



# Thermal Temperature Monitoring Solution

## Quick Installation Guide

V1.0.2

Dahua Technology Co., Ltd

# Foreword




---

## General

This manual offers reference material and general information about the basic operation, maintenance, and troubleshooting for a Dahua Network Camera. Read, follow, and retain the following safety instructions. Heed all warning on the unit and in the operating instructions before operating the unit. Keep this guide for future reference.

## Safety Instructions

The following categorized signal words with defined meaning might appear in the Guide.

Signal Words	Meaning
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	January 2019
2	V1.0.1	Revised for North America	April 2020
3	V1.0.2	Feature Revision	May 2020

## Privacy Protection Notice

As the device user or data controller, you may collect personal data such as face images, fingerprints, license plate number, email address, phone number, GPS location and other sensitive or private information. You must ensure that your organization is in compliance with local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact

## About the Guide

- This user guide has been compiled with great care and the information it contains has been thoroughly reviewed and verified.
- The text was complete and correct at the time of printing. This guide may be periodically updated to reflect changes to the product or to correct previous information and the content of this guide can change without notice.
- If you encounter an error or have any questions regarding the contents of this guide, contact customer service for the latest documentation and supplementary information.
- Dahua accepts no liability for damage resulting directly or indirectly from faults, incompleteness, or discrepancies between this guide and the product described. Dahua is not liable for any loss caused by installation, operation, or maintenance inconsistent with the information in this guide.
- All the designs and software are subject to change without prior written notice. The product updates may cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- Video loss is inherent to all digital surveillance and recording devices; therefore Dahua cannot be held liable for any damage that results from missing video information. To minimize the occurrence of lost digital information, Dahua recommends multiple, redundant recording systems, and adoption of backup procedure for all data.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- Contact the supplier or customer service if you encounter any issue while using this unit.

## FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference;
- This device must accept any interference received, including interference that may cause undesired operation.

## FCC compliance :

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. 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. 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.

## Legal Notices

### **Copyright**

This user guide is ©2020, Dahua Technology Company, LTD.

This user guide is the intellectual property of Dahua Technology Company, LTD and is protected by copyright. All rights reserved.

### **Trademarks**

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

# Important Safeguards and Warnings

---

This chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it well for future reference.

## Installation and Maintenance Professionals Requirements

- All installation and maintenance professionals must have adequate qualifications or experiences to install and maintain CCTV systems and electric apparatus, and to work above the ground. The professionals must have the following knowledge and operation skills:
- Basic knowledge and installation of CCTV systems.
- Basic knowledge and operation skills of low voltage wiring and low voltage electronic circuit wire connection.
- Basic knowledge and operation skills of electric apparatus installation and maintenance in hazardous sites.

## Power Requirements

- Install the unit in accordance with the manufacturer's instructions and in accordance with applicable local codes.
- All installation and operation must conform to your local electrical safety codes.
- Do not overload outlets and extension cords, which may cause fire or electrical shock.
- Do not place the camera near or in a place where the camera may contact overhead power lines, power circuits, or electrical lights.
- Ensure power conforms to SELV (Safety Extra Low Voltage) and that the limited power source is rated AC 24V as specified in IEC60950-1. (Power supply requirement is subject to the device label).
- All input/output ports are SELV circuits. Ensure that SELV circuits are connected only to other SELV circuits.
- Ground the unit using the ground connection of the power supply to protect the unit from damage, especially in damp environments.
- Please install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Protect the plug and power cord from foot traffic, being pinched, and its exit from the unit.
- Do not attempt to service the unit. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified personnel.

- If the unit is damaged and requires service, unplug the unit from the main AC power supply and from the PoE supply and refer to qualified service personnel. Damage may include, but is not limited to:
  - The power supply cord or plug is damaged.
  - Liquid has spilled in or on the unit.
  - An object has fallen on the unit.
  - The unit has been dropped and the housing is damaged.
  - The unit displays a marked change in performance.
  - The unit does not operate in the expected manner when the user correctly follows the proper operating procedures.
- Ensure a service technician uses replacement parts specified by the manufacturer, or that have the same characteristics as the original parts. Unauthorized parts may cause fire, electrical shock, or other hazards. Dahua is not liable for any damage or harm caused by unauthorized modifications or repairs.
- Perform safety checks after completion of service or repairs to the unit.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Incorporate a readily accessible disconnect device in the building installation wiring for quick power disconnect to the camera.
- Dahua assumes no liability or responsibility for any fire or electrical shock caused by improper handling or installation.

## Application Environment Requirements

- Transport, use, and store the unit within the specified temperature and humidity range.
- Do not place the unit in a wet, dusty, extremely hot or an extremely cold environment; and avoid environments with strong electromagnetic radiation or unstable lighting.
- Do not use the device in the corrosive environment such as high salt fog area (sea, beach and coastal area), acid gas environment and chemical plants.
- Do not use the device in applications with strong vibrations such as in boats and vehicles.
- Never push objects of any kind into this unit through openings as they may touch dangerous voltage points or cause a short circuit that may result in fire or electrical shock. Take care to not spill any liquid on the unit.
- If your installation environment is subjected to one of the conditions above, contact our sales staff to purchase cameras intended for the particular environment.
- Do not install the device near the place with heat source, such as radiator, heater, stove or other heating equipment, which is to avoid fire.
- Do not aim the lens at an intense radiation source (such as the sun, a laser, and molten steel for example) to avoid damage to the thermal detector.
- Use the factory default package or material with equal quality to pack the device when transporting.

## Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the unit. This part of the unit is hot and may cause a burn.
- Do not open or dismantle the device; there are no components that a user can fix or replace. Opening the unit may cause water leakage or expose components to direct light. Contact the manufacturer or a qualified service representative to service the camera or to replace a component, including the desiccant.
- Dahua recommends the use of a thunder-proof device in concert with the unit.
- Do not touch the CCD or the CMOS optic sensor. Use a blower to clean dust or dirt on the lens surface. Use a dry cloth dampened with alcohol and gently wipe away any dust on the lens.
- Use a dry soft cloth to clean the unit's housing. If the unit is particularly dusty, use water to dilute a mild detergent, apply the diluted detergent to a soft cloth, then gently clean the device. Finally, use a dry cloth to wipe the unit dry. Do not use a volatile solvent like alcohol, benzene, or thinner; or use a strong detergent with abrasives, which may damage the surface coating or reduce the working performance of the unit.
- Do not touch or wipe a dome cover during installation, this cover is an optical device. Refer to the following methods clean the dome cover:
  - Stained with dirt: Use an oil-free soft brush or blower to gently remove the dirt.
  - Stained with grease or fingerprints: Use a soft cloth to wipe gently the water droplet or the oil from the dome cover. Then, use an oil-free cotton cloth or paper soaked with alcohol or detergent to clean the lens from the center of the dome to outside. Change the cloth several times to ensure the dome cover is clean.



### WARNING

- Modify the default password after login.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Internal and external ground connection should be stable.
- Do not supply power via the Ethernet connection (PoE) when power is supplied via the power connector.
- Disconnect power before device maintenance and overhaul. It is prohibited to open the cover with power on in an explosive environment.
- Contact the local dealer or the nearest service center if the device fails to work normally, do not dismantle or modify the device.

# Cybersecurity Recommendations

---

## Mandatory actions to take for increased cybersecurity

- **Change Passwords and Use Strong Passwords**
  - The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should consist of at least eight characters and a combination of special characters, numbers, and upper and lower case letters.
- **Update Firmware**
  - As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

## Recommendations to improve your network security

- **Change Passwords Regularly**
  - The length should be greater than 8 characters;
  - Include at least two types of characters; character types include upper and lower case letters, numbers, and symbols;
  - Do not use an account name or the account name in reverse order;
  - Do not use sequential characters, such as 123, abc, etc.;
  - Do not use repeated characters, such as 111, aaa, etc.;
- **Change Default HTTP and TCP Ports**
  - Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
  - These ports can be changed to any set of numbers between 1025 and 65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.
- **Update Firmware and Client Software**
  - Keep your network-enabled equipment (such as NVRs, DVRs, IP cameras, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
  - Download and use the latest version of client software.
- **Enable HTTPS/SSL**
  - Set up an SSL Certificate and enable HTTPS to encrypt all communication between your devices and recorder.
- **Enable IP Filter**
  - Enable the IP filter to prevent unauthorized access to the system.



- **Change ONVIF Password**
  - Older IP camera firmware does not automatically change the ONVIF password when the system credentials are changed. Update the camera's firmware to the latest revision or manually change the ONVIF password.
- **Forward Only Ports You Need**
  - Forward only the HTTP and TCP ports that are required. Do not forward a wide range of numbers to the device. Do not DMZ the device's IP address.
  - Do not forward any ports for individual cameras if they are all connected to a recorder on site. Simply forward the NVR port.
- **Disable Auto-Login on SmartPSS**
  - Disable the Auto-Login feature on SmartPSS installed on a computer that is used by multiple people. Disabling auto-login prevents users without the appropriate credentials from accessing the system.
- **Use a Different Username and Password for SmartPSS**
  - Do not use a username/password combination that you have in use for other accounts, including social media, bank account, or email in case the account is compromised. Use a different username and password for your security system to make it difficult for an unauthorized user to gain access to the IP system.
- **Limit Features of Guest Accounts**
  - Ensure that each user has rights to features and functions they need to perform their job.
- **Disable Unnecessary Services and Choose Secure Modes**
  - Turn off specific services, such as SNMP, SMTP, and UPnP, to reduce network compromise from unused services.
  - It is recommended to use safe modes, including but not limited to the following services:
    - SNMP: Choose SNMP v3 and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access a mailbox server.
    - FTP: Choose SFTP and use strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode and use strong passwords.
- **Multicast**
  - Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast. Deactivate this feature if not in use to enhance network security.
- **Check the Log**
  - The information stored in the network log file is limited due to the equipment's limited storage capacity. Enable the network log function to ensure that the critical logs are synchronized to the network log server if saving log files is required.
  - Check the system log if you suspect that someone has gained unauthorized access to the system. The system log shows the IP addresses used to login to the system and the devices accessed.
- **Physically Lock Down the Device**
  - Perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement access control permission and key management to prevent unauthorized personnel from accessing the equipment.

- **Connect IP Cameras to the PoE Ports on the Back of an NVR**
  - Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.
- **Isolate NVR and IP Camera Network**
  - Ensure that the network for the NVR and IP cameras should not be the same network as a public computer network. Separate networks prevent unauthorized users accessing the same network the security system.
- **Secure Auditing**
  - Check online users regularly to ensure unauthorized accounts are not logged in to a device.
  - Check the equipment log to access the IP addresses used to login to devices and their key operations.

# Table of Contents

---

Foreword.....	I
Important Safeguards and Warnings.....	IV
Cybersecurity Recommendations .....	VII
Table of Contents .....	X
<b>1 Overview .....</b>	<b>1</b>
1.1 Solution Components .....	1
1.2 Prerequisites .....	1
<b>2 Installation .....</b>	<b>2</b>
2.1 Blackbody/Camera Attachment.....	2
2.2 Thermal Camera and Blackbody Setup.....	2
2.3 Monitoring Parameters .....	2
2.4 Installation Diagrams .....	3
<b>3 Camera Configuration.....</b>	<b>4</b>
3.1 Initializing Camera .....	4
3.2 Modifying IP Address .....	5
3.3 Live Video.....	6
3.4 Smart Thermal Configuration .....	7
3.5 Global Setup.....	7
3.6 Human Temperature Measurement Setup.....	8
3.6.1 Configure Alarms .....	9
3.6.2 Link an Audio Prompt.....	10
3.7 Configure Blackbody Parameters .....	11
3.7.1 Setting Blackbody Abnormal Parameters .....	12
3.7.2 Intelligent Detect Channel Settings .....	13
<b>4 Correcting Temperature Readings .....</b>	<b>14</b>
4.1 Checking the Ambient Temperature .....	14
4.2 Verifying the Temperature Correction Value .....	15
<b>5 Thermal Hybrid Camera Calibration .....</b>	<b>16</b>
5.1 Event Verification.....	17

# 1 Overview

The Dahua Thermal Temperature Monitoring Solution offers the latest hybrid thermal network camera that combines a Vanadium Oxide (VOx) sensor with a 2 MP visible-light sensor. The solution also provides a blackbody calibration device that maintains a customizable constant temperature as a reference point for the thermal camera. The thermal camera coupled with the blackbody calibration device and a feature-rich 4 TB Network Video Recorder delivers a contactless solution for continuous and non-invasive comparison of human skin temperature compared to the blackbody device. Thermal Temperature Monitoring technology enables quick detection of elevated skin temperatures compared to the customizable blackbody calibration device. Thermal imaging equipment can easily be installed and implemented to detect elevated skin temperature in environments such as airports, hospitals, clinics, office buildings, cruise ships, and any large public gathering location.

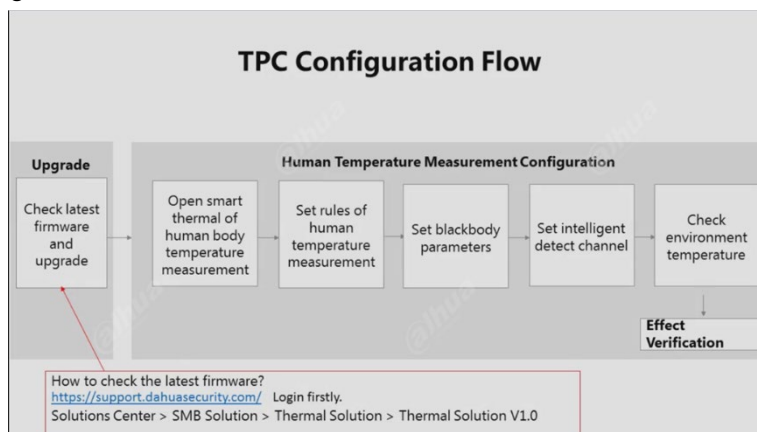
The Dahua Thermal Temperature Monitoring Solution is not a medical device and is not designed or intended for diagnosis, prevention, or treatment of any disease or condition. The solution is a screening tool that businesses and households can use to identify individuals with elevated skin temperature compared to a customizable reference temperature on or entering their premises.

## 1.1 Solution Components

- Required Components (sold separately)
  - DH-TPC-BF5421-T Thermal Hybrid Network Camera
  - JQ-D70Z Blackbody
  - DHI-NVR5216-16P-I 16-channel NVR
- Recommended Accessories (sold separately)
  - VCT-999 Tripod (x2)
  - RQW026-00 Bracket (x2)

## 1.2 Prerequisites

- Upgrade the firmware for the Thermal Camera.



# 2 Installation

Important Installations Notes:

- Do not point the camera towards the entrance or the outside of the building.
- Deploy the solution indoors only in an environment with a constant temperature and no wind.
- It is recommend to setup a queuing area to manage the flow of people.

## 2.1 Blackbody/Camera Attachment

- Blackbody and Camera connection to the VCT-999 Tripod using the RQW026-00 Bracket.



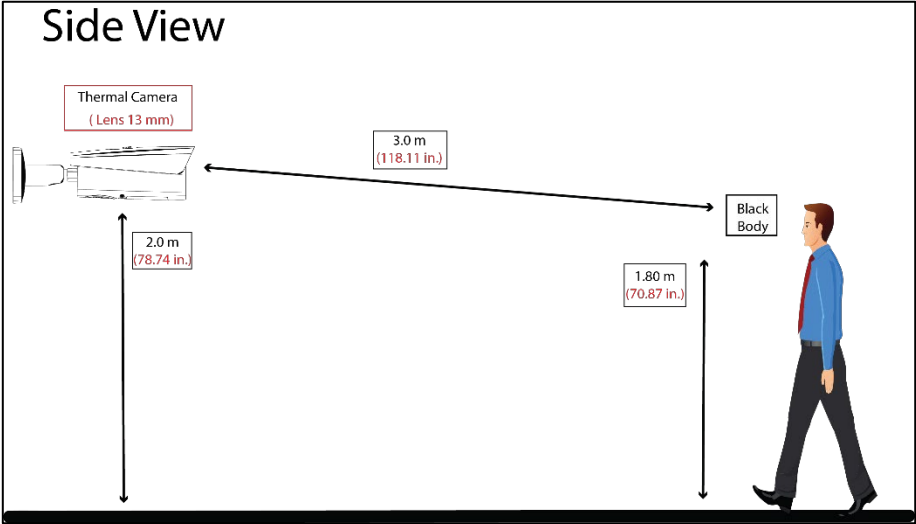
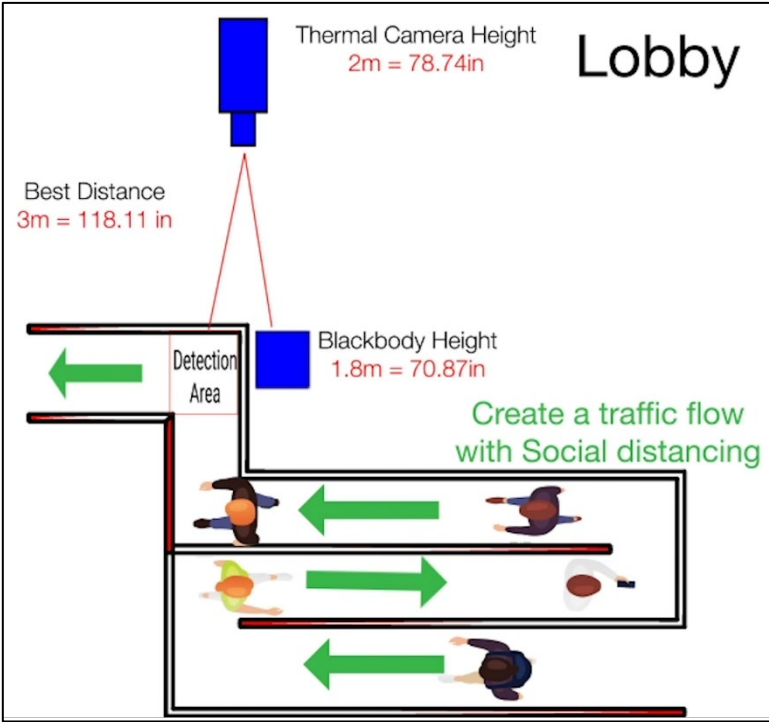
## 2.2 Thermal Camera and Blackbody Setup

Lens Focal Length	Distance Between Camera and Blackbody	Distance Between the Human Forehead and the Camera	Channel Width
13.0 mm	3.0 m (118.11 in.)	3.0 m (118.11 in.)	1.50 m (59.01 in.)
Note: The accuracy of temperature monitoring is best when the human forehead and blackbody are at the same distance from the camera.			

## 2.3 Monitoring Parameters

Height	Thermal Camera: 2.0 m (78.74 in.)
	Blackbody: 1.80 m (70.87 in.)
Distance	Up to 4.57 m (15.0 ft or 180.0 in.)
Rate	Up to 30 people per second

# 2.4 Installation Diagrams



# 3 Camera Configuration

## 3.1 Initializing Camera

Dahua IP cameras feature a built-in Web interface to control all aspects of camera operation. This section includes details about the supported network protocols, configuring IP addresses, and configuring alarms and local recording options. Refer to the camera's Operations Manual for full details.

- The camera will not operate if not properly initialized.
- Protect the administrator password after initialization and modify it regularly.
- Ensure the camera's IP address and the computer's IP address are on the same network  
The default camera IP address is 192.168.1.108.

1. Open a Web browser, input camera default IP address in the address bar, and then press **Enter**. The Device Initialization interface is displayed.

**Device Initialization**

Username: admin

Password:

Confirm Password:

Email Address:

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : & )

To reset password, please input properly or update in time.

Save

2. Set the Administrator login password

Parameter	Description
Password	The password must contain 8 to 32 nonblank characters that can comprise numbers, letters, and special characters (except "" "" , " : " and "&"), and must contain at least two types of characters. Please set the password with high security according to the password intensity prompt.
Confirm Password	
Email Address	Enter an email address to send a password change prompt.

3. Click **Save** to finish initialization.

## 3.2 Modifying IP Address

To configure the camera for your network, you need the following information:

- Camera IP address – This address is an identifier for the camera on an IP network. For example, 140.11.2.115 is valid syntax for an IP address.
  - Subnet mask – A mask is used to determine the subnet an IP address belongs to.
  - Gateway IP address – This address is a node on a network that serves as an entrance to another network.
  - Port – A port is an endpoint to a logical connection in an IP network. Log in camera web interface in the IE browser.
    - The factory default IP address is: 192.168.1.108.
    - The default user ID is “admin” and use the password set at initialization.
1. Select **Setup > Network > TCP/IP** to access TCP/IP interface.
  2. Modify the IP Address and any other applicable network parameter.

The screenshot shows the TCP/IP configuration page. The title is "TCP/IP". The fields are as follows:

- Host Name: TPCDome
- Ethernet Card: Wire(DEFAULT)
- Mode:  Static  DHCP
- MAC Address: [Greyed out]
- IP Version: IPv4
- IP Address: [Greyed out]
- Subnet Mask: [Greyed out]
- Default Gateway: [Greyed out]
- Preferred DNS: 8 . 8 . 8 . 8
- Alternate DNS: 8 . 8 . 4 . 4

At the bottom, there is a checkbox labeled "Enable ARP/Ping to set IP address service" which is checked. Below the checkbox are three buttons: "Default", "Refresh", and "Save".



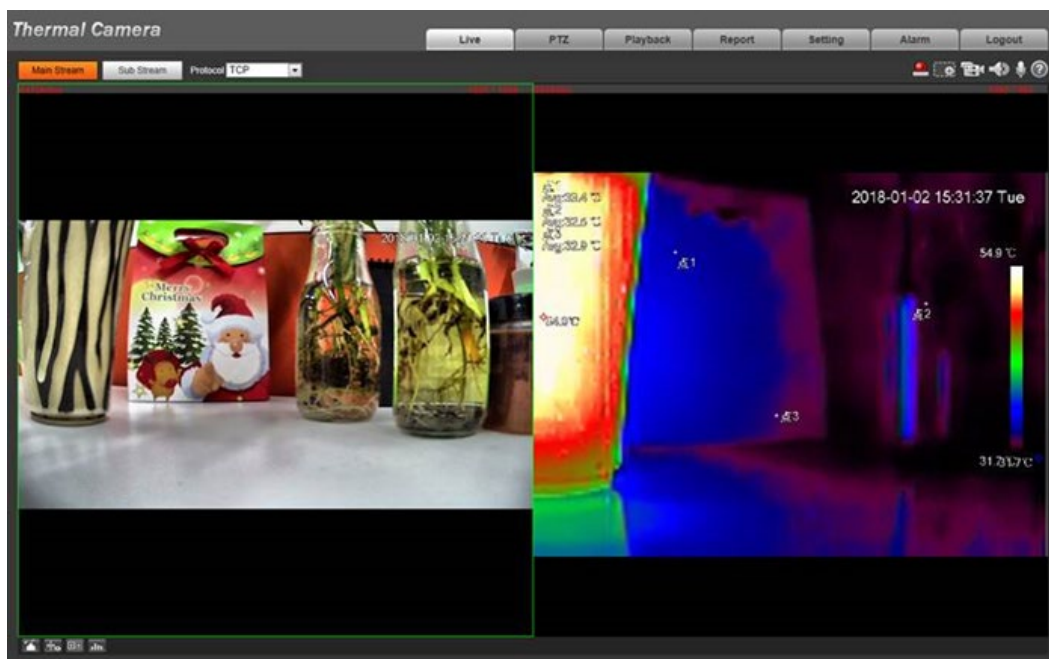
3. Click **Save** to finish modification and store the modified network parameters.

## 3.3 Live Video

Each camera can be accessed directly from the Internet Explorer Web browser. The Web Interface allows you to set camera parameter, configure alarm inputs and outputs, view live camera images, and review recorded video.

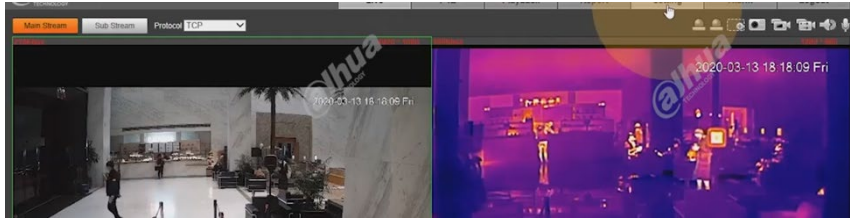
**Note:** Different devices may have different Web interfaces, the figures below are for reference only, and may not represent the Web Interface for your camera. Refer to the Web Operation Manual, included on the CD shipped with the camera, for more details.

1. Launch a Web browser and type the modified camera IP address in the address bar to access the Login page.
2. Type the Username and Password for the camera. Then, click Login. The Web browser opens the Live View page.



## 3.4 Smart Thermal Configuration

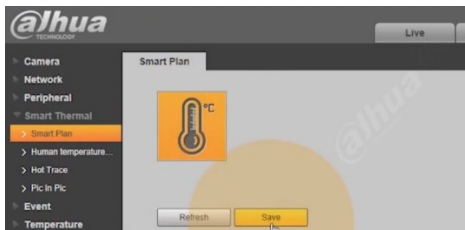
1. Click the Settings Tab.



2. Select Smart Thermal.



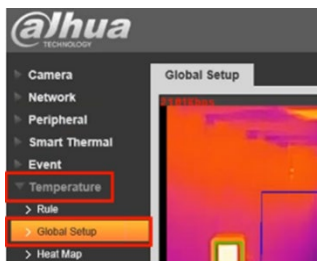
3. Select Smart Plan.



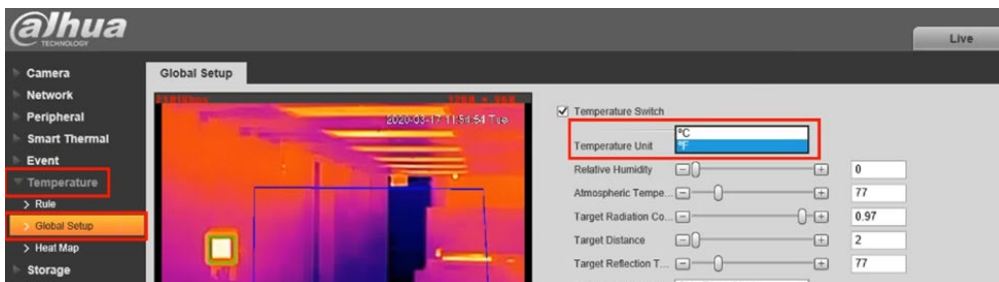
4. Select the Smart Plan Icon, then click Save.

## 3.5 Global Setup

1. Select the Temperature option in the menu, and click Global Setup.



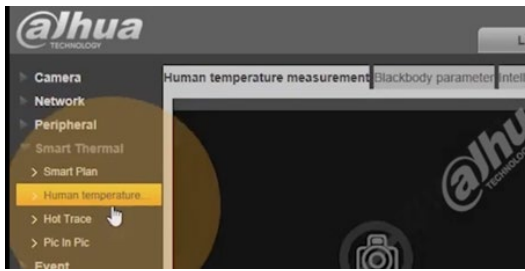
2. Set the temperature unit to Celsius or Fahrenheit, depending on your region.



3. Click Save.

## 3.6 Human Temperature Measurement Setup

1. Select the Smart Thermal option in the menu, and then click Human Temperature.



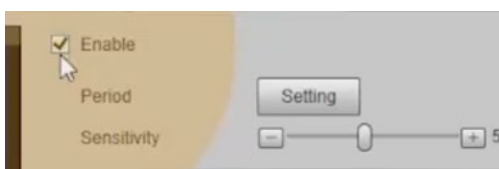
2. Configure the rules for human temperature measurement.



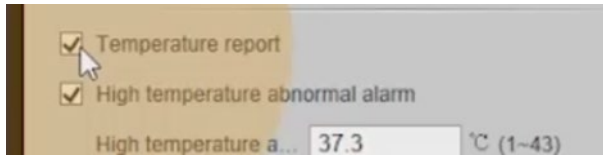
- a) Have a test subject stand in the ideal temperature measurement position near the blackbody.



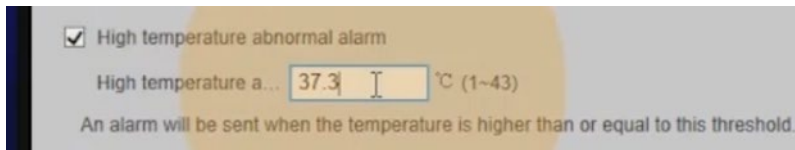
- b) Make sure the head and shoulders are visible in the picture.
  - c) Draw the bottom border of rule near the shoulder.
  - d) Draw the rule box in the center of the 16-grid picture with 4 grids and close to the black body
  - e) Draw the lower border. Ensure the border is not too close to the bottom of the monitoring area, because an object approaching the monitoring area will be too high and cause false alarm.
3. Click the Enable check box to turn on temperature measurement.



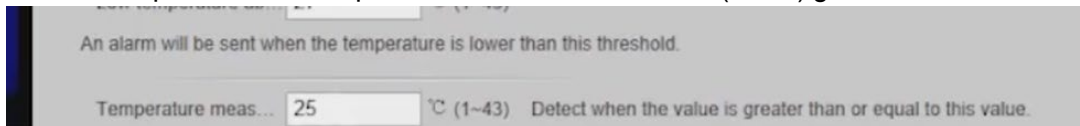
4. Enable the temperature report.



5. Set the High Temperature Abnormal Alarm.

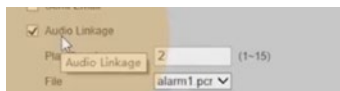


- The default temperature setting is 37.3° C (94.14° F)
- An object that registers a temperature of 50° C (122 ° F) does not generate an alarm.
- In the example below, a temperate detected above 25° C (77° F) generates an alarm:

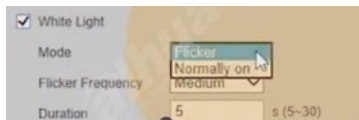


### 3.6.1 Configure Alarms

1. Click the Audio Linkage checkbox to enable the built-in audio alarm.



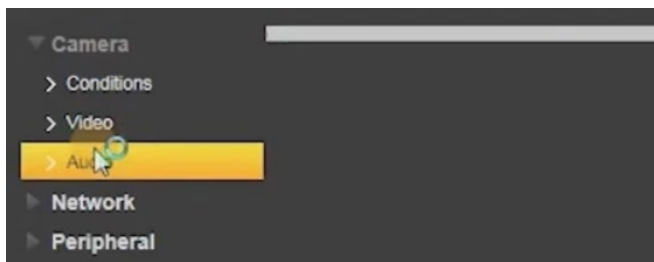
2. Click the White Light checkbox to enable the white light to illuminate on an alarm.



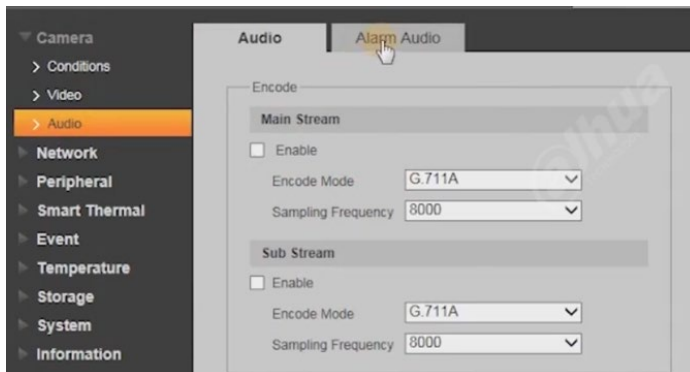
3. Click Enable Snapshot. Then click Access Control to disable the feature.
4. Click Save.

## 3.6.2 Link an Audio Prompt

1. Click Audio.



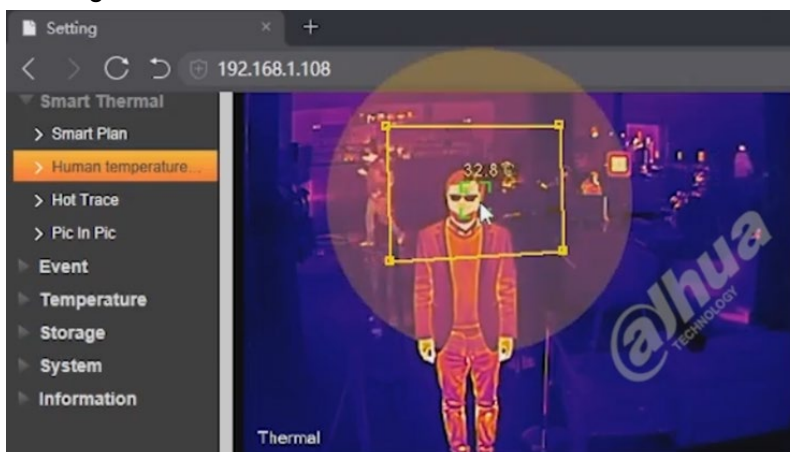
2. Click the Alarm Audio tab.



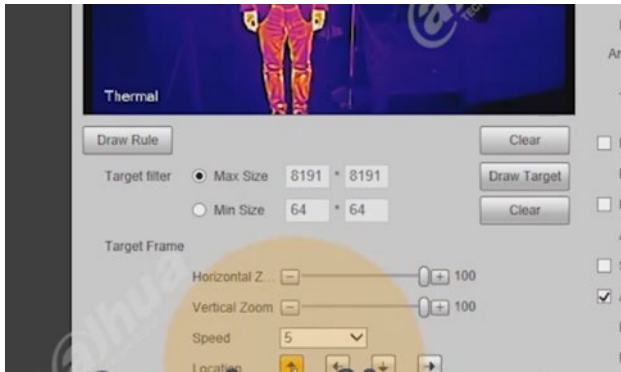
3. Click the Add Audio File button. Note the system supports the PCM audio file format.
4. Navigate to the PCM audio file and select to upload the file. Then, click Upload.



5. Return to the Human Temperature Measurement tab and click Save. The system returns to the target frame.



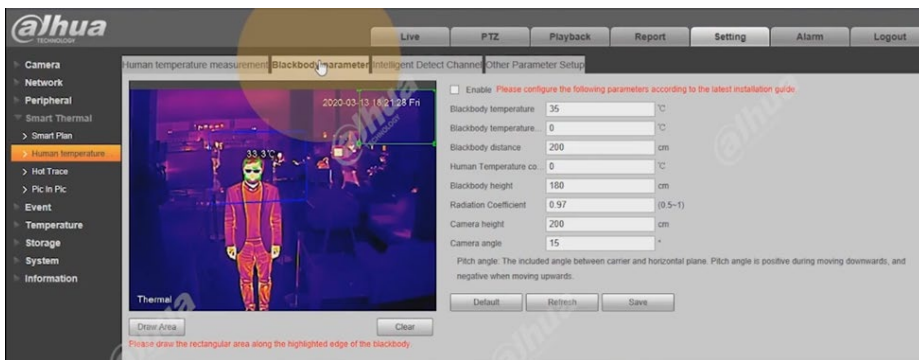
6. Adjust the horizontal and vertical zoom.



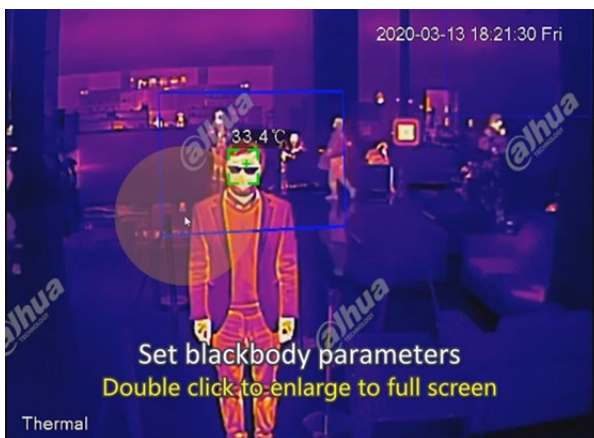
7. Set the step speed and the target location that is appropriate for the application.
8. Click Save.

## 3.7 Configure Blackbody Parameters

1. Click the Blackbody Parameter tab.



2. Double-click the target area to expand to full screen.



3. Select the green rule box to draw.
4. Draw the rule box along the bold highlighted edge.
5. Surround the highlighted area.

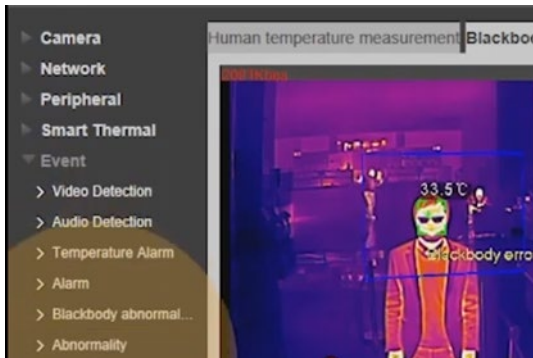


6. Double-click the target area again to return the parameter panel.
7. Click the Enable check box. The system defaults the blackbody temperature as 35° C (90.0° F).

### 3.7.1 Setting Blackbody Abnormal Parameters

Calibrating the blackbody may be required when:

- More than five samples of the scene are standing at the optimal temperature measuring distance.
  - The temperature is generally high or low.
1. Select the Event option on the menu and click Blackbody Abnormal.

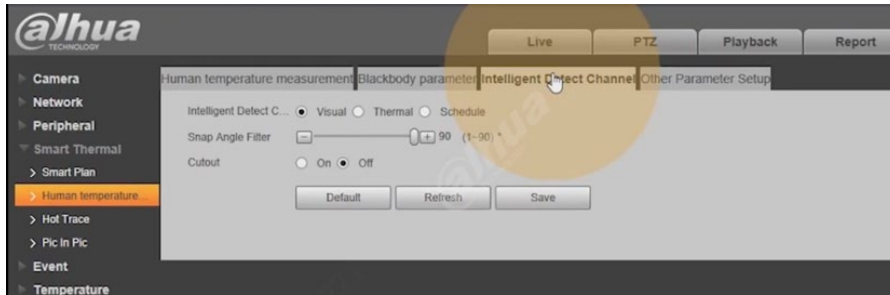


2. Set the blackbody parameters if the actual temperature is within the range of error sensitivity, it can be corrected to the fault temperature automatically.



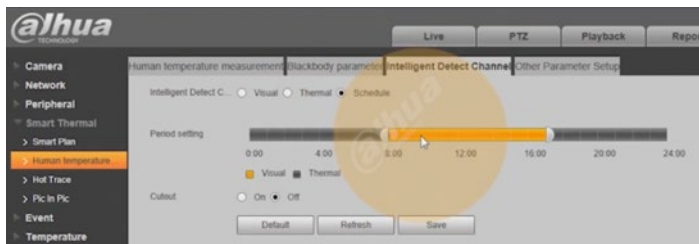
## 3.7.2 Intelligent Detect Channel Settings

Click the Intelligent Detect Channel tab.

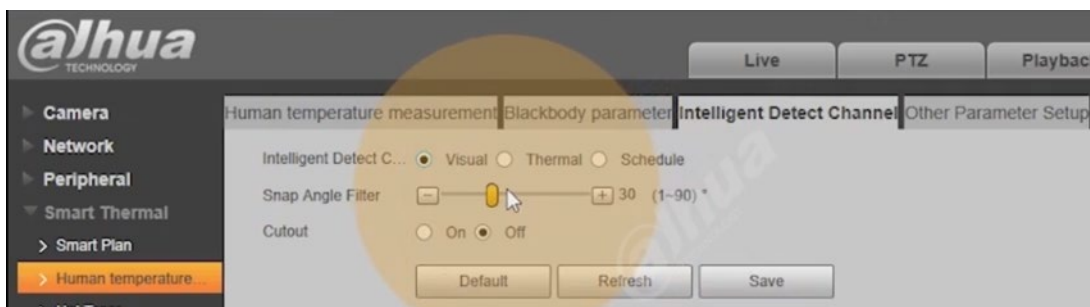


Set the following parameters:

- Visual and Thermal Channels are optional.
- Use the Visual Channel for normal scenes to detect faces by default.
- Use the Thermal Channel for scenes that are too dark or backlit.
- Set the schedule for better detection.



- The Visual channel supports the snapshot angle filter. The larger the Snap Angle Filter the easier it is to capture the side face. For example, when the value is 1, the system detects only the front of the face.

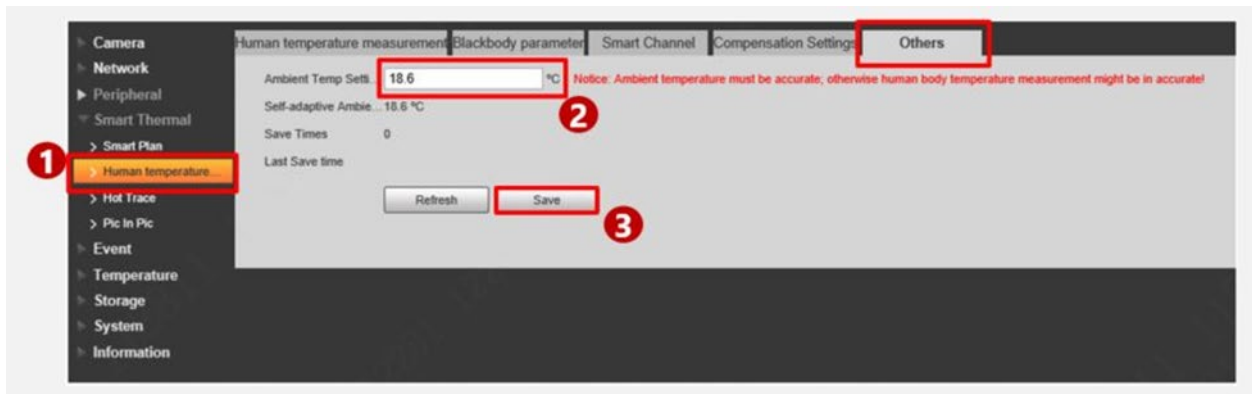




# 4 Correcting Temperature Readings

Use the following procedure to improve the accuracy of the thermal camera's temperature measurement. The procedure offers two main steps: Ambient Temperature Check and Temperature Correction verification.

## 4.1 Checking the Ambient Temperature

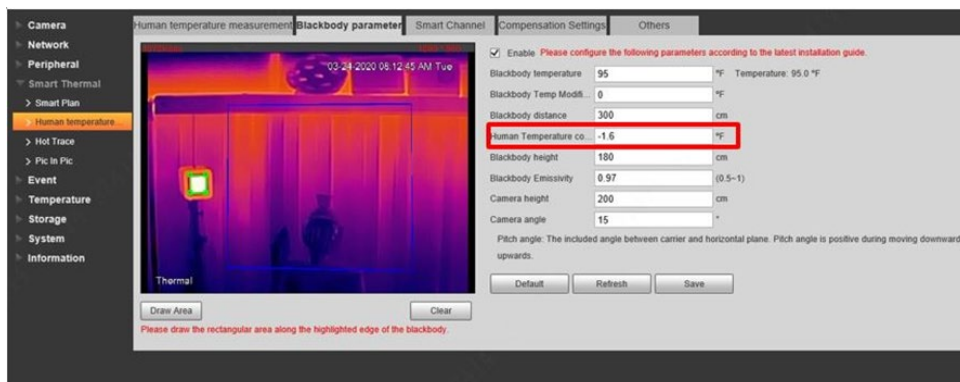


1. Log into the Web interface.
2. Select Setting, and then choose Smart Thermal and Human temperature measurement. Then click the Others tab.
3. Use a thermometer to measure the actual ambient temperature on site and input the temperature.
4. Click Save.
5. If the temperature measurement is still inaccurate, proceed to the next section.

## 4.2 Verifying the Temperature Correction Value

The actual human body temperature, on average, is 37° C (98.6° F) by a thermometer. The thermal camera measures the same human temperature as 37.8° C (100° F). The value for the Human Temperature correction is:  
 $37^{\circ}\text{C} - 37.8^{\circ}\text{C}$  ( $98.6^{\circ}\text{F} - 100^{\circ}\text{F}$ ) =  $-0.8^{\circ}\text{C}$  ( $-1.4^{\circ}\text{F}$ ).

1. Use a thermometer to measure the actual human body temperature.
2. Calculate the difference between the actual human body temperature and temperature measured by the thermal camera.
3. Type the difference in the Human Temperature correction value.



4. Click Save.

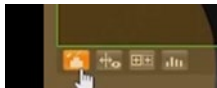
# 5 Thermal Hybrid Camera Calibration

This section details calibrating the face rule box on a thermal hybrid camera.

1. Log into the Web Interface.



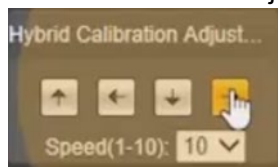
2. Click the icon located in the lower left corner of the Live View window.



3. Navigate to the Hybrid Calibration Adjustment panel:

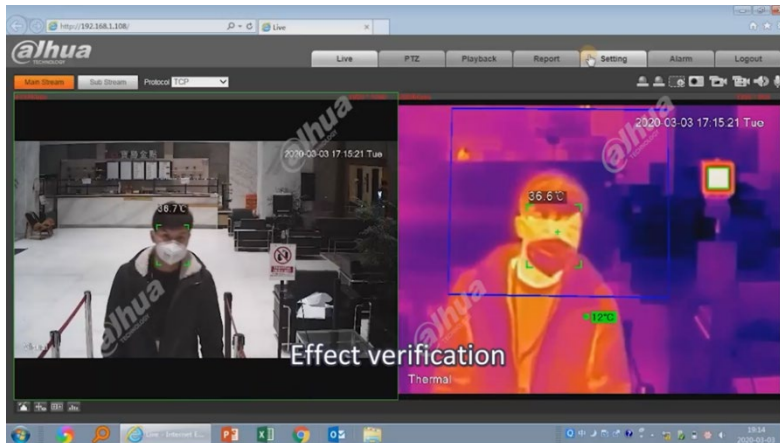


4. Use the arrows to adjust the Speed Sensitivity and the Face Frame angle.



## 5.1 Event Verification

1. Return to the Live View to verify the temperature measurement.



2. Check the temperature measurement value on the screen.
3. Compare it with the value on the frontal temperature gun (if available).
4. Put hot water on the subject's forehead to simulate an elevated temperature to trigger the alarm.





Dahua Technology USA

23 Hubble

Irvine, CA 92618

Tel: (949) 679-7777

Fax: (949) 679-5760

Support: 877-606-1590

Sales: [sales.usa@dahuatech.com](mailto:sales.usa@dahuatech.com)

Support: [support.usa@dahuatech.com](mailto:support.usa@dahuatech.com)