

VIDEO DOORBELL

User Manual

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

Safety Instruction

The following symbols or words may be found in this manual.

Symbols/Words	Description
 Warning	Indicates a medium or low potential hazardous situation which, if not avoided, will or could result in slight or moderate injury.
 Caution	Indicates a potential risk which, if not avoided, will or could result in device damage, data loss, lower performance or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the text.

About the Manual

- This manual is suitable for many models. All examples, screenshots, figures, charts, and illustrations used in the manual are for reference purpose, and actual products may be different with this Manual.
- Please read this user manual carefully to ensure that you can use the device correctly and safely.
- Within the maximum scope permitted by the law, the products described in this Manual (including hardware, software, firmware, etc.) are provided "AS IS". The information in this document (including URL and other Internet site reference data) is subject to change without notice. This Manual may contain technical incorrect places or printing errors. This information will be periodically updated, and these changes will be added into the latest version of this Manual without prior notice.

Use of the Product

- This product should not be used for illegal purposes.
- The company does not allow anyone to use the Company's products to infringe the privacy, personal information, and portrait rights of others. The user shall not use this product for any illegal use or any prohibited use under these terms, conditions, and declarations. When using this product, the user shall not damage, disable, overload or obstruct any of the hardware of this product in any way, or interfere with the use of this product by any other users. Also, the user should not attempt to use the product or the software, by hacking, stealing the password, or any other means.

Electrical 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/2 A or POE 48V/ 350mA or AC24V (depending on models), no more than 2000m altitude of operation and Tma+60 Deg. C.

- As for the modes with PoE function, the function of the ITE being investigated to IEC 60950-1 standard is considered not likely to require connection to an Ethernet network with outside plant routing, including campus environment and the ITE is to be connected only to PoE networks without routing to the outside plant.
- Improper handling and/or installation could run the risk of fire or electrical shock.
- The product must be grounded to reduce the risk of electric shock.
- ⚠ Warning: Wear anti-static gloves or discharge static electricity before removing the bubble or cover of the camera.
- ⚠ Caution: Do not provide two power supply sources at the same time for the device unless otherwise specified; it may result in device damage!

Environment

- Heavy stress, violent vibration or exposure to water is not allowed during transportation, storage and installation.
- Avoid aiming the camera directly towards extremely bright objects, such as, sun, as this may damage the image sensor.
- 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.
- Do not place the device in a damp, dusty extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Make sure that no reflective surface is too close to the camera lens. The IR light from the camera may reflect back into the lens, resulting in image blur.

Operation and Daily Maintenance

- There are no user-serviceable parts inside. Please contact the nearest service center if the product does not work properly.
- Please shut down the device and then unplug the power cable before you begin any maintenance work.
- ⚠ Warning: All the examination and repair work should be done by qualified personnel.
- Do not touch the CMOS sensor optic component. You can use a blower to clean the dust on the lens surface.
- Always use the dry soft cloth to clean the device. If there is too much dust, use a cloth cleaning (such as using cloth) may result in poor IR functionality and/or IR reflection.
- Dome cover is an optical device, please don't touch or wipe the cover surface directly during installation and use. For dust, use oil-free soft brush or hair dryer to remove it gently; for grease or finger print, use oil-free cotton cloth or paper soaked with detergent to wipe from the lens center outward. Change the cloth and wipe several times if it is not clean enough.

Privacy Protection

- When installing cameras in public areas, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range.
- As the device user or data controller, you might collect the personal data of others, such as face, car plate number, etc. As a result, you shall implement reasonable and necessary measures to protect the legitimate rights and interests of other people, avoiding data leakage, improper use, including but not limited to, setting up access control, providing clear and visible notice to inform people of the existence of the surveillance area, providing required contact information and so on.

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.
- Regularly change the passwords of your devices to ensure that only authorized users can access the system (recommended time is 90 days).
- 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.

RoHS

The products have been 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	Network Connection	2
2.1	APP Connection.....	2
2.2	Wired Network Connection	3
2.2.1	Access through IP-Tool	3
2.2.2	Wi-Fi Connection	6
2.2.3	WAN.....	7
3	Configuration via APP.....	9
3.1	Live View via APP	9
3.2	Receive/Reject a Call or Open the Door via APP	9
3.3	Remote Playback via APP	10
3.4	Disable Push Notifications via APP	11
3.5	Device Settings via APP	11
3.6	Unbind the Doorbell from the APP	12
4	Live View via Web.....	13
5	Configuration via Web.....	15
5.1	Face Detection Settings	15
5.2	People Management	16
5.3	Access Control System Settings	17
5.4	Door Lock Settings	18
5.5	Door Contact Settings	19
5.6	Wiegand Settings	20
5.7	Tampering Alarm Settings	20
5.8	System Settings	21
5.8.1	Basic Information	21
5.8.2	Date and Time	21
5.8.3	Local Config	22
5.8.4	Storage	23
5.9	Image Configuration	25
5.9.1	Display Configuration	25
5.9.2	Video / Audio Configuration	27
5.9.3	OSD Configuration	29
5.9.4	White Light Control	29
5.10	Alarm Configuration	30
5.10.1	Video Exception Detection	30
5.10.2	Alarm In	31
5.11	Network Configuration	32
5.11.1	TCP/IP	32

5.11.2 Port.....	33
5.11.3 Server Configuration.....	33
5.11.4 Onvif.....	34
5.11.5 DDNS.....	35
5.11.6 802.1x.....	36
5.11.7 RTSP.....	36
5.11.8 UPnP.....	37
5.11.9 Email.....	38
5.11.10 FTP.....	39
5.11.11 HTTPS.....	39
5.11.12 P2P.....	40
5.11.13 QoS.....	41
5.11.14 Wi-Fi Settings.....	41
5.12 Security Configuration.....	42
5.12.1 User Configuration.....	42
5.12.2 Online User.....	44
5.12.3 Block and Allow Lists.....	45
5.12.4 Security Management.....	45
5.13 Maintenance Configuration.....	46
5.13.1 Backup and Restore.....	46
5.13.2 Reboot.....	47
5.13.3 Upgrade.....	47
5.13.4 Operation Log.....	47
6 Search.....	49
6.1 Image Search.....	49
6.2 Video Search.....	51
6.2.1 Local Video Search.....	51
6.2.2 SD Card Video Search.....	52
Appendix.....	54
Appendix 1 Troubleshooting.....	54

1 Introduction

Main Features

- Max. resolution: 2MP (1920×1080)
- Wide field of view achieving doorway security monitoring
- Access control function
- Noise suppression and echo cancellation
- Visual intercom function: two-way remote communication between the doorbell and mobile APP
- Support door opening by swiping card or mobile APP
- Support IR and white LED lights
- Support tampering alarm and door contact alarm
- 2.4G Wi-Fi
- Built-in micro SD card slot, up to 256GB
- Intelligent Analysis: video exception detection, face detection, face capture, etc.

2 Network Connection

2.1 APP Connection

- ① Enable Wi-Fi network of your phone. Then scan the QR Code of the APP in the QSG (Quick Start Guide) or open your phone's APP store and search "Superlive Plus". Then install the mobile APP (Superlive Plus) in your phone.
- ② Run the mobile APP and then log in your account of the APP (if you don't register, please register and log in first). Then enter the server list interface of the APP.
- ③ Power on your video doorbell. Then tap "Add Device" in the server list interface of the APP. Scan the QR Code attached on the back of the video doorbell or the QR Code of the video doorbell in the QSG. After that, go to the Wi-Fi configuration interface by tapping "Add". When the indicator of the doorbell is blue, check "Confirmed that..." and tap "Next Step".



- ④ Enter the key (or password) of the Wi-Fi network. Tap "Next Step". Then join the Wi-Fi network by tapping "Join" as shown below. After that, the doorbell will be automatically added to the server list.



Note: 1. When configuring the Wi-Fi network via the APP, (a). **DO NOT** connect the network cable to the Ethernet connector of the device; (b). your mobile phone must be connected to the Wi-Fi network; (c). the doorbell must be within the mobile phone signal covering area. **DO NOT** move your phone too far away with the doorbell.

2. After the Wi-Fi of the doorbell is successfully connected, you can use Wi-Fi or mobile web in your mobile phone as needed. However, if you want to remotely view the doorbell video via mobile web, please make sure the wireless router/AP connected the doorbell has been connected to the Ethernet.

2.2 Wired Network Connection

Here we take device access via Web browser for example.

Web browser: IE (plug-in required)/ Firefox/Edge/Safari/Google Chrome

It is recommended to use the latest version of these web browsers.

The menu display and operation of the camera may be slightly different by using the browser with plug-in or without plug-in. Installing plug-in will display more functions of the camera. Connect IP-Cam via LAN or WAN. Here only take IE browser for example. The details are as follows:

2.2.1 Access through IP-Tool

Network connection:



① Make sure the PC and device are connected to the same 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:



If there are many devices, please find your device via its MAC address.

③ Double click the IP address and then the system will pop up the IE browser to connect IP-CAM. After you read the privacy statement, check and click "Already Read". Then activate the device.

Device Activation

User Name

admin

☐ Activate Onvif User

New Password

8-16 characters; Numbers, special characters, upper case letters and lower case letters must be included.

Confirm Password

OK

Please self-define the password of admin according to the tip.

If "Activate Onvif User" is enabled, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use the default username and the password set above to connect.

After that, follow directions to download, install and run the Active X control if prompted.

Re-connect your camera via IE browser and then a login box will appear.

A login form with four input fields: 'Name' with 'admin', 'Password' with masked characters, 'Stream Type' with '1920x1080 25fps', and 'Language' with 'English'. Each field has a dropdown arrow on the right. Below the fields is a link 'Forget Password?' and a blue 'Login' button.

Name:	admin
Password:	*****
Stream Type:	1920x1080 25fps
Language:	English
Forget Password?	
Login	

Please enter the user name (admin) and password. Then select the stream type and language as needed.

The security questions must be set after you click "Login" button. It is very important for you to reset your password. Please remember these answers.

A form titled 'Safety Question' with three sections. Each section has a 'Security Question' dropdown and an 'Answer' text field. The questions are 'Your father's name?', 'Your mother's name?', and 'Your primary school name?'. There is a 'Go' button at the bottom.

Safety Question	
Security Question1	Your father's name?
Answer	
Security Question2	Your mother's name?
Answer	
Security Question3	Your primary school name?
Answer	
Go	

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page. Then you can reset the password by the security questions and answers you set.

You can set the account security question during the activation, or you can go to Config→Security→User, click **Safety Question**, select the security questions and input your answers.

After that, you can add your device to the APP. The steps are as follows:

- 1) Scan the QR Code of the APP in the QSG (Quick Start Guide) or open your phone's APP store and search "Superlive Plus". Then install the mobile APP (Superlive Plus) in your phone.
- 2) Run the mobile APP and then log in your account of the APP (if you don't register, please register and log in first). Then enter the server list interface of the APP.
- 3) Tap "Add Device" in the server list interface of the APP. Scan the QR Code (log in via

web and then go to Config→ Basic Information interface) to directly add the device to the server list of the APP.

2.2.2 Wi-Fi Connection



- ① Use the network cable to connect the device 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 device via its MAC address. 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 2.2.1 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.

LAN	
☐	Obtain an IP address automatically
☒	Use the following IP address
IP Address	192.168.1.201
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Preferred DNS Server	192.168.1.1
Alternate DNS Server	8.8.8.8

- 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.
- After that, you can also use the downloaded APP to scan the QR code of the device to directly add it to the server list of the APP.

2.2.3 WAN



To remotely access the device via Web, the setting steps are as follows:

- 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.

HTTP Port	80
HTTPS Port	443
Data Port	9008
RTSP Port	554

Port Setup

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

☐ Obtain an IP address automatically
☒ Use the following IP address

IP Address:
 Subnet Mask:
 Gateway:
 Preferred DNS Server:
 Alternate DNS Server:

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".

Port Range						
Application	Start	End	Protocol	IP Address	Enable	
1	9007	to 9008	Both	192.168.1.201	☐	
2	80	to 81	Both	192.168.1.201	☐	
3	10000	to 10001	Both	192.168.1.166	☐	
4	21000	to 21001	Both	192.168.1.166	☐	

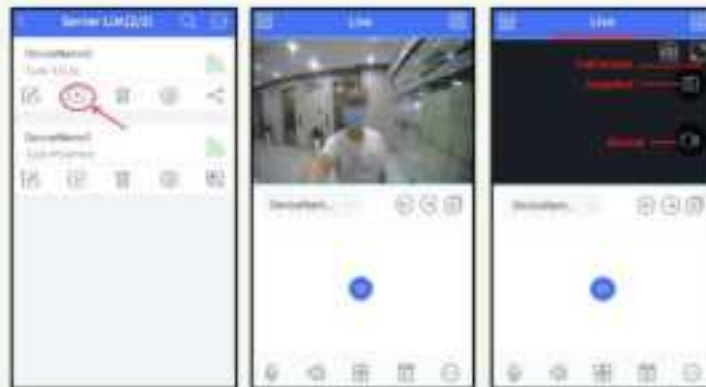
Router Setup

- 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 "192.168.1.201:81" in the address bar of web browser to access).

3 Configuration via APP

3.1 Live View via APP

After the device is added to the APP, tap  in the server list interface to view the video.



Tap the video and then multiple icons will be displayed. You can do the above-mentioned operations as needed (like take a snapshot, record, switch definition).

Note: You can add the device to the APP by directly scanning the QR Code of the device, or connect the device to the Ethernet via the wired/wireless network connection first and then scan the QR Code of the device to add it via the APP.

3.2 Receive/Reject a Call or Open the Door via APP

You can receive or reject a call when the APP window is opened or closed.

1. When the APP is opened,



Press the Call button of the doorbell, and then a calling interface will be shown in the APP. Now, you can answer or hang up the call, or choose to remotely open the door as needed.

2. When the APP is closed.



Press the Call button of the doorbell, and then a message will pop up on the top of the page. Tap this message within 60s to enter to the calling interface.

Note: You must enable the notification function of the APP in your phone first, or no message will be received.

3.3 Remote Playback via APP

You can remotely play back the recorded files stored on the SD card via the APP. In the live view interface of the APP, select the video doorbell channel and then tap  to remotely play back the video. You can select the playback time on the timescale.



In the remote playback interface, tap  to select the detailed date and time as needed.

3.4 Disable Push Notifications via APP

If you don't want to receive the doorbell information, you can disable the relevant push notifications via APP.



Tap **Main Menu**→**Push Setting**. Select the doorbell channel name to enter. Disabling "Message Subscription" will turn off all intelligent alarm notifications of the device. You can also disable one more items listed on the interface as needed.

3.5 Device Settings via APP

In the server list interface, tap  under the doorbell name. This will take you to the device information interface as shown below:



In the device information page, you can view basic information, SD card information, Wi-Fi information of the device. There is also an option to enable or disable "Dismantle Alarm" (Tampering alarm).

Note: If your SD card has been used in other devices before it is inserted in this device, you need to format it first.

3.6 Unbind the Doorbell from the APP

In the server list interface of the APP, tap  under the video doorbell name to unbind it.



Note that the device also can be unbound from the APP via Web (Config→System→Basic Information). See [Basic Information](#) section for details.

4 Live View via Web

After logging in, the following window will be shown.



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		Tampering alarm indicator
	Enable/disable audio		Alarm input indicator
	Snapshot		Face detection indicator
	Start/stop local recording		Face Detection

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

* Plug-in free live view: the local recording is not supported and the preview mode switch (real-time/balanced/fluent mode) is not available too.

➤ **Face Detection View**

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



5 Configuration via Web

In the Webcam client, choose "Config" to go to the configuration interface.

Note: Wherever applicable, click the "Save" button to save the settings.

5.1 Face Detection Settings

Face detection function is to detect the face appearing in the surveillance scene. Alarms will be triggered when a face is detected.

Go to the face detection configuration interface via Web Client to set the face detection parameters.

1. Go to Config→Face Detection→ Detection Config interface.

Detection Config	Area	Advanced	Schedule
State: Working			
☒ Enable			
Alarm Holding Time: 20 Seconds			
☐ Trigger SD Card Snapshot			
☒ Trigger SD Recording			
☐ Trigger Email			
☐ Trigger FTP			
Save			

2. Enable the face detection.

3. Set alarm holding time and alarm trigger options.

Trigger SD Card Snapshot: If selected, the system will capture images and save the images on an SD card once a face is detected.

Trigger SD Card Recording: If selected, video will be recorded on an SD card once a face is detected.

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 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).

5. Advanced settings.

Deduplication Period: In the set period, delete the repeated detection results.

Snapshot Number: If the snapshot number is enabled and set (eg. 3) and the deduplication period is set to "5 seconds", the camera will capture the same target once every 5 seconds and it will capture this target 3 times at most during its continuous tracking period. If the snapshot number is disabled, the camera will capture the same target once every 5 seconds until the target disappears in the detected area.

6. Set the schedule of the face detection. The setup steps of the schedule are the same as schedule recording setup (See [Schedule Recording](#)).

5.2 People Management

Please log in to the video doorbell via Web client and then Click "Config"→"People Management" tab.

There are two ways to add personnel information.

① Adding personal information one by one

Click  to pop up an adding user box. After that, fill out the relevant information and click "Entry" to add.

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

Note: Please swipe the card on the device when adding the user information and then the ID number will be automatically filled in.

② Adding the information of many people at a time

Click and then add the information of many people once according to the prompted rules.

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

After the personal information is added, you can search them by name, gender, ID number and so on.

Index	ID NO.	Name	Gender	Type	Card NO.	Operate
1	80472	Jane	Female	Allow list	0037146216	<button>Modify</button> <button>Delete</button>
2	123	Mr	Male	Allow list	0000123	<button>Modify</button> <button>Delete</button>

Click "Modify" to change people information and click "Delete" to delete the personal information.

Note: Face pictures are not supported in the face database.

5.3 Access Control System Settings

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

Config Custom Voice

Select Voice English(EN) ▼

Volume 100

Select Voice: Select the language of the voice prompt.

Volume: Set the volume of the voice prompt.

● 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.

Config Custom Voice

Voice List

Custom Voice Custom Voice ▼

Audio List Ring Card ▼ Listen Listen

Upload Audio

Select Voice Ring Road Control ▼

Upload Path Browse

Audio Name Ring Card Upload

Tip: audio format (WAV, 32000Hz, mono, 8000, less than 3000)

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.

5.4 Door Lock Settings

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

Config

Unlocking Group Visitor (including All) ▼

Unlocking Delay Time 2

Unlocking Duration 5

Save

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 "Swiping Card" and the delay time is set to "2" seconds; the door will be opened 2 seconds later after successfully reading card.

Unlocking Duration: If the door has been unlocked for a period that exceeds the unlocking duration, the door will be automatically locked. The time range is from 0 to 10 seconds. For example, the duration is set to "3" seconds; the unlocking door will be automatically locked 3 seconds later.

5.5 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. (The value ranges from 0~999. If "0" is selected, it means that alarms will be triggered immediately.)

Please select the alarm trigger options as needed.

Trigger Audio Alarm: if enabled, you will hear the warning sound when the door contact alarm is triggered.

The setup steps of other alarm trigger options are similar to the face detection settings. Please refer to face detection settings chapter for details.

5.6 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.

5.7 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 doorbell is removed or damaged by the external force.

The setup steps of other alarm trigger options are similar to the face detection settings. Please refer to face detection settings chapter for details.

5.8 System Settings

5.8.1 Basic Information

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

Device Name	IPC
Product Model	
Brand	Customer
Software Version	5.1.1.0132290
Software Build Date	2022-05-23
Client version	21.12
OCX version	2.2.1.8
MAC	0018aa0009d3c
Device ID	E8D8806C2879
Binding state	Bound(11374440314)
About this machine	View
Privacy Statement	View



In the above interface, you can unbind the device from the account of the APP. Click “Unbind” to unbind the device.

5.8.2 Date and Time

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

Date and Time	
Zone	(GMT+08:00) London, London, Reykjavik
DST	
☒ Auto DST ☐ Manual DST	
Start Time	January 01, 2021 00:00:00
End Time	February 01, 2021 00:00:00
Time Offset	0:00:00

Select the time zone and DST as required.

Note: The time zone of the camera and the computer must be the same. It is recommended to modify the time zone of the camera according to the time zone of the computer. If the time zone of the computer is modified, the current web client needs to be closed. Then re-open it and log in again.

Click the "Date and Time" tab to set the time mode and time format.

5.8.3 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, "Local smart snapshot storage" can be enabled or disabled here. If enabled, the captured pictures triggered by smart events will be saved to the local PC.

Rendering Mode: High-efficient mode, compatible mode or low-efficient mode can be optional.

If the performance of your computer is not compatible with the IE client or your computer has no graphics card, low-efficient mode is suggested.

Note: when you access your camera by the web browser without the plug-in, only Show Bitrate can be set in the above interface.

5.8.4 Storage

Go to Config→System→Storage to go to the interface as shown below.

Management	Eject	Format
Total picture capacity	128 MB	
Picture remaining space	128 MB	
Total recording capacity	128 MB	
Record remaining time	128 MB	
State	Normal	
Snapshot Quota	50 %	
Video Quota	50 %	

Changes in the quota ratio need to be formatted before they become effective.

● SD Card Management

Click the “Format” button to format the SD card. All data will be cleared by clicking this button.

Click the “Eject” button to stop writing data to SD card. Then the SD card can be ejected safely.

Snapshot Quota: Set the capacity proportion of captured pictures on the SD card.

Video Quota: Set the capacity proportion of record files on the SD card.

● Schedule Recording Settings

1. Go to Config→System→Storage→Record to go to the interface as shown below.

Record Parameters
Record Stream
Pre Record Time
Cycle Write

Timing

☐ Enable Schedule Record

2. Set record stream, pre-record time, cycle writing.

Pre Record Time: Set the time to record before the actual recording begins.

3. Set schedule recording. Check “Enable Schedule Record” and set the schedule.

Weekly schedule

Set the alarm time from Monday to Sunday for a single week. Each day is divided in one hour increments. Green means scheduled. Blank means unscheduled.

“Add”: Add the schedule for a special day. Drag the mouse to set the time on the timeline.

“Erase”: Delete the schedule. Drag the mouse to erase the time on the timeline.

Manual Input: Click it for a specific day to enter specific start and end times. This adds more granularities (minutes).

Day schedule

Set the alarm time for alarm a special day, such as a holiday.

Note: Holiday schedule takes priority over weekly schedule.

- **Snapshot Settings**

Go to Config→System→Storage→Snapshot to go to the interface as shown below.

Management: Record Snapshot	
Snapshot Parameters	
Image Format	JPEG
Resolution	704x576
Image Quality	Low
Event Trigger	
Snapshot Interval	1 Second
Snapshot Quantity	5
Timing	
☒ Enable Timing Snapshot	
Snapshot Interval	5 Second

Set the format, resolution and quality of the image saved on the SD card and the snapshot interval and quantity and the timing snapshot here.

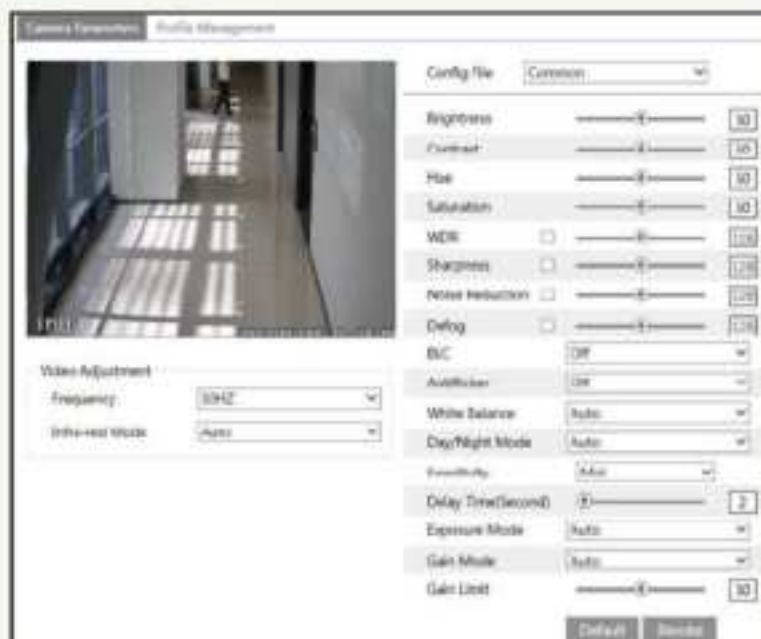
Snapshot Quantity: The number you set here is the maximum quantity of snapshots. The actual quantity of snapshots may be less than this number. Supposing the occurrence time of an alarm event is less than the time of capturing pictures, the actual quantity of snapshots is less than the set quantity of snapshots.

Timing Snapshot: Enable timing snapshot first and then set the snapshot interval and schedule. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).

5.9 Image Configuration

5.9.1 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.

Day/Night Mode: Choose "Auto", "Day", "Night" or "Timing".

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 (within the set gain limit value) 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.

Frequency: 50Hz and 60Hz can be optional.

Infra-red Mode: Choose "Auto", "ON" or "OFF".

Note: For some items, if selected/enabled, the camera will reboot automatically. After that, clicking "Default" button will not take effect.

Schedule Settings of Image Parameters:

Click the "Profile Management" 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.

5.9.2 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.

The screenshot shows a configuration window with a 'Video' tab selected. It contains a table for configuring two video streams. Below the table are checkboxes for 'Send Snapshot (Only primary)', 'Video encode slice split', and 'Watermark (H.264, H.265)', along with a text field for 'Watermark content'.

Index	Stream	Resolution	Frame	Bitrate	Bitrate (Kbps)	Video	I-Frame	Video	Profile
1	Main stream	1080x1920	25	VBR	2000	High	10	1024	High Profile
2	Sub stream	720x1280	25	VBR	1024	High	10	1024	High Profile

Send Snapshot (Only primary) ☐ Size (194K/30s)

☐ Video encode slice split

☐ Watermark (H.264, H.265) Watermark content:

OK

Two 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, H.264+, H.264, H.265, H.265+ can be optional. MJPEG is not available for main stream. 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.



The Audio Configuration interface has two tabs: 'Audio' and 'Audio'. The 'Audio' tab is active. It contains three settings: 'Enable' with a checked checkbox, 'Audio Encoding' set to 'G711A' in a dropdown menu, and 'Audio Type' set to 'MIC' in a dropdown menu. A 'Save' button is located at the bottom right.

Audio Encoding: G711A and G711U are selectable.

Audio Type: MIC.

5.9.3 OSD Configuration

Go to Image→OSD interface as shown below.



The OSD Configuration interface features a video preview window on the left showing a hallway. On the right, there are four settings: 'Data Format' set to 'H264 H265', 'Show Timestamp' with a checked checkbox, 'Device Name' set to 'IPC', and 'Show Device Name' with an unchecked checkbox. A 'Save' button is at the bottom right.

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.

5.9.4 White Light Control

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



The White Light Control Configuration interface has two tabs: 'Config' and 'Config'. The 'Config' tab is active. It contains two settings: 'White Light Mode' set to 'Auto' in a dropdown menu, and 'Duration Time' set to '2 Minutes' in a dropdown menu. A 'Save' button is at the bottom right.

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.

5.10 Alarm Configuration

5.10.1 Video Exception Detection

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

To set exception detection:

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

The screenshot shows a configuration window titled "Detection Config" with a "Sensitivity" tab. It contains several settings: "Scene Change Detection" (checked), "Video Blur Detection" (checked), "Video Cast Detection" (checked), "Alarm Holding Time" (set to 20 Seconds), and several unchecked options: "Trigger Audio Alarm", "Trigger SD Card Snapshot", "Trigger SD Recording", "Trigger Email", and "Trigger FTP". A "Save" button is at the bottom right.

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 image is abnormal caused by color deviation.

2. Set the alarm holding time.
3. Set alarm trigger options.

Trigger Audio Alarm: If selected, you will hear the warning sound when the video exception happens.

Trigger SD Card Snapshot: If selected, the system will capture images on video exception detection and save the images on an SD card.

Trigger SD Card Recording: If selected, video will be recorded on an SD card on video

exception detection.

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 the sensitivity of the exception detection. Drag the slider to set the sensitivity value or directly enter the sensitivity value in the textbox.

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 color shift of the image.

5. Click "Save" button to save the settings.

5.10.2 Alarm In

To set sensor alarm (alarm in):

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

The screenshot shows the 'Detection Config' window with two tabs: 'Detection Config' (active) and 'Schedule'. The 'Detection Config' tab contains the following settings:

- ☒ Enable
- Alarm Type: NO (dropdown menu)
- Alarm Holding Time: 10 Seconds (input field with a minus button)
- Sensor Name: (empty text box)
- ☐ Trigger Audio Alarm
- ☐ Trigger SD Card Snapshot
- ☐ Trigger SD Recording
- ☐ Trigger Email
- ☐ Trigger FTP
- Save button (bottom right)

1. Click "Enable" and set the alarm type, alarm holding time and sensor name.
2. Set alarm trigger options. The setup steps are the same as the alarm trigger settings of video exception.
3. Set the schedule of the sensor alarm. The setup steps of schedule are the same as the schedule recording (See [Schedule Recording](#)).
4. Click "Save" button to save the settings.

5.11 Network Configuration

5.11.1 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.

5.11.2 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.

Persistent Connection Port: The port is used for a persistent connection of the third-party platform to push smart data, like face pictures.

WebSocket Port: Communication protocol port for plug-in free preview.

5.11.3 Server Configuration

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

☒ Enable	
Server Port	2009
Server Address	
Device ID	1
Save	

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.

5.11.4 Onvif

The camera can be searched and connected to the third-party platform via ONVIF/RTSP protocol.

If "Activate Onvif User" is enabled in the device activation interface, the ONVIF user can be activated simultaneously. When you connect the camera through the ONVIF protocol in the third-party platform, you can use this onvif user to connect.

You can also add new users in the Onvif interface.

The screenshot shows a web interface for Onvif user management. At the top, there are tabs for 'Users', 'Groups', and 'Devices'. The 'Users' tab is selected. Below the tabs, there is a table with columns 'Index', 'User Name', and 'User Type'. An 'Add User' button is located above the table. A red circle highlights the 'Add User' button, and a red arrow points to it. The 'Add User' dialog box is open, showing fields for 'User Name', 'Password', 'Confirm Password', and 'User Type'. A note states: 'The password can be composed of numbers, special characters, upper or lower case letters.' The 'OK' and 'Cancel' buttons are at the bottom of the dialog.

Note: when adding the device to the third-party platform with ONVIF/RTSP protocol, please

use the onvif user in the above interface.

5.11.5 DDNS

If the camera is set up with a DHCP connection, DDNS should be set for the internet.

1. Go to Config→Network→DDNS.

Enable ☒

Server Type: www.dyndns.com

User Name:

Password:

Domain:

Save

2. Apply for a domain name. Take www.dvrdynds.com for example.

Enter www.dvrdynds.com in the IE address bar to visit its website. Then Click the "Registration" button.

NEW USER REGISTRATION

Username:

Password:

Password Confirmation:

First Name:

Last Name:

Security Question:

Answer:

CAPTCHA:

Submit Reset

Create domain name:

www.dynds.com Request Domain

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.

5.11.6 802.1x

If it is enabled, the camera's data can be protected. When the camera is connected to the network protected by the IEEE802.1x, user authentication is needed.

☒ Enable	
Protocol Type	EAP_MD5
EAPOL Version	1
User Name	test
Password	*****
Confirm Password	*****

To use this function, the camera shall be connected to a switch supporting 802.1x protocol.

The switch can be reckoned as an authentication system to identify the device in a local network. If the camera connected to the network interface of the switch has passed the authentication of the switch, it can be accessed via the local network.

Protocol type and EAPOL version: Please use the default settings.

User name and password: The user name and password must be the same with the user name and password applied for and registered in the authentication server.

5.11.7 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".

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 supports local preview 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 preview 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 MPEG, the video may be disordered at some resolutions.

5.11.8 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.

☒ Enable
 UPrP Name:

5.11.9 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
 Sender Address:
 User Name: ☐ Anonymous Login
 Password:
 Server Address:
 Secure Connection: ☒
 SMTP Port: 25
☐ Send Interval(S): 60

Recipient

 Recipient Address:

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.

5.11.10 FTP

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

Go to Config→Network→FTP.

The screenshot shows the 'Add FTP' dialog box. The fields are as follows:

Field	Value
Server Name	
Server Address	
Upload Path	Example FTP Folder
Port	21
User Name	
Password	

Buttons: OK, Cancel, Help.

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.

5.11.11 HTTPS

HTTPs provides authentication of the web site and protects user privacy.

Go to Config → Network → HTTPS as shown below.



Certificate installed

Issued to: User1, CN=User1, OU=, O=, C=US, OU=Microsoft Windows, CN=Certificate
 Issued by: User1, CN=User1, OU=, O=, C=US, OU=Microsoft Windows, CN=Certificate
 Expiration date: 2014-12-25 00:00:00

Info

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.

5.11.12 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.

☒ P2P	Save
---	-------------------------------------

5.11.13 QoS

QoS (Quality of Service) function is used to provide different quality of services for different network applications. With the deficient bandwidth, the router or switch will sort the data streams and transfer them according to their priority to solve the network delay and network congestion by using this function.

Go to Config→Network→QoS.

Video/Audio DSCP	13
Alarm DSCP	35
Manager DSCP	53

Video/Audio DSCP: The range is from 0 to 63.

Alarm DSCP: The range is from 0 to 63.

Manager DSCP: The range is from 0 to 63.

Generally speaking, the larger the number is, the higher the priority is.

5.11.14 Wi-Fi Settings

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

Wi-Fi Networks

Index	SSID	Working Mode	Security Mode	Channel	Signal	Mbps	Connection
1	TP-LINK_8113	Manager	WPA2-personal	4	100	150	Connected

Wi-Fi:

SSID: TP-LINK_8113

Security Mode: WPA2-personal

Key 1: W

Encryption Type: AES

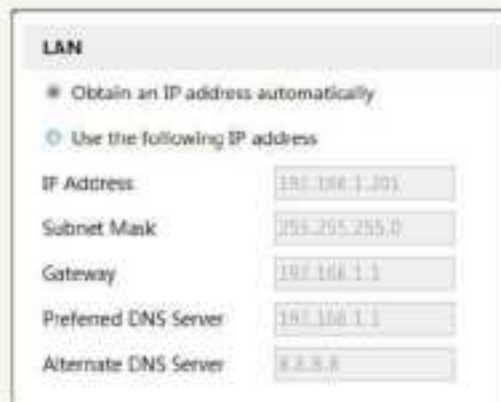
1. Checkmark "Enable" to enable Wi-Fi.

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".



LAN

☒ Obtain an IP address automatically

☐ Use the following IP address

IP Address:

Subnet Mask:

Gateway:

Preferred DNS Server:

Alternate DNS Server:

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/...

5.12 Security Configuration

5.12.1 User Configuration

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

Add Modify Delete			
Index	User Name	User Type	Binding MAC
1	admin	Administrator	

Add user:

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

2. Enter user name in the "User Name" textbox.
3. Enter the password in the "Password" and "Confirm Password" textbox. Please set the password according to the requirement of the password security level (Go to Config→Security→Security Management→Password Security interface to set the security level).
4. Choose the user type and select the desired user permissions.
5. 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 if necessary in the user configuration list box.
2. The "Edit user" dialog box pops up by clicking the "Modify" button.

Edit User

User Name:

Old Password:

New Password:

Level:

Confirm Password:

User Type:

SELECT ALL

- ☐ Remote storage settings
- ☐ Remote image settings
- ☐ Remote PTZ control
- ☐ Remote alarm server configuration
- ☐ Remote intelligent event configuration
- ☐ Remote network advanced configuration
- ☐ Remote security management

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. Select the user permissions for advanced or normal user.
6. Click the "OK" button to save the settings.

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.

Safety Question Settings: set the questions and answers for admin so as to reset the password after you forget the password.

5.12.2 Online User

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

ID	Client Address	Port	User Name	User Type	Push Button
1	192.168.1.132	55130	admin	Administrator	Push Button

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

5.12.3 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 and then enter IP address in the address box and click the "Add" button.

5.12.4 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 five times will make the login interface locked. The camera can be logged in again after a half hour or after the camera reboots.

Trigger Email: if enabled, e-mail will be sent when logging in/out or illegal login lock occurs.

● Password Security

Please set the password level and expiration time as needed.

Password Level: Weak, Medium or Strong.

Weak level: Numbers, special characters, upper or lower case letters can be used. You can choose one of them or any combination of them when setting the password.

Medium Level: 8~16 characters, including at least two of the following categories: numbers, special characters, upper case letters and lower case letters.

Strong Level: 8~16 characters. Numbers, special characters, upper case letters and lower case letters must be included.

For your account security, it is recommended to set a strong password and change your password regularly.

HTTP Authentication: Basic or Token is selectable.

The screenshot shows a web interface for 'Security Settings'. It has three tabs: 'Password Security' and 'Authentication'. The 'Authentication' tab is selected. Below the tabs, there is a label 'HTTP Authentication' followed by a dropdown menu currently set to 'Basic'. A 'Save' button is located at the bottom right of the form.

5.13 Maintenance Configuration

5.13.1 Backup and Restore

Go to Config→Maintenance→Backup & Restore.

The screenshot shows a web interface for 'Import Setting', 'Export Settings', and 'Default Settings'. The 'Import Setting' section has a 'Path' input field with a 'Browse' button and an 'Import Setting' button. The 'Export Settings' section has an 'Export Settings' button. The 'Default Settings' section has a 'Keep' label and three checkboxes: 'Network Config', 'Security Configuration', and 'Image Configuration'. A 'Load Default' button is at the bottom.

Configuration settings of the camera can be exported from 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.

Note: The login password needs to be entered after clicking the "Import Setting" button.

• Default Settings

Click the "Load Default" button and then verify the password to restore all system settings to the default factory settings except those you want to keep.

5.13.2 Reboot

Go to Config→Maintenance→Reboot.

Click the "Reboot" button and then enter the password 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, click the "Save" button and then enter the password to save the settings.

5.13.3 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. Enter the correct password and then the device will restart automatically

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

5.13.4 Operation Log

To query and export log:

1. Go to Config→Maintenance→Operation Log.

Main Type:	All log	Sub Type:	All log		
Start Time:	2015-07-14 00:00:00	End Time:	2015-07-14 23:59:59	Search	Export
Index	Time	Main Type	Sub Type	User Name	Login IP
1	2015-07-14 11:11:38	Operation	Log in	admin	192.168.1.13
2	2015-07-14 11:12:02	Exception	Disconnected		192.168.1.13
3	2015-07-14 15:12:17	Exception	Disconnected		192.168.1.12

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.

6 Search

6.1 Image Search

Click **Search** to go to the interface as shown below. Images that are saved on the SD card can be found here.

Note: When using the plug-in free browser, the local images cannot be searched.



● Local Image Search

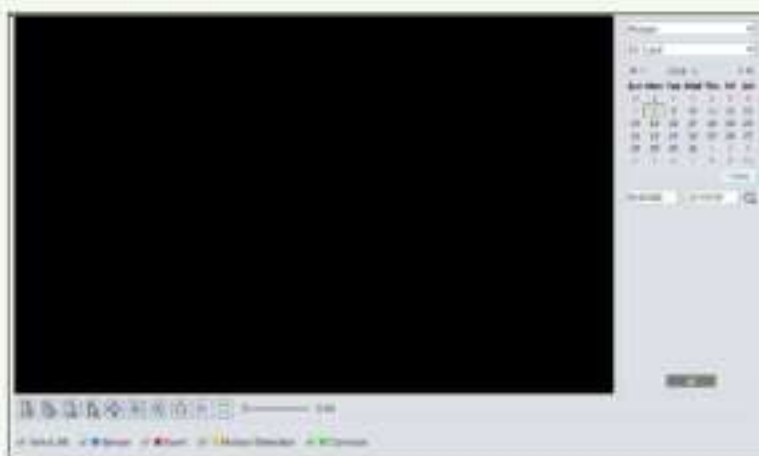
1. Choose "Picture"—"Local".
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.



Click  to return to the previous interface.

● SD Card Image Search

1. Choose "Picture"—"SD Card".



2. Set time: Select date and choose the start and end time.
 3. Choose the alarm events at the bottom of the interface.
 4. Click  to search the images.
 5. Double click a file name in the list to view the captured photos.
- 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.
	Save: Click this button to select the path for saving the image on the PC.		Save all: Click this button to select the path for saving all pictures on the PC.
	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.
	Play speed: Play speed of the slide show.		

6.2 Video Search

6.2.1 Local 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.

Note: When using the plug-in free browser, the local videos cannot be searched.



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.

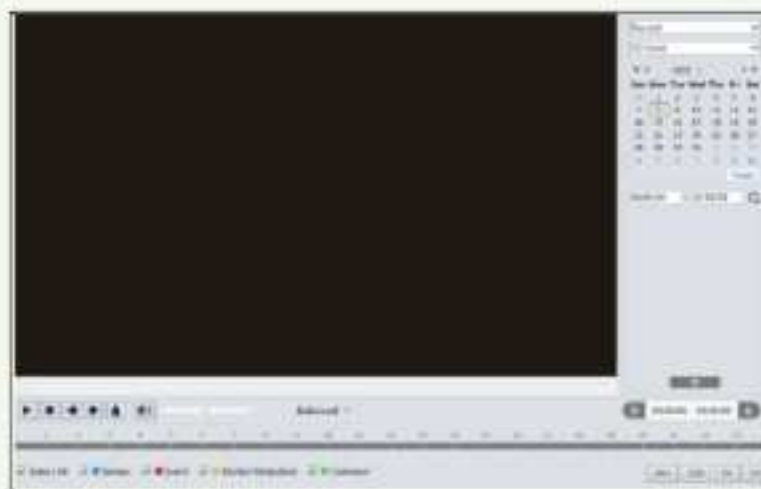


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

6.2.2 SD Card Video Search

Click Search to go to the interface as shown below. Videos that were recorded on the SD card can be played in this interface.

1. Choose "Record"—"SD Card".
2. Set search time: Select the date and choose the start and end time.
3. Click  to search the images.



4. Select the alarm events at the bottom of the interface.
5. Select mix stream (video and audio stream) or video stream as needed.
6. Double click on a file name in the list to start playback.



Note: ⏮ and ⏭ cannot be displayed in the above interface via the plug-in free browser. Additionally, for plug-in free playback, playback mode switch (balanced/real-time/fluent mode) and downloading functions are not supported too.

The time table can be shown in 24H/12H/2H/1H format by clicking the corresponding buttons.

Video clip and downloading

1. Search the video files according to the above mentioned steps.
2. Select the start time by clicking on the time table.
3. Click ⏮ to set the start time and then this button turns blue (⏮).
4. Select the end time by clicking on the time table. Then click ⏭ to set the end time.
5. Click ⏴ to download the video file in the PC.

Index	Process	Record	Start Time	End Time	Path	Operate
1	100%	Yes	2020-11-01 11:11:11	2020-11-01 11:11:11	\\192.168.1.100\111111	⏮ ⏭ ⏴ ⏵

Set up: D:\Favorites Close List Close

Click "Set up" to set the storage directory of the video files.

Click "Open" to play the video.

Click "Clear List" to clear the downloading list.

Click "Close" to close the downloading window.

Appendix

Appendix 1 Troubleshooting

How to find the password?

A: The password for *admin* can be reset through "Edit Safety Question" function.

Click "Forget Password" in the login window and then enter the corresponding answer of the selected question in the popup window. After you correctly answer all questions, you can reset the password for *admin*. If you forget the answer of the question, this way will be invalid, please contact your dealer for help.

B: The passwords of other users can be reset by *admin*.

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.

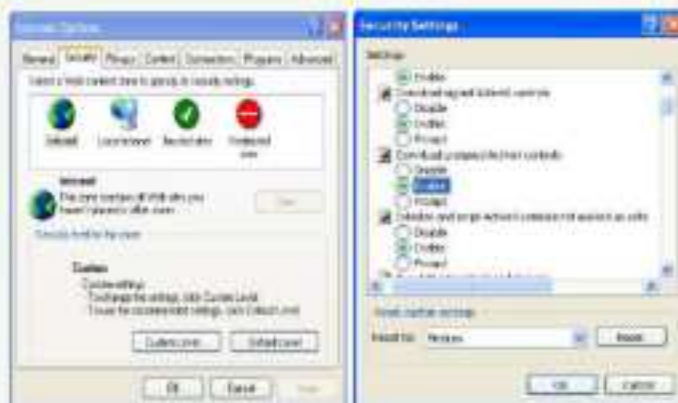


② Select Security-----Custom Level....

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.

How to modify IP address through IP-Tool?

A: After you install the IP-Tool, run it as shown below.



The default IP address of this camera is DHCP. 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.



Modify Network Parameter

Mac Address 08:00:20:11:35:77

IP Address 192.168.1.201

Subnet Mask 255.255.255.0

Gateway 192.168.1.1

•••••• Modify

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 "admin" which is set in the device activation interface in advance and then click the "Modify" button to change the network parameters.