2 Megapixel

FACE RECOGNITION &ACCESS CONTROL TERMINAL

User Manual

Please read this instruction carefully before operating the unit and keep it for further reference

Notes on Safety

- This product is intended to be supplied by a Listed Power Unit, marked with 'Limited Power Source', 'LPS' on unit, output rated minimum 12V/1 A, no more than 2000m altitude of operation and Tma=60 Deg.C.
- Do not attempt to disassemble the camera; in order to prevent electric shock, do not remove screws or covers.
- There are no user-serviceable parts inside. Please contact the nearest service center as soon as possible if there is any failure.
- Avoid from incorrect operation, shock vibration, heavy pressing which can cause damage to product.
- Do not use corrosive detergent to clean main body of the camera. If necessary, please use soft dry cloth to wipe dirt; for hard contamination, use neutral detergent. Any cleanser for high grade furniture is applicable.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- Please follow the instructions to install the camera. Do not reverse the camera, or the reversing image will be received.
- Do not operate it in case temperature, humidity and power supply are beyond the limited stipulations.
- Keep away from heat sources such as radiators, heat registers, stove, etc.
- Do not expose the product to the direct airflow from an air conditioner.
- This manual is for using and managing the product. We may reserve the rights of amending the typographical errors, inconsistencies with the latest version, software upgrades and product improvements, interpretation and modification. These changes will be published in the latest version without special notification.
- All pictures, charts, images in this manual are only for description and explanation of our products. In this manual, the trademarks, product names, service names, company names, products that are not owned by our company are the properties of their respective owners.
- This manual is suitable for face recognition &access control terminal.

Disclaimer

- With regard to the product with internet access, the use of product shall be wholly at your own risks. Our company shall be irresponsible for abnormal operation, privacy leakage or other damages resulting from cyber attack, hacker attack, virus inspection, or other internet security risks; however, our company will provide timely technical support if necessary.
- Surveillance laws vary from country to country. Check all laws in your local region before using this product for surveillance purposes. We shall not take the responsibility for any consequences resulting from illegal operations.

Cybersecurity Recommendations

- Use a strong password. At least 8 characters or a combination of characters, numbers, and upper and lower case letters should be used in your password.
- It is recommended to change the service default ports (like HTTP-80, HTTPS-443, etc.) to reduce the risk of outsiders being able to access.
- It is recommended to set the firewall of your router. But note that some important ports cannot be closed (like HTTP port, HTTPS port, Data Port).
- It is not recommended to expose the device to the public network. When it is necessary to be exposed to the public network, please set the external hardware firewall and the corresponding firewall policy.
- It is not recommended to use the v1 and v2 functions of SNMP.
- In order to enhance the security of WEB client access, please create a TLS certificate to enable HTTPS.
- Use black and white list to filter the IP address. This will prevent everyone, except those specified IP addresses from accessing the system.
- If you add multiple users, please limit functions of guest accounts.
- If you enable UPnP, it will automatically try to forward ports in your router or modem. It is really very convenient for users, but this will increase the risk of data leakage when the system automatically forwards ports. Disabling UPnP is recommended when the function is not used in real applications.
- Check the log. If you want to know whether your device has been accessed by unauthorized users or not, you can check the log. The system log will show you which IP addresses were used to log in your system and what was accessed.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

1. FCC compliance

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

2. FCC conditions:

- This device complies with part 15 of the FCC Rules. Operation of this product is subject the following two conditions:
- This device may not cause harmful interface.
- This device must accept any interference received, including interference that may cause undesired operation.

  This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

CE Information

CE The products have been manufactured to comply with the following directives.

EMC Directive 2014/30/EU

RoHS

The products have designed and manufactured in accordance with Directive EU RoHS Directive 2011/65/EU and its amendment Directive EU 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

2012/19/EU (WEEE directive): The Directive on waste electrical and electronic equipment (WEEE Directive). To improve the environmental management of WEEE, the improvement of collection, treatment and recycling of electronics at the end of their life is essential. Therefore, the product marked with this symbol must be disposed of in a responsible manner.

Directive 94/62/EC: The Directive aims at the management of packaging and packaging waste and environmental protection. The packaging and packaging waste of the product in this manual refers to must be disposed of at designated collection points for proper recycling and environmental protection.

REACH(EC1907/2006): REACH concerns the Registration, Evaluation, Authorization and Restriction of Chemicals, which aims to ensure a high level of protection of human health and the environment through better and earlier identification of the intrinsic properties of chemical substances. The product in this manual refers to conforms to the rules and regulations of REACH. For more information of REACH, please refer to DG GROWTH or ECHA websites.

Table of Contents

1 Introduction 1

2 Login & Network Connection 2

2.1 Wired Network Connection 2

2.1.1 Access through IP-Tool 2

2.1.2 Directly Access through IE 4

2.1.3 WAN 5

2.2 Wi-Fi Connection 8

2.3 APP Connection 9

3 Face Recognition Configuration 11

3.1 Face Match Settings 11

3.2 Face Database Management 13

4 Live View 16

4.1 Face Recognition View 16

4.2 Live View via Web 16

5 Access Control Settings 19

5.1 Access Control System Settings 19

5.2 Door Lock Settings 20

5.3 Door Contact Settings 21

5.4 Wiegand Settings 22

5.5 Tampering Alarm Settings 22

6 Other Configurations 23

6.1 System Settings 23

6.1.1 Basic Information 23

6.1.2 Date and Time 23

6.1.3 Local Config 24

6.2 Image Configuration 24

6.2.1 Display Configuration 24

6.2.2 Video / Audio Configuration 26

6.2.3 OSD Configuration 28

6.2.4 White Light Control 28

6.3 Alarm Configuration 29

6.3.1 Exception Detection 29

6.4 Network Configuration 30

6.4.1 TCP/IP 30

6.4.2 Wi-Fi Settings 31

6.4.3 Port 32

6.4.4 Server Configuration 33

6.4.5 DDNS 33

6.4.6 RTSP 34
6.4.7 UPnP 35
6.4.8 Email 36
6.4.9 FTP 37
6.4.10 HTTPS 37
6.4.11 P2P 38
6.5 Security Configuration 39
6.5.1 User Configuration 39
6.5.2 Online User 40
6.5.3 Block and Allow Lists 41
6.5.4 Security Management 41
6.6 Maintenance Configuration 41
6.6.1 Backup and Restore 41
6.6.2 Reboot 42
6.6.3 Upgrade 42
6.6.4 Operation Log 43
7 Search 44
7.1 Image Search 44
7.2 Video Search 45
8 Face Match Result Search 47
Appendix 48
Appendix 1 Troubleshooting 48
Appendix 2 Specifications 50

1 Introduction

This series of product is specially designed and developed for face recognition and access control applications, featuring high performance and reliability, faster recognition and higher accuracy rate. Based on deep-learning algorithm, it combines identity authorization and access control.

It can be widely used in the entrances and exits of community, schools, hospitals, scenic areas, hotels, shopping malls, office buildings, public services and construction sites for identity authorization and access control.

Main Features

- 3.5 inch LCD touch screen
- Max. resolution: 2MP (1920×1080)
- Face liveness detection technology distinguishing real faces from non-real face spoof attacks
- Highly accurate face recognition using deep learning algorithm
- Stand-alone device, ready for networking
- Communication via wired network (TCP/TP) and Wi-Fi
- Supports multiple door opening modes (card, card + password, card + face recognition, etc.)
- Intelligent Analysis: video exception detection, face detection, face capture, face match, etc.

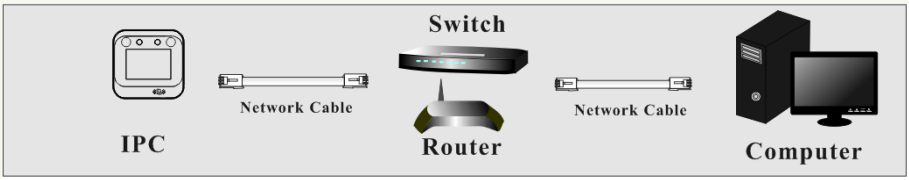
2 Login & Network Connection

2.1 Wired Network Connection

In LAN, there are two ways to access IP-Cam: 1. access through IP-Tool; 2. directly access through IE browser.

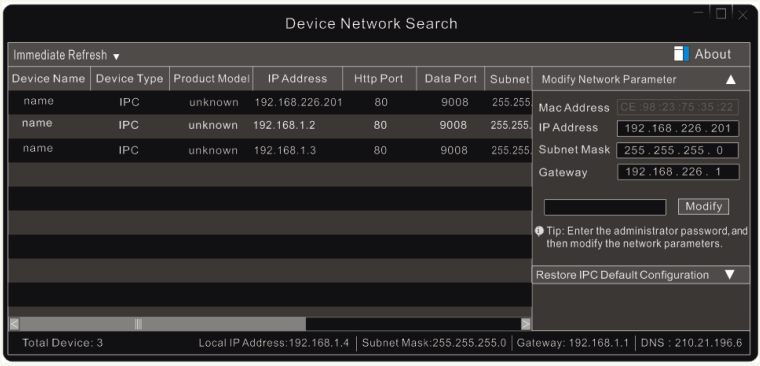
2.1.1 Access through IP-Tool

Network connection:

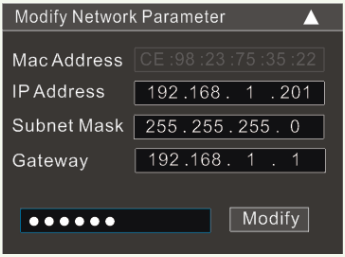


① Make sure the PC and IP-Cam are connected to the local network and the IP-Tool is installed in the PC from the supplier.

② Double click the IP-Tool icon on the desktop to run this software as shown below:



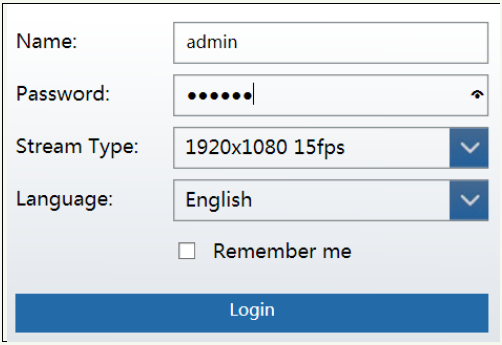
③ Modify the IP address. The default IP address of this camera is 192.168.226.201. Click the information of the camera listed in the above table to show the network information on the right hand. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer's. Please modify the IP address of your device according to the practical situation.



For example, the IP address of your computer is 192.168.1.4. So the IP address of the camera shall be changed to 192.168.1.X. After modification, please enter the password of the administrator and click the "Modify" button to modify the setting.

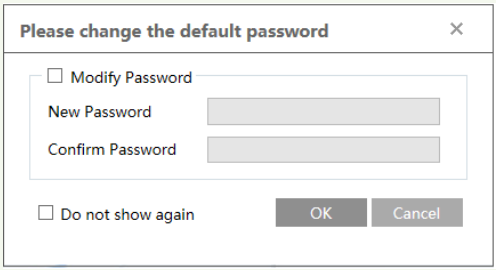
☞ The default password of the administrator is "***123456***".

④ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. Follow directions to download, install and run the Active X control.



Enter the username and password in the login window to log in.

☞ The default username is "***admin***"; the default password is "***123456***".

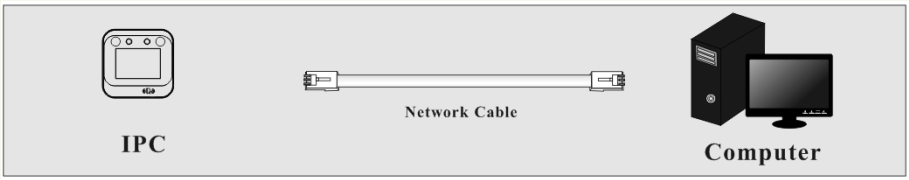


The system will pop up the above-mentioned textbox to ask you to change the default password. It is strongly recommended to change the default password for account security. If "Do not show again" is checked, the textbox will not appear next time.

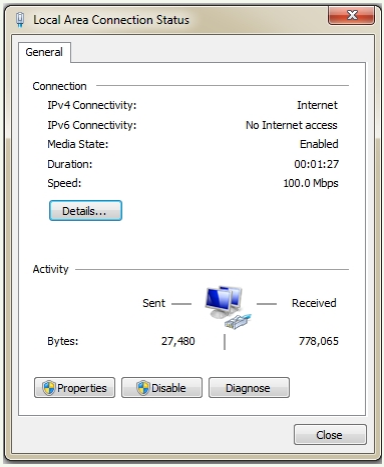
2.1.2 Directly Access through IE

The default network settings are as shown below:
IP address: **192.168.226.201**
Subnet Mask: **255.255.255.0**
Gateway: **192.168.226.1**
HTTP: **80**
Data port: **9008**

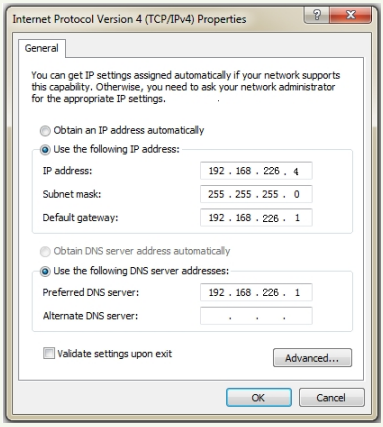
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



① Manually set the IP address of the PC and the network segment should be as the same as the default settings of the IP camera. Open the network and share center. Click "Local Area Connection" to pop up the following window.



Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



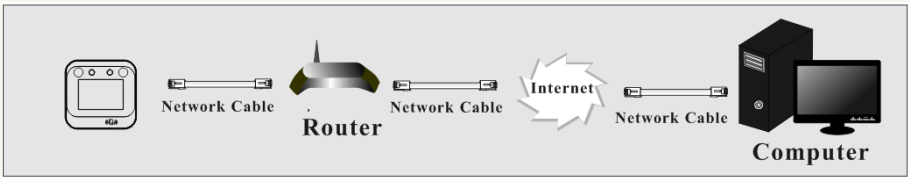
② Open the IE browser and enter the default address of IP-CAM and confirm.

③ Follow directions to download and install the Active X control.

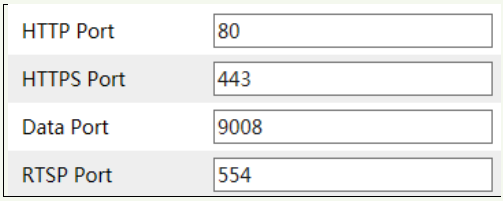
④ Enter the default username and password in the login window and then enter to view.

2.1.3 WAN

- **Access through the router or virtual server**

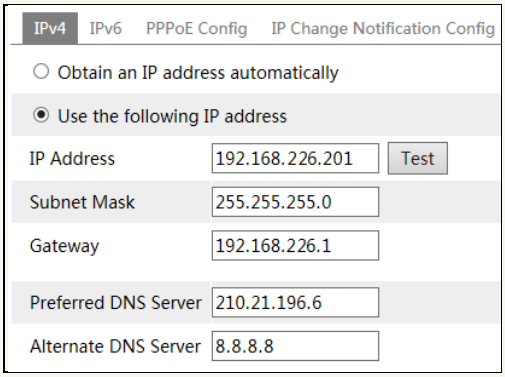


① Make sure the camera is well connected via LAN and then log in the camera via LAN and go to Config→Network→Port menu to set the port number.



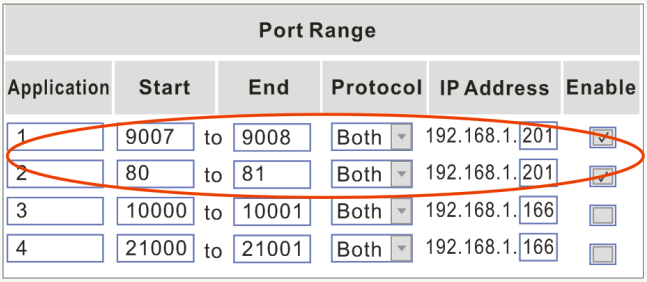
Port Setup

② Go to Config →Network→TCP/IP menu to modify the IP address.



IP Setup

③ Go to the router's management interface through IE browser to forward the IP address and port of the camera in the "Virtual Server".

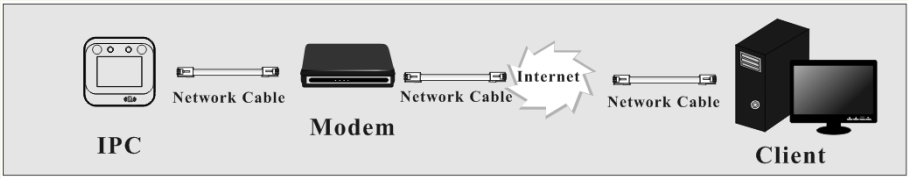


Router Setup

④ Open the IE browser and enter its WAN IP and http port to access. (for example, if the http port is changed to 81, please enter "192.198.1.201:81" in the address bar of web browser to access).

➢ **Access through PPPoE dial-up**

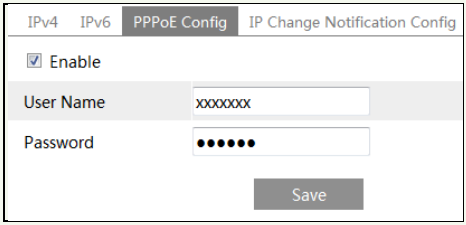
Network connection



Access the camera through PPPoE auto dial-up. The setting steps are as follow:

① Go to Config→Network→Port menu to set the port number.

② Go to Config →Network→TCP/IP→PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

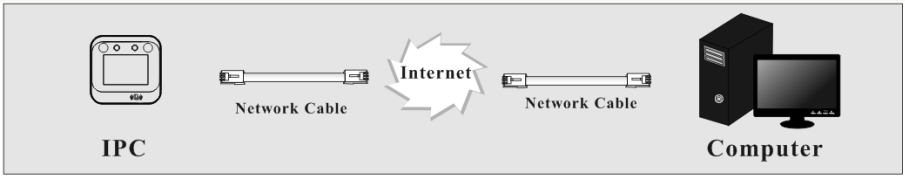


③ Go to Config →Network→DDNS menu. Before configuring the DDNS, please apply for a domain name first. Please refer to DDNS configuration for detail information.

④ Open the IE browser and enter the domain name and http port to access.

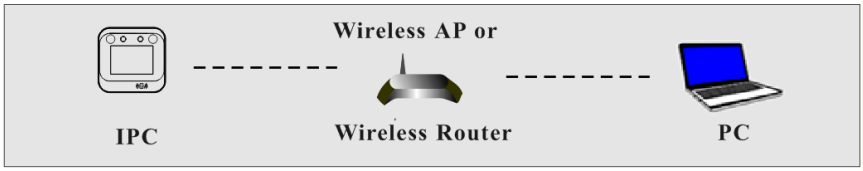
➢ **Access through static IP**

Network connection

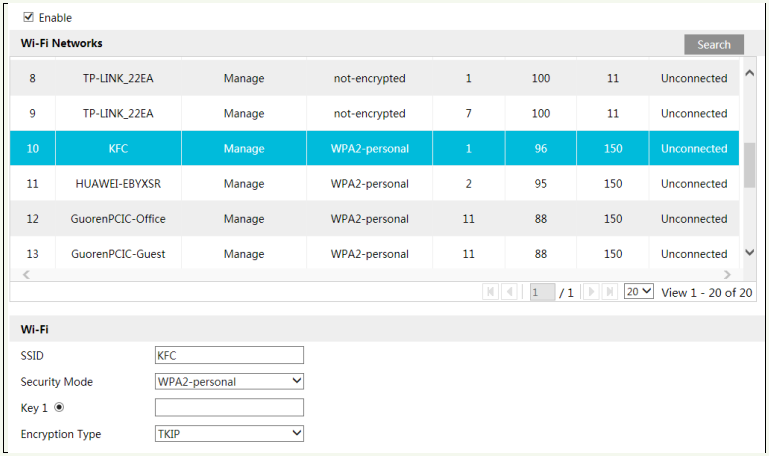


The setting steps are as follow:
① Go to Config→Network→Port menu to set the port number.
② Go to Config →Network→TCP/IP menu to set the IP address. Check "Use the following IP address" and then enter the static IP address and other parameters.
③ Open the IE browser and enter its WAN IP and http port to access.

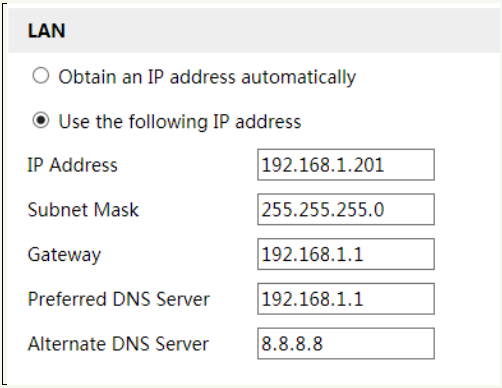
2.2 Wi-Fi Connection



① Use the network cable to connect the camera and wireless router or AP.
② Connect to the above wireless network with your PC. Then run the IP-Tool on your PC and then find the IP address of the camera. The default IP address of this camera is 192.168.226.201. Modify the IP address and gateway of the camera and make sure its network address is in the same local network segment as the computer's. Then double click it. This will bring you to the login interface of the camera. Enter the default username and password to log in. (See 2.1.1 for details)
③ Click Config→Network→WIFI to go to the following interface. Enable WI-FI, select the desired router, enter the key and select encryption type.



After that, select “Obtain an IP address automatically” or manually enter the IP address by clicking “Use the following IP address”. Then click “Save” to save the settings.



④ Pull the network cable out of the camera.

⑤ Run the IP-Tool and find the camera through IP address or MAC address. Then double click it listed in the IP-Tool or enter the IP address of the camera in the address bar of the web browser to access the camera.

2.3 APP Connection

- **In LAN**

① Enable Wi-Fi function of your phone, then open your phone’s APP store and search “Superlive Plus”.

② Install this APP in your phone.

③ Make sure your camera and phone are in the same local network.

④ Run this APP in your phone and then add the camera to the APP by entering IP address or domain name. After that, enter the username and password of the IPC.
Username: the default username is “admin”.
Password: the default password is “123456”.
④ View the image through the APP. Please refer to the Mobile Surveillance User Manual for more details.

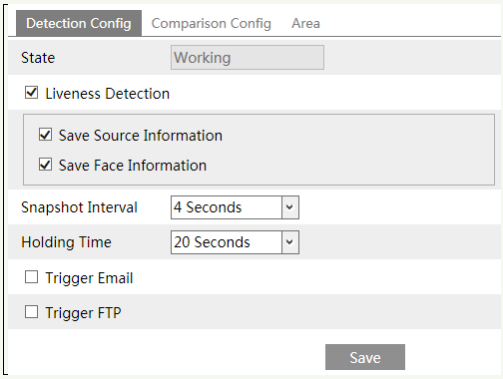
- **In WAN**

① Make sure your camera is connected to the Ethernet.
② Enable 2G/3G/4G/5G network of your phone.
③ Install the mobile APP (Superlive Plus) in your phone.
④ Run the mobile APP and then add the camera by scanning the QRcode of the IPC (Go to Config→System→Basic Information interface through IE browser).
⑤ View the image through the APP. Please refer to the Mobile Surveillance User Manual for more details.

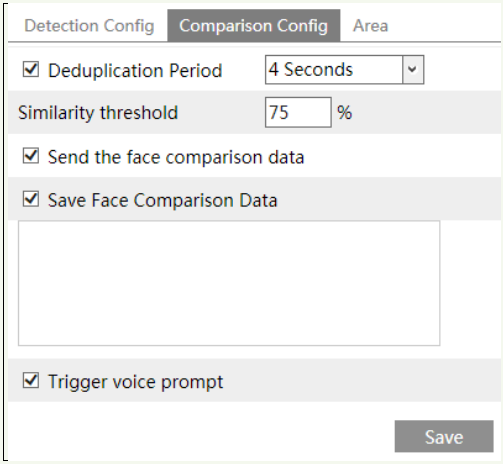
3 Face Recognition Configuration

3.1 Face Match Settings

Go to the face match configuration interface via Web Client to set the face match parameters.
1. Go to Config→Face→Face Match Config interface.

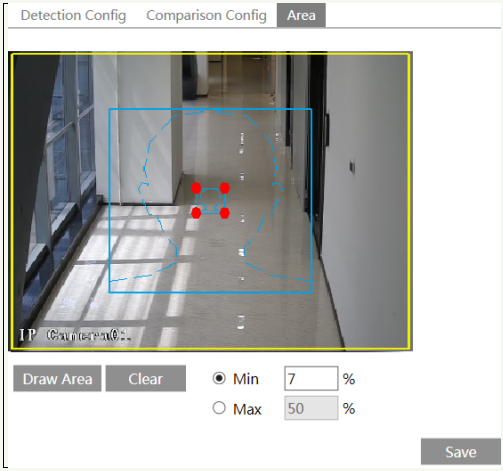


2. Enable liveness detection. If enabled, the system can distinguish real faces from non-real face spoof attacks.
Save Source Information: if enabled, the system will send the original picture to the pre-defined Email/FTP server when faces are detected and “Trigger Email/FTP” is checked.
Save Face Information: if enabled, the system will send the face picture to the pre-defined Email/FTP server when faces are detected and “Trigger Email/FTP” is checked.
3. Set alarm holding time and alarm trigger options.
Trigger Email: If “Trigger Email” and “Attach Picture” are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.
Trigger FTP: If “Trigger FTP” is checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.
4. Set face comparison options.



Deduplication Period: In the set period, delete the repeated comparison results.
Similarity threshold: When the similarity of the captured face picture and the face picture added into the face database exceeds the similarity threshold, alarms will be triggered.
Send the face comparison data: if it is disabled, the face comparison result will be displayed neither on the screen of the terminal nor on the live interface of the web client.
Save face comparison data: if enabled, the comparison data will be saved and you can search the face recognition result from the data record interface. If disabled, the face comparison data after you disable this function will not be searched in the data record interface.
Trigger voice prompt: Voice prompt will be triggered when the detected face is matched successfully. Please select the voice in advance (go to Config→Access Control System Config interface to set).

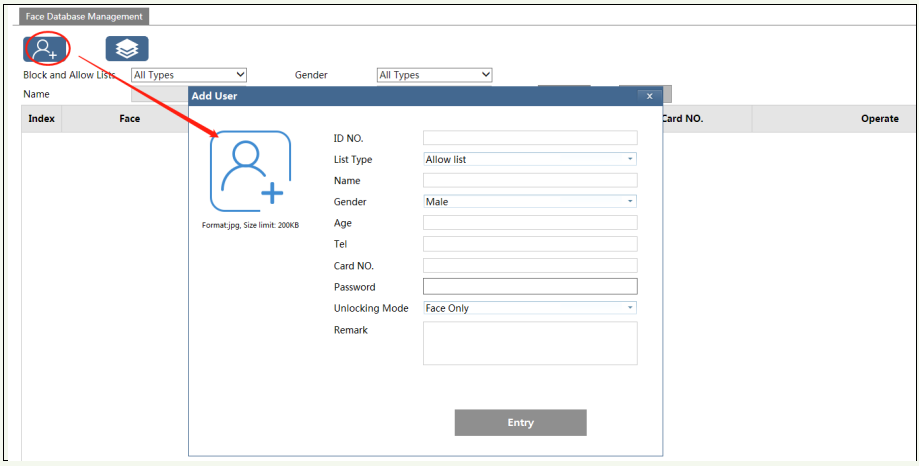
4. Set alarm detection area.



Click “Draw Area” and drag the border lines of the rectangle to modify its size. Move the rectangle to change its position. Click “Stop Draw” to stop drawing the area. Click “Clear” to clear the area. Then set the detectable face size by defining the maximum value and the minimum value (The default size range of a single face image occupies from 3% to 50% of the entire image).

3.2 Face Database Management

Please log in to the terminal via Web client and then Click “Config”→“Face Database Management” tab. This will enter the following interface.



There are four ways to add face pictures.

① Adding face pictures one by one

Click to pop up an adding user box. Then click to select a face picture saved on the local PC. Please select the picture according to the specified format and size limit. After that, fill out the relevant information of the face picture and click "Entry" to add.

List type: it includes allow list, visitor, block list.

Note: if the person needs to pass by swiping a card, please swiping the card on the device when adding the user information and then the ID number will be automatically filled in.

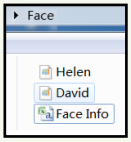
② Adding multiple face pictures at a time

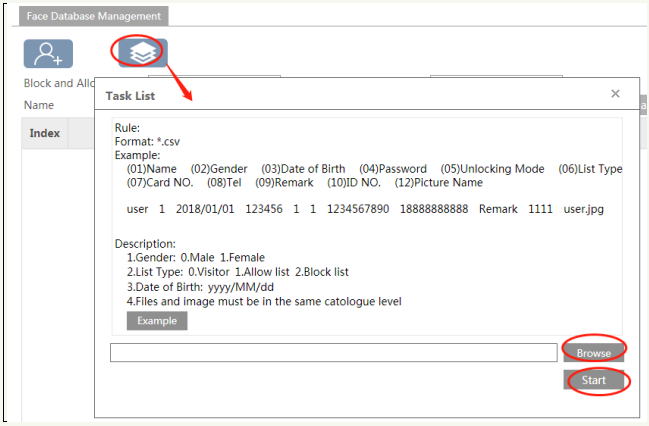
Click and then add multiple face pictures once according to the prompted rules.

Here is the example of the people information file (.csv).

	A	B	C	D	E	F	G	H	I	J	K	L
1	(01)Name	(02)Gende	(03)Birtl	(04)Passv	(05)Unlock	(06)List	(07)Card NO.	(08)Tel	(09)Remai	(10)ID N(	(12)Picture name	
2	Helen	1	2018/1/1	123456	1	1	1234567890	18888888888	Remark	1111	Helen.jpg	
3	David	0	2009/1/1	123456	1	1	1234561123	13700000000	Remark	222	David.jpg	

Put the people information file and images into the same directory as shown on the below left.



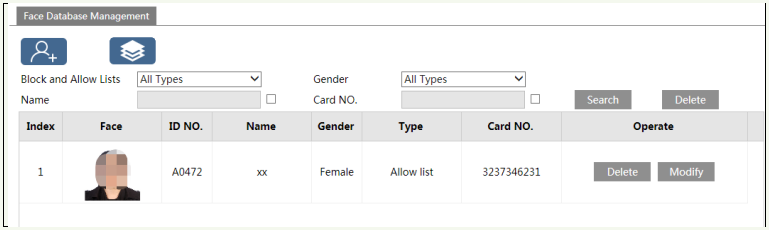


Click "Browse" to select the directory and then click "Start" to upload.

③ Add face pictures by using face album management tool

④ Add the captured picture in the live mode (See ***Add captured face pictures to the face database***).

After adding face pictures, you can search them by name, gender, ID number and so on.

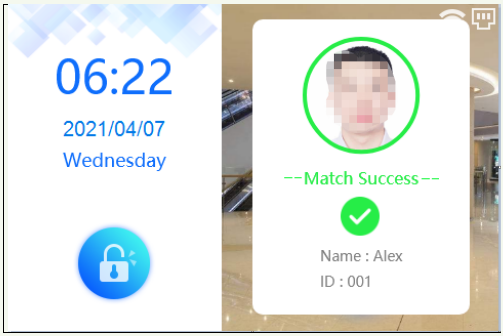


Click “Modify” to change people information and click “Delete” to delete this face picture.

4 Live View

4.1 Face Recognition View

After configuring face database and face match, the face match result will be viewed on the screen.
When detecting a face, the device will display the following interface.

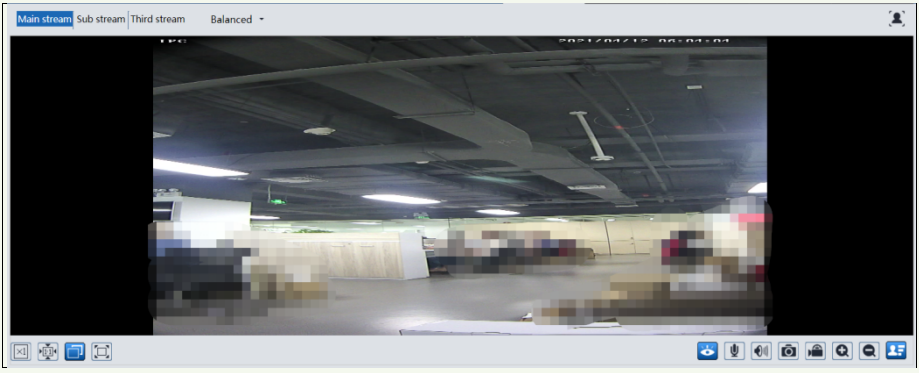


When the captured face is successfully matched, it will display “Match Success”.
When the captured face is not added to the face database or the similarity is lower than the pre-defined value, it will display “Match Failure” and the box will turn red.

4.2 Live View via Web

After logging in, the following window will be shown.

In this interface click and then you will see the captured face and match result.



The following table is the instructions of the icons on the live view interface.

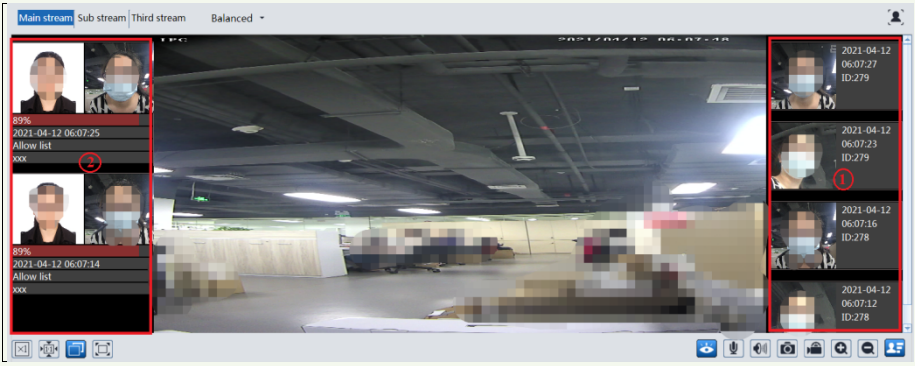
Icon	Description	Icon	Description
	Original size		Zoom in
	Fit correct scale		Zoom out
	Auto (fill the window)		Color abnormal indicator
	Full screen		Abnormal clarity indicator
	Start/stop live view		Scene change indicator
	Start/stop two-way audio		Face detection indicator
	Enable/disable audio		Face Detection
	Snapshot		Tampering alarm indicator
	Start/stop local recording		

Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

➢ **Face Match View**

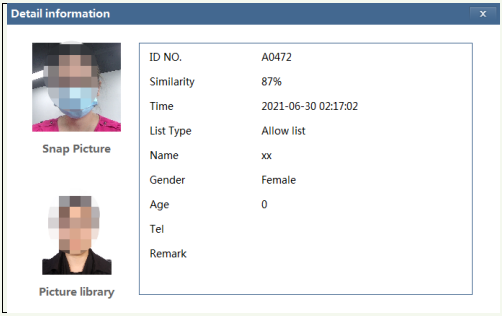
After all face comparison settings are set successfully, enter the live view interface. Click to view the captured face pictures and face comparison information.

Area ①: captured face pictures; area ②: face comparison area



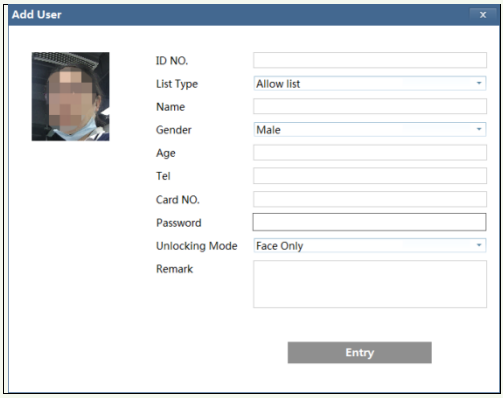
● **View the comparison details**

In area ②, click the compared face picture to bring up the following window. In this interface, you can view the detailed comparison information.



- **Add captured face pictures to the face database**

Click a captured picture in area ①. This will bring a face picture adding box.



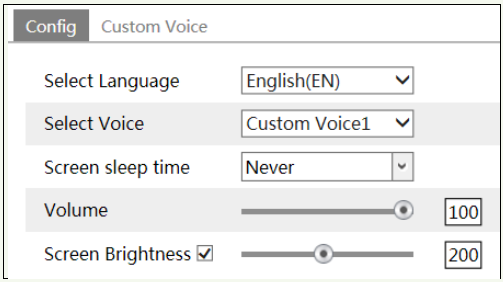
Fill out the relevant information and click “Entry” to add this face picture.

5 Access Control Settings

Here we take the access control settings of Web client for example.

5.1 Access Control System Settings

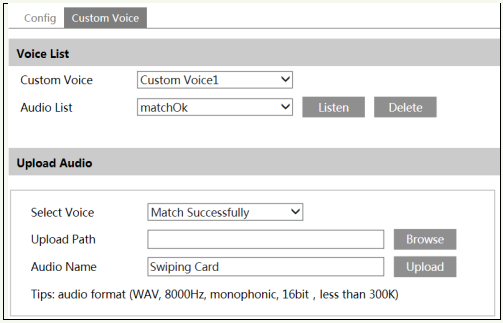
Click Config→Access Control→Access Control System Settings to go to the following interface.



Select Language: Select the screen display language on the panel/tablet.
Select Voice: Select the language of the voice prompt or the custom voice prompt.
Screen Sleep Time: Set how long the screen display will turn off after no person appears. The default time is 30s. Please set it as needed. In a sleep state, once a person is detected by the panel, it will be aroused immediately.
Volume: Set the volume of the voice prompt.
Screen Brightness: Set the brightness of the screen of the terminal (panel/tablet). The adjustable range is from 150 to 255.

- **Customizing Voice**

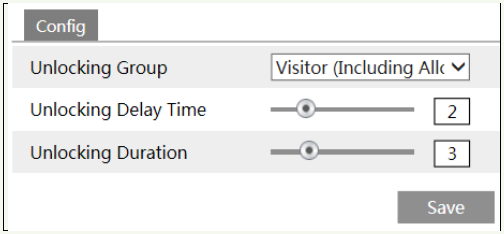
If you are dissatisfied with the default voice prompt, you can customize your own voice prompt. In the above interface, click “Custom Voice” tab to go to the following interface.



Select the voice you want to replace and then click "browse" to select the desired audio file. After that, click "Upload" to upload the audio file. Rename the audio as needed.
After your own voice prompt is uploaded, you can select it from the audio list and click "Listen" to listen to your voice prompt.

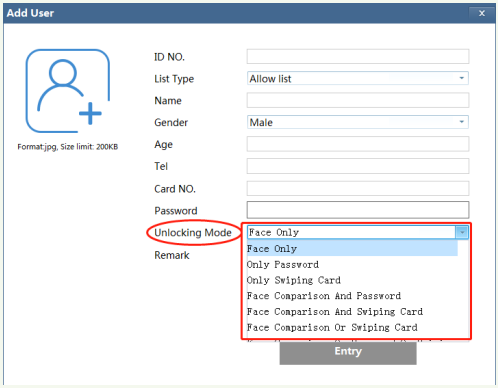
5.2 Door Lock Settings

Click Config→Access Control→Door Lock to go to the following interface. After the access control device is connected to the terminal, you can set unlocking mode in this interface.



Unlocking Group: Allow list, visitor (including allow list), stranger (including visitor and allow list).
Unlocking Delay Time: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Face only" and the delay time is set to "2" seconds; the door will be opened 2 seconds later after face recognition.
Unlocking Duration: If the door has been unlocked for a period that exceeds the duration, the door will be automatically locked. The time range is from 0 to 10 seconds. For example, the unlocking mode is "Face only" and the duration is set to "3" seconds; the unlocking door will be automatically locked 3 seconds later.

The way to set the unlocking mode:
You can set the unlocking mode when adding a user.

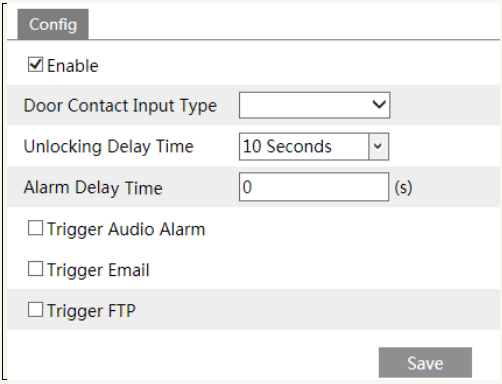


For example, supposed that the unlocking mode of someone is set to “Face Comparison and Swiping Card”, this person shall be matched successfully and swipe the card on the device, and then he/she can pass.

For a stranger, if you want to allow his/her access, the list type shall be set as “Stranger (including visitor and allow list), or the door cannot be linked to open.

5.3 Door Contact Settings

Click Config→Access Control→Door Contact Setting to go to the following interface.



Door Contact Input Type: NO or NC

Unlocking Delay Time: the allowable unlocking time. For example, if it is set to 10 seconds, alarms will be triggered when the door is not closed after 10 seconds.

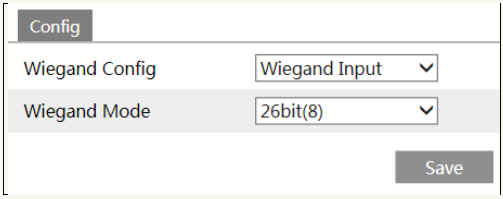
Alarm Delay Time: set the alarm delay time when faults of the door contact are detected. For example, if it is set to 3s, when detecting the failure of the door contact, alarms will be triggered 3s later.

Please select the alarm trigger options as needed. The setup steps of the alarm trigger options

are similar to the face match settings. Please refer to face match settings chapter for details.

5.4 Wiegand Settings

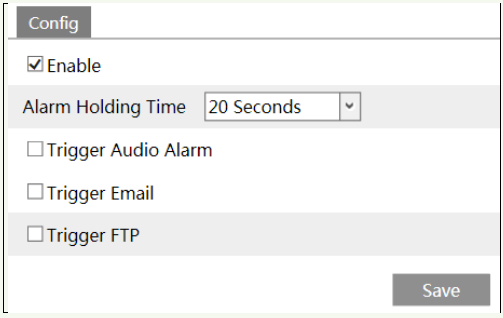
Click Config→Access Control→Wiegand Config to go to the following interface.



Wiegand Config: Wiegand Input, Wiegand Output or Off can be selected. If the card reader is connected to the Wiegand interface, please select "Wiegand Input". If the access controller is connected to the Wiegand interface, please select "Wiegand Output".
Wiegand Mode: 26bit(8), 26bit(10), 34bit, 37bit, 42bit, 46bit, 58bit or 66bit can be selectable.

5.5 Tampering Alarm Settings

In order to avoid the removal or damage by the external force, the tampering alarm can be set for the terminal. Click Config→Access Control→Tampering Alarm Setting to go to the following interface.



Enable "Tampering Alarm" and then set the alarm holding time and alarm trigger options.
Trigger Audio Alarm: if enabled, you will hear the warning sound when the terminal is removed or damaged by the external force.
The setup steps of other alarm trigger options are similar to the face match settings. Please refer to face match settings chapter for details.

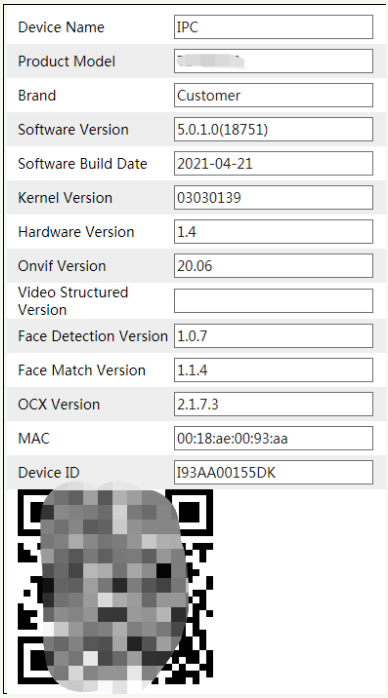
6 Other Configurations

You can set other configurations via the terminal or Web Client. Their setting steps are similar. Here we take the configurations of Web Client for example to introduce.
In the Webcam client, choose “Config” to go to the configuration interface.
Note: Wherever applicable, click the “Save” button to save the settings.

6.1 System Settings

6.1.1 Basic Information

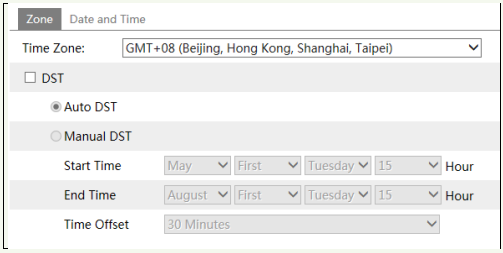
In the “Basic Information” interface, the system information of the device is listed.



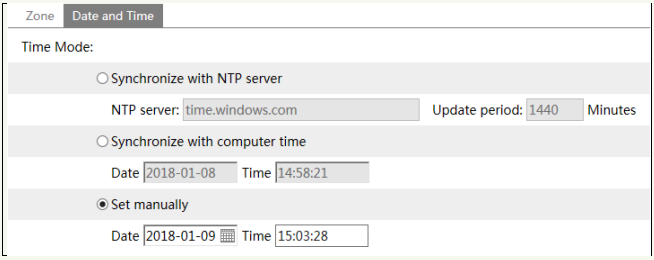
Here you can view the device ID and QR code. The network camera can be quickly added to mobile surveillance client by scanning the QR code or entering device ID.

6.1.2 Date and Time

Go to Config→System→Date and Time. Please refer to the following interface.

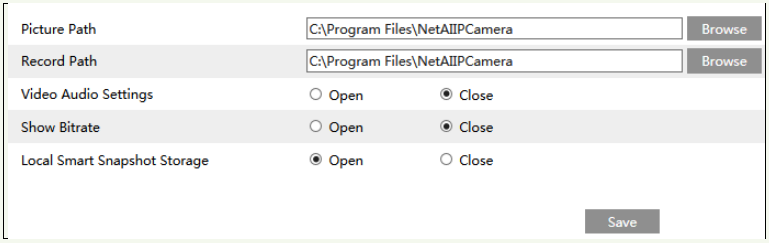


Select the time zone and DST as required.
Click the "Date and Time" tab to set the time mode.



6.1.3 Local Config

Go to Config→System→Local Config to set up the storage path of captured pictures and recorded videos on the local PC. There is also an option to enable or disable the bitrate display in the recorded files.

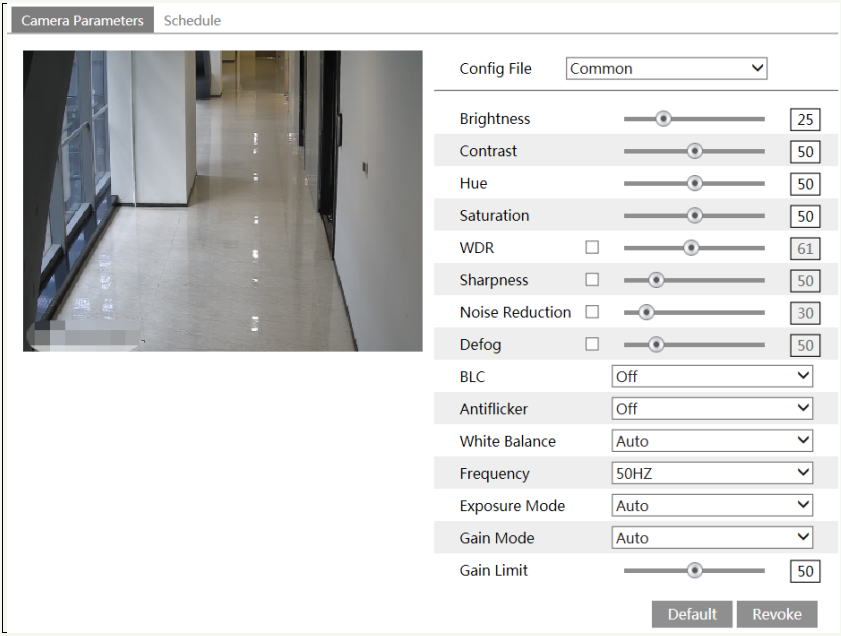


Additionally, the local smart snapshot (face snapshot) storage can be enabled/disable here.

6.2 Image Configuration

6.2.1 Display Configuration

Go to Image→Display interface as shown below. The image's brightness, contrast, hue and saturation and so on for common, day and night mode can be set up separately. The image effect can be quickly seen by switching the configuration file.



Brightness: Set the brightness level of the camera's image.
Contrast: Set the color difference between the brightest and darkest parts.
Hue: Set the total color degree of the image.
Saturation: Set the degree of color purity. The purer the color, the brighter the image is.
WDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field of the view by lowering the brightness of the bright area and increasing the brightness of the dark area. Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR mode.
Sharpness: Set the resolution level of the image plane and the sharpness level of the image edge.
Noise Reduction: Decrease the noise and make the image more thorough. Increasing the value will make the noise reduction effect better but it will reduce the image resolution.
Defog: Activating this function and setting an appropriate value as needed in foggy, dusty, smoggy or rainy environment to get clear images.
Backlight Compensation (BLC):

- Off: disables the backlight compensation function. It is the default mode.
- HLC: lowers the brightness of the entire image by suppressing the brightness of the image's bright area and reducing the size of the halo area.
- BLC: If enabled, the auto exposure will activate according to the scene so that the object of the image in the darkest area will be seen clearly.

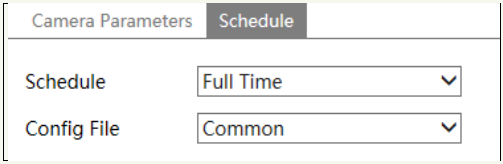
Antiflicker:

- Off: disables the anti-flicker function. This is used mostly in outdoor installations.
- 50Hz: reduces flicker in 50Hz lighting conditions.

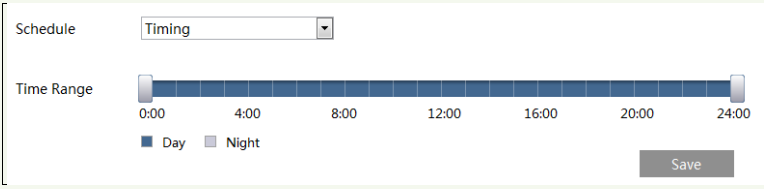
- 60Hz: reduces flicker in 60Hz lighting conditions.

White Balance: Adjust the color temperature according to the environment automatically.
Frequency: 50Hz and 60Hz can be optional.
Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.
Gain Mode: Choose "Auto" or "Manual". If "Auto" is selected, the gain value will be automatically adjusted according to the actual situation. If "Manual" is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

Schedule Settings of Image Parameters:
Click the "Schedule" tab as shown below.



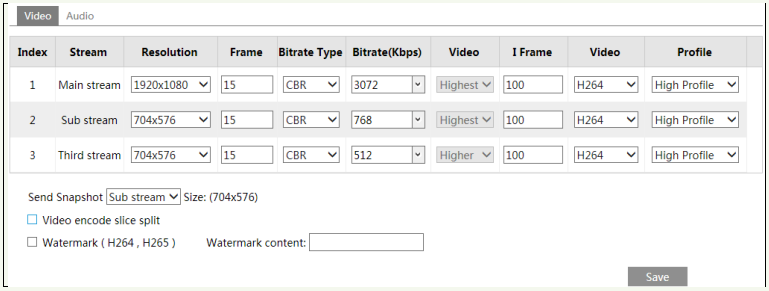
Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose "Timing" in the drop-down box of schedule as shown below.



Drag " " icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

6.2.2 Video / Audio Configuration

Go to Image→Video / Audio interface as shown below. In this interface, set the resolution, frame rate, bitrate type, video quality and so on subject to the actual network condition.



Three video streams can be adjustable.

Resolution: The size of image.

Frame rate: The higher the frame rate, the video is smoother.

Bitrate type: CBR and VBR are optional. Bitrate is related to image quality. CBR means that no matter how much change is seen in the video scene, the compression bitrate will be kept constant. VBR means that the compression bitrate will be adjusted according to scene changes. For example, for scenes that do not have much movement, the bitrate will be kept at a lower value. This can help optimize the network bandwidth usage.

Bitrate: it can be adjusted when the mode is set to CBR. The higher the bitrate, the better the image quality will be.

Video Quality: It can be adjusted when the mode is set to VBR. The higher the image quality, the more bitrate will be required.

I Frame interval: It determines how many frames are allowed between a “group of pictures”. When a new scene begins in a video, until that scene ends, the entire group of frames (or pictures) can be considered as a group of pictures. If there is not much movement in the scene, setting the value higher than the frame rate is fine, potentially resulting in less bandwidth usage. However, if the value is set too high, and there is a high frequency of movement in the video, there is a risk of frame skipping.

Video Compression: MJPEG**,** H264+, H264, H265, H265+ can be optional. If H.265/H.265+ is chosen, make sure the client system is able to decode H.265/H.265+.

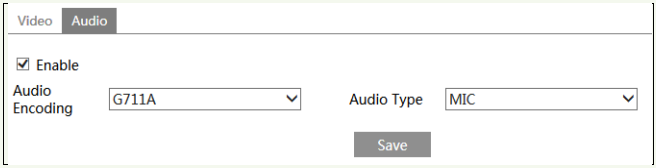
Profile: For H.264. Baseline, main and high profiles are selectable.

Send Snapshot: Select the snapshot stream.

Video encode slice split: If this function is enabled, smooth image can be gotten even though using the low-performance PC.

Watermark: When playing back the local recorded video in the search interface, the watermark can be displayed. To enable it, check the watermark box and enter the watermark text.

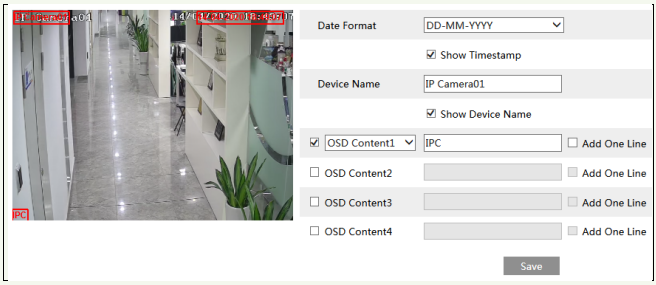
Click the “Audio” tab to go to the interface as shown below.



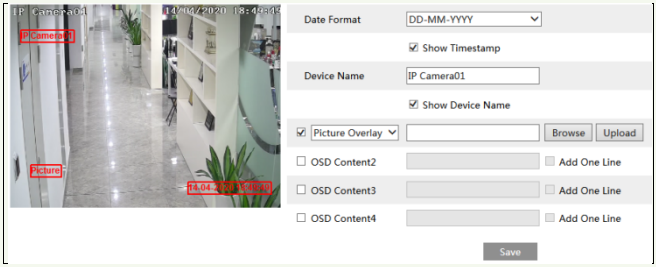
Audio Encoding: G711A and G711U are selectable.
Audio Type: MIC.

6.2.3 OSD Configuration

Go to Image→OSD interface as shown below.



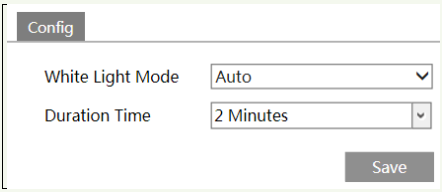
Set time stamp, device name, OSD content and picture overlap here. After enabling the corresponding display and entering the content, drag them to change their position. Then click the "Save" button to save the settings.

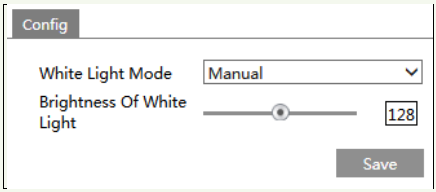


Picture Overlap Settings:
Check "OSD Content1", choose "Picture Overlay" and click "Browse" to select the overlap picture. Then click "Upload" to upload the overlap picture. The pixel of the image shall not exceed 200*200, or it cannot be uploaded.

6.2.4 White Light Control

Click Config→Image→White Light Control to go to the following interface.





White Light Mode: "OFF", "Manual" or "Auto" is optional. In low illumination condition, this mode can be enabled.

Auto: The white light will be automatically enabled when collecting a face in low illumination condition. If the auto mode is selected, the duration time should be set for saving energy. For example, the white light is on and the duration time is set to "2 minutes"; if no face appears in the detection area after 2 minutes, the white light will be turned off automatically.

Manual: Select this mode and click "Save". The white light will be turned on. In this mode, you can also set the brightness of white light as needed.

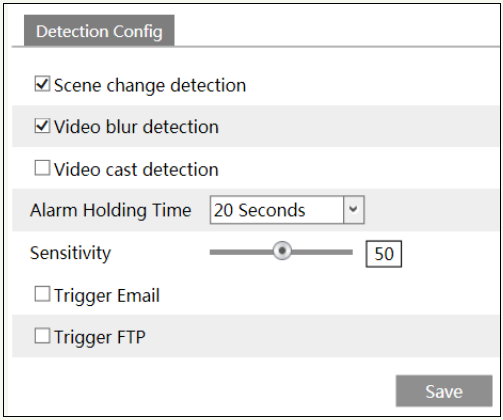
6.3 Alarm Configuration

6.3.1 Exception Detection

This function can detect changes in the surveillance environment affected by the external factors.

To set exception detection:

Go to Config→Alarm→Exception interface as shown below.



1. Enable the applicable detection that's desired.

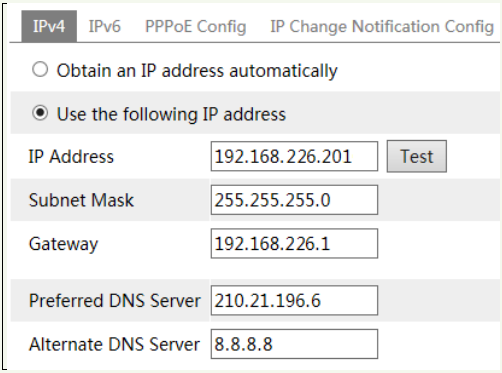
Scene Change Detection: Alarms will be triggered if the scene of the monitor video has changed.

Video Blur Detection: Alarms will be triggered if the video becomes blurry.
Video Cast Detection: Alarms will be triggered if the video becomes obscured.
2. Set the alarm holding time.
3. Set the sensitivity of the exception detection. Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox. Click "Save" button to save the settings.
The sensitivity value of Scene Change Detection: The higher the value is, the more sensitive the system responds to the amplitude of the scene change.
The sensitivity value of Video Blur Detection: The higher the value is, the more sensitive the system responds to the blurriness of the image.
The sensitivity value of Video Cast Detection: The higher the value is, the more sensitive the system responds to the obscuring of the image.
4. Set alarm trigger options.
Trigger Email: If "Trigger Email" and "Attach Picture" are checked (email address must be set first in the Email configuration interface), the captured pictures and triggered event will be sent into those addresses.
Trigger FTP: If "Trigger FTP" is checked, the captured pictures will be sent into FTP server address. Please refer to FTP configuration chapter for more details.
5. Click "Save" button to save the settings.

6.4 Network Configuration

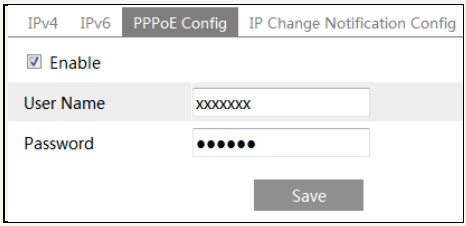
6.4.1 TCP/IP

Go to Config→Network→TCP/IP interface as shown below. There are two ways for network connection.

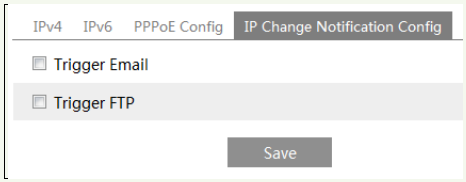


Use IP address (take IPv4 for example)-There are two options for IP setup: obtain an IP address automatically by DHCP and use the following IP address. Please choose one of the options as needed.
Test: Test the effectiveness of the IP address by clicking this button.
Use PPPoE-Click the "PPPoE Config" tab to go to the interface as shown below. Enable

PPPoE and then enter the user name and password from your ISP.



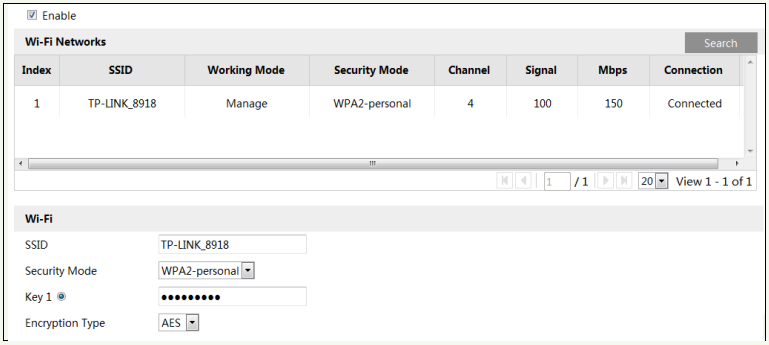
Either method of network connection can be used. If PPPoE is used to connect internet, the camera will get a dynamic WAN IP address. This IP address will change frequently. To be notified, the IP change notification function can be used.
Click "IP Change Notification Config" to go to the interface as shown below.



Trigger Email: when the IP address of the device is changed, the new IP address will be sent to the email address that has been set up.
Trigger FTP: when the IP address of the device is changed, the new IP address will be sent to FTP server that has been set up.

6.4.2 Wi-Fi Settings

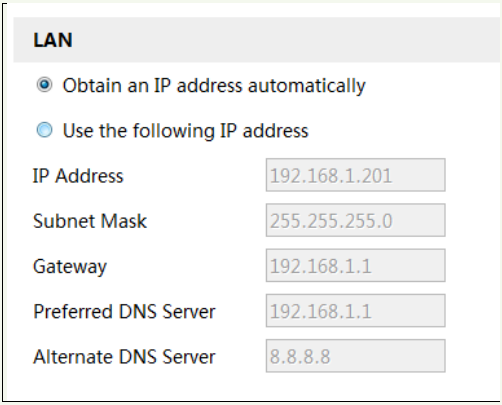
Go to Config→Network→WIFI interface as shown below.



1. Checkmark "Enable" to enable Wi-Fi.
Click "Search" to refresh the online wireless devices.

2. Choose a wireless device on the list. The SSID and security mode of the wireless device will be shown automatically. Please don't change it manually.
3. Enter the key to connect the wireless device. This key should be set on the wireless device in advance for wireless network connection.

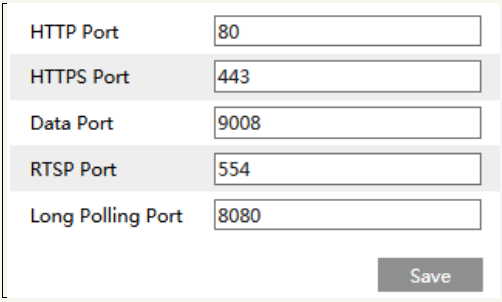
After the above-mentioned wireless network is configured, you can choose "Obtain an IP address automatically" or "Use the following IP address".



If you choose "Obtain an IP address automatically", you shall get the IP address from the router. Or you can choose "Use the following IP address" to set the network parameters manually. Then you can use this IP address to log in mobile surveillance APP/ web client/CMS/NVR/…

6.4.3 Port

Go to Config→Network→Port interface as shown below. HTTP port, Data port and RTSP port can be set.

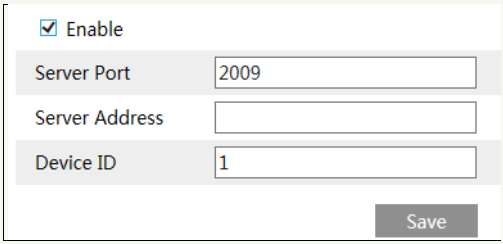


HTTP Port: The default HTTP port is 80. It can be changed to any port which is not occupied.

HTTPS Port: The default HTTPs port is 443. It can be changed to any port which is not occupied.
Data Port: The default data port is 9008. Please change it as necessary.
RTSP Port: The default port is 554. Please change it as necessary.
Long Polling Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.

6.4.4 Server Configuration

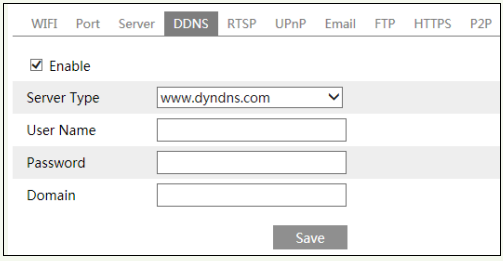
This function is mainly used for connecting network video management system.



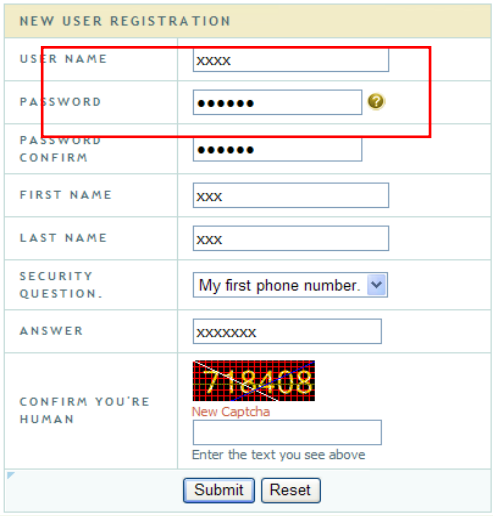
1. Check “Enable”.
2. Check the IP address and port of the transfer media server in the ECMS/NVMS. Then enable the auto report in the ECMS/NVMS when adding a new device. Next, enter the remaining information of the device in the ECMS/NVMS. After that, the system will automatically allot a device ID. Please check it in the ECMS/NVMS.
3. Enter the above-mentioned server address, server port and device ID in the corresponding boxes. Click the “Save” button to save the settings.

6.4.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.
1. Go to Config→Network→ DDNS.

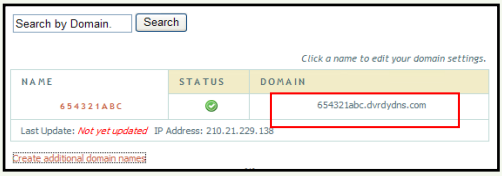


2. Apply for a domain name. Take www.dvrdyndns.com for example.
Enter www.dvrdydns.com in the IE address bar to visit its website. Then Click the “Registration” button.



Create domain name.

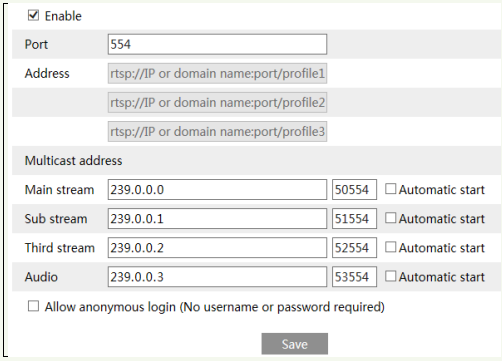
After the domain name is successfully applied for, the domain name will be listed as below.



3. Enter the username, password, domain you apply for in the DDNS configuration interface.
4. Click the “Save” button to save the settings.

6.4.6 RTSP

Go to Config→Network→RTSP.



Select “Enable” to enable the RTSP function.
Port: Access port of the streaming media. The default number is 554.
RTSP Address: The RTSP address (unicast) format that can be used to play the stream in a media player.

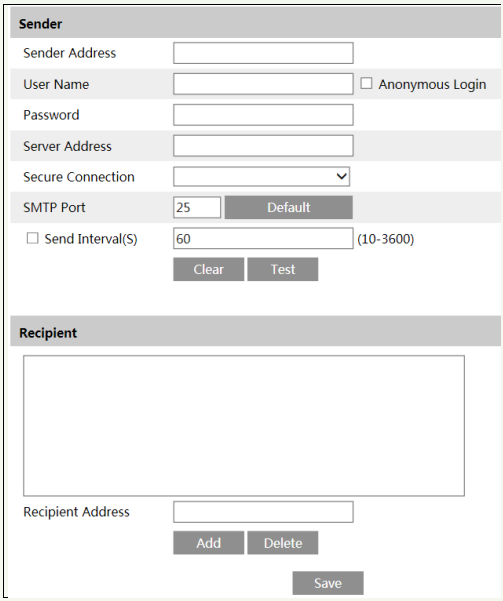
Multicast Address
Main stream: The address format is
“rtsp://IP address: rtsp port/profile1?transportmode=mcast”.
Sub stream: The address format is
“rtsp://IP address: rtsp port/profile2?transportmode=mcast”.
Third stream: The address format is
“rtsp://IP address: rtsp port/profile3?transportmode=mcast”.
Audio: Having entered the main/sub stream in a VLC player, the video and audio will play automatically.
If “Allow anonymous login…” is checked, there is no need to enter the username and password to view the video.
If “auto start” is enabled, the multicast received data should be added into a VLC player to play the video.
Note:1. This camera support local play through a VLC player. Enter the RTSP address (unicast or multicast, eg. rtsp://192.168.226.201:554/profile1?transportmode=mcast) in a VLC player to realize the simultaneous play with the web client.
2. The IP address mentioned above cannot be the address of IPv6.
3. Avoid the use of the same multicast address in the same local network.
4. When playing the video through the multicast streams in a VLC player, please pay attention to the mode of the VLC player. If it is set to TCP mode, the video cannot be played.
5. If the coding format of the video of the main stream is MJPEG, the video may be disordered at some resolutions.

6.4.7 UPnP

If this function is enabled, the camera can be quickly accessed through the LAN.
Go to Config→Network→UPnP. Enable UPNP and then enter UPnP name.

6.4.8 Email

If you need to trigger Email when an alarm happens or IP address is changed, please set the Email here first.
Go to Config→Network →Email.

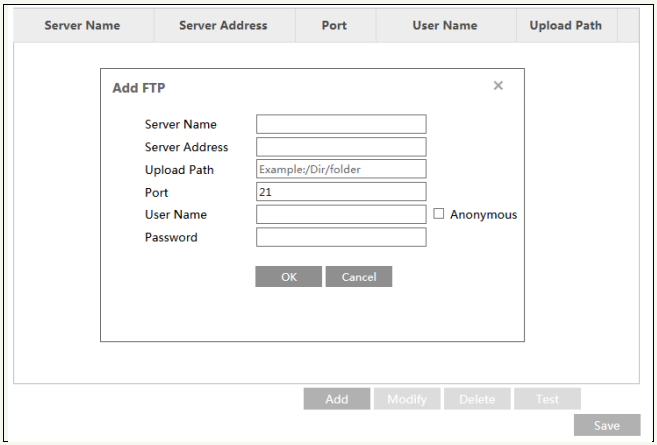


Sender Address: sender's e-mail address.
User name and password: sender's user name and password. If "Anonymous login" is selected, an anonymous Email will be sent when an alarm is triggered.
Server Address: The SMTP IP address or host name.
Select the secure connection type at the "Secure Connection" pull-down list according to what's required.
SMTP Port: The SMTP port.
Send Interval(S): The time interval of sending email. For example, if it is set to 60 seconds and multiple motion detection alarms are triggered within 60 seconds, they will be considered as only one alarm event and only one email will be sent. If one motion alarm event is triggered and then another motion detection alarm event is triggered after 60 seconds, two emails will be sent. When different alarms are triggered at the same time, multiple emails will be sent separately.

Click the "Test" button to test the connection of the account.
Recipient Address: receiver's e-mail address.

6.4.9 FTP

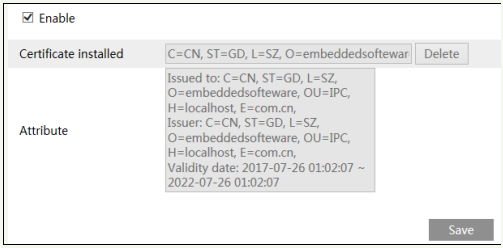
After an FTP server is set up, captured pictures from events will be uploaded to the FTP server.
Go to Config→Network →FTP.



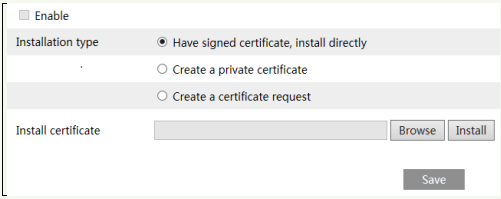
Server Name: The name of the FTP server.
Server Address: The IP address or domain name of the FTP.
Upload Path: The directory where files will be uploaded to.
Port: The port of the FTP server.
User Name and Password: The username and password that are used to login to the FTP server.

6.4.10 HTTPS

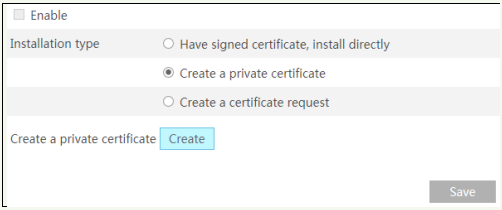
HTTPs provides authentication of the web site and protects user privacy.
Go to Config →Network→HTTPS as shown below.



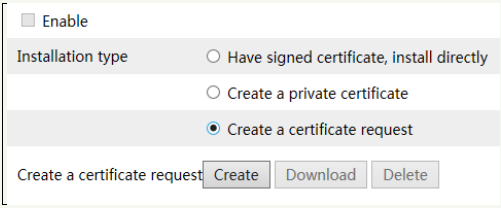
There is a certificate installed by default as shown above. Enable this function and save it. Then the camera can be accessed by entering https://IP: https port via the web browser (eg. https://192.168.226.201:443).
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



* If there is a signed certificate, click "Browse" to select it and then click "Install" to install it.
* Click "Create a private certificate" to enter the following creation interface.



Click the "Create" button to create a private certificate. Enter the country (only two letters available), domain (camera's IP address/domain), validity date, password, province/state, region and so on. Then click "OK" to save the settings.
* Click "Create a certificate request" to enter the following interface.

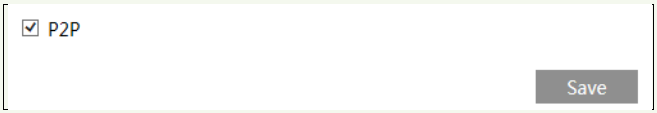


Click "Create" to create the certificate request. Then download the certificate request and submit it to the trusted certificate authority for signature. After receiving the signed certificate, import the certificate to the device.

6.4.11 P2P

If this function is enabled, the network camera can be quickly accessed by adding the device ID in mobile surveillance client or CMS/NVMS client via WAN. This function is enabled by

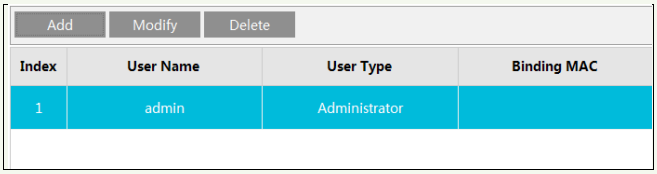
default.



6.5 Security Configuration

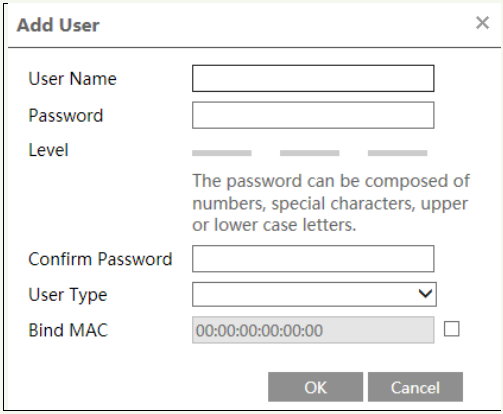
6.5.1 User Configuration

Go to Config→Security→User interface as shown below.



Add user:

1. Click the "Add" button to pop up the following textbox.



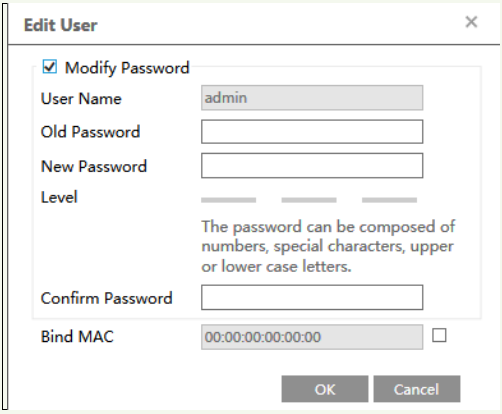
2. Enter user name in "User Name" textbox.
3. Enter the password in the "Password" and "Confirm Password" textbox.

It is recommended to set a high level password that shall be composed of numbers, special characters, upper or lower case letters for your account security.

4. Choose the user type. Administrator has all permissions. Normal user can only view the live video. Advanced user has the same permissions as an Administrator except for; user, backup settings, factory reset, and upgrading the firmware.
5. Enter the MAC address of the PC in the "Bind MAC" textbox.

If this option is enabled, only the PC with the specified MAC address can access the camera for that user.
6. Click the "OK" button and then the newly added user will be displayed in the user list.

Modify user:
1. Select a user to modify password and MAC address if necessary in the user configuration list box.
2. The "Edit user" dialog box pops up by clicking the "Modify" button.



3. Enter the old password of the user in the "Old Password" text box.
4. Enter the new password in the "New password" and "Confirm Password" text box.
5. Enter computer's MAC address as necessary.
6. Click the "OK" button to save the settings.
Note: To change the access level of a user, the user must be deleted and added again with the new access level.

Delete user:
1. Select the user to be deleted in the user configuration list box.
2. Click the "Delete" button to delete the user.
Note: The default administrator account cannot be deleted.

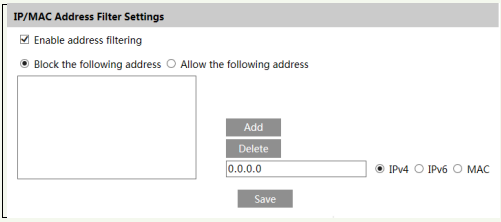
6.5.2 Online User

Go to Config→Security→Online User to view the user who is viewing the live video.

An administrator user can kick out all the other users (including other administrators).

6.5.3 Block and Allow Lists

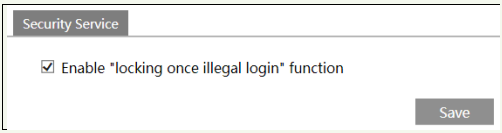
Go to Config→Security→Block and Allow Lists as shown below.



The setup steps are as follows:
Check the “Enable address filtering” check box.
Select “Block/Allow the following address”, IPv4/IPv6/MAC and then enter IP address or MAC address in the address box and click the “Add” button.

6.5.4 Security Management

Go to Config→Security→Security Management as shown below.

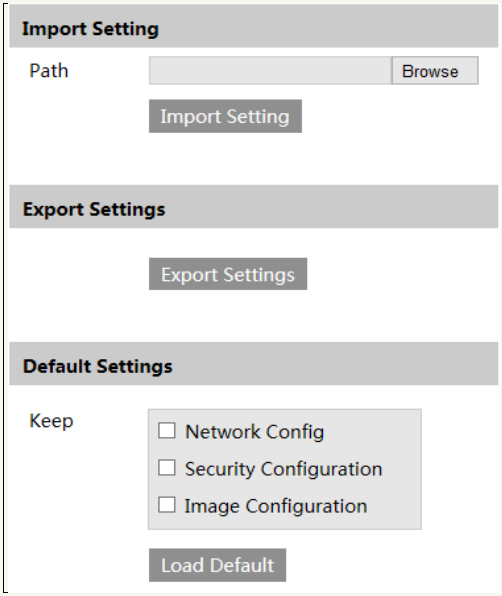


In order to prevent against malicious password unlocking, “locking once illegal login” function can be enabled here. If this function is enabled, login failure after trying six times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

6.6 Maintenance Configuration

6.6.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.



- **Import & Export Settings**

Configuration settings of the camera can be exported form a camera into another camera.
1. Click “Browse” to select the save path for import or export information on the PC.
2. Click the “Import Setting” or “Export Setting” button.

- **Default Settings**

Click the “Load Default” button to restore all system settings to the default factory settings except those you want to keep.

6.6.2 Reboot

Go to Config→Maintenance→Reboot.
Click the “Reboot” button to reboot the device.

Timed Reboot Setting:
If necessary, the camera can be set up to reboot on a time interval. Enable “Time Settings”, set the date and time and then click the “Save” button to save the settings.

6.6.3 Upgrade

Go to Config→Maintenance→Upgrade. In this interface, the camera firmware can be updated.

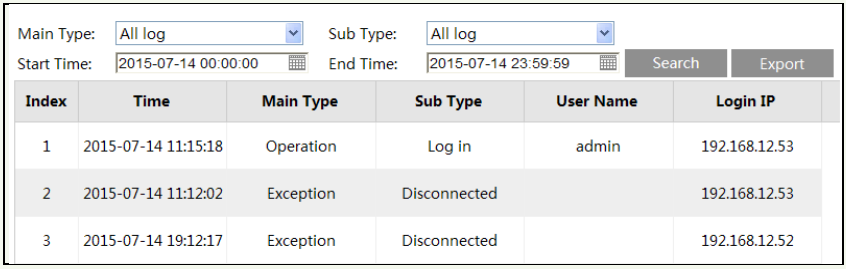
1. Click the “Browse” button to select the save path of the upgrade file
2. Click the “Upgrade” button to start upgrading the firmware.
3. The device will restart automatically

Caution! Do not close the browser or disconnect the camera from the network during the upgrade.

6.6.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

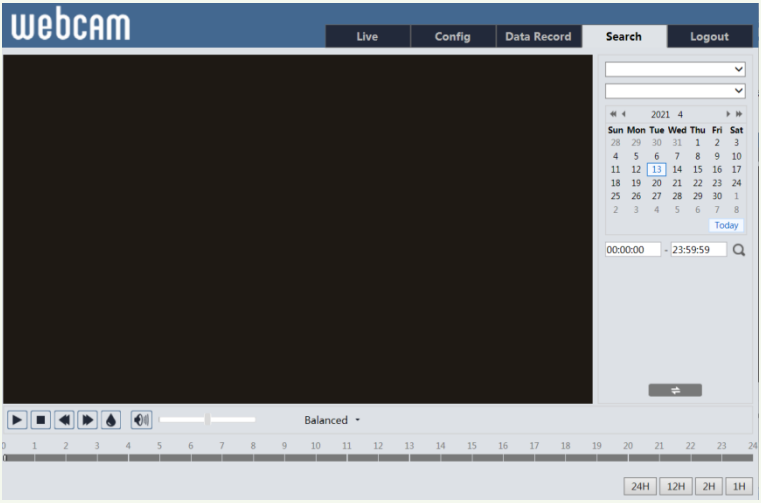


Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:15:18	Operation	Log in	admin	192.168.12.53
2	2015-07-14 11:12:02	Exception	Disconnected		192.168.12.53
3	2015-07-14 19:12:17	Exception	Disconnected		192.168.12.52

2. Select the main type, sub type, start and end time.
3. Click “Search” to view the operation log.
4. Click “Export” to export the operation log.

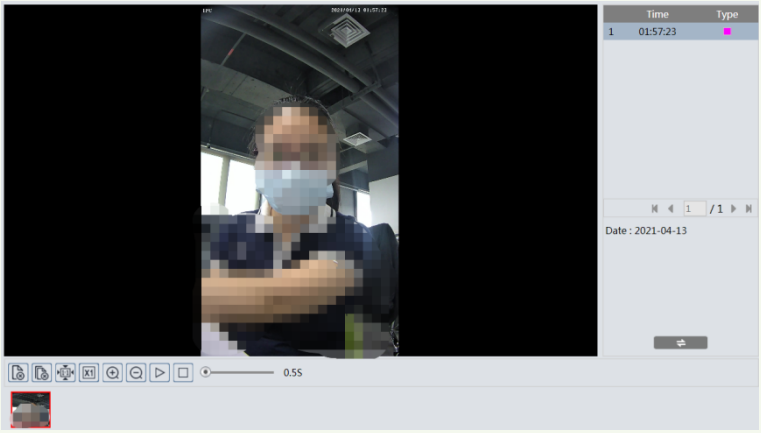
7.1 Image Search

Click Search to go to the interface as shown below.



- **Local Image Search**

1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click to search the images.



4. Double click a file name in the list to view the captured photos as shown above.

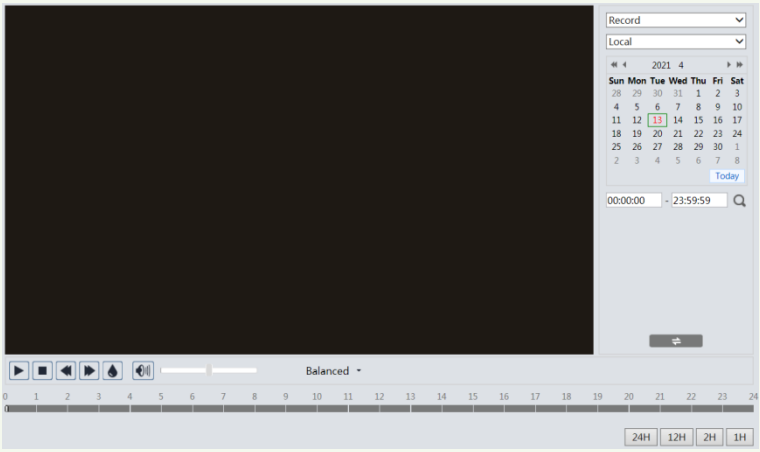
Click ⇌ to return to the previous interface.

The descriptions of the buttons are shown as follows.

Icon	Description	Icon	Description
	Close: Select an image and click this button to close the image.		Close all: Click this button to close all images.
	Fit size: Click to fit the image on the screen.		Actual size: Click this button to display the actual size of the image.
	Zoom in: Click this button to digitally zoom in.		Zoom out: Click this button to digitally zoom out.
	Slide show play: Click this button to start the slide show mode.		Stop: Click this button to stop the slide show.
5.5S	Play speed: Play speed of the slide show.		

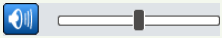
7.2 Video Search

Click Search to go to the interface as shown below. Videos were recorded locally to the PC can be played in this interface.



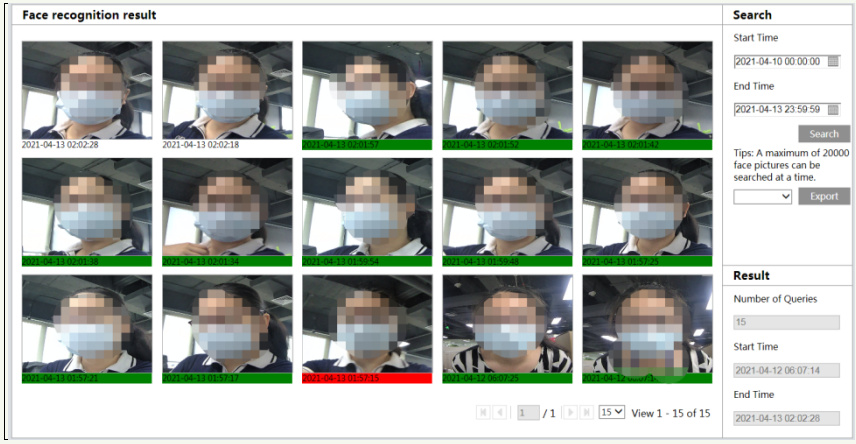
1. Choose “Record”—“Local”.
2. Set search time: Select the date and choose the start and end time.
3. Click 🔍 to search the images.

4. Double click on a file name in the list to start playback.

Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

8 Face Match Result Search

Click “Data Record” tab to go to the face recognition result search interface.
Set the start time and end time and click “Search” to view the face recognition result.



Red time tag means no comparison result. Green time tag means there is a comparison result. Click the picture with green time tag and then the face comparison information can be viewed as shown below.

Click the picture with red time tag. This will bring an adding user box. You can add this face picture into the face database.
Click “Export” to export the captured pictures. You can choose to export image and file or file only.

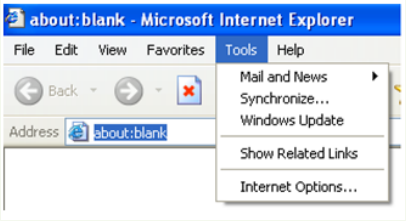
Appendix 1 Troubleshooting

How to find the password?
A：Reset the device to the default factory settings.
Default IP: 192.168.226.201; User name: admin; Password: 123456

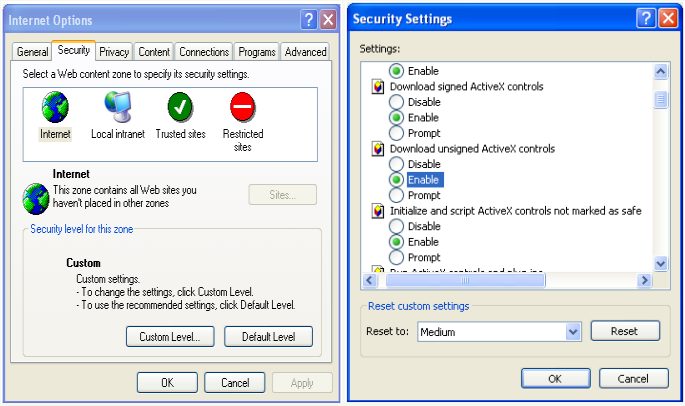
Fail to connect devices through IE browser.
A: Network is not well connected. Check the connection and make sure it is connected well.
B: IP address is not available. Reset the IP address.
C: Web port number has been changed: contact administrator to get the correct port number.
D: Exclude the above reasons. Restore to default setting by IP-Tool.

IP tool cannot search devices.
It may be caused by the anti-virus software in your computer. Please exit it and try to search device again.

IE cannot download ActiveX control.
A. IE browser may be set up to block ActiveX. Follow the steps below.
① Open IE browser and then click Tools-----Internet Options.



② Select Security------Custom Level….
③ Enable all the options under "ActiveX controls and plug-ins".
④ Click OK to finish setup.
B. Other plug-ins or anti-virus blocks ActiveX. Please uninstall or close them.



No sound can be heard.

A： Audio input device is not connected. Please connect and try again.

B: Audio function is not enabled at the corresponding channel. Please enable this function.

Appendix 2 Specifications

Camera	
Image Sensor	1/2.8" Progressive Scan CMOS
Image Size	1920×1080
Electronic Shutter	1/2s ~ 1/100000s
IRIS Type	Fixed IRIS
MIN. Illumination	0 lux
Lens	2MP dual lens; f=3.6mm @F2.4; Vertical horizontal field of view: approx. 65°; horizontal field of view: approx. 50°
Lens Mount	M12
WDR	74dB
BLC	Yes
HLC	Yes
Defog	Yes
DNR	2D/3D NR
Image	
Video Compression	H.265+/H.265/ H.264+/H.264/MJPEG
H.264 Compression Standard	Baseline Profile/Main Profile/High Profile
Bit rate Type	VBR/CBR
Bit Rate	128Kbps ~ 6Mbps
Resolution	1080P(1920×1080), 720P(1280×720), D1
Main Stream	50Hz/60Hz: 1920×1080/1280×720(1~15fps)
Sub Stream	50Hz/60Hz: 720P/D1(1~15fps)
Third Stream	50Hz/60Hz: D1(1~15fps)
Image Setting	Saturation, hue, brightness, contrast, wide dynamic range, sharpness, NR, etc., adjustable through client or web browser
Audio Compression	G711A/U
Screen	
3.5 inch Touch Screen	Resolution: 320 (RGB)v 480
Brightness	250cd/m^2
Card	
Card Type	Mifare card /Desfire card/FM1208 Card/Gicard
Card Reading Protocol	ISO14443A/B
Card Reading Frequency	13.56MHz
Card Reading Duration	<1s
Card Reading Distance	0~3cm
Interfaces	
Network	100M RJ45
Audio	Built-in MIC×1, built-in speaker×1
Door Lock Output	1CH
Exit Button	1 CH
Door Contact Input	1 CH

Anti-Tamper Interface	1 CH
Reset Button	1
Wiegand Interface	Yes (Wiegand input or output configurable)
WiFi	Supports 2.4G WiFi function
Function	
Remote Monitoring	Web client/CMS remote control
Online Connection	Supports simultaneous monitoring for up to 3 users Supports multi-stream real time transmission
Network Protocol	UDP, IPv4, IPv6, DHCP, NTP, RTSP, PPPoE, DDNS, SMTP, FTP, UPnP, HTTPS, HTTP
Interface Protocol	ONVIF
Storage	Network remote storage
Intelligent Analytics	Face detection, face capture, face match, scene change detection, video blur detection, video color cast detection
General Function	Watermark, IP address filtering, video mask, heartbeat, illegal login, image distortion correction
PoE	Yes (802.3af)
Whit Light Distance	0.3-0.5m soft light
IR Light Distance	0.3-1m
Face	
Face Picture Database	3000
Face Comparison Storage	10,000
Intelligent Light Compensation	Built-in high efficient white light LEDs
Others	
Power	DC12V/1A
Power Consumption	< 12W
Working Environment	-20℃~50℃, Humidity: less than 95% (non-condensing)
Dimensions(mm)	118mm×114mm×25.1mm
Weight (net)	Approx. 300g
Installation	Wall mounting; Standing on desktop