Face Recognition Terminal (with Temperature Monitoring Unit)

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Face Recognition Access Terminal (hereinafter referred to as the "Access Terminal"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ 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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First Release.	December 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Access Terminal, hazard prevention, and prevention of property damage. Read carefully before using the Access Terminal, and comply with the guidelines when using it.

Transportation Requirement

⚠

Transport, use and store the Access Terminal under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Access Terminal under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Access Terminal while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Access Controller.
- Do not connect the Access Terminal to two or more kinds of power supplies, to avoid damage to the Access Terminal.
- Improper use of the battery might result in a fire or explosion.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Access Terminal in a place exposed to sunlight or near heat sources.
- Keep the Access Terminal away from dampness, dust, and soot.
- Install the Access Terminal on a stable surface to prevent it from falling.
- Install the Access Terminal in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the Access Terminal label.
- The Access Terminal is a class I electrical appliance. Make sure that the power supply of the Access Terminal is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Access Terminal while the adapter is powered on.
- Operate the Access Terminal within the rated range of power input and output.

- Use the Access Terminal under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Terminal, and make sure that there is no object filled with liquid on the Access Terminal to prevent liquid from flowing into it.
- Do not disassemble the Access Terminal without professional instruction.

Table of Contents

1 Structure

The Face Recognition Access Terminal has 2 types of models, which are model X and model Y. The front appearance might differ depending on different models of the Access Terminal.

Model X

Figure 1-1 Dimensions of Model X (unit: mm[inch])

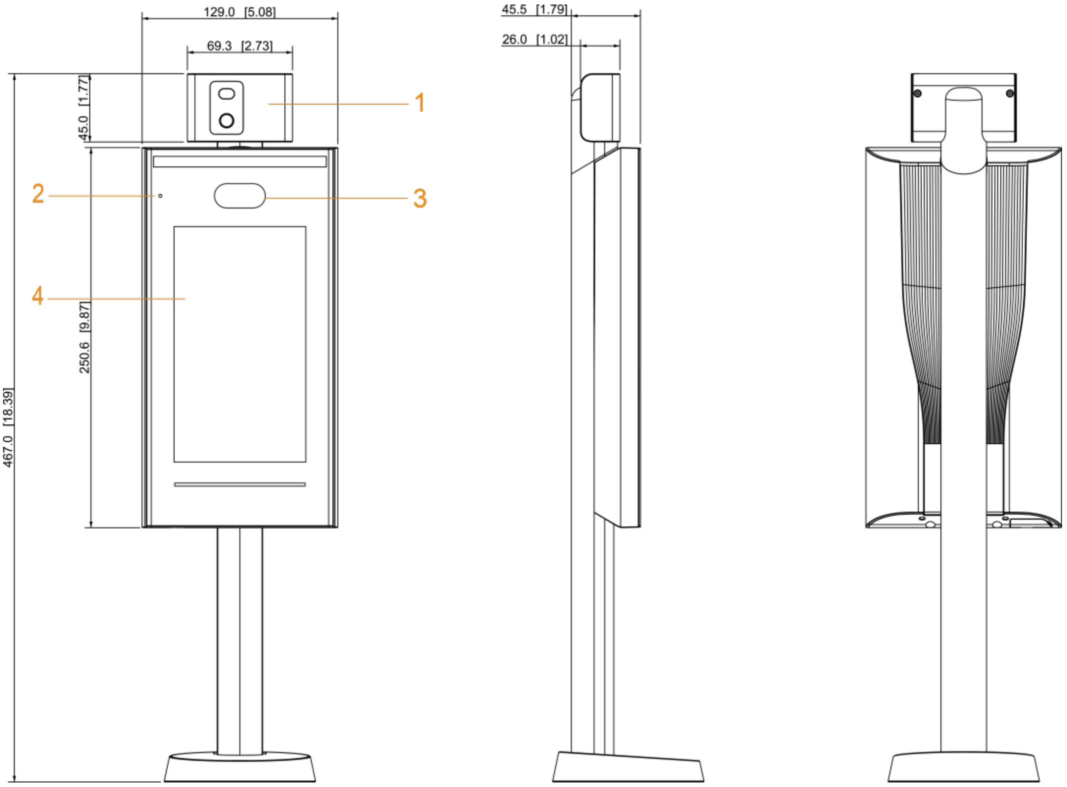
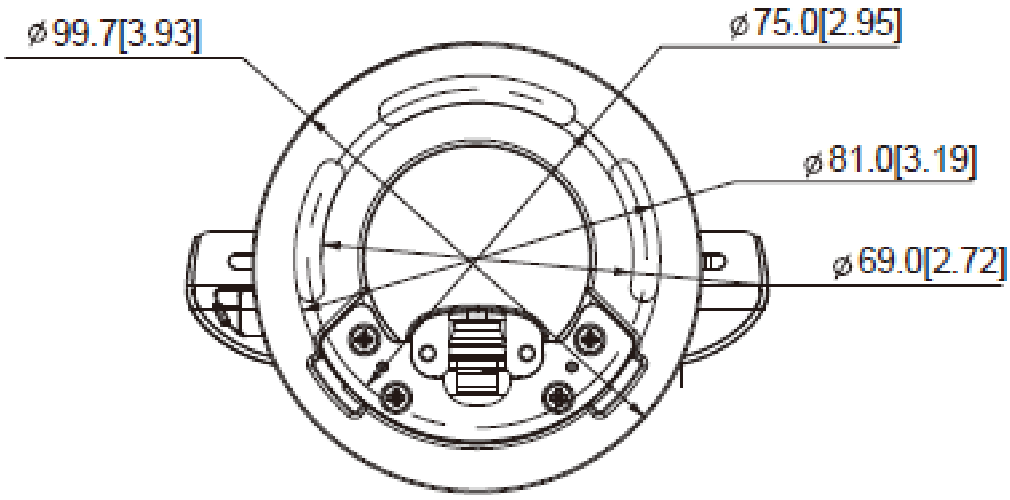


Figure 1-2 Bottom view of model X



Model Y

Figure 1-3 Model Y (unit: mm[inch])

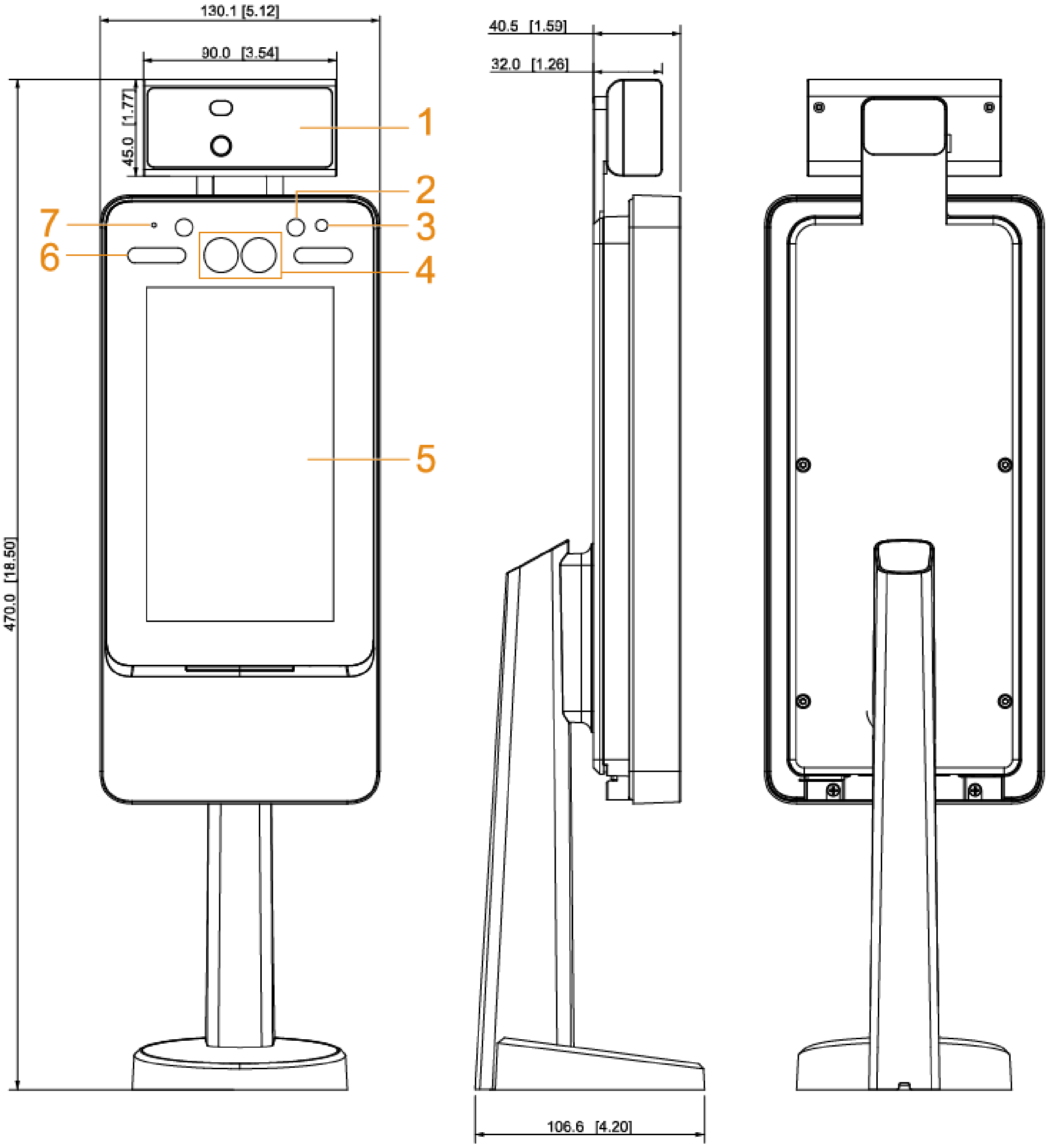
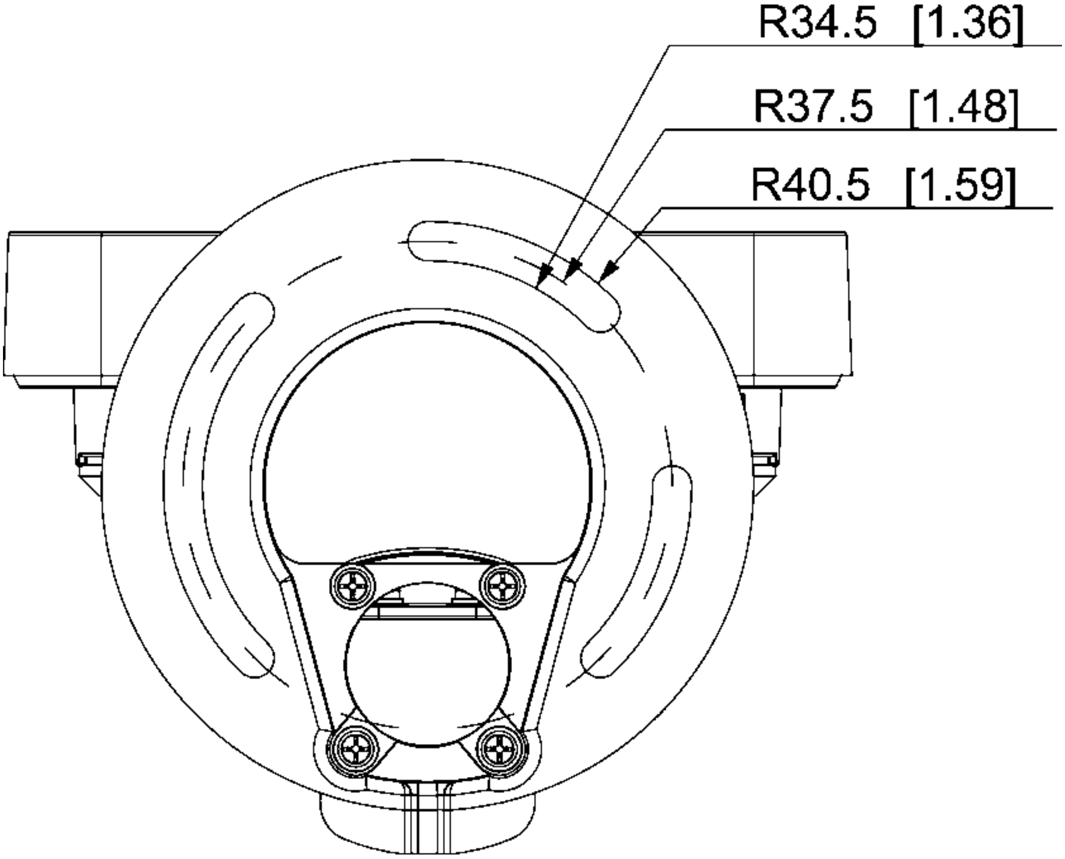


Table 1-2 Component description

No.	Parameters
1	Temperature monitoring unit
2	IR light
3	Phototransistor
4	Dual cameras
5	Display
6	White LED illuminator
7	MIC

Figure 1-4 Bottom view of model Y

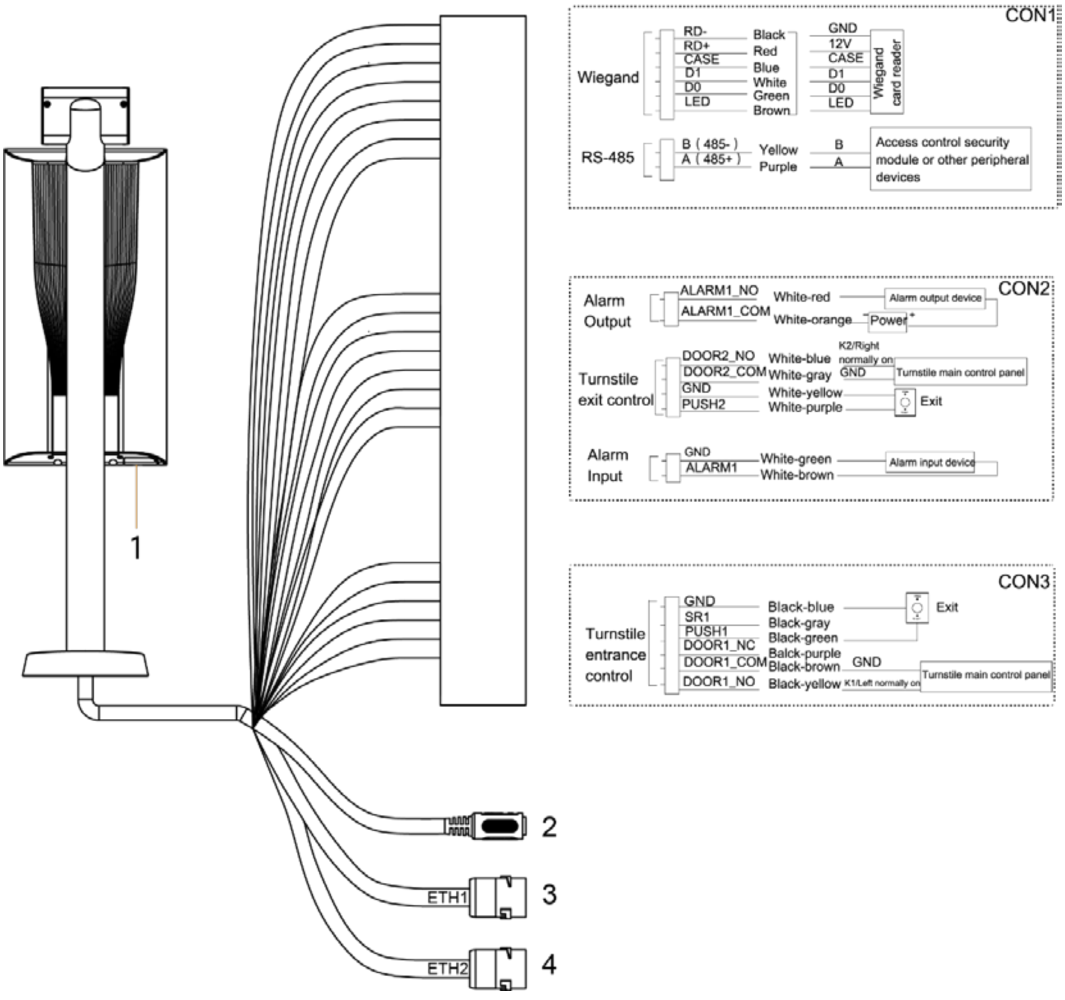


2 Connection and Installation

2.1 Wiring

The wiring of model X and model Y is almost the same. Ports might differ depending on models of the product. This section uses the model X as an example.

Figure 2-1 Wring of model X



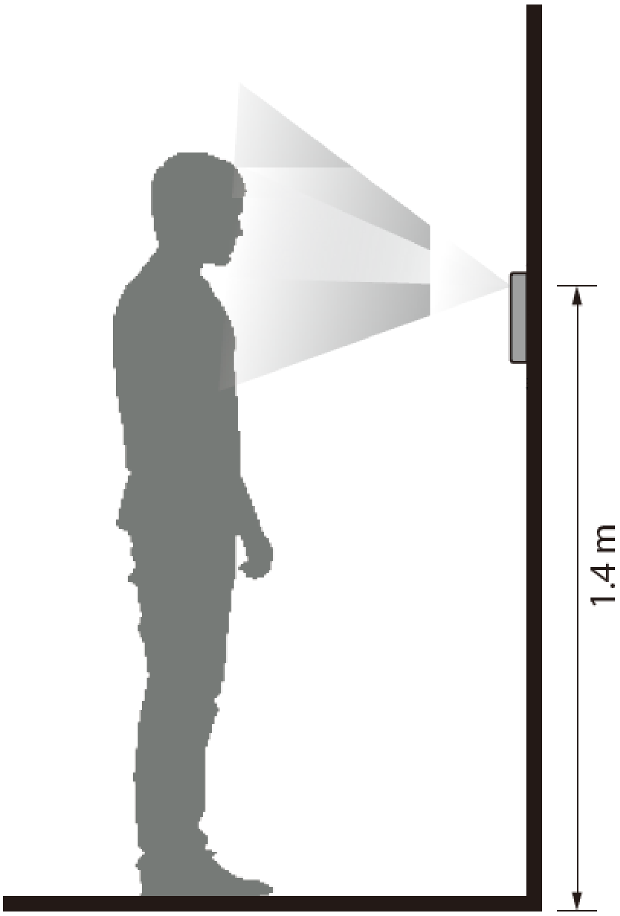
- If you want to connect a security module, a security module needs to be purchased separately by customers. The security module needs a separate power supply.
- When the security module function is turned on, the exit button, lock and alarm linkage door opening are not effective.

2.2 Installation Requirements

- The recommended installation height (from the lens to ground) is 1.4 m.
- The light at the 0.5 meters away from the Access Terminal should be no less than 100 Lux.
- We recommend you install the Access Terminal indoors, at least 3 meters away from windows and doors, and 2 meters away from the light source.
- Avoid backlight, direct sunlight, close light, and oblique light.

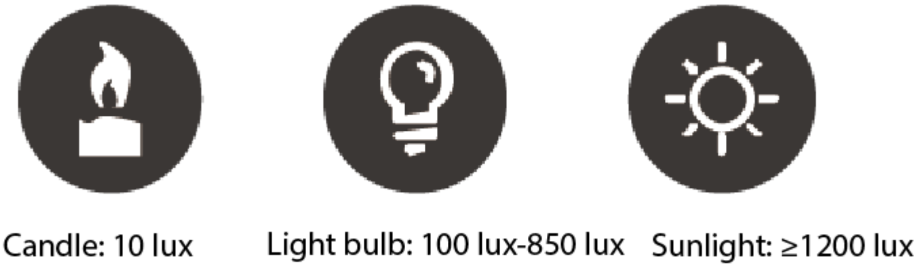
Installation Height

Figure 2-2 Installation height requirement



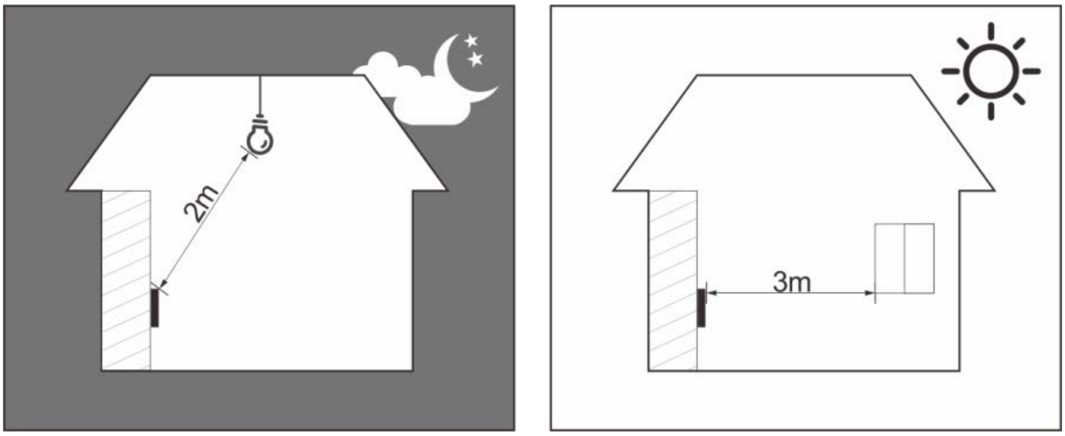
Ambient Illumination Requirements

Figure 2-3 Ambient illumination requirements



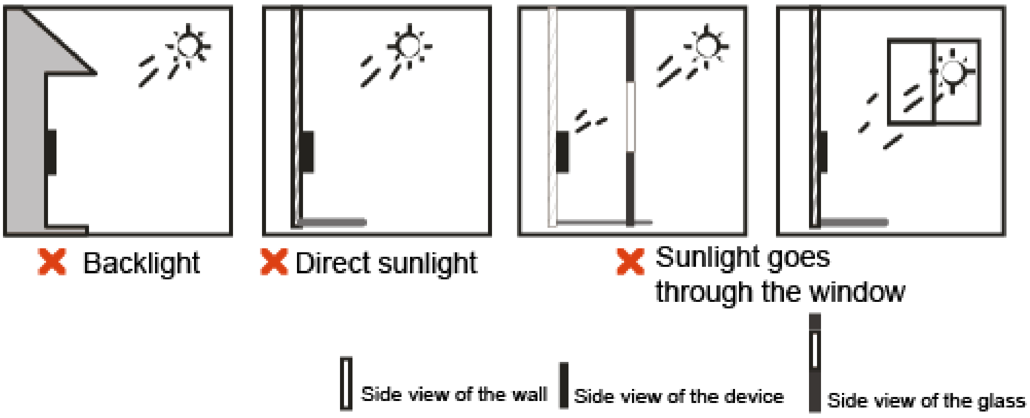
Recommended Installation Location

Figure 2-4 Recommended installation location



Installation Location Not Recommended

Figure 2-5 Installation location not recommended



2.3 Installation Procedure

The Installation procedure of model X and model Y is almost the same. This section uses model X as an example.

Step 1 Thread the wires of the Access Terminal through the turnstile.

Step 2 Put the waterproof silica gel plug on the cable.

Step 3 Fix the Access Terminal to the turnstile with M5 screws.

Figure 2-6 Fix the Access Terminal to the turnstile

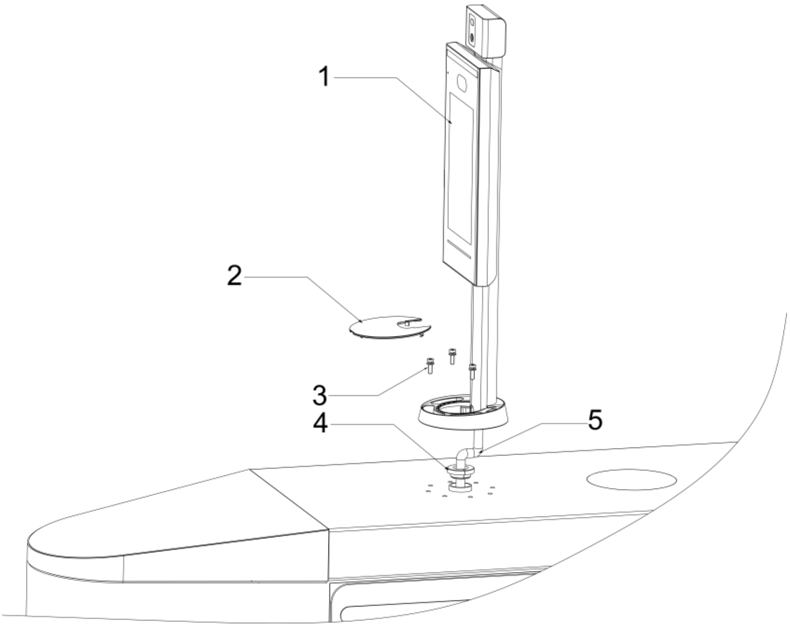


Table 2-2 Component description

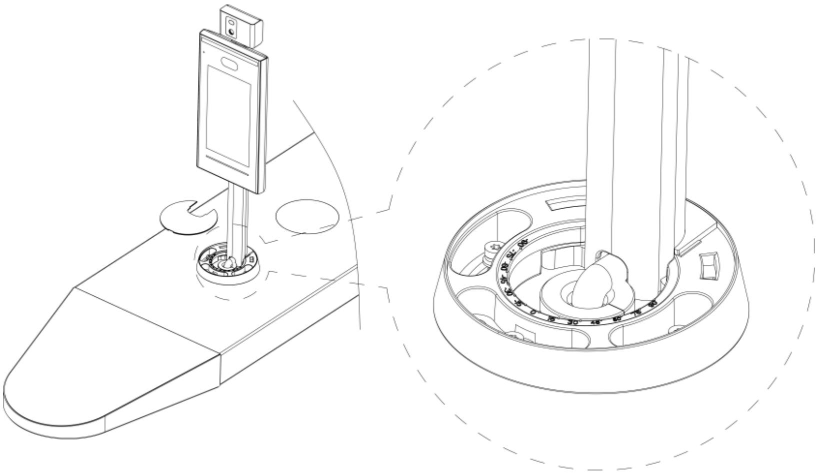
No.	Name
1	Screen
2	Cover
3	M5 screw
4	Cable
5	Waterproof silica gel plug

Step 4 Wire the Access Terminal. For details, see "2.1 Wiring".

Step 5 Apply sealant to gaps between the waterproof silica gel plug and turnstile.

Step 6 Install the cover to the base of the Access Terminal.

Figure 2-7 Apply sealant



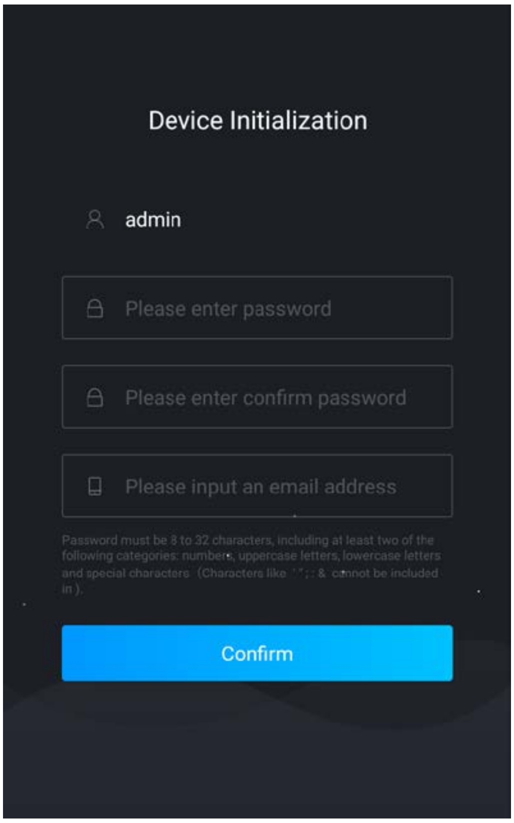
3 Local Configurations

Local operations might differ depending on different models of Access Terminal.

3.1 Initialization

For the first-time use or after restoring factory defaults, you need to set a password and email address for the admin account. You can use the admin account to log in to the main menu screen of the Access Terminal and its webpage.

Figure 3-1 Initialization



Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

- If you forget the administrator password, send a reset request to your linked e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

3.2 Adding New Users

You can add new users, view user/admin list and edit user information.

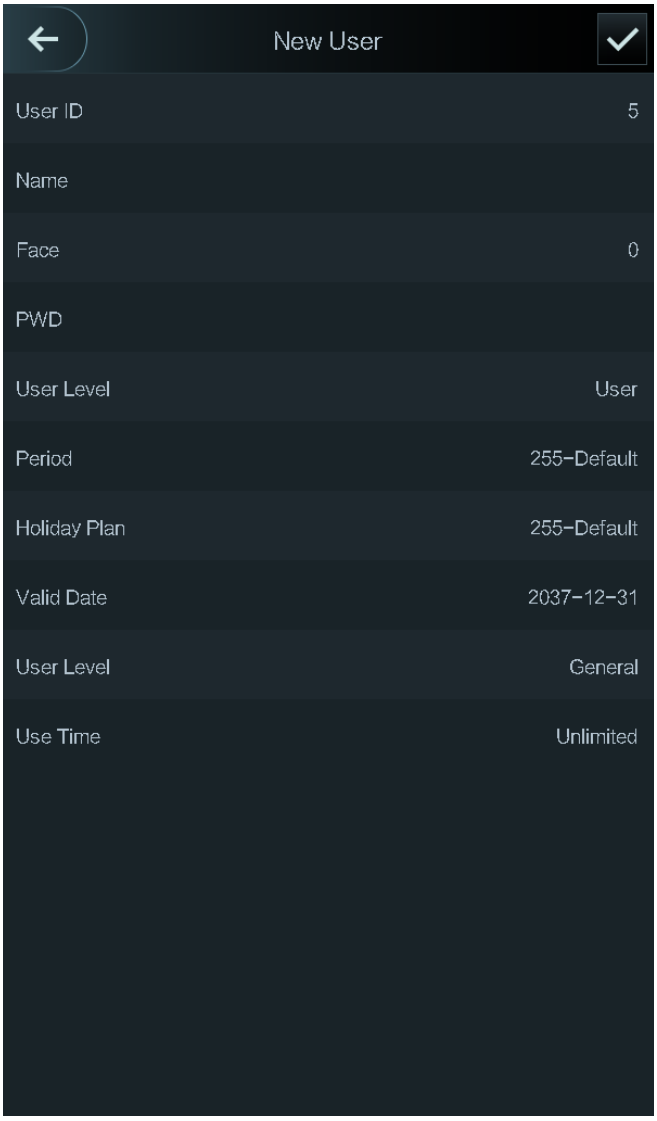
The pictures in this manual are for reference only, and might differ from the actual product.

Step 1 On the **Main Menu**, select **User** > **New User**.

Step 2 Configure the parameters.

The parameters of new users might differ depending on the models of the product.

Figure 3-2 New user



New User

User ID	5
Name	
Face	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

Table 3-1 Description of new user parameters

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter name with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the image capturing frame, and an image of the face will be captured and analyzed automatically.
PWD	Enter the user password. The maximum length of the password is 8 digits.
User Level	You can select a user level for new users. ● **User**: Users only have door access permission. ● **Admin**: Administrators can unlock the door and configure the access terminal.

Parameter	Description
Period	People can unlock the door only during the defined period.
Holiday Plan	People can unlock the door only during the defined holiday plan.
Valid Date	Set a date on which the access permissions of the person will be expired.
User Level	● **General**: General users can unlock the door. ● **Blocklist**: When users in the blocklist unlock the door, service personnel will receive a notification. ● **Guest**: Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● **Patrol**: Patrol users will have their attendance tracked, but they have no unlocking permissions. ● **VIP**: When VIP unlock the door, service personnel will receive a notice. ● **Special**: When they unlock the door, the door will stay unlocked for 5 more seconds.
Use Time	When the user level is set to guest, you can set the maximum number of times that the user can unlock the door.

Step 3 Tap ☑ to save the configuration.

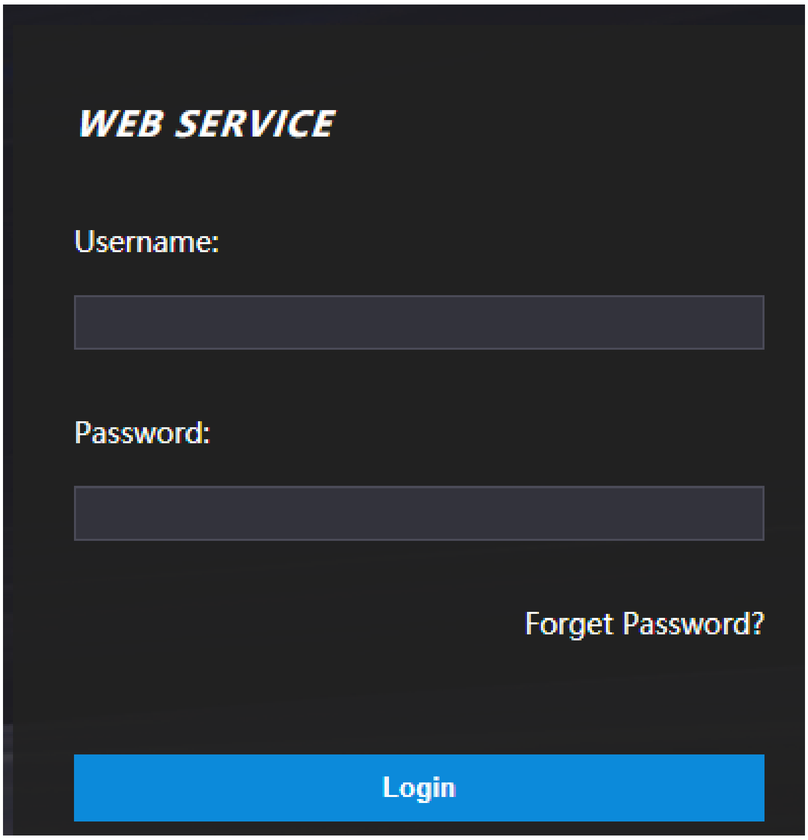
4 Logging In to the Webpage

On the webpage, you can also configure and update the Access Terminal.

- Web configurations differ depending on models of the Access Terminal.
- Make sure that the computer used to log in to the webpage is on the same LAN as the Access Terminal.

Step 1 Open a browser, enter the IP address of the Access Terminal in the Address bar, and press the Enter key.

Figure 4-1 Login



Step 2 Enter the user name and password.

- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?**

Step 3 Click **Login**.

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Access Terminal; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Access Terminal at least two meters away from light source and at least three meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access terminal.

During Registration

- You can register faces through the Access Terminal or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

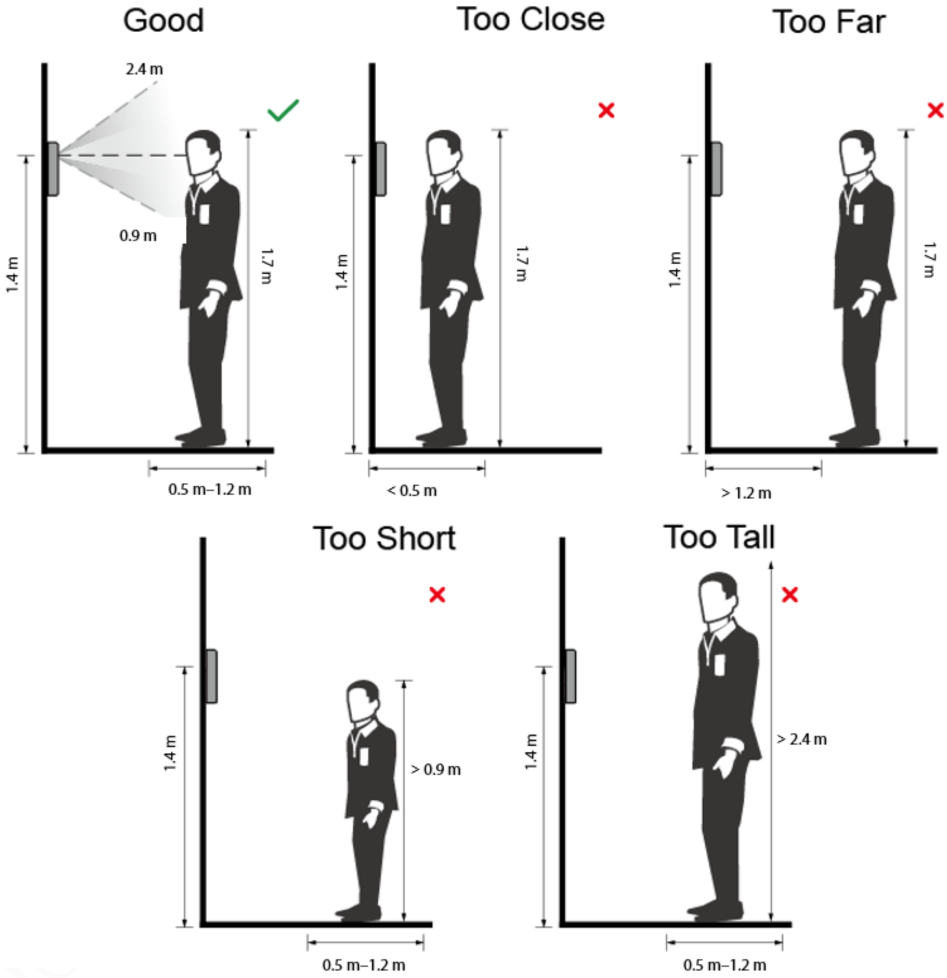
📖

- Do not shake your head or body, otherwise the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

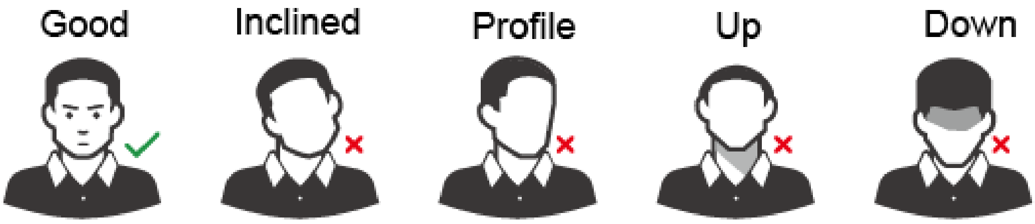
Appendix Figure 1-1 Appropriate face position



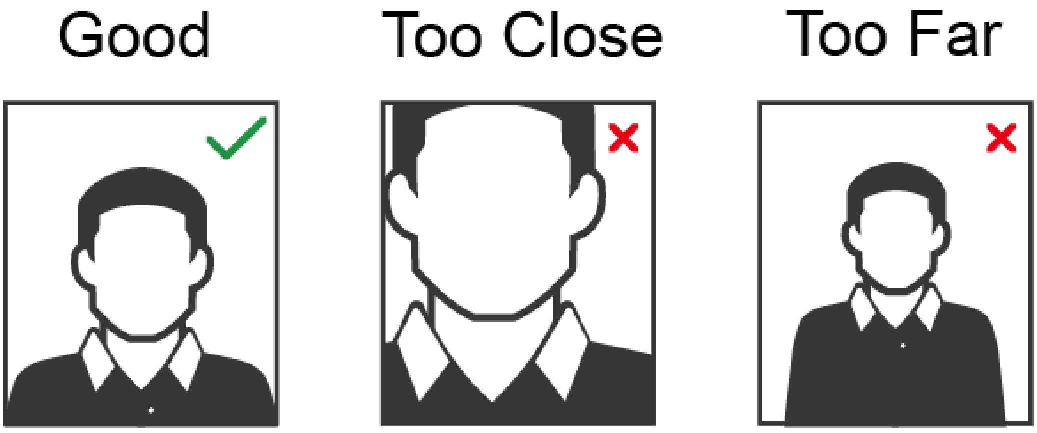
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300 pixels–600 × 1200 pixels; image pixels are more than 500 × 500 pixels; image size is less than 100 KB, and image name and person ID are the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, 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.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you 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 mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.