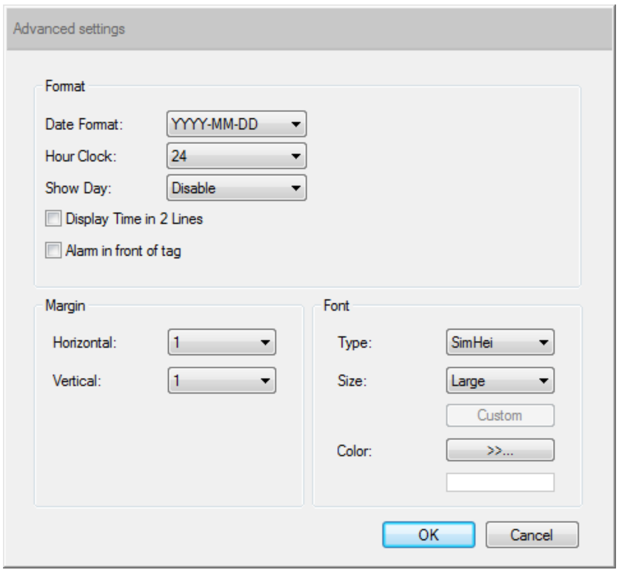
□ Time ☑ Lable ☑ Alarm □ PTZ □ OSD1 □ OSD2 □ OSD3 □ OSD4 □ OSD5 □ OSD6

Picture 3-46 OSD

2) Select options in “Content” according to requirements and preview the effect in the window below, options including "Time", "Label", "Alarm", "PTZ" and "OSD";

3) Configure format. Click “Advanced” and set “Format”, “Font” and “Margin” on the popup interface;

- Format configuration includes "Time Format" (“MM-DD-YYYY”, “YYYY-MM-DD” and “DD-MM-YYYY”), "Display time in 2 lines" (to display time and date in different lines) and "Alarm in front of tag" (to display alarm text over label text).
- Font configuration includes font "Type", "Size" and "Color".
- Margin configuration includes adjustment of the distance between OSD border and image border, i.e. the distance from the yellow frame to the image border.



Advanced settings

Format

Date Format: YYYY-MM-DD

Hour Clock: 24

Show Day: Disable

□ Display Time in 2 Lines

□ Alarm in front of tag

Margin

Horizontal: 1

Vertical: 1

Font

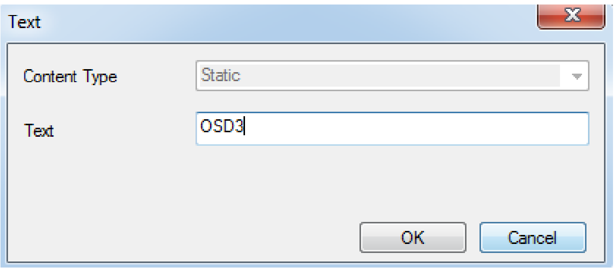
Type: SimHei

Size: Large

Color:

Picture 3-47 Advanced setting

4) Edit OSD texts: select the checkbox to show the content, double-click the OSD textbox on the image and input characters on the popup interface. Click “OK” to display the configured text;



Text

Content Type: Static

Text: OSD3

Picture 3-48 OSD setting

5) Edit OSD positions: select the OSD in the window and drag mouse to change its position. The white and light blue boxes can be moved freely in the yellow box and they can even overlap with each other. The time, label and alarm texts in white box can be moved with the box; while the custom texts and PTZ text in light blue box can be moved freely in the light blue box;

Note: The OSD box size changes with the font size, and the sizes of dark blue and light blue boxes change with the sizes of OSD boxes.

6) Load font. Click “Load”, and select from “Default Font”, “Large Font”, “Medium Font” and ‘Small Font”;

7) Click "Save" to validate setting.

Note:

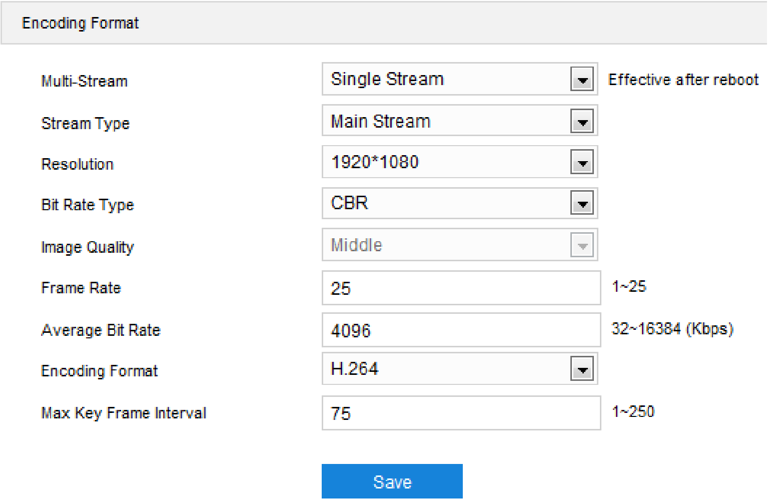
- A number, an English letter or a punctuation mark occupies one character.
- After selecting load font, configure display contents, edit positions and text info according to the above steps.

3.5.2 Video

Go to **Settings > Camera > Video**, and configure video parameters such as encoding format, ROI, privacy mask and video info overlay.

3.5.2.1 Encoding Format

Go to **Settings > Camera > Video > Encoding Format**, and configure parameters such as stream type, resolution, bit rate type and etc.



Encoding Format

Multi-Stream	Single Stream	Effective after reboot
Stream Type	Main Stream	
Resolution	1920*1080	
Bit Rate Type	CBR	
Image Quality	Middle	
Frame Rate	25	1~25
Average Bit Rate	4096	32~16384 (Kbps)
Encoding Format	H.264	
Max Key Frame Interval	75	1~250

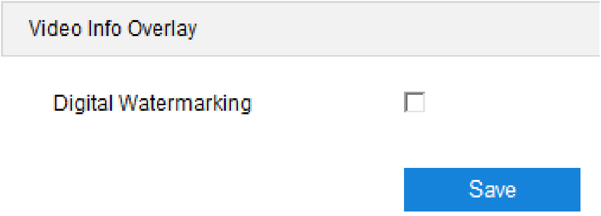
Picture 3-49 Encoding format

- Multi-Stream: The access control device supports only single stream.
- Stream Type: The default is main stream, non-configurable.
- Resolution: The default is 1920*1080, non-configurable.
- Bit Rate Type: The default is CBR, non-configurable.
- Image Quality: The default is middle, non-configurable.
- Frame Rate: Set the encoding frames per second. The higher the frame rate is, the more bandwidth is required and the more storage it will take.
- Average Bit Rate: Set the average bit rate.
- Encoding Format: The default is H.264, non-configurable.

- Max Key Frame Interval: Configure the interval frames between two key frames, ranging 1 ~ 250. Suggest applying the default value 75. The larger the value is, the less fluctuation of the stream there will be and the worse the image will be, vice versa.

3.5.2.2 Video Info Overlay

Go to **Settings > Camera > Video > Video Info Overlay**, and overlay digital watermarking into the surveillance image.



Video Info Overlay

Digital Watermarking □

Picture 3-50 Video info overlay

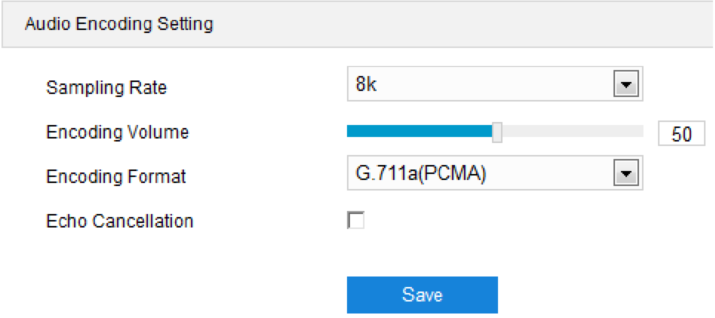
- Digital Watermarking: Select “Digital Watermarking” to overlay digital watermarking into the video recordings so as to protect the videos from being tampered.

After finishing, click “Save” to validate setting.

3.5.3 Audio

Go to **Settings > Camera > Audio**, and configure audio parameters such as audio encoding and decoding.

3.5.3.1 Audio Encoding



Audio Encoding Setting

Sampling Rate 8k

Encoding Volume 50

Encoding Format G.711a(PCMA)

Echo Cancellation □

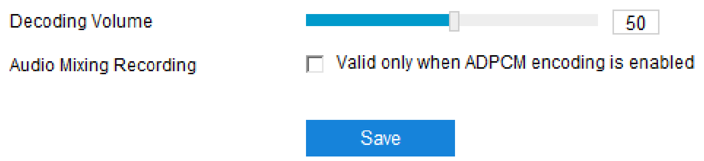
Picture 3-51 Audio encoding

- Sampling Rate: It means the sampling times to sound signals by the audio-recording device in 1 second. The higher the sampling rate is, the more real and natural the sound reproduction will be.
- Encoding Volume: Drag the slide bar to adjust audio encoding volume, i.e. audio input volume.
- Encoding Format: Select audio encoding format from the dropdown list, by default G.711a (PCMA).

- Echo Cancellation: Select the checkbox to cancel noises in the input audio and thus improve the audio quality.

3.5.3.2 Audio Decoding

Go to **Settings > Camera > Audio > Audio Decoding**, and configure audio decoding.



Decoding Volume: 50

Audio Mixing Recording: □ Valid only when ADPCM encoding is enabled

Picture 3-52 Audio decoding

- Decoding Volume: Drag the slide bar to adjust audio decoding volume, i.e. audio output volume.
- Audio Mixing Recording: Select the checkbox to enable audio mixing recording function, which is valid only when "ADPCM" is selected.

Note: When "Audio Mixing Recording" is disabled, there will be only heard sound without calling sound during video recording; when it is enabled, there will be both heard and calling sound during video recording.

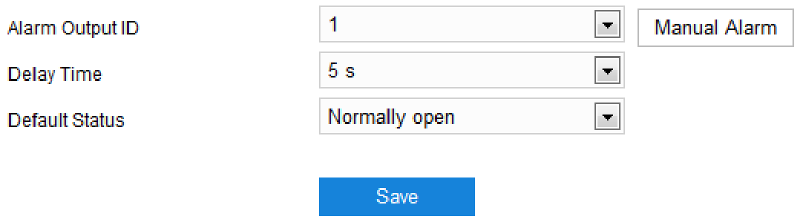
After finishing, click "Save" to validate setting.

3.6 Event

3.6.1 Alarm Output

Please make sure the device has been connected to alarm output device such as alarm light before configuration, and the device will transmit alarm signal to alarm output device to trigger alarm. Configuration steps are as follows:

1) Go to **Settings > Event > Alarm Output**;



Alarm Output ID: 1

Delay Time: 5 s

Default Status: Normally open

Picture 3-53 Alarm Output

2) Select alarm output ID according to actual condition, or click "Manual Alarm" to send alarm signal manually and click "Manual Alarm Elimination" to cancel alarm;

3) Select an option from the dropdown list of delay time of alarm output, options including "Without Delay", 1s, 5s, 10s, 30s, 1min, 2min, 5min and 10min. The default

delay time of alarm output is 5s, and it will eliminate alarm automatically after the delay time ends;

Note: The alarm output duration is by default 5s, and the delay time means the extended continuous time after the default 5s.

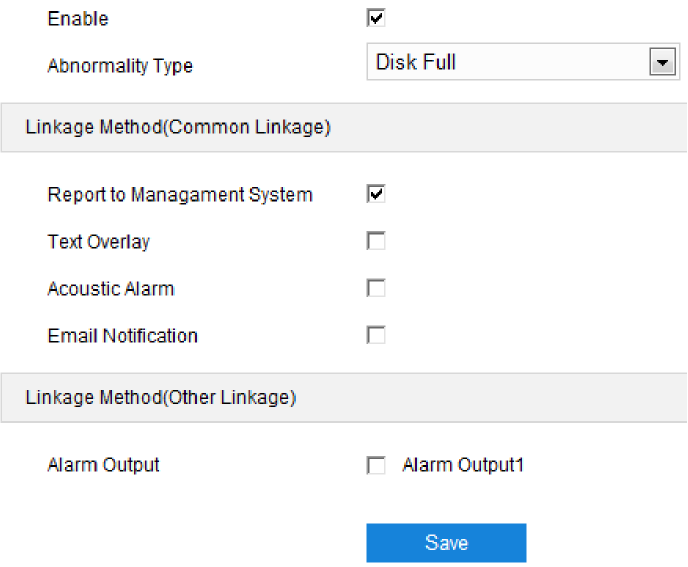
4) Select default status, options including “Normally open” and “Normally closed”;

5) Click “Save” to validate setting.

3.6.2 Abnormality Linkage

Configure the alarm linkage method for abnormal events. When any exception occurs, the device will trigger alarm according to the result of its judgment. Configuration steps are as follows:

1) Go to **Settings > Event > Abnormality Linkage**;



Enable ☑

Abnormality Type: Disk Full

Linkage Method(Common Linkage)

Report to Managament System ☑

Text Overlay □

Acoustic Alarm □

Email Notification □

Linkage Method(Other Linkage)

Alarm Output □ Alarm Output1

Picture 3-54 Abnormality linkage

2) Select "Enable";

3) Select an option from the dropdown list of abnormality type;

Note:

- Disk Full: when the disk storage is insufficient.
- Disk Error: when the disk cannot be recognized.
- Internet Disconnected: when the device isn't connected to the internet normally.

4) Select linkage method(s), which is/are the alarm output method(s) when an event triggers an alarm;

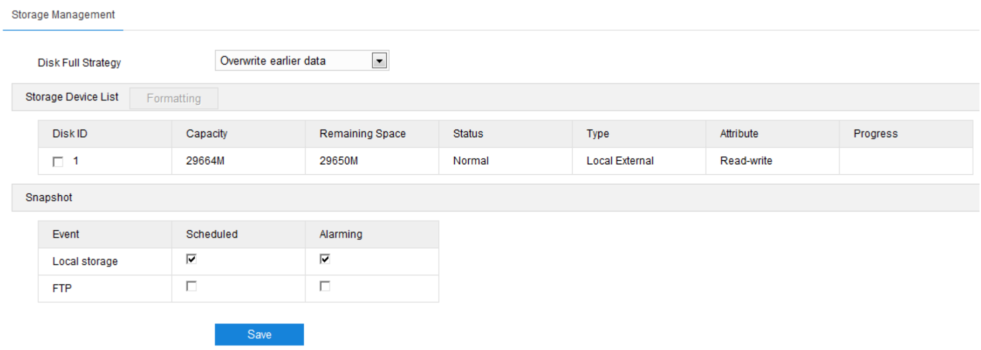
5) Click "Save" to validate settings.

3.7 Storage

3.7.1 Storage Management

Go to **Settings > Storage > Storage Management**, and configure disk full strategy; view storage device list and format TF card; configure storage position of captured snapshots.

Note: When the device is installed with a TF card and it works normally, user can configure scheduled recording and scheduled snapshot.



Storage Management

Disk Full Strategy: Overwrite earlier data

Storage Device List

Disk ID	Capacity	Remaining Space	Status	Type	Attribute	Progress
□ 1	29664M	29650M	Normal	Local External	Read-write	

Snapshot

Event	Scheduled	Alarming
Local storage	☑	☑
FTP	□	□

Picture 3-55 Storage management

- Disk Full Strategy: Configure the video recording strategy when there is insufficient storage space.
  - Overwrite earlier data: when there is insufficient storage space, overwrite the oldest videos;
  - Stop: when there is insufficient storage space, stop video recording automatically.

    Go to **Settings > Event > Abnormality Linkage** and select "Disk Full" for abnormality type to remind user that local video recording has stopped.
- Storage Device List: Display the status, capacity, progress and other information of all storage devices.
  - Disk ID: It shows the serial numbers of the storage devices.
  - Capacity: It displays the storage capacity of the storage devices.
  - Remaining Space: It displays the remaining space of the storage devices.
  - Status: It shows the status of storage devices such as "Normal" (with a card and normally read and write), "Does not Exist" (without a card), "Not Formatted" (need to format when first inserting a card) and etc.
  - Type: It shows the installation positions of the storage devices.
  - Attribute: It shows the read and write attributes of the storage devices, read-only, write-only or read-write.

- Progress: It shows the percentage of the formatting progress of TF card. Select the disk and click "Formatting" to format the selected disk.

- Snapshot: Configure the save path of snapshots. According to actual requirements, select "Local storage" (TF card in camera) or "FTP" (server) to save scheduled snapshots and alarming snapshots.

Note: Some models have no TF card by default and they need customization before going out if necessary. When using the TF card for the first time, please click "Formatting" first.

3.7.2 Recording

When scheduled recording is enabled, the device will record videos automatically in the configured durations and save the videos in the TF card. Configuration steps are shown below:

1) Go to **Settings > Storage > Storage Management** to configure disk full strategy and format the storage card recognized by the device. If formatting is successful, the status will turn “Normal” which means the storage card can work normally;

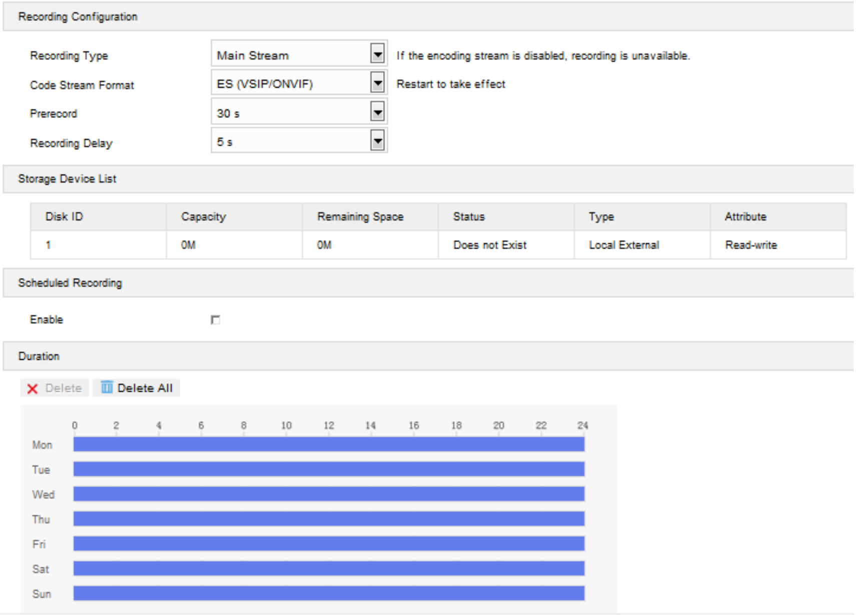
2) Go to **Settings > Storage > Recording** to configure video recording;

- Recording Type: Select the stream to be recorded;

- Code Stream Format: Select video format according to the type of access protocol;

- Prerecord: Select prerecord duration, i.e. the prerecord duration before recording starts, which is certain to be 30s;

- Recording Delay: Select recording delay time, i.e. the additional recording duration plus to the configured duration;



Recording Configuration

Recording Type: Main Stream — If the encoding stream is disabled, recording is unavailable.

Code Stream Format: ES (VSIP/ONVIF) — Restart to take effect

Prerecord: 30 s

Recording Delay: 5 s

Storage Device List

Disk ID	Capacity	Remaining Space	Status	Type	Attribute
1	0M	0M	Does not Exist	Local External	Read-write

Scheduled Recording

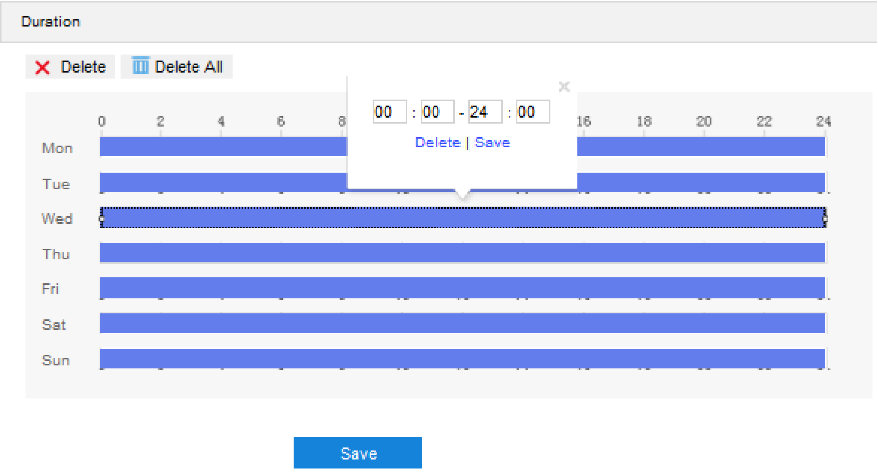
Enable □

Duration

Picture 3-56 Scheduled recording

3) Select "Enable" to enable scheduled recording;

4) Configure durations for scheduled recording. The default setting is 24 hours in bright blue color bars, or you can customize the durations;



Picture 3-57 Arming durations

- Set durations: Configure video recording durations according to the requirements.
  - Click the color bar to pop up a window for editing the accurate start time and end time; click "Save" to validate setting.
  - Click the color bar and there will be small white squares at the ends of it. Drag the small white squares to edit the start time and end time.
  - Select the default color bar on a day and delete it. Left click and drag the mouse from left to right on the timeline to form a new color bar, on the top of which it will show the start time and end time.
- Copy: Click the copy icon behind the timeline and copy the durations on the day to one or several other days;
- Delete: Click "Delete All" on the top of the timeline to delete all the durations. Select a duration and click "Delete" on the popup window or on the top of the timeline to delete the duration;

ⓘ Note: Click to select duration and drag it on the timeline to change its start time and end time but without changing the length of the video duration.

5) Click "Save" to validate settings.

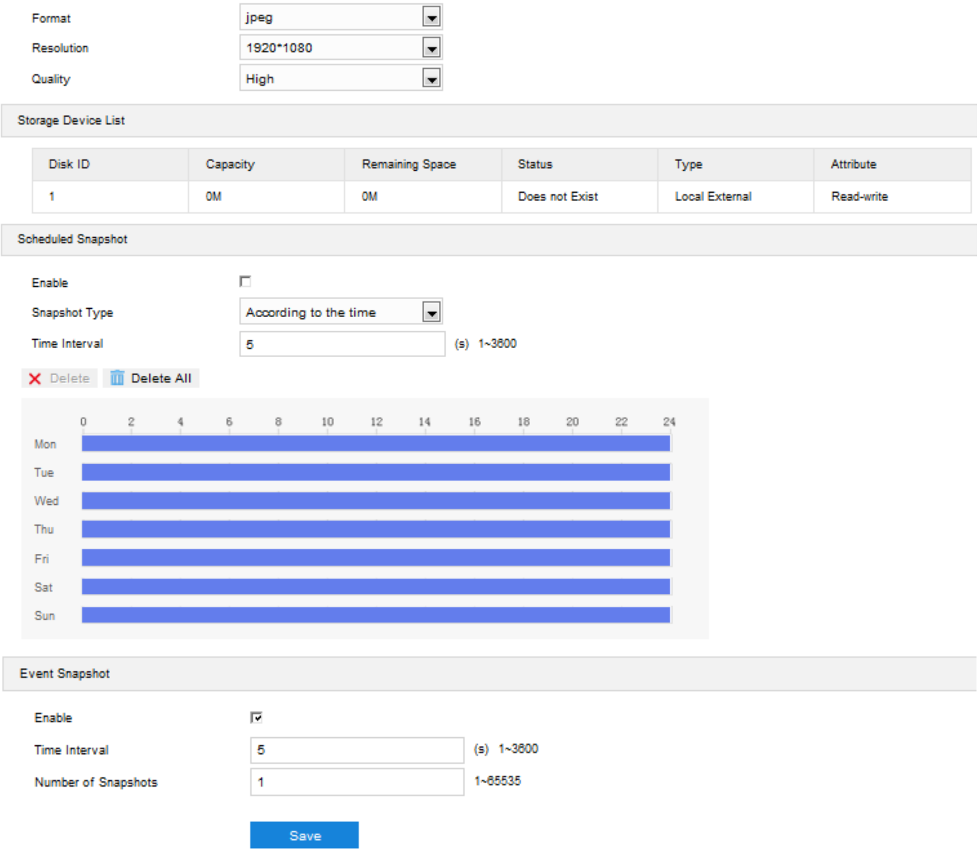
3.7.3 Snapshot

After configuring snapshot parameters, the device will perform different capturing tasks automatically in the configured durations and save the snapshots in TF card. Configuration steps are as follows:

1) Go to **Settings > Storage > Storage Management** to configure disk full strategy and format the TF card recognized by the camera. If formatting is successful, the status will turn “Normal” which means the storage card can be used normally;

2) Go to **Settings > Storage > Snapshot** to configure snapshot parameters;

- Format: It only supports .jpeg format;
- Resolution: It’s the same as that of current main stream;
- Quality: Configure the quality of captured image;



Format: jpeg

Resolution: 1920*1080

Quality: High

Storage Device List

Disk ID	Capacity	Remaining Space	Status	Type	Attribute
1	0M	0M	Does not Exist	Local External	Read-write

Scheduled Snapshot

Enable □

Snapshot Type: According to the time

Time Interval: 5 (s) 1~3600

Event Snapshot

Enable ☑

Time Interval: 5 (s) 1~3600

Number of Snapshots: 1 1~65535

Picture 3-58 Scheduled snapshot

3) Configure scheduled snapshot parameters:

a) Select “Enable” to enable scheduled snapshot;

b) Select snapshot type, “According to the time” or “According to the number”. When selecting “According to the number”, configure time interval and number of snapshots;

c) Configure time interval between snapshots;

d) Configure durations for scheduled recording. The default setting is 24 hours in bright blue color bars, or you can customize the durations;

- Set durations: Configure scheduled snapshot durations according to the requirements.

- Click the color bar to pop up a window for editing the accurate start time and end time; click "Save" to validate setting.
- Click the color bar and there will be small white squares at the ends of it. Drag the small white squares to edit the start time and end time.
- Select the default color bar on a day and delete it. Left click and drag the mouse from left to right on the timeline to form a new color bar, on the top of which it will show the start time and end time.

■ Copy: Click the copy icon behind the timeline and copy the durations on the day to one or several other days;

■ Delete: Click "Delete All" on the top of the timeline to delete all the durations. Select a duration and click "Delete" on the popup window or on the top of the timeline to delete the duration;

ⓘ Note: Click to select duration and drag it on the timeline to change its start time and end time but without changing the length of the video duration.

4) Configure event snapshot parameters:

a) Select “Enable” under event snapshot;

b) Configure time interval between capturing;

c) Configure number of snapshots for each capturing.

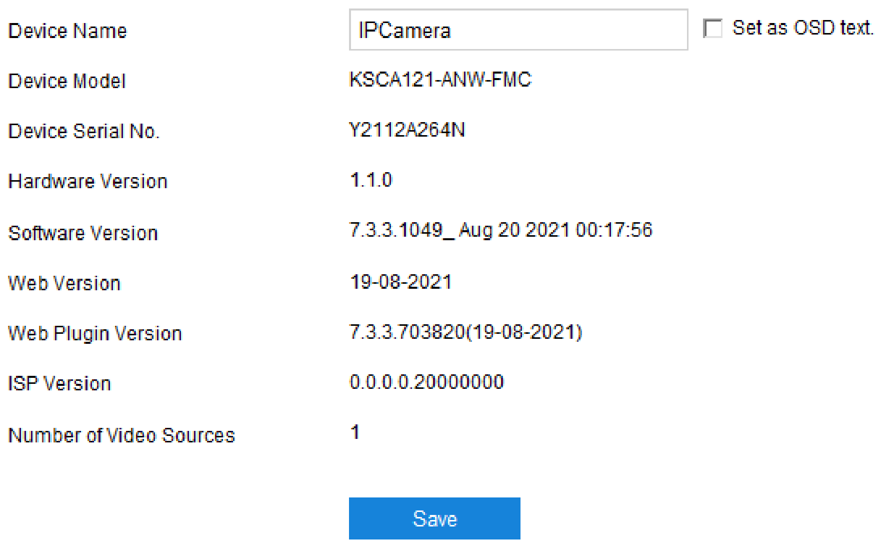
5) Click "Save" to validate settings.

3.8 System

3.8.1 Device Info

Go to **Settings > System > Device Info**, and view device info.

Device info includes device name, device model, device serial No. and etc. User can customize device name and select “Set as OSD text”. Device name doesn’t support specific symbols. If “Set as OSD text” is selected and saved, the device name will be synchronized to the OSD, as shown below:



Device Name	IPCamera ☐ Set as OSD text.
Device Model	KSCA121-ANW-FMC
Device Serial No.	Y2112A264N
Hardware Version	1.1.0
Software Version	7.3.3.1049_Aug 20 2021 00:17:56
Web Version	19-08-2021
Web Plugin Version	7.3.3.703820(19-08-2021)
ISP Version	0.0.0.0.20000000
Number of Video Sources	1

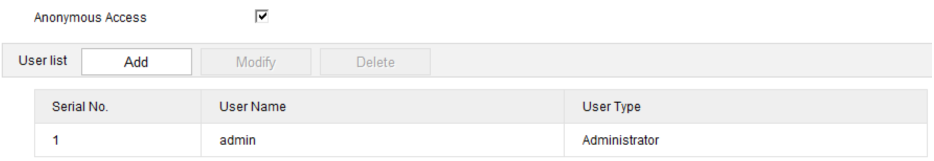
Picture 3-59 Device info

3.8.2 User Security

Go to **Settings > System > User Security**, and configure parameters such as user info, RTSP authorization, IP filter and security service.

3.8.2.1 User

Go to **Settings > System > User Security > User**, and add or delete user, edit user name and password, configure user authorizations and etc.

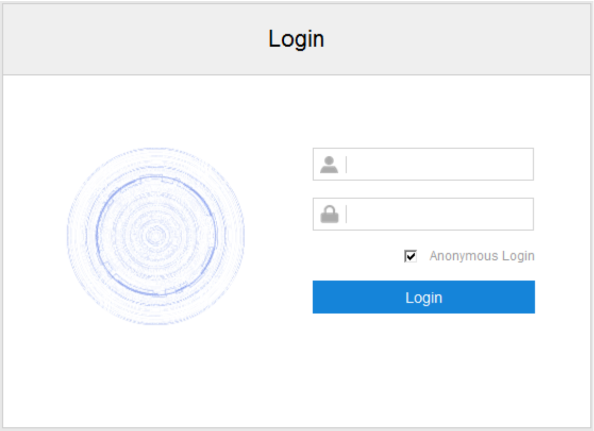


Anonymous Access ☑

Serial No.	User Name	User Type
1	admin	Administrator

Picture 3-60 User

- Anonymous Access: After selecting the checkbox, user will be able to select "Anonymous Login" on the login interface to log anonymously.

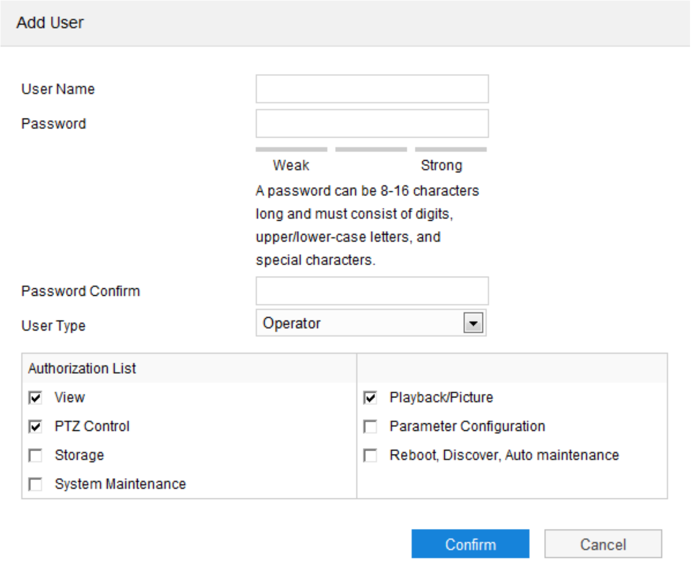


☑ Anonymous Login

Picture 3-61 Anonymous login

Note: Anonymous login user has the authorization of live view only.

- Add user: Click “Add”, and enter user name and password on the popup interface. Select user type from the dropdown list, and assign operation rights to newly added user from the authorization list. After setting, click “Confirm”.



Add User

User Name

Password

Weak Strong

A password can be 8-16 characters long and must consist of digits, upper/lower-case letters, and special characters.

Password Confirm

User Type: Operator

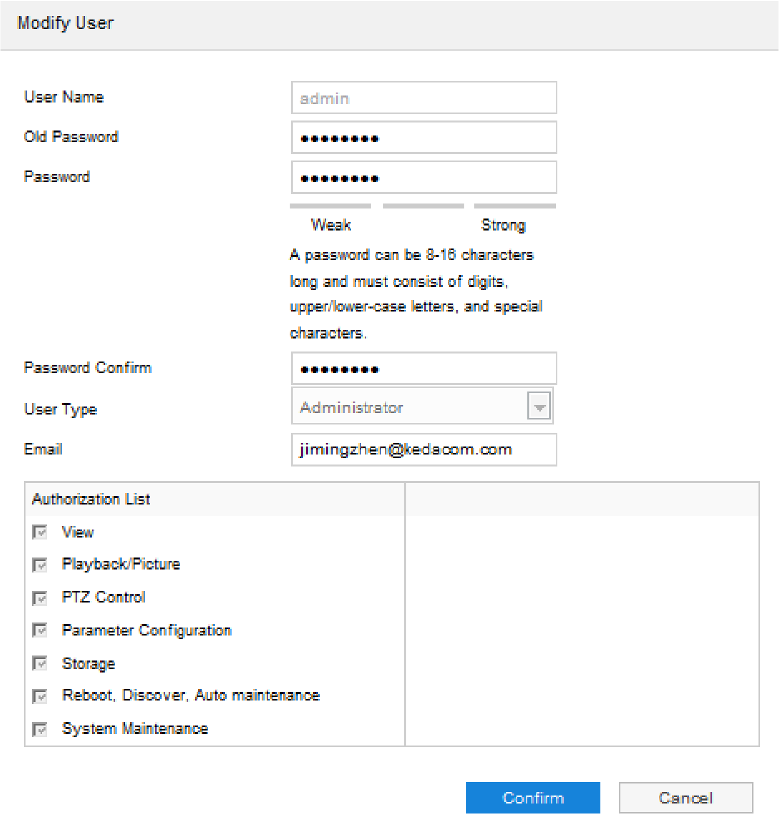
Authorization List	
☑ View	☑ Playback/Picture
☑ PTZ Control	□ Parameter Configuration
□ Storage	□ Reboot, Discover, Auto maintenance
□ System Maintenance	

Picture 3-62 Add user

Note:

- ♦ By default, all options are available to administrator users; live view, playback/snapshot, and PTZ control authorizations are available to operator users; a viewer user can only view the live video from the device.
- ♦ Some settings take effect after rebooting the device, which requires user with both the authorizations of configuration and rebooting.

- Modify user: Select user and click “Modify” to modify on the popup interface.



Modify User

User Name: admin

Old Password: ••••••••

Password: ••••••••

Weak Strong

A password can be 8-16 characters long and must consist of digits, upper/lower-case letters, and special characters.

Password Confirm: ••••••••

User Type: Administrator

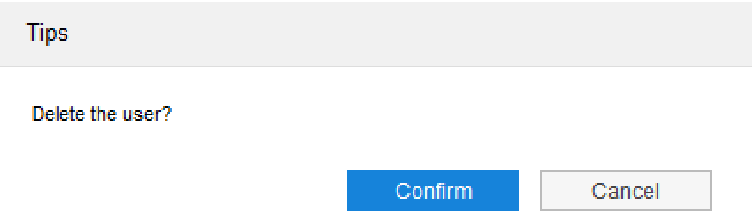
Email: jimingzhen@kedacom.com

Authorization List

- ☑ View
- ☑ Playback/Picture
- ☑ PTZ Control
- ☑ Parameter Configuration
- ☑ Storage
- ☑ Reboot, Discover, Auto maintenance
- ☑ System Maintenance

Picture 3-63 Modify user

- Delete user: Select user and click “Delete” to delete the user.



Tips

Delete the user?

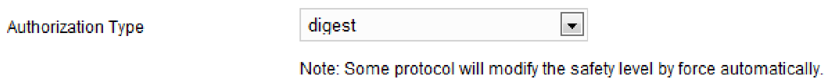
Picture 3-64 Delete user

Attention: “admin” user cannot be deleted and its user name cannot be edited.

3.8.2.2 RTSP Authorization

Go to **Settings > System > User Security > RTSP**, and select authorization type from the dropdown list, options including “none”, “basic/digest” and “digest”. By default, it is “basic/digest”.

Note: Basic, i.e. basic authorization. As its stream is transmitted without encryption transformation, there is severe security risk. Digest, i.e. digest authorization. As its stream is processed by MD5 Hash conversion, it is more secure.


Authorization Type: digest

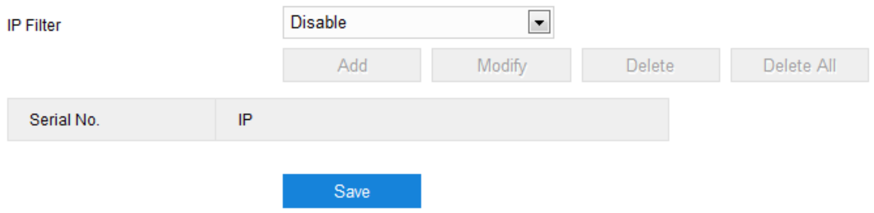
Note: Some protocol will modify the safety level by force automatically.

Picture 3-65 RTSP authorization

3.8.2.3 IP Filter

IP filter is to configure access limitation of IP address. Configuration steps are as follows:

1) Go to **Settings > System > User Security > IP Filter;**


IP Filter: Disable

Picture 3-66 IP filter

2) Select IP filtering mode from the dropdown list, options including “Disable”, “Blacklist” and “Whitelist”;

- Disable: To disable IP filtering setting.
- Whitelist: A list of IP addresses able to access to the device.
- Blacklist: A list of IP addresses unable to access to the device.

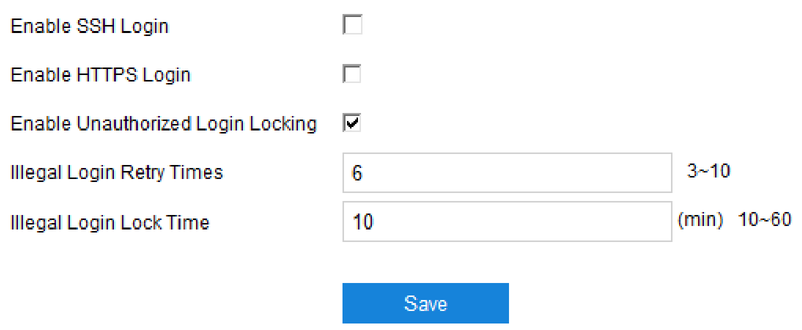
3) Edit Blacklist/ Whitelist.

- Add blacklist/whitelist: Click “Add” and enter IP address on the pop up interface, and click “Confirm”.
- Modify blacklist/whitelist: Select the IP address from the list and click “Modify”. On the popup interface, modify the IP address and click “Confirm”.
- Delete blacklist/whitelist: Select the IP address from the list and click “Delete” to delete the IP address. Click “Delete All” to delete all the added IP addresses.

4) After finish setting, click "Save" to validate setting.

3.8.2.4 Security Service

Go to **Settings > System > User Security > Security Service** and configure the parameters to ensure account safety.



Enable SSH Login □

Enable HTTPS Login □

Enable Unauthorized Login Locking ☑

Illegal Login Retry Times 6 3~10

Illegal Login Lock Time 10 (min) 10~60

Picture 3-67 Security service

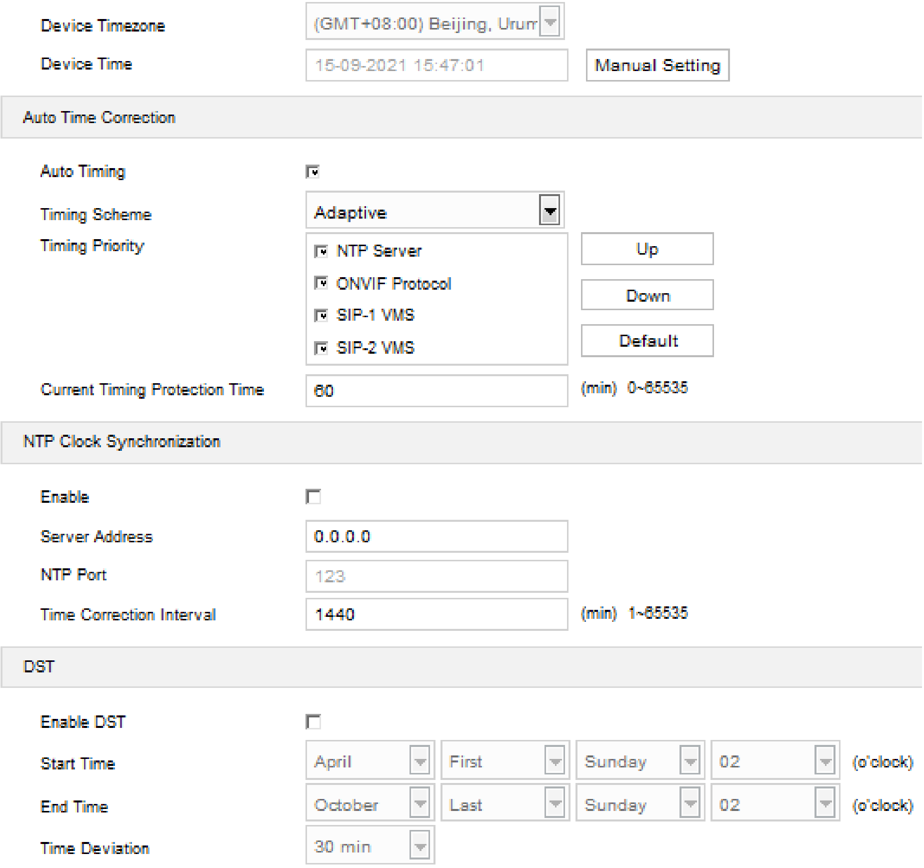
- Enable SSH Login: Select “Enable SSH Login” to enable SSH service and user can login by SSH mode. Usually it's unnecessary to enable when the camera works normally.
- Enable HTTPS Login: Select “Enable HTTPS Login” to enable HTTPS service and user can login by HTTPS mode. Usually it's unnecessary to enable when the camera works normally.
- Enable Unauthorized Login Locking: Select “Enable Unauthorized Login Locking” to enable unauthorized login locking, and configure illegal login retry times and illegal login lock time.
  - Illegal Login Retry Times: Configure illegal login retry times, and the default is 6 times.
  - Illegal Login Lock Time: Configure illegal login lock time, and the default is 10 minutes.

Note: After selecting “Enable Unauthorized Login Locking”, when the locking conditions meet, the IP address of the illegal login PC will be locked.

After finishing, click “Save”.

3.8.3 Time

Go to **Settings > System > Time**, and configure time parameters such as device time zone, device time, auto time correction, NTP synchronization and DST. Configure parameters by request and click "Save" to validate setting.



Device Timezone (GMT+08:00) Beijing, Urum

Device Time 15-09-2021 15:47:01 Manual Setting

Auto Time Correction

Auto Timing ☑

Timing Scheme Adaptive

Timing Priority
☑ NTP Server
☑ ONVIF Protocol
☑ SIP-1 VMS
☑ SIP-2 VMS

Current Timing Protection Time 60 (min) 0~65535

NTP Clock Synchronization

Enable □

Server Address 0.0.0.0

NTP Port 123

Time Correction Interval 1440 (min) 1~65535

DST

Enable DST □

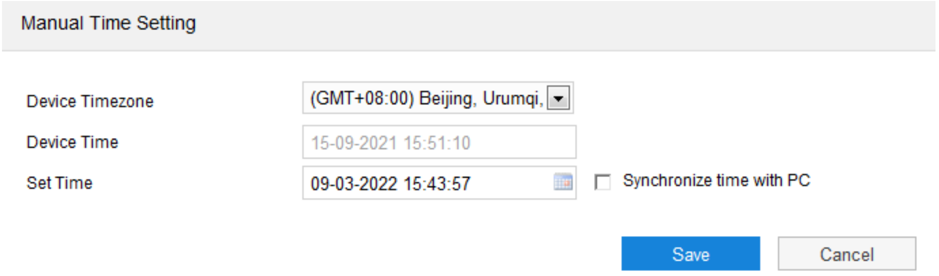
Start Time April First Sunday 02 (o'clock)

End Time October Last Sunday 02 (o'clock)

Time Deviation 30 min

Picture 3-68 Time setting

- Time Setting: Set device time zone and device time. Click "Manual Setting", configure device time zone and device time on the popup interface. Select "Synchronize time with PC" to synchronize device time with PC time, and click "Save" to validate setting.



Manual Time Setting

Device Timezone (GMT+08:00) Beijing, Urumqi,

Device Time 15-09-2021 15:51:10

Set Time 09-03-2022 15:43:57 □ Synchronize time with PC

Picture 3-69 Manual time setting

- Auto Time Correction: Select "Auto Timing" and the system will correct time automatically according to access protocol or adaptive, and configure current timing protection time.
  - Adaptive: When selecting “Adaptive”, select necessary adaptive protocols, set the timing priority sequence and configure current timing protection time (i.e. the save time during protocol switching).
  - Protocol: i.e. the protocol for the device to access to platform or server. When selecting a protocol, the system will correct time automatically according to the platform or server by the protocol;

Note:

- In the box of timing priority, the above one owns higher timing priority.
- Select the protocol whose priority needs adjustment, click “UP” to improve its priority; click “Down” to lower its priority; click “Default” to follow the default timing priorities.
- When selecting “NTP server”, configure relative parameters such as NTP server address, NTP port and time correction interval.

- NTP Clock Synchronization: Select “Enable” and configure “Server Address”, “NTP Port” and “Time Correction Interval”. When it is enabled, the camera will correct time on a time basis of the configured interval.

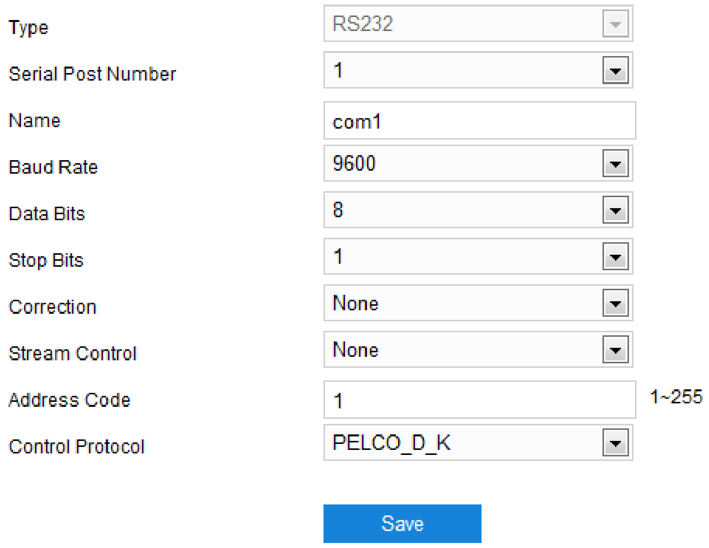
Note: NTP (Network Time Protocol) is a protocol to synchronize time. It enables PC to synchronize with its server or time source such as quartz and GPS); it provides highly precise time correction (difference less than 1ms with the standard on LAN, decades ms on WAN), and it’s able to prevent vicious protocol attack by encryption confirmation.

- DST: DST (daylight saving time) is the practice of advancing clocks during summer months so that evening daylight lasts longer, while sacrificing normal sunrise times and the time applied during DST is called DST time. Select "Enable DST" and set “Start Time”, “End Time” and “Time Deviation”.

3.8.4 Serial Port

Go to **Settings > System > Serial Port**, and configure serial port.

Serial port is used to control extended alarm input or device debugging (subject to devices). Usually serial port is identified as RS485 A/B. Pair the ports by configuring RS485 port parameters. Please configure the parameters such as “Baud Rate”, “Data Bits” and “Address Code” according to the actual conditions. After finishing, click “Save” to validate setting.



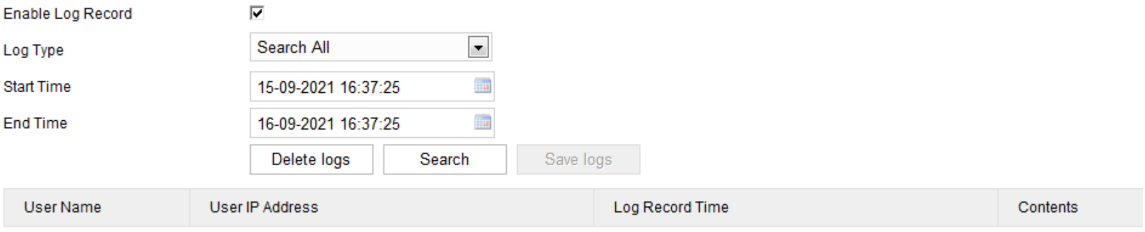
Type	RS232	
Serial Post Number	1	
Name	com1	
Baud Rate	9600	
Data Bits	8	
Stop Bits	1	
Correction	None	
Stream Control	None	
Address Code	1	1~255
Control Protocol	PELCO_D_K	

Picture 3-70 Serial port

3.8.5 Log

➢ Logs

Go to **Settings > System > Log > Logs**, select "Enable Log Record" to search, view and download logs.



Enable Log Record	☑
Log Type	Search All
Start Time	15-09-2021 16:37:25
End Time	16-09-2021 16:37:25

User Name	User IP Address	Log Record Time	Contents

Picture 3-71 Logs

Operation steps are as follows:

1) On the dropdown list of log type, select a log type, otherwise the default is "Search All";

2) Select start time and end time, and click "Search". The search result will show on the list below;

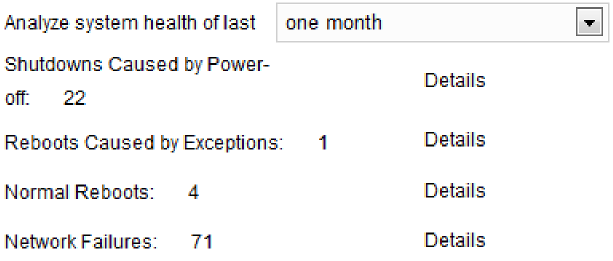
3) Click "Save logs" to download all logs locally; click "Delete logs" to clear all logs.

Note:

- ♦ When the log type is “User Operation” or “Alarm Info”, select “Secondary type” to narrow the search scope.
- ♦ The system can save maximum 2,000 entries of logs.

➢ System Health

Go to **Settings > System > Log > System Health**, and view system health status in recent one month, two months or three months.



Analyze system health of last: one month

Shutdowns Caused by Power-off: 22 Details

Reboots Caused by Exceptions: 1 Details

Normal Reboots: 4 Details

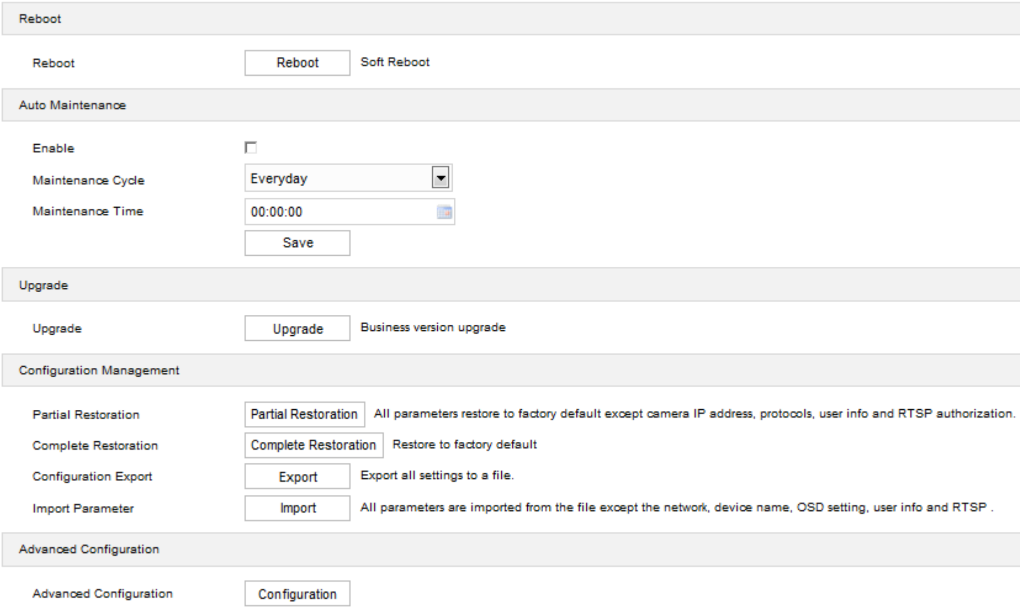
Network Failures: 71 Details

Picture 3-72 System health

3.8.6 System Maintenance

➢ System Maintenance

Go to **Settings > System > System Maintenance > System Maintenance**, and perform maintenance operations such as rebooting and upgrading the device.



Reboot

Reboot: [Reboot] Soft Reboot

Auto Maintenance

Enable: □

Maintenance Cycle: Everyday

Maintenance Time: 00:00:00

[Save]

Upgrade

Upgrade: [Upgrade] Business version upgrade

Configuration Management

Partial Restoration: [Partial Restoration] All parameters restore to factory default except camera IP address, protocols, user info and RTSP authorization.

Complete Restoration: [Complete Restoration] Restore to factory default

Configuration Export: [Export] Export all settings to a file.

Import Parameter: [Import] All parameters are imported from the file except the network, device name, OSD setting, user info and RTSP .

Advanced Configuration

Advanced Configuration: [Configuration]

Picture 3-73 System maintenance

- ■ Reboot: Click "Reboot" to reboot the device softly.
- ■ Auto Maintenance: Select "Enable", and configure maintenance cycle and maintenance time. Click "Save" to validate setting.
- ■ Upgrade: Upgrade system version. Click “Upgrade” and open local upgrade file in <*.pkg> format. During upgrading, please do nothing but waiting. After upgrading, re-login to the web client. If it is necessary to upgrade the web client, the system will prompt to download the plug-in.
- ■ Configuration Management: including partial restoration, complete restoration, configuration export and import parameter.
  - Partial Restoration: Click this button and all parameters will restore to factory default except network setting, access protocol, user info and RTSP authorization.
  - Complete Restoration: Click this button and all parameters will restore to factory default.
  - Configuration Export: After configuring camera mode, export the configuration to local PC for copying the configurations to other devices. Click "Export" and select a local save path to export.

- Import Parameter: Import local configuration file of other devices from PC without manual setting. Click "Import" and select local configuration file to import.

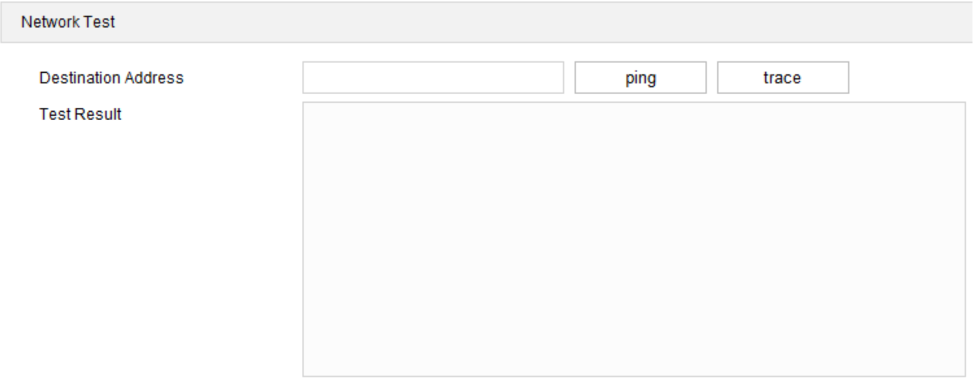
- Advanced Configuration: Only "admin" user can perform advanced configuration. Click "Configuration", input the right password for advanced user and click "Confirm" to enter the configuration interface. Configure parameters such as VSIP protocol compatibility, keep alive the stream UDP and network adaptation if necessary.

- Network Test

  Go to **Settings > System > System Maintenance > Network Test**.

  - Enter an IP address in “Destination Address” and click “ping”. The test result will show on the list below. It’s used to test the network connectivity between the device and the destination device.

  - Enter an IP address in “Destination Address” and click “trace”. The test result will show the routing entries visiting the destination address. It is used to test the network routing information between the device and the destination address.



Picture 3-74 Network test

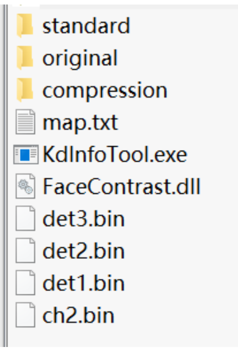
Appendix: Personnel Import Through Web Client

- Prepare face pictures

Prepare the personnel pictures to import into the device. The face resolution cannot be lower than 150*150 pixels and the format must be .jpg.

- Edit pictures with Kedacom image-processing tool

Obtain kdpic.zip packet and uncompress it to get the following files and folders.



standard
original
compression
map.txt
KdInfoTool.exe
FaceContrast.dll
det3.bin
det2.bin
det1.bin
ch2.bin

1) Save all the personnel face pictures in the folder of “original”.
2) Open the file of “kdinfotool.exe”.
3) Click “Start” and the personnel picture in the folder will display above the status bar on the left.
4) Input name of the person in the picture; select certificate type and number.
5) Click “Save” and the picture of next person will show on the left. Repeat the above steps and input personnel information one by one.

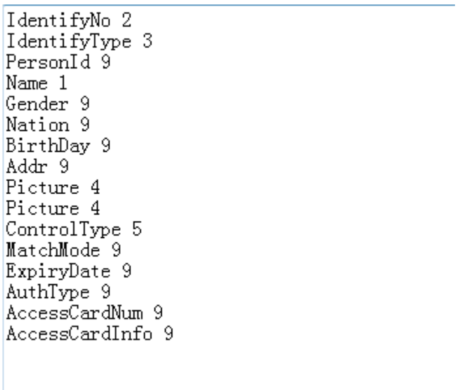
Note: The pictures in the folder will display in the sequence of file names.

6) After inputting all the personnel information, the status bar will show the number of processed entries and indicate starting compression; click “Compression” and there will be a file named “kedacom.zip” generated under directory “compression”.
7) Uncompress “kedacom.zip” and obtain “config.csv” and processed personnel pictures, which are renamed in the format of certificate number.
8) Check if the data is wrong. If it’s all correct, edit “config.csv” file; copy any row and add it to the top and the bottom.

Note: When editing “config.csv” file, you cannot edit through “excel” file but through “text document” or other file editor such as “editplus”.

9) Open “map.txt” file, edit as the following picture indicates. The number behind the line means the column number in the “config.csv” file.

Note: For example, “Name 1” means the person’s name is in the first column of “config.csv” file; “IdentifyNo 2” means the unique ID is in the second column of “config.csv” file.



```
IdentifyNo 2
IdentifyType 3
PersonId 9
Name 1
Gender 9
Nation 9
BirthDay 9
Addr 9
Picture 4
Picture 4
ControlType 5
MatchMode 9
ExpiryDate 9
AuthType 9
AccessCardNum 9
AccessCardInfo 9
```

10) Comparing with “map.txt” file, find the corresponding columns in “config.csv” and modify the parameters. Edit “config.csv” and “map.txt” files and make sure the relationship and personnel information are all correct.
11) Rename the file “config.csv” as “user.csv”; after confirmation, compress the files of “images”, “user.csv” and “map.txt” into .zip file.

- Import through web client

Log into the web client of the device; go to **Settings > Access Control > Personnel > Import**, and click “Import” to pop up a dialogue box indicating “Would you like to import personnel info?”; click “Confirm”, browse and open the .zip file compressed in the above steps, and when the progress bar is full, the importing is finished.