SafetyTemp Series
Thermal Temperature Station
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 the Dahua Thermal Temperature Station. 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.	April 2020
2	V1.0.1	Revised for North America	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 was 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 updated periodically 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 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

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 requited. 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 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

1 Overview

The Dahua Thermal Temperature Station offers a compact and easily deployed solution for monitoring human skin temperature. Install and implement the station to detect elevated skin temperature in environments such as hospitals, clinics, office buildings, and retail locations.

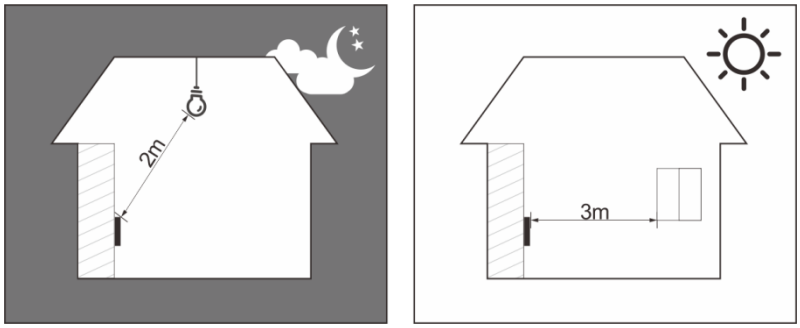
The Dahua Thermal Temperature Station is not a medical device and is not designed or intended for diagnosis, prevention, or treatment of any disease or condition. The solution is a screening tool that businesses and households can use to identify individuals with elevated skin temperature compared to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

1.1 Temperature Monitoring Requirements

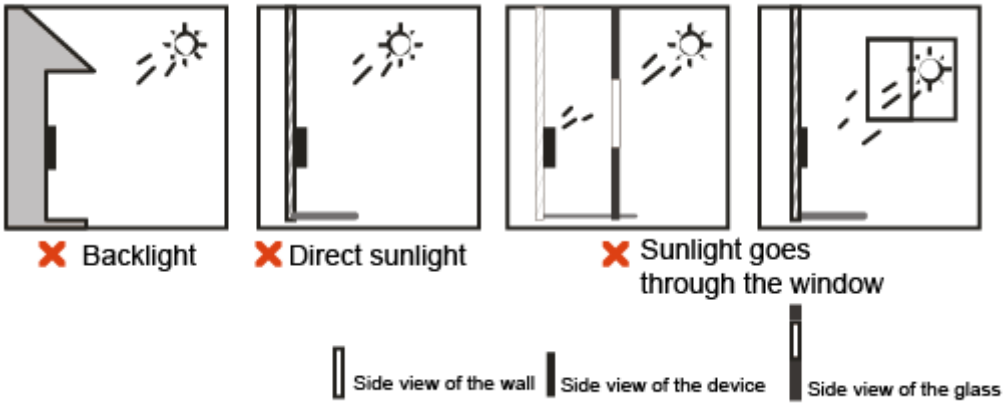
- Install the thermal temperature station in an indoor windless environment in a location relatively isolated area from the outdoor environment.
- Maintain an ambient temperature at between 15° C to 32° C (59° F to 89.6 ° F).
- Warm-up the station for at least 20 minutes after power-on to enable the station to reach thermal equilibrium.
- Setup a temporary monitoring area with a stable ambient temperature if there is no suitable indoor environment near the entranceway, especially if direct light, fluctuating temperatures, or wind effects the entrance.
- Sunlight, wind, cold air, and air conditioning can affect the surface temperature of human skin and the working status of the station. These factors can cause a deviation between the monitored and the actual temperature.
- The following factors affect temperature measurement accuracy:
  - Wind can cool the forehead.
  - Sweat is the body’s way of removing excess heat and is a way for the body to automatically cool down and dissipate heat.
  - Room temperature, whether high or low, affects the surface temperature of human skin. Avoid positioning the station near air conditioning outlets, heating ducts, and glass surfaces.
  - Light sources with a wavelength between 10 μm to 15 μm can affect the station. Avoid positioning the station in direct sunlight and fluorescent light sources.

1.2 Locations

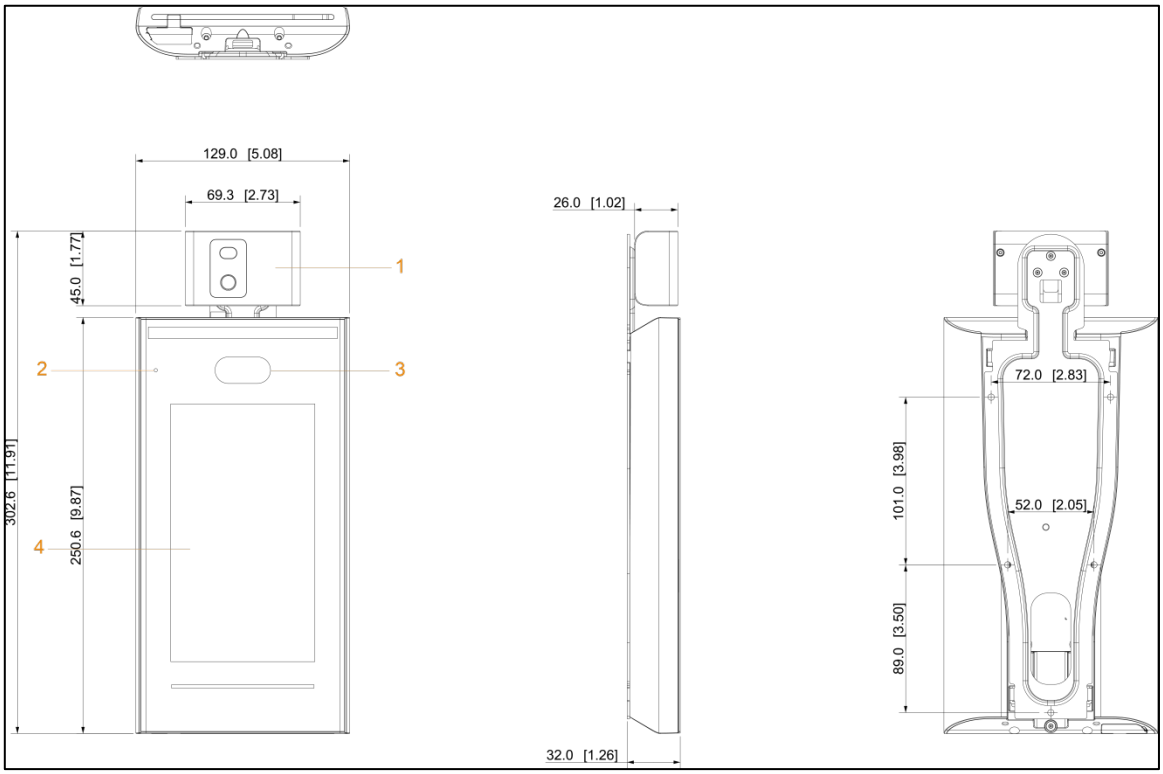
1.2.1 Recommended Locations



1.2.2 NOT Recommended



1.3 Dimensions



Ref.	Description	Ref.	Description
1	Temperature Monitoring Station	3	Dual Cameras
2	Microphone	4	Display

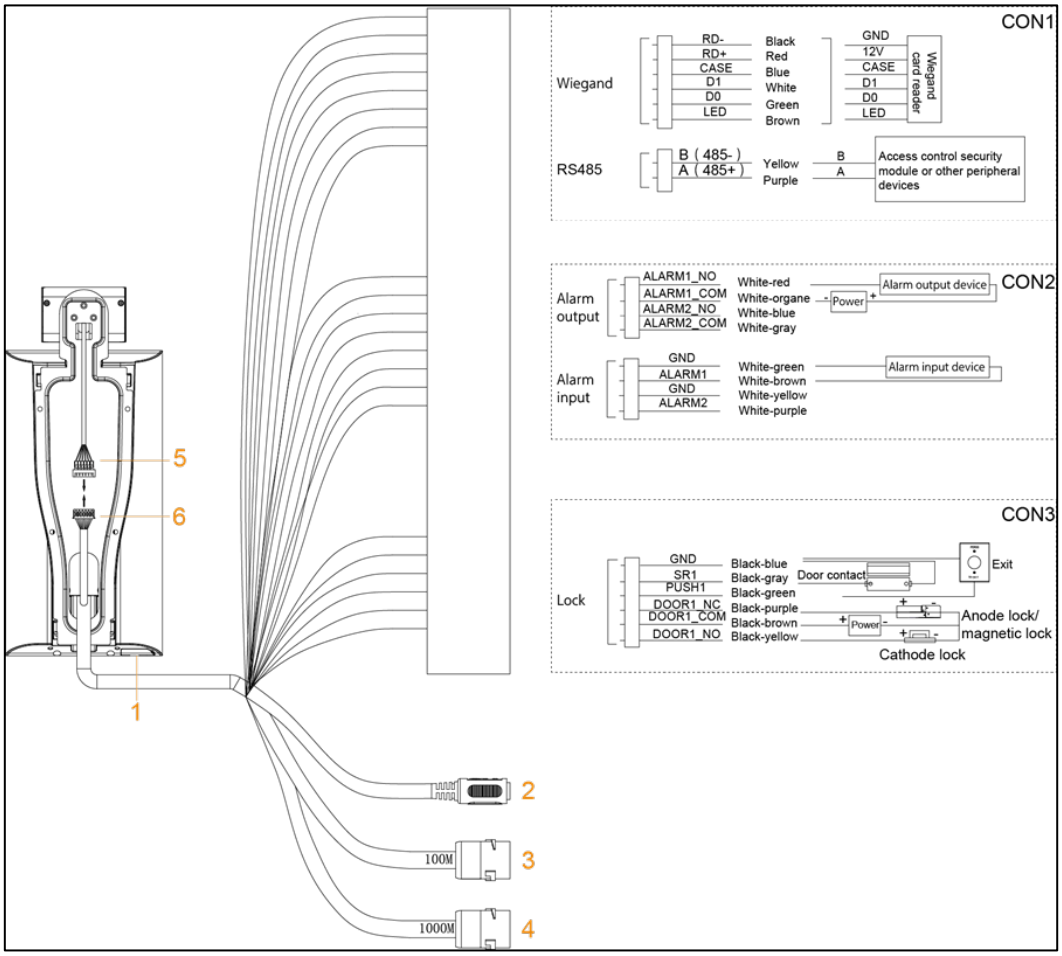
2 Installation

Important Installations Notes:

- If there is light source 0.50 m (1.64 ft) away from the access controller, the minimum illumination should be no less than 100 lux.
- Install the station indoors, at least 3 m (9.84 ft) away from windows and doors, and 2 m (6.56 ft) away from lights.
- Avoid backlight and direct sunlight.

2.1 Cable Connections

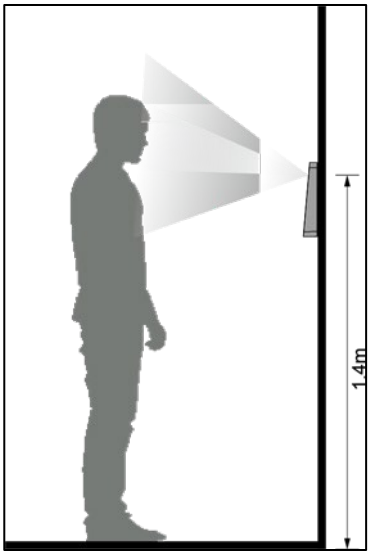
- Ensure the access control security module is enabled in Function > Security Module. If enabled, purchase the module separately. The security module needs separate power supply.
- Once the security module is enabled, the exit button, lock control, and firefighting links are disabled.



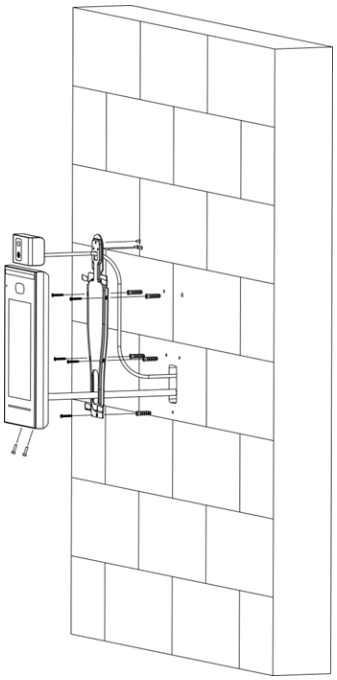
Ref.	Description	Ref.	
1	USB Port	4	1000 Mbps Network Port
2	Power Input	5,6	Port and Connector for Station
3	100 Mbps Network Port		

2.2 Mounting the Station

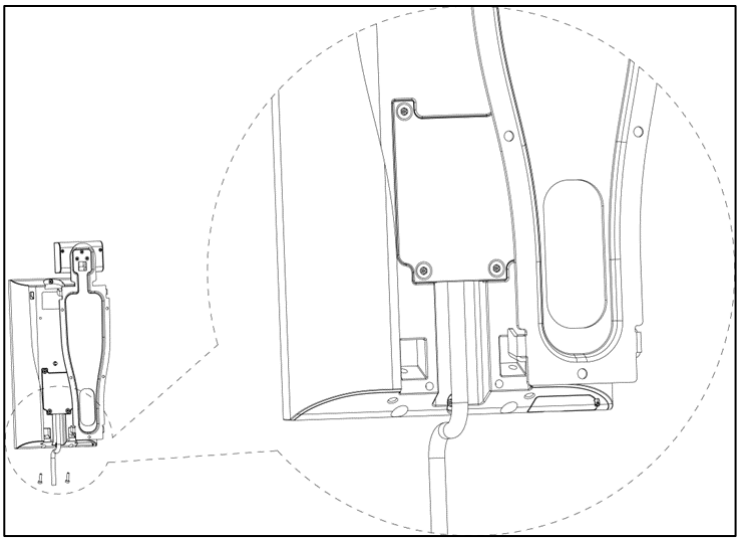
1. Mark a spot on the wall that is at least 1.40 m (4.59 ft) above the ground to mount the station.



2. Attach the station to the bracket with three (3) screws.
3. Drill six (6) holes (5 for the bracket and 1 for cable entry) in the wall using the bracket as a guide.
4. Install an expansion screw into each hole, and then affix the bracket to the wall using five (5) screws.



5. Make the cable connections. Refer to Section 2.1, Cable Connections, for more information.
6. Attach the station to the bracket hook.
7. Tighten the screws at the bottom of the station.
8. Apply silicon sealant to the cable outlet on the bottom of the station.



3 System Operations

3.1 Initializing the Station

Set the station's administrator password and supply a valid email address after the station is turned on.

- Reset the administrator password via the email address entered during initialization.
- The password must consist of 8 to 32 non-blank characters and contain at least two of the following types of characters: upper case, lower case, number, and special characters (excluding ' " ; : &).
- For access controller without touch screen, initialize through the web interface. See the user manual for details.

3.2 Adding New Users

Add new users by entering user IDs, names, importing fingerprints, face images, passwords, and selecting user levels.

1. Select **User -> New User** to start.
2. Configure the parameters, using the table below.
3. Tap the Check Icon to save the configuration.

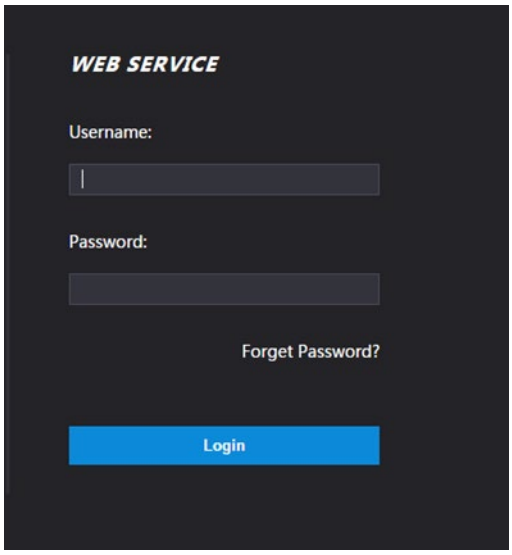
Parameter	Description
User ID	The ID consists of 32 characters (including numbers and letters). Each ID must be unique.
Name	Enter a name for the user (no more than 32 characters).
Face	Center the face in the frame. Once centered the station takes a picture of the face. Refer to for details about face image recording.
Card	Register a card for the user. Register up to five (5) cards per user. Enter the card number or swipe the card to associate with the user. Additionally, enable the Duress function for a card on the interface.
PWD	Enter a password for the user to use to unlock a door connected to the station. The maximum length of the password is eight (8) characters.
Level	Select one of the following access levels for the user: ● User: Users only have door unlock permission. ● Admin: Administrators can unlock the door and configure parameters.
Period	Enter the time range when a user can unlock the door.
Holiday Plan	Set dates and times during holiday periods when a user can unlock the door.
Valid Date	Set the date range when a user can unlock the door.
User Level	Select from one of six levels: ● General: User can unlock the door. ● Blacklist: A user on the blacklist triggers an alarm when accessing the door. ● Guest: Guests can unlock the door at certain times in certain periods. ● Patrol: Patrolling user's attendance is tracked, but they cannot unlock the door. ● VIP: VIP users trigger a prompt to management when they unlock a door. ● Special: Special users are granted a delay of five (5) seconds before the door is closed.
Use Time	Set the maximum number of times that a Guest user can unlock the door.

4 Web Operations

Configure the station and operations via the web interface. Set parameters including network parameters, video parameters, and access controller parameters; maintain and update the system. For details, see the user manual.

Note: Set a password and an email address before logging in to the web interface for the first time.

1. Open an Internet Explorer browser instance.
2. Type the station's IP address in the address bar and then press Enter key.
   - Ensure the computer and the station are on the same LAN.
   - The station has dual NICs with the following default IP addresses:
     - 1000 Mbps network: 192.168.1.108
     - 100 Mbps network: 192.168.2.108



3. Enter the Username and Password.
   - The default Username is "admin." Use the Password set during the initialization process.
   - Click Forgot Password to reset the administrator's password.
4. Click Login.

5 Appendix: Face Recording

Note: The face recording and facial recognition features may not be available on certain Thermal Temperature Station devices.

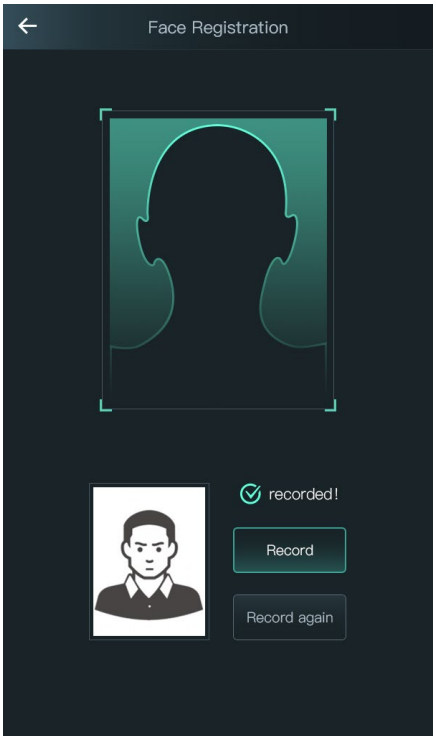
5.1 Prior to Face Registration

Instruct personnel that:

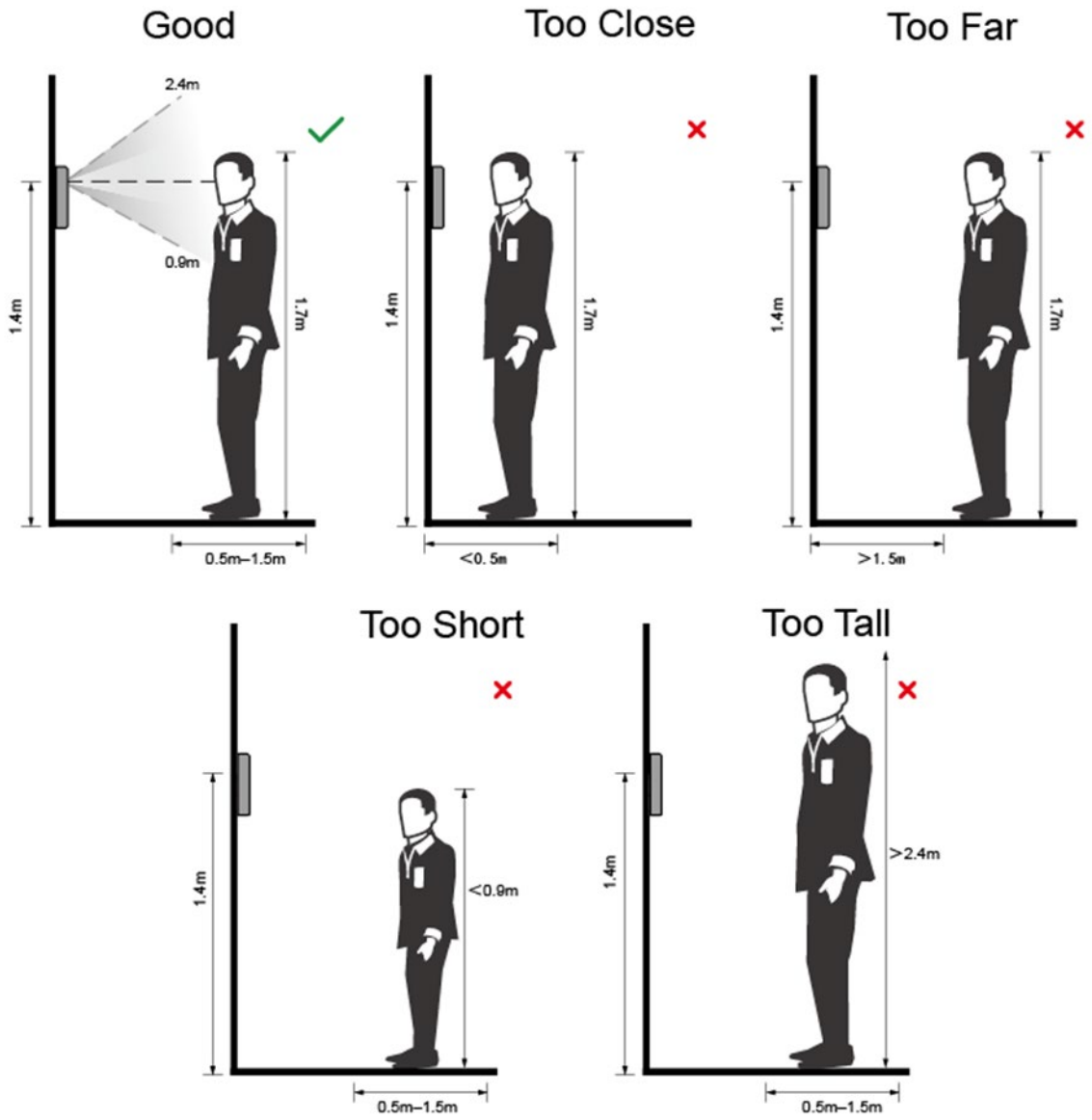
- Glasses, hats, and beards may influence face recognition performance.
- Do not cover eyebrows when wearing hats.
- Instruct personnel with beards that removing their beard or drastically changing can affect facial recognition and the station may not recognize the user.
- Keep their face clean.

5.2 During Registration

- Keep the device at least 2 m (6.56 ft) away from a light source and at least 3 m (9.84 ft) away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the device.
- Register faces through the station or through the platform. For registration through the platform, see the platform user manual.
- Keep the head and body still.
- Avoid multiple faces in the capture frame at one time.
- Center the face in the photo capture frame. The station automatically captures the face once it detects a centered face.

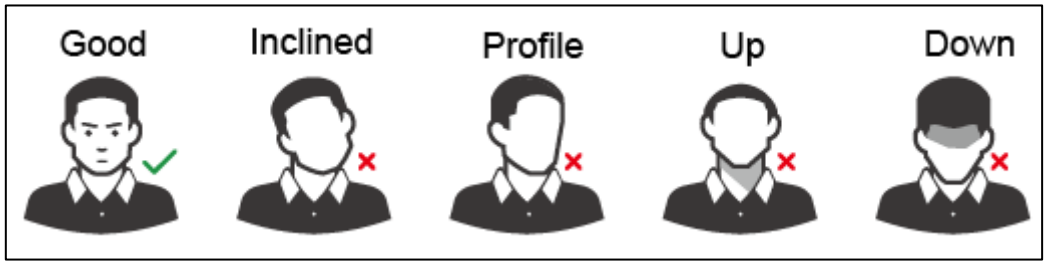


5.3 Face Position

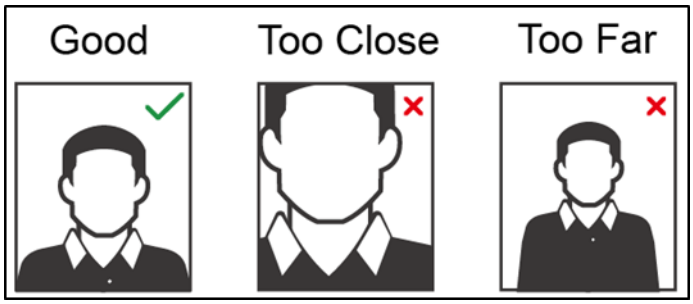


5.4 Requirements for a Good Face Capture

- Make sure that the face is clean and that the forehead is not covered by hair.
- Instruct the subject to remove glasses, hats, or other facial ornamentation that could influence the capture.
- Make sure that face does not take 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.
- Ensure the subject's eyes are open, assumes a neutral facial expressions, and is facing the camera.



- Ensure the face is at an optimal distance from the camera.



- After a successful capture, check the following:
  - Image resolution is within the range of 150 x 300 to 600 x 1200.
  - Image pixels are more than 500 x 500.
  - Image size is less than 75 KB.
  - Name and ID associated with the image are correct.

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