Face Recognition Terminal

User’s Manual

V1.0.0

Foreword

General

This manual introduces the installation and basic operation of the Face Recognition Terminal (hereinafter referred to as "terminal").

Safety Instructions

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

Signal Words	Meaning
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First Release	September 2019

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual 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.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operation Requirement

- Do not place or install the terminal in a place exposed to sunlight or near the heat source.
- Keep the terminal away from dampness, dust or soot.
- Keep the terminal installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the terminal, and make sure there is no object filled with liquid on the terminal to prevent liquid from flowing into the terminal.
- Install the terminal in a well-ventilated place, and do not block the ventilation of the terminal.
- Operate the terminal within the rated range of power input and output.
- Do not dissemble the terminal.
- Transport, use and store the terminal under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the terminal; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (type-I structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword I
Important Safeguards and Warnings II
1 Overview 1
1.1 Introduction 1
1.2 Features 1
1.3 Dimension and Component 2
2 Installation 5
2.1 Installation Notes 5
2.2 Installation Drawings 6
2.3 Cable Connections 7
2.4 Installation 9
3 System Operation 11
3.1 Initialization 11
3.2 Standby Interface 11
3.3 Unlocking Methods 12
3.3.1 Face 12
3.3.2 User Passwords 12
3.3.3 Administrator Password 13
3.4 Main Menu 13
3.5 User Management 15
3.5.1 Adding New Users 15
3.5.2 Viewing User Information 17
3.6 Access Management 17
3.6.1 Period Management 17
3.6.2 Unlock 18
3.6.3 Alarm Configuration 21
3.6.4 Door Status 22
3.6.5 Lock Holding Time 22
3.7 Network Communication 22
3.7.1 IP Address 22
3.7.2 Serial Port Settings 24
3.7.3 Wiegand Configuration 24
3.8 System 25
3.8.1 Time 25
3.8.2 Face Parameter 26
3.8.3 Fill Light Mode Setting 27
3.8.4 Fill Light Brightness Setting 27
3.8.5 Volume Adjustment 27
3.8.6 IR Light Brightness Adjustment 27
3.8.7 Restore to Factory Settings 27
3.8.8 Reboot 27

3.9 USB 27
3.9.1 USB Export 28
3.9.2 USB Import 28
3.9.3 USB Update 29
3.9.4 Features 29
3.9.5 Result Feedback 32
3.10 Record 34
3.11 Auto Test 35
3.12 System Info 35
4 Web Operation 36
4.1 Initialization 36
4.1 Login 38
4.2 Resetting the Password 38
4.3 Alarm Linkage 40
4.3.1 Setting Alarm Linkage 40
4.3.2 Alarm Log 41
4.4 Data Capacity 42
4.5 Video Setting 42
4.5.1 Data Rate 43
4.5.2 Image 43
4.5.3 Exposure 45
4.5.4 Motion Detection 46
4.5.5 Volume Setting 47
4.5.6 Image Mode 47
4.6 Face Detect 48
4.7 Network Setting 49
4.7.1 TCP/IP 49
4.7.2 Port 50
4.7.3 Register 51
4.7.4 P2P 51
4.8 Safety Management 52
4.8.1 IP Authority 52
4.8.2 Systems 53
4.9 User Management 53
4.9.1 Adding Users 54
4.9.2 Modifying User Information 54
4.10 Maintenance 54
4.11 Configuration Management 54
4.11.1 Upgrade 55
4.11.2 Version Information 55
4.11.3 Online User 55
4.12 System Log 56
4.12.1 Querying Logs 56
4.12.2 Backing up Logs 56
4.13 Admin Log 56
4.14 Exit 57
5 SmartPSS Configuration 58

5.1 Login 58
5.2 Adding Devices 58
5.2.1 Auto Search 58
5.2.2 Manual Add 59
5.3 Adding Users 60
5.3.1 Card Type Selection 61
5.3.2 Adding One User 62
5.4 Adding Door Group 63
5.5 Access Permission Configuration 65
5.5.1 Giving Permission by Door Group 65
5.5.2 Giving Permission by User ID 67
Appendix 1 Notes of Face Recording/Comparison 69
Appendix 2 Cybersecurity Recommendations 73

1 Overview

1.1 Introduction

The terminal is an access control panel that supports unlock through faces, passwords, and supports unlock through their combinations.

1.2 Features

- Support face unlock and password unlock; unlock by period
- With face detection box; the largest face among faces that appear at the same time is recognized first; the maximum face size can be configured on the web
- 2MP wide-angle WDR lens; with auto/manual fill light
- Face-camera distance: 0.3 m–2.0 m; human height: 0.9 m–2.4 m
- With face recognition algorithm, the terminal can recognize more than 360 positions on human face
- Face verification accuracy>99.5%; low false recognition rate
- Support profile recognition; the profile angle is 0°–90°
- Support liveness detection
- Support duress alarm and tamper alarm
- Support general users, duress users, patrol users, blacklist users, VIP users, guest users, and special users
- Various unlock status display modes protect user privacy

1.3 Dimension and Component

7-Inch Terminal

Figure 1-1 Dimensions and components of model A (mm [inch])

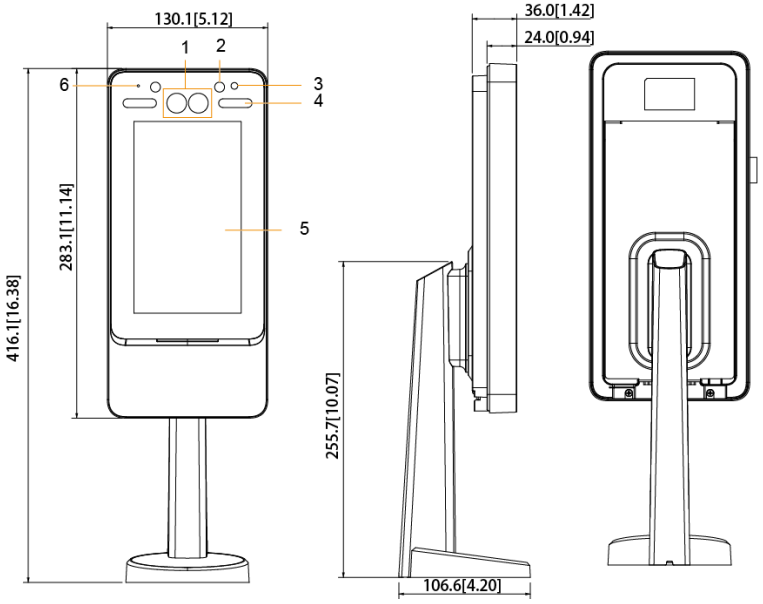


Table 1-1 Component description (1)

No.	Name
1	Dual camera
2	IR light
3	Phototransistor
4	White fill light
5	Display
6	MIC

Figure 1-2 Dimensions and components of model B (mm [inch])

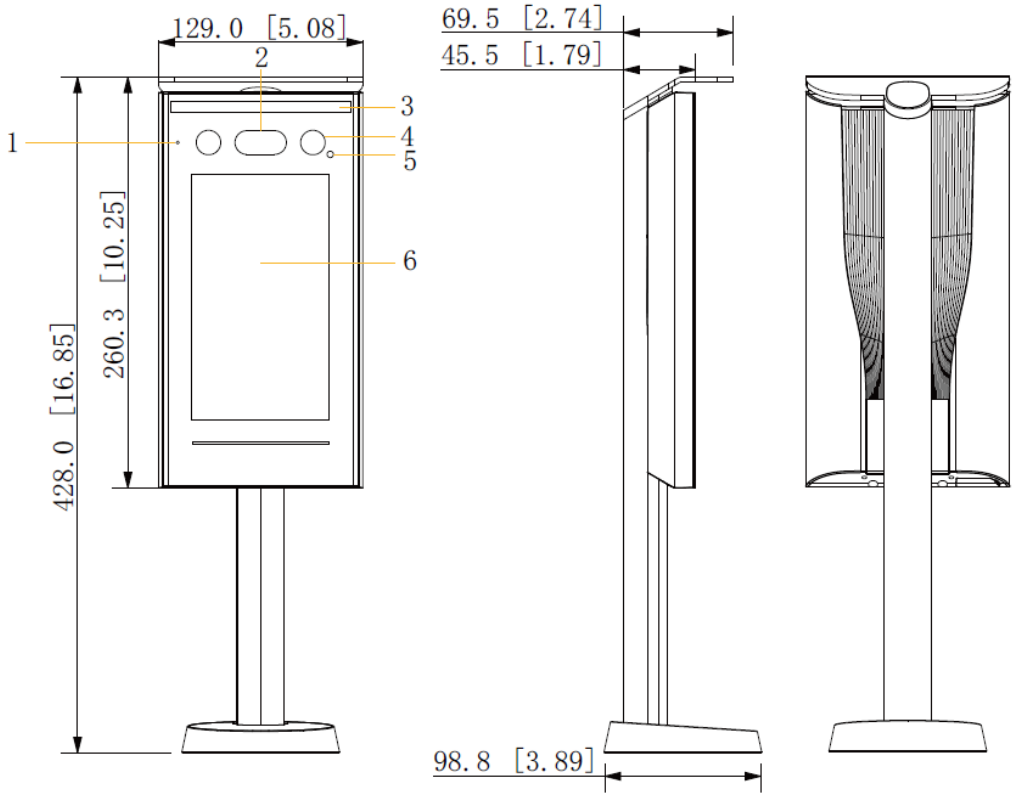


Table 1-2 Component description (2)

No.	Name
1	MIC
2	Dual camera
3	White fill light
4	IR light
5	Phototransistor
6	Display

10-Inch Terminal

Figure 1-3 Dimensions and components (mm [inch])

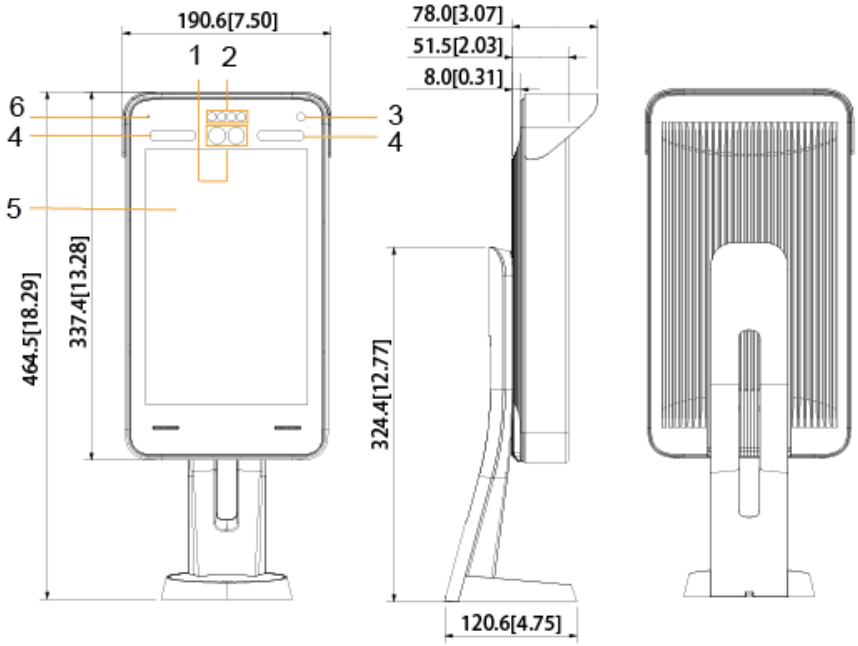


Table 1-3 Component description

No.	Name
1	Dual camera
2	IR light
3	Phototransistor
4	White fill light
5	Display
6	MIC

2 Installation

2.1 Installation Notes

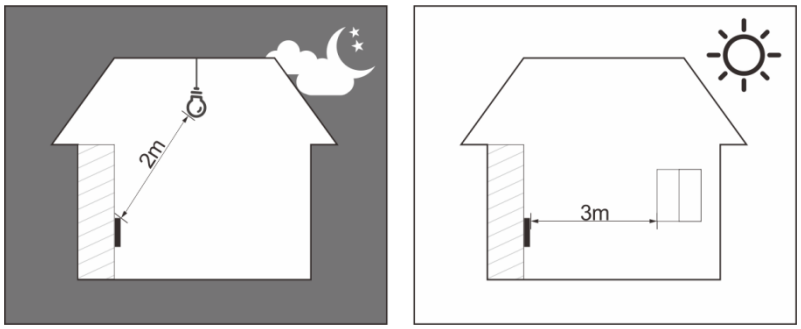
- If there is light source 0.5 meters away from the device, the minimum illumination should be no less than 100Lux.
- It is recommended that the device is installed indoors, at least 3 meters away from windows and doors and 2 meters away from lights.
- Avoid back light and direct sunlight.

Ambient Illumination Requirement

Figure 2-1 Ambient illumination requirement

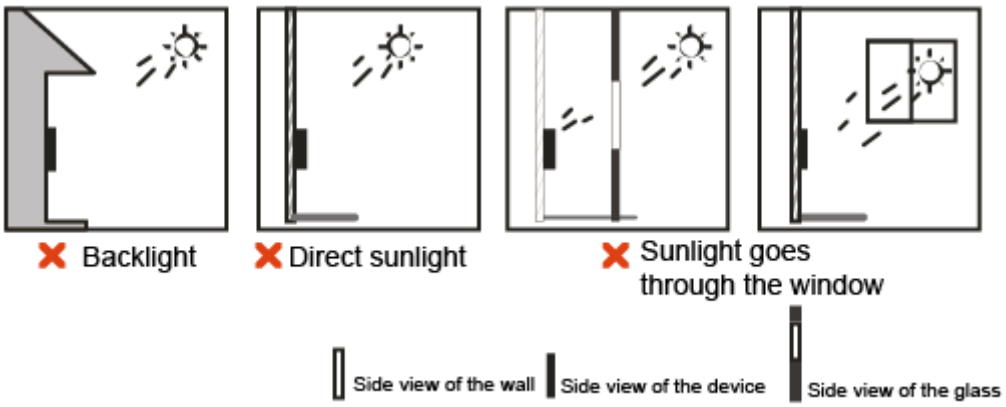
Places Recommended

Figure 2-2 Places recommended



Places Not Recommended

Figure 2-3 Places not recommended



2.2 Installation Drawings

7-Inch Terminal

Figure 2-4 Installation drawings of model A (mm[inch])

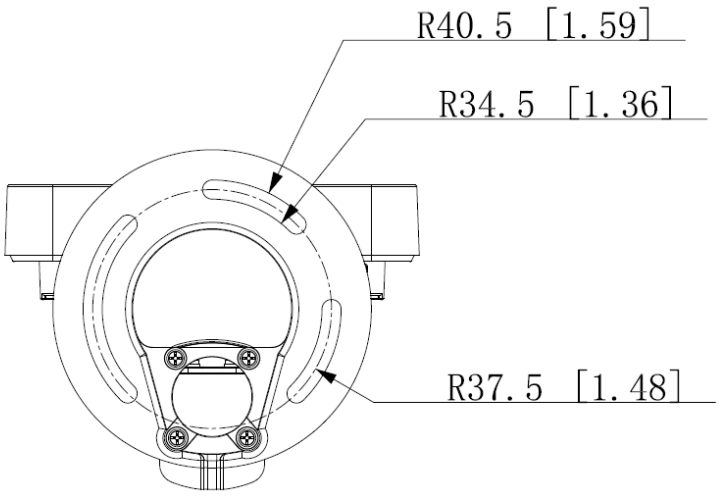
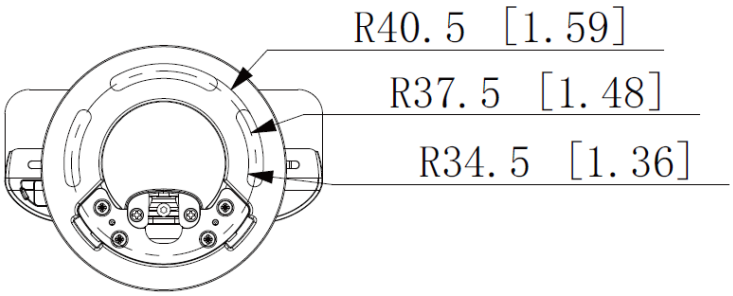
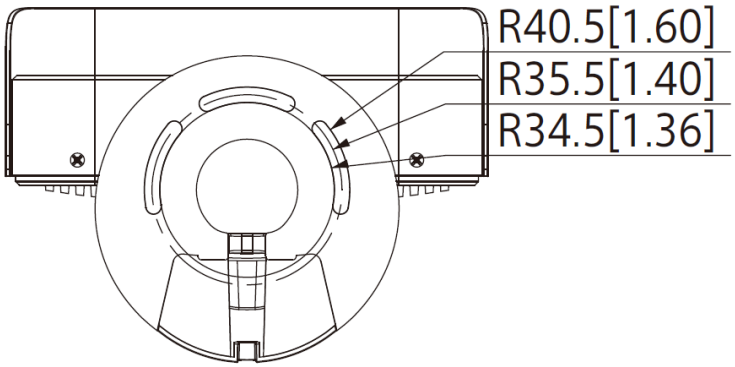


Figure 2-5 Installation drawings of model B (mm[inch])



10-Inch Terminal

Figure 2-6 Installation drawings (mm[inch])



2.3 Cable Connections

- Check if the access control security module is enabled in **Function > Security Module**. If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power.
- Once the security module is enabled, the exit button, turnstile control, and firefighting linkage will be invalid.

Cable connections are the same for all terminals. The 7-inch terminal will be taken as an example.

Figure 2-7 Cable connection

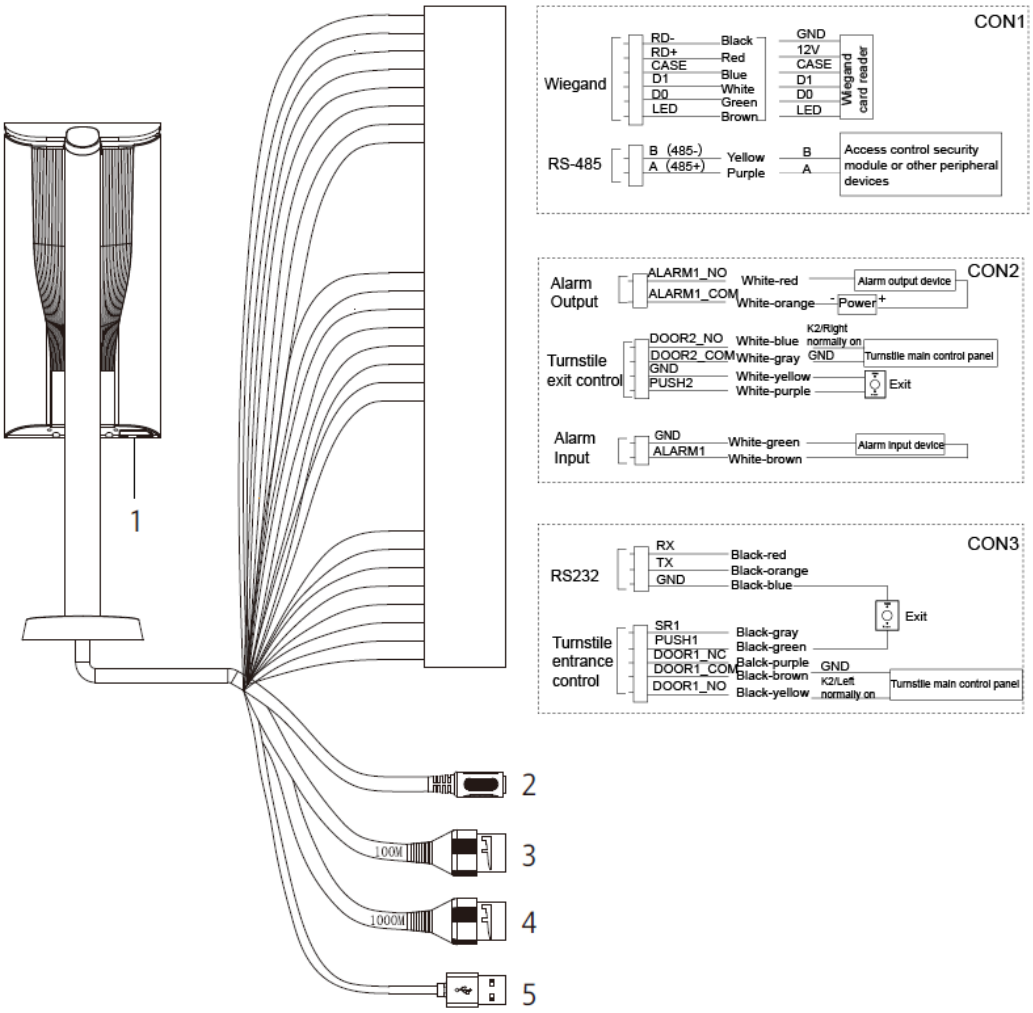


Table 2-1 Component description

No.	Name
1	USB port
2	Power port
3	Ethernet port
4	Ethernet port (only supported by 7-inch model B terminals)
5	USB port

2.4 Installation

Figure 2-8 Installation of the 7-inch model A terminal

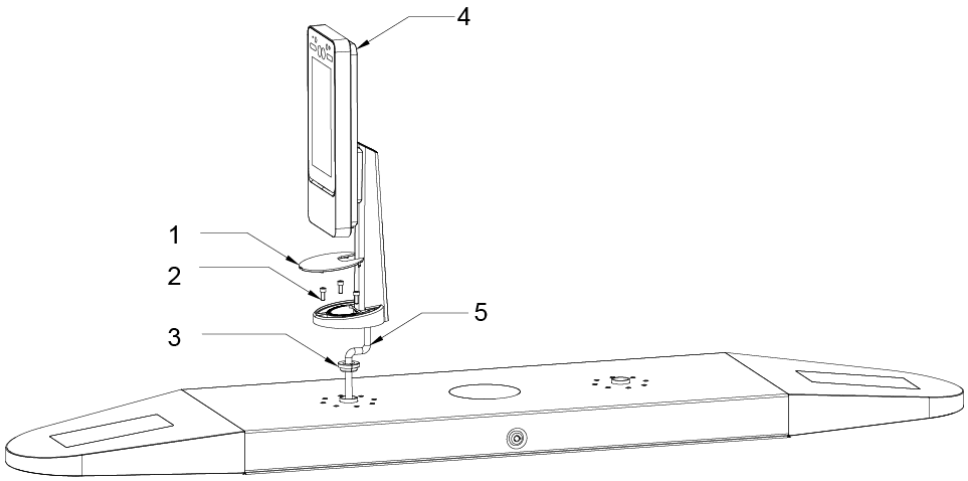


Figure 2-9 Applying silicon sealant to the 7-inch model B terminal

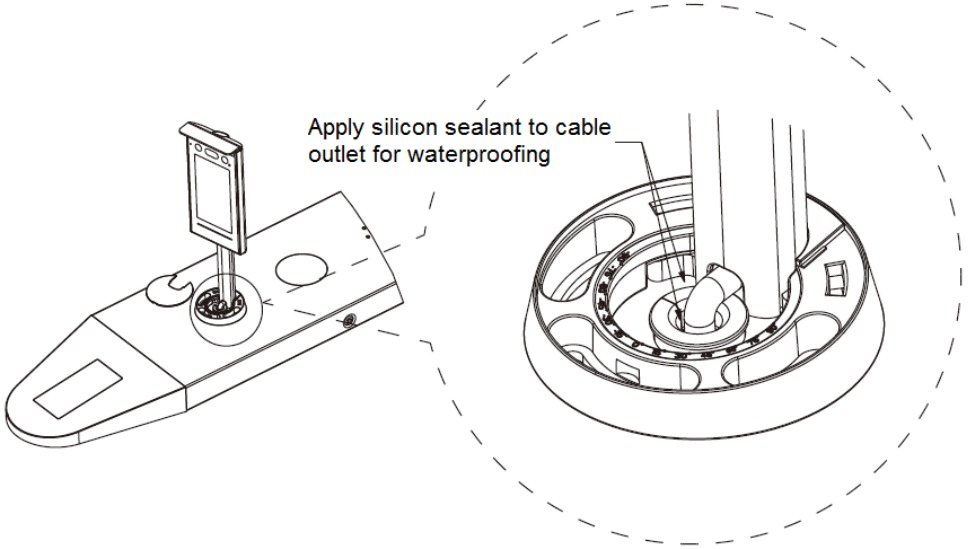


Figure 2-10 Installation of 10-inch terminals

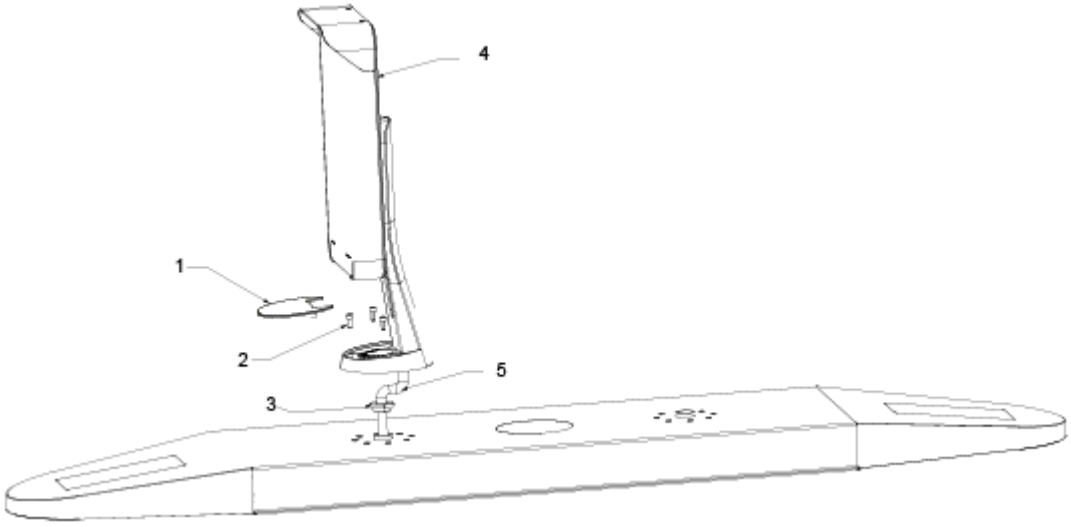


Figure 2-11 Applying silicon sealant to the 10-inch terminal

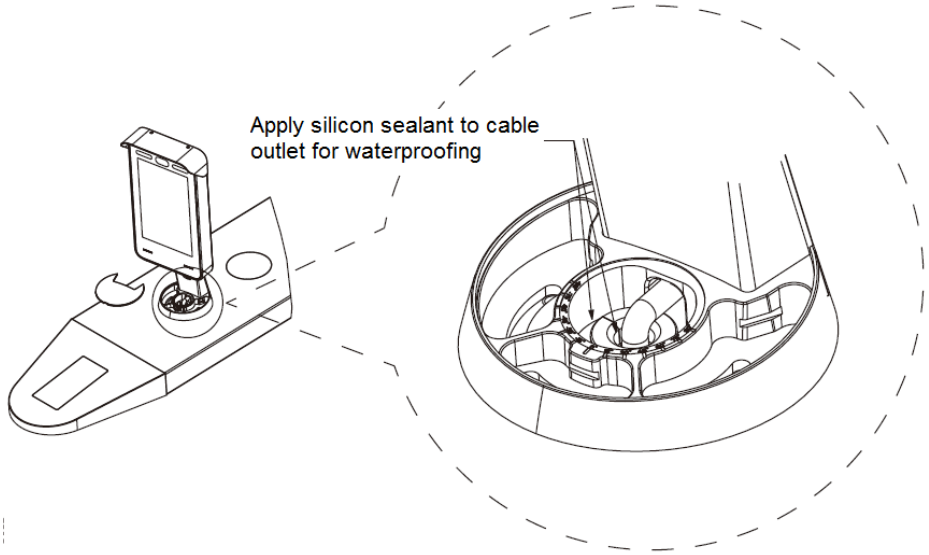


Table 2-2 Component description

No.	Name
1	Ornamental cover
2	M5 screw
3	Waterproof silica gel plug
4	Terminal
5	Cable

Installation Procedure

Step 1 Thread cable through the turnstile.

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

Step 3 Fix the terminal onto the turnstile with M5 screw.

Connect cables for terminal. See "2.3 Cable Connections."

Step 4 Apply sealant to gaps between the waterproof silica gel plug and turnstile. See Figure 2-9.

Step 5 Install the ornamental cover on the base of the terminal.

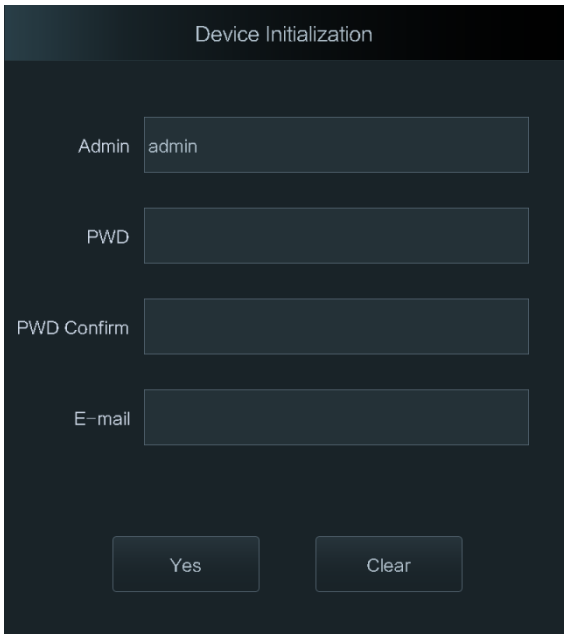
The installation is competed.

3 System Operation

3.1 Initialization

Administrator password and an email should be set the first time the terminal is turned on; otherwise the terminal cannot be used. See Figure 3-1.

Figure 3-1 Initialization



- Administrator and password set on this interface are used to log in to the web management platform.
- The administrator password can be reset through the email address you entered if the administrator forgets the administrator password.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

3.2 Standby Interface

You can unlock the door through faces, passwords, and QR code. See Table 3-1.

- If there are no operations in 30 seconds, the terminal will go to the standby mode.
- The following figures are for reference only, and the actual interface shall prevail.

Figure 3-2 Homepage

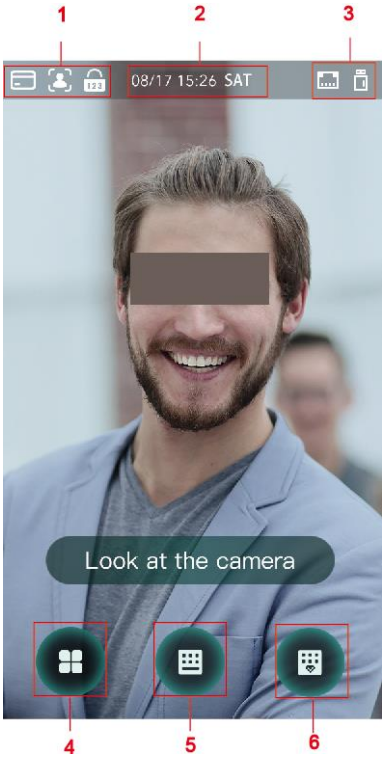


Table 3-1 Homepage description

No.	Description
1	Unlock methods: Card, face, and password.
2	Date & Time: Current date and time is displayed here.
3	Network status and battery status are displayed here.
4	Main menu icon. Only the administrator can enter the main menu.
5	Password unlock icon.
6	Administrator password unlock icon.

3.3 Unlocking Methods

You can unlock the door through face, passwords, and card.

3.3.1 Face

Make sure that your face is centered on the face recognition frame, and then you can unlock the door.

3.3.2 User Passwords

Enter the user passwords, and then you can unlock the door.

Step 1 Tap on the homepage.

Step 2 Enter the User ID, and then tap .

Step 3 Enter the User password, and then tap ☑.

The door is unlocked.

3.3.3 Administrator Password

Enter the administrator password, and then you can unlock the door. There is only one administrator password for one terminal. The administrator password can unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback.

Administrator password cannot be used when NC is selected at "NC Period."

Step 1 Tap on the homepage.

Step 2 Tap **Please Enter Administrator PWD**.

Step 3 Enter the administrator password, and then tap ☑.

The door is unlocked.

3.4 Main Menu

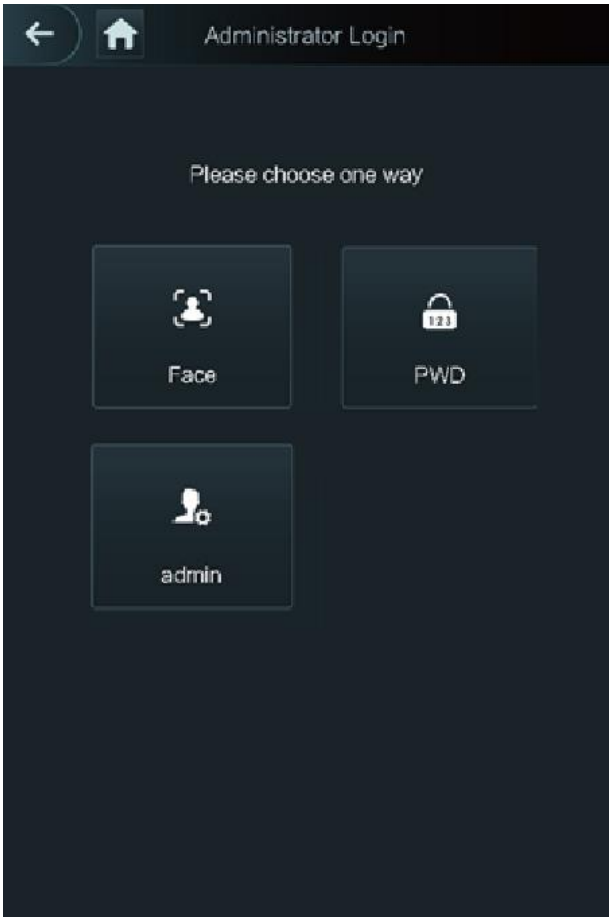
Administrators can add users of different levels, set access-related parameters, do network configuration, view access records and system information, and more in the main menu.

Step 1 Tap on the standby interface.

The **Administrator Login** interface is displayed.

Different modes support different unlock methods, and the actual interface shall prevail.

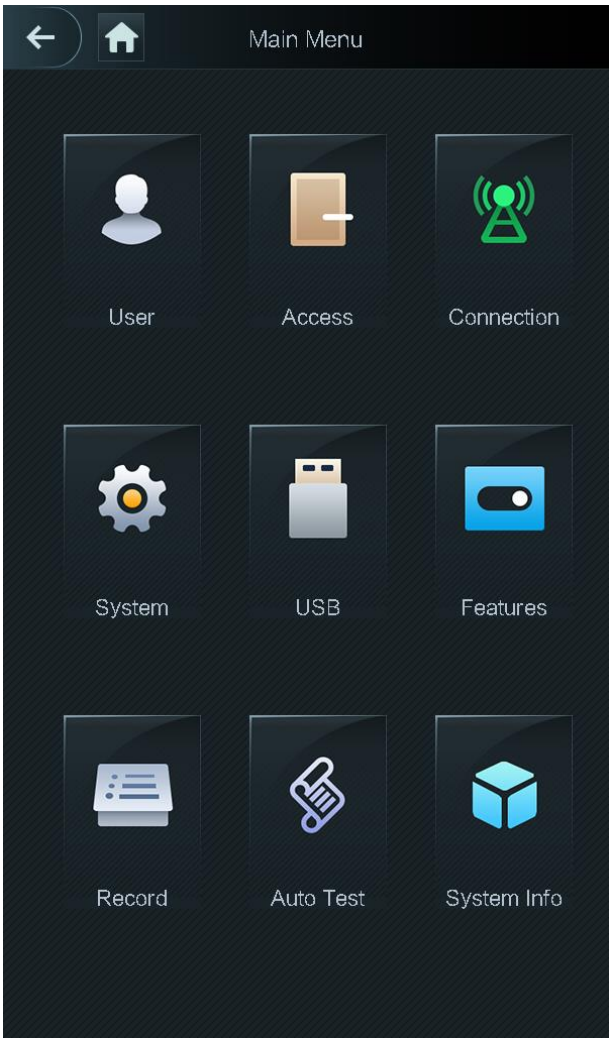
Figure 3-3 Administrator login



Step 2 Select a main menu entering method.

The main menu interface is displayed.

Figure 3-4 Main Menu



3.5 User Management

You can add new users, view user lists, admin lists, and modify the administrator password on the User interface.

3.5.1 Adding New Users

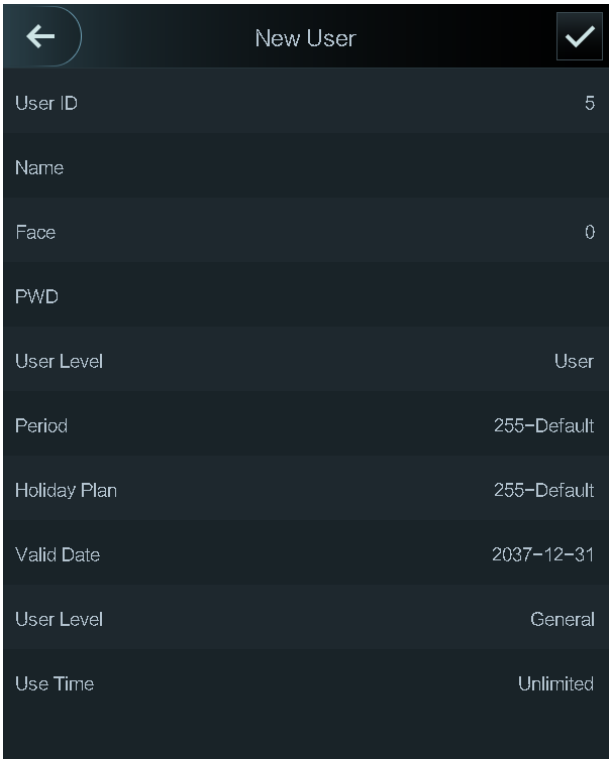
You can add new users by entering their user IDs, names, importing face images, passwords, selecting their user levels, and more.

Step 3 Select **User > New User**.

The **New User** interface is displayed. See Figure 3-5.

The following figure is for reference only and the actual interface shall prevail.

Figure 3-5 New user



Step 4 Configure parameters on the interface. See Table 3-2.

Table 3-2 New user parameter description

Parameter	Description
User ID	You can enter user IDs. The IDs consist of 32 characters (including numbers and letters), and each ID is unique.
Name	You can enter names with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the picture capturing frame, and then a picture of your face will be automatically captured. For details about face image recording, see "Appendix 1 Notes of Face Recording/Comparison."
Password	The door unlocking password. The maximum length of the password is 8 characters. If the terminal is without touch screen, you need to connect the terminal to a peripheral card reader. There are buttons on the card reader.
Level	You can select a user level for new users. There are two options. ● User: Users only have door unlock authority. ● Admin: Administrators can not only unlock the door but also have parameter configuration authority. In case that you forget the administrator password, you had better create more than one administrator.
Period	You can set a period in which the user can unlock the door. For detailed period settings, see the configuration manual.
Holiday Plan	You can set a holiday plan in which the user can unlock the door. For detailed holiday plan settings, see the user manual.

Parameter	Description
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	There are six levels: ● General: General users can unlock the door normally. ● Blacklist: When users in the blacklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times in certain periods. Once they exceed the maximum times and periods, they cannot unlock the door again. ● Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Special: When special people unlock the door, there will be a delay of 5 seconds before the door is closed.
Use Time	When the user level is Guest, you can set the maximum number of times that the guest can unlock the door.

Step 5 After you have configured all the parameters, tap ☑ to save the configuration.

For terminals without touch screen, adding new users can be completed through the web. See the user manual for details.

3.5.2 Viewing User Information

You can view user list, admin list and enable administrator password through the User interface.

3.6 Access Management

You can do access management on period, unlock mode, alarm, door status, and lock holding time.

Tap **Access** to go to the access management interface.

3.6.1 Period Management

You can set periods, holiday periods, holiday plan periods, door normally open periods, door normally closed periods, and remote verification periods.

3.6.1.1 Period Config

You can configure 128 periods (weeks) whose number range is 0–127. You can set four periods on each day of a period (week). Users can only unlock the door in the periods that you set.

3.6.1.2 Holiday Group

You can set group holidays, and then you can set plans for holiday groups. You can configure 128 groups whose number range is 0–127. You can add 16 holidays into a group. Configure the

start time and end time of a holiday group, and then users can only unlock the door in the periods that you set.

You can enter names with 32 characters (including numbers, symbols, and letters). Tap ✓ to save the holiday group name.

3.6.1.3 Holiday Plan

You can add holiday groups into holiday plans. You can use holiday plans to manage user access authority in different holiday groups. Users can only unlock the door in the period that you set.

3.6.1.4 NO Period

If a period is added to the **NO** period, then the door is normally open in that period.

The **NO/NC** period permissions are higher than permissions in other periods.

3.6.1.5 NC Period

If a period is added to the NC period, then the door is normally closed in that period. Users can not unlock the door in this period.

3.6.1.6 Remote Verification Period

If you configured the remote verification period, then when unlock doors during the period you configured, remote verification is required. To unlock the door in this period, a door unlock instruction sent by the management platform is needed.

You need to enable the **Remote Verification Period**.

- ON means enabled.
- OFF means not enabled.

3.6.2 Unlock

There are three unlock modes: unlock mode, unlock by period, and group combination. Unlock modes vary with terminal models, and the actual terminal shall prevail.

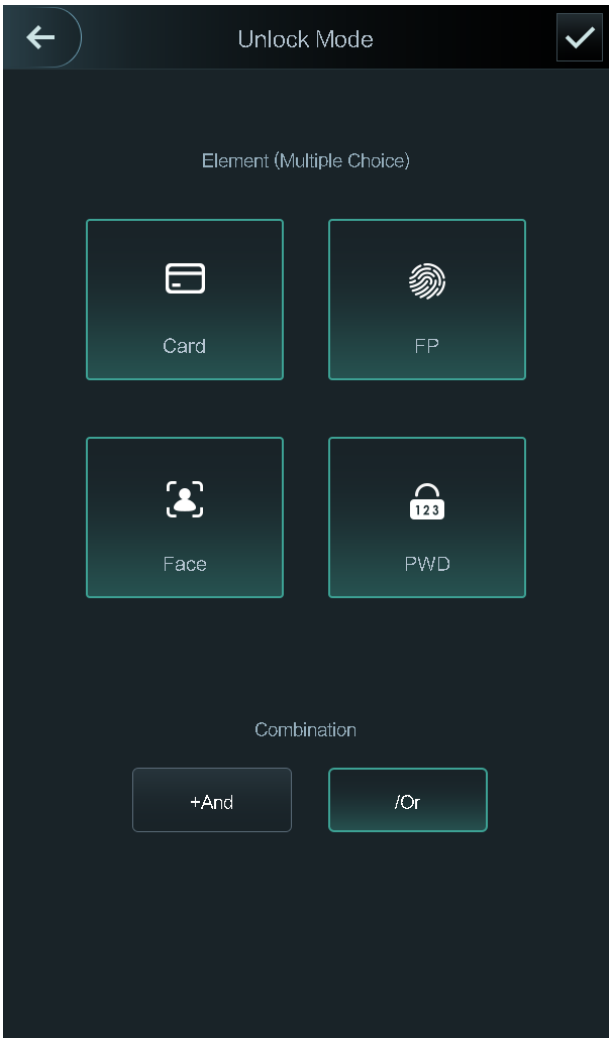
3.6.2.1 Unlock Mode

When the **Unlock Mode** is on, users can unlock through cards, fingerprints, faces, passwords, or any one of all the unlocking methods.

Step 1 Select **Access > Unlock Mode > Unlock Mode**.

The **Element (Multiple Choice)** interface is displayed. See Figure 3-6.

Figure 3-6 Element (multiple choice)



Step 2 Select unlock mode(s).

Tap a selected unlock mode again, the unlock mode will be deleted.

Step 3 Select a combination mode.

- **+ And** means "and". For example, if you selected card + FP, it means, to unlock the door, you need to swipe your card first, and then get your fingerprint scanned.
- **/ Or** means "or". For example, if you selected card/FP, it means, to unlock the door, you can either swipe your card or get your fingerprints scanned.

Step 4 Tap to save the settings.

And then the **Unlock Mode** interface is displayed.

Step 5 Enable the **Unlock Mode**.

- means enabled.
- means not enabled.

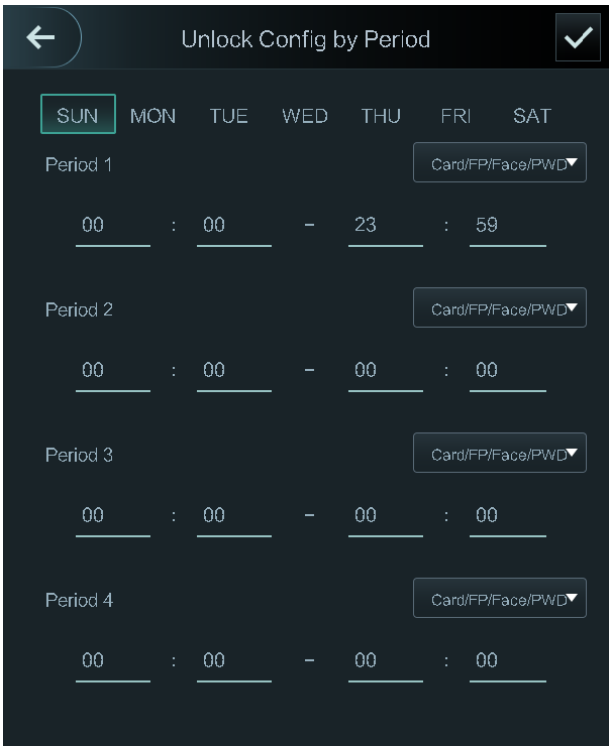
3.6.2.2 Unlock by Period

Doors can be unlocked through different unlock modes in different periods. For example, in period 1, the door can only be unlocked through card; and in period 2, doors can only be unlocked through fingerprints.

Step 1 Select **Access > Unlock Mode > Unlock by Period**.

The **Unlock Config by Period** interface is displayed. See Figure 3-7.

Figure 3-7 Unlock by period



Step 2 Set starting time and end time for a period, and then select a unlock mode.

Step 3 Tap to save the settings.

The **Unlock Mode** interface is displayed.

Step 4 Enable the **Unlock by Period** function.

- means enabled.
- means not enabled.

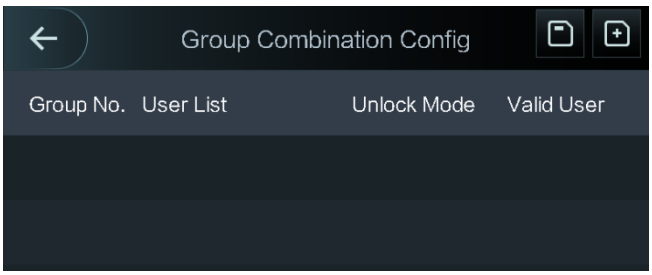
3.6.2.3 Group Combination

Doors can only be unlocked by a group or groups that consist of more than two users if the **Group Combination** is enabled.

Step 1 Select **Access > Unlock Mode > Group Combination**.

The **Group Combination Config** interface is displayed. See Figure 3-8.

Figure 3-8 Group combination



Step 2 Tap to create a group.

The **Add Group** interface is displayed. See Figure 3-9.

Figure 3-9 Add a group

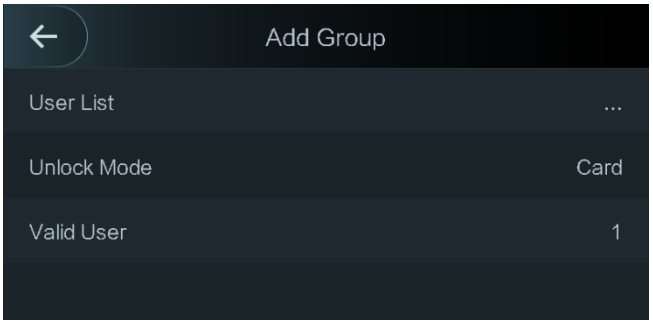


Table 3-3 Group parameter

Parameter	Description
User List	Add users to the newly created group. 1. Tap **User List**. The **User List** interface is displayed. 2. Tap , and then enter a user ID. 3. Tap to save the settings.
Unlock Mode	There are two options: **PWD** and **Face**.
Valid User	Valid users are the ones that have unlock authority. Doors can be unlocked only when the number of users to unlock the doors equals the valid user number. ● Valid users cannot exceed the total number of users in a group. ● If valid users equal total user numbers in a group, doors can only be unlocked by all the users in the group. ● If valid users are less than the total number of users in a group, doors can be unlocked by any users whose number equals the valid user number.

Step 3 Tap to go back to the previous interface.

Step 4 Tap to save the settings.

Step 5 Enable the **Group Combination**.

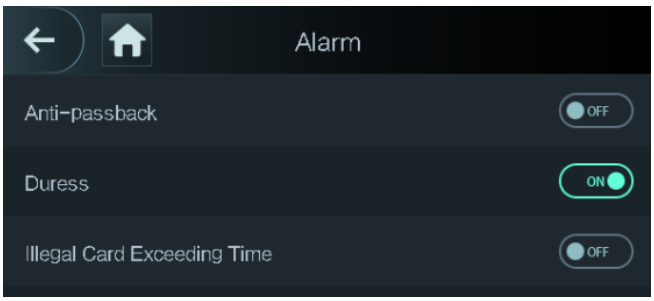
- means enabled.
- means not enabled.

3.6.3 Alarm Configuration

Administrators can manage visitors' unlock authority through alarm configuration.

Select **Access > Alarm**. The **Alarm** interface is displayed. See Figure 3-10.

Figure 3-10 Alarm



- means enabled.

- means not enabled.

Table 3-4 Parameters on the alarm interface

Parameter	Description
Anti-passback	● If a person unlocks the door with the identity checked by the terminal, but when the person gets out without getting the identity checked by the terminal, an alarm will be triggered and the person will have no authority to unlock the door any more. ● If a person gets inside a building or a room without swiping the card, and the person swiped the card to get out, then the person will have no authority to unlock the door any more.
Duress	An alarm will be triggered when a duress card, duress password, or duress fingerprint is used to unlock the door.
Illegal Card Exceeding Time	After an unauthorized card is used to unlock the door more than 5 times in 50 seconds, an alarm will be triggered.

3.6.4 Door Status

There are three options: **NO**, **NC**, and **Normal**.

- NO: If **NO** is selected, the door status is normally open, which means the door will never be closed.
- NC: If **NC** is selected, the door status is normally closed, which means the door will not be unlocked.
- Normal: If Normal is selected, the door will be unlocked and locked depending on your settings.

3.6.5 Lock Holding Time

Lock Holding Time is the duration in which the lock is unlocked. If the lock has been unlocked for a period that exceeds the duration, the lock will be automatically locked.

3.7 Network Communication

To make the terminal work normally, you need to configure parameters for network, serial ports and wiegand ports.

3.7.1 IP Address

3.7.1.1 IP Configuration

Configure an IP address for the terminal to make it be connected to the network. See Figure 3-11 and Table 3-5.

Figure 3-11 IP address configuration

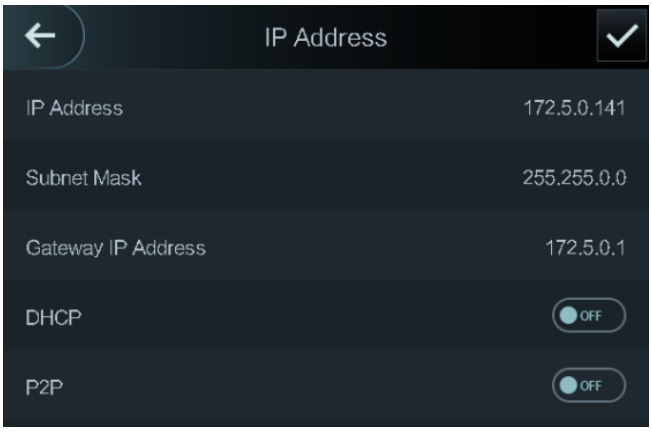


Table 3-5 IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway IP Address	The IP address, subnet mask, and gateway IP address should be on the same network segment. After configuration, tap ✓ to save the configurations.
DHCP	DHCP (Dynamic Host Configuration Protocol). When the DHCP is enabled, the IP address can be automatically acquired, and the IP address, subnet mask and gateway IP address cannot be manually configured.
P2P	P2P is a private network traversal technology which enables user to manage devices without requiring DDNS, port mapping or transit server.

- Make sure that the computer used to log in to the web is in the same LAN with the device.
- 7-inch model B access controllers of have dual NICs. The default management address for 1000M Ethernet port is 192.168.1.108, and for 100M Ethernet port is 192.168.2.108.

3.7.1.2 Active Register

By active registering, you can connect the terminal to the management platform, and then you can manage the terminal through the management platform.

Configurations you have made can be cleared on the managing platform, and the terminal can be initialized, you need to protect the platform managing authority in case of data loss caused by improper operation.

For active register parameter, see Table 3-6.

Table 3-6 Active register

Name	Parameter
Server IP Address	IP address of the managing platform.
Port	Port number of the managing platform.
Device ID	Subordinate device number on the managing platform.

3.7.1.3 Wi-Fi

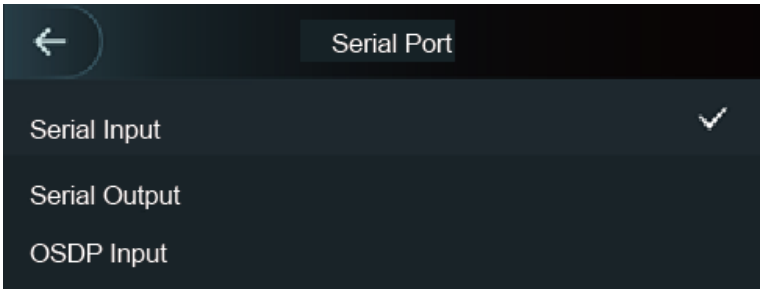
You can connect the terminal to the network through Wi-Fi if the terminal has Wi-Fi function.

3.7.2 Serial Port Settings

Select serial input or serial output according to the entering direction and exiting direction.

Select **Connection > Serial Port**, and then the **Serial Port** interface is displayed. See Figure 3-12.

Figure 3-12 Serial port



- Select **Serial Input** when external devices that are with card reading and writing functions are connected to the terminal. **Serial Input** is selected to enable access card information to be sent to the terminal and the management platform.
- When **Serial Input** is selected to make the terminal be connected to the reader in the turnstile, you need to select Door 1 or Door 2 as needed.
  - ◇ Door 1: If Door 1 is selected, then the reader and terminal control the same door opening direction. For example, both the reader and terminal control the entering direction into a place or all control the exiting direction from a place.
  - ◇ Door 2: If Door 2 is selected, the reader and terminal control different door opening directions. For example, the terminal controls the entering direction into a place and the reader controls the exiting direction from a place.
- For terminals with face recognition, fingerprint recognition, card reading and writing functions, if you select **Serial Output**, terminal will send lock/unlock information to the terminal. There are two types of lock/unlock information:
  - ◇ User ID
  - ◇ Card No.
- Select OSDP Input when card reader of OSDP protocol is connected to the terminal. The terminal can send card information to the management platform.

3.7.3 Wiegand Configuration

Select **Wiegand Input** or **Wiegand Output** according to the entering direction and exiting direction.

Select **Connection > Wiegand**, and then the Wiegand interface is displayed. See Figure 3-13.

Figure 3-13 Wiegand

- Select **Wiegand Input** when an external card swipe mechanism is connected to the terminal.
- When **Serial Input** is selected to make the terminal be connected to the reader in the turnstile, you need to select Door 1 or Door 2 as needed.
  - ◇ Door 1: If Door 1 is selected, then the reader and terminal control the same door opening direction. For example, both the reader and terminal control the entering direction into a place or all control the exiting direction from a place.
  - ◇ Door 2: If Door 2 is selected, the reader and terminal control different door opening directions. For example, the terminal controls the entering direction into a place and the reader controls the exiting direction from a place.
- Select **Wiegand Output** when the terminal works as a reader that can be connected to the terminal. See Table 3-7.

Table 3-7 Wiegand output

Parameter	Description
Wiegand Output Type	The Wiegand Output Type determines the card number or the digit of the number than can be recognized by the terminal. ● Wiegand26, three bytes, six digits. ● Wiegand34, four bytes, eight digits. ● Wiegand66, eight bytes, sixteen digits.
Pulse Width	You can set pulse width and pulse interval.
Pulse Interval	
Output Data Type	You can select the types of output data. ● User ID: If User ID is selected, and then user ID will be output. ● Card No.: If Card No. is selected, and then card number will be output.

3.8 System

3.8.1 Time

You can do date format setting, date setting, time setting, DST setting, NTP check, time zone settings.

- When you select Network Time Protocol (NTP), you need to configure the following parameters. You need to enable the NTP Check function first. Server IP Address: enter the IP address of the time server, time of the terminal will be synchronized with the time server.
- Port: Enter the port number of the time server.

- Interval (min): NPT check interval. Tap the save icon to save.

3.8.2 Face Parameter

Figure 3-14 Face parameter

Tap a parameter and do configuration, and then tap .

Table 3-8 Face parameter

Name	Description
Face Recognition Threshold	Face recognition accuracy can be adjusted. The larger the value is, the higher the accuracy will be.
Max. Angle of Face Recognition	You can set the control panel shooting angle of profiles. The larger the value is, the wider range of the profiles will be recognized.
Recognition Timeout	When a person who does not have the access authority stands in front of the terminal and gets the face recognized, the terminal will prompt that face recognition failed. The prompt interval is called recognition timeout.
Pupillary Distance	Pupillary distance is the pixel value of the image between the centers of the pupils in each eye. You need to set an appropriate value so that the terminal can recognize faces as needed. The value changes according to the face sizes and the distance between faces and the lens. The closer the face is to the lens, the greater the value should be. If an adult is 1.5 meters away from the lens, the pupillary distance value can be within 50 to 70.
Recognition Interval	When a person who has the access authority stands in front of the terminal and gets the face recognized, the terminal will prompt that face recognition succeeded. The prompt interval is the recognition interval.
Anti-fake Threshold	This function prevents people from unlocking by human face images or face models. The larger the value is, the more difficult face images can unlock the door. The recommended value range is above 80.

3.8.3 Fill Light Mode Setting

You can select fill light modes according to your needs. There are three modes:

- Auto: When the photo sensor detects that the ambient environment is not dark, the fill light is normally off; otherwise, the fill light will be on.
- NO: The fill light is normally open.
- NC: The fill light is normally closed.

3.8.4 Fill Light Brightness Setting

You can select fill light brightness according to your needs.

3.8.5 Volume Adjustment

Tap or to adjust the volume.

3.8.6 IR Light Brightness Adjustment

The larger the value is, the clearer the images will be; otherwise the unclearer the images will be.

3.8.7 Restore to Factory Settings

- Data will be lost if you restore the terminal to the factory settings.
- After the terminal is restored to the factory settings, IP address will not be changed.

You can select whether to retained user information and logs.

- You can select to restore the terminal to the factory settings with all user information and device information deleted.
- You can select to restore the terminal to the factory settings with user information and device information retained.

3.8.8 Reboot

Select **Setting > Reboot**, tap **Reboot**, and the terminal will be rebooted.

3.9 USB

- Make sure that the USB is inserted before exporting user information and updating. During exporting or updating, do not pull out the USB or do other operations; otherwise the exporting or updating will fail.

- You need to import information from one terminal to the USB before using USB to import information to another terminal.
- USB can also be used to update the program.

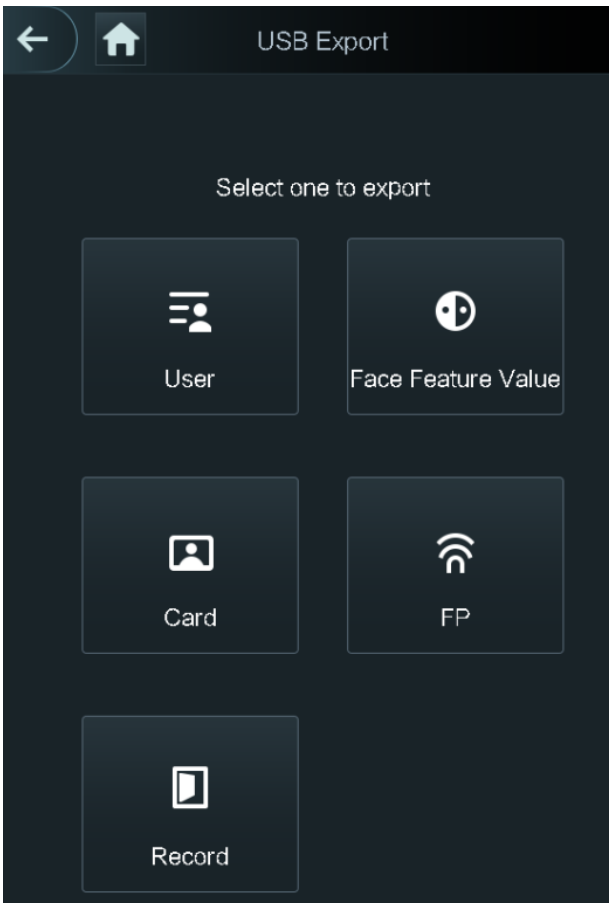
3.9.1 USB Export

You can export data from the terminal to the USB after inserting the USB. The data exported is encrypted and cannot be edited.

Step 1 Select **USB > USB Export**.

The **USB Export** interface is displayed. See Figure 3-15.

Figure 3-15 USB export



Step 2 Select the data type that you want to export.

The prompt **Confirm to export** is displayed.

Step 3 Tap **OK**.

Data exported will be saved in the USB.

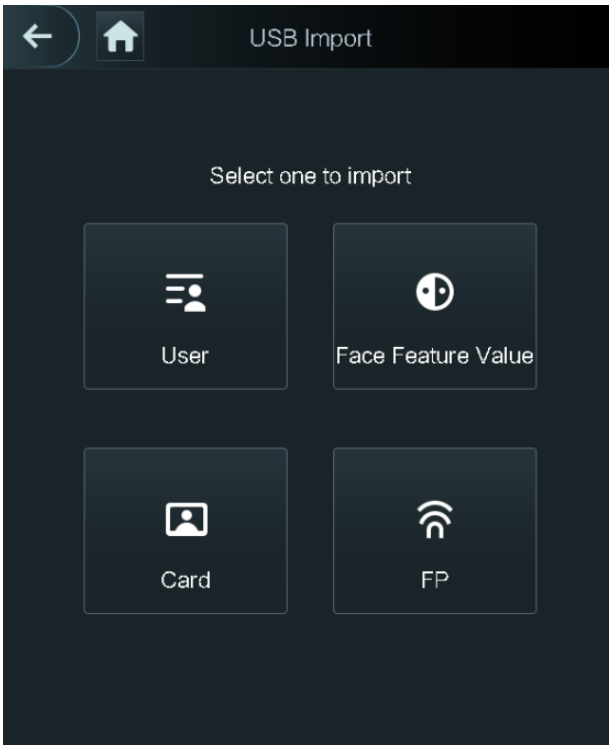
3.9.2 USB Import

Only data in the USB flash drive that was exported from one terminal can be imported into another terminal.

Step 1 Select **USB > USB Import**.

The **USB Import** interface is displayed. See Figure 3-16.

Figure 3-16 USB Import



Step 2 Select the data type that you want to import.
The prompt **Confirm to import** is displayed.

Step 3 Tap **OK**.
Data in the USB flash drive will be imported into the terminal.

3.9.3 USB Update

USB flash drive can be used to update the system.

Step 1 Rename the updating file name to "update.bin", and save the "update.bin" file in the root directory of the USB.

Step 2 Select **USB > USB Update**.
The prompt **Confirm to Update** is displayed.

Step 3 Tap **OK**.
The update starts, and the terminal will restart after the update is finished.

3.9.4 Features

You can do settings about privacies, card number reverse, security module, door sensor type, and result feedback. For details of the functions mentioned, see Figure 3-17 and Table 3-9.

Figure 3-17 Features

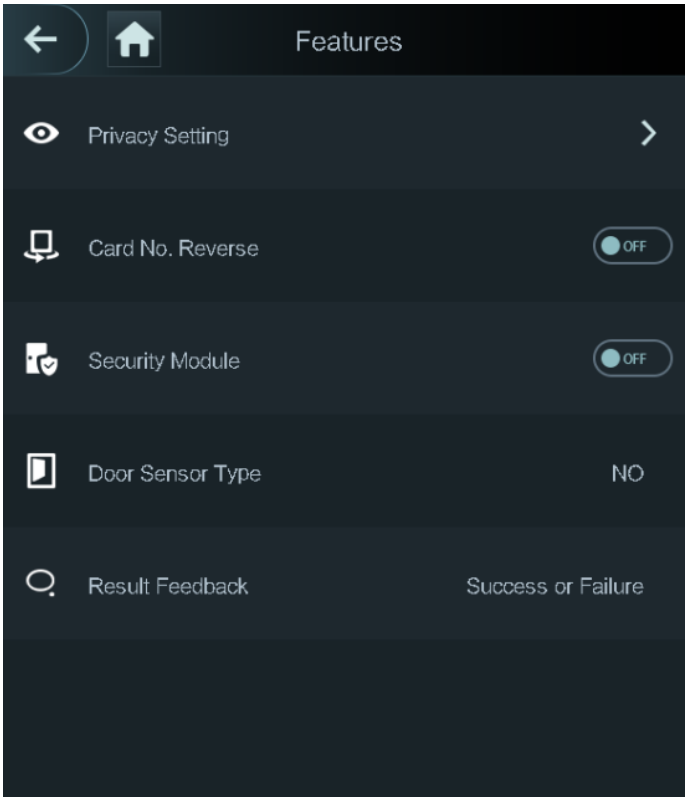


Table 3-9 Feature description

Parameter	Description
Privacy Setting	See "0 Privacy Setting" for details.
Card No. Reverse	If the third party card reader needs to be connected to the terminal through the wiegand output port, you need to enable the Card No. Reverse function; otherwise the communication between the terminal and the third party card reader might fail due to protocol discrepancy.
Security Module	● If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power. ● Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.
Door Sensor Type	There are two options: **NO** and **NC**.
Result Feedback	Displays whether the unlock succeeded or failed.

Privacy Setting

Figure 3-18 Privacy setting

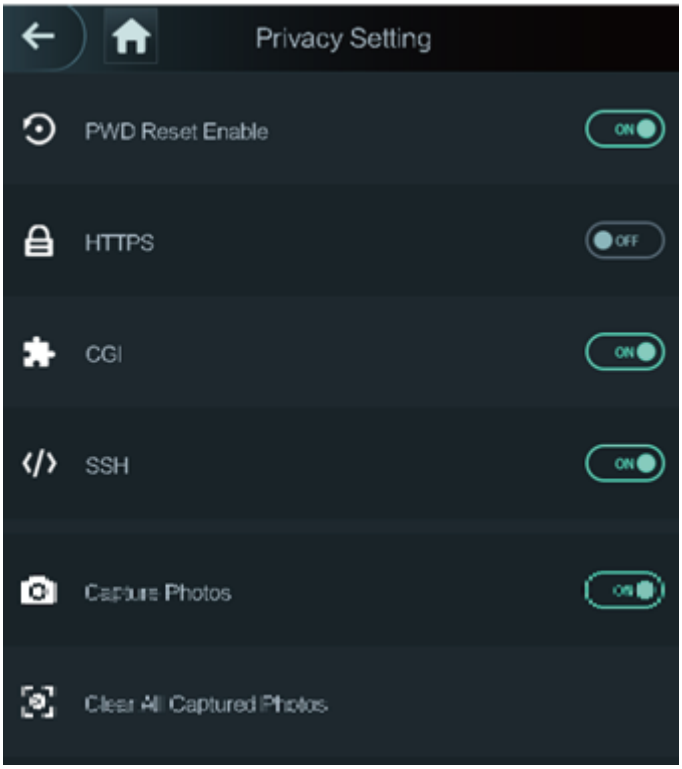


Table 3-10 Features

Parameter	Description
PWD Reset Enable	If the **PWD Reset Enable** function is enabled, you can reset the password. The PWD Reset function is enabled by default.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs that execute like console applications running on a server that generates web pages dynamically. When CGI is enabled, CGI commands can be used. The CGI is enabled by default.
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. When SSH is enabled, SSH provides cryptographic service for the data transmission.
Capture photo	If you select ON, when a user unlocks the door, the user's photo will be automatically taken. This function is ON by default.
Clear all captured photos	Tap the icon, and you can delete all captured photos.

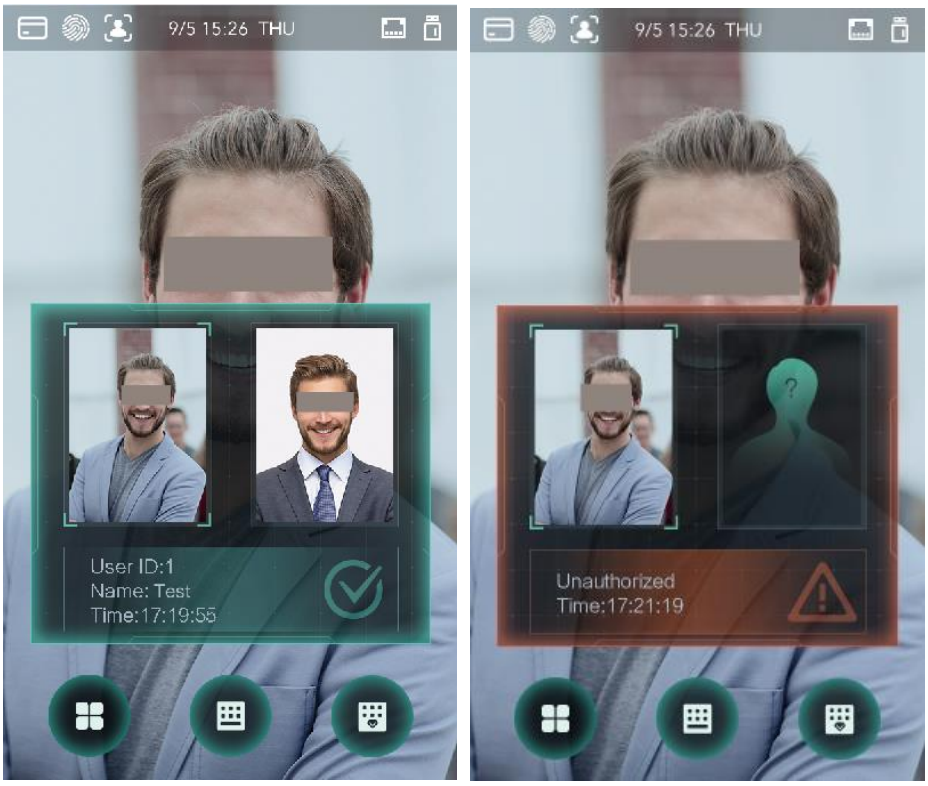
When HTTPS is enabled, the terminal will restart automatically.

3.9.5 Result Feedback

You can select a result feedback mode as needed.

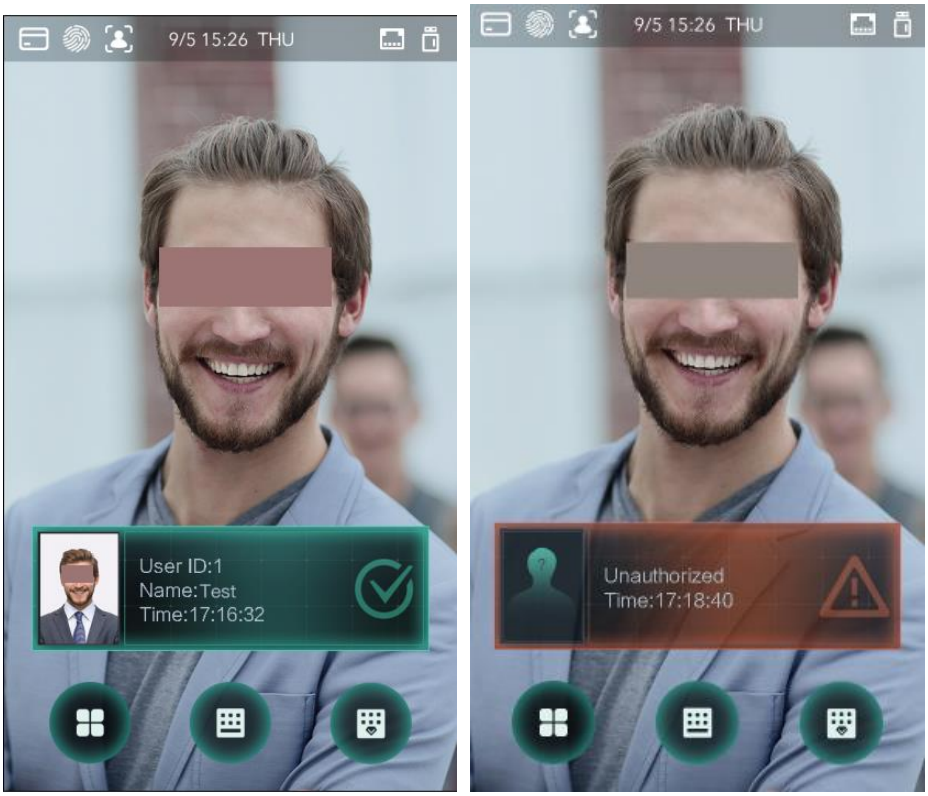
Mode 1

Figure 3-19 Mode 1



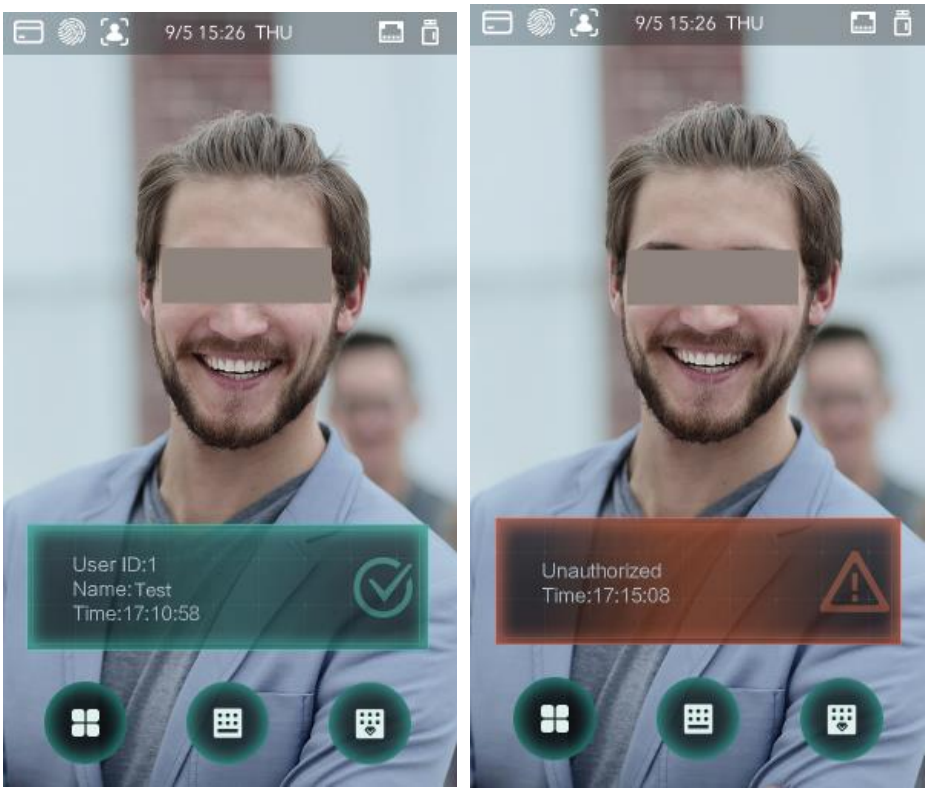
Mode 2

Figure 3-20 Mode 2



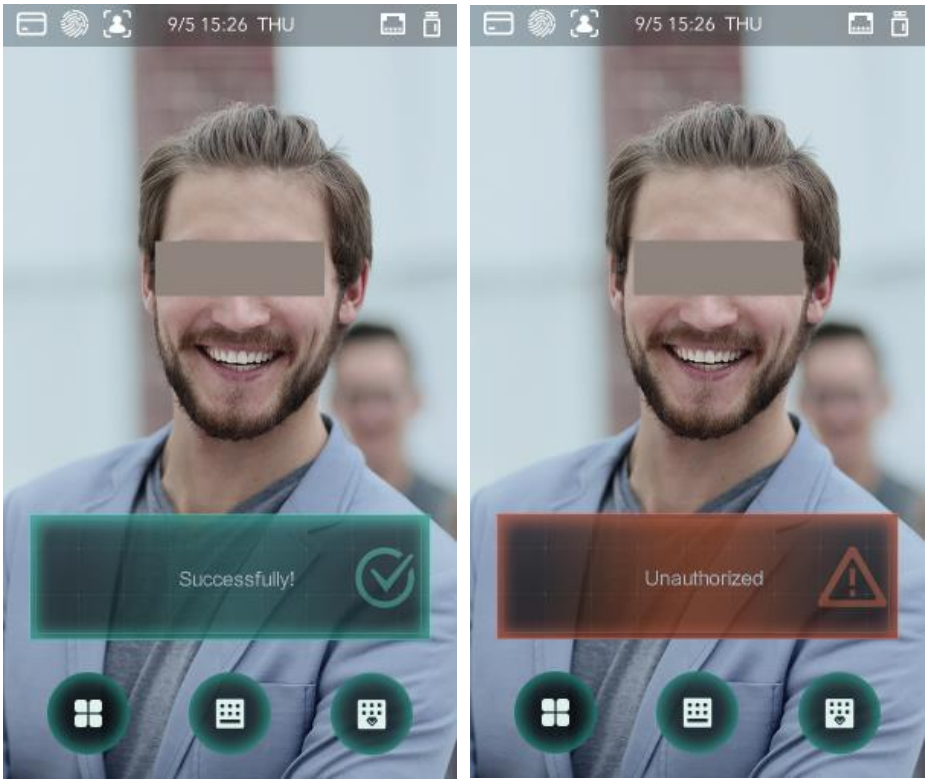
Mode 3

Figure 3-21 Mode 3



Mode 4

Figure 3-22 Mode 4



3.10 Record

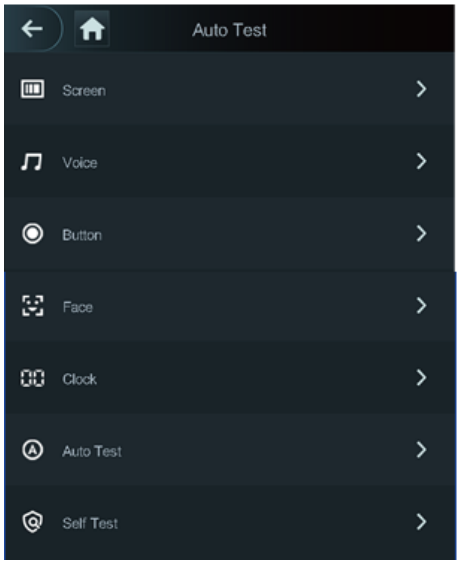
You can query all unlocking records.

Figure 3-23 Search punch records

3.11 Auto Test

When you use the terminal for the first time or when the terminal malfunctioned, you can use auto test function to check whether the terminal can work normally. Do actions according to the prompts.

Figure 3-24 Auto test



When you select **Auto Test**, the terminal will guide you to do all the auto tests.

3.12 System Info

You can view data capacity, device version, and firmware information of the terminal on the **System Info** interface.

4 Web Operation

The terminal can be configured and operated on the web. Through the web you can set parameters including network parameters, video parameters, and terminal parameters; and you can also maintain and update the system.

4.1 Initialization

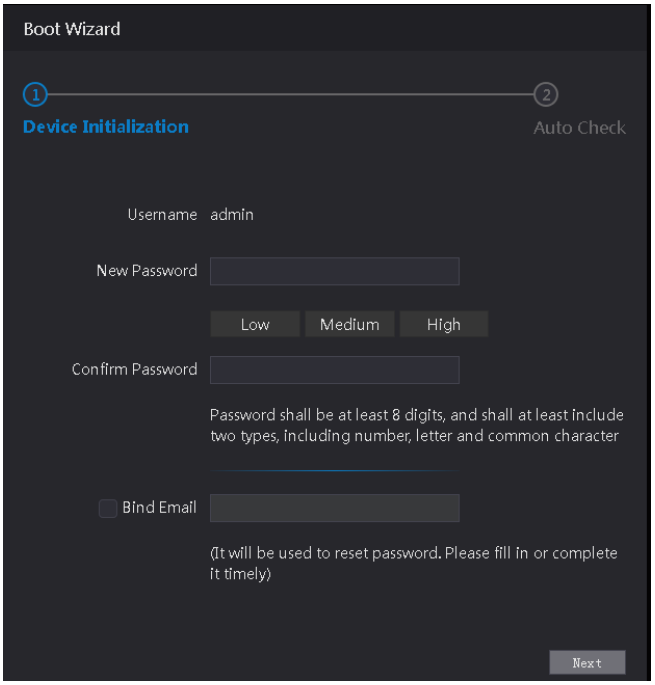
You need to set a password and an email address before logging in to the web for the first time.

Step 1 Open IE web browser, and enter the IP address (the default address is 192.168.1.108) of the access controller in the address bar, and then press Enter.

The **Initialization** interface is displayed. See Figure 4-1.

- Use browser newer than IE 8, otherwise you might not log in to the web.
- Make sure that the computer used to log in to the web is in the same LAN with the device.
- 7-inch model B access controllers of have dual NICs. The default management address for 1000M Ethernet port is 192.168.1.108, and for 100M Ethernet port is 192.168.2.108.

Figure 4-1 Initialization



Step 2 Enter the user name and password.

- The default username of administrator is admin, and the password is the login password after initializing the terminal. Modify the administrator password regularly and keep it properly for security.
- If you forget the administrator login password, you can click **Forget Password?** to reset it. See the user manual.

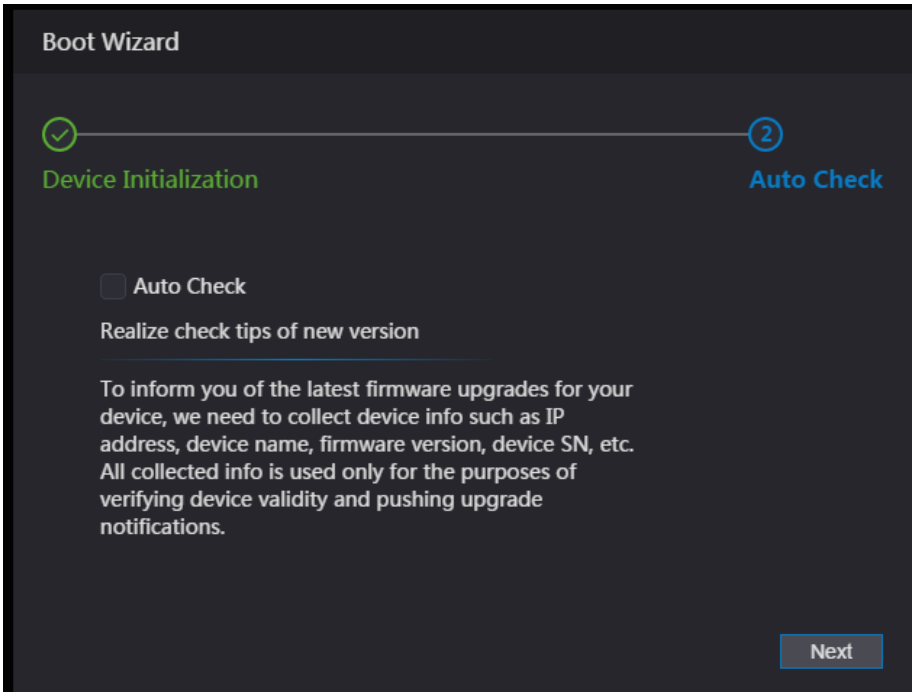
Step 3 Click **Login**.

The homepage of the web is displayed.

Step 4 Click **Next**.

The **Auto Check** interface is displayed. See Figure 4-2.

Figure 4-2 Auto check



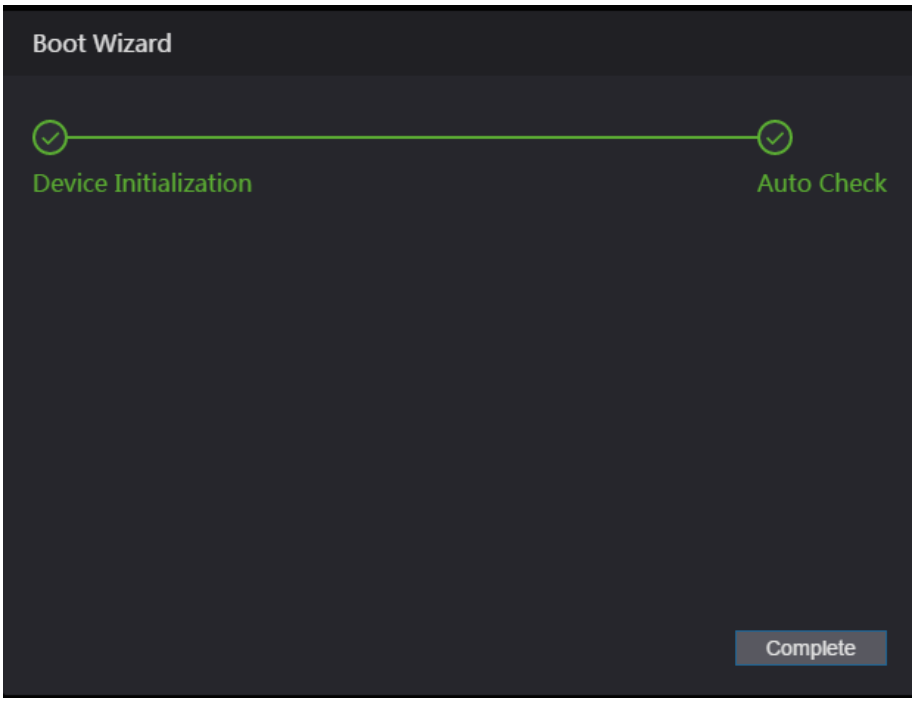
Step 5 You can decide whether to select **Auto Check** or not.

It is recommended that **Auto Check** be selected to get the latest program in time.

Step 6 Click **Next**.

The configuration is finished..

Figure 4-3 Auto check completed



Step 7 Click **Complete**, and the initialization is completed.

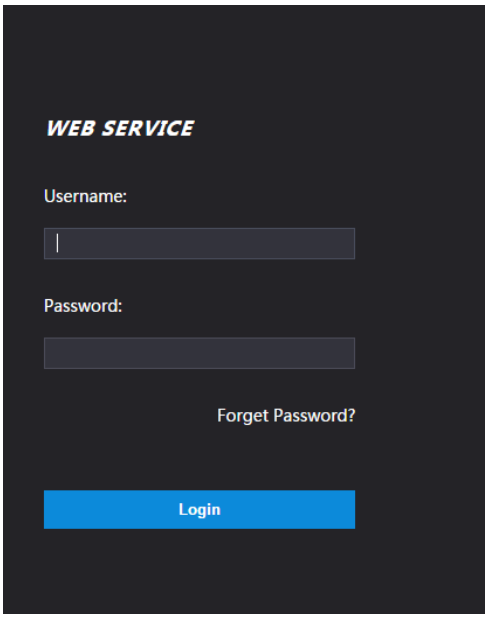
The web login interface is displayed.

4.1 Login

Step 1 Open IE web browser, enter the IP address of the terminal in the address bar, and press Enter.

- Use browser newer than IE 8, otherwise you might not log in to the web.
- Make sure that the IP address of computer used to log in to the web is in the same LAN with the terminal.
- 7-inch model B terminals have dual NICs. The default management address for 1000M Ethernet port is 192.168.1.108, and for 100M Ethernet port is 192.168.2.108.

Figure 4-4 Login



Step 2 Enter the username and password.

- The default administrator name is admin, and the password is the login password after initializing the terminal. Modify the administrator regularly and keep it properly for the sake of security.
- If you forget the administrator login password, you can click **Forget password?** to reset it. See "4.2 Resetting the Password."

Step 3 Click **Login**.

The web interface is logged in.

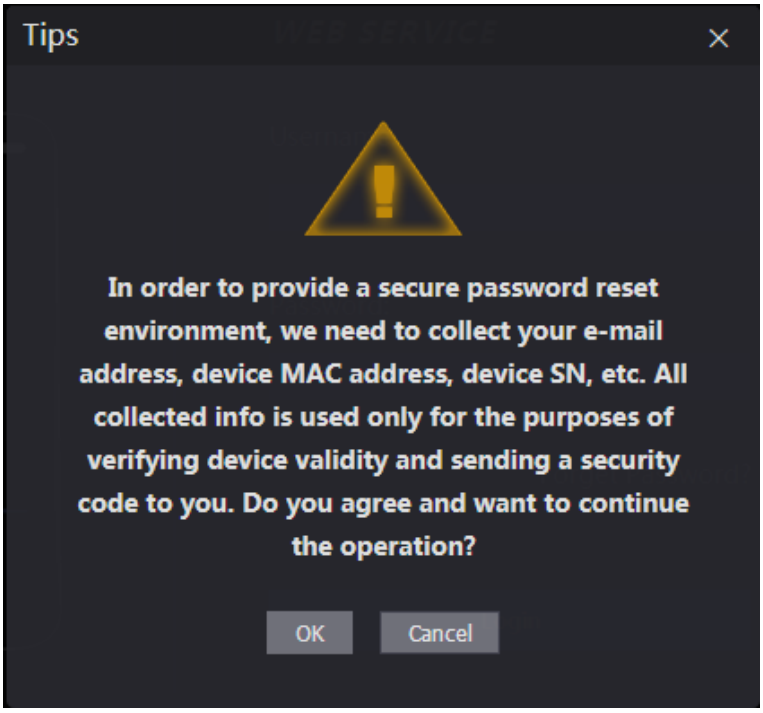
4.2 Resetting the Password

When resetting the password of the admin account, your email address will be needed.

Step 1 Click **Forget password?** on the login interface.

The **Tips** interface is displayed.

Figure 4-5 Tips

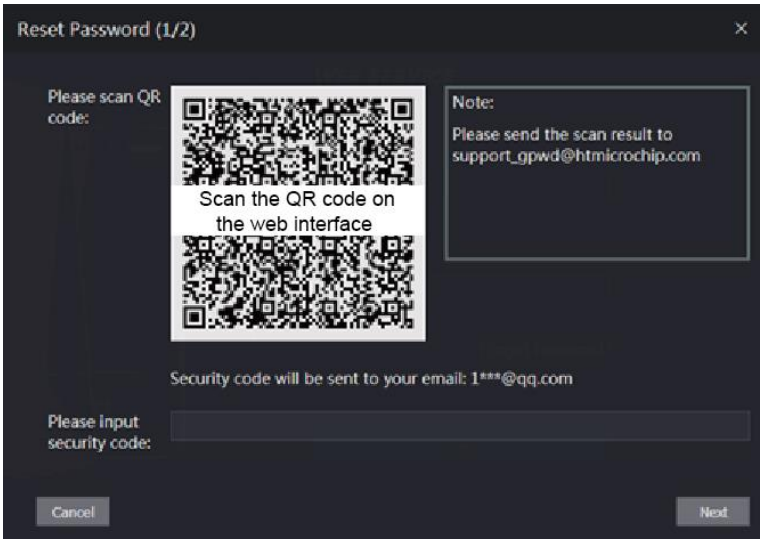


Step 2 Read the tips.

Step 3 Click **OK**.

The **Reset Password** interface is displayed.

Figure 4-6 Reset password



Step 4 Scan the QR code on the interface, and you will get the security code.

- At most two security codes will be generated by scanning the same QR code. To get more security code, refresh the QR code.
- You need to send the content you get after you scanned the QR code to the designated email address, and then you will get the security code.
- Please use the security code within 24 hours after you receive it. Otherwise, it will become invalid.
- If wrong security codes are entered for consecutive five times, the administrator will be frozen for five minutes.

Step 5 Enter the security code you have received.

Step 6 Click **Next**.

The **Reset Password** interface is displayed.

Step 7 Reset and confirm the new password.

The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Step 8 Click **OK**, and the reset is completed.

4.3 Alarm Linkage

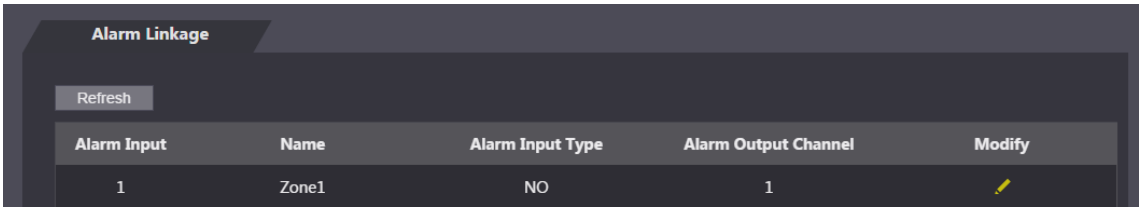
4.3.1 Setting Alarm Linkage

Alarm input devices can be connected to the terminal, and you can modify the alarm linkage parameter as needed.

Step 1 Select **Alarm Linkage** on the navigation bar.

The **Alarm Linkage** interface is displayed. See Figure 4-7.

Figure 4-7 Alarm linkage



Step 2 Click , and then you can modify alarm linkage parameters. See Figure 4-8

Figure 4-8 Modifying alarm linkage parameter

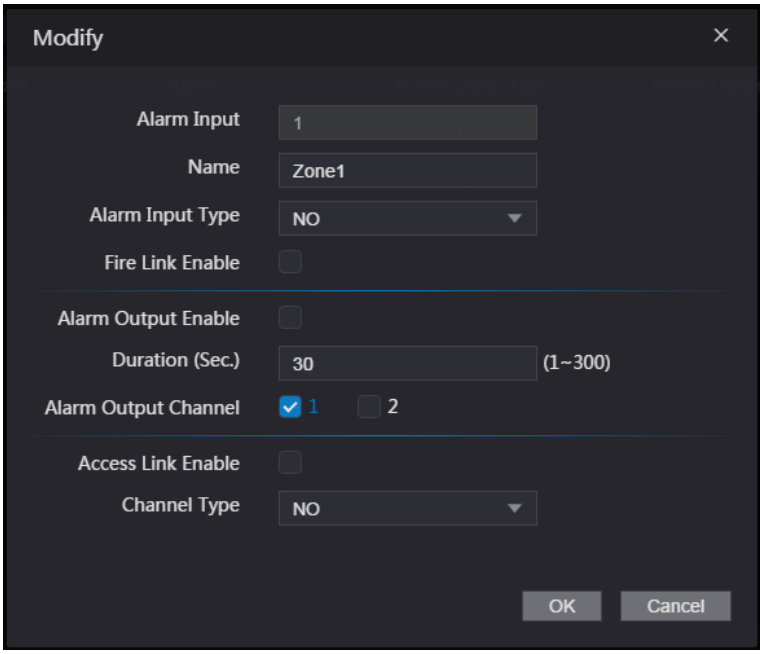


Table 4-1 Alarm linkage parameter description

Parameter	Description
Alarm Input	You cannot modify the value. Keep it default.
Name	Enter a zone name.

Parameter	Description
Alarm Input Type	There are two options: NO and NC. If alarm input type of the alarm device you purchased is NO, then you should select NO; otherwise you should select NC.
Fire Link Enable	If fire link is enabled the terminal will output alarms when fire alarms are triggered. The alarm details will be displayed in the alarm log. Alarm output and access link are NO by default if fire link is enabled.
Alarm Output Enable	The relay can output alarm information (will be sent to the management platform) if the **Alarm Output** is enabled.
Duration (Sec.)	The alarm duration, and the range is 1–300 seconds.
Alarm Output Channel	You can select an alarm output channel according to the alarming device that you have installed. Each alarm device can be regarded as a channel.
Access Link Enable	After the Access Link is enabled, the terminal will be normally open or normally closed when there are input alarm signals.
Channel Type	There are two options: NO and NC.

Step 3 Click **OK**, and then the configuration is completed.

The configuration on the web will be synchronized with the configuration in the client if the terminal is added to a client.

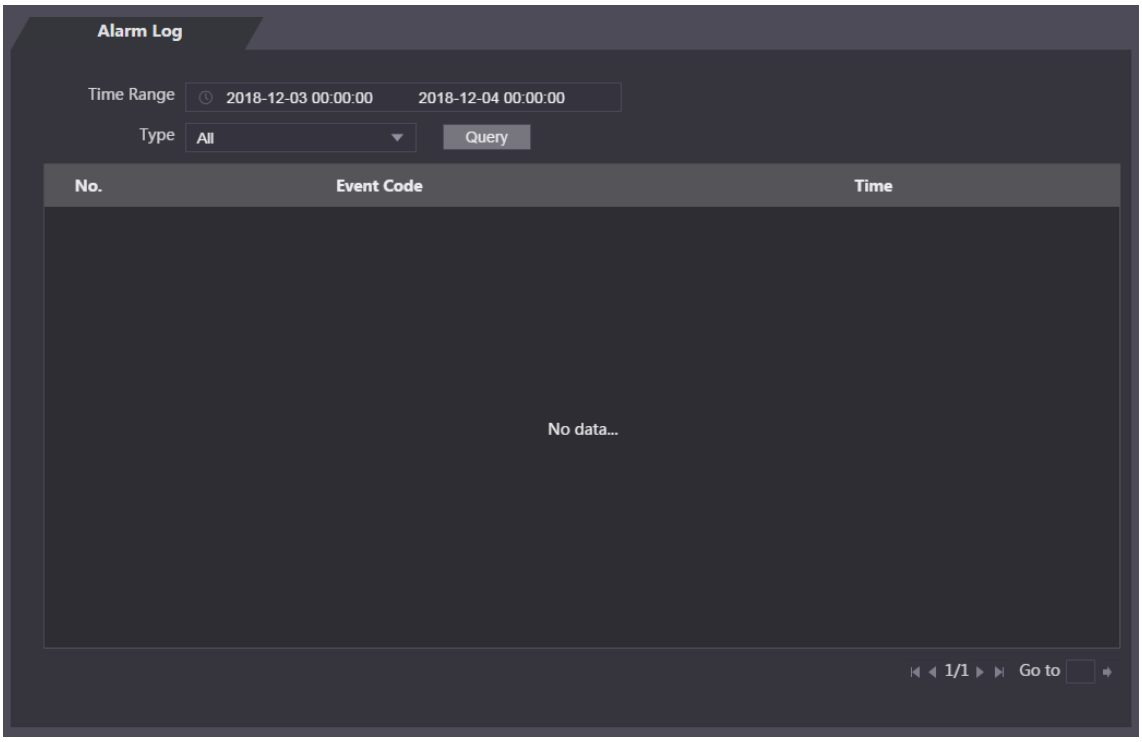
4.3.2 Alarm Log

You can view the alarm type and time range in the **Alarm Log** interface.

Step 1 Select **Alarm Linkage > Alarm Log**.

The **Alarm Log** interface is displayed. See Figure 4-9.

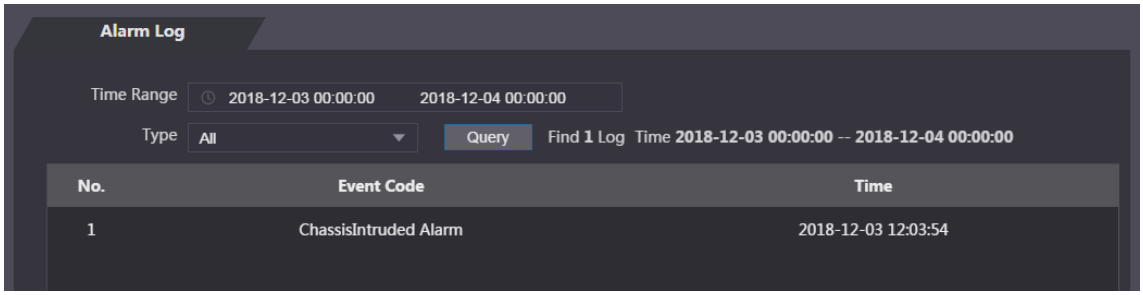
Figure 4-9 Alarm log



Step 2 Select a time range and alarm type, and then click **Query**.

The query results are displayed. See Figure 4-10.

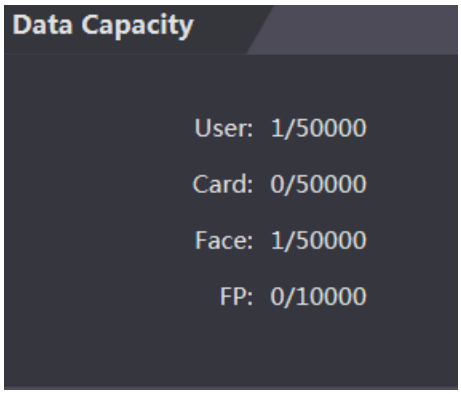
Figure 4-10 Query results



4.4 Data Capacity

You can see how many users, cards, face images, and fingerprints the terminal can hold on the **Data Capacity** interface.

Figure 4-11 Data capacity



4.5 Video Setting

You can set parameters including data rate, image parameters (brightness, contrast, hue, saturation, etc.), and exposure on the **Video Setting** interface.

4.5.1 Data Rate

Figure 4-12 Data rate

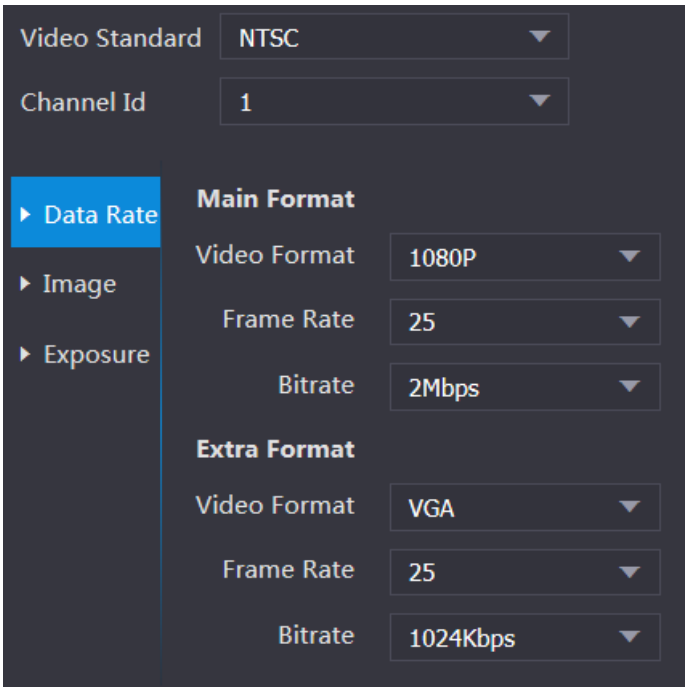


Table 4-2 Data rate parameter description

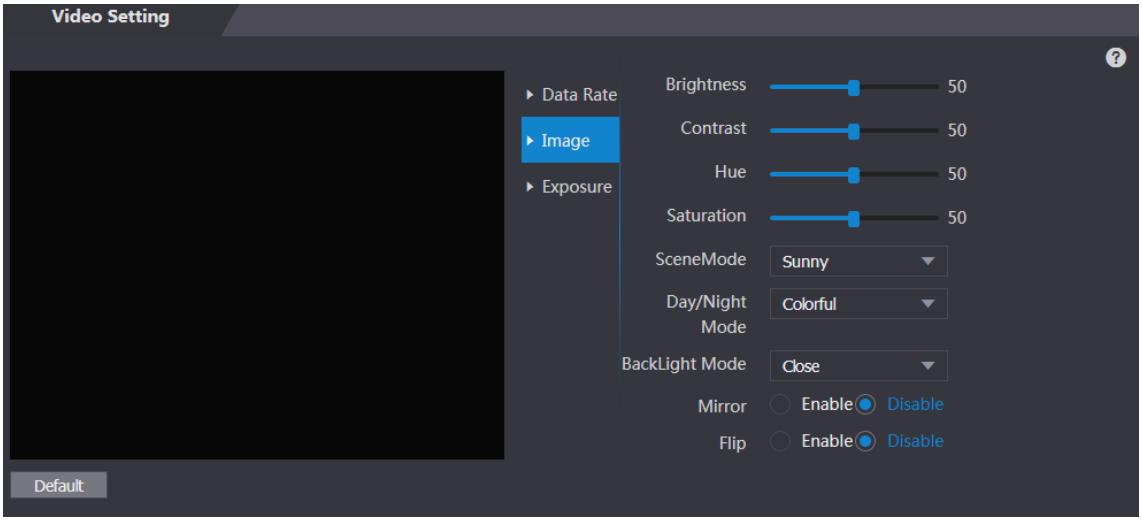
Parameter		Description
Video Standard		There are two options: NTSC and PAL. Select a standard according to the video standard of your region.
Channel		There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
Main Format	Video Format	There are four options: D1, VGA, 720p and 1080p. Select an option according to the video quality you want.
	Frame Rate	The rate at which consecutive frames appear on a display. The frame rate range is 1–30fps.
	Bit Rate	The number of bits that are conveyed or processed per unit of time. There are five options: 2Mbps, 4Mbps, 6Mbps, 8Mbps, and 10Mbps.
Extra Format	Video Format	There are three options: D1, VGA, and QVGA.
	Frame Rate	The rate at which consecutive frames appear on a display. The frame rate range is 1–30fps.
	Bit Rate	The number of bits that are conveyed or processed per unit of time. There are options: 512Kbps, 640Kbps, 768Kbps, 896Kbps, 1024Kbps, 1.25Mbps, 1.5Mbps, 1.75Mbps, and 2Mbps.

4.5.2 Image

There are two channels, and you need to configure parameters for each channel.

Step 1 Select **Video Setting > Video Setting > Image**.

Figure 4-13 Image



Step 2 Select **Wide Dynamic** in the Backlight Mode.

Table 4-3 Image parameter description

Parameter	Description
Brightness	The larger the value is, the brighter the images will be.
Contrast	Contrast is the difference in luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the brightness and color contrast will be.
Hue	The larger the value is, the deeper the color will be.
Saturation	The larger the value is, the brighter the colors will be. The value does not change image brightness.
Scene Mode	● Close: without modes. ● Auto: The system automatically adjusts scene modes. ● Sunny: In this mode, image hue will be reduced. ● Night: In this mode, image hue will be increased. **Sunny** is selected by default.
Day/Night Mode	Day/Night mode decides the working status of the fill light. ● Auto: The system automatically adjusts the day/night modes. ● Colorful: In this mode, images are with colors. ● Black and white: In this mode. Images are in black and white.

Parameter	Description
Back Light Mode	● Close: Without back light. ● BLC: Backlight compensation corrects regions with extremely high or low levels of light to maintain a normal and usable level of light for the object in focus. ● WDR: In the wide dynamic range mode, the system dims bright areas and compensates dark areas to ensure the definition of objects in the bright areas and dark areas. When human faces are in the backlight, you need to enable the Wide Dynamic. ● HLC: Highlight compensation is needed to compensate for overexposure of highlights or strong light sources like spotlights, headlights, porch lights, etc. to create an image that is usable and not overtaken by a bright light.
Mirror	When the function is enabled, images will be displayed with left and right side reversed.
Flip	When this function is enabled, videos can be flipped over.

4.5.3 Exposure

Table 4-4 Exposure parameter description

Parameter	Description
Anti-flicker	● 50Hz: When the utility frequency of alternating current is 50Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. ● 60Hz: When the utility frequency of alternating current is 60Hz, the exposure is automatically adjusted to make sure that there are no stripes on images. ● Outdoor: When **Outdoor** is selected, the exposure mode can be switched.
Exposure Mode	● When you select **Outdoor** in the **Anti-flicker** drop-down list, you can select **Shutter Priority** as the exposure mode. ● Exposure modes of different devices might vary, and the actual product shall prevail. You can select from: ● Auto: The terminal will automatically adjust brightness of images. ● Shutter Priority: The terminal will adjust image brightness according to shutter exposure value range. If the image brightness is not enough and the shutter value has reached upper or lower limit, the terminal will adjust gain value automatically to get ideal brightness. ● Manual: You can configure gain and shutter value manually to adjust image brightness.
Shutter	The larger the shutter value is and the shorter the exposure time is, the darker the images will be.

Parameter	Description
Shutter Value Range	If you select **Customized Range**, you can customize the shutter value range.
Gain Value Range	When the gain value range is set, video quality will be improved.
Exposure Compensation	You can increase video brightness by adjusting exposure compensation value.
3D NR	When 3D Noise Reduction (RD) is enabled, video noise can be reduced, and high definition videos will be produced.
Grade	You can adjust the value of the 3D NR when 3D NR is enabled. The larger the value is, the less the noise there will be.

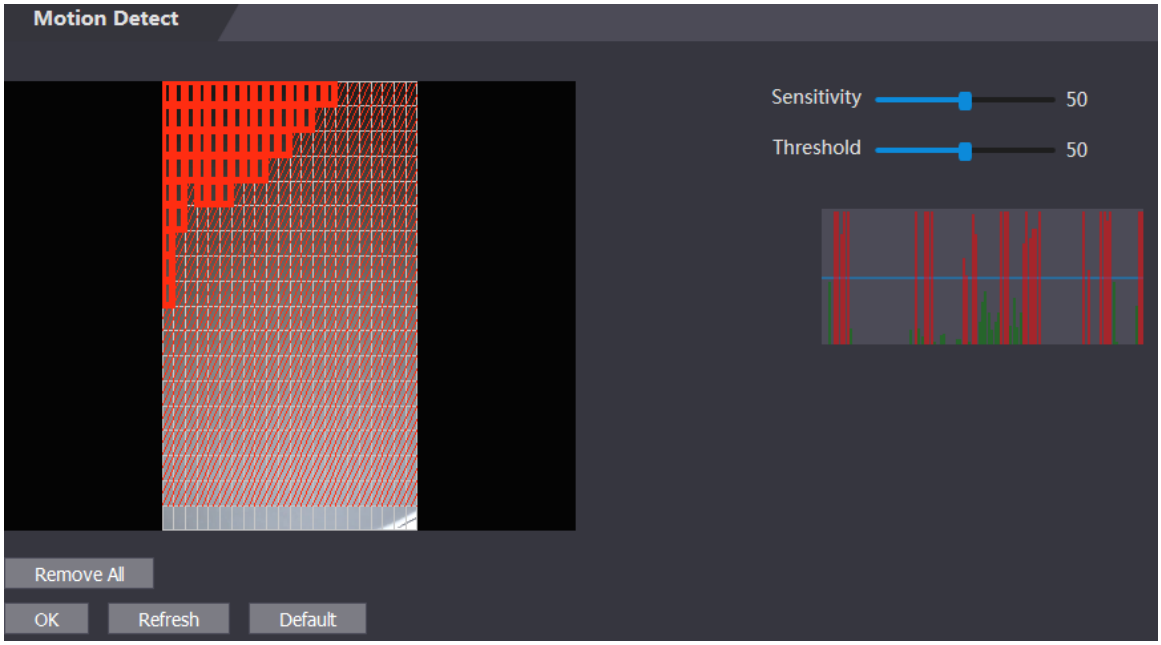
4.5.4 Motion Detection

Set a range in which moving objects can be detected.

Step 1 Select **Video Setting > Video Setting > Motion Detection**.

The **Motion Detection** interface is displayed. See Figure 4-14.

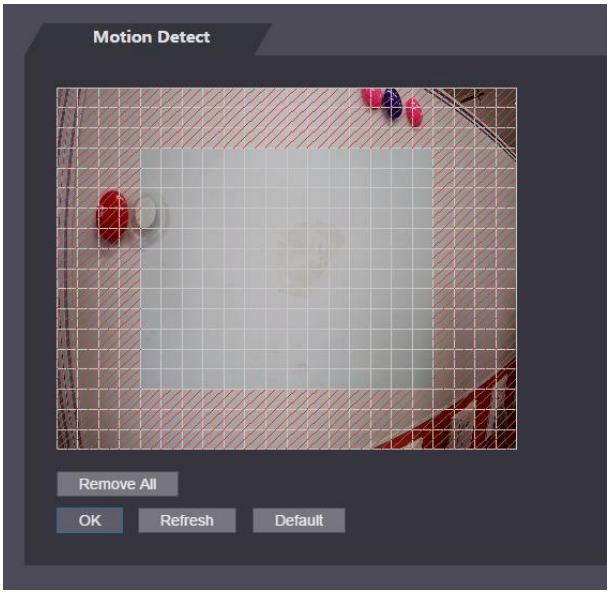
Figure 4-14 Motion detection



Step 2 Press and hold the left mouse button, and then drag the mouse in the red area. The **Motion Detection** area is displayed. See Figure 4-15.

- The red rectangles are motion detection area. The default motion detection range is all the rectangles.
- To draw a motion detection area, you need to click **Remove All** first.
- The motion detection area you draw will be a non-motion detection area if you draw in the default motion detection area.

Figure 4-15 Motion detection area



Step 3 Set sensitivity and threshold.

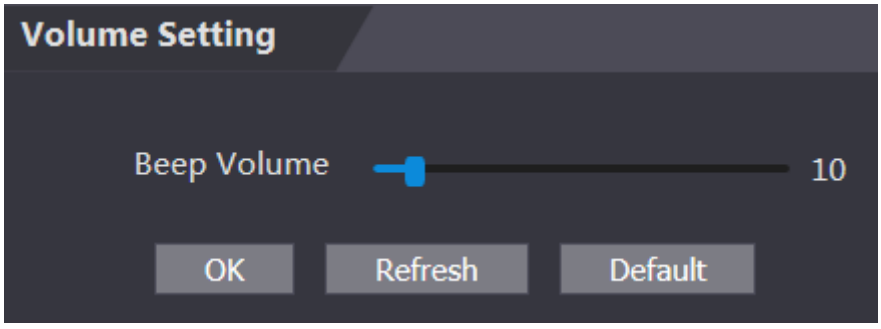
- Sensitivity represents the ability of each grid to sense motion. The larger the value is, the higher the sensitivity is.
- Threshold is the condition of motion detection. When grid number reaches the threshold, motion detection will be triggered. The smaller the value is, the more likely the motion detection will be triggered.
- When grid number is smaller than the threshold, green line will appear; when grid number is more than the threshold, red line will appear. See Figure 4-14.

Step 4 Click **OK** to finish the setting.

4.5.5 Volume Setting

You can adjust volume of the terminal speaker.

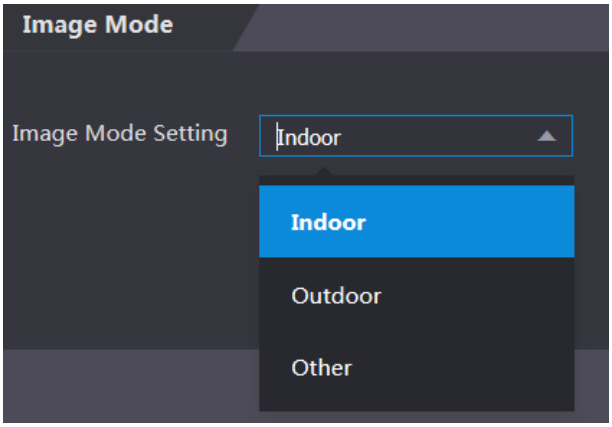
Figure 4-16 Volume setting



4.5.6 Image Mode

There are three options: indoor, outdoor and other. Select **Indoor** when the terminal is installed indoors; select **Outdoor** when the terminal is installed outdoors; and select **Other** when the terminal is installed at places with backlights like corridors and hallways.

Figure 4-17 Image mode



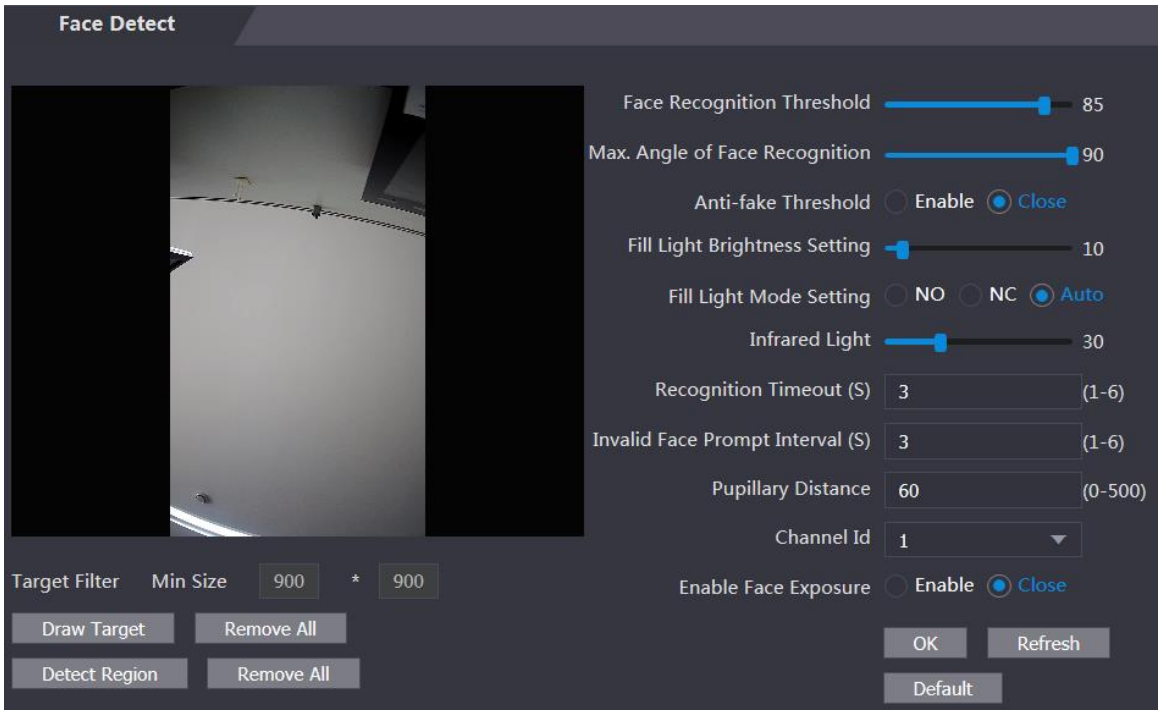
4.6 Face Detect

You can configure human face related parameters on this interface to increase the accuracy of the face recognition.

Step 1 Select **Face Detect**.

The **Face Detect** interface is displayed. See Figure 4-18.

Figure 4-18 Face detect



Step 2 Configure parameters. See Table 4-5.

Table 4-5 Face detect parameter description

Parameter	Description
Face Recognition Threshold	The larger the value is, the higher the accuracy will be.
Max. Angle of Face Recognition	The larger the angle is, the wider range of the profiles will be recognized.
Anti-fake Threshold	This function prevents people from unlocking by human face images or human face models.

Parameter	Description
	The larger the value is, the more difficult face images or human face models can unlock the door.
Fill Light Brightness Setting	You can set fill light brightness.
Fill Light Mode Setting	There are three fill light modes. ● NO: Fill light is normally open. ● NC: Fill light is normally closed. ● Auto: Fill light will be automatically on when a motion detection event is triggered. When **Auto** is selected, the fill light will not be on even if Infrared Light value is greater than 19.
Infrared Light	Adjust IR brightnees by dragging the scroll bar.
Recognition Timeout	When a person who does not have the access authority stands in front of the terminal and gets the face recognized, the terminal will prompt that face recognition failed. The prompt interval is called recognition timeout.
Invalid Face Prompt Interval	When a face has no access authority stands in front of the terminal, the terminal will prompt that the face is invalid. The prompt interval is invalid face prompt interval.
Pupillary Distance	Pupillary distance is the pixel value of the image between the centers of the pupils in each eye. You need to set an appropriate value so that the terminal can recognize faces as needed. The value changes according to the face sizes and the distance between faces and the lens. The closer the face is to the lens, the greater the value should be. If an adult is 1.5 meters away from the lens, the pupillary distance value can be within 50 to 70.
Enable Face Exposure	After face exposure is enabled, human face will be clearer when the terminal is installed outdoors.
Channel Id	There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
Draw Target	Click **Draw Target**, and then you can draw the minimum face detection frame. Click **Remove All**, and you can remove all the frames you drew.
Detect Region	Click **Detect Region**, move your mouse, and you can adjust the face detection region. Click **Remove All**, and you can remove all the detection regions.

Step 3 Click **OK** to finish the setting.

4.7 Network Setting

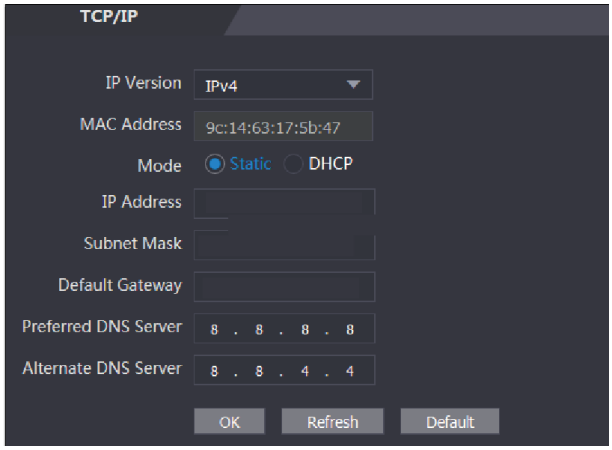
4.7.1 TCP/IP

You need to configure IP address and DNS server to make sure that the terminal can communicate with other devices.

Make sure that the terminal is connected to the network correctly.

Step 1 Select **Network Setting > TCP/IP**.

Figure 4-19 TCP/IP



Step 2 Configure parameters.

Table 4-6 TCP/IP

Parameter	Description
IP Version	There is one option: IPv4.
MAC	MAC address of the **terminal** is displayed.
Mode	● Static Set IP address, subnet mask, and gateway address manually. ● DHCP ◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured. ◇ If DHCP is effective, IP address, subnet mask, and gateway address will be displayed automatically; if DHCP is not effective, IP address, subnet mask, and gateway address will all be zero. ◇ If you want to see the default IP when DHCP is effective, disable DHCP.
Link-local Address	Link-local address is only available when IPv6 is selected in the IP version. Unique link-local addresses will be assigned to network interface controller in each local area network to enable communications. The link-local address cannot be modified.
IP Address	Enter IP address, and then configure subnet mask and gateway address. IP address and gateway address must be in the same network segment.
Subnet Mask	
Gateway	
Preferred DNS Server	Set IP address of the preferred DNS server.
Alternate DNS Server	Set IP address of the alternate DNS server.

Step 3 Click **OK** to complete the setting.

4.7.2 Port

Set the maximum connections clients that the terminal can be connected to and port numbers.

Step 1 Select **Network Setting > Port**.

The **Port** interface is displayed.

Step 2 Configure port numbers. See the following table.

Except max connection, you need to reboot the terminal to make the configuration effective after modifying values.

Table 4-7 Port description

Parameter	Description
Max Connection	You can set the maximum connections of clients that the terminal can be connected to. Platform clients like Smartpss are not counted.
TCP Port	Default value is 37777.
HTTP Port	Default value is 80. If other value is used as port number, you need to add this value behind the address when logging in through browsers.
HTTPS Port	Default value is 443.
RTSP Port	Default value is 554.

Step 3 Click **OK** to complete the setting.

4.7.3 Register

When connected to external network, the terminal will report its address to the server that is designated by the user so that clients can get access to the terminal.

Step 1 Select **Network Setting > Auto Register**.

The **Auto Register** interface is displayed.

Step 2 Select **Enable**, and enter host IP, port, and sub device ID.

Table 4-8 Auto register description

Parameter	Description
Host IP	Server IP address or server domain name.
Port	Server port used for auto registeration.
Sub Device ID	Terminal ID assigned by the server.

Step 3 Click **OK** to complete the setting.

4.7.4 P2P

Peer-to-peer computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Users can download mobile application by scanning QR code, and then register an account so that more than one terminal can be managed on the mobile app. You do not need to apply dynamic domain name, do port mapping or do not need transit server.

If you are to use P2P, you must connect the terminal to external network; otherwise the terminal cannot be used.

Figure 4-20 P2P

Step 1 Select **Network Setting > P2P**.

The **P2P** interface is displayed.

Step 2 Select **Enable** to enable P2P function.

Step 3 Click **OK** to complete the setting.

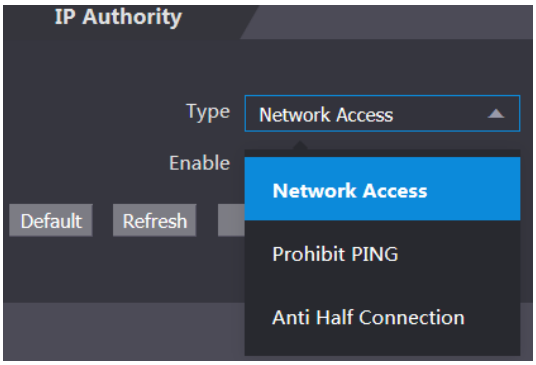
Scan the QR code on your web interface to get the serial number of the terminal.

4.8 Safety Management

4.8.1 IP Authority

Select a cyber security mode as needed.

Figure 4-21 IP authority



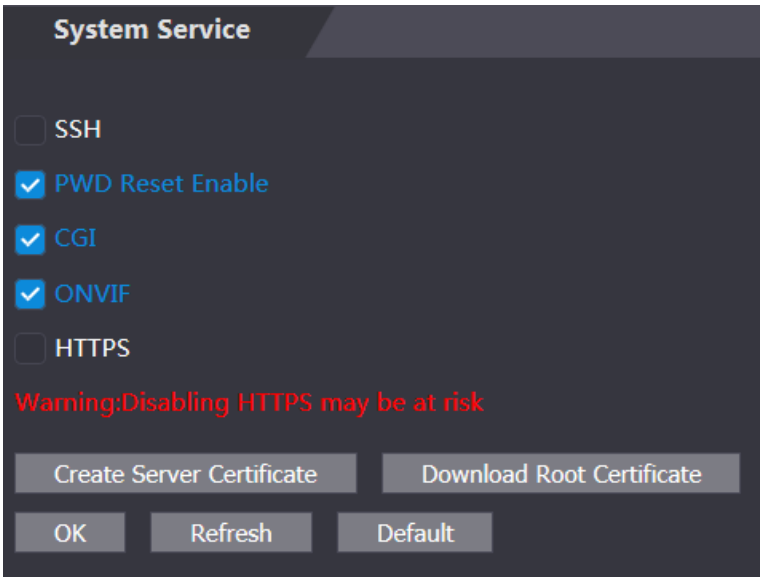
4.8.2 Systems

4.8.2.1 System Service

There are four options: SSH, PWD Reset Enable, CGI, and HTTPS. Refer to "3.9.4 Features" to select one or more than one of them.

The system service configuration done on the web page and the configuration on the **Features** interface of the terminal will be synchronized.

Figure 4-22 System service



4.8.2.2 Creating Server Certificate

Click **Create Server Certificate**, enter needed information, click **Save**, and then the terminal will reboot.

4.8.2.3 Downloading Root Certificate

Step 1 Click **Download Root Certificate**.
Select a path to save the certificate on the **Save File** dialog box.

Step 2 Double-click **Root Certificate** that you have downloaded to install the certificate. Install the certificate by following the onscreen instructions.

4.9 User Management

You can add and delete users, modify users' passwords, and enter an email address for resetting the password when you forget your password.

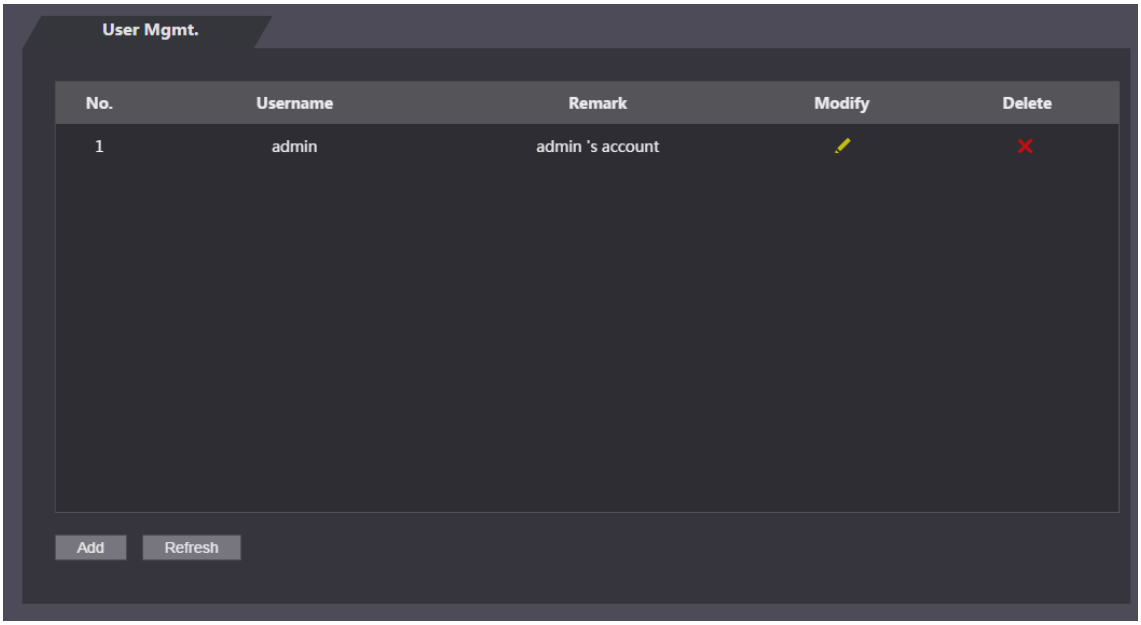
4.9.1 Adding Users

Click **Add** on the **User Mgmt.** interface to add users, and then enter username, password, confirmed password, and remark. Click **OK** to complete the user adding.

4.9.2 Modifying User Information

You can modify user information by clicking on the **User Mgmt.** interface. See Figure 4-23.

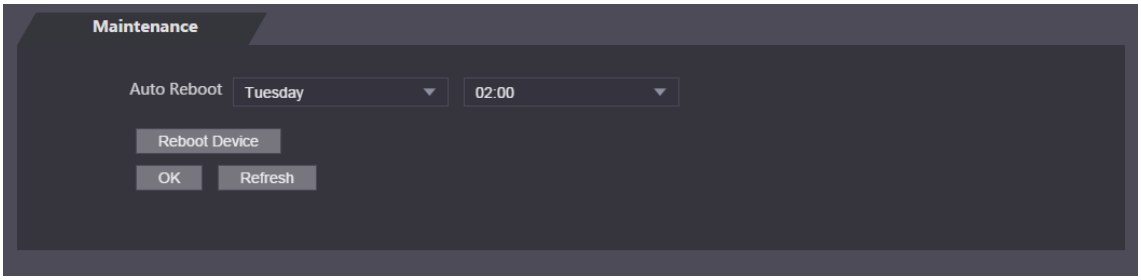
Figure 4-23 User management



4.10 Maintenance

You can make the terminal reboot itself in idle time to improve the running speed of the terminal. See Figure 4-24.

Figure 4-24 Maintenance

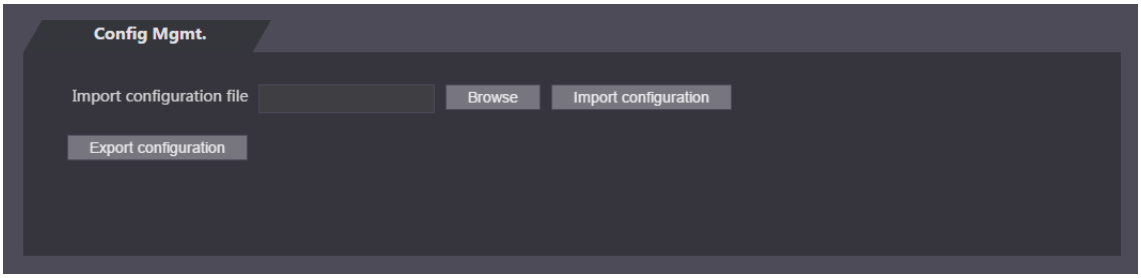


Select the auto reboot date and time. The default reboot time is at 2 O'clock in the morning on Tuesday. Click **Reboot Device**, the terminal will reboot immediately. Click **OK**, the terminal will reboot at 2 O'clock in the morning every Tuesday.

4.11 Configuration Management

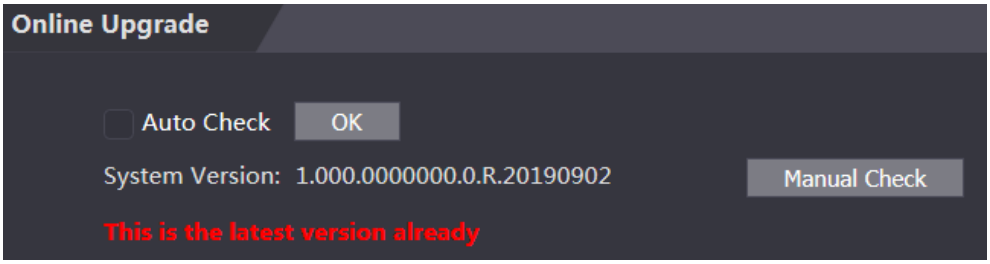
When more than one terminal needs the same configuration, you can configure parameters for them by importing or exporting configuration files. See Figure 4-25.

Figure 4-25 Configuration management



4.11.1 Upgrade

You can select **Auto Check** to upgrade the system automatically. You can also select **Manual Check** to upgrade the system manually.



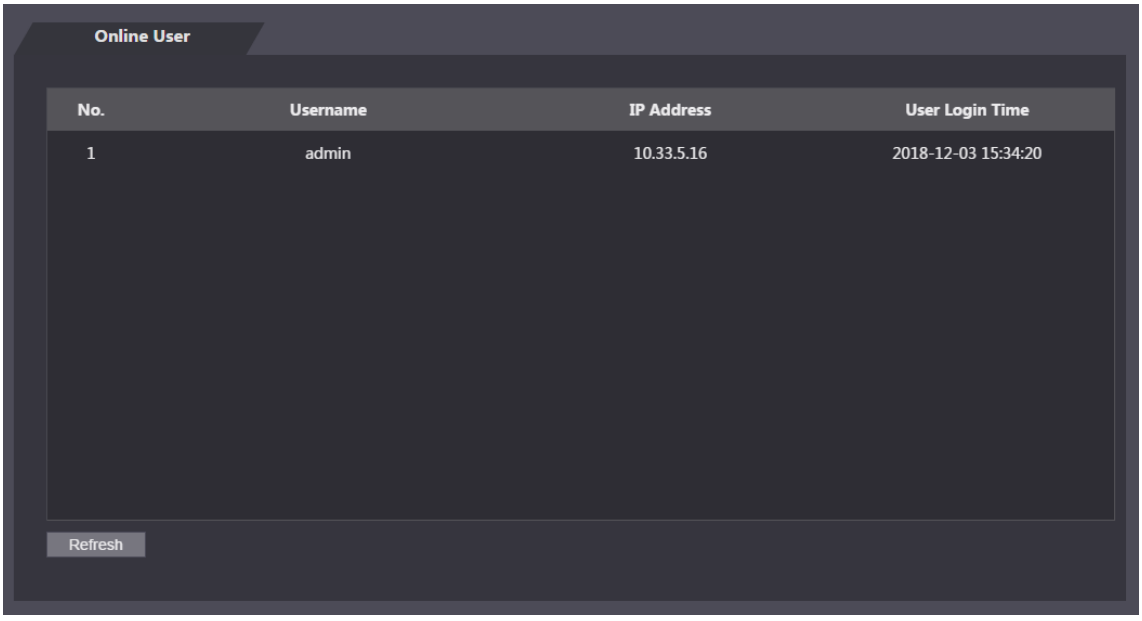
4.11.2 Version Information

You can view information including MAC address, serial number, MCU version, web version, security baseline version, and system version.

4.11.3 Online User

You can view username, IP address, and user login time on the **Online User** interface. See Figure 4-26.

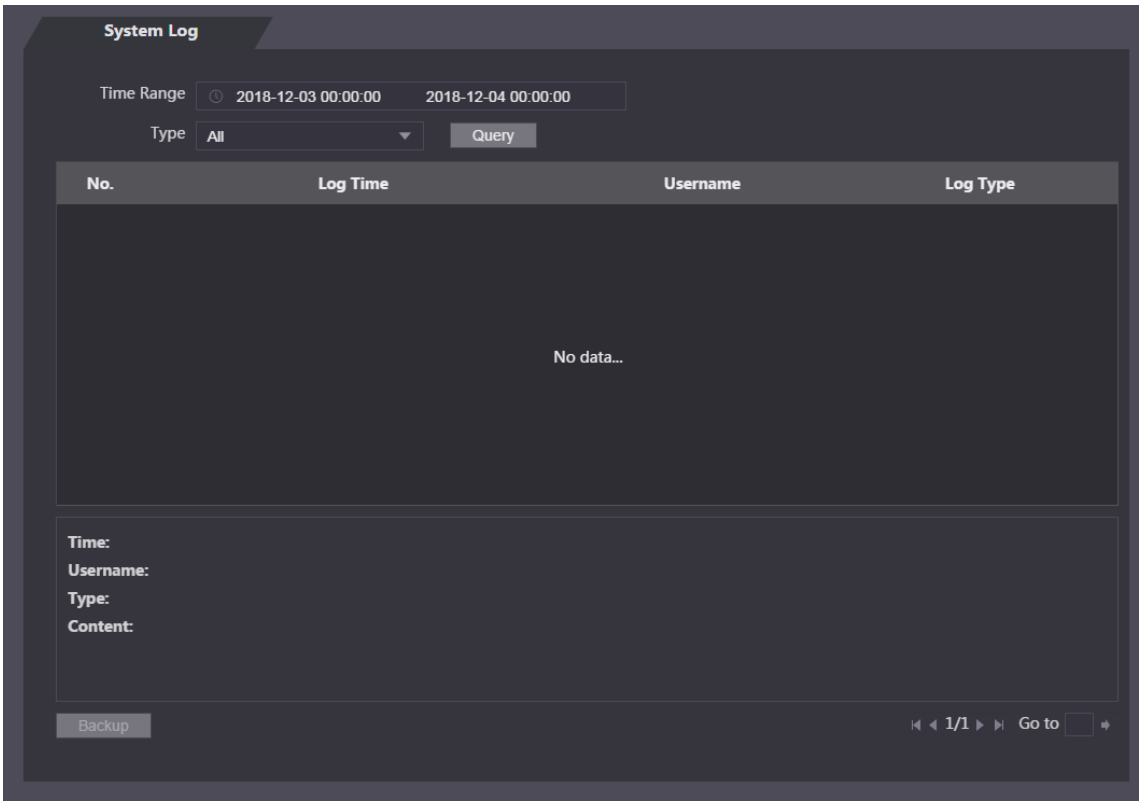
Figure 4-26 Online user



4.12 System Log

You can view and backup the system log on the **System Log** interface. See Figure 4-27.

Figure 4-27 System log



4.12.1 Querying Logs

Select a time range, type, click **Query**, and logs meet the conditions will be displayed.

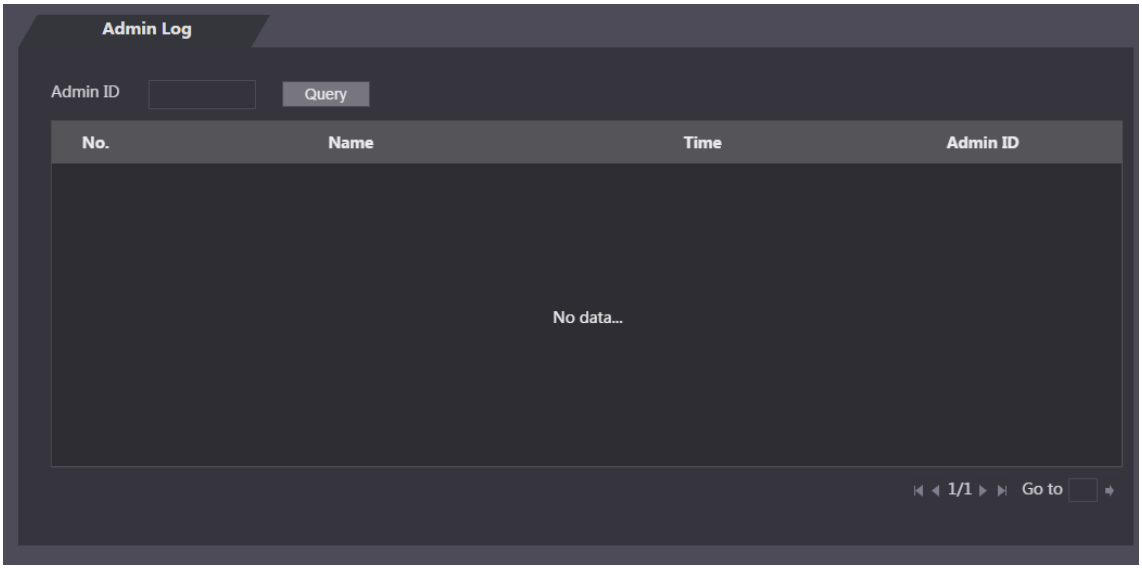
4.12.2 Backing up Logs

Click **Backup** to back up the logs displayed.

4.13 Admin Log

Enter Admin ID on the **Admin Log** interface, click **Query**, and then you will see the administrator's operation records. See Figure 4-28.

Figure 4-28 Admin log



Hover the mouse cursor over , and then you can see detailed information of the current user.

4.14 Exit

Click , click **OK**, and then you will log out the web interface.

5 SmartPSS Configuration

You can do access permission configuration to a single door or door groups through the Smart PSS client. For detailed configurations, see the SmartPSS user manual.

Smart PSS interfaces might vary with versions, and the actual interface shall prevail.

5.1 Login

Install the Smart PSS (the username is admin, and the password is admin123 by default), double-click

to operate it. Follow the instructions to finish the initialization and log in.

5.2 Adding Devices

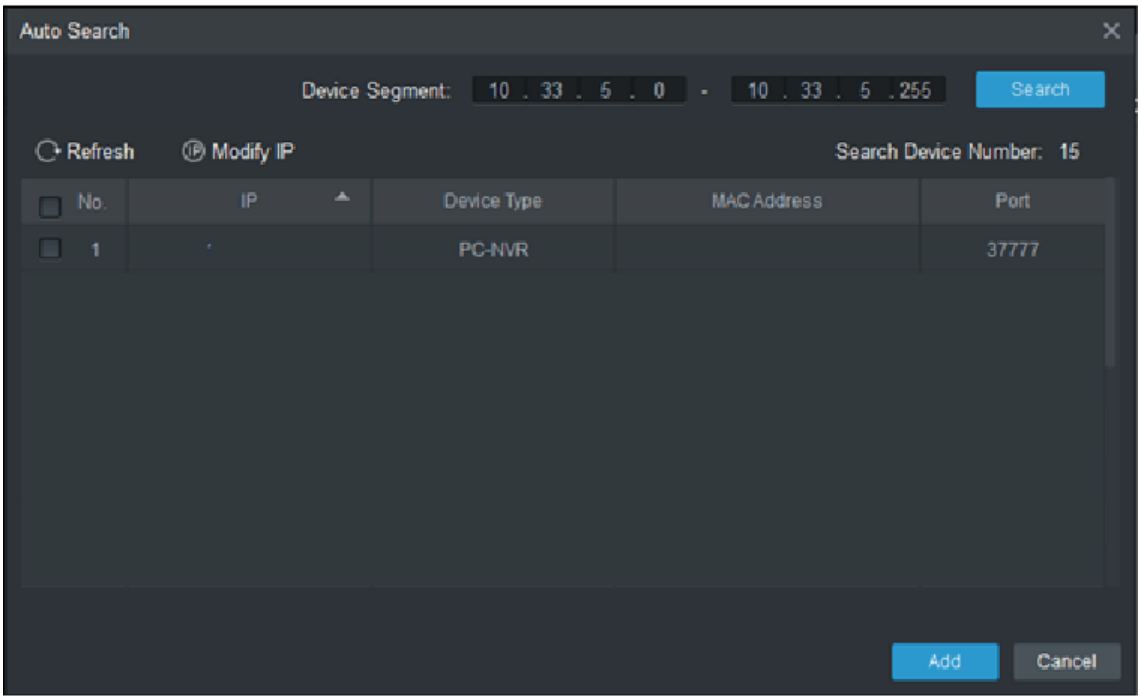
You need to add terminals to the Smart PSS. You can click **Auto Search** to add and click **Add** to manually add.

5.2.1 Auto Search

You can search and add terminals at the same network segment to the SmartPSS. See Figure 5-1 and Figure 5-2.

Figure 5-1 Devices

Figure 5-2 Auto search



Step 1 Click **Auto Search**, enter the network segment, and then click **Search**. A list will be displayed.

Step 2 Select terminals that you want to add to the Smart PSS, and then click **Add**, the **Login information** dialog box will be displayed.

Step 3 Enter the username and the login password to login.

You can see the added terminal on the **Devices** interface.

Select a terminal, click **Modify IP**, and you can modify the terminal's IP address. For details about IP address modification, see Smart PSS user manual.

5.2.2 Manual Add

You need to know IP addresses and domain names of terminals that you want to add. See Figure 5-3 and Figure 5-4.

Figure 5-3 Devices

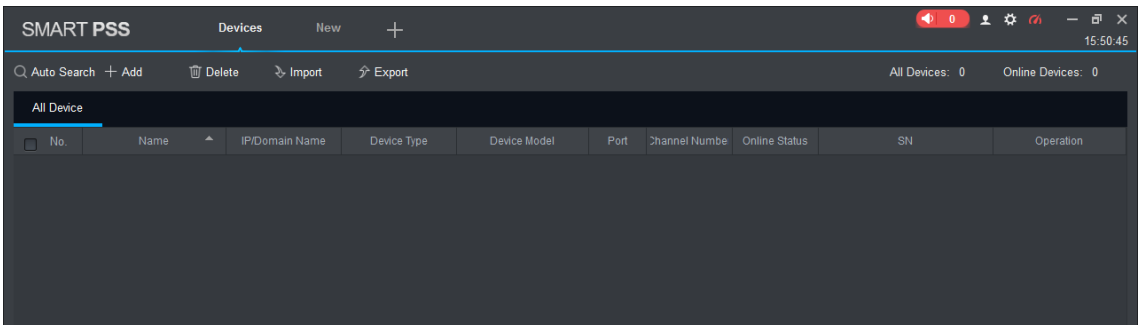
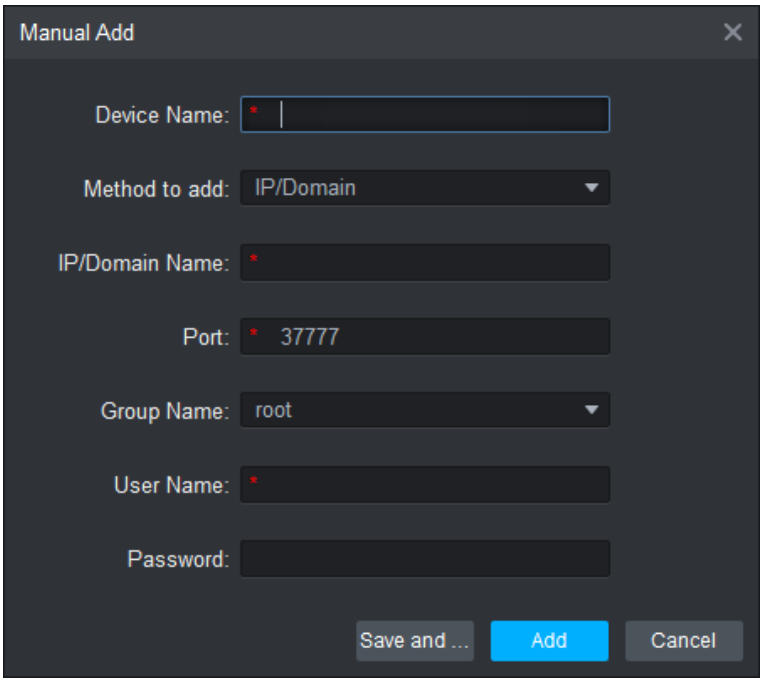


Figure 5-4 Manual add



Step 1 Click **Add** on the **Devices** interface, and the **Manual Add** interface will be displayed.

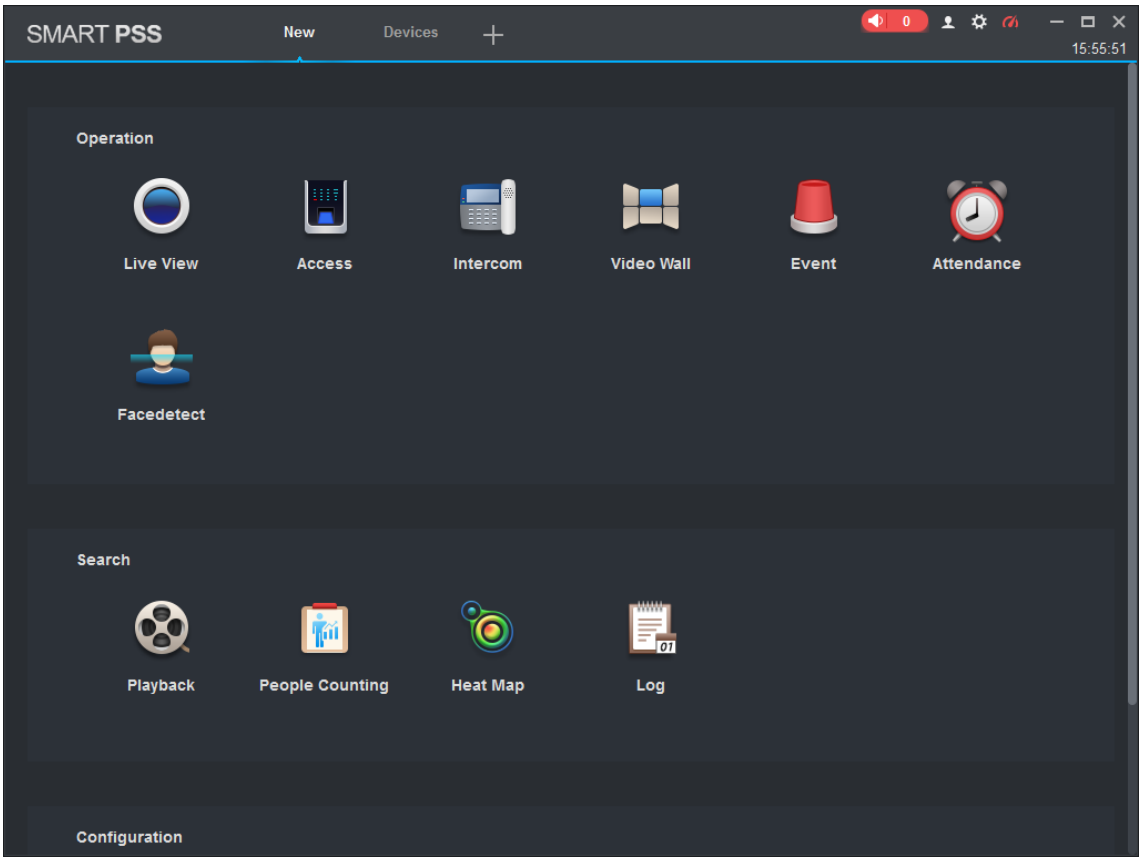
Step 2 Enter the **Device Name**, select a method to add, enter the **IP/Domain Name**, **Port number** (37777 by default), **Group Name**, **User Name**, and **Password**.

Step 3 Click **Add**, and then you can see the added terminal on the **Devices** interface.

5.3 Adding Users

Users are bound with cards. After you have added users to the Smart PSS, you can configure users access permissions on the **New > Access**. See Figure 5-5.

Figure 5-5 New



5.3.1 Card Type Selection

Card types must be the same as card issuer types, otherwise card numbers cannot be read.

On the **Access** interface, click , then click the IC or ID card icon, and then select a card type. There are two options: ID Card and IC Card. See Figure 5-6 and Figure 5-7.

Figure 5-6 Access

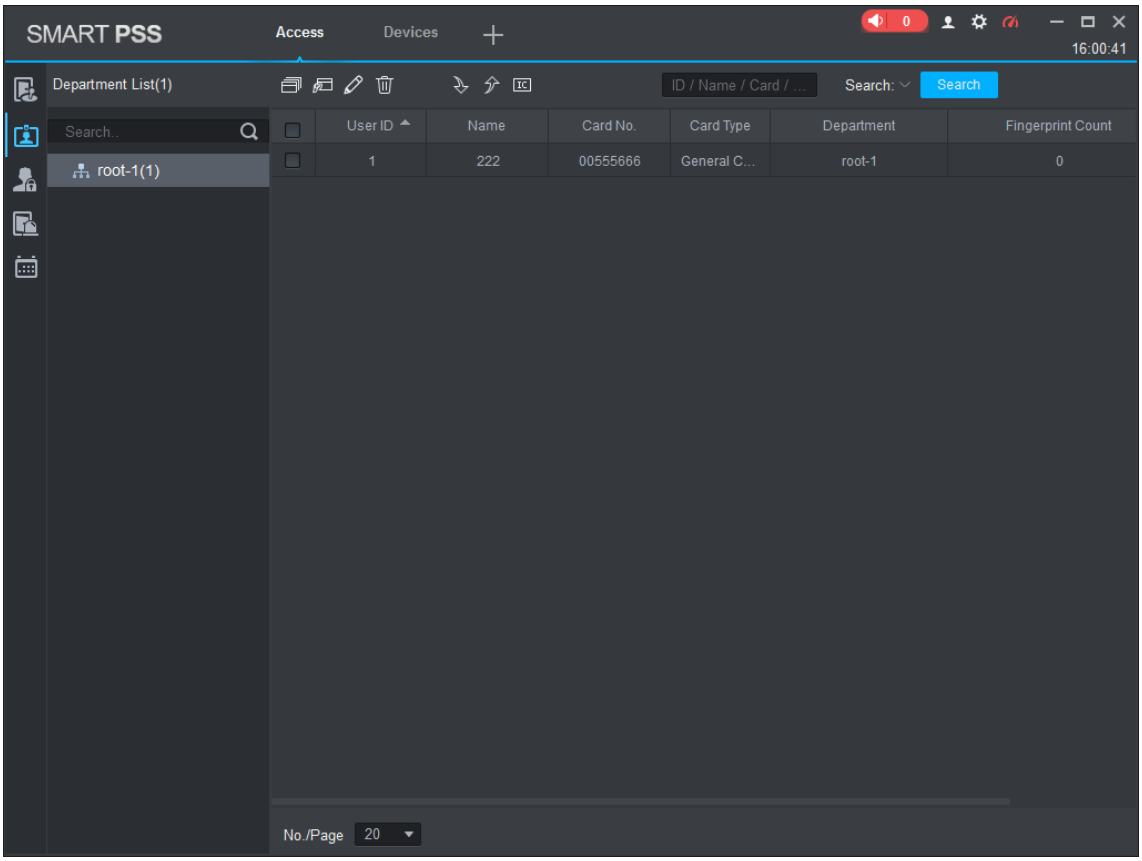
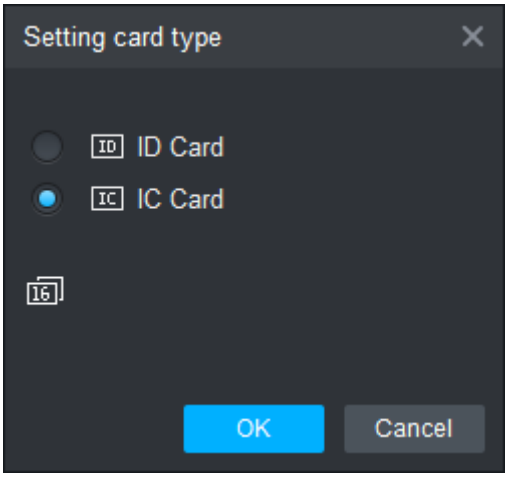


Figure 5-7 Setting card type



5.3.2 Adding One User

You can add users one by one.

On the **Access** interface, click , then click , and then enter user's information. Click **Finish** to complete the user adding. See Figure 5-8 and Figure 5-9.

Figure 5-8 Access

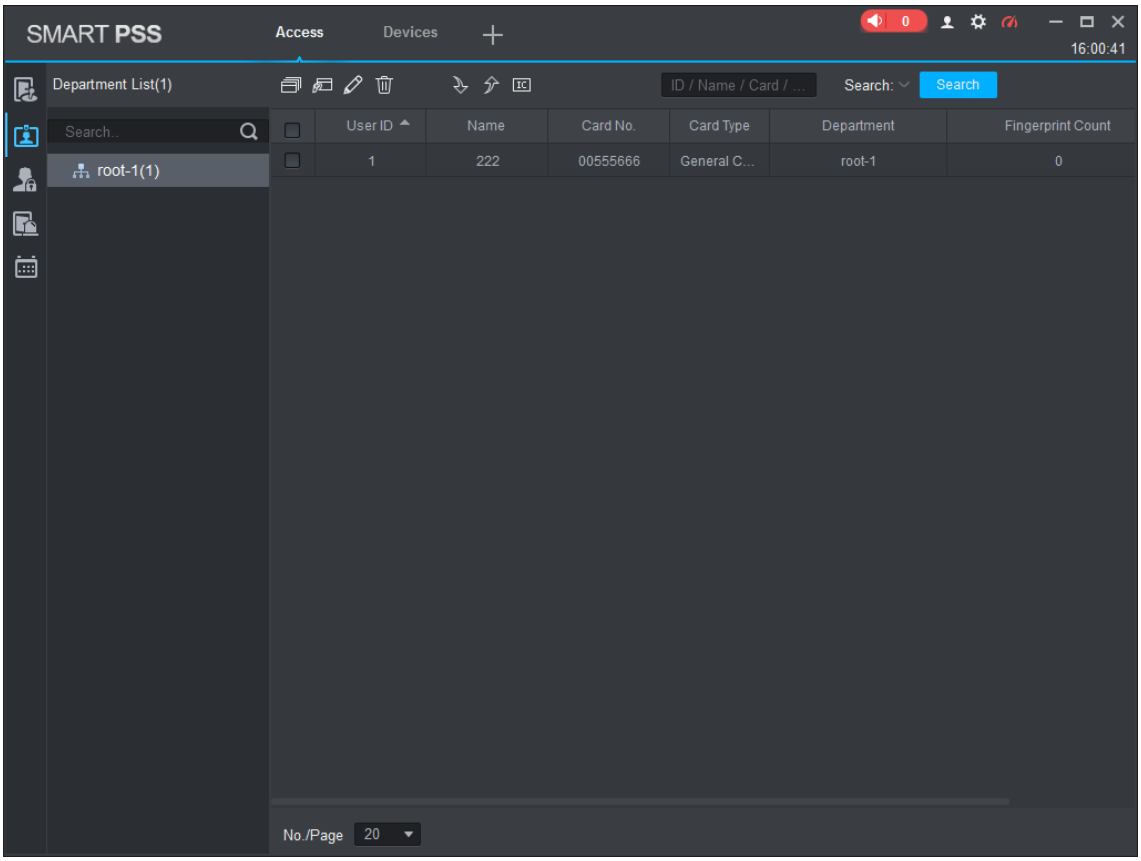
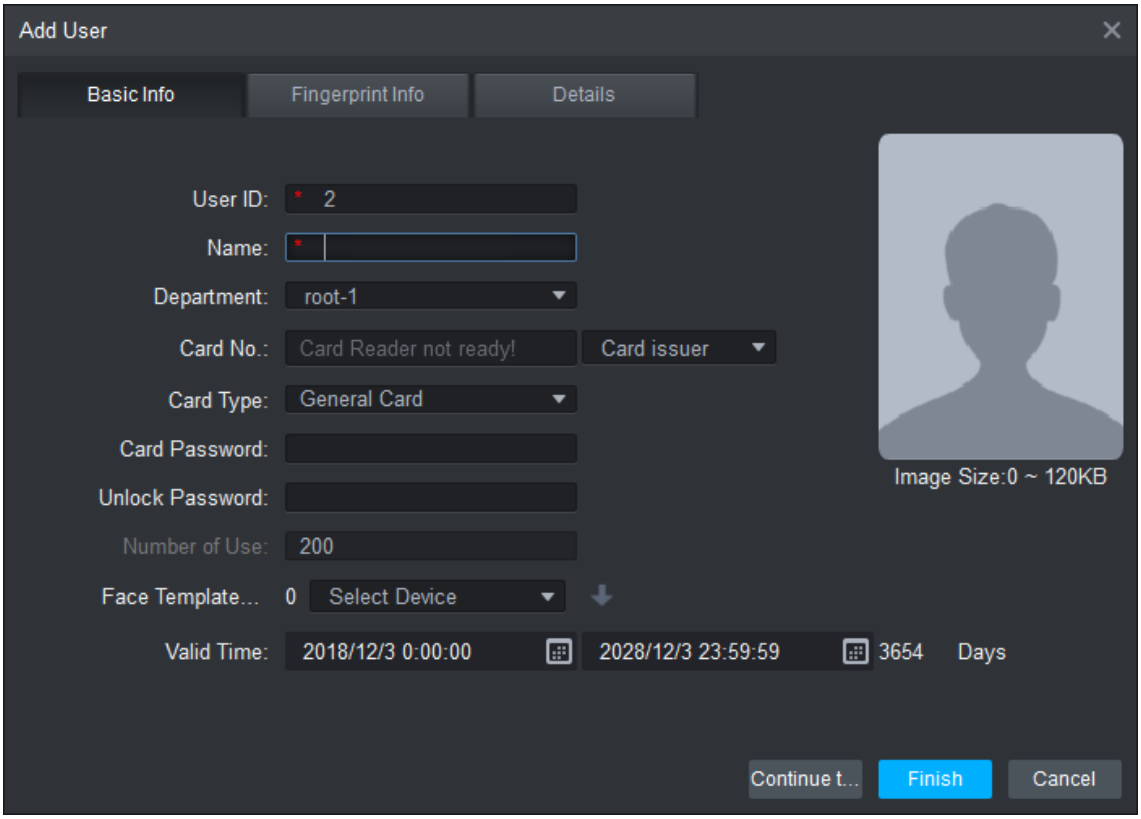


Figure 5-9 Add user



5.4 Adding Door Group

You can manage doors by grouping doors.

On the **Access** interface, click , click **Add**, enter door group name, select a time zone. Click **Finish** to complete the user adding. See Figure 5-10 and Figure 5-11.

Figure 5-10 Access

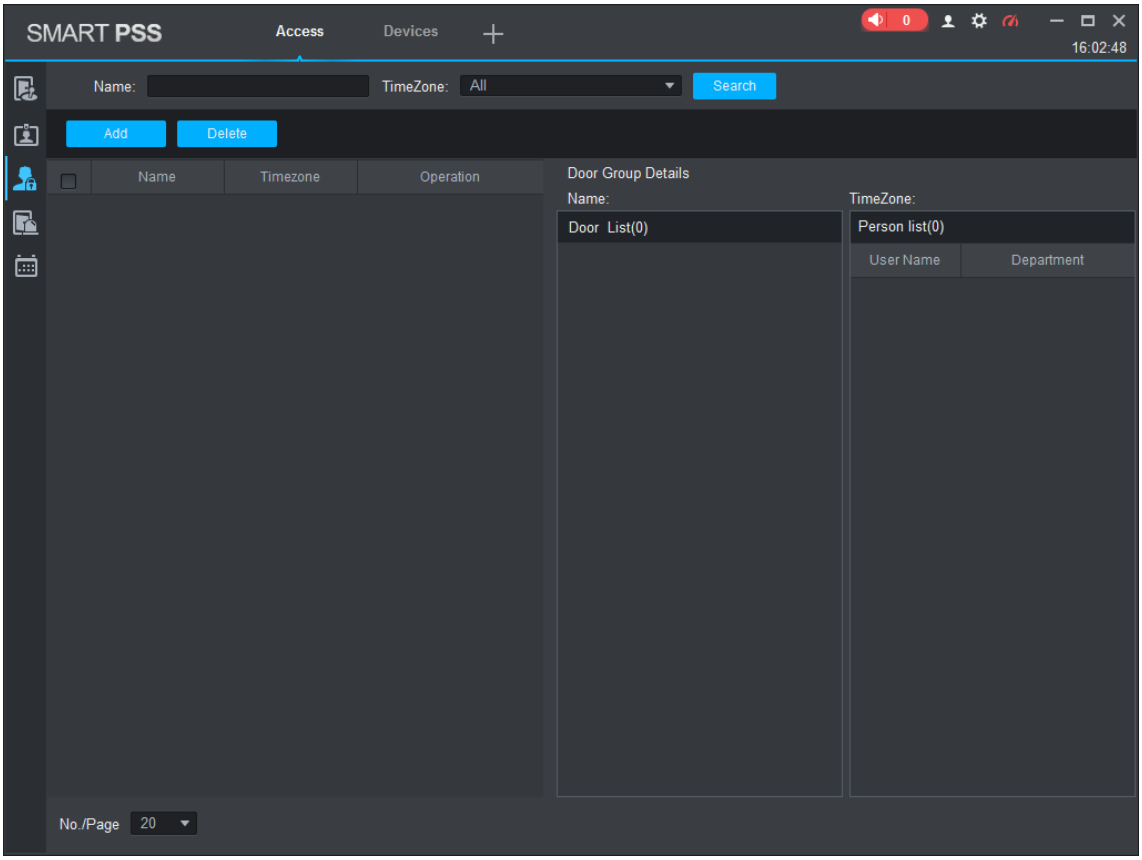
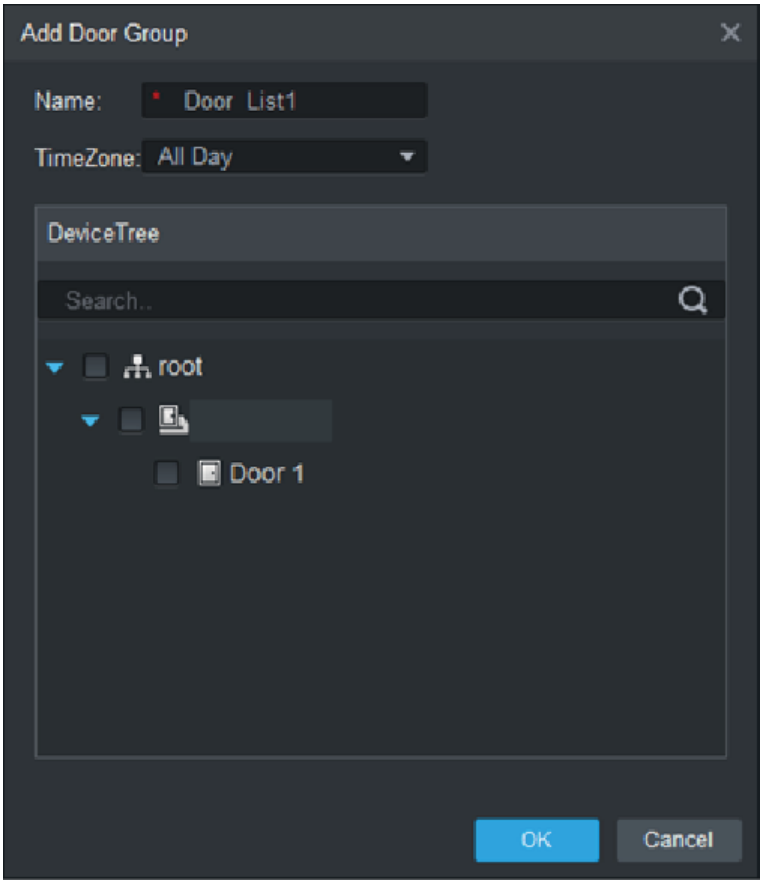


Figure 5-11 Add door group



5.5 Access Permission Configuration

You can do access permission configuration. There are two options: door group access permission and user access permission. Information of users who are given access permission in the Smart PSS and terminals will be synchronized.

5.5.1 Giving Permission by Door Group

Select a door group, add users to the door list, and then users on the door list get access permissions of all doors on the door list. See Figure 5-12 and Figure 5-13.

Figure 5-12 Access

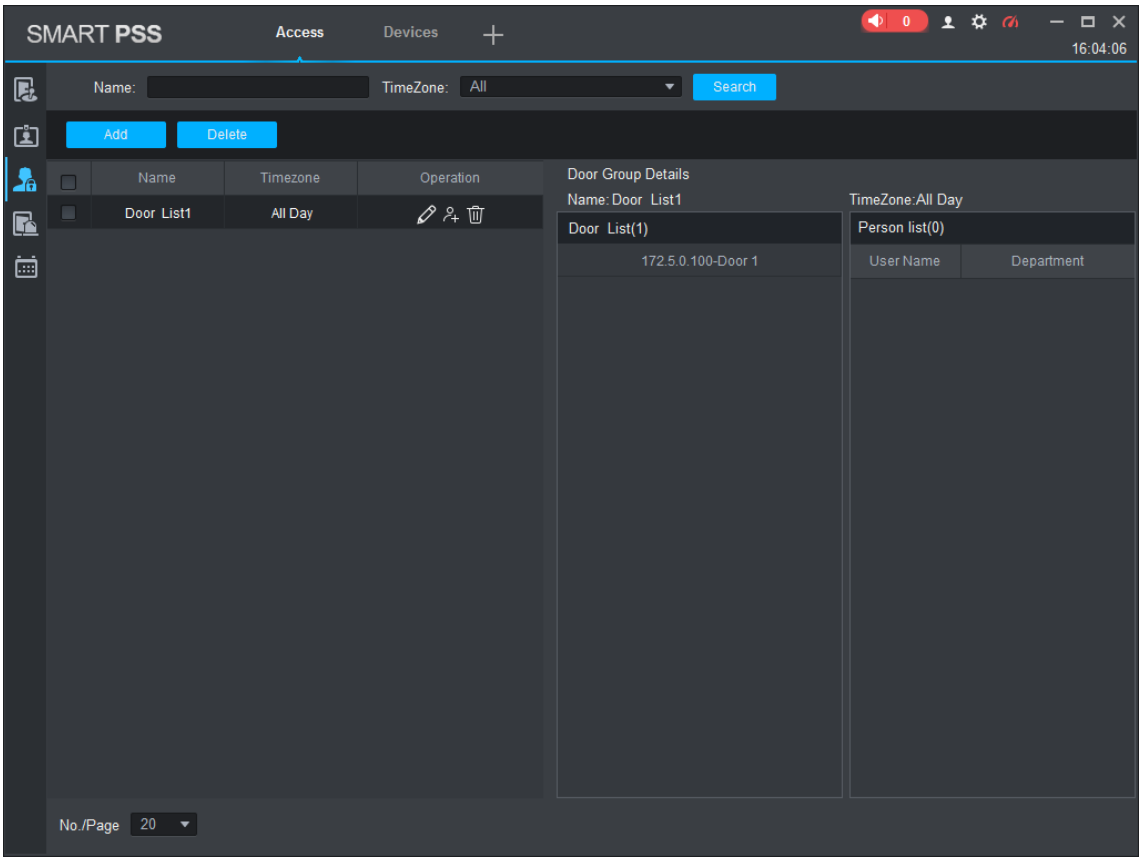
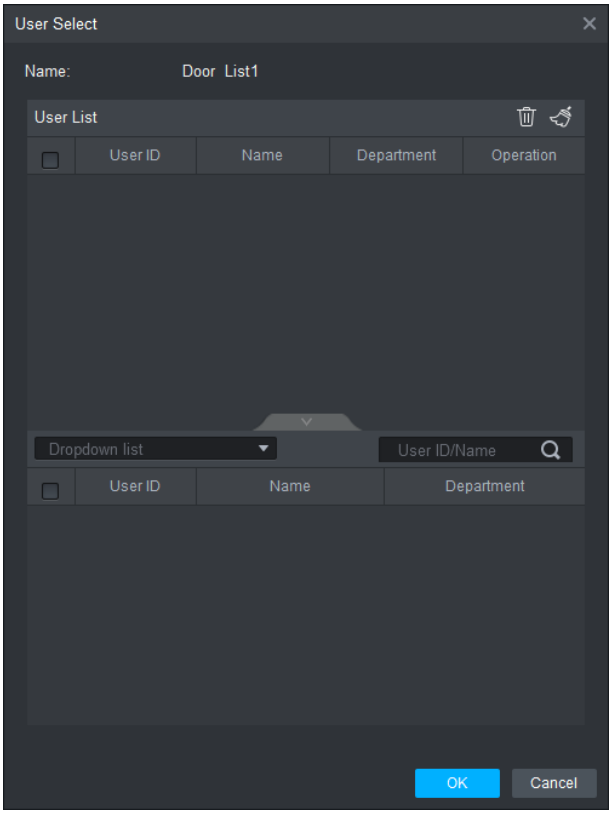


Figure 5-13 User select



Step 1 On the **Access** interface, click , click **Add**, click **Door Group Permission**.

Step 2 Click . Select user department in the Dropdown list, or enter user **ID/Name**, and

then search users. Select users from the users you found.

Step 3 Click **Finish** to complete the configuration.

Users without user ID cannot be found.

5.5.2 Giving Permission by User ID

You can give access permission to a user by selecting a user, and then select door groups for the user. See Figure 5-14 and Figure 5-15.

Figure 5-14 Access

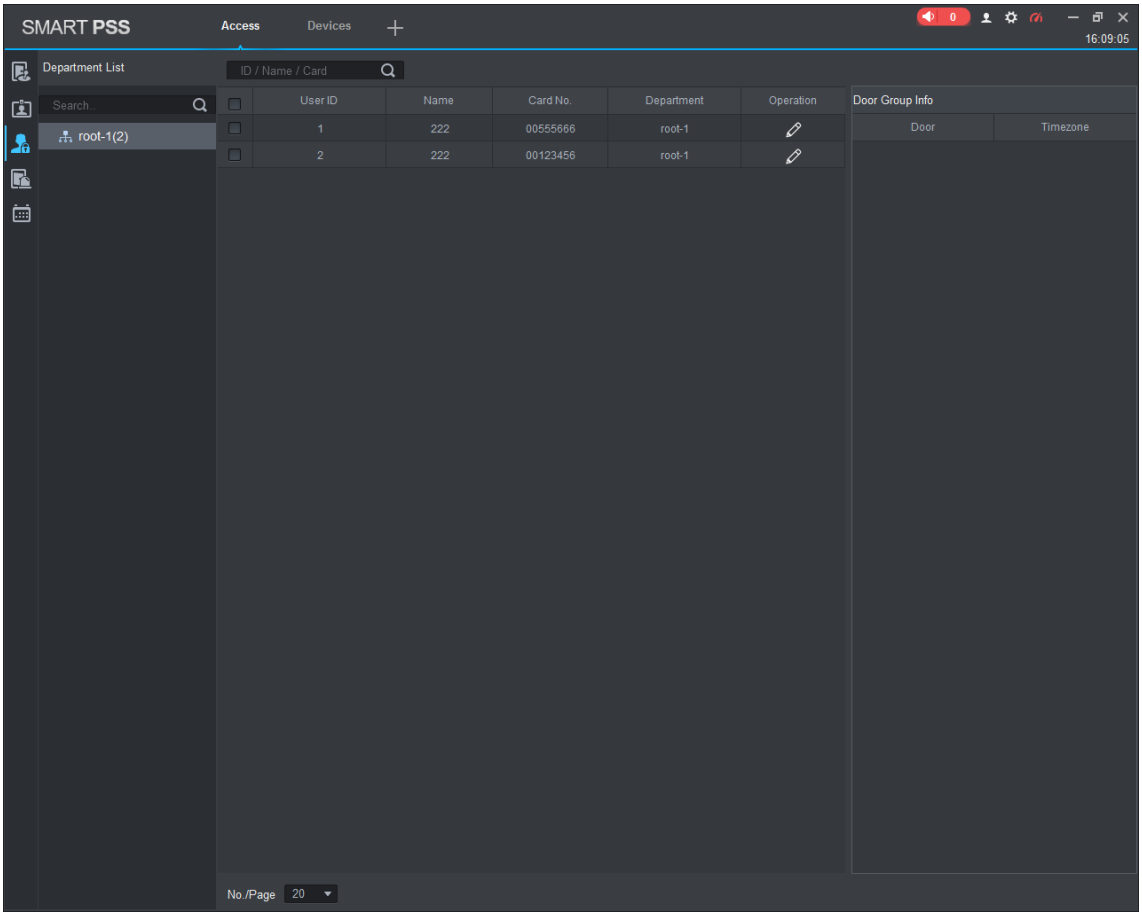
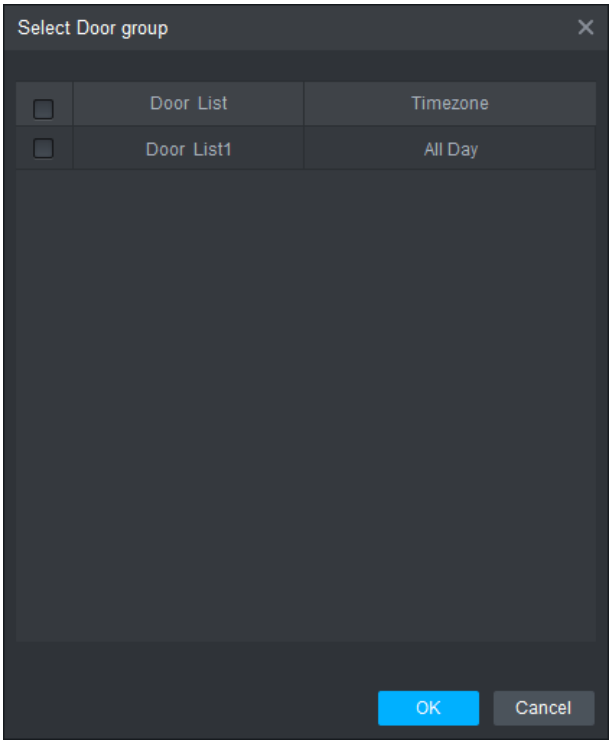


Figure 5-15 Select door group



Step 1 On the **Access** interface, click .

Step 2 Click . The **Select Door Group** interface is displayed.

Step 3 Select user department in the dropdown list, or enter user **ID/Name**, and then select a door list.

Step 4 Click **Finish** to complete the configuration.

Appendix 1 Notes of Face Recording/Comparison

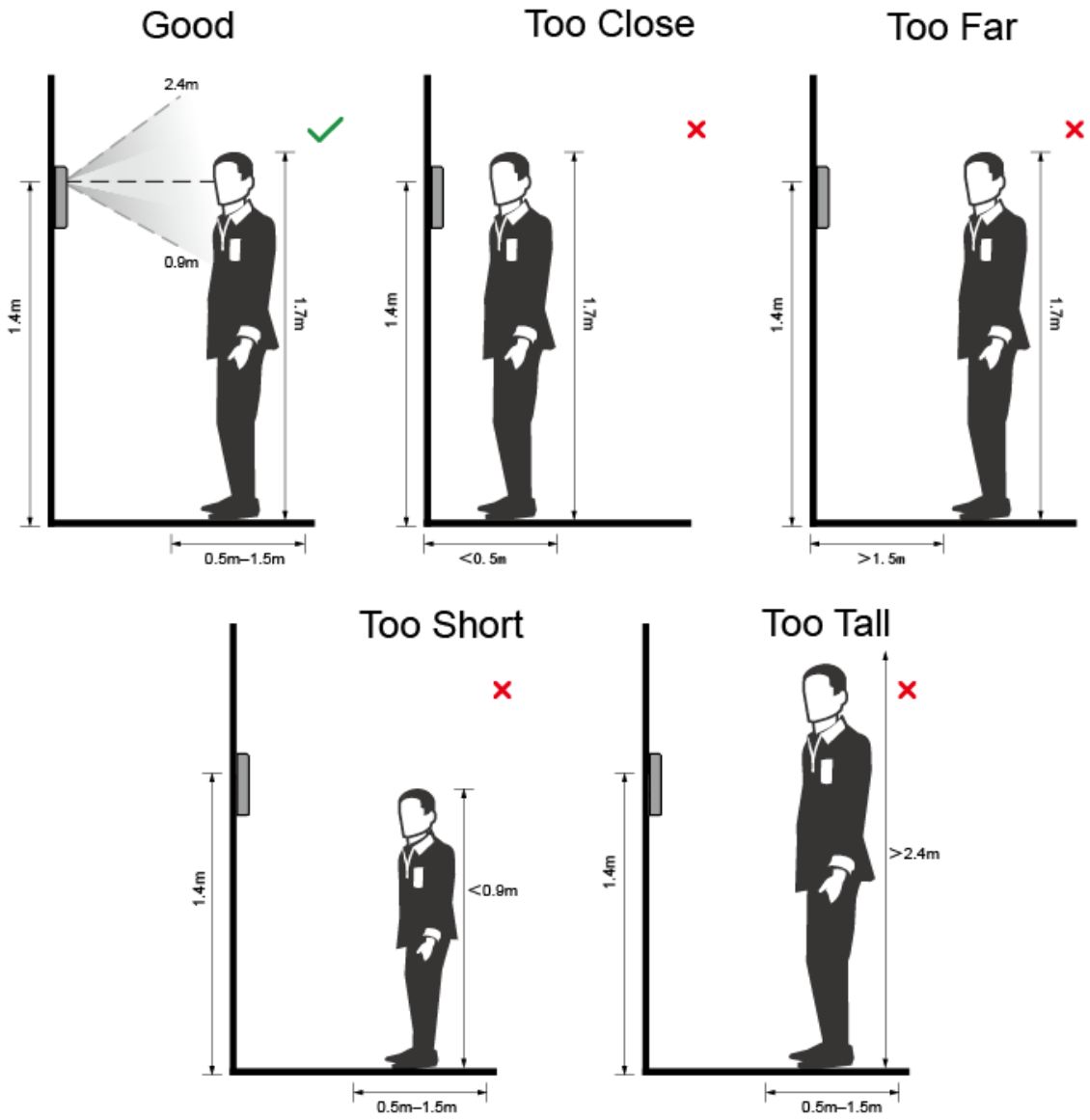
Before Registration

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

Face Position

If your face is not at the appropriate position, face recognition effect might be influenced.

Appendix figure 1-1 Appropriate face position

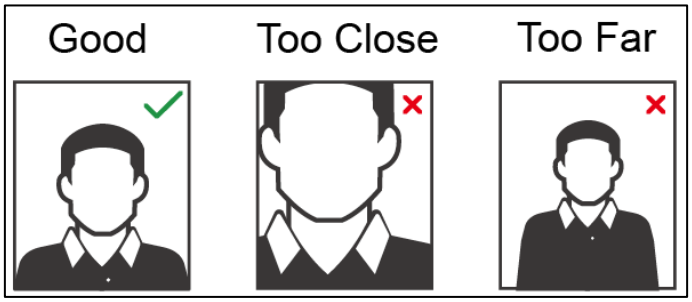


Requirements of Faces

- 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



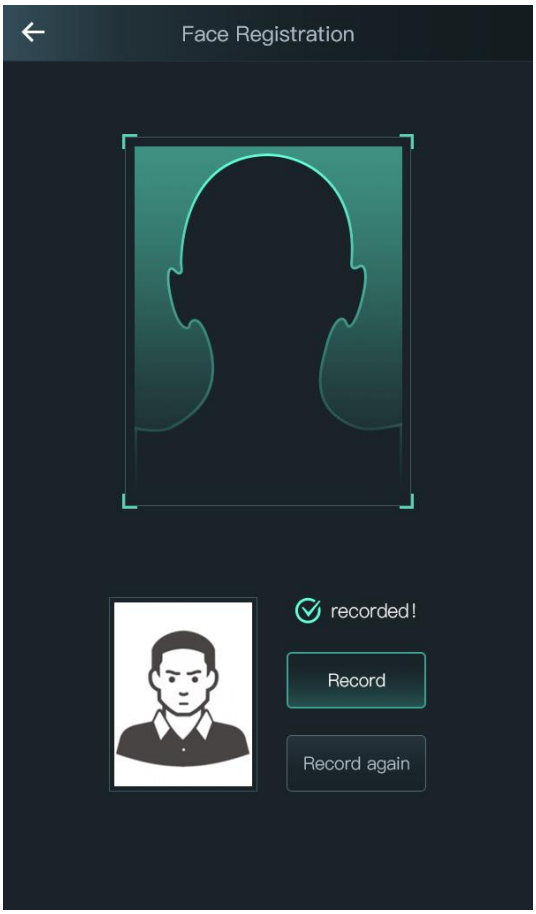
- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300–600 × 1200; image pixels are more than 500 × 500; image size is less than 75 KB, and image name and person ID are the same.
- Make sure that face does not take 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

During Registration

You can register faces through the terminal or through the platform. For registration through the platform, see the platform user manual.

Make your head center on the photo capture frame. A picture of your face will be captured automatically.

Appendix figure 1-4 Registration



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

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **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.

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **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.

13. **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.

14. **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.

Face Recognition Terminal

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation and basic operation of the Face Recognition Terminal (hereinafter referred to as "terminal").

Safety Instructions

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

Signal Words	Meaning
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

Version	Revision Content	Release Date
V1.0.0	First release	November 2019

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual 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.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operation Requirement

- Do not place or install the terminal in a place exposed to sunlight or near the heat source.
- Keep the terminal away from dampness, dust or soot.
- Keep the terminal installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the terminal, and make sure there is no object filled with liquid on the terminal to prevent liquid from flowing into the terminal.
- Install the terminal in a well-ventilated place, and do not block the ventilation of the terminal.
- Operate the terminal within the rated range of power input and output.
- Do not dissemble the terminal.
- Transport, use and store the terminal under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the terminal; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **II**
1 Dimensions and Components **1**
2 Installation **4**
2.1 Installation Notes 4
2.2 Installation Drawings 5
2.3 Cable Connections 6
2.4 Installation 8
3 System Operation **10**
3.1 Initialization 10
3.2 Adding New Users 10
4 Web Operation **13**
Appendix 1 Notes of Face Recording/Comparison **14**
Appendix 2 Cybersecurity Recommendations **18**

1 Dimensions and Components

The terminal has two dimensions: 7-inch and 10-inch. For details, see Figure 1-1 to Figure 1-3.

The 7-inch terminal has two models: model A and model B. For details, see Figure 1-1 and Figure 1-2.

7-Inch Terminal

Figure 1-1 Dimensions and components of model A (mm [inch])

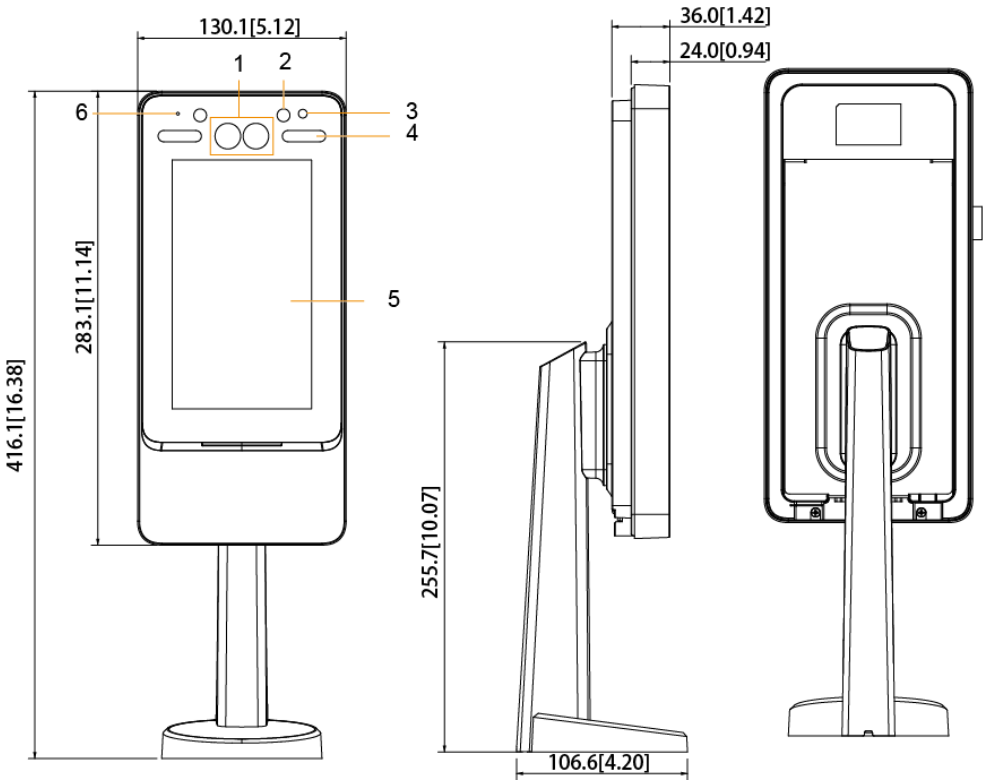


Table 1-1 Component description (1)

No.	Name
1	Dual camera
2	IR light
3	Phototransistor
4	White fill light
5	Display
6	MIC

Figure 1-2 Dimensions and components of model B (mm [inch])

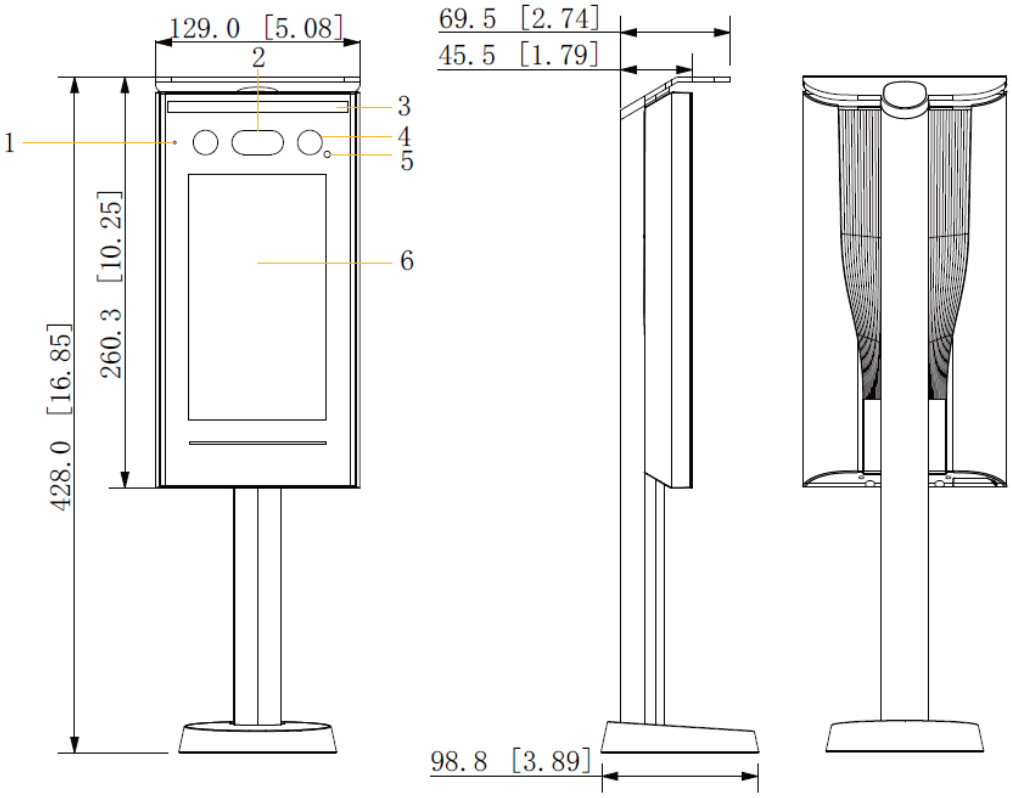


Table 1-2 Component description (2)

No.	Name
1	MIC
2	Dual camera
3	White fill light
4	IR light
5	Phototransistor
6	Display

10-Inch Terminal

Figure 1-3 Dimensions and components (mm [inch])

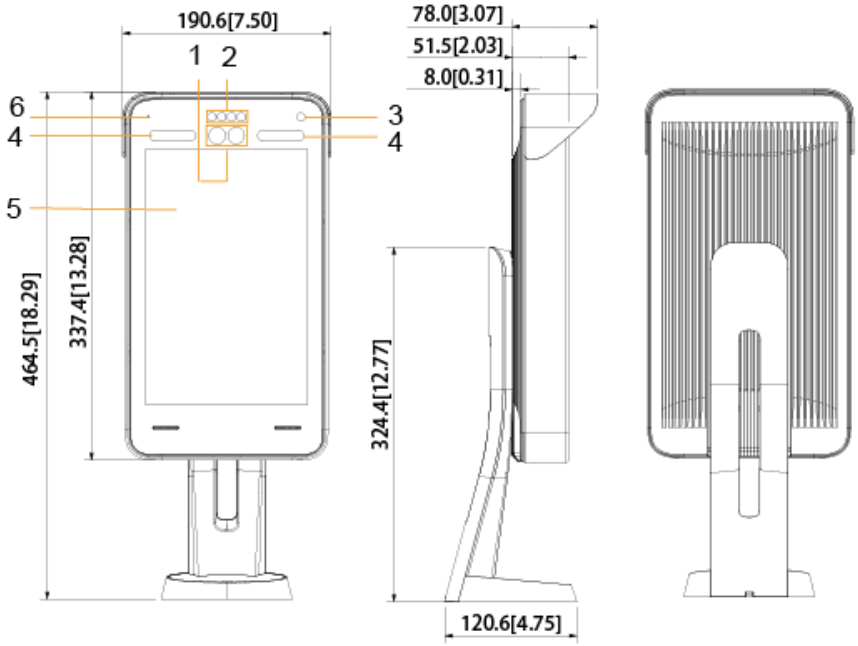


Table 1-3 Component description

No.	Name
1	Dual camera
2	IR light
3	Phototransistor
4	White fill light
5	Display
6	MIC

2 Installation

2.1 Installation Notes

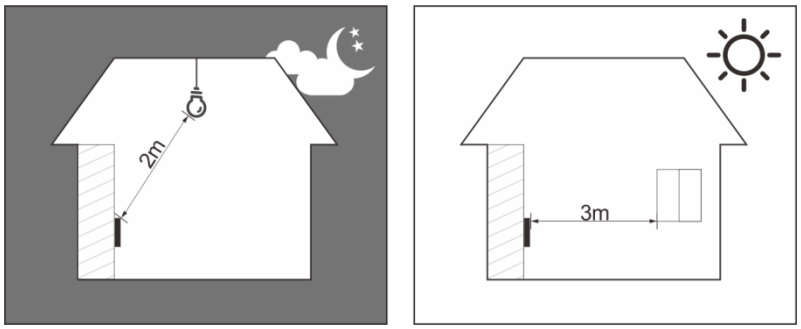
- If there is light source 0.5 meters away from the device, the minimum illumination should be no less than 100Lux.
- It is recommended that the device is installed indoors, at least 3 meters away from windows and doors and 2 meters away from lights.
- Avoid back light and direct sunlight.

Ambient Illumination Requirement

Figure 2-1 Ambient illumination requirement

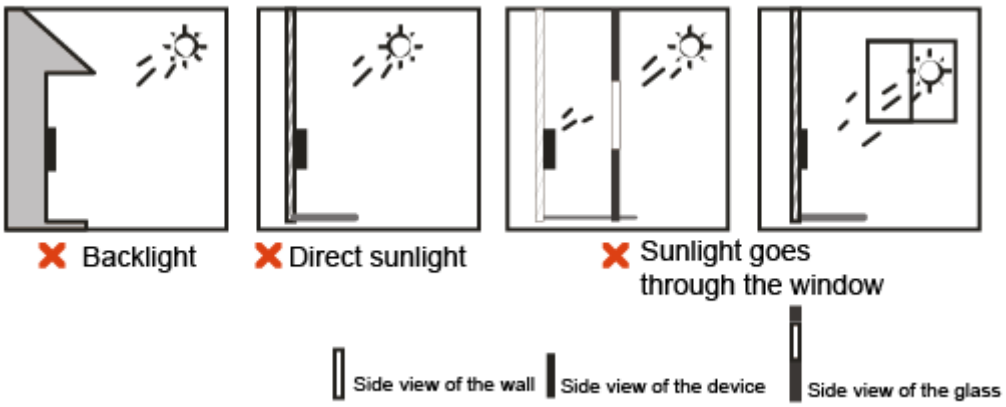
Places Recommended

Figure 2-2 Places recommended



Places Not Recommended

Figure 2-3 Places not recommended



2.2 Installation Drawings

7-Inch Terminal

Figure 2-4 Installation drawings of model A (mm[inch])

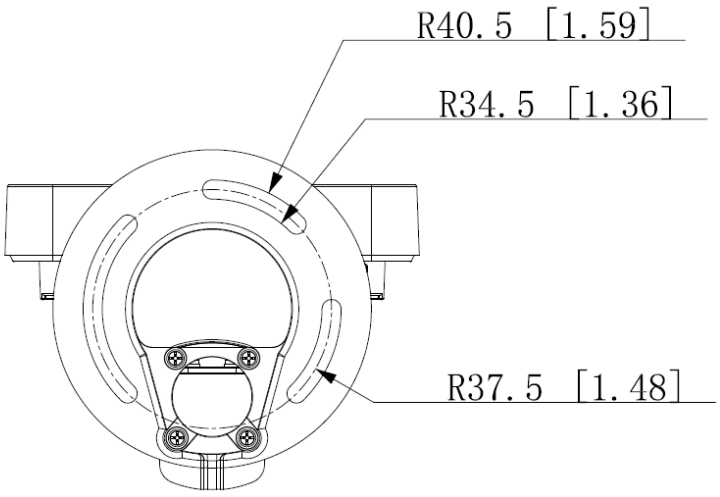
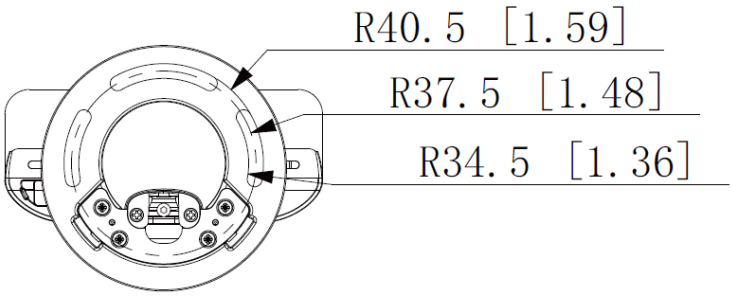
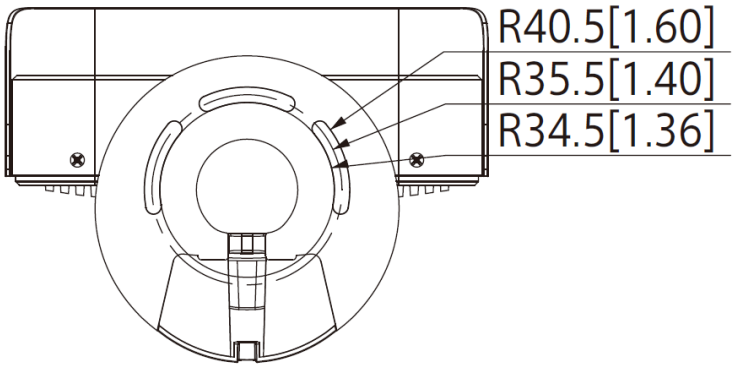


Figure 2-5 Installation drawings of model B (mm[inch])



10-Inch Terminal

Figure 2-6 Installation drawings (mm[inch])



2.3 Cable Connections

- Check if the access control security module is enabled in **Function > Security Module**. If the security module is enabled, you need to purchase access control security module separately. The security module needs separate power supply to provide power.
- Once the security module is enabled, the exit button, turnstile control, and firefighting linkage will be invalid.

Cable connections are the same for all terminals. The 7-inch terminal will be taken as an example.

Figure 2-7 Cable connection

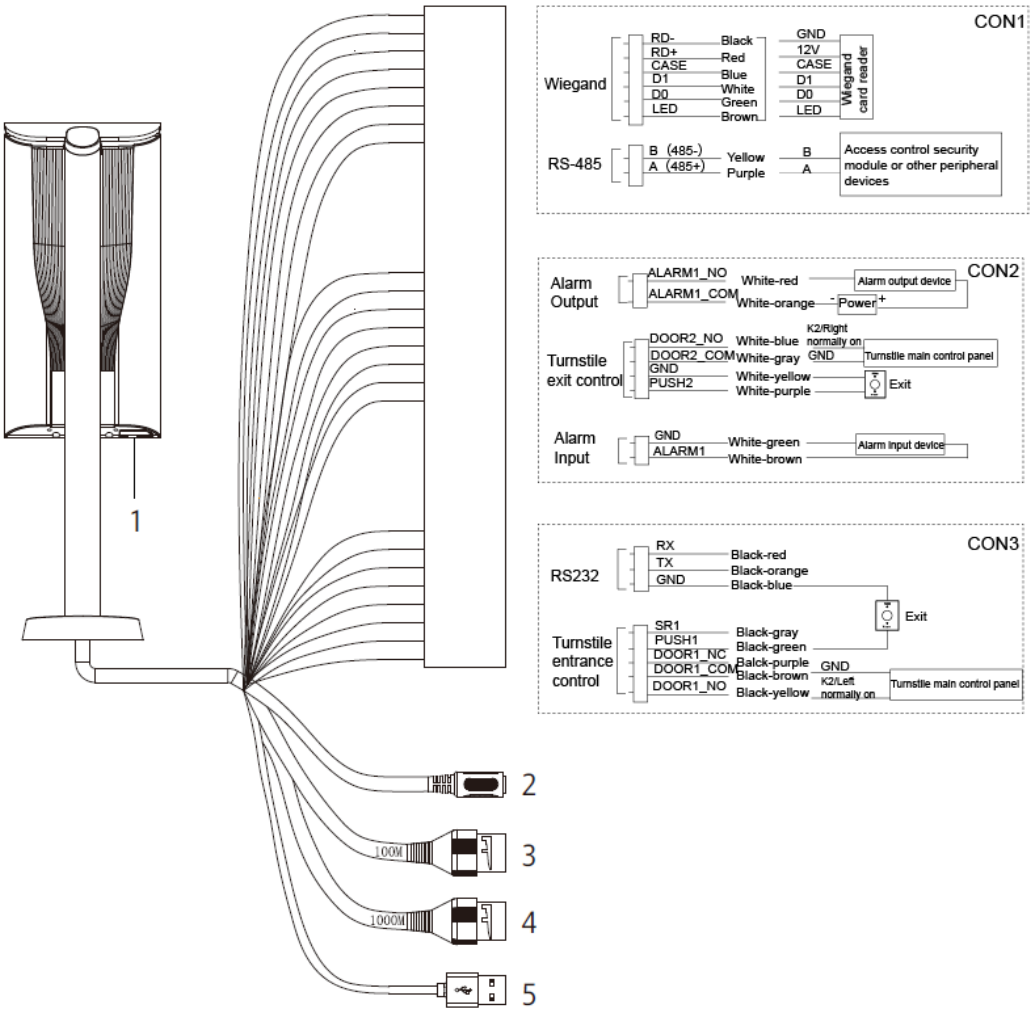


Table 2-1 Component description

No.	Name
1	USB port
2	Power port
3	Ethernet port
4	Ethernet port (only supported by 7-inch model B access controllers
5	USB port

2.4 Installation

Figure 2-8 Installation of the 7-inch model A terminal

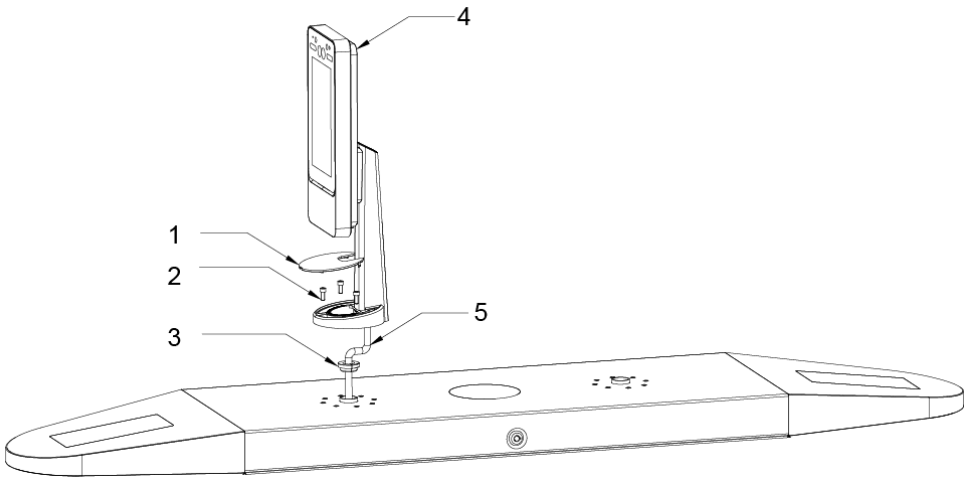


Figure 2-9 Applying silicon sealant to the 7-inch model B terminal

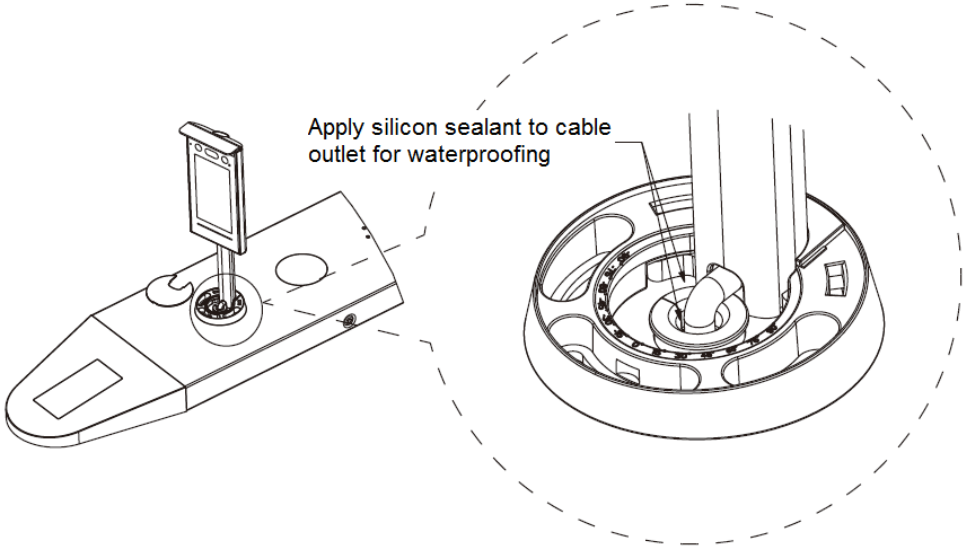


Figure 2-10 Installation of 10-inch terminals

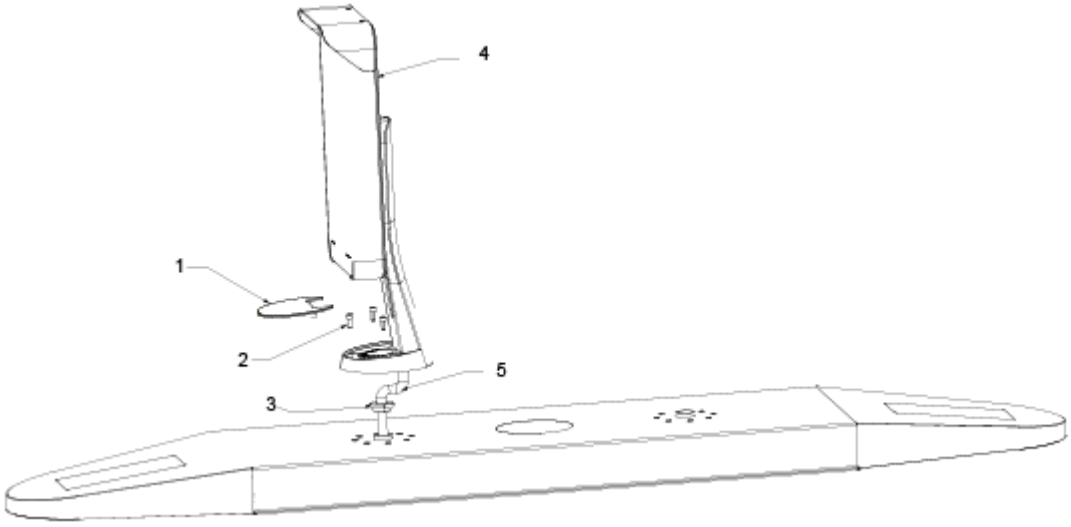


Figure 2-11 Applying silicon sealant to the 10-inch terminal

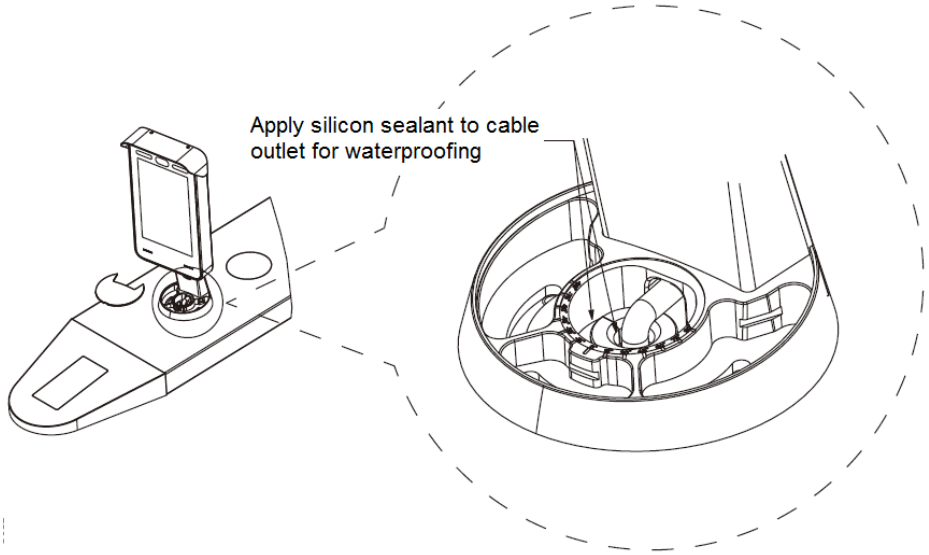


Table 2-2 Component description

No.	Name
1	Ornamental cover
2	M5 screw
3	Waterproof silica gel plug
4	Terminal
5	Cable

Installation Procedure

Step 1 Thread cable through the turnstile.

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

Step 3 Fix the terminal onto the turnstile with M5 screw.
Connect cables for terminal. See "2.3 Cable Connections."

Step 4 Apply sealant to gaps between the waterproof silica gel plug and turnstile. See Figure 2-9.

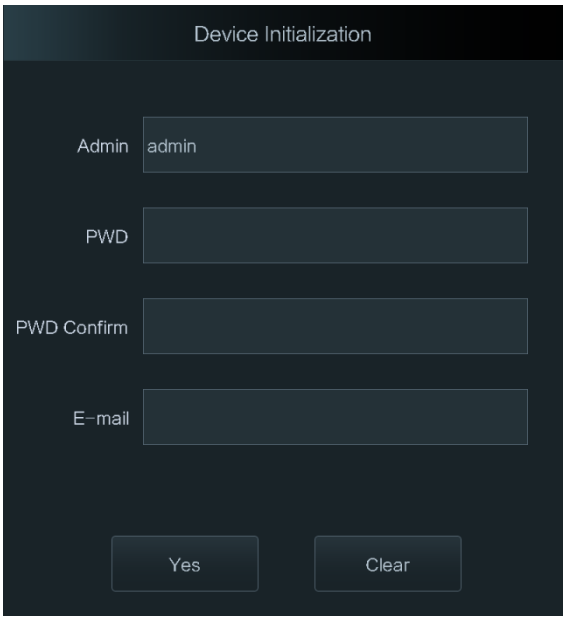
Step 5 Install the ornamental cover on the base of the terminal.
The installation is competed.

3 System Operation

3.1 Initialization

Administrator password and an email should be set the first time the terminal is turned on; otherwise the terminal cannot be used. See Figure 3-1.

Figure 3-1 Initialization



- The administrator password can be reset through the email address you entered if the administrator forgets the administrator password.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
- For terminal without touch screen, initialization can be completed through the web. See the user manual for details.

3.2 Adding New Users

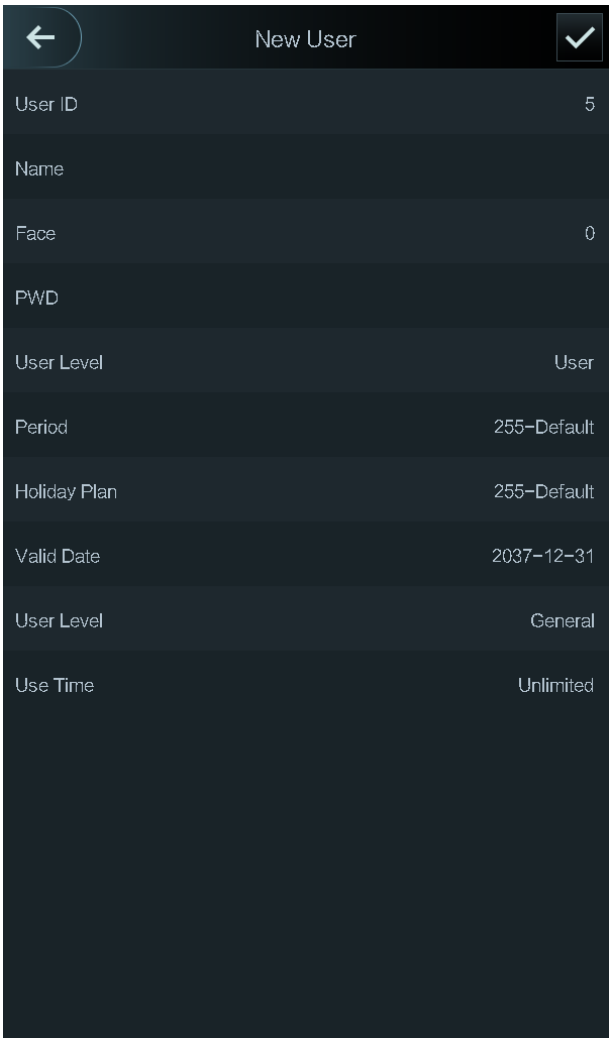
You can add new users by entering their user IDs, names, importing face images, passwords, selecting their user levels, and more.

Step 1 Select **User > New User**.

The **New User** interface is displayed. See Figure 3-2.

The following figure is for reference only and the actual interface shall prevail.

Figure 3-2 New user



Step 2 Configure parameters on the interface. See Table 3-1.

Table 3-1 New user parameter description

Parameter	Description
User ID	You can enter user IDs. The IDs consist of 32 characters (including numbers and letters), and each ID is unique.
Name	You can enter names with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the picture capturing frame, and then a picture of your face will be automatically captured. For details about face image recording, see "Appendix 1 Notes of Face Recording/Comparison."
Password	The door unlocking password. The maximum length of the password is 8 characters. If the terminal is without touch screen, you need to connect the terminal to a peripheral card reader. There are buttons on the card reader.

Parameter	Description
Level	You can select a user level for new users. There are two options. ● User: Users only have door unlock authority. ● Admin: Administrators can not only unlock the door but also have parameter configuration authority. In case that you forget the administrator password, you had better create more than one administrator.
Period	You can set a period in which the user can unlock the door. For detailed period settings, see the configuration manual.
Holiday Plan	You can set a holiday plan in which the user can unlock the door. For detailed holiday plan settings, see the user manual.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	There are six levels: ● General: General users can unlock the door normally. ● Blacklist: When users in the blacklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times in certain periods. Once they exceed the maximum times and periods, they cannot unlock the door again. ● Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Special: When special people unlock the door, there will be a delay of 5 seconds before the door is closed.
Use Time	When the user level is Guest, you can set the maximum number of times that the guest can unlock the door.

Step 3 After you have configured all the parameters, tap to save the configuration.

For terminals without touch screen, adding new users can be completed through the web. See the user manual for details.

4 Web Operation

The terminal can be configured and operated on the web. Through the web you can set parameters including network parameters, video parameters, and terminal parameters; and you can also maintain and update the system.

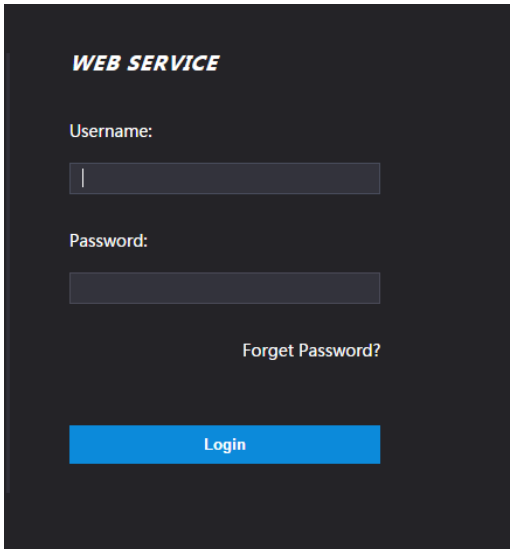
Login

You need to set a password and an email address before logging in to the web for the first time. Password you set is used to log in to the web, and the email is used to retrieve passwords.

Step 1 Open IE web browser, enter the IP address (192.168.1.108 by default) of the terminal in the address bar, and then press Enter.

- Make sure that the IP address of computer used to log in to the web is in the same LAN with the terminal.
- 7-inch model B access controllers have dual NICs. The default management address for 1000M Ethernet port is 192.168.1.108, and for 100M Ethernet port is 192.168.2.108.

Figure 4-1 Login



Step 2 Enter the user name and password.

- The default username of administrator is admin, and the password is the login password after initializing the terminal. Modify the administrator password regularly and keep it properly for security.
- If you forget the administrator login password, you can click **Forget Password?** to reset it. See the user manual.

Step 3 Click **Login**.

The homepage of the web is displayed.

Appendix 1 Notes of Face Recording/Comparison

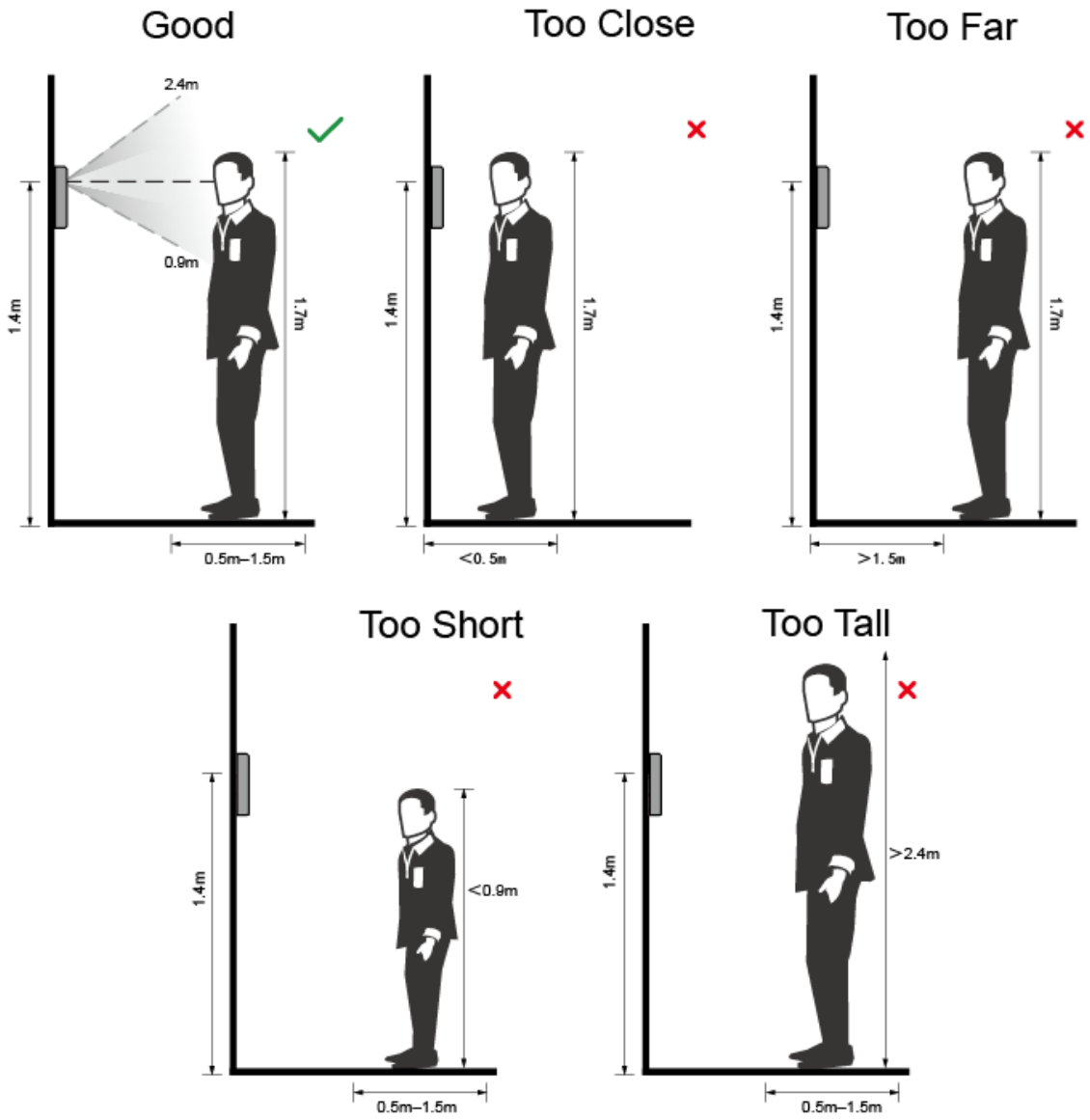
Before Registration

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

Face Position

If your face is not at the appropriate position, face recognition effect might be influenced.

Appendix figure 1-1 Appropriate face position

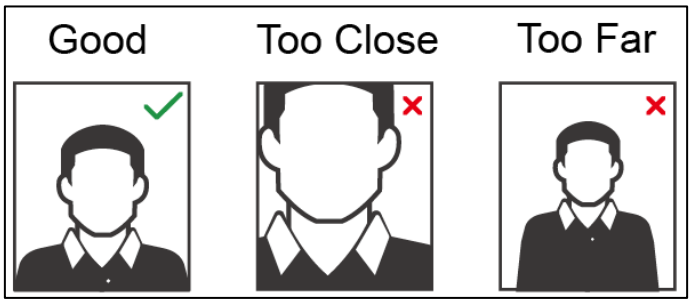


Requirements of Faces

- 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 is 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



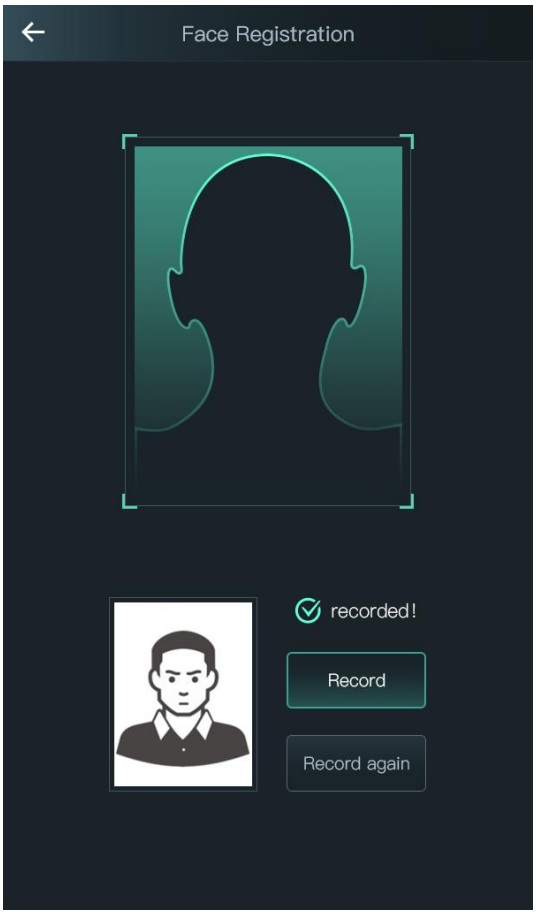
- When importing face images through the management platform, make sure that image resolution is within the range 150 × 300–600 × 1200; image pixels are more than 500 × 500; image size is less than 75 KB, and image name and person ID are the same.
- Make sure that face does not take 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

During Registration

You can register faces through the terminal or through the platform. For registration through the platform, see the platform user manual.

Make your head center on the photo capture frame. A picture of your face will be captured automatically.

Appendix figure 1-4 Registration



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

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **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.

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **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.

13. **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.

14. **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.