KEDACOM

User Manual for Access Control System

V1.1 (May, 2020)

Trademark

Kedacom™ and KEDACOM™ are 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
http://www.kedacom.com/en
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 in the preparation of 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

Applicable Models

KSCA120 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.

Contents

1. Product Brief

KSCA120 series are a kind of face recognition access control and attendance system. It supports multiple opening modes, including face/card, face & card, 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 people access needs to be controlled.

Picture 1-1 Product Appearance

Features:

- 2.0MP 1/2.8” high-performance image sensor, 0.0001 Lux starlight low illumination imaging;
- H.265/H.264 encoding, 1080P@30fps HD live video;
- 5-inch capacitive touch screen, show face comparison information and provide good man-machine interaction;

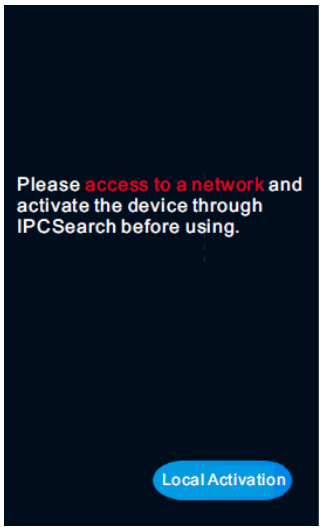
- Binocular UHD wide-angle lens, face recognition distance 0.3~2m, suitable for height range 1.2 to 1.9m;
- Deep-learning algorithm, support 2,0000-face archive and 100,000-card archive, fast recognition speed and high accuracy rate;
- Live face detection, prevent photo-fraud and video-fraud effectively;
- Intelligent facial fill light, enable fill light automatically according to the light condition to suit outdoor backlight;
- Support multiple opening modes, including face/card, face & card, 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 RS485 port, to connect to access control system;
- Built-in MIC and speaker, support two-way audio and voice broadcast;
- Support WiFi for convenient internet service;
- Support extending card reader, support people and card verification and registration;
- TF card local storage (maximum 256 G), support ANR;
- IP66-rated water-proof and dust-proof, -40°C~+60°C wide temperature range, to suit outdoor severe environment.

2. Device Touch Screen

2.1 Startup

2.1.1 Local Activation

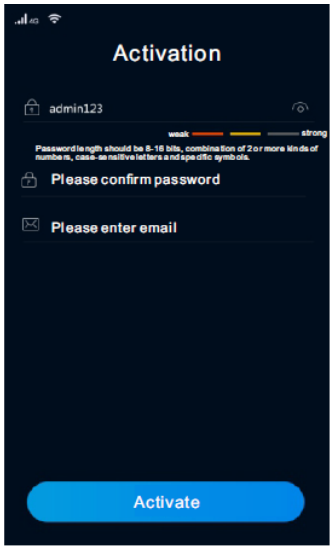
Electrify and start the device. If the device is not activated before use, it will come to the activation interface automatically.



Picture 2-1 Activation prompt

Operation steps are as follows:

- Tap “Local Activation” on the interface;



Picture 2-2 Local activation

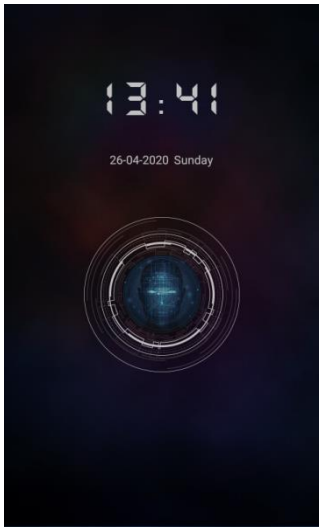
- Enter password, confirm password, and the email address for claiming password;
- Tap “Activate” to activate the device.

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.

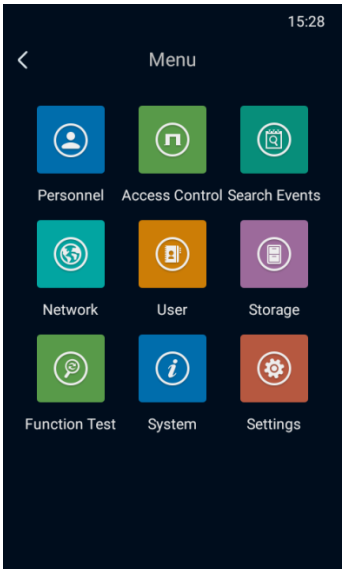


Picture 2-3 Stand-by interface

- If the man is in the database and the face recognition score reaches the standard, it will show verification succeeded and display the man's name at the bottom of the screen.
- If the man is out of the database, it will show verification failed.

2.2 Login

After logging into the device, user can perform operations such as personnel management, access control configuration, event search and etc.



Picture 2-4 Menu

- Login

  1) Long-press on the touch screen for over 3 seconds and the login interface will pop up;

  2) Enter the password set during activation;

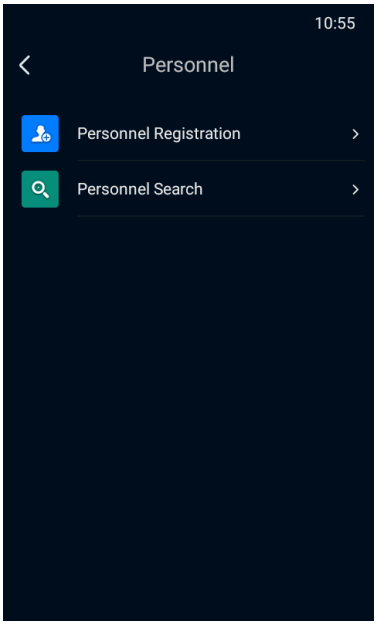
  3) Click “OK” to enter menu interface.

- Exit

  Tap the “<” key at top left corner of the screen and tap “OK” to exit login and return to stand-by interface.

2.3 Personnel Management

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

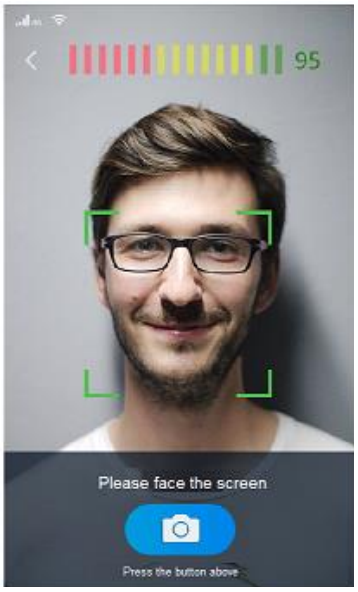


Picture 2-5 Personnel management

2.3.1 Personnel Registration

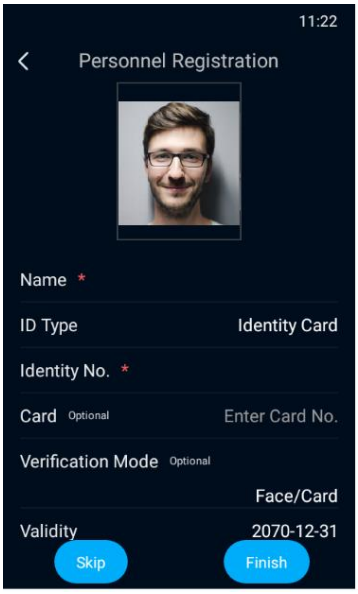
Tap **Menu>Personnel>Personnel Registration**, and add new user and register information such as name, ID type, Identity ID and etc.

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



Picture 2-6 Personnel registration

2) Tap “OK” to enter the information registration interface and input name, ID type, Identity ID and etc.



Picture 2-7 Register information

3) Tap “Finish” to complete personnel registration;

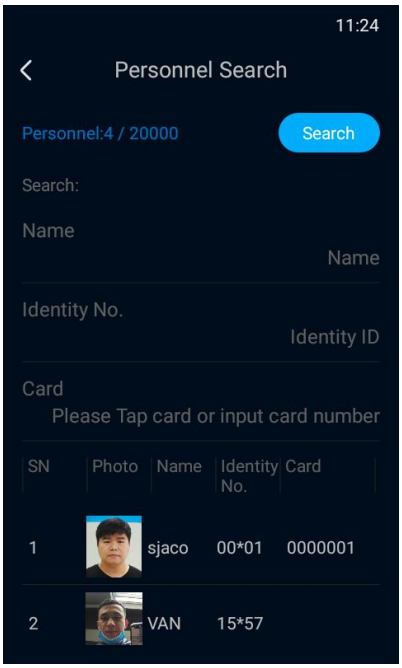
Note: If the identity ID of the same ID type already exists when saving the information, it will pop up “the identity ID already exists, please confirm if you would like to save.” Tap “OK” to overwrite the old data.

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

Note: The snapshot may fail when not facing the camera rightly or the distance to the camera being too close or too far. When it occurs, tap “Snapshot Again” to re-capture.

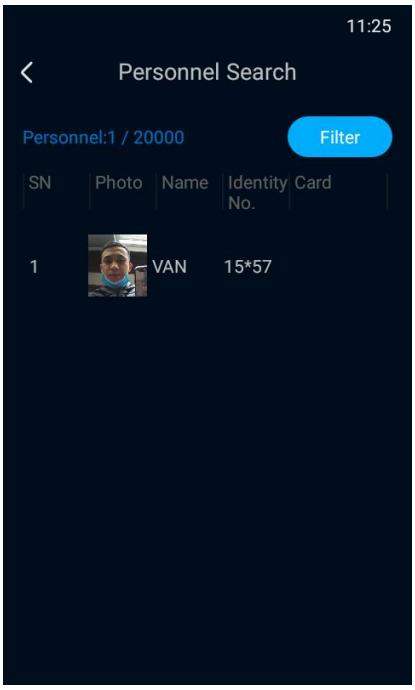
2.3.2 Personnel Search

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



Picture 2-8 Personnel search

Input name, identity ID and/or card number and tap “Search” to enter the information interface.



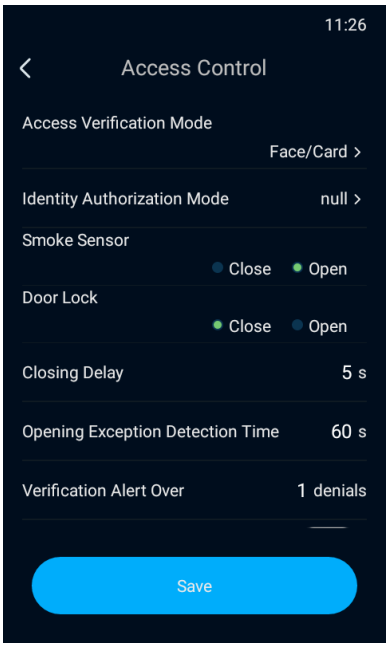
Picture 2-9 Search result

The searched personnel will show on the list; select any one and tap to view the details.

Tap “Filter” to return to the personnel search interface and re-input the search conditions.

2.4 Access Control Configuration

Tap **Menu>Access Control** to configure default verification mode, temporary authorization mode, smoke sensor, door magnetism, closing delay, opening exception detection time, alarm threshold and tamper alarm. Tap “Save” to finish configuration.



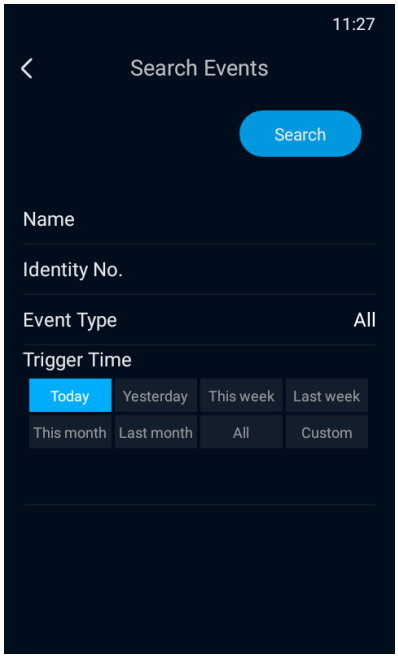
Picture 2-10 Access control

- Default Verification Mode: Tap “Default Verification Mode” and select a verification mode on the popup interface, options including “Face”, “Card”, “Face & Card” and “Face/Card”.
- Temporary Authorization Mode: Configure the authorization mode for different verification modes. Tap “Temporary Authorization Mode” and select the mode(s) on the popup interface, options including “Face”, “Card” and “Face and Card”. Tap “OK”.
- Smoke Sensor: Select “Close” or “Open”, by default “Open”.
- Door Magnetism: Select “Close” or “Open”, the default being “Close”. When selecting “Close”, the door magnetism port SENS connects to the door magnetism switch NC port, and GND to door magnetism COM port; when selecting “Open”, the door magnetism port SENS connects to the door magnetism switch NO port, and GND to door magnetism COM port.
- Closing Delay: Configure the delay time from door opening to door closing, the range being 1~255 s, the default being 5 s.

- Opening Exception Detection Time: 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.
- Alarm Threshold: Configure the maximum times of recognition failures, the range being 1~255 times, the default being 5 times; if the recognition failure exceeds the maximum times, an alarm will be triggered.
- Tamper Alarm: Turn on “Tamper Alarm” to enable tamperproof button alarming. After enabling this function, when the tamperproof button is triggered, the device will alarm.
- Card Type: Configure the supported card types for card recognition, options including “Citizen Card”, “CPU Card”, “M1 Card” and “IC Card”.

2.5 Search Events

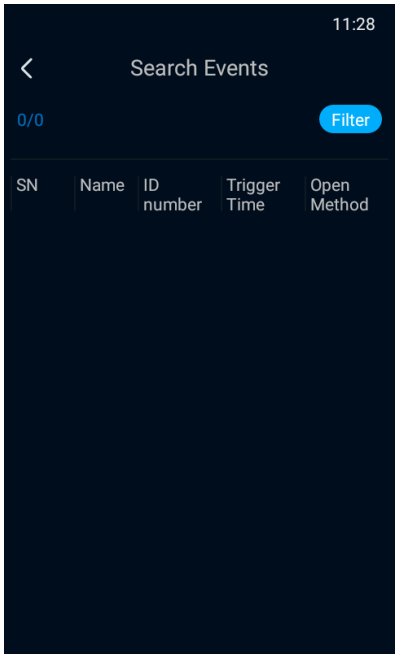
Tap **Menu>Search Events** and search event records.



Picture 2-11 Search events

Input name, identity ID, event type and/or trigger time and tap “Search” to search expected event records; options for event type include “All”, “Face”, “Card”, “Face and Card Verification”, “Door Switch”, “Help Center”, “Fire Alarm”, “Abnormal Unlocked”, “Help User”, “Authorization Code” and etc.; options for trigger time include “Today”, “Yesterday”, “This week”, “Last week”, “This month”, “Last month”, “All” or “Custom”, which requires manual input of start time and

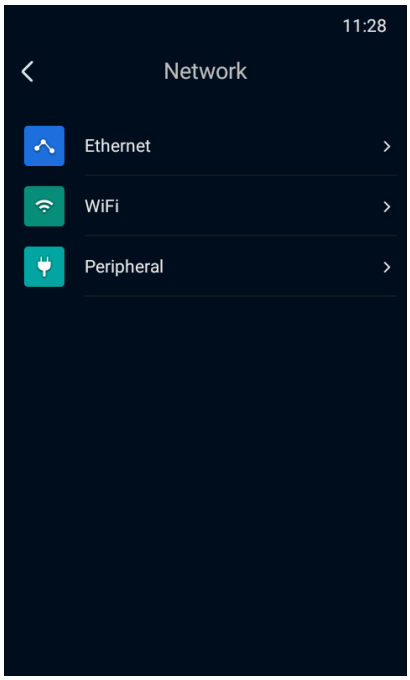
stop time; tap “Search” to view the events filtered by name, identity ID, event type and trigger time.



Picture 2-12 Search result

2.6 Network

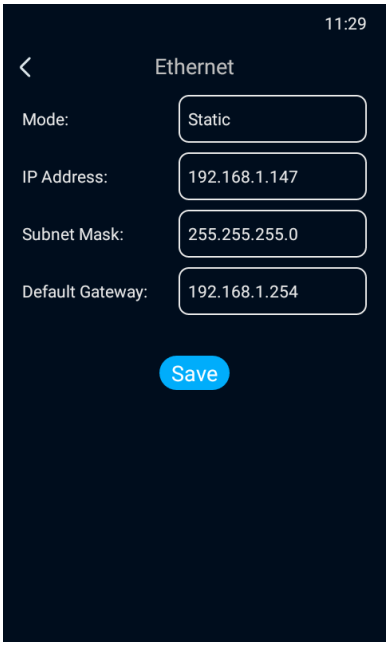
Tap **Menu>Network** and configure Ethernet, WiFi and Peripheral.



Picture 2-13 Network

2.6.1 Ethernet

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

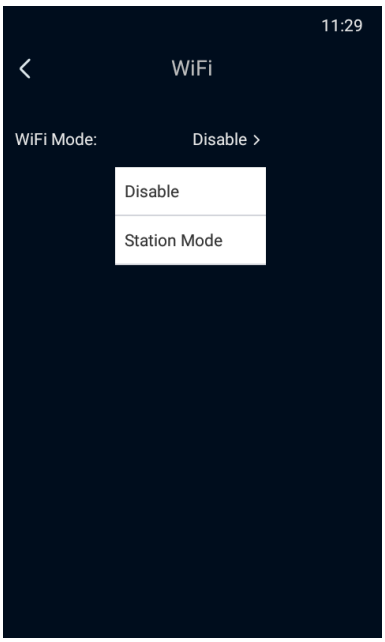


Picture 2-14 Ethernet

Select “Mode”. If selecting “Static”, input “IP Address”, “Subnet Mask” and “Default Gateway” manually; tap “Save” to finish configuration.

2.6.2 WiFi

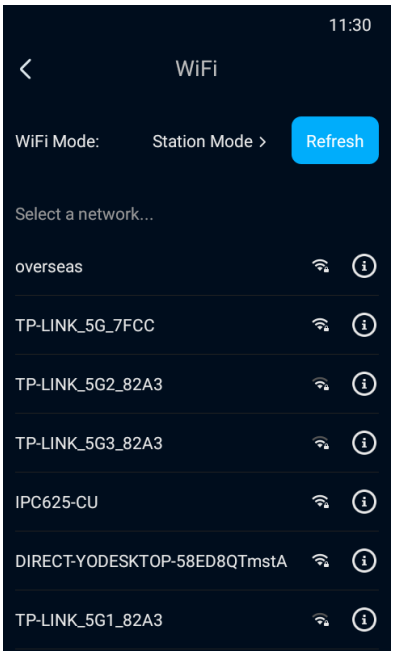
Tap **Menu>Network>WiFi** and configure WiFi parameters. WiFi mode options include “Disable” and “Station Mode”.



Picture 2-15 WiFi

- Station Mode

  Under “Station Mode”, the device can be connected to AP hotspot.

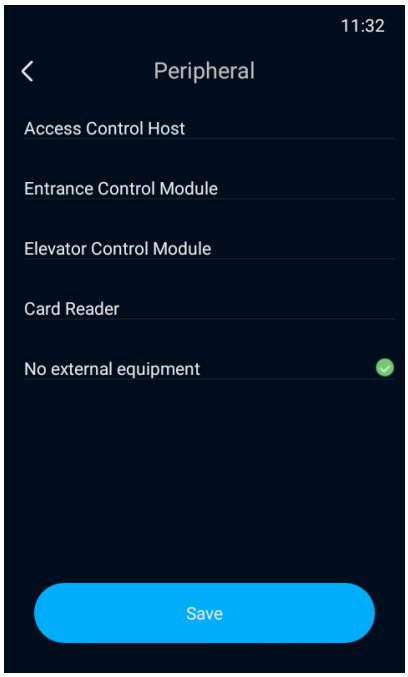


Picture 2-19 Station mode

Tap “Refresh” and the nearby AP hotspots will show on the list below. Select a hotspot from the list and enter the “WiFi Setting” interface; select mode according to actual request, including “Static” and “Dynamic”, the latter being the default and if selecting the former, configure IP address manually; input “Password” and tap “Save” to connect to the selected WiFi network.

2.6.3 Peripheral

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

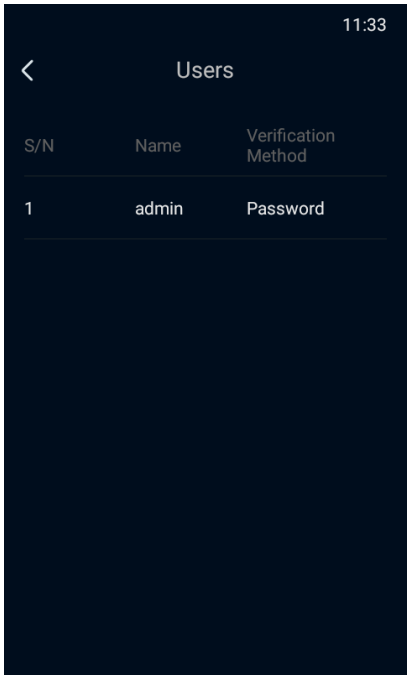


Picture 2-20 Peripheral

Select a peripheral device, options including “Access Control Host”, “Entrance Control Module”, “Elevator Control Module”, “Card Reader” and “No external equipment”. Tap “Save” to finish.

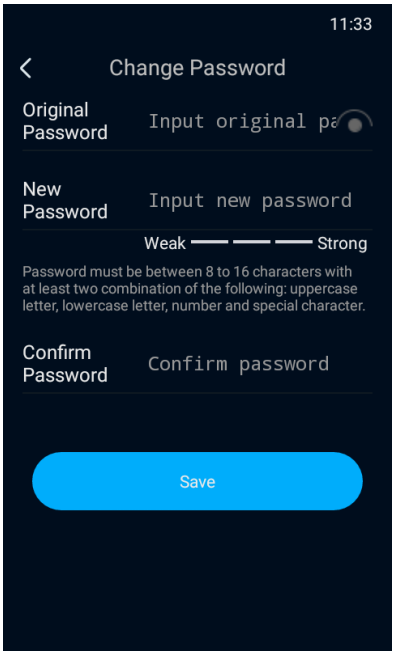
2.7 User

Tap **Menu>User** and edit the password for “admin” user.



Picture 2-21 User

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



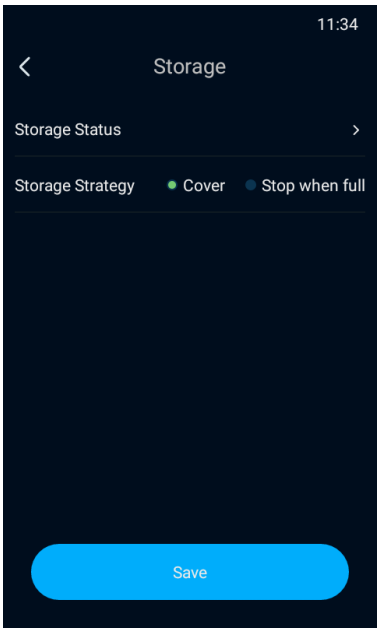
Picture 2-22 Change password

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.

2.8 Storage

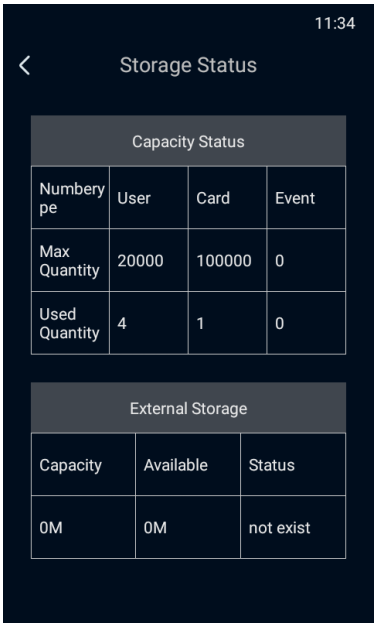
Tap **Menu>Storage** and view the “Storage Status” and “Storage Strategy”.



Picture 2-23 Storage

- Storage Status

Tap “Storage Status” to enter “Storage Status” interface and view “Capacity Status” and “External Storage”.



Picture 2-24 Storage status

- Capacity Status: This table shows the “Max Quantity” and “Used Quantity” of “User”, “Card” and “Event”.
- External Storage: This table shows the “Capacity”, “Available” and “Status” of external storage.

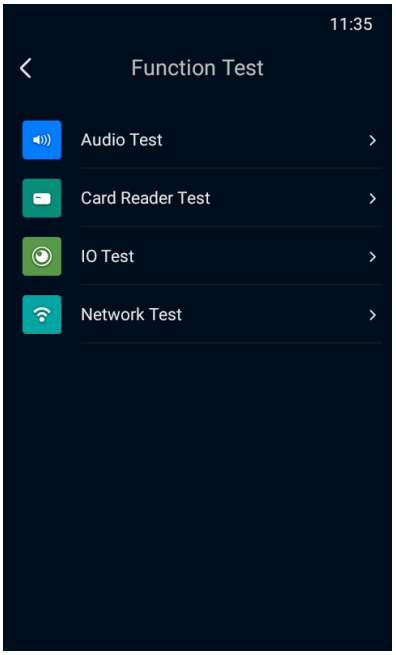
- Storage Strategy

Tap to select the storage strategy, options including “Cover” and “Stop when full”. If selecting “Cover”, when the storage is full, the device will cover the earliest data automatically; if selecting “Stop when full”, when the storage is full, the device will stop storing data.

After finishing configuration, tap “Save”.

2.9 Function Test

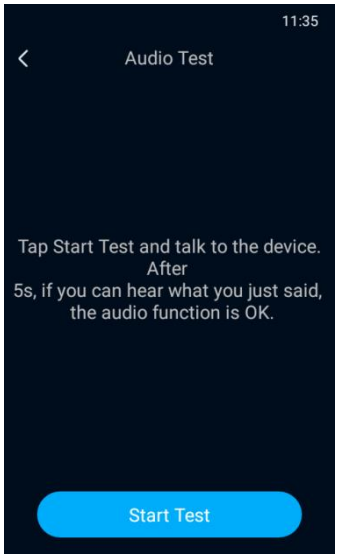
Tap **Menu>Function Test** and perform “Audio Test”, “Card Reader Test”, “IO Test” and “Network Test”.



Picture 2-25 Function test

2.9.1 Audio Test

Tap **Menu>Function Test>Audio Test** and test the audio function of the device and check if it is normal.

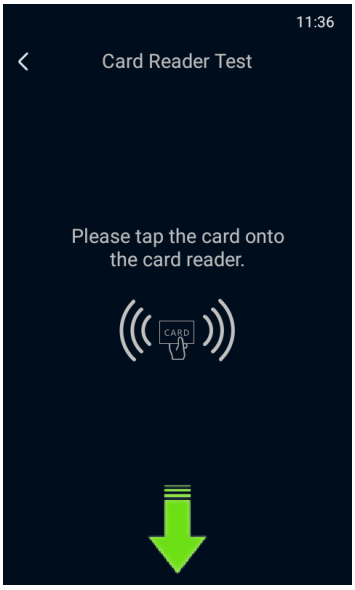


Picture 2-26 Audio test

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

2.9.2 Card Reader Test

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

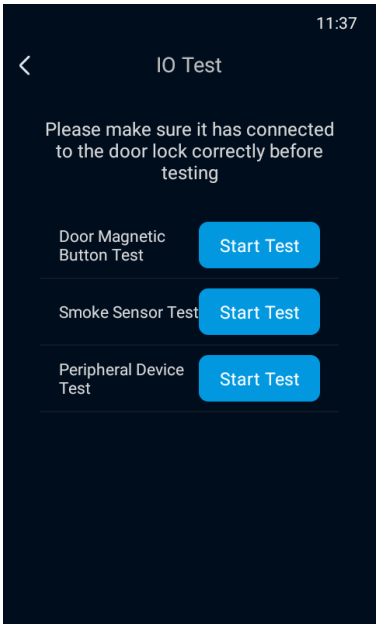


Picture 2-27 Card reader test

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.

2.9.3 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.



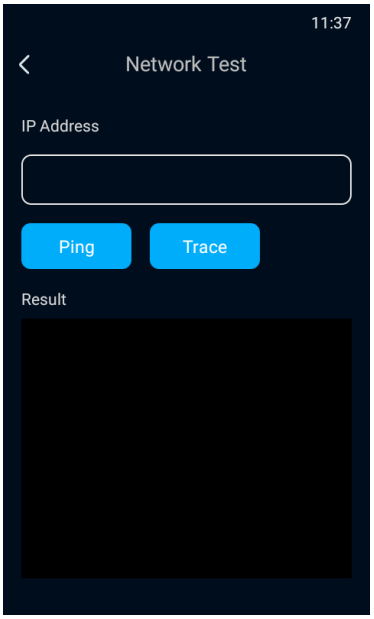
Picture 2-28 IO test

- Door Magnetic Button Test: Confirm the device is connected to the doo lock correctly. Tap “Start Test” and if the door lock is normal, the door megnetic button triggers normally.
- Smoke Sensor Test: Confirm the device is connected to the doo lock correctly. Tap “Start Test” and if the door lock is normal, the smoke sensor triggers normally.
- Peripheral Device Test: Confirm the device is connected to the doo lock correctly. Tap “Start Test” 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 the “Function Test” interface.

2.9.4 Network Test

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

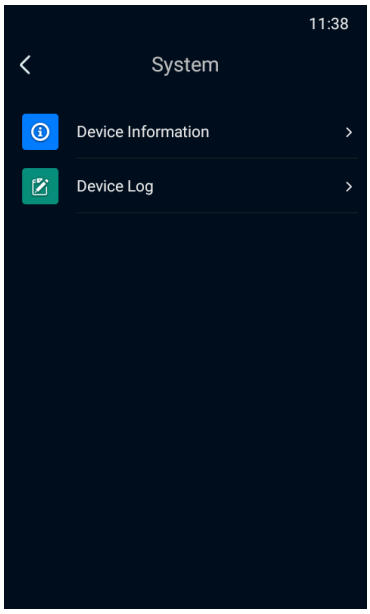


Picture 2-29 Network test

- In “IP 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 “IP 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.

2.10 System

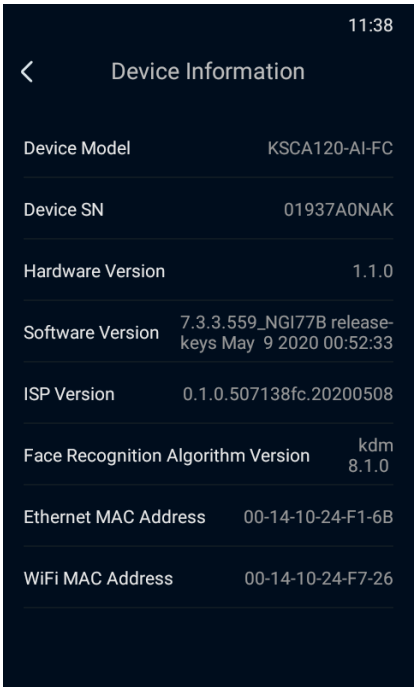
Tap **Menu>System,** and view device information and device log.



Picture 2-30 System

2.10.1 Device Information

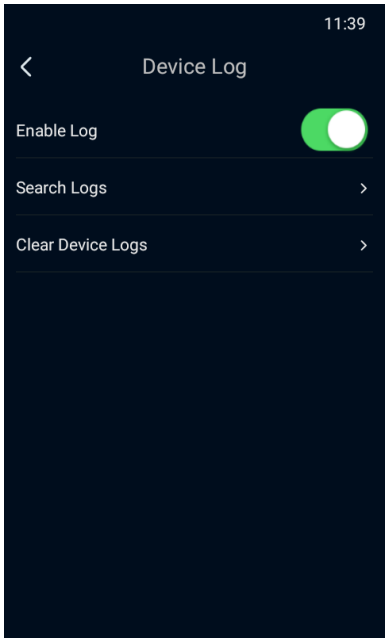
Tap **Menu>System>Device Information** and view information such as “Device Model”, “Device SN”, “Hardware Version”, “Software Version”, “ISP Version”, “Ethernet MAC Address”, “WiFi MAC Address” and etc.



Picture 2-31 Device information

2.10.2 Device Log

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



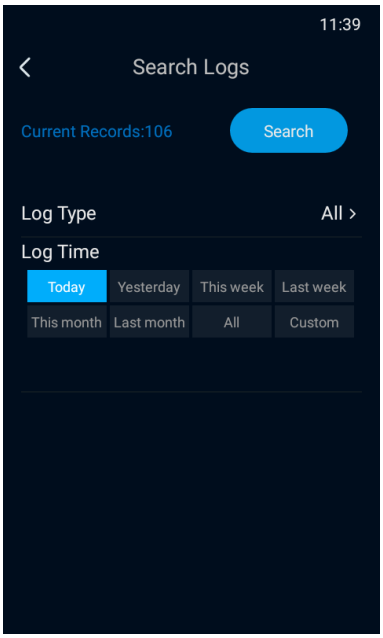
Picture 2-32 Device log

- Enable Log Records

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

- Search Logs

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



Picture 2-33 Search logs

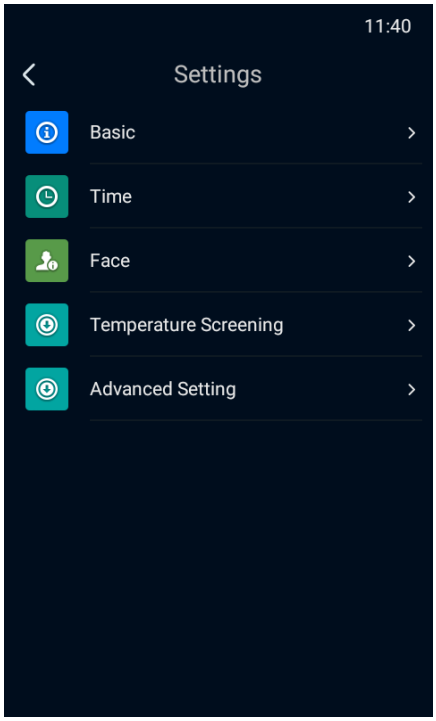
Tap “Log Type” and select a type, options including “All”, “User Operation”, “Alarm”, “System Task” and “System Exception”; select “Log Time”, options including “Today”, “Yesterday”, “This Week”, “Last Week”, “This Month”, “Last Month”, “All” and “Custom”. When selecting “Custom”, user needs to input “Start Time” and “Stop Time”; tap “Search” and view log information such as “Username”, “User IP Address”, “Log Record Time” amd “Log Content”.

- Clear Device Logs

Tap “Clear Device Logs” and select "OK" on the popup interface to delete device logs.

2.11 Settings

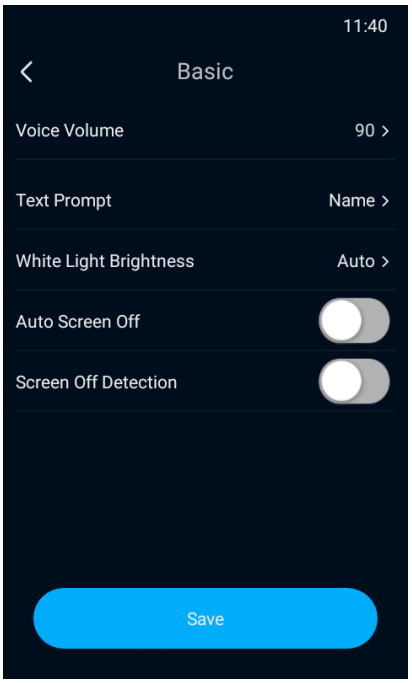
Tap **Menu>Settings** and configure “Basic”, “Time”, “Face” and “Advanced” parameters.



Picture 2-34 Settings

2.11.1 Basic

Tap **Menu>Settings>Basic** and configure “Voice Volume”, “Text Prompt”, “White Light Brightness”, “Auto Blackout Duration” and “Blackout Detection”.



Picture 2-35 Basic information

- Voice Volume

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

- 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”, “Name & ID” and “Disable”; if selecting “Disable”, when the device recognizes a user, there will be no text prompt; tap “Save” to validate setting.

- White Light Brightness

Tap “White Light Brightness” and enable or disable “Self-Adaptive Brightness”; if enabled, the device will adjust white light brightness automatically according to the environment luminance; if disabled, drag the slide bar below to configure white light brightness manually, the range being 0~100 and the default being 50; tap “Save” to validate setting.

- Auto Blackout Duration

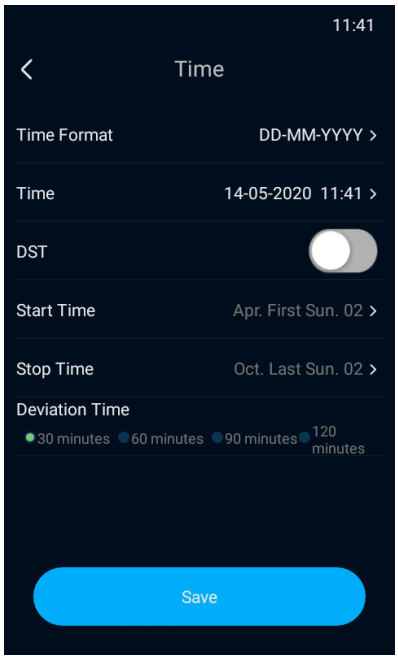
Tap “Auto Blackout Duration” to enable or disable the function. If enabled, you can configure the auto blackout time, the range being 10~300 s. If no operation is done to the device in the configured duration, the device will go in stand-by mode. If disabled, the device will not black out automatically.

- Blackout Detection

  Tap “Blackout Detection” to enable or disable blackout detection.

2.11.2 Time

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



Picture 2-36 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.

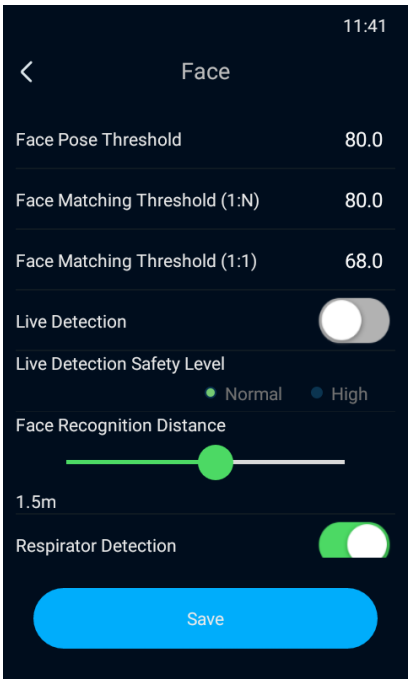
- DST: Tap “DST” to enable or disable DST, and configure “Start Time”, “Stop Time” and “Deviation Time”.

- 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.
- Stop Time: Tap “Stop Time” to enter time setting interface and configure DST stop 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.

2.11.3 Face

Tap **Menu>System>Face** and configure “Face Pose Threshold”, “Face Matching Threshold (1:N)”, “Face Matching Threshold (1:1)”, “Live Detection”, “Live Detection Safety Level”, “Face Recognition Distance” and “Respirator Detection”.



Picture 2-37 Face

- Face Pose Threshold: Configure the threshold score for face recognition, the range being 0~100 points. The device will value face pose from the perspective of vertical pitching angle, horizontal level angle and interorbital distance; if the score is lower

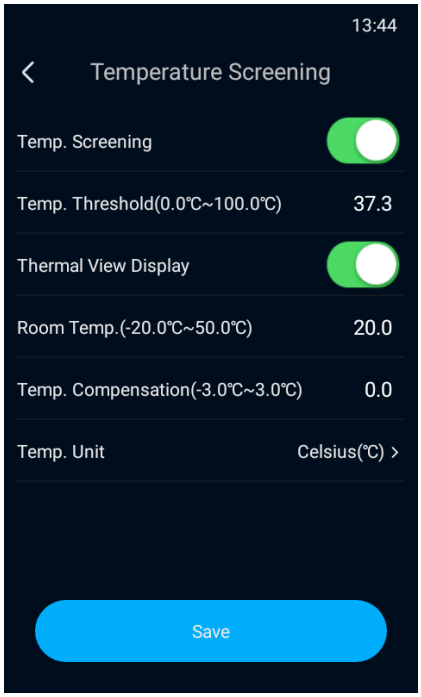
than the preset one, the face recognition will not pass, and face matching or face inputting will fail.

- Face Matching Threshold (1:N): Configure the threshold score for face matching 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 Matching Threshold (1:1): Configure the threshold score for face matching 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.
- Live Detection: Tap the “Live Detection” button to enable or disable live detection function. After enabling the function, the device will judge if the object is the living man himself/herself, and will distinguish it from fraudulent images such as photo, false face, mask, shielding, screen video duplicate and etc.; if the object is not the living man himself/herself, face matching or face inputting will fail.
- Live Detection Safety Level: After enabling “Live Detection”, you can configure live detection safety level, “Normal” or “High”; if selecting “High”, the false recognition rate will be low and the rejection rate will be 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.
- Respirator Detection: Tap “Respirator Detection” button to enable or disable the function.

Tap “Save” to validate setting.

2.11.4 *Temperature Screening

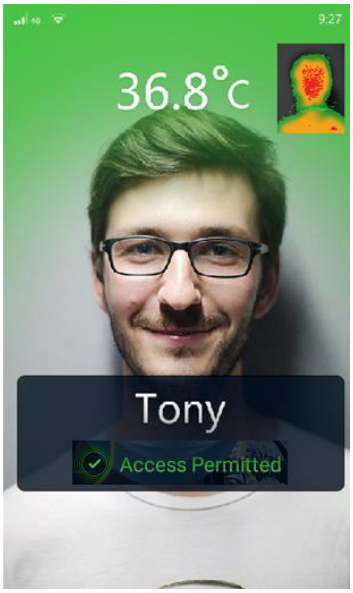
Tap **Menu>System>Temperature Screening** and configure “Temp. Screening”, “Temp. Threshold”, “Thermal View Display”, “Room Temp.”, “Temp. Compensation” and “Temp. Unit”.

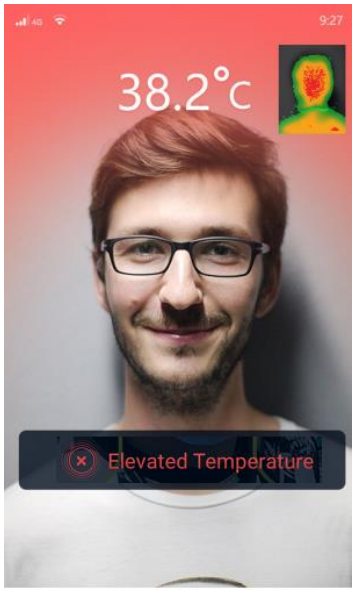


Picture 2-38 Temperature screening

Note: Temperature screening is only available on fever screening models.

- Temp. Screening: Tap the button to enable or disable the function of temperature screening.
- Temp. Threshold: Configure the temperature threshold for triggering an alarm, the range being 0.0°C~100.0°C. You can configure it 37.3°C, and when someone is measured over 37.3°C, the system will trigger an alarm.



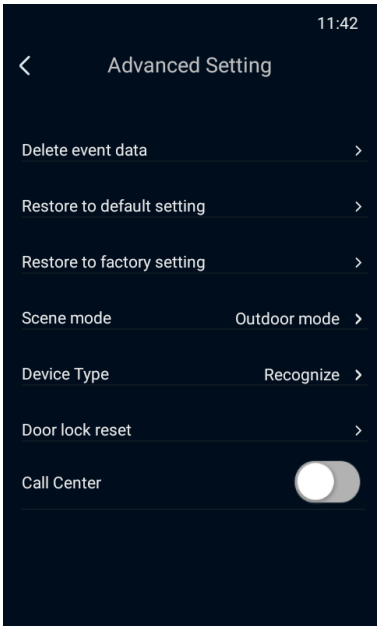


Picture 2-39 Temperature threshold

- Thermal View Display: Tap the button to show or hide thermal view on the screen.
- Room Temp.: The range is -20.0°C~50.0°C, and the default is 20.0°C. Only when the room temperature is extremely hot or cold, you need to configure this parameter; otherwise, remain the default value.
- Temp. Compensation: The range is -3.0°C~3.0°C, and the default is 0.0°C. Usually it's unnecessary to configure this parameter.
- Temp. Unit: Select "Celsius(°C)" or "Fahrenheit(°F)" according to actual request.

2.11.5 Advanced

Tap **Menu>Settings>Advanced** to delete event information, restore to default setting, restore factory default, configure scene mode and call for help.



Picture 2-40 Advanced

- Delete Event Data

  Tap "Delete Event Data" and it will pop up a prompt dialogue box. Tap "OK" and the device will clear all event information.

- Restore to Default Setting

Tap “Restore to Default Setting” and and it will pop up a prompt dialogue box. Tap “OK” and the device will reboot automatically and restore to default setting.

- Restore Factory Setting

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

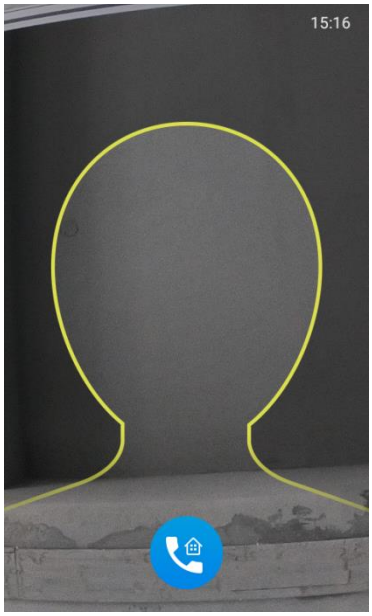
- Scene Mode

Select a mode according to the installation of the device, options including “Ourdoor Mode” and “Indoor Mode”.

- Call Center

Tap “Call Center” to call the back-end center and start talking when there is a response; tap “Hang Up” to end talking. If the dialogue is more than 2 minutes, the device will hang up automatically. To continue talking, tap “Call Center” again.

.



Picture 2-41 Call for help

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

Tap “Save” to validate setting.

3. Web Client

3.1 Startup

For device installation and wiring, please referred 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:

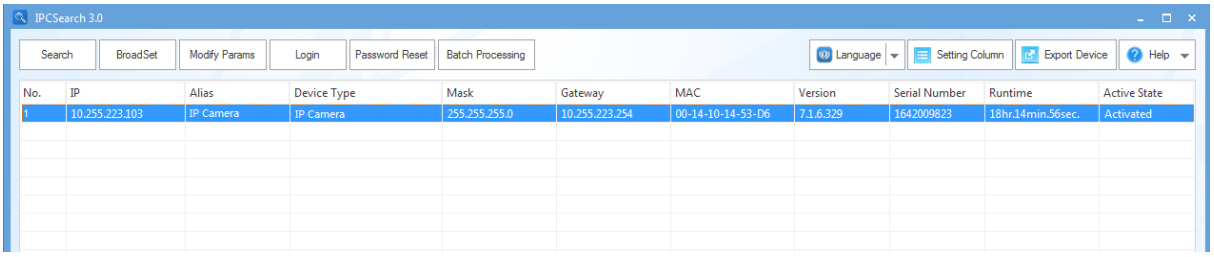
- Processor: 3.3 GHz Intel CORE®i3 series and later version or other equivalent processors
- RAM Memory: 4GB or above
- Operating System: Windows 7 or later
- Browser: Suggest using Kernel browser, otherwise it will affect some functions of the client
- DirectX：9.0c

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.

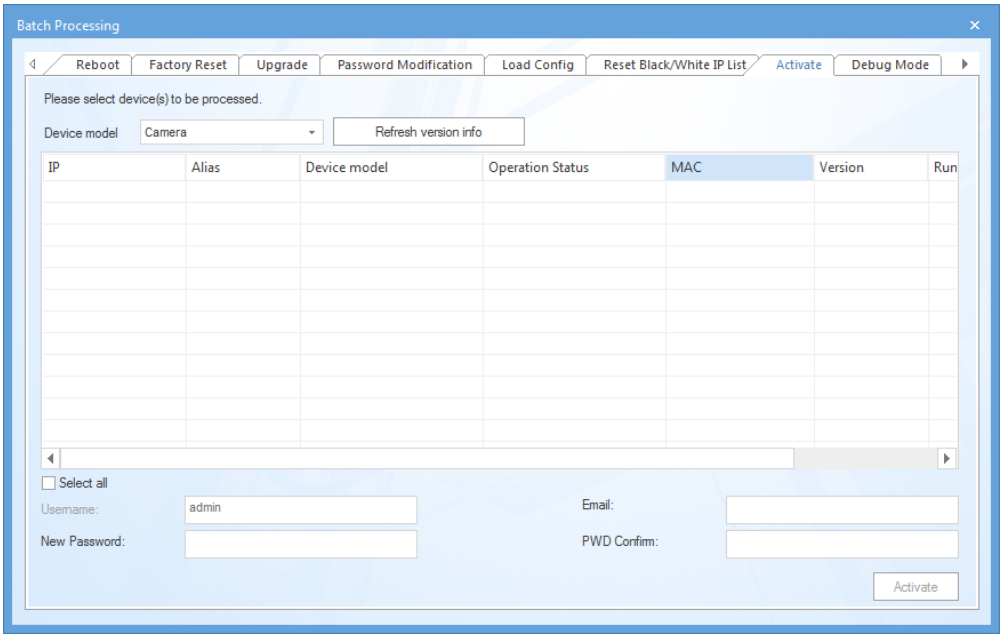


Picture 3-1 IPCSearch

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.

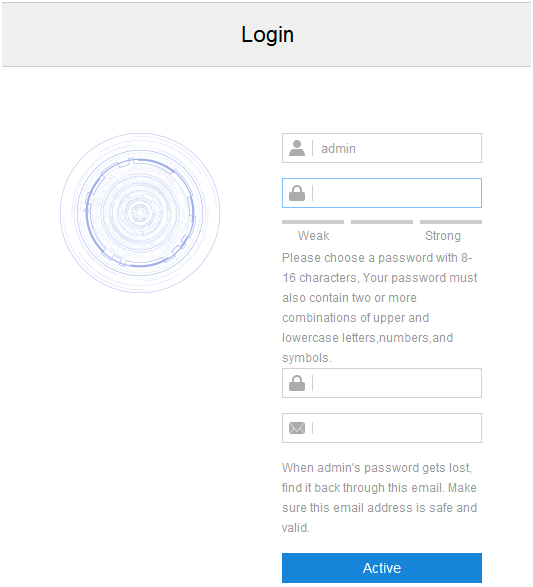
Note: When there are more than one non-activated devices, select the device and click “**Batch processing**”. On the popup interface, set admin user’s password and the email address to claiming password. Click “**Activate**” and wait for rebooting.



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 in browser. The device activation interface will pop up, as shown below:



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 activation automatically. Operate according to the prompts to finish activation. Please refer to chapter 2.1.1 for details.

Note:

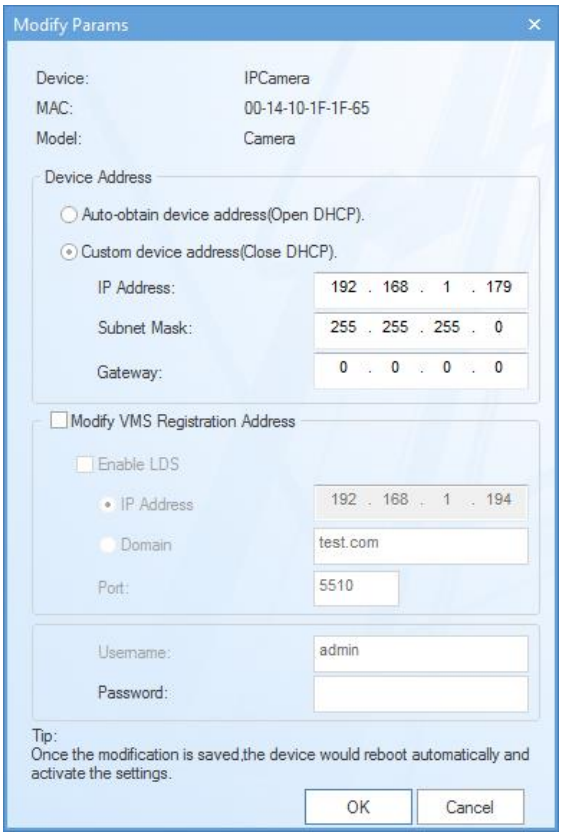
- To ensure the safety of device on internet, it is strongly recommended that you set a strong password composed of at least 2 kinds of the following, numbers, upper-case letters, lower-case letters or specific symbols with length of 8 to 16 characters.
- Please modify the password periodically such 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.

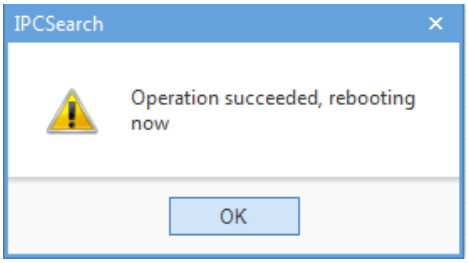
1) Run IPCSearch and the system will search the cameras in LAN automatically and display the result on the list;

2) Select a camera 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.



Picture 3-4 Modify Parameter

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



Picture 3-5 Camera Reboot

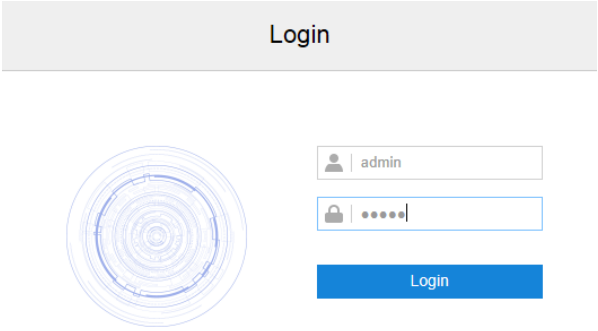
Note: For more network parameters of the camera, login to the web client and configure.

3.1.3 Login and Log Out of the Web Client

- Login to the Web Client

After activating the camera and modifying its network parameters, the camera will reboot automatically. After rebooting, select either of the following methods to login:

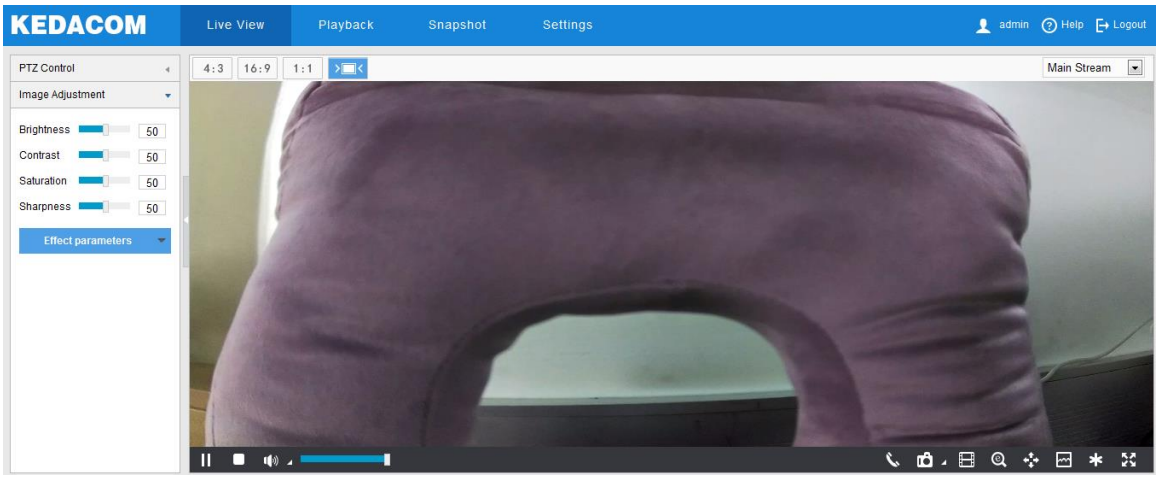
- Select the device from IPCSearch and click “Login” or double-click the line which the device is in to enter the web client. Input username and the password set during activation and click “**Login**”.
- Input camera IP address in the browser to enter the login interface. Input username and the password set during activation and click “**Login**”.



Picture 3-6 Web Client Login Interface

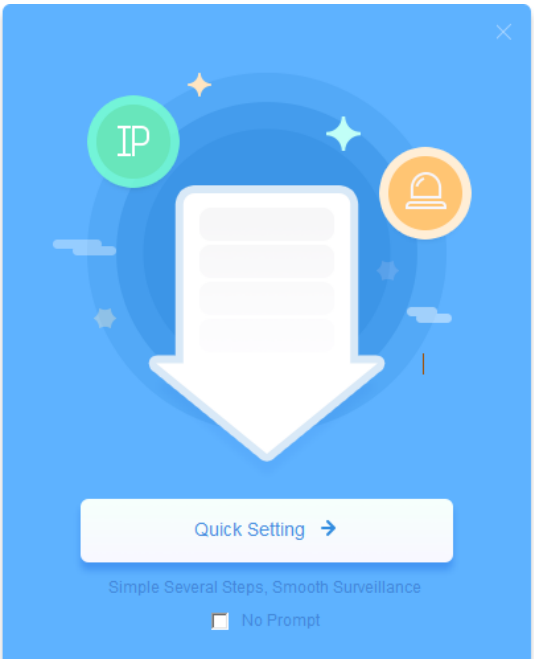
After login successfully for the first time, download and install the plug-in according to the prompts. Close the browser when installing the plug-in. After finishing, re-login and enter the following interface.

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

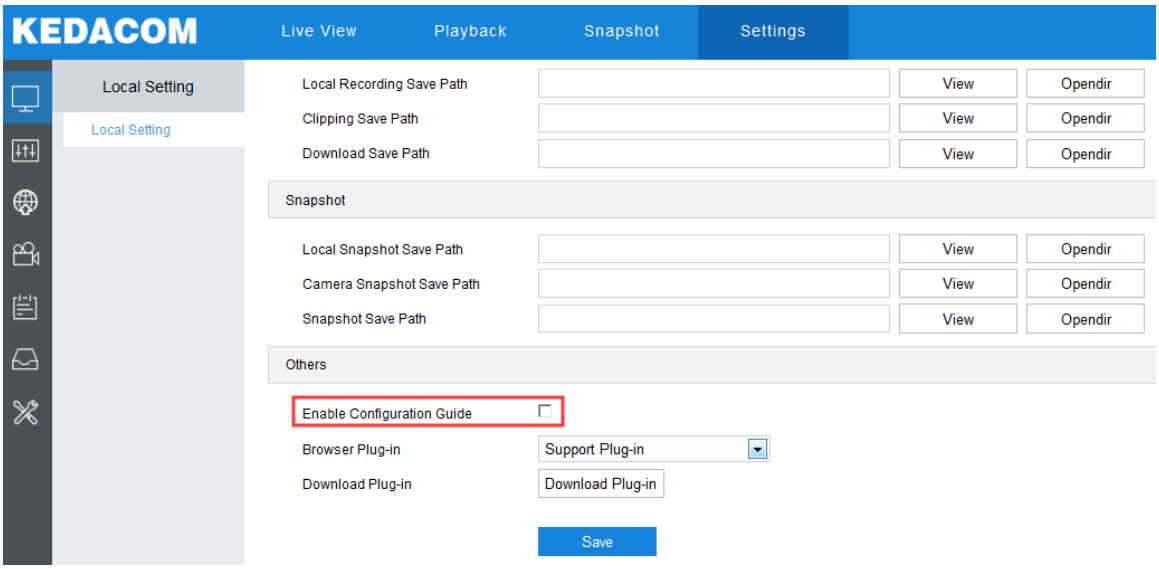


Picture 3-7 Web Client Interface

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



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 

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

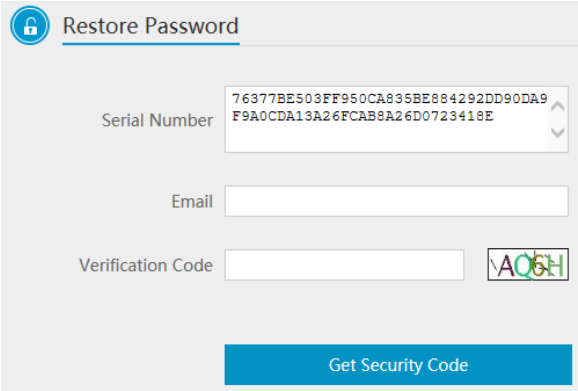
3.1.4 Reset Password

If user enters a wrong username or password for 6 times (configurable), the camera IP will be locked up for 10 minutes (configurable), 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:

Picture 3-10 Password Reset

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



Picture 3-11 Password Reset

3) Login to the email address to get a security code and fill in "**Command**" blank in Picture 2-10 and click "**OK**". Please remember the new password on the popup window and click "OK". The device will reboot.

3.1.5 Main Interface

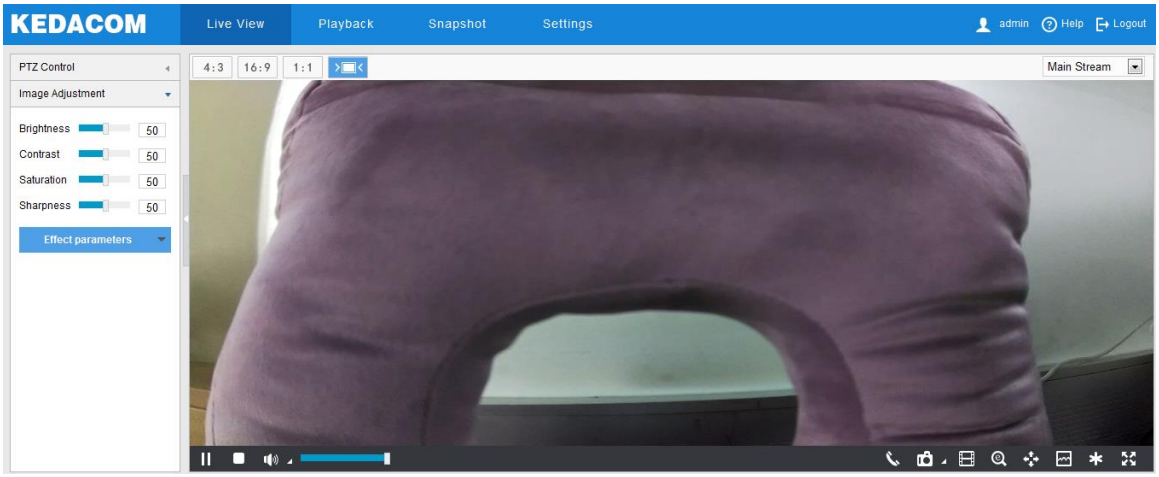
On the main interface of the client, you can view live video, playback video records, manage snapshots and configure settings.

- 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

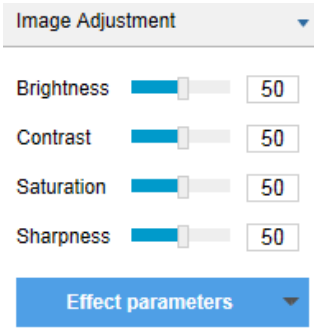
Click “Live View” to enter the preview interface.



Picture 3-12 Live View

3.2.1.1 Image Adjustment

Click Image Adjustment to show the following interface:



Picture 3-13 Image adjustment

Drag the slide bar to adjust the brightness, contrast, saturation and sharpness of the preview image, or configure the values beside the slide bar.

- **Brightness:** Drag Brightness slide bar to adjust image brightness by request. The higher the value is, the brighter the image will be.
- **Contrast:** Drag Contrast slide bar to adjust image contrast by request. The higher the value is, the clearer contrast between the dark and the bright of the image there will be.
- **Saturation:** Drag Saturation slide bar to adjust image saturation by request. The higher the value is, the fresher the image will be.
- **Sharpness:** Drag Sharpness slide bar to adjust image sharpness by request. The higher the value is, the more distinct the objects on the image will look.
- **Effect Parameters:** Load preset image effects according to actual request. Configure in **Settings > Camera > Image**.

3.2.1.2 Live View Window

➢ Aspect Ratio

Icon	Function
4:3	It means the live view window displays image in standard screen ratio 4:3.
16:9	It means the live view window displays image in wide screen ratio of 16:9.
1:1	It means the live view window displays image in actual size 1:1.
	It makes the image window adaptive to your PC resolution.

➢ Stream Selection

Menu	Function
Main Stream	Display HD images. The encoding format of live view, can be set in **Settings > Camera > Video > Encoding Format**.
Secondary Stream	Display SD images. The encoding format of live view, can be set in **Settings > Camera > Video > Encoding Format**.
Third Stream	Display SD images. The encoding format of live view, can be set in **Settings > Camera > Video > Encoding Format**.

Note: Go to **Settings > Camera > Video** and enable “Triple-Stream”. Then “Third Stream” option will display on the live view window.

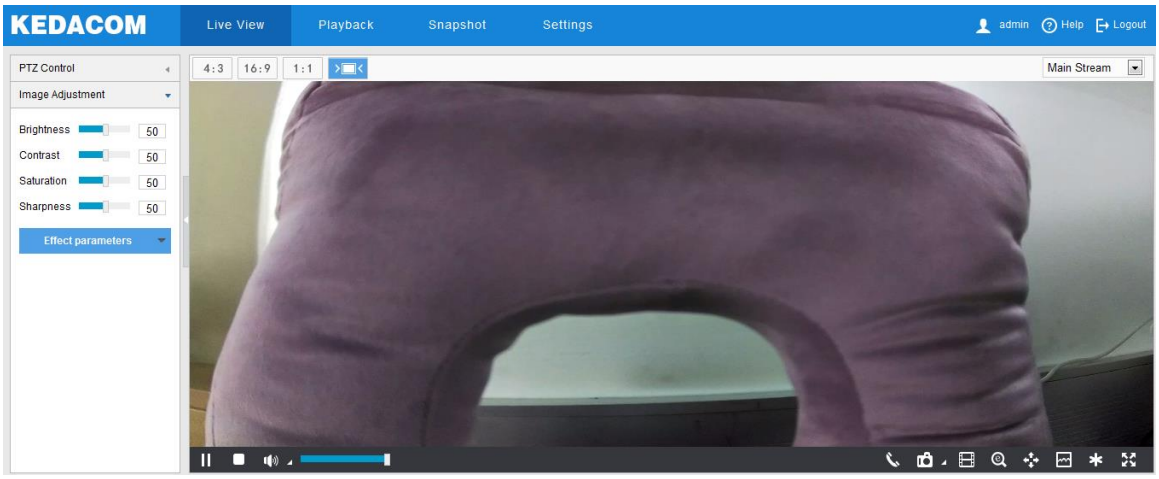
- Toolbar

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 the white triangle icon 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 this button to capture current image. Snapshot includes Camera Snapshot and 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. During video freeze, the PTZ function is disabled.
	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 SD card.



Picture 3-14 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 "Recording Linkage".
- 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 VMS or NVR, 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;

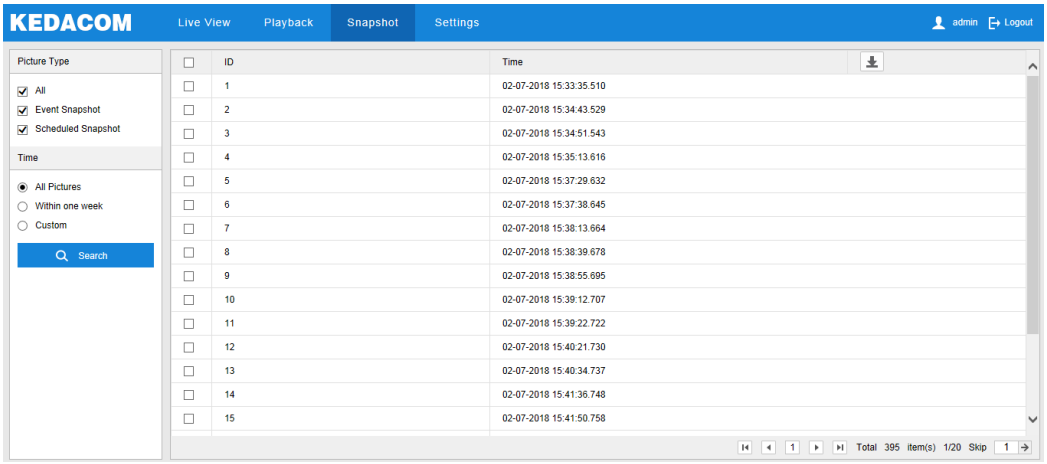
4) Put the cursor of the mouse on the timeline to show the time of the video. Double-click or press the left button of the mouse and drag the timeline to the left or right to skip playing. Alternatively, enter a time under “Go To” and click .

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.
	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 SD card.



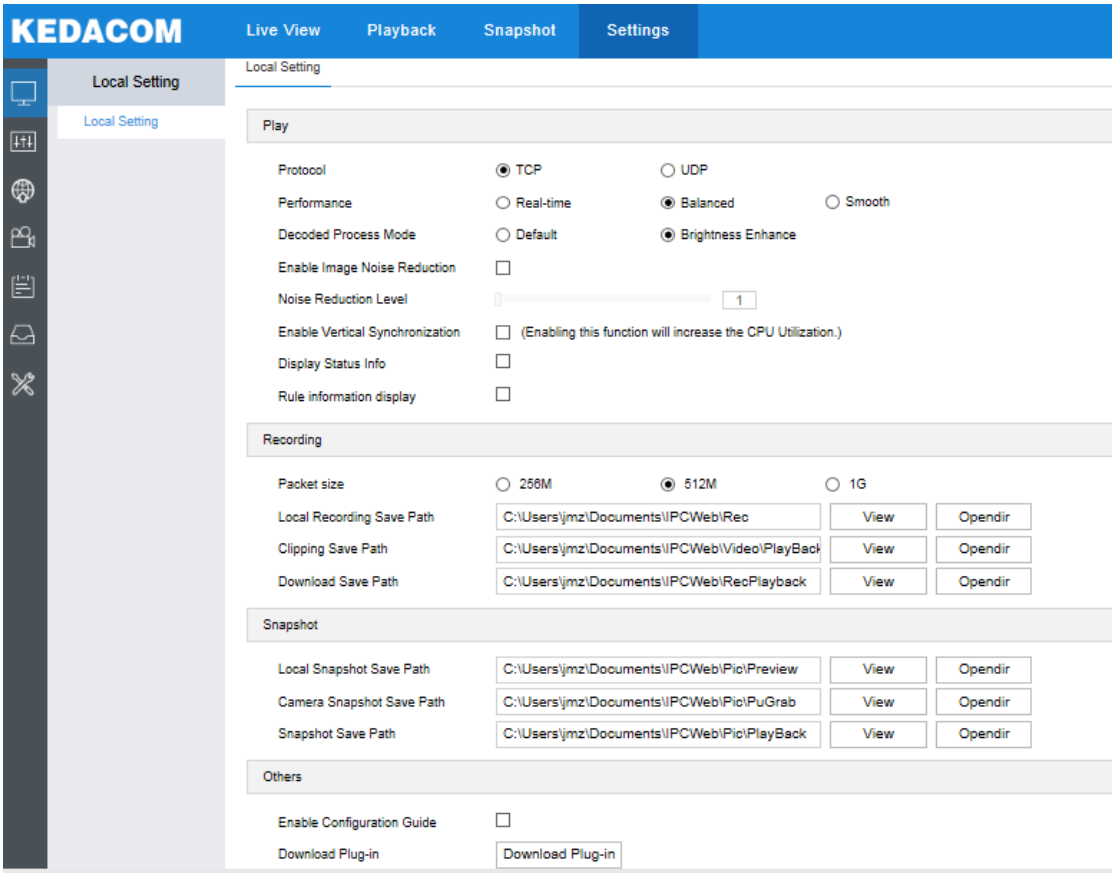
Picture 3-15 Snapshot

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 "**Download**" icon to download the selected pictures. Snapshot save path can be set in Local Setting > Camera Snapshot Save Path.

3.2.4 Local Setting

On the interface of "**Settings > Local Setting**", user can configure parameters of video playing, the size and save path of video records and snapshots on local PC, as shown in the following picture.



Picture 3-16 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 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: Click the button of "**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.

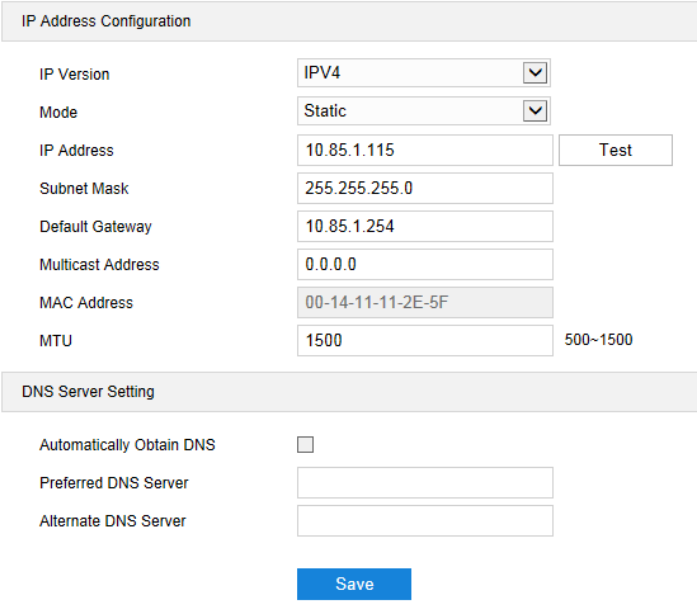
3.3 Network

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

Configure network parameters on the interface of LAN.



Picture 3-17 LAN

- IP Address Configuration

IP Version: Select IPV4.

Mode: Select Static or DHCP mode. When selecting static mode, you need to configure IP Address, Subnet Mask and Default Gateway manually; when selecting DHCP mode, the system obtains IP address automatically;

Multicast Address: Multicast address for sending streams. Input according to actual request.

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.

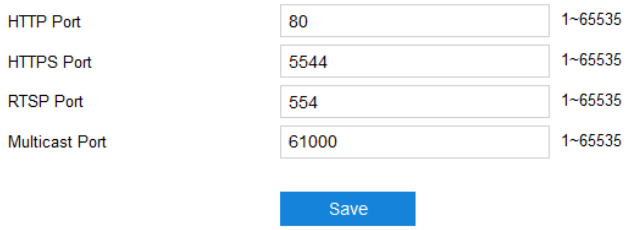
MTU: Maximum transmission unit, the maximum size of data packet transmitted through TCP/UDP protocol, ranging 500 ~ 1500, by default 1500.

- DNS Server Setting

When camera accesses to external platform in form of domain name, user needs to configure DNS server.

3.3.1.2 Port

On the interface of Port, configure HTTP Port, HTTPS Port, RTSP Port and Multicast Port. When logging in through network, configure corresponding ports by request.



Picture 3-18 Port

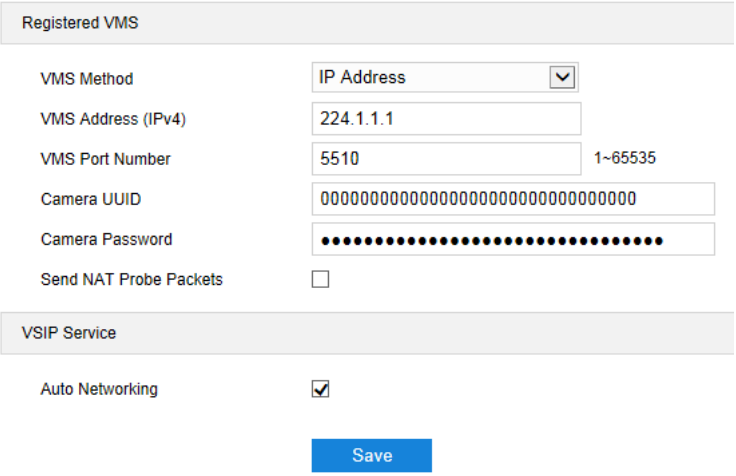
- **HTTP Port:** Hypertext Transport Protocol Port. When login through browser, you need to add a port number behind camera IP address. For example, if HTTP port is edited as 83, when you login through browser, you need to input "http://camera IP address:83. The number is 80 by default, ranging 1 ~ 65535.
- **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 5555, when you login through browser, you need to input "http://camera IP address:5555. 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. RTSP port number is 554 by default, ranging 1 ~ 65535. When login by RTSP port, rtsp://camera IP address/id=0 (id=0 play main stream, id=1 play secondary stream).
- **Multicast Port:** Configure multicast port up to actual request, 61000 by default, ranging 1 ~ 65535.

3.3.2 Access Protocol

3.3.2.1 VSIP

The web client supports accessing to back-end platform through VSIP protocol.

Configuration steps:



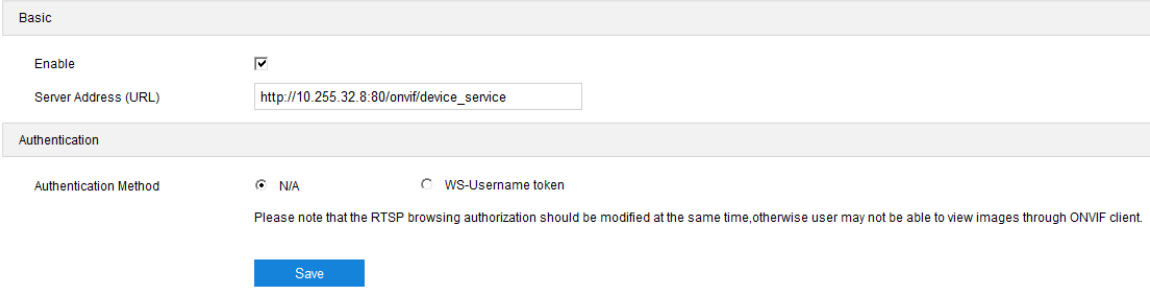
Picture 3-19 VSIP

1) Select a method from the dropdown list of VMS Method, "IP Address" or "Domain". If selecting "IP Address", input VMS address in "VMS Address (IPv4)"; if selecting "Domain", input VMS domain name in "Registered VMS Domain";
2) Input "VMS Port Number", 5510 by default;
3) Input "Camera UUID" and "Camera Password". Camera UUID is distributed by VMS and the password needs no verification so you don't have to input;
4) When the camera is in NAT, select "Send NAT Probe Packets"; you can select "Auto Networking" to enable function of auto networking;
5) After finish, click "**Save**" to validate setting.

Note:

- Please refer to the User Manual for PMC Client for adding cameras to the VMS;
- VSIP protocol only supports registering to VMS of this company or other SDK-integrated back-end platforms.

3.3.2.2 ONVIF



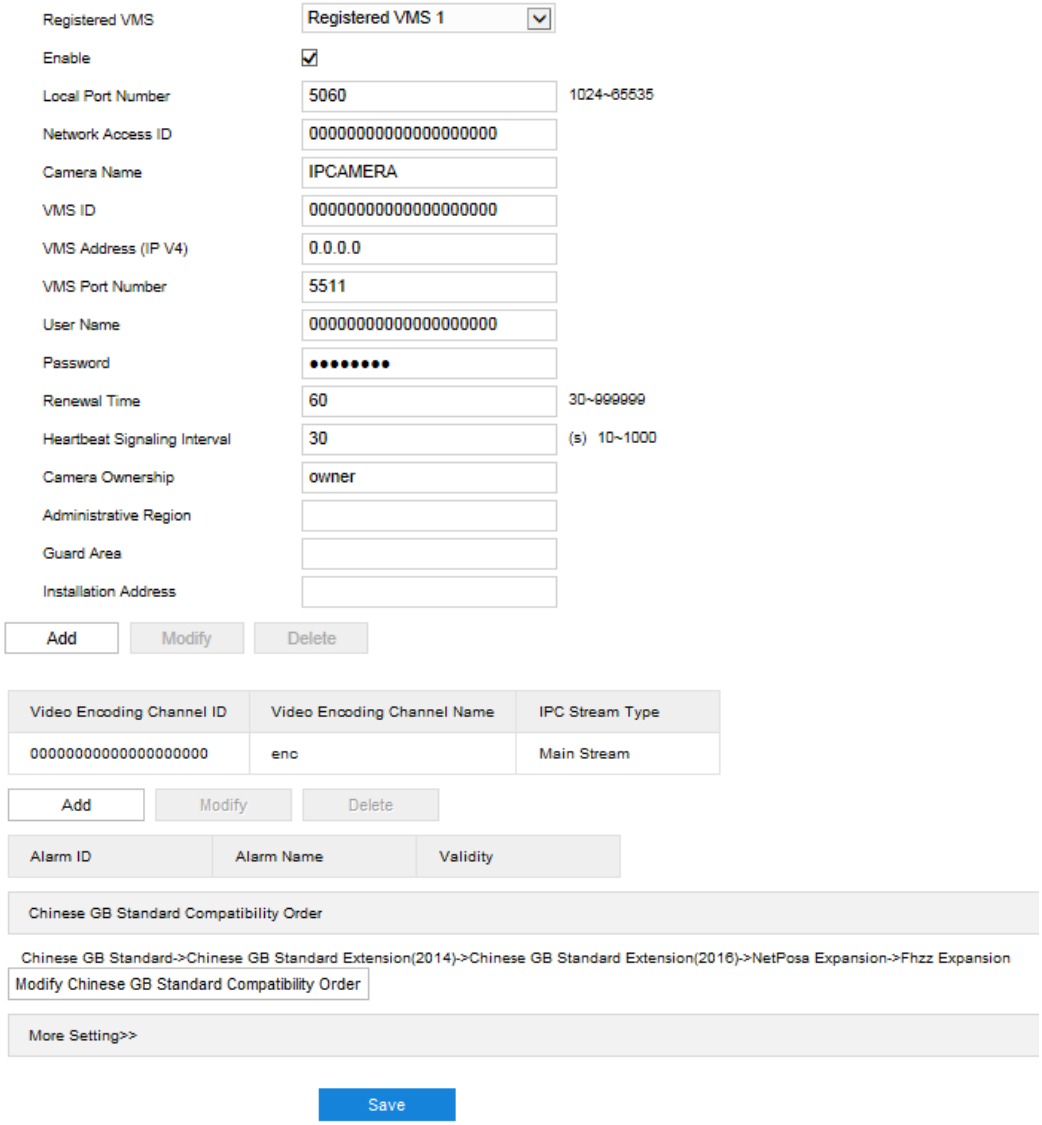
Picture 3-20 ONVIF

Basic: ONVIF protocol is enabled by default. User can register camera to ONVIF-supported VMS, VMS port being 80 by default. The camera will generate "Server Address (URL)" automatically.

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

3.3.2.3 GB28181 (SIP)

On GB28181 interface, add the camera to GB platform according to the requirements of GB/T28181. Configuration steps:



Picture 3-21 GB28181

1) Select “Enable” and select the “Registered VMS” (Registered VMS 1 or Registered VMS 2). The camera supports registered to 2 different VMS;

2) Enter Network Access ID, VMS ID, VMS Port Number, User Name/ Password and Video Encoding Channel ID, which are all provided by VMS;

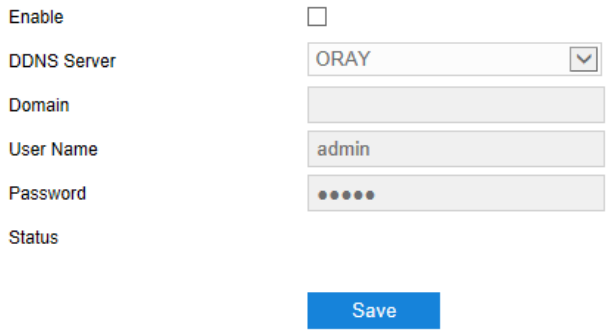
3) Click “**Save**” to validate settings.

3.3.3 Other Protocol

3.3.3.1 DDNS

DDNS (Dynamic Domain Name Server) is to connect the camera to various servers so that user can login to the camera 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.



Picture 3-22 DDNS

1) Select "Enable";

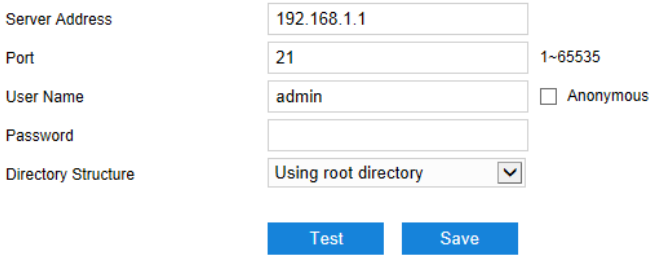
2) Select DDNS Server type;

3) Input the domain login information according to the selected DDNS server;

4) Click "**Save**" to validate setting.

3.3.3.2 FTP

File Transfer Protocol, the web client supports FTP protocol and user can upload the pictures of the camera to specific FTP server.



Picture 3-23 FTP

1) Input FTP server address and port;

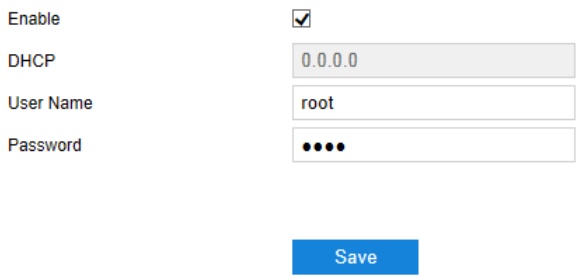
2) Input FTP server username and password, and you can select "Anonymous" to visit FTP server anonymously;

3) Configure directory structure, i.e. file save path. Select from the dropdown list by actual request;

4) Click "**Test**" to verify if current FTP is available, and click "**Save**" to validate setting.

3.3.3.3 PPPoE

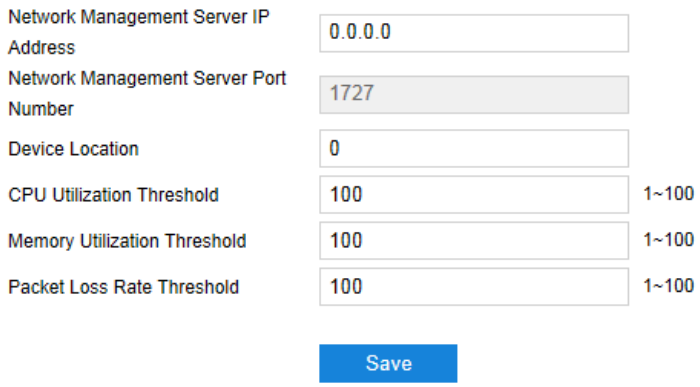
PPPoE (Point-to-Point Protocol over Ethernet) function is to access camera to the internet by dialing the account provided by ISP (Telecom, Unicom and CMCC).



Picture 3-24 PPPoE

1) Select "Enable" to enable PPPoE function;
2) Input user name and password provided by ISP;
3) Click "**Save**" to validate setting. It will show dynamic IP after dialing succeeds.

3.3.3.4 K-SNMP



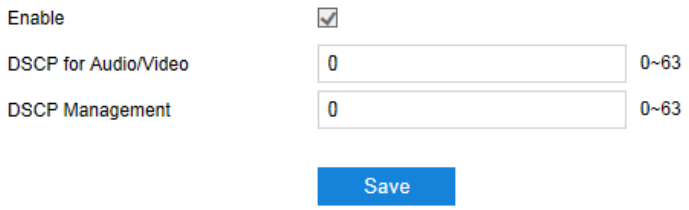
Picture 3-25 K-SNMP

The camera supports KEDACOM private network management protocol. Configuration steps are as follows:

1) Input "Network Management Server IP Address" and "Device Location";
2) Configure "CPU Utilization Threshold", "Memory Utilization Threshold" and "Packet Loss Rate Threshold". The default values are all 100, ranging 1 ~ 100;
3) Click "**Save**" to validate setting.

3.3.3.5 QoS

Note: QoS function needs support of network transmission device such as a router.



Picture 3-26 QoS

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

1) Select “Enable” to enable QoS function;

2) 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.

3) Click "**Save**" to validate setting.

3.3.3.6 UPnP

Picture 3-27 UPnP

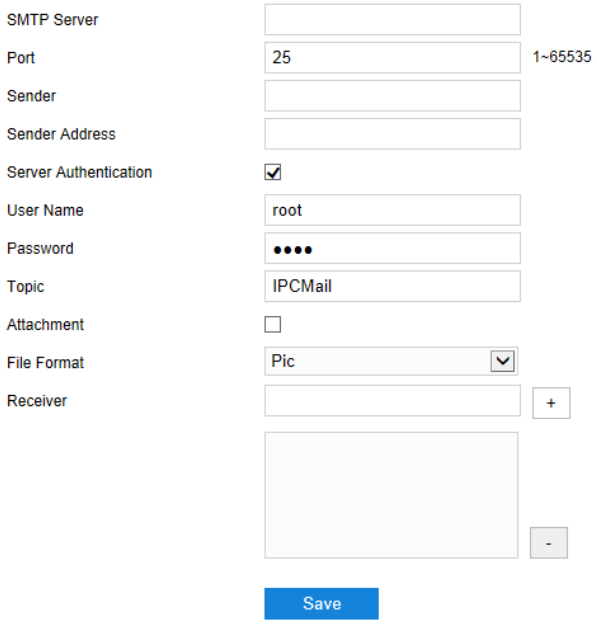
Note: For a camera in an Ethernet, UPnP function can make gateway or router perform auto-port-mapping which maps the camera monitor port from gateway or router

to the Ethernet device, thus the firewall module on the gateway or router starts to open this port to other PCs on the internet.

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:

1) Select “Enable” to enable UPnP function;
2) 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;
3) Select "Auto" or "Manual" for Mapping Mode;
4) Click "Save" to validate setting.

3.3.3.7 SMTP



Picture 3-28 SMTP

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) Input SMTP server IP address and port number, which ranges 1 ~ 65535, 25 by default;
2) Input "Sender" and "Sender Address"; optionally select "Server Authentication" and input correct user name and password;
3) Input email topic; optionally select "Attachment" and choose attached file format, then the email sent will attach the relative file;
4) 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;
5) Click "***Save***" to validate setting.

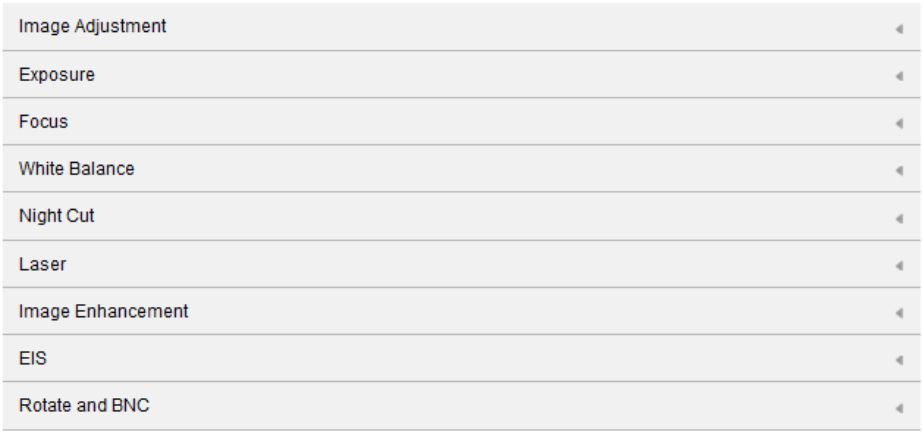
Note: This function is available only when email notification is enabled. Method to enable email notification can be referred to in the chapter of *Intelligent Function*.

3.4 Camera

Go to **Settings > Camera** to configure camera parameters, including Image, OSD, Video, Audio and PTZ interfaces.

3.4.1 Image

Go to Settings > Camera > Image, as shown below.

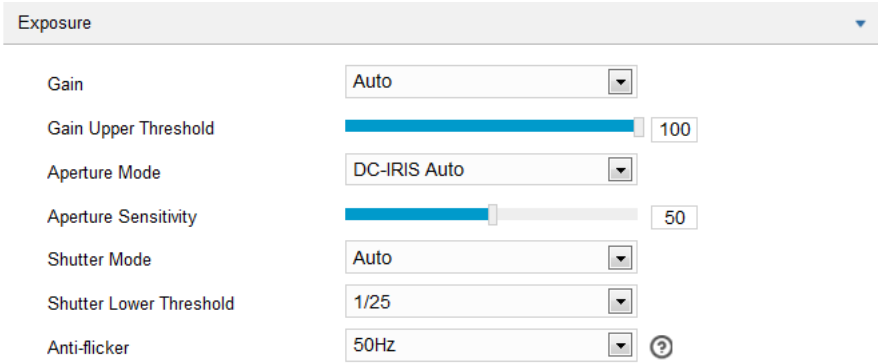


Picture 3-29 Image

3.4.1.1 Image Adjustment

The image adjustment in this part is the same as that on the Live View interface, which can be referred to in the chapter of *Image Adjustment*.

3.4.1.2 Exposure



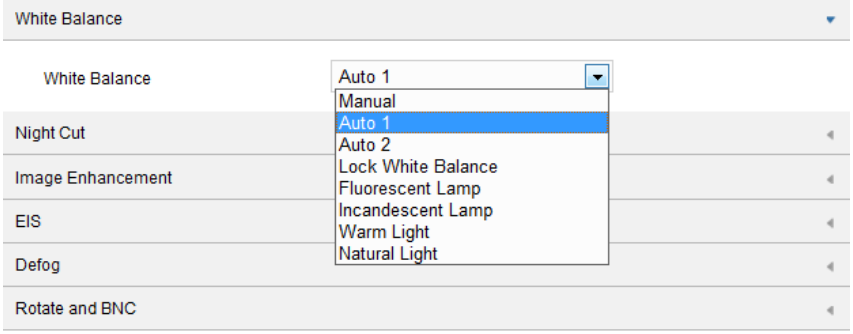
Picture 3-30 Exposure

- Gain: A higher gain will make the image look brighter. However, meanwhile there will be more noise points on the image. Auto mode is suggested. When selecting "Auto" mode, drag the slide bar below to set Gain Upper Threshold. Then the value of gain can only be adjusted automatically within the range of 0 to the set upper threshold; when selecting "Manual" mode, drag the slide bar below to set Gain Level and the value will remain.
- Aperture Mode: Aperture controls the light input through the lens. A large aperture allows more light input and the image looks bright. Options including “DC-IRIS Auto” and “DC-IRIS-Manual”. Drag the slide bar of Aperture Sensitivity to adjust the aperture sensitivity and auto mode is suggested. If selecting “DC-IRIS Manual”, drag the slide bar of Aperture Size to set the value and the aperture will remain as the set value.
- Shutter Mode: Camera shutter means the exposure shutter speed of image pixels. The smaller the value is, the darker the image will look. Options include "Auto" and "Manual". Suggest “Auto". When selecting "Auto", you can select Shutter Lower Threshold from the dropdown list below. Then the shutter will be adjusted within the range from the lower threshold to the minimum shutter value automatically; when selecting

"Manual", you can select Shutter Level from the dropdown list below. Then the value of shutter will remain.

- Anti-flicker: When there are floating cross stripes on the image, select the correct anti-flicker frequency (50Hz or 60Hz or natural light) to solve the problem. The frequency should be in accordance with that of the nation's AC frequency and light frequency.

3.4.1.3 White Balance

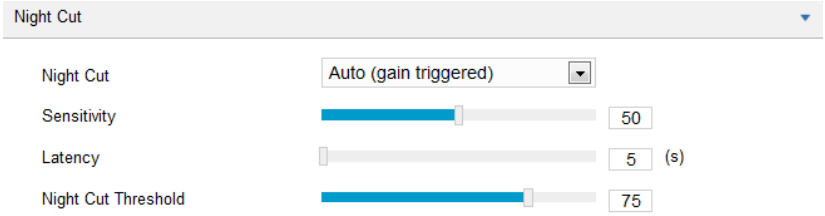


Picture 3-31 White Balance

Under different light conditions, there will be color cast in different images. White balance adjustment can restore white objects to be white regardless of the color temperature of the light source. Select an option from the dropdown list of white balance mode. Suggest "Auto".

- Manual: support R Gain and B Gain adjustment. Drag the slide bar of White Balance R Gain and White Balance B Gain to adjust the value, ranging 0 ~ 100.
- Auto 2: has a larger white balance range than “Auto 1”, though both are auto mode.
- Lock White Balance: lock current color correction matrix. If the camera works under light which provides fixed light condition, select from the following 4 options according to actual environment.
- Fluorescent Lamp: for color temperature of 6500K.
- Incandescent Lamp: for color temperature of 3000K.
- Warm Light: for color temperature of 4000K.
- Natural Light: for color temperature of 5500K.

3.4.1.4 Night Cut



Picture 3-32 Night Cut

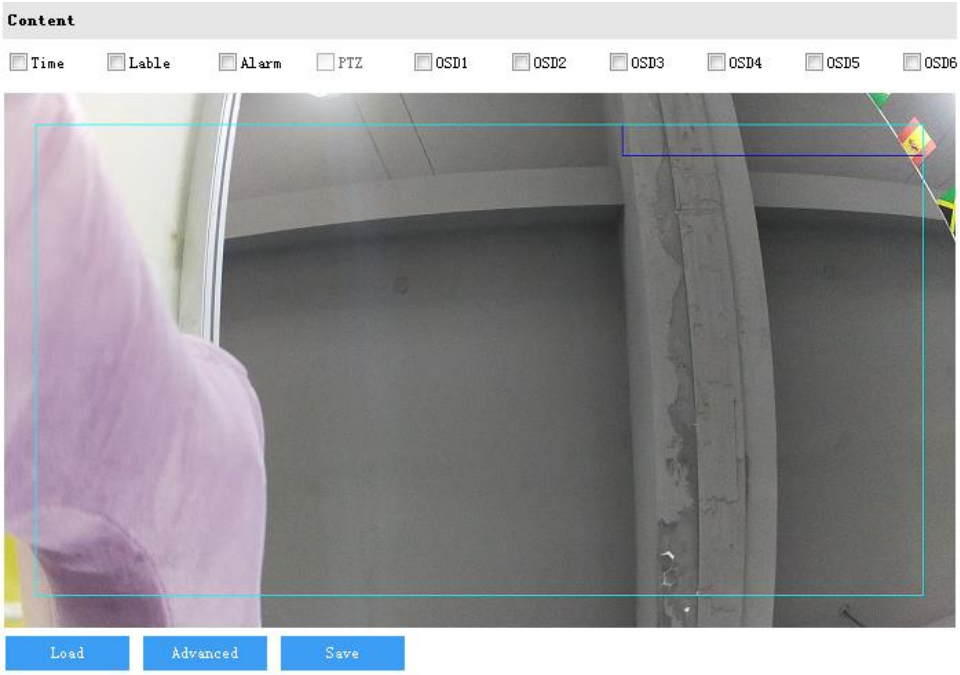
Select night cut mode from the dropdown list up to request. Explanation of different modes is as follows:

- Day: Under "Day" mode, the image keeps colored all the time.
- Night: Under "Night" mode, the image keeps black and white all the time.
- Auto (gain triggered): The camera switches day/night mode automatically according to the gain values. When selecting this mode, configure Sensitivity, Latency and Night Cut Threshold according to actual request.
- Scheduled Day/Night: Under "Scheduled Day/Night" mode, click "Edit Time" and configure "Day Mode Start Time" and "Day Mode End Time" on the popup interface. The camera will switch day and night modes according to the scheduled durations.

3.4.1.5 Effect Parameters

There are 2 modes of effect parameters by default, “Auto Mode” and “Standard Mode”. Alternatively, you can configure the parameters by actual requirements and save them as a mode for future use.

3.4.2 OSD



Picture 3-33 OSD

On OSD interface, you can configure OSD text on the surveillance window. Configuration steps are as follows:

1) Select options in “Content” according to requirements and preview the effect in the window below, options including "Time", "Label", "Alarm", "PTZ" and "OSD";
2) Click “**Advanced**” to set “Format”, “Font” and “Margin”. In the part of format, you can set "Time Format", "Display time in 2 lines" and "Alarm in front of tag"; in the part of font, you can set font "Type", "Size" and "Color"; in the part of margin, you can adjust the distance between OSD and border both horizontal and vertical;
3) Edit OSD texts: double click the OSD textbox and input characters in the popup interface. Click “**OK**". Each OSD can be set maximum 32 characters and so is the label;
4) Edit OSD positions: drag the OSD in the window with mouse to change its position. Each OSD can be dragged within the blue box only. If you want to drag it out of the blue box, move the blue box first;
5) Load font: Click “**Load**” to load “Default Font”, "Large Font", "Medium Font" or "Small Font". Then edit content and position according to the above steps;

6) Click "**Save**" to validate setting.

Note:

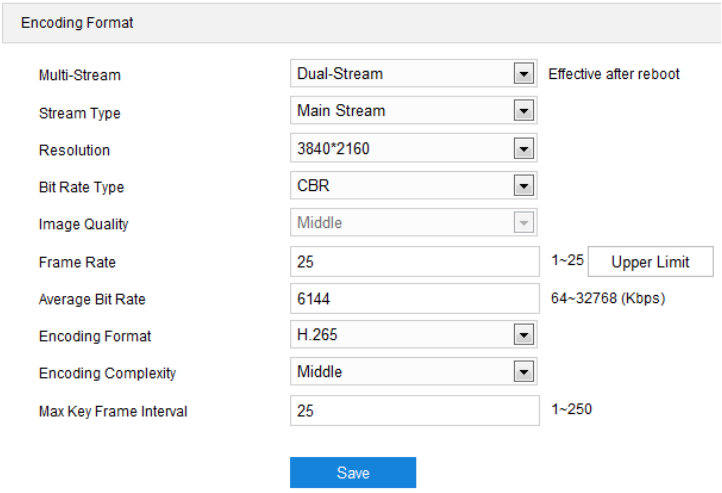
- A number, an English letter or a punctuation mark occupies one character.
- You can load “Default Font”, "Large Font", "Medium Font" or "Small Font". Then edit content and position according to the above steps.

3.4.3 Video

Video parameters include Encoding Format, ROI, Privacy Mask and Video Info Overlay.

3.4.3.1 Encoding Format

On the interface of “Encoding Format”, configure parameters of stream type, resolution, bit rate type and etc., as shown below.



Picture 3-34 Encoding Format

- Multi-Stream: It means the same video source is encoded in several streams with different resolutions. This parameter can be configured according to actual request and the setting will be validated after reboot.
- Stream Type: Configure the resolution and bitrate of main or secondary stream. The main stream is used for HD storage and preview while the secondary or third stream is for SD storage and preview when there is insufficient network bandwidth.
- Resolution: According to the requirements of image quality by user, select resolution from the dropdown list. The higher the resolution is, the more bandwidth it requires.

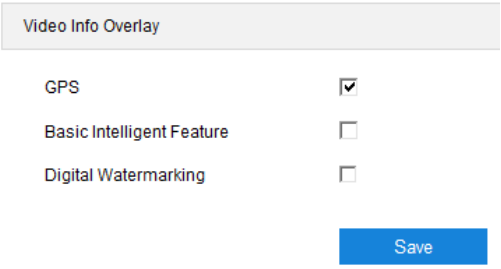
- Bit Rate Type: Options include CBR and VBR, by which you can control stream rate. CBR is fixed bit rate while VBR means the bit rate is adaptive within the upper limit. CBR transfers stream by average bitrate with high speed compressing, but there may be mosaic on the images; while VBR adjusts bitrate automatically with slow compressing, but could ensure image sharpness under complex conditions.
- Image Quality: When selecting “VBR”, select image quality level from the dropdown list according to actual requirements. The higher the level is, the clearer the image will look.
- 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 for CBR.
- Encoding Format: Select according to actual requirements, options including H.264, H.265 and MJPEG.
- Encoding Complexity: Select encoding complexity level according to actual request. Under the same bitrate, the higher the complexity level is, the better quality the image will have and the bandwidth it will require.
- 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.

Note:

1) When the Bit Rate Type is “VBR”, the parameter of Average Bit Rate will turn Bit Rate Upper Limit and you need to configure the value manually, ranging 64 ~ 32768 (Kbps), by default 6144.
2) The parameter of Image Quality is enabled only when “VBR” is selected and it will remain “Middle” when “CBR” is selected.
3) The higher the Encoding Complexity is, the more the stream will be compressed. In this way it will relieve bandwidth restriction somehow, but

meanwhile it will also occupy the CPU resource of more devices. Suggest using the default level.

3.4.3.2 Video Info Overlay

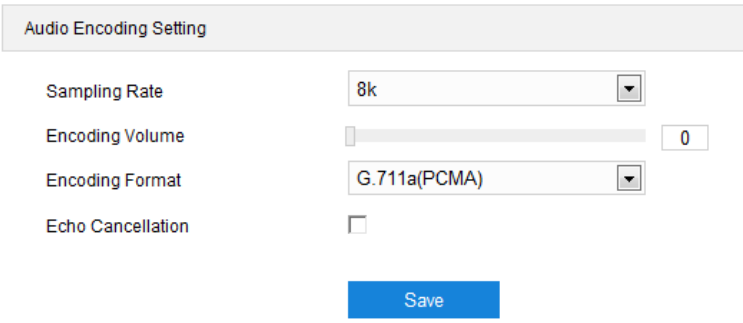


Picture 3-35 Video info overlay

- **GPS:** Select **GPS** to show camera coordinates.
- **Basic Intelligent Feature:** After configuring intelligent functions (on the interface of Settings > Event > Intelligent Function), select this option and select "Rule Information Display" in Settings > Local Setting, then the intelligent area will be displayed in live view window.
- **Digital Watermarking:** Select **Digital Watermarking** to show digital watermarking.

3.4.4 Audio

3.4.4.1 Audio Encoding

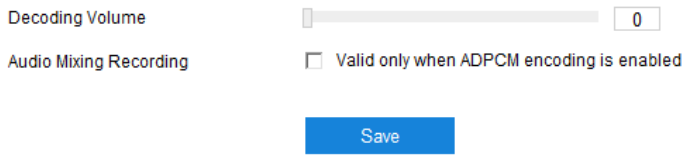


Picture 3-36 Audio encoding

- 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. The default option is “8k”.
- Encoding Volume: Drag the slide bar to adjust audio encoding volume, i.e. audio input volume. The larger the value is, the higher the voice will be.

- Encoding Format: Select audio encoding format from the dropdown list, by default G.711 a (PCMA).
- Echo Cancellation: Select the checkbox to cancel noises in the input audio and thus improve the audio quality.

3.4.4.2 Audio Decoding



Picture 3-37 Audio decoding

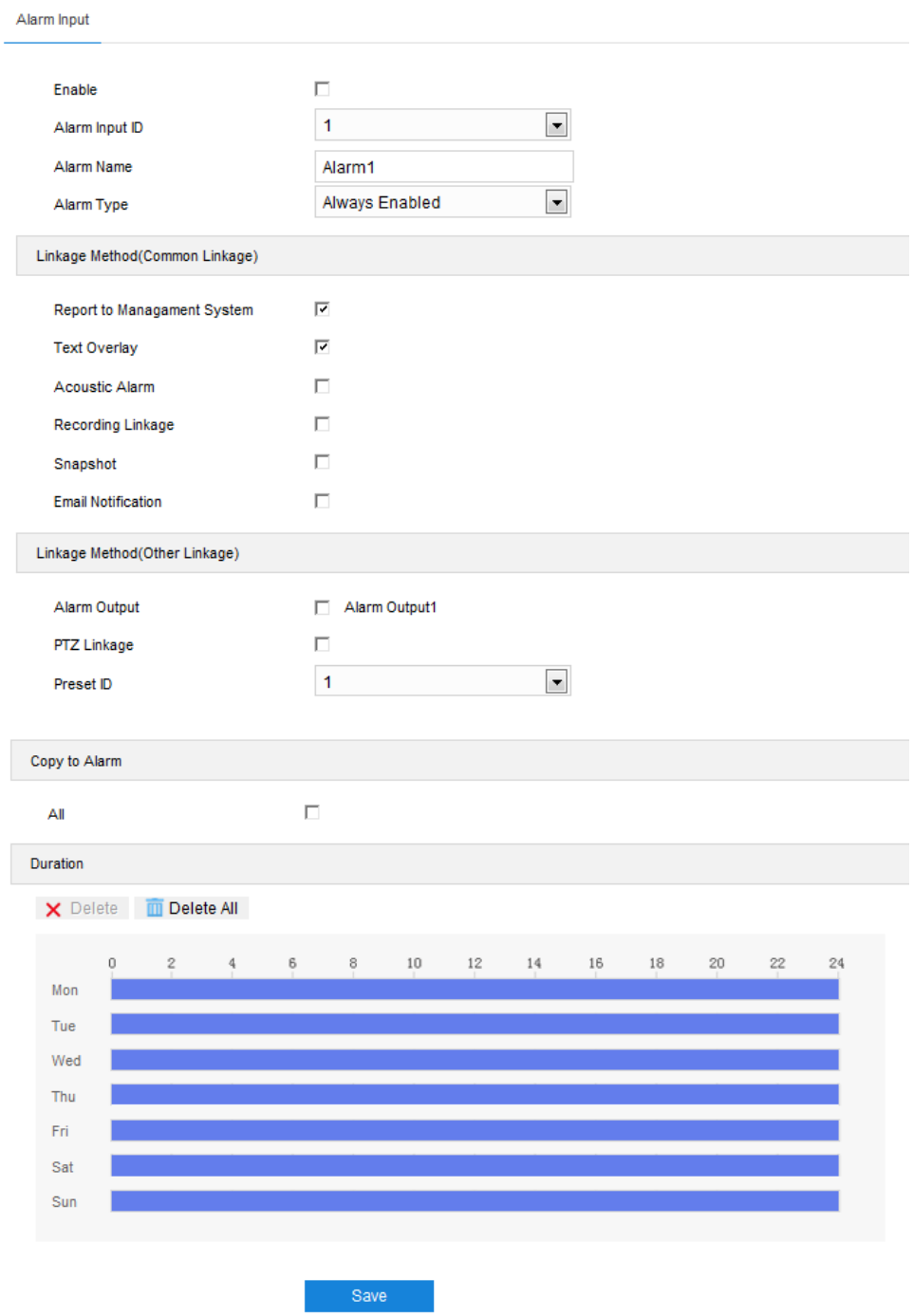
- Decoding Volume: Drag the slide bar to adjust audio decoding volume, i.e. audio output volume.
- Audio Mixing Recording: Select the checkbox to enable audio mixing recording function, which is valid only when “ADPCM” is selected.

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.

3.5 Event

3.5.1 Alarm Input

Camera supports connecting with on-off alarm devices. If the alarm input device is always disabled, when it alarms, the circuit will become a loop and the camera will trigger alarm output by the set alarm linkage type. If the alarm input device is always enabled, when it alarms, the circuit will become open and the camera will trigger alarm output by the set alarm linkage type.



Picture 3-38 Alarm Input

Operation steps are as follows:

1) Confirm that the alarm input device is always enabled or always disabled and has been rightly connected with the alarm input port of camera;

2) Go to **Settings > Event > Alarm Input** and select "**Enable**";

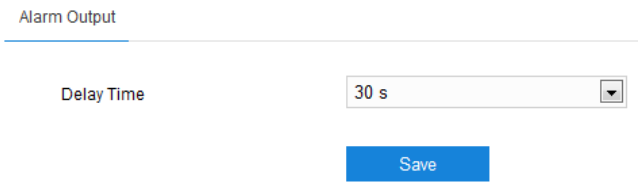
3) Select a number from the dropdown list of **Alarm Input ID** (corresponding to the connected input ID);

4) Enter alarm name. If the alarm input device is always disabled, which means the circuit is usually open, user must select "**Always Disabled**" from the dropdown list of Alarm Type. If the alarm input device is always enabled, which means the circuit is usually loop, user must select "**Always Enabled**" from the dropdown list of Alarm Type. The default setting is "Always Disabled";
5) Select linkage method to trigger actions when an alarm is triggered;
6) If user sets several alarm inputs, select "All" under Copy to Alarm to copy all configurations of current alarm input to other alarm inputs;
7) Duration: there can be maximum 10 durations on one day and each can have a start time and end time. Please refer to the steps in chapter *Motion Detection* for details;
8) Click "**Save**" to validate setting.

3.5.2 Alarm Output

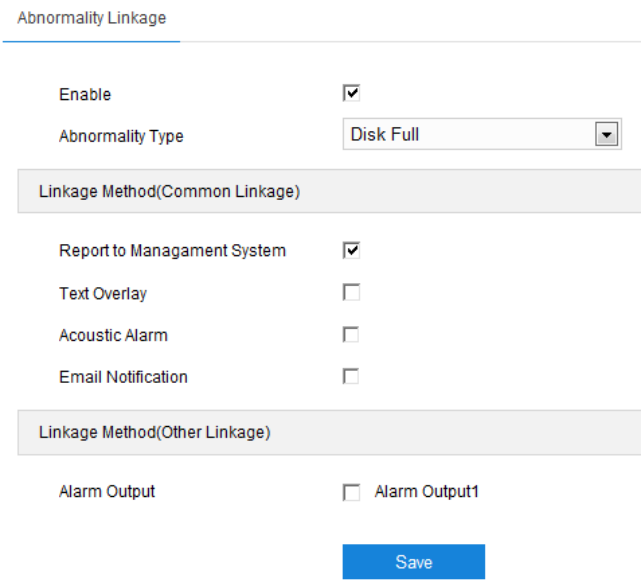
The default duration of alarm output is 5s, and the delay time means the prolonged period of time after the default 5s. Please select an option from the dropdown list according to actual request and click "**Save**" to validate setting.

Note: Alarm output is effective only when "Alarm Output" is selected under Linkage Method on the interface of Alarm Input.



Picture 3-39 Alarm Output

3.5.3 Abnormality Linkage



Picture 3-40 Abnormality Linkage

Configure the alarm linkage method for abnormal events. Operation steps are as follows:

1) Select "Enable" and 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.

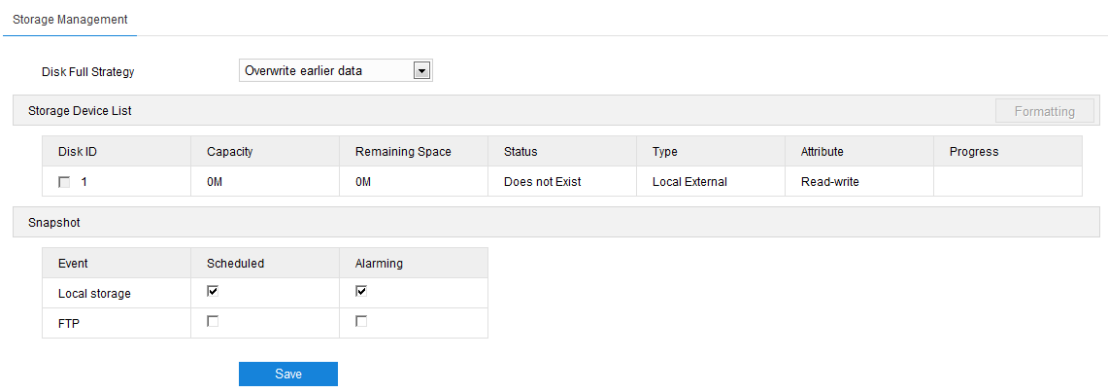
2) Select linkage type(s), which is/are the alarm output method(s) when an event triggers an alarm;

3) Click "**Save**" to validate settings.

3.6 Storage

3.6.1 Storage Management

When the camera is installed with a storage card and works normally, you can configure scheduled recording and scheduled snapshot.



Picture 3-41 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 **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; in "Status" column, 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.; in "Progress" column, it shows the percentage of the formatting progress of the storage 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: The storage card is installed in the camera when going out of the factory. When using the local storage card for the first time, please click "Formatting" first.

3.6.2 Recording

When scheduled recording is enabled, the camera will record videos automatically in the configured durations and save the videos in the storage 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 camera. If formatting is successful, the Status will turn “Normal” which means the storage card can be used normally;

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

- Recording Type: select the stream to be recorded;
- Code Stream Format: select according to the type of access protocol;
- Prerecord: select prerecord duration, i.e. the prerecord duration before recording starts, by default 30s;
- Recording Delay: select recording delay time, i.e. the prolonged recording duration plus to the configured duration;

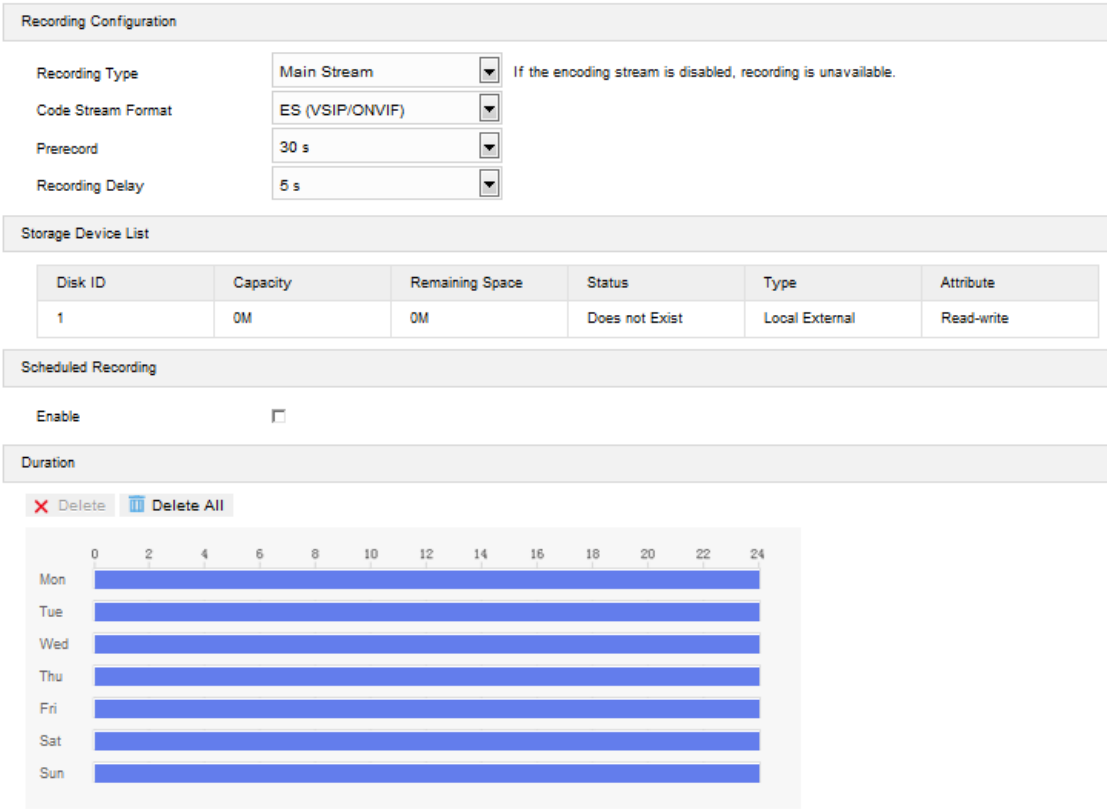
3) Select "Enable" to enable Scheduled Recording;

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

- Set durations: select a day and put the mouse on a point of the timeline, left-click and drag the mouse to the right to draw a bright blue color bar, on the top of which shows the start time and end time; click the color bar to pop up a window for editing the accurate start time and end time; click "***Save***" to validate setting. It allows several (max 4) durations on one day and the durations cannot overlap with each other;
- 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;

5) Click "***Save***" to validate settings.

Note: When the camera registers to GB platform, the Code Stream Format must be “PS (GB28181)”.



Picture 3-42 Scheduled Recording

3.6.3 Snapshot

After configuring snapshot parameters, the camera will capture images automatically.

1) Go to **Settings > Storage > Storage Management** to configure disk full strategy and format the storage 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;

   - Format: only support .jpeg format;
   - Resolution: same as that of current main stream;
   - Quality: the quality of captured image;

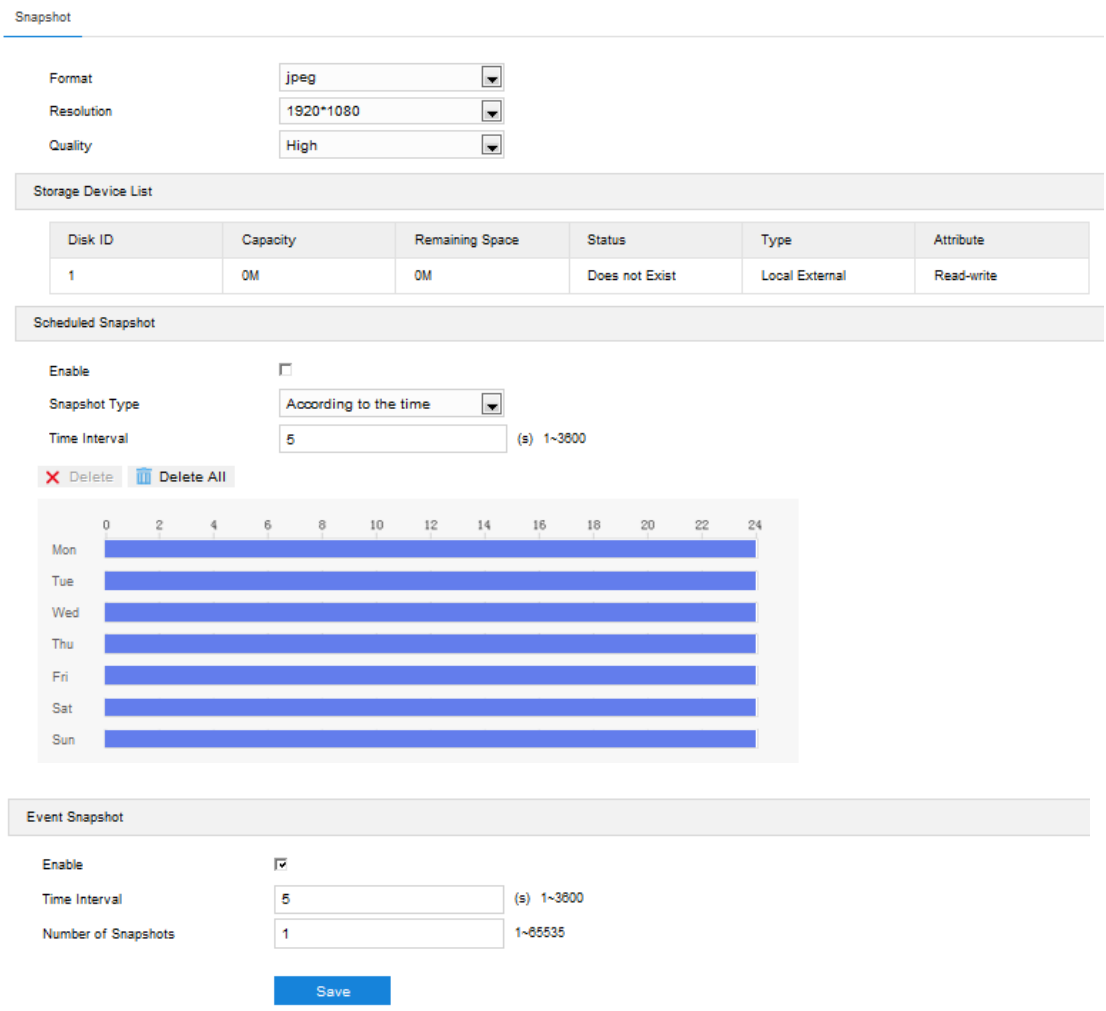
3) Configure scheduled snapshot:

   - Enable: select the checkbox to enable scheduled snapshot;
   - Snapshot Type: select “According to the time” or “According to the number”;
   - Time Interval: select the interval between snapshots;

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

- Set durations: select a day and put the mouse on a point of the timeline, left-click and drag the mouse to the right to draw a bright blue color bar, on the top of which shows the start time and end time; click the color bar to pop up a window for editing the accurate start time and end time; click "***Save***" to validate setting. It allows several (max 4) durations on one day and the durations cannot overlap with each other;
- 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;

5) Select the checkbox behind “Enable” under Event Snapshot, and configure time interval and number of snapshots (the number of snapshots captured at each event).
6) Click "***Save***" to validate settings.

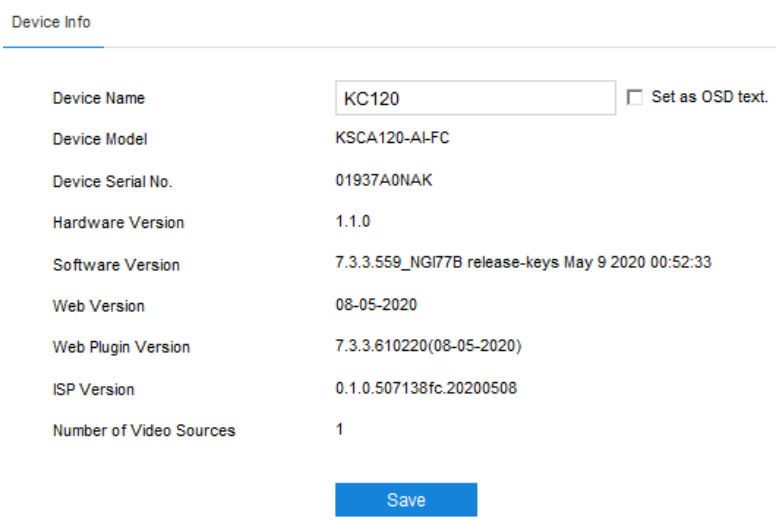


Picture 3-43 Scheduled Snapshot

3.7 System

3.7.1 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, the device name will be synchronized to the OSD, interface shown below:

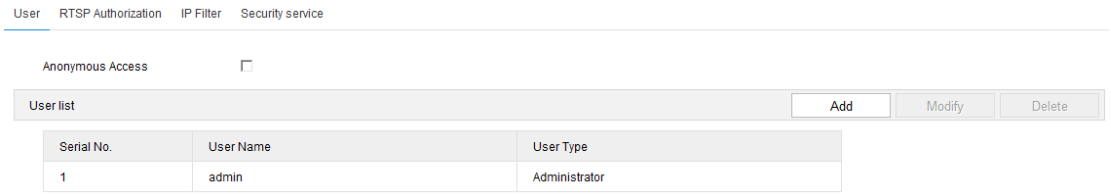


Picture 3-44 Device info

3.7.2 User Security

3.7.2.1 User

On "User" interface, you can add or delete user, edit username and password, configure user authorizations and etc.



Picture 3-45 User

- Anonymous Access: After select the checkbox, you will be able to select "Anonymous Login" on the login interface.

Note: Anonymous 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**”.

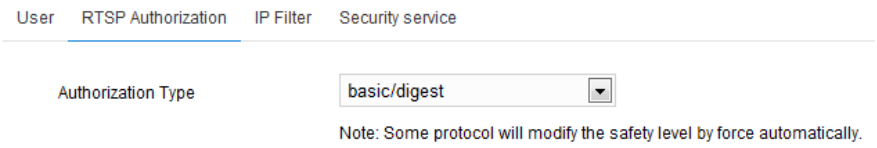
Note:

- By default, all options are available to administrator users; Live View, Playback/Snapshot, and PTZ Control options are available to operator users; a browser can only view the live video from the camera.

- ♦ Some settings take effect after rebooting the camera, which requires user with both the authorizations of configuration and reboot.
- ■ Delete user: Select user and click “**Delete**” to delete the user.
- ■ Modify user: Select user and click “**Modify**” to modify on the popup interface.

3.7.2.2 RTSP Authorization

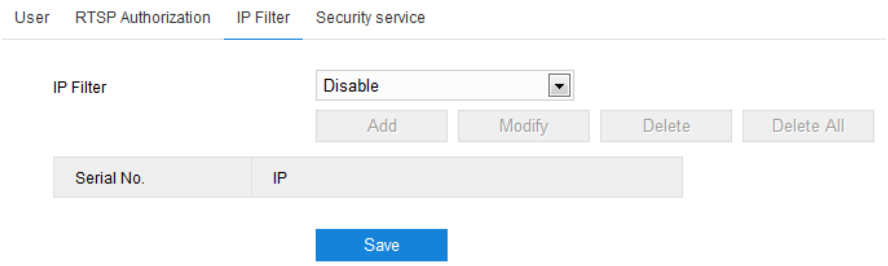
Select authorization type from the dropdown list, options including “none”, “basic/digest” and “digest”. By default, it is “basic/digest”.



Picture 3-46 RTSP Authorization

3.7.2.3 IP Filter

By setting IP filter, user can manage access limitation to the web client. White List includes IP addresses able to access to the client while Black List includes IP addresses unable to access to the client.



Picture 3-47 IP Filter

Configuration steps are as follows:

1) Select IP filter from the dropdown list up to request, options including “Disable”, “Black List” and “White List”;

Note: If selecting “Disable”, IP filter is disabled.

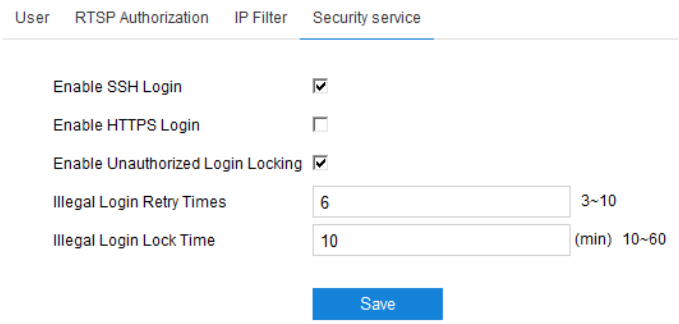
2) After selecting filter method, click “**Add**” and input IP address on the popup interface, and click “**Confirm**”;

3) After finish setting, click "**Save**" to validate setting.

- ■ Modify Black/ White List: Select IP address from the black/ white list and click “**Modify**” to modify the IP address, and click “**Confirm**”.

- Delete Black/ White List: Select IP address from the black/ white list and click “**Delete**” to delete the IP address. Click “**Delete All**” to clear all the added IP addresses.

3.7.2.4 Security Service



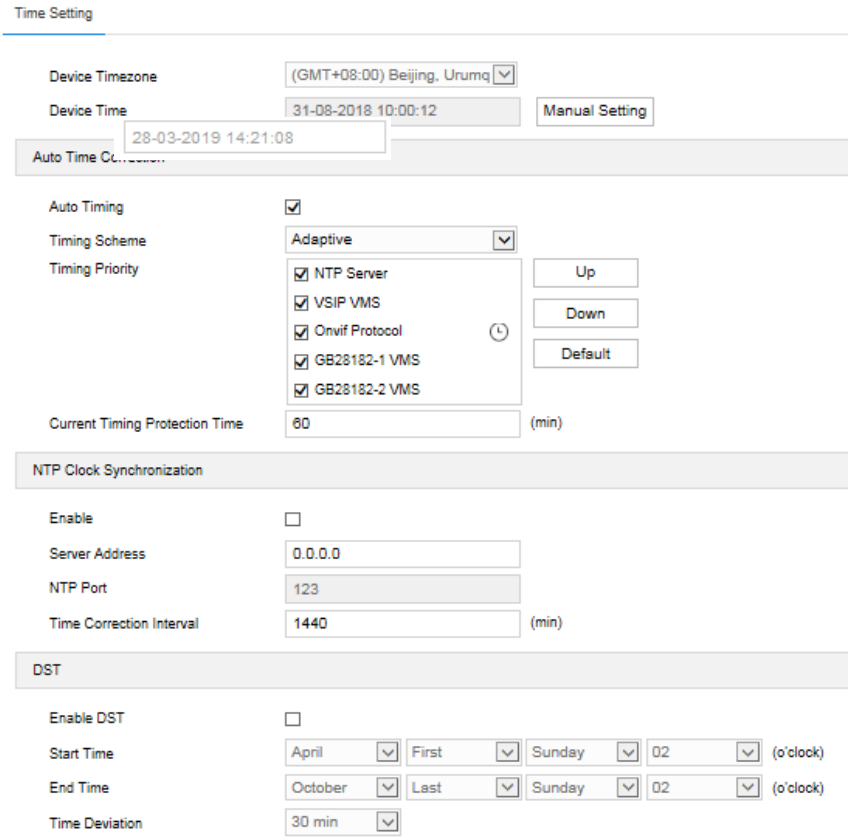
Picture 3-48 Security Service

- Enable SSH Login: Select it to enable SSH login, which means SSH service is enabled and you can login by SSH mode. Usually it's unnecessary to enable when the camera works normally.
- Enable Unauthorized Login Locking: Select it to enable unauthorized login locking.
- Illegal Login Retry Times: Configure illegal login retry times.
- Illegal Login Lock Time: Configure illegal login lock time.

Note: Select “Enable Unauthorized Login Locking” and configure Illegal Login Retry Times and Illegal Login Lock Time. Click “Save”. When user logs in and input wrong user name or password for the configured times (3 ~ 10, configurable), the user IP will be locked up for a certain period of time (10 ~ 60 minutes, configurable), during which the user cannot log in.

3.7.3 Time

Time setting includes Device Timezone, Device Time, Auto Time Correction and DST. Configure parameters by request and click "**Save**" to validate setting.



Picture 3-49 Time Setting

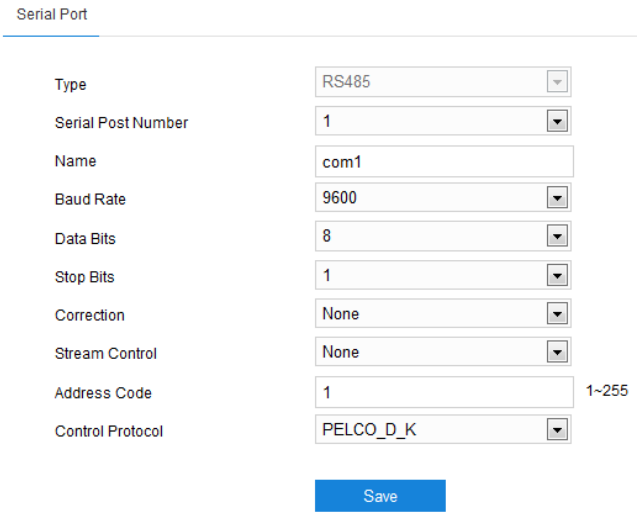
- Time Setting: Set Device timezone and device time. Click "**Manual Setting**", select timezone and set time on the popup interface. You can select "Synchronize time with PC" and click "**Save**" to validate setting.
- Auto Time Correction: Select "Auto Timing" and the system will correct time automatically according to access protocol or NTP server or adaptive. When selecting a protocol, the system will correct time automatically according to the protocol; when selecting “NTP server”, you need to fill NTP Server Address and NTP Port and configure Time Correction Interval; when selecting “Adaptive”, select necessary adaptive protocols, set the Timing Priority sequence and enter current Timing Protection Time (i.e. the save time during protocol switching).

Note: Access protocol means the protocol that the camera connects to a platform; NTP means Network Time Protocol, a protocol for clock synchronization between computer systems.

- 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.
- 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”.

3.7.4 Serial Port

Serial port is used to control camera rotation, extended alarm input or device adjustment (subject to devices). Usually serial port is identified as RS485 A/B. Match 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.

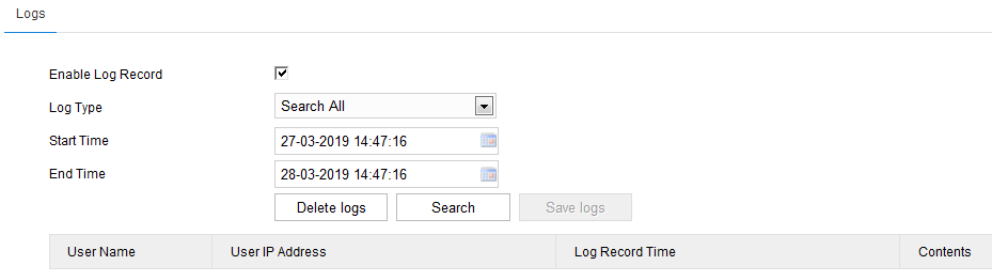


Picture 3-50 Serial port

Note: It's suggested not to edit the parameters of RS485 port in case the PTZ will be out of control.

3.7.5 Log

On Log interface, you can select "Enable Log Record" to search, view and download logs.



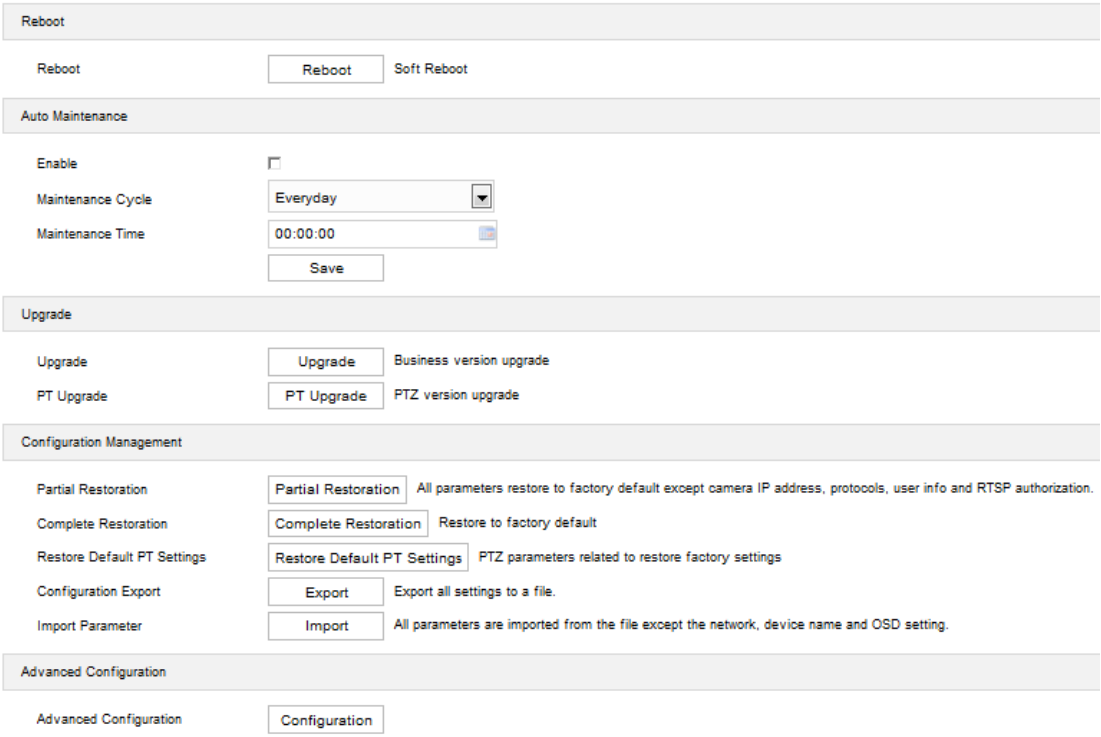
Picture 3-51 Log

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: The system can save maximum 2,000 entries of logs.

3.7.6 System Maintenance



Picture 3-52 System maintenance

On the interface of "System Maintenance", you can reboot and upgrade cameras or perform other maintenance over the device.

- Reboot: Click "**Reboot**" to reboot the camera.
- 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.

Note: PT Upgrade is necessary only when there is BUG in the PT version.

- 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.
  - Restore Default PT Settings: Reset PT settings to factory default.
  - Configuration Export: After configuring camera mode, you can export the configuration to local PC for copying the configurations. Click "**Export**" and select a local save path to export.
  - Import Parameter: You can import local configuration file 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. You can configure parameters such as VSIP Protocol Compatibility, Keep Alive the Stream UDP and Network Adaptation if necessary.

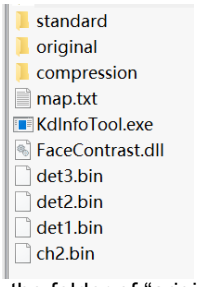
4. Appendix: Personnel Import Through Web Client

- 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.



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 ID 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>People**, 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.