



Thermal Hybrid Camera

Quick Installation Guide

V1.0.1

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
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 NOTE	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

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

- Please use the device within the allowed humidity (<95%RH) and altitude (<3000m).
- 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.
- Please don't 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 already 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.
- Please contact the local dealer or the nearest service center if the device fails to work normally, please don't dismantle or modify the device.

Cybersecurity Recommendations

Mandatory actions to be taken towards 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 be made up of at least 8 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
1 Overview	1
1.1 Camera Components.....	1
1.2 Dimensions.....	2
1.3 Cable Detail.....	2
1.4 Alarm Connections	3
2 Installing the Camera	4
2.1 Installation Tips.....	4
2.2 Selecting Cables.....	4
2.2.1 Power Cables	4
2.2.2 Signal Cables	5
2.3 Inserting an SD Card (optional).....	5
2.4 Mounting the Camera to a Wall.....	6
2.5 Adjusting the Sun Shield	8
2.6 Adjusting the Camera Angle.....	9
3 Camera Configuration	10
3.1 Initializing Camera	10
3.2 Modifying IP Address	11
3.3 Live Video.....	12
4 Alarm Configuration	13
4.1 Alarm Input and Output Connection Description.....	13
4.2 Alarm Input and Output Figures	14
4.2.1 Alarm Input	14
4.2.2 Alarm Output	14
5 Lightning and Surge Protection	15

1 Overview

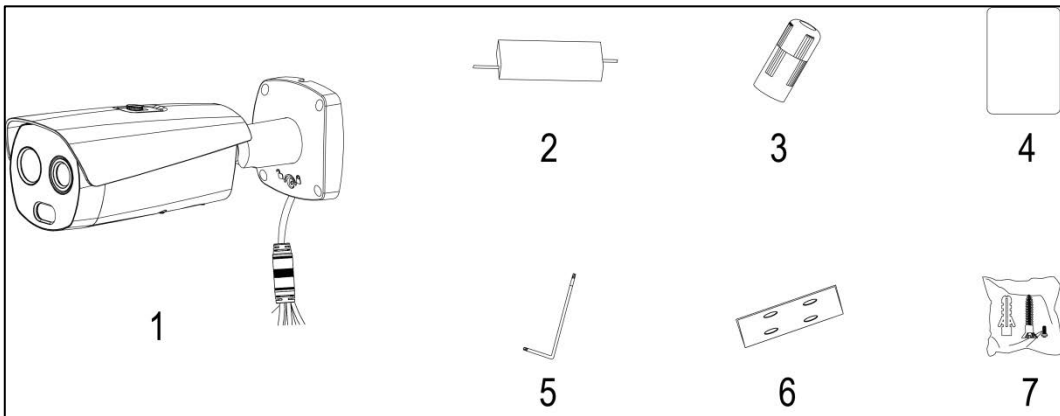
The Hybrid Thermal Network camera combines an uncooled VOx thermal sensor with a 2 MP visible-light sensor for cost-effective, long-range surveillance in a rugged all-in-one package. The thermal imager coupled with an athermalized, focus-free lens produces crisp images in total darkness and sees through rain, fog, and snow. The visible sensor with an IR illuminator delivers superior video in any lighting condition.

1.1 Camera Components

This equipment should be unpacked and handled with care. If an item appears to have sustained damage during shipping, notify the shipper immediately.

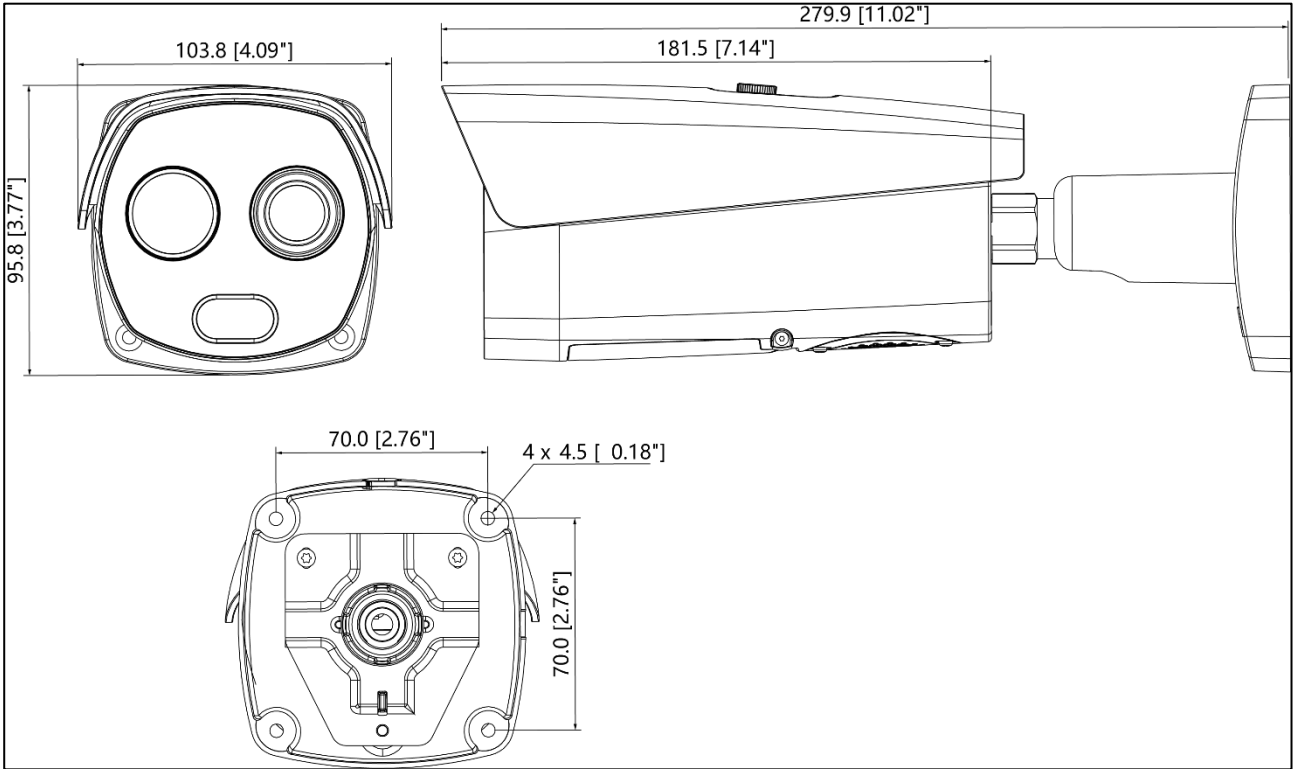
Verify that all the parts listed below are included. If an item is missing, contact customer support or your local representative.

The original packing carton is the safest container to transport the unit, in the event the unit must be returned for service. Retain the carton and all shipping material for future use.

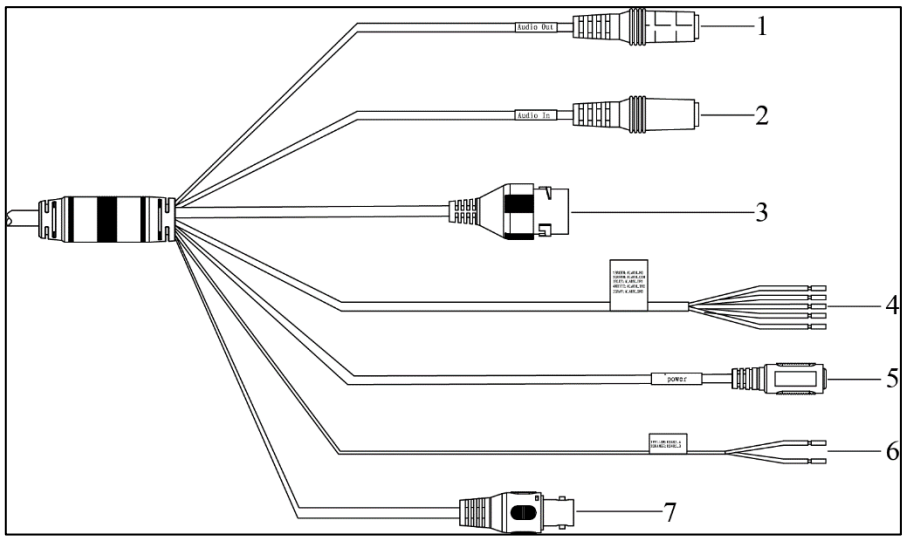


Reference	Description
1	Thermal Hybrid Camera
2	Power Cable
3	Waterproof Ethernet Connector
4	Quick Start Guide
5	Hex Wrench
6	Mounting Template
7	Hardware Components

1.2 Dimensions




1.3 Cable Detail



Ref	Port	Port Name	Function Description
1	AUDIO OUT	Audio output port	3.5mm Jack, output audio signal to speakers.
2	AUDIO IN	Audio input port	3.5mm Jack, input audio signal receives analog audio signal from a microphone or other audio pick up.
3	LAN	Network port	Connect to standard Ethernet cable.
4	I/O	I/O port	Alarm signal input/output.
5	POWER	Power input port	Input 12V DC. Use in accordance with device label instructions.
6	RS485_A (Yellow)	RS-485	Control external PTZ cameras.
	RS485_A (Orange)		
7	VIDEO OUT	Video output port	Output for analog video signal to connect to a spot monitor for installation.

1.4 Alarm Connections

Port	Color	Cable port name	Function description
I/O port	Green	ALARM_COM1	Alarm output common port. 
	Pink	ALARM_COM2	Use ALARM_COM1 together with ALARM_NO1 and use ALARM_COM2 together with ALARM_NO2.
	Blue	ALARM_NO1	Alarm output port, output alarm signal to alarm device. NO: Normally open alarm output port.
	Gray	ALARM_NO2	Use ALARM_NO1 together with ALARM_COM1 and use ALARM_NO2 together with ALARM_COM2.
	Purple	ALARM_IN1	Alarm input ports; receive the on-off signal of external alarm source.
	Brown	ALARM_IN2	
	Green/ White	ALARM_GND	Grounded terminal.

2 Installing the Camera

The camera ships with all the components to mount the camera to a wall. Before installing the camera consider the following:

- Review the “Installation Tips” section to help you choose an ideal mounting location.
- Decide whether to run the cables through the wall or along the wall.

2.1 Installation Tips

This section details installing the camera to a wall or to a ceiling. Note that the wall or ceiling must be capable of supporting a minimum of three times the weight of the camera and a bracket (if used).

- **Warning:** DO NOT connect the camera to the power supply during installation.
- **Warning:** For units intended to be installed outdoors: All wiring connecting to the unit must be routed separately inside a different permanently earthed metal conduits (not supplied).
- **Warning:** Install external interconnecting cables in accordance to NEC, ANSI/NFPA70 (for US application) and Canadian Electrical Code, Part I, CSA C22.1 (for CAN application) and in accordance to local country codes for all other countries. Branch circuit protection incorporating a 20 A, 2-pole Listed Circuit Breaker or Branch Rated Fuses are required as part of the building installation. A readily accessible 2-pole disconnect device with a contact separation of at least 3 mm must be incorporated.
- **Warning:** DO NOT remove the protective film from the dome until the installation is complete to protect the dome from distortions from fingerprints, oil, grease or other contaminants.
- Note: Dahua recommends attaching a “drip loop” (flex or hard conduit) during installation to ensure condensation does not form in the mount or the conduit.

2.2 Selecting Cables

2.2.1 Power Cables

The maximum transmission distance is recommended when the size of the wire diameter is fixed and DC 12V voltage transmission power is 10W. Refer to the following table for more details.

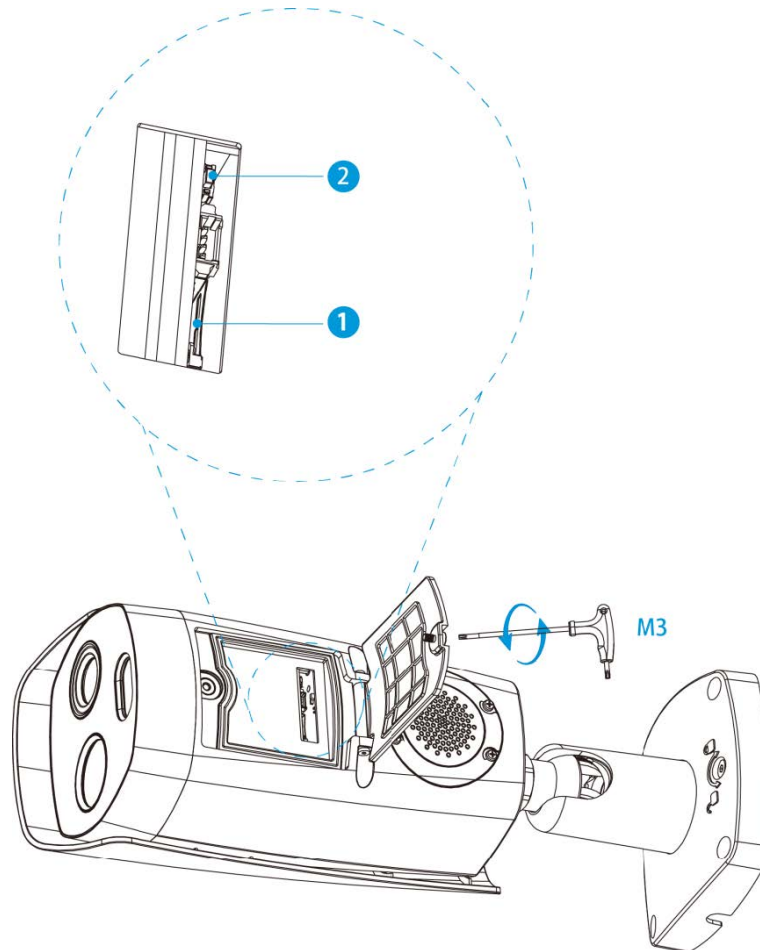
Wire Diameter (mm)	Maximum Distance
0.800	18.61 m (61.06 ft)
1.000	29.08 m (95.41 ft)
1.250	149.08 (45.44)
2.000	381.66 (116.33)

2.2.2 Signal Cables

Use at least a 0.56 mm (24 AWG) wire for all signal cables, including audio, alarm input and output, and RS-485.

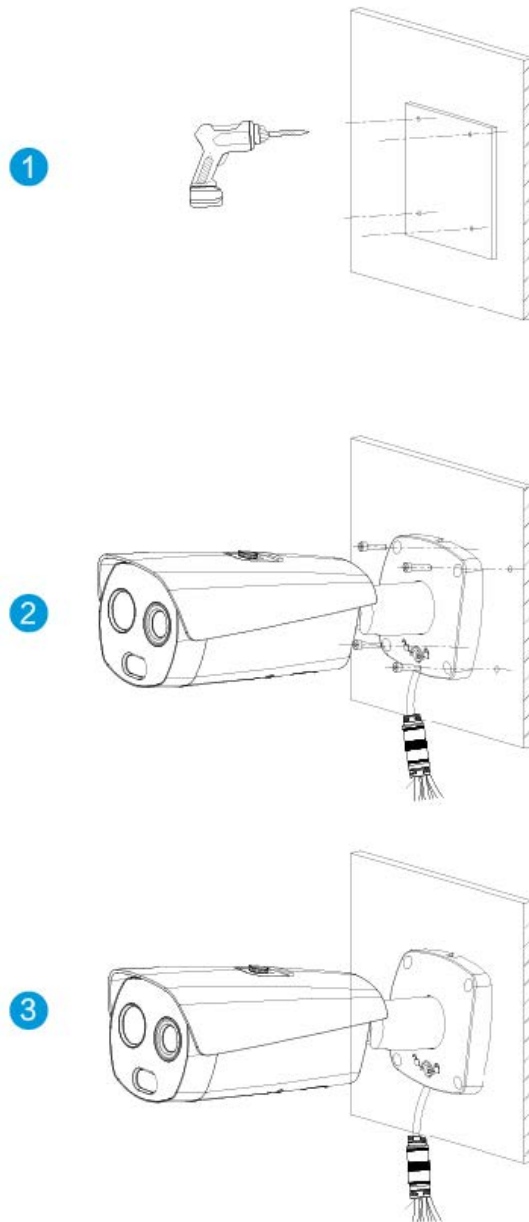
2.3 Inserting an SD Card (optional)

- Disconnect the camera from the power supply prior to installation.
- Be sure to place the SD card into the appropriate slot. Do not mistake the Reset button for the Micro SD card slot.
- Press the Reset button for 4 to 5 seconds to reset the camera to its factory defaults.
- Ensure the waterproof ring is seated properly before closing the cover. If the ring is not seated properly the waterproof performance will be compromised.



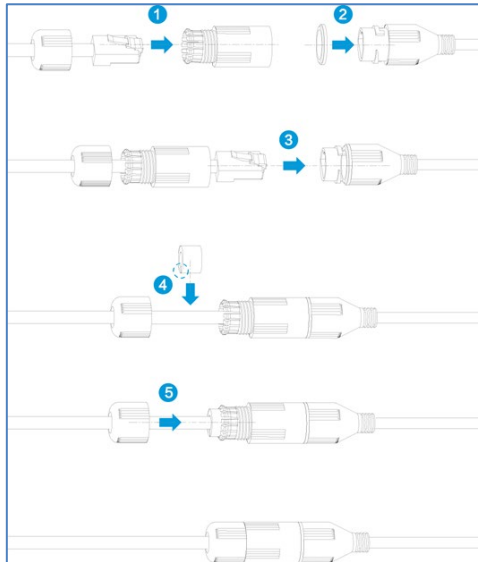
Ref.	Description
1	Micro SD Card Slot
2	Reset

2.4 Mounting the Camera to a Wall



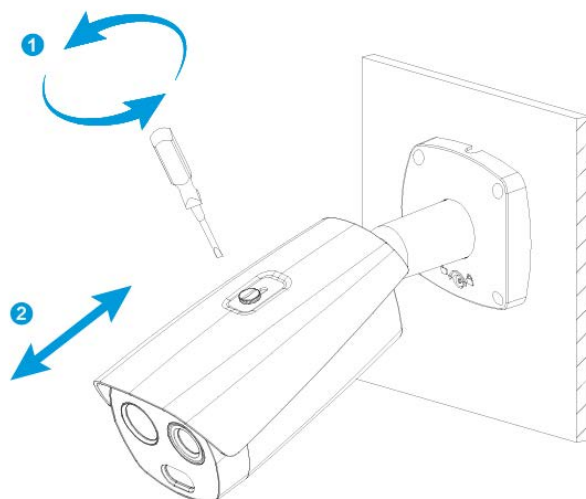
1. Remove the camera, the mounting template, and the hardware package from the box.
2. Apply the mounting template to the installation medium. Pre-drill the four perimeter holes for the expansion bolts, using a drill bit that is no wider than the expansion bolt. (Item 1)
3. Drill the center hole to route the cables from the camera through the installation medium or run the cables through conduit.
4. Insert an expansion bolt into each pre-drilled perimeter hole. (Item 2)

5. Attach the waterproof network connector if the camera is used outdoors.



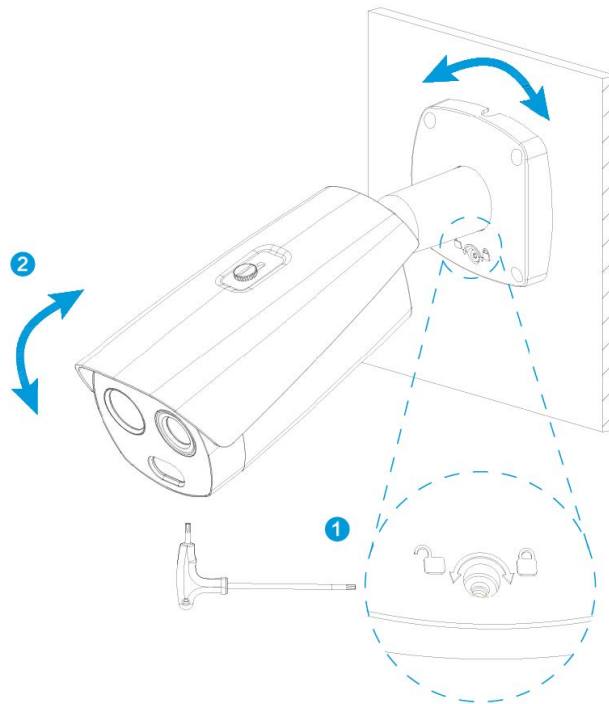
- a) Place the wide side of the rubber ring onto the end of the network cable extending out from the camera.
 - b) Pull the waterproof cable end without the Ethernet connector through the body of the Waterproof Connector. Thread the cable through the Fixing Rubber Ring and the Waterproof Locking Cover.
 - c) Attach the male Ethernet connector to the network cable coming from the camera. Ensure the Waterproof Connector shroud covers the Ethernet connection.
 - d) Connect the other end of the waterproof connector to the network port and rotate it clockwise to lock the network port and waterproof connector firmly.
 - e) Slide the Waterproof Locking Cover over the main body of waterproof connector and rotate it clockwise to seal the connection.
6. Connect the remaining cables to the camera ports and use insulating tape to seal each port to prevent water ingress.

2.5 Adjusting the Sun Shield



1. Adjust the sunshield, if necessary. Loosen the screw on the top of the camera and slide the sunshield back and forth to the desired location, then tighten the screw.

2.6 Adjusting the Camera Angle



1. Adjust the monitoring direction of the camera. Use a screwdriver to loosen the adjusting screw on the base of the camera.
2. Position the camera by tilting, twisting, and rotating the camera as shown above. Use the following camera adjustment limits:
 - Pan: 0° to 360°
 - Tilt: 0° to 90°
 - Rotation: 0° to 360°
 - Note: Do not rotate the camera more than three (3) times in any one direction.
3. Tighten the adjusting screw once the proper scene is attained.

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:

Weak Middle Strong

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 ' " ; : &)

Email Address

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 properly 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

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

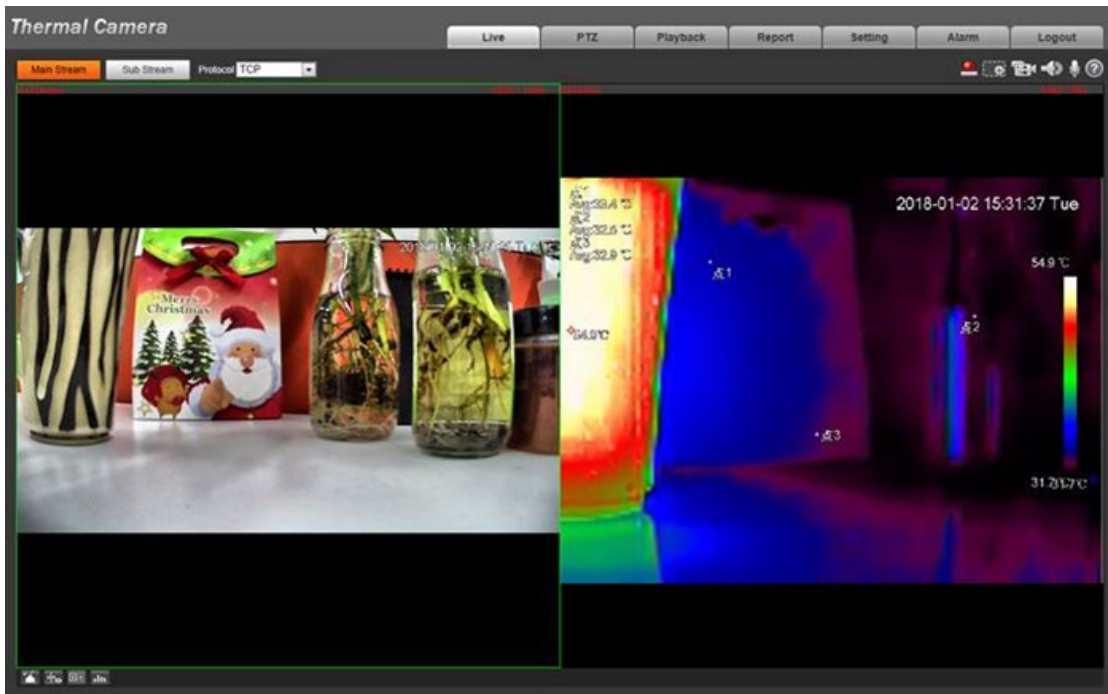
3. Click **Save** to finish modification and store the modified network parameters.

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.

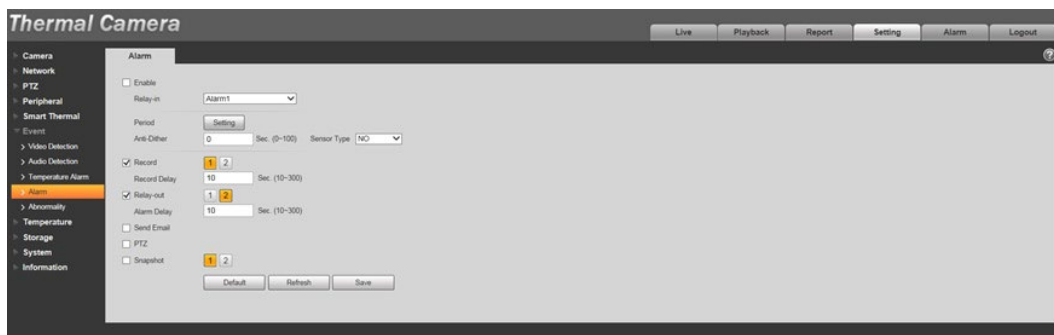
1. Launch a Web browser and type the modified camera IP address in the address bar to access the Login page.
2. Type the Username and Password for the camera. Then, click Login. The Web browser opens the Live View page.



4 Alarm Configuration

4.1 Alarm Input and Output Connection Description

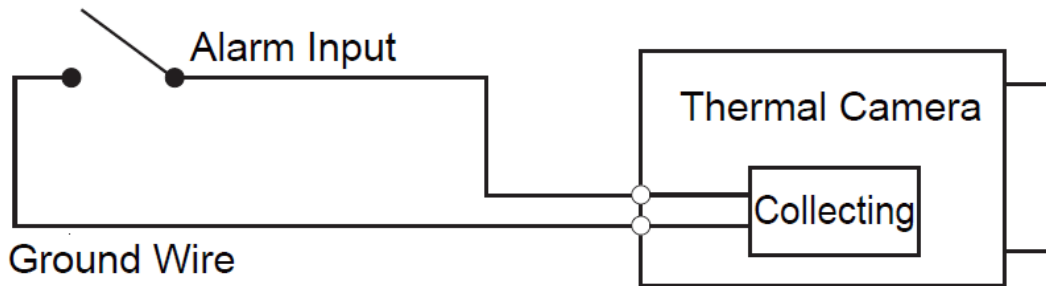
1. Disconnect the camera from the power supply prior to connecting any alarm cables.
2. Connect alarm input device to alarm input port of I/O cable.
3. Connect alarm output device to alarm output port of I/O cable. Alarm output is relay switch output, and the alarm output port can only be connected to NO alarm device.
4. Open the Web interface, select **Setting > Event > Alarm**.
5. Make corresponding settings upon alarm input and output in the alarm setup interface, and then click **Save**.
 - Set the alarm input and output parameters. Set the Sensor Type to NO or NC for each alarm input. The alarm input set corresponds to the device I/O port cable. When an alarm is triggered, the alarm input device generates a high- and low-level signal.
 - Set the alarm output (or relay out) parameters for the device connected to the ALARM_OUT port.



4.2 Alarm Input and Output Figures

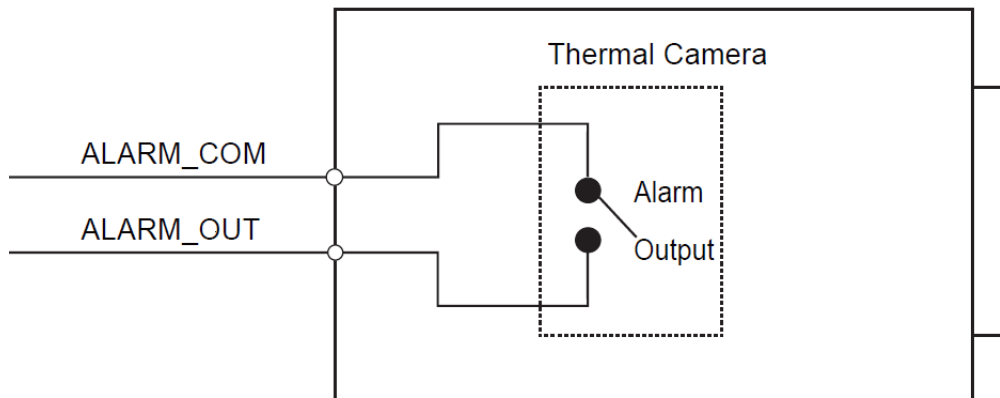
4.2.1 Alarm Input

The device collects that status of the alarm input port when the input signal is idle or grounded. If the input signal is connected to the 3.3 V or it is idle then the device receives the alarm input signal. If input signal is grounded, then no alarm input signal is detected.



4.2.2 Alarm Output

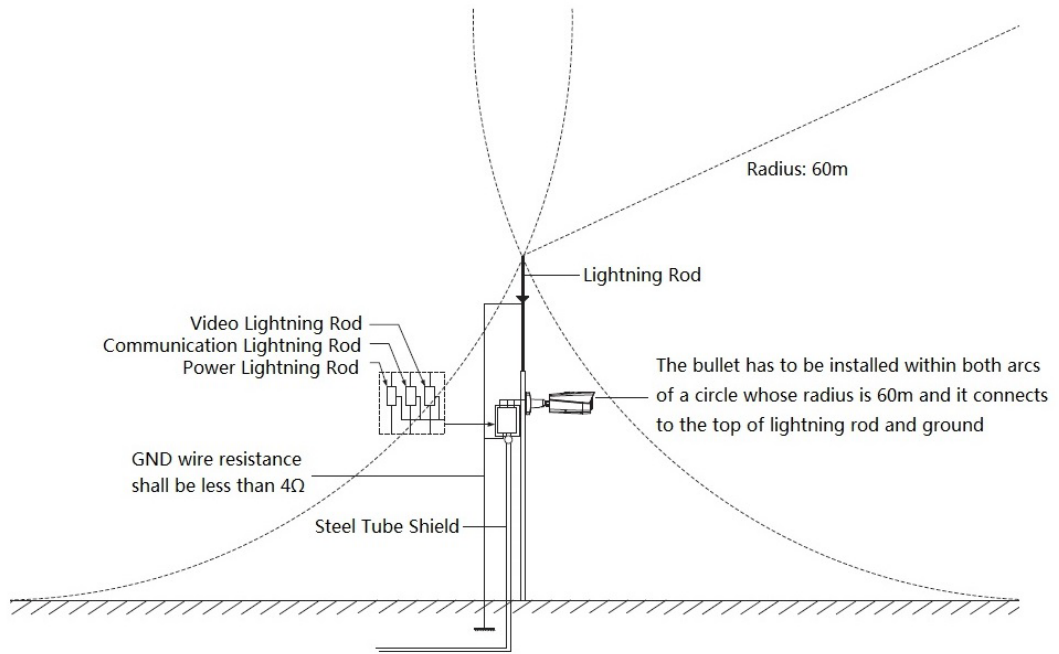
The ports ALARM_OUT and ALARM_OUT_GND form a switch that is used to provide alarm output. Normally the switch is on. The switch turns off when there is alarm output.



5 Lightning and Surge Protection

This camera uses TVS lightning protection technology to prevent damage from various pulse signals below 6000V, such as lightning and power surge. While maintaining your local electrical safety code, you still need to take necessary precaution measures when installing the camera outdoors.

- The distance between the signal transmission cable and high-voltage devices (or high-voltage cables) shall be at least 50 meters.
- Outdoor cable layout shall be routed beneath the housing if possible.
- Use a sealing steel tube below ground to implement cable layout and connect one point to the earth. An open floor cable layout is forbidden.
- Install a 10 KA lightning rod near the camera's power input port and Ethernet port. For cameras with an AC to DC power adapter, install a 10KA lightning rod near the adapter's input port.
- For a camera installed on a steel tower, connect the camera's ground wire to the tower's ground wire if the tower's wire is connected properly into the ground. In addition:
 - Ensure the camera is over 3 m away from the top point of the tower's lightning rod.
 - Use several strands of copper wire whose total diameter is up to 16 mm².
 - Ensure the camera is installed within both arcs of circles whose radius is 60 m. See the figure below.
- If there is no ground wire on the tower, connect the camera's ground wire directly to the ground.
- In areas of strong thunderstorm activity or near high voltage structures (such as a high-voltage transformer substation), install additional high-power lightning protection devices or a lightning rod.
- The lightning protection and earth ground of the outdoor device and cable shall be considered in the building whole thunder protection and conform to your local national or industry standard.
- The system shall adopt equal-potential wiring. The earth device shall meet anti-jamming and at the same time conform to local electrical safety codes. The earth device shall not short circuit to N (neutral) line of high voltage power grid or mixed with other wires. When you connect the system to the earth alone, the earth resistance shall not be more than 4Ω and earth cable cross-sectional area shall be no less than 25 mm².





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

Support: support.usa@dahuatech.com