

Temperature Measurement & Face Recognition Terminal Art. IPTHPAN02FA

Please read this manual thoroughly before use and keep it for future reference

www.comelitgroup.com

The logo for Comelit, featuring a green stylized 'C' icon followed by the word 'Comelit' in a bold, sans-serif font. Below the company name, the tagline 'Passion. Technology. Design.' is written in a smaller, lighter font.

Comelit®
Passion. Technology. Design.

Via Don Arrigoni, 5 - 24020 Rovetta (BG) - Italy

- 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 device; 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. The ownerships of trademarks, logos and other intellectual properties related to Microsoft, Apple and Google belong to the above-mentioned companies.
- This manual is suitable for face recognition network devices.

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.

Regulatory Information

FCC Information

1. FCC compliance

The products have been tested and found in compliance with the council FCC rules and regulations part 15 subpart B. These limits are designed to provide reasonable protection against harmful interference. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. The user will be required to correct the interface at his own expense in case the harmful interference occurs.

2. FCC conditions:

Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE Information



The products have been manufactured to comply with the following directives. EMC Directive 2014/30/EU

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	LAN	2
2.1.1	Access through IP-Tool	2
2.1.2	Directly Access through IE	4
2.2	WAN	5
3	Temperature Measurement & Face Recognition Configuration	9
3.1	Temperature Measurement Settings	9
3.2	Face Match Configuration	10
3.3	Face Database Management	11
3.4	Mask Detection	12
4	Live View	14
4.1	Temperature Measurement & Face Recognition View	14
4.1.1	Temperature Measurement Requirements	14
4.1.2	Temperature Measurement & Face Recognition View	15
4.2	Live View via Web	16
5	Access Control Settings	19
5.1	Door Lock Settings	19
5.2	Wiegand Settings	19
5.3	Tampering Alarm Settings	20
6	Other Configurations	21
6.1	System Settings	21
6.1.1	Basic Information	21
6.1.2	Date and Time	21
6.1.3	Local Config	22
6.1.4	Storage	22
6.2	Image Configuration	25
6.2.1	Display Configuration	25
6.2.2	Video / Audio Configuration	27
6.2.3	OSD Configuration	28
6.2.4	Screen Brightness	29
6.2.5	White Light Control	29
6.2.6	Face Exposure	30
6.3	Alarm Configuration	30
6.3.1	Exception	30
6.3.2	Micro-SD card Full	32
6.3.3	Micro-SD card Error	32
6.3.4	IP Address Conflict	33

6.3.5	Cable Disconnection	33
6.3.6	Alarm In	33
6.3.7	Alarm Out	34
6.4	Network Configuration	35
6.4.1	TCP/IP	35
6.4.2	Port	37
6.4.3	Server Configuration	37
6.4.4	DDNS	37
6.4.5	RTSP	39
6.4.6	UPnP	40
6.4.7	Email	40
6.4.8	FTP	41
6.4.9	HTTPS	41
6.5	Security Configuration	43
6.5.1	User Configuration	43
6.5.2	Online User	45
6.5.3	Block and Allow Lists	45
6.5.4	Security Management	45
6.6	Maintenance Configuration	46
6.6.1	Backup and Restore	46
6.6.2	Reboot	47
6.6.3	Upgrade	47
6.6.4	Operation Log	48
7	Search	49
7.1	Image Search	49
7.2	Video Search	51
7.2.1	Local Video Search	51
7.2.2	Micro-SD card Video Search	52
8	Face Match Result Search	55
	Appendix Troubleshooting	56

1 Introduction

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

Main Features

- 8 inch LCD screen
- High-accuracy IR wrist temperature measurement
- Non-contact body temperature measurement
- Human-sounding voice prompt
- Real-time face mask detection
- 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

2 Network

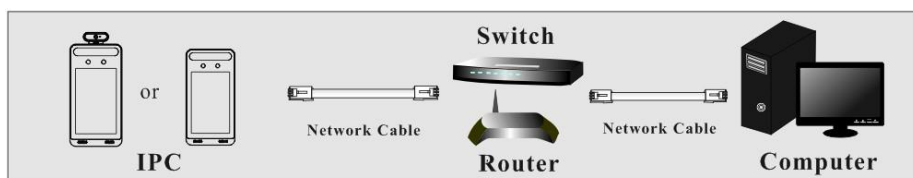
Connect IP-Cam via LAN or WAN. The details are as follows:

1.1 LAN

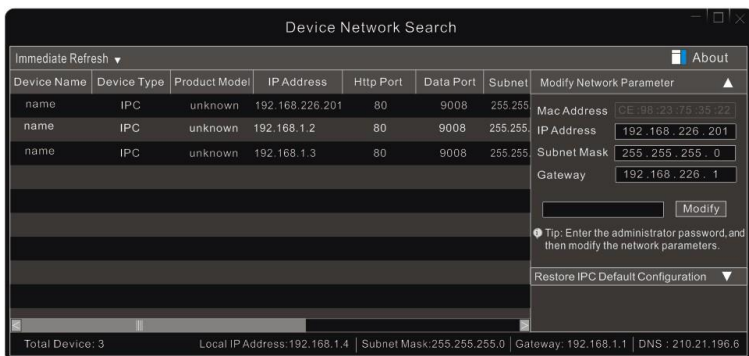
In LAN, there are two ways to access: 1. access through IP-Tool; 2. directly access through Internet Explorer browser.

1.1.1 Access through IP-Tool

Network connection:



- ① Make sure the PC and the device are connected to the LAN and the IP-Tool is installed in the PC.
- 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 **192.168.1.150**. 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

IP Address

Subnet Mask

Gateway

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 **admin**.

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.

Comelit

Name:

Password:

Stream Type: ▼

Language: ▼

☐ Remember me

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



The **default Username** is **admin**; the **default Password** is **admin**.

Please change the default password X

☐ Modify Password

New Password

Confirm Password

☐ Do not show again

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.

1.1.2 Directly Access through Internet Explorer

The default network settings are as shown

below: IP address: **192.168.1.150**

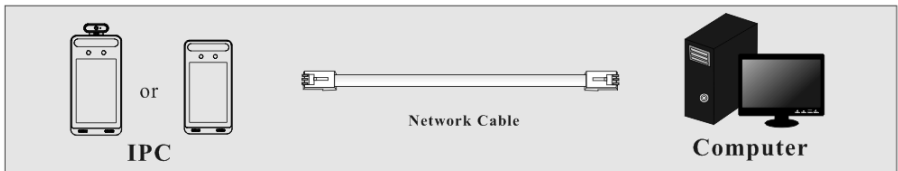
Subnet Mask: **255.255.255.0**

Gateway: **192.168.226.1**

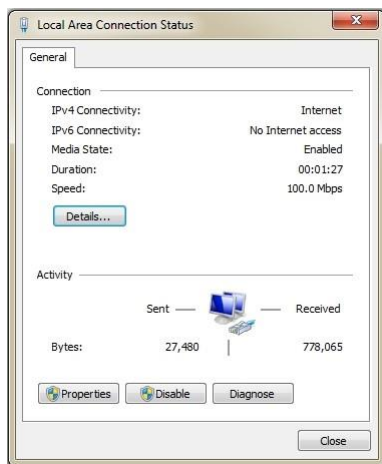
HTTP: **80**

Data port: **9008**

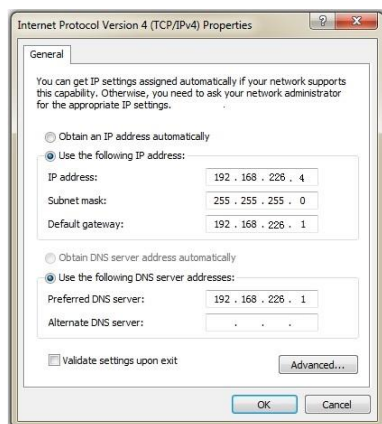
Use the above default settings when logging in the camera for the first time. Directly connect the camera to the computer through network cable.



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.



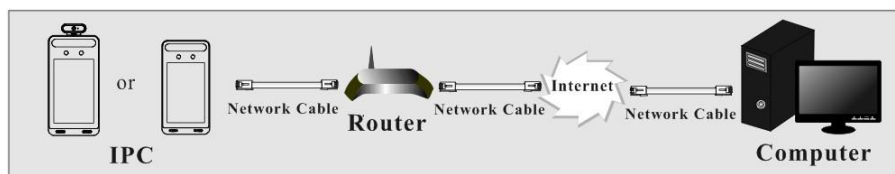
Select “Properties” and then select internet protocol according to the actual situation (for example: IPv4). Next, click the “Properties” button to set the network of the PC.



- 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.

1.2 WAN

- Access through the router or virtual server



- ① Make sure the camera is connected to the local network 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.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☐ Obtain an IP address automatically			
☒ Use the following IP address			
IP Address	192.168.1.150	Test	
Subnet Mask	255.255.255.0		
Gateway	192.168.1.1		
Preferred DNS Server	8.8.8.8		
Alternate DNS Server	8.8.8.8		

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".

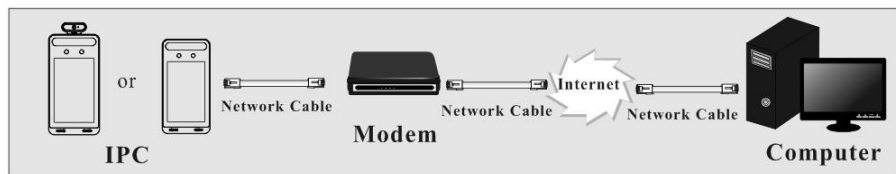
Port Range					
Application	Start	End	Protocol	IP Address	Enable
1	9007	to 9008	Both	192.168.1.201	☒
2	80	to 81	Both	192.168.1.201	☒
3	10000	to 10001	Both	192.168.1.166	☐
4	21000	to 21001	Both	192.168.1.166	☐

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 “192.198.1.150:81” 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 setup steps are as follow:

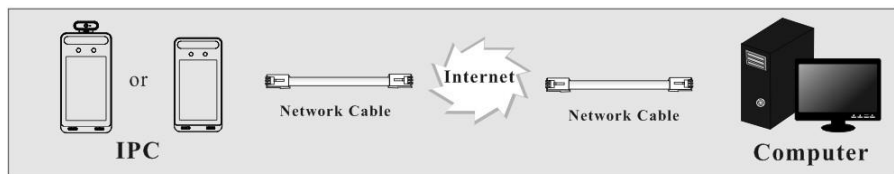
- ① Go to Config ▢ Network ▢ Port menu to set the port number.
- ② Go to Config ▢ Network ▢ TCP/IP ▢ PPPoE Config menu. Enable PPPoE and then enter the user name and password from your internet service provider.

IPv4	IPv6	PPPoE Config	IP Change Notification Config
☒ Enable			
User Name		xxxxxxxx	
Password		•••••	
Save			

- 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 setup 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.

3 Temp Measurement & Face Recognition Config

3.1 Temperature Measurement Settings

After the network is connected, go to the web client. Click Config□Temperature Measurement to go to the following interface.

The screenshot shows the 'Alarm Config' web interface. At the top, there is a tab labeled 'Alarm Config'. Below it, the 'Enable' checkbox is checked. A 'Temperature Switch' dropdown menu is set to '°F'. Two alarm thresholds are configured: 'High Temperature Alarm' at 99.0 (range 32.0-212.0)°F and 'Low Temperature Alarm' at 96.0 (range 32.0-212.0)°F. The 'Alarm Holding Time' is set to 20 Seconds. Under 'Trigger Alarm Out', there are checkboxes for 'Alarm Out 0' and 'Alarm Out 1', both of which are unchecked. Below this, there are five unchecked checkboxes for 'Trigger Audio Alarm', 'Trigger SD Snap', 'Trigger SD Recording', 'Trigger Email', and 'Trigger FTP'. A 'Save' button is located at the bottom right of the form.

1. Enable Temperature Measurement, select Celsius or Fahrenheit temperature as needed and then set the high temperature threshold and the low temperature threshold. When the wrist temperature measured is higher or lower than the set value, it will trigger alarms.
2. Set the alarm holding time.
3. Set the alarm trigger options.

Trigger Alarm Out: If enabled, the alarm output device will be triggered when detecting abnormal temperature.

Trigger Audio Alarm: If enabled, the system will broadcast the current wrist temperature detected. No matter whether the detected wrist temperature is normal or not, the corresponding voice prompt will be heard. If this item is disabled, the detected temperature will be not broadcasted.

Trigger SD Snap: If enabled, the system will capture images on detecting abnormal

temperature alarm and save the images on an Micro-SD card.

Trigger SD Recording: If selected, video will be recorded on an Micro-SD card on detecting abnormal temperature alarm.

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. Click “Save” to save the settings.

3.2 Face Match Configuration

The setting steps are as follows.

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

The screenshot shows the 'Face Match Configuration' interface. It has two tabs: 'Detection Config' and 'Comparison Config'. The 'Detection Config' tab is active. Inside this tab, there is a 'State' dropdown menu currently set to 'Working'. Below the state menu, there are two checkboxes, both of which are checked: 'Save Source Information' and 'Save Face Information'. Further down, there is a 'Holding Time' dropdown menu set to '3 Seconds'. At the bottom of the configuration area, there are four more checkboxes, all of which are unchecked: 'Trigger SD Snap', 'Trigger SD Recording', 'Trigger Email', and 'Trigger FTP'. A 'Save' button is located at the bottom right of the interface.

2. Enable “Save Source Information” or “Save Face Information”.

Save Source Information: if checked, the whole picture will be saved to the Micro-SD card when detecting a face.

Save Face Information: if checked, the captured face picture will be saved to the Micro-SD card when detecting a face.

Note: To save images to the local PC, please enable the local smart snapshot storage first (Config→System→Local Config). To save images to the Micro-SD card, please install an Micro-SD card first.

3. Set alarm holding time and alarm trigger options.

3. Set face comparison options.

Detection Config
Comparison Config

☒ Deduplication Period 4 Seconds ▾

Similarity threshold 75 %

☐ Send the face comparison data

☐ Alarm Out 1 ☐ Alarm Out 2

Save

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 (check the box Alarm Out 1, Alarm Out 2).

3.3 Face Database Management

Click “Face Database Management” tab. This will enter the following interface.

Add
Batch Add

Block and Allow Lists

All Types

Gender

Name

ID number

Search

Delete

Index	Face	ID	Name	Gender	Type	ID number	Operate
Add User X List Type Stranger Name Gender Male Age Tel ID number Remark Entry							

There are four ways to add face pictures.

① Adding face pictures one by one

Click Add 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.

② Adding multiple face pictures at a time

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

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.

Block and Allow Lists

All Types

Gender

All Types

Name

ID number

Search

Update

Index	Face	ID	Name	Gender	Type	ID number	Operate
1		1546395331	#T1#S0#A23#	Female			Delete Modify
2		1546395330	#T0#S0#A20#	Female			Delete Modify
3		1546395329	#T2#S0#A21#	Female			Delete Modify
4		1546395328	T0#S1#A55#	Female			Delete Modify
5		1546395327	T2#S1#A31#	Male			Delete Modify

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

34 Mask Detection

Click ConfigAlarmMask Detection to go to the following interface.

Alarm Config

☒ Enable

Alarm Holding Time20 Seconds

Trigger Alarm Out

☐ Alarm Out 0

☐ Alarm Out 1

☒ Trigger Audio Alarm

☐ Trigger SD Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

- ① Enable “Mask Detection” as
- ② needed. Set the alarm holding
- ③ time.

Set the alarm trigger options.

Alarm Out: If enabled, alarm output will be triggered when the detected person doesn't wear a mask.

Trigger Audio Alarm: If enabled, the alarm voice will be heard when the detected person doesn't wear a mask.

The setup steps of other alarm trigger options are the same as temperature measurement settings. Please refer to temperature measurement settings chapter for details.

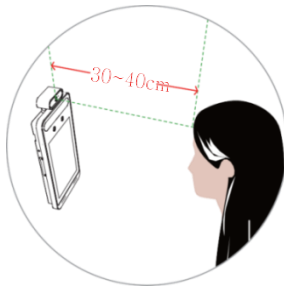
4 Live View

4.1 Temperature Measurement & Face Recognition View

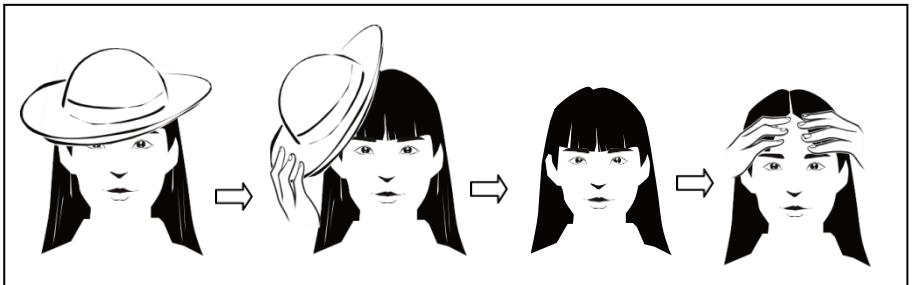
4.1.1 Temperature Measurement Requirements

Some recommendations:

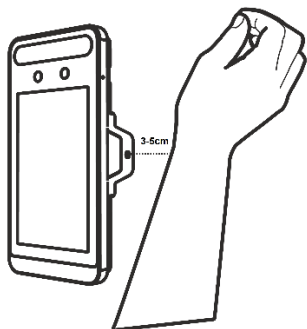
1. The face image of the detected person shall be within the pre-defined face detection area. The detected face shall be 30cm~40cm away from the temperature measurement sensor.



2. Please remove the hat/cap/helmet/hair covering the forehead.



3. The installation height shall fit the height of the detected people.
4. Raise your wrist and then make your inside wrist point at the temperature measurement sensor (3~5cm away from the sensor).



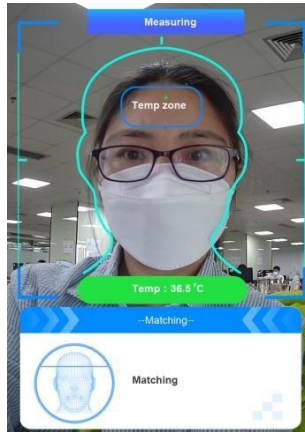
4.1.2 Temperature Measurement & Face Recognition View

After configuring temperature measurement and face match, the temperature and face match result can be viewed on the screen.

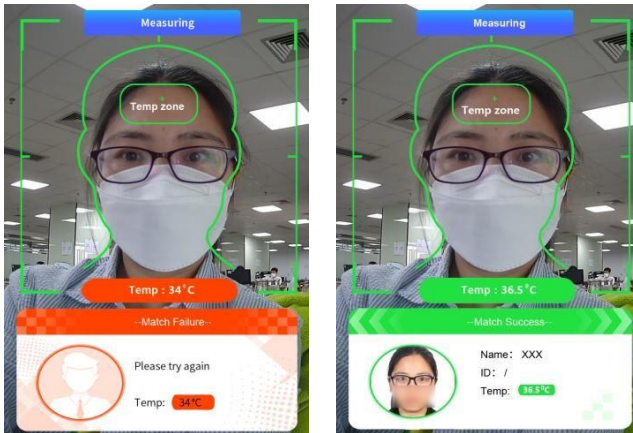
When detecting a face, the device will display the following interface.

Please measure the body temperature according to the above-mentioned temperature measurement requirements.

Abnormal temperature: the red block and temperature will be shown. Normal temperature: the green block and temperature will be shown. If "Trigger Alarm Audio" is selected, you will hear the alarm voice.



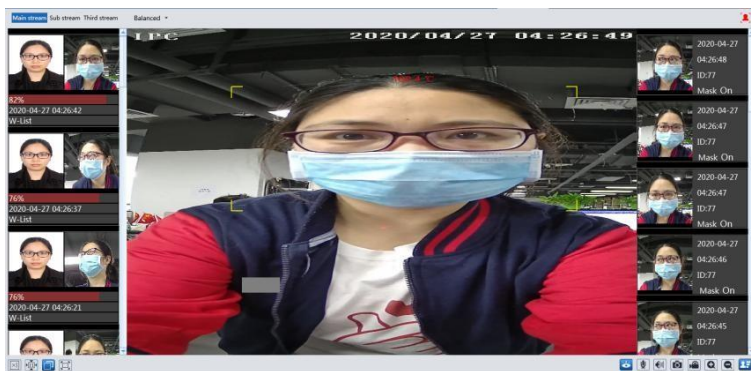
The system will measure the temperature and compare the captured face at the same time as shown below.



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. If the mask detection and “Trigger Audio Alarm” are selected, warning voice will be heard if no mask is detected.

4.2 Live View via Web

After logging in, the following window will be shown. In this interface you will see the captured face, match result and body temperature.



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

Icon	Description	Icon	Description
	Original size		Start/stop local recording
	Fit correct scale		Zoom in
	Auto (fill the window)		Zoom out
	Full screen		Micro-SD card recording indicator
	Start/stop live view		Sensor alarm indicator
	Start/stop two-way audio		Motion alarm indicator
	Enable/disable audio		Face detection indicator
	Snapshot		Face match

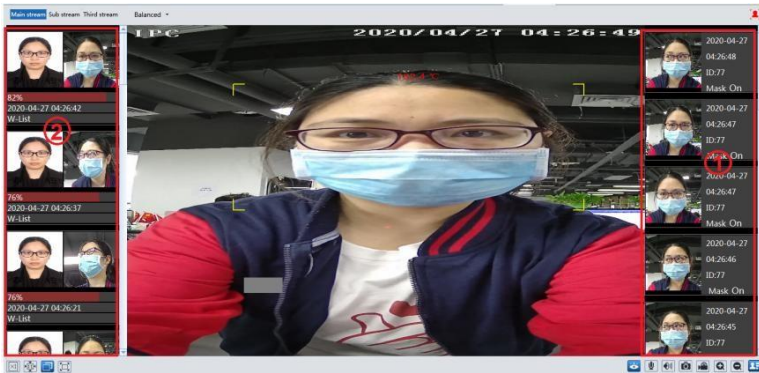
Those smart alarm indicators will flash only when the camera supports those functions and the corresponding events are enabled.

➤ 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.



Snap Picture



Picture library

ID 1583537377

Similarity 76%

Time 2020-04-14 18:03:02

List Type Allow list

Name XXXX

Gender Female

Age 0

Tel

ID Number

□ Add captured face pictures to the face database

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



Time 2020-04-14 10:03:04

ID 948

List Type

Name

Gender

Age

Tel

ID Number

Remark

Entry

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

5 Access Control Setting

5.1 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.

Config

Unlocking Mode

☐ By Face Recognition

☒ Normal Temperature

☒ Mask On

☒ By Password

Unlocking Delay Time

Unlocking Duration

Save

Unlocking Mode: three options--face recognition, normal temperature and mask. Please check as needed.

By Face Recognition: if the capture face picture is successfully matched, the door can be unlocked.

Normal Temperature: if the temperature of the person measured is normal, the door will be unlocked.

Mask On: if there is a mask on the face of the detected person, the door will be unlocked.

By Password: if the password is successfully matched, the door can be unlocked

Unlocking Delay Time: Set the door unlocking delay time. The time range is from 0 to 10 seconds. For example, "By Face Recognition" is selected 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, "By Face Recognition" is selected and the duration is set to "3" seconds; the unlocking door will be automatically locked 3 seconds later.

5.2 Wiegand Settings

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

Config

Alarm Trigger Mode

Wiegand Input
Wiegand Output
Off

☒ Alarm Out 0 ☐ Alarm Out 1

Save

Alarm Trigger Mode: 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”.

You can also select the alarm output as needed.

5.3 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.

Config

☒ Enable

Alarm Holding Time 20 Seconds

Trigger Alarm Out

☐ Alarm Out 0 ☐ Alarm Out 1

☐ Trigger SD Snap

☐ Trigger SD Recording

☐ Trigger Email

☐ Trigger FTP

Save

Enable “Tampering Alarm” and then set the alarm holding time and alarm trigger options. The setup steps of the alarm trigger options are the same as temperature measurement settings. Please refer to temperature measurement settings chapter for details.

6 Other Configurations

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.

Device Name	IPC
Product Model	IPCAMA02ZA
Brand	Comelet
Software Version	5.0.1.0(1911)
Software Build Date	2019-10-29
Kernel Version	20190906
Hardware Version	1.3
Onvif Version	19.06
Video Structured Version	1.1.7
Face Detection Version	1.1.25
OCX Version	2.0.7.3
MAC	00:18:ae:ad:b3:7a

Some versions may support device ID and QR code. If P2P is enabled (see Network Configuration-[P2P](#)), 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.

6.1.4 Storage

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

Management	Record	Snapshot
Total picture capacity	76 MB	
Picture remaining space	0 MB	
Total recording capacity	7488 MB	
Record remaining space	2048 MB	
State	Normal	
Snapshot Quota	1 %	
Video Quota	99 %	
Changes in the quota ratio need to be formatted before they become effective.		
Eject Format		

□ Micro-SD card Management

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

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

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

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

□ Schedule Recording Settings

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

Management	Record	Snapshot
Record Parameters		
Record Stream	Main stream	▼
Pre Record Time	No Pre Record	▼ (H264,H265,MJPEG)
Cycle Write	Yes	▼
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.

The screenshot displays a user interface for setting alarm schedules. It is divided into two main sections: 'Week Schedule' and 'Holiday Schedule'.

Week Schedule: This section allows setting alarm times for each day of the week (Sun. through Sat.). Each day's entry consists of a timeline from 0 to 24 hours. A green bar indicates a scheduled alarm period. For example, on Sunday, the alarm is scheduled from 00:00 to 24:00. Below each timeline, there is a 'Manual Input' button. At the top right of this section are 'Erase' and 'Add' buttons.

Holiday Schedule: This section is used for setting alarm times for specific holidays. It includes a 'Date' input field (currently showing '11-12'), an 'Add' button, and a 'Delete' button. Below this, there is another timeline from 0 to 24 hours with a green bar indicating a scheduled period from 00:00 to 24:00, and a 'Manual Input' button.

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 Micro-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](#)).

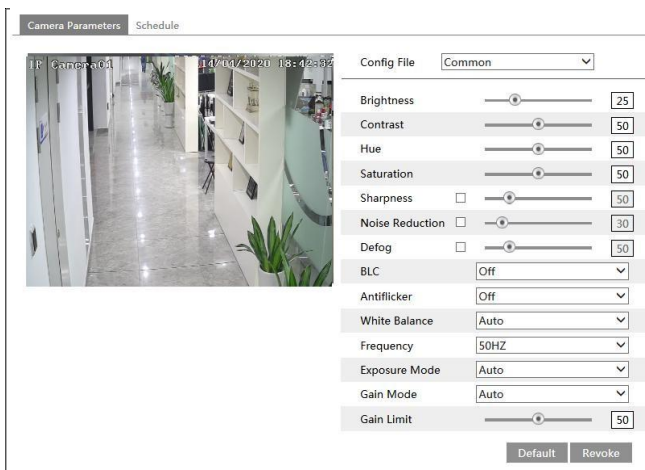
☐ **USB disk**

This function is only available for the model with USB interface. In this interface, you can view the state and capacity of the USB flash disk.

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 saturation.

Sharpness: Set 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.
- ☐ HWDR: WDR can adjust the camera to provide a better image when there are both very bright and very dark areas simultaneously in the field.

Recording will be stopped for a few seconds while the mode is changing from non-WDR to WDR 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.

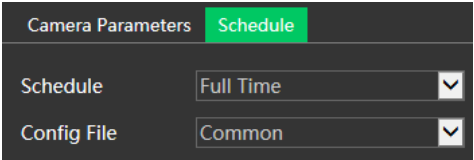
Frequency: 50Hz and 60Hz can be optional.

Exposure Mode: Choose "Auto" or "Manual". If manual is chosen, the digital shutter speed can be adjusted.

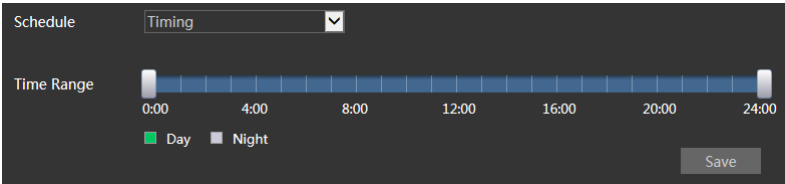
Gain Mode: Choose “Auto” or “Manual”. If “Auto” is selected, the gain value will be automatically adjusted according to the actual situation. If “Manual” is selected, the gain value shall be set manually. The higher the value is, the brighter the image is.

Schedule Settings of Image

Parameters: Click the “Schedule” tab as shown below.



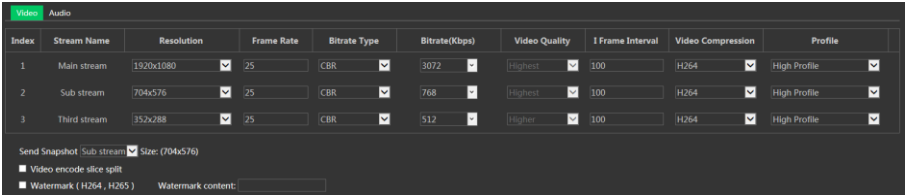
Set full time schedule for common, day, night mode and specified time schedule for day and night. Choose “Timing” in the drop-down box of schedule as shown below.



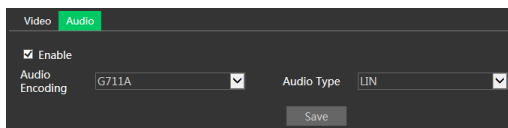
Drag “” icons to set the time of day and night. Blue means day time and blank means night time. If the current mode of camera parameters is set to schedule, the image configuration mode will automatically switch between day and night according to the schedule.

6.2.2 Video / Audio Configuration

Go to ImageVideo / 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.



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



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: How many snapshots to generate for an event.

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.

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 Overlay 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 Screen Brightness

Click Config Screen Brightness to go to the following interface.

In this interface, you can set the brightness of the screen of the terminal. The adjustable range is from 150 to 255.

6.2.5 White Light Control

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

Config

White Light Mode Manual

Brightness Of White Light 128

Save

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

6.2.6 Face Exposure

To enable and set face exposure, please go to Config□Image□Face Exposure interface.

Face Exposure ☒ 50

When the brightness of the captured face is not enough, it can be enabled.

6.3 Alarm Configuration

6.3.1 Exception

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

To set exception detection:

Go to Config□Event□Exception interface as shown below.

Detection Config
SD Card Full
SD Card Error
IP Address Collision
Cable Disconnected

☐ Scene change detection

☐ Video blur detection

☐ Video cast detection

Alarm Holding Time
20 Seconds

Sensitivity
50

Trigger Alarm Out
☐ Alarm Out 1
☐ Alarm Out 2

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.

Enable Video Color Cast Detection: Alarms will be triggered if the video becomes obscured.

2. Set the alarm holding time and alarm trigger options. The setup steps of alarm trigger options are the same as temperature measurement settings. Please refer to temperature measurement settings chapter for details.

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

4. Set the sensitivity of the exception detection. Click "Sensitivity" tab to go to the interface as shown below.

5.

Detection Config
Sensitivity

Sensitivity
50

Save

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 Color Cast Detection: The higher the value is, the more sensitive the system responds to the obscuring of the image.

6.3.2 Micro-SD card Full

1. Go to Config→Alarm→Anomaly→Micro-SD card Full.
- 2.

Detection ConfigSD Card FullSD Card ErrorIP Address CollisionCable Disconnected

☒ Enable

Alarm Holding Time20 Seconds

Trigger Alarm Out

☐ Alarm Out0☐ Alarm Out1

☐ Trigger Email

☐ Trigger FTP

3. Click “Enable” and set the alarm holding time.
4. Set alarm trigger options. The setup steps are the same as temperature measurement settings. Please refer to temperature measurement settings chapter for details.

6.3.3 Micro-SD card Error

When there are some errors in writing to the Micro-SD card, the corresponding alarms will be triggered.

1. Go to Config→Alarm→Anomaly→Micro-SD card Error as shown below.
- 2.

Detection ConfigSD Card FullSD Card ErrorIP Address CollisionCable Disconnected

☒ Enable

Alarm Holding Time20 Seconds

Trigger Alarm Out

☐ Alarm Out0☐ Alarm Out1

☐ Trigger Email

☐ Trigger FTP

3. Click “Enable” and set the alarm holding time.

4. Set alarm trigger options. Trigger alarm out, Email and FTP. The setup steps are the same as temperature measurement settings. Please refer to temperature measurement settings chapter for details.

6.3.4 IP Address Conflict

1. Go to Config☐Alarm☐Anomaly☐IP Address Collision as shown below.

The screenshot shows a configuration menu with tabs: Detection Config, SD Card Full, SD Card Error, IP Address Collision (selected), and Cable Disconnected. The IP Address Collision tab is active, displaying the following settings:
- **Enable:** A checkbox that is checked.
- **Alarm Holding Time:** A dropdown menu set to "20 Seconds".
- **Trigger Alarm Out:** A section containing two unchecked checkboxes: "Alarm Out0" and "Alarm Out1".
At the bottom of the configuration area is a "Save" button.

- 2. Click “Enable alarm” and set the alarm holding time.
- 3. Trigger alarm out. When the IP address of the camera is in conflict with the IP address of other devices, the system will trigger the alarm out.

6.3.5 Cable Disconnection

1. Go to Config☐Alarm☐Anomaly☐Cable Disconnected as shown below.

The screenshot shows a configuration menu with tabs: SD Card Full, SD Card Error, IP Address Collision, and Cable Disconnected (selected). The Cable Disconnected tab is active, displaying the following settings:
- **Enable:** A checkbox that is checked.
- **Alarm Holding Time:** A dropdown menu set to "20 Seconds".
- **Trigger Alarm Out:** A section containing one unchecked checkbox: "Alarm Out".
The interface has a dark theme.

- 2. Click “Enable” and set the alarm holding time.
- 3. Trigger alarm out. When the camera is disconnected, the system will trigger the alarm out.

6.3.6 Alarm In

To set sensor alarm (alarm in):
Go to Config☐Alarm☐Alarm In interface as shown below.

1. Select the sensor ID, 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 temperature measurement settings. Please refer to temperature measurement settings chapter for details.
 3. Click “Save” button to save the settings.
 4. Set the schedule of the sensor alarm. The setup steps of the schedule are the same as the schedule recording setup. (See [Schedule Recording](#)).
- Click “Apply settings to” to quickly apply the settings to the other alarm input.

6.3.7 Alarm Out

Go to Config □ Alarm □ Alarm Out.

Alarm Out ID: Select the alarm out ID.

Alarm Out Mode: Alarm linkage, manual operation, day/night switch linkage and timing are optional.

Alarm Linkage: Having selected this mode, select alarm out name, alarm holding time at the “Alarm Holding Time” pull down list box and alarm type.

Manual Operation: Having selected this mode, select the alarm type and click “Open” to trigger the alarm out immediately; click “Close” to stop alarm.

Alarm Out ID	Alarm Out0	▼
Alarm Out Mode	Manual Operation	▼
Alarm Type	NC	▼
Manual Operation	Open	Close
Save		

Day/Night Switch Linkage: Having selected this mode, select the alarm type and then choose to open or close alarm out when the camera switches to day mode or night mode.

Alarm Out ID	Alarm Out0	▼
Alarm Out Mode	Day/night switch linkage	▼
Alarm Type	NC	▼
Day	Close	▼
Night	Close	▼
Save		

Timing: Select the alarm type. Then click “Add” and drag the mouse on the timeline to set the schedule of alarm out; click “Erase” and drag the mouse on the timeline to erase the set time schedule. After this schedule is saved, the alarm out will be triggered in the specified time.

Alarm Out ID	Alarm Out0	▼
Alarm Out Mode	Timing	▼
Alarm Type	NC	▼
Time Range	☐ Erase ☒ Add 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Manual Input	
Save		

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 Port

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

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

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

HTTPS Port: The default HTTPSs 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.

6.4.3 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.

6.4.4 DDNS

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

1. Go to Config→Network→ DDNS.

The screenshot shows a web management interface with a top navigation bar containing the following tabs: Port, Server, DDNS (highlighted in green), SNMP, 802.1X, RTSP, UPnP, Email, FTP, HTTPS, P2P, and QoS. Below the navigation bar, the DDNS configuration section includes:

- An "Enable" checkbox that is checked.
- A "Server Type" dropdown menu currently displaying "www.comelitdns.com".
- A "User Name" text input field.
- A "Password" text input field.
- A "Domain" text input field.
- A "Save" button located at the bottom right of the configuration area.

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

6.4.5 RTSP

Go to Config□Network□RTSP.

☒ Enable

Port

554

Address

rtsp://IP or domain name:port/profile1

rtsp://IP or domain name:port/profile2

rtsp://IP or domain name:port/profile3

Multicast address

Main stream

239.0.0.0

50554

☐ Automatic start

Sub stream

239.0.0.1

51554

☐ Automatic start

Third stream

239.0.0.2

52554

☐ Automatic start

Audio

239.0.0.3

53554

☐ Automatic start

☐ Allow anonymous login (No username or password required)

Save

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 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.

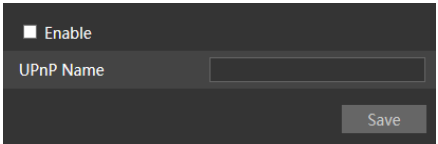
3. Avoid the use of the same multicast address in the same local network.

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 maybe disordered at some resolutions.

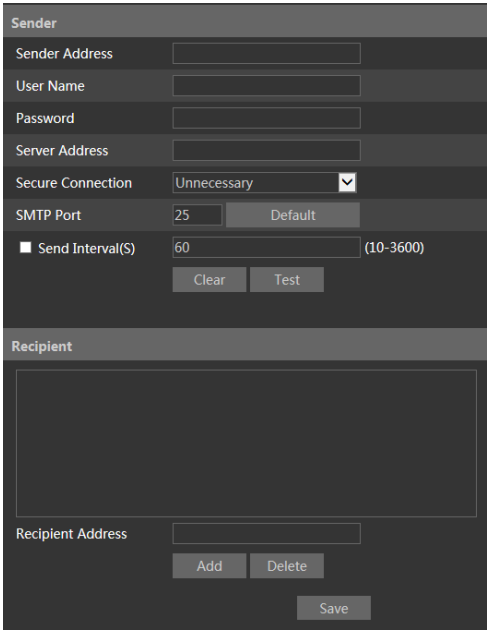
6.4.6 UPnP

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.

A screenshot of the UPnP configuration interface. It features a dark background with light-colored text and input fields. At the top, there is a checkbox labeled "Enable". Below it is a text input field labeled "UPnP Name". At the bottom right, there is a "Save" button.

6.4.7 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.

A screenshot of the Email configuration interface. It is divided into two main sections: "Sender" and "Recipient". The "Sender" section includes fields for "Sender Address", "User Name", "Password", and "Server Address". It also has a "Secure Connection" dropdown menu set to "Unnecessary", an "SMTP Port" field set to "25" with a "Default" button, and a "Send Interval(S)" field set to "60" with a range "(10-3600)" and "Clear" and "Test" buttons. The "Recipient" section features a large text area for email content, a "Recipient Address" field, and "Add", "Delete", and "Save" buttons.

Sender Address: sender’s e-mail address.

User name and password: sender’s user name and password.

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.

6.4.8 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	Server Address	Port	User Name	Upload Path
-------------	----------------	------	-----------	-------------

AddModifyDeleteTestSave

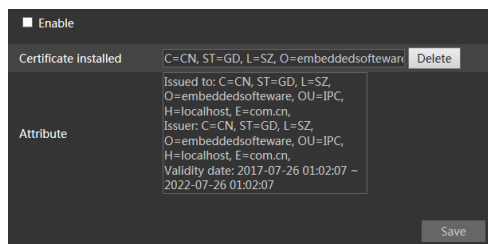
Server Name: The name of the FTP server.

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.

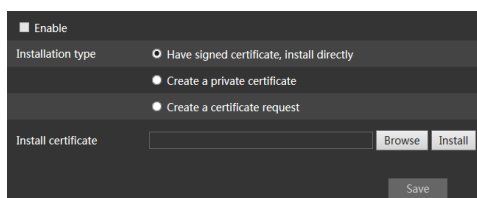
6.4.9 HTTPS

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://192.168.1.150:443).

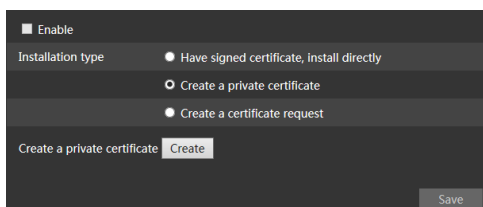
A private certificate can be created if users don't want to use the default one. Click "Delete" to cancel the default certificate. Then the following interface will be displayed.



* 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.

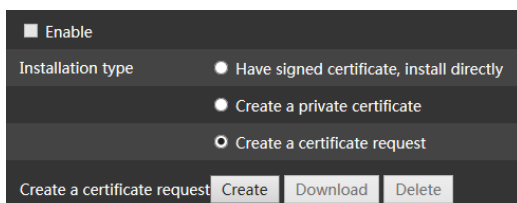
*



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.

6.5 Security Configuration

6.5.1 User Configuration

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

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

Add user:

1. Click the “Add” button to pop up the following textbox.
- 2.

Add User

User Name

Password

Level

The password can be composed of numbers, special characters, upper or lower case letters.

Confirm Password

User Type

Administrator

Bind MAC

00:00:00:00:00:00

OK

Cancel

3. Enter user name in “User Name” textbox.
4. 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).
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.
5. 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.
6. 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.
7. 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.

4. Enter the old password of the user in the “Old Password” text box.
5. Enter the new password in the “New password” and “Confirm Password” text box.
6. Enter computer’s MAC address as necessary.
7. 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.

Index	Client Address	Port	User Name	User Type	
1	172.25.150.98	18158	admin	Administrator	<button>Kick off</button>

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.

IP/MAC Address Filter Settings

☒ Enable address filtering

☐ Block the following address

☒ Allow the following address

Add

Delete

0.0.0.0

☐ IPv4 ☒ IPv6 ☐ MAC

Save

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.

Security Service Password Security

☒ Enable “locking once illegal login” function

Save

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.

□ Password Security

Security Service	Password Security
Password Level	Weak ▼
Expiration Time	Never ▼

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: 9~15 characters, including at least two of the following categories: numbers, special characters, upper case letters, lower case letters.

Strong Level: 9~15 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.

6.6 Maintenance Configuration

6.6.1 Backup and Restore

Go to Config□Maintenance□Backup & Restore.

The screenshot displays a settings menu with three main sections: 'Import Setting', 'Export Settings', and 'Default Settings'. The 'Import Setting' section includes a 'Path' field with a text input and a 'Sforgia...' button, followed by an 'Import Setting' button. The 'Export Settings' section contains an 'Export Settings' button. The 'Default Settings' section features a 'Keep' label, a list of three checkboxes ('Network Config', 'Security Configuration', and 'Image Configuration'), and a 'Load Default' button at the bottom.

□ **Import & Export Settings**

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.

□ **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.

Local upgrade

Path

Browse

Upgrade

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.
- 2.

Main Type	All log	☒	Sub Type	All log	☒		
Start Time	2019-11-12 00:00:00	☐	End Time	2019-11-12 23:59:59	☐	Search	Export
Index	Time		Main Type	Sub Type		User Name	Login IP
1	2019-11-12 17:40:00		Alarm				
2	2019-11-12 17:38:46		Operation	System config modify			
3	2019-11-12 17:36:46		Alarm				

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

7 Search

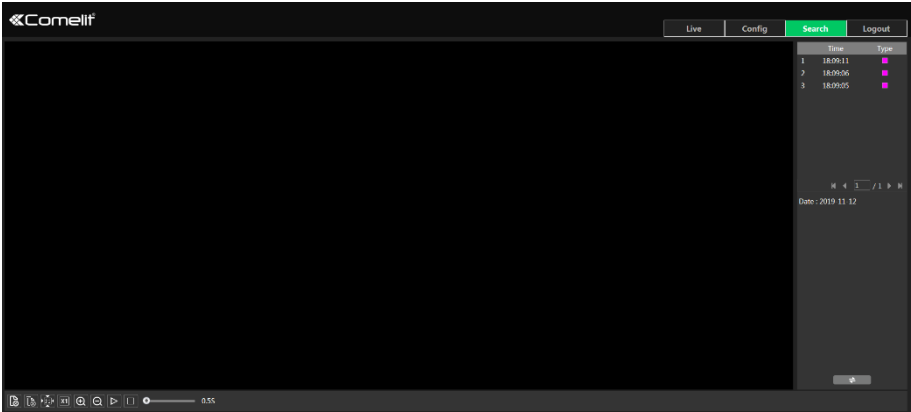
7.1 Image Search

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



□ Local Image Search

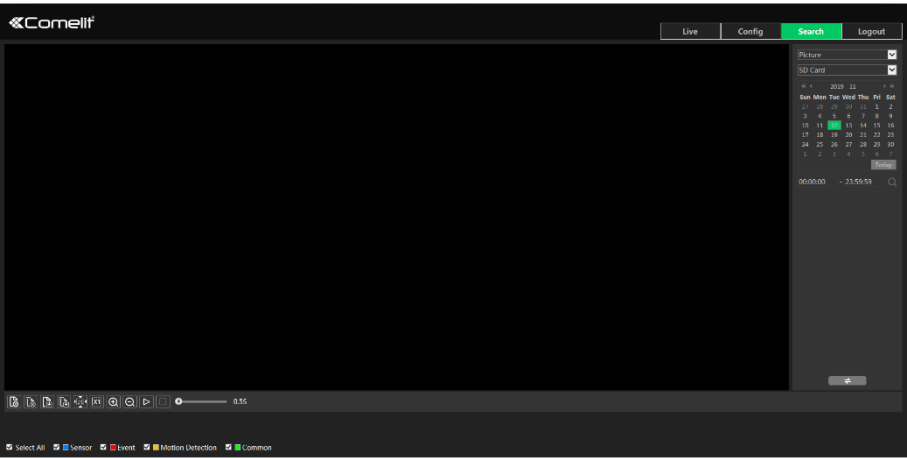
1. Choose “Picture”—“Local”.
2. Set time: Select date and choose the start and end time.
3. Click  to search the images.
4. Double click a file name in the list to view the captured photos as shown above.



Click  to return to the previous interface.

☐ Micro-SD card Image Search

1. Choose “Picture”—“Micro-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.

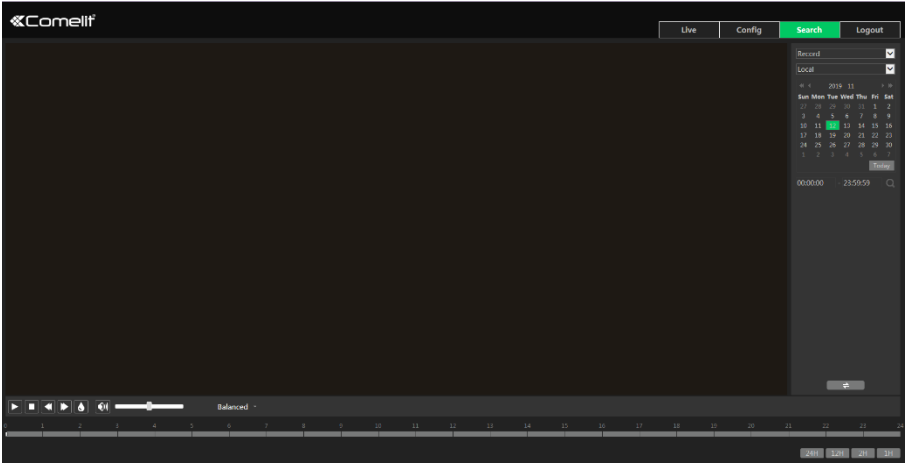
The descriptions of the buttons are shown as follows.

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.		

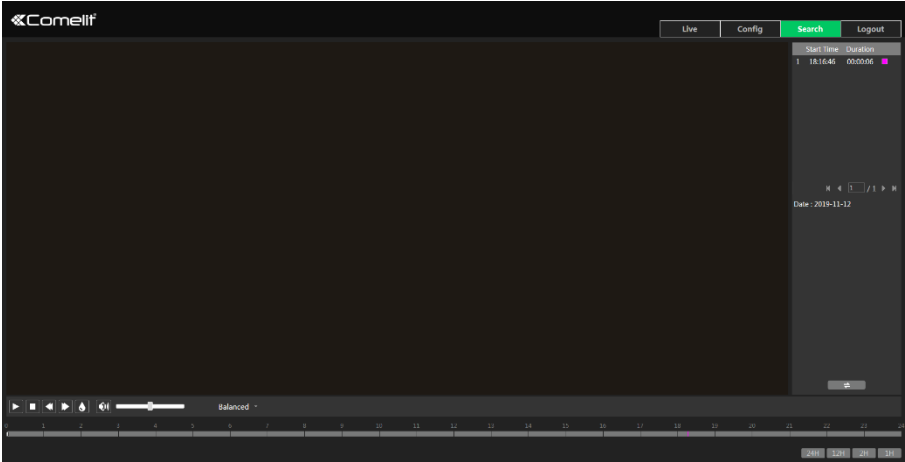
7.2 Video Search

7.2.1 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.



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.

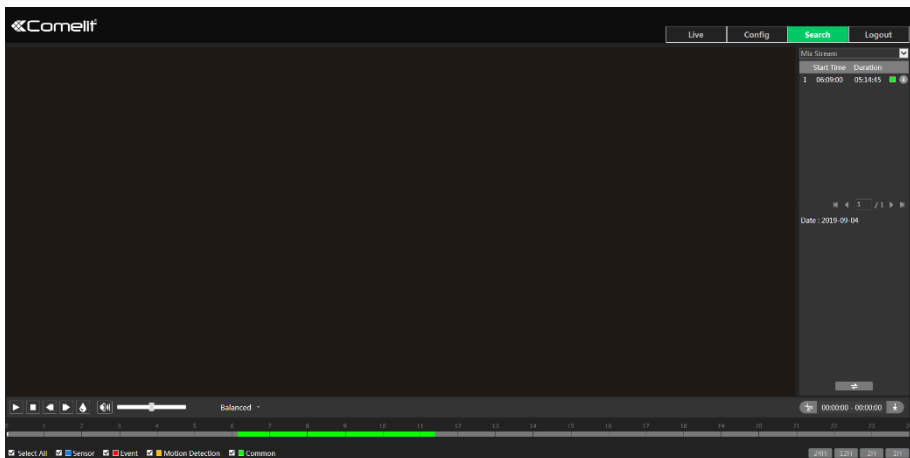


Icon	Description	Icon	Description
	Play button. After pausing the video, click this button to continue playing.		Pause button
	Stop button		Speed down
	Speed up		Watermark display
	Enable / disable audio; drag the slider to adjust the volume after enabling audio.		

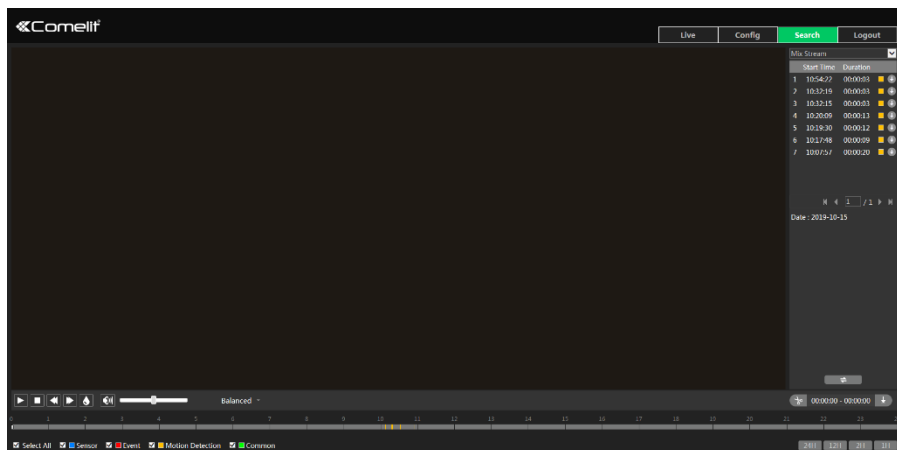
7.2.2 Micro-SD card Video Search

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

1. Choose “Record” — “Micro-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.



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 green (.
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.

8 Face Match Result Search

Click “Face Log” 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.



Appendix

Troubleshooting

Password forgot

A: Reset the device to the default factory settings.

Default IP: 192.168.1.150; Username: admin; Password: admin

Fail to connect devices through Internet Explorer browser.

A: Network is not well connected. Check the connection.

B: IP address is not available. Change 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 Comelit Advance IP Tool.

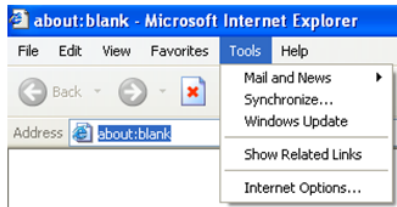
Comelit Advance IP tool cannot search devices.

The anti-virus software in your computer may cause it. Please stop it and try to search device again.

Internet Explorer cannot download ActiveX control.

A. Internet Explorer browser may be setup to block ActiveX. Follow the steps below.

① Open the browser and then click Tools → Internet Options.

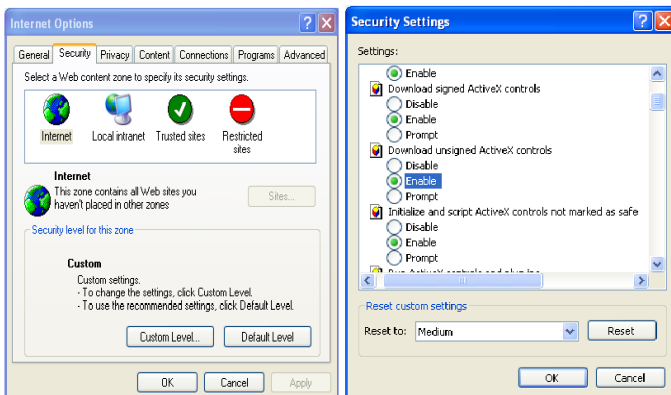


② Select Security → Custom Level....

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.

www.comelitgroup.com

Comelit
Passion. Technology. Design.