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
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
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 2020

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.
- For the terminal with a temperature monitoring unit:
  - ◇ Install the temperature monitoring unit in a windless indoor environment, and maintain the indoor ambient temperature at 15°C to 32°C.
  - ◇ Warm up the temperature monitoring unit for more than 20 minutes after power-on to enable the temperature monitoring unit to reach thermal equilibrium.

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

1 Overview

1.1 Introduction

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

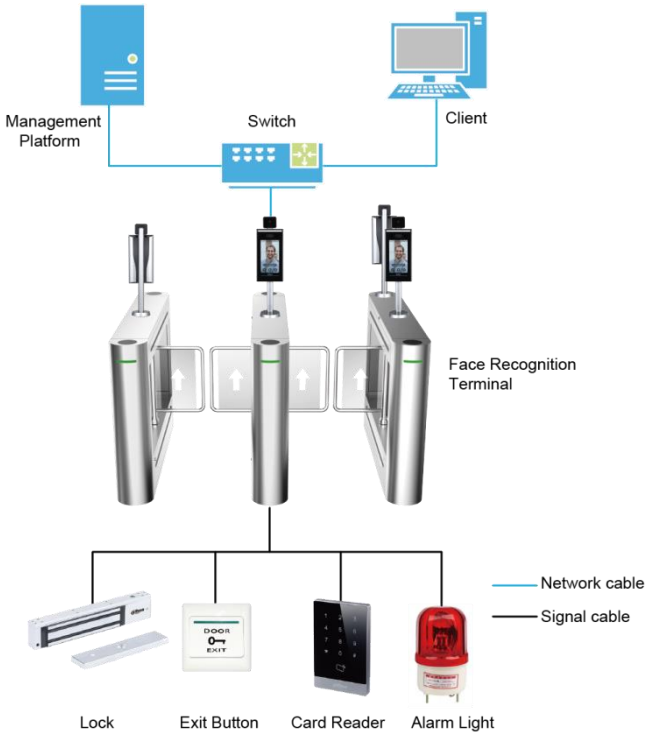
1.2 Features

- LCD display, the resolution of 7-inch terminal is 1024 × 600
- 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 illuminator
- 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
- Support body temperature monitoring through peripheral temperature monitoring unit

1.3 Application

The terminal is applicable for parks, office buildings, schools, factories, residential areas and other places. The identity is verified through face recognition to achieve passage without perception.

Figure 1-1 Networking



1.4 Dimension and Component

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

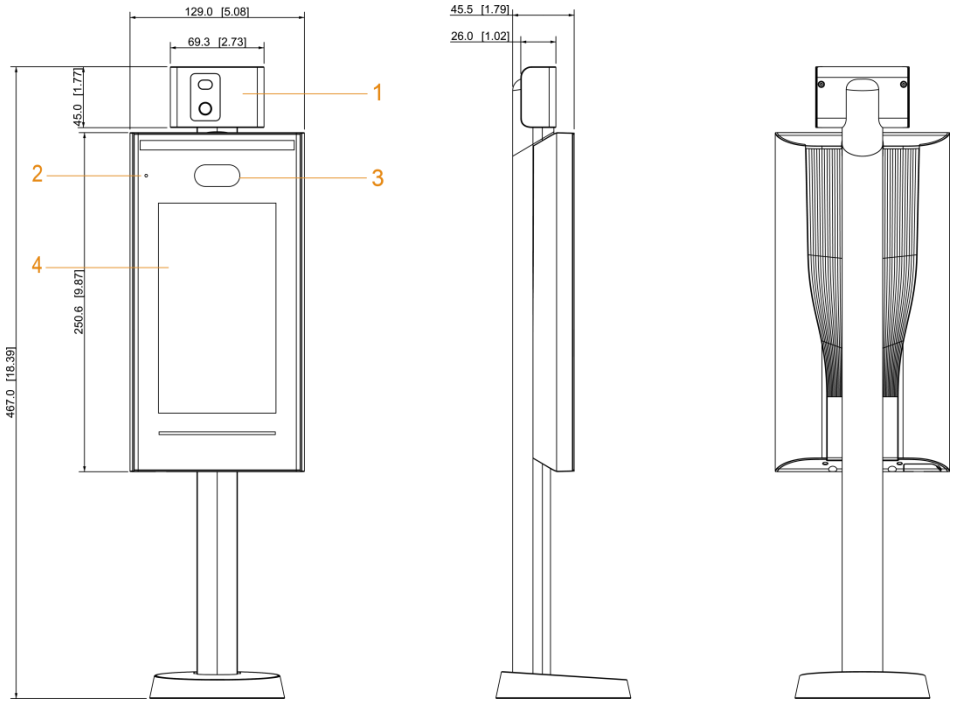


Table 1-1 Component description (1)

No.	Name	No.	Name
1	Temperature monitoring unit	3	Dual cameras
2	MIC	4	Display

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

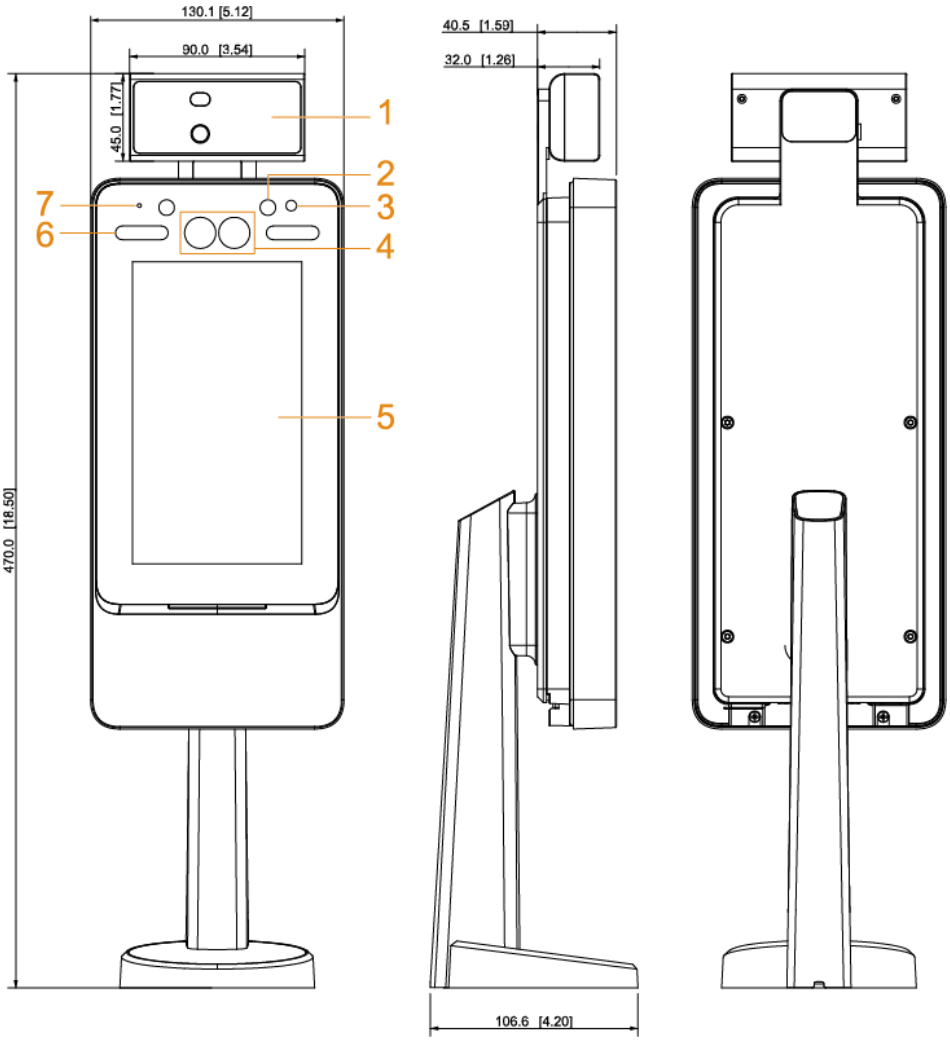


Table 1-2 Component description (2)

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

2 Connection and Installation

2.1 Cable Connections

The cable connection of model X and model Y is the same. This section takes the model X as an example.

⚠

- Check whether 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.

Figure 2-1 Cable connections

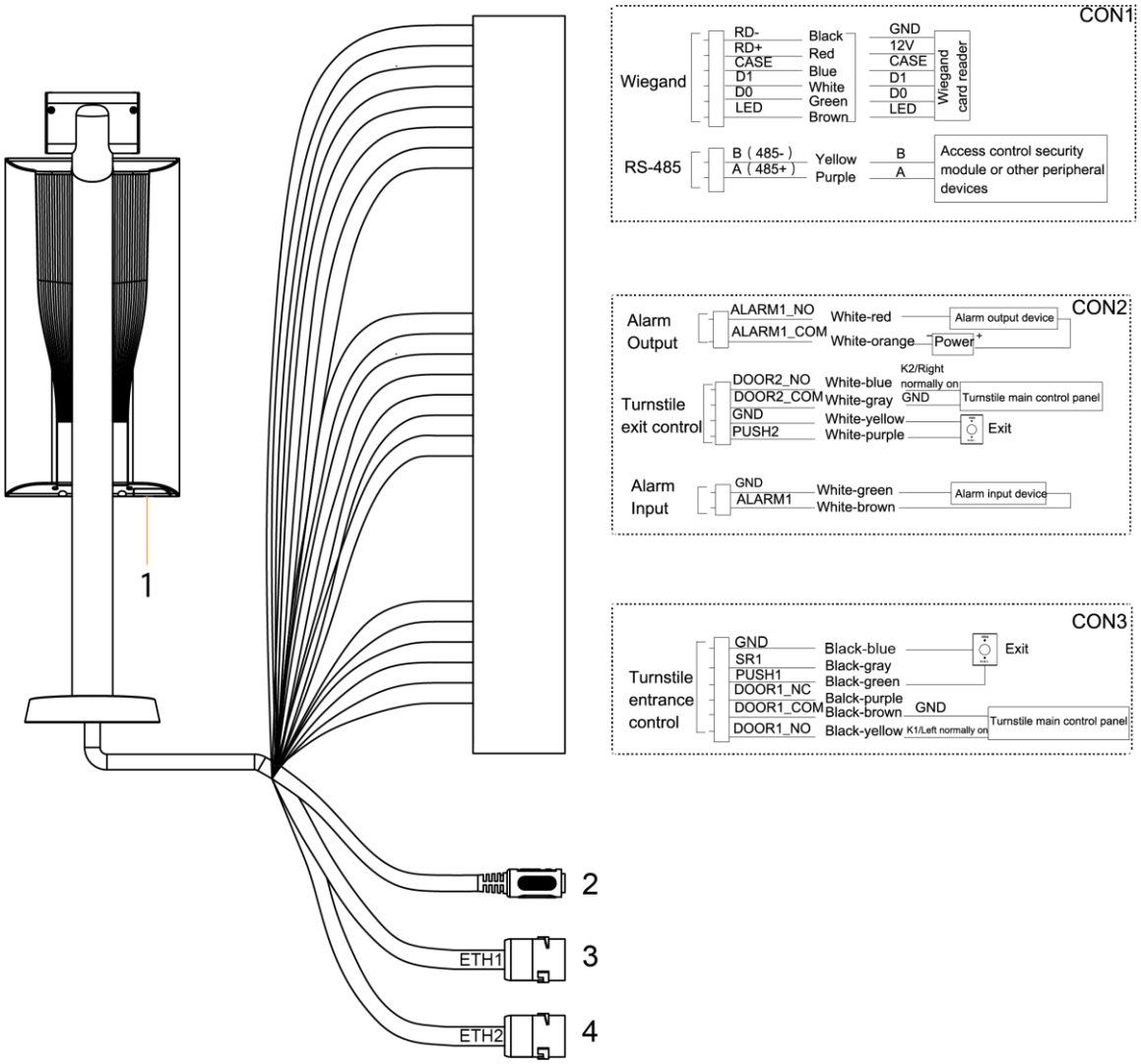


Table 2-1 Component description

No.	Name
1	USB port
2	Power port

No.	Name
3	Ethernet port
4	Ethernet port (only supported by 7-inch model B access controllers)

Table 2-2 Port description

Port	Cable color	Cable name	Description
CON1	Black	RD–	Negative electrode of external card reader.
	Red	RD+	Positive electrode of external card reader.
	Blue	CASE	Tamper alarm input of the external card reader.
	White	D1	Wiegand D1 input (connected to external card reader)/output (connected to controller).
	Green	D0	Wiegand D0 input (connected to external card reader)/output (connected to controller).
	Brown	LED	Connected to external reader indicator in
	Yellow	B	RS-485 negative electrode input (connected to external card reader)/output (connected to controller, or connected to door control 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.
	Purple	A	RS-485 positive electrode input (connected to external card reader)/output (connected to controller, or connected to door control 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.
CON2	White and red	ALARM1_NO	Alarm 1 normally open output port.
	White and orange	ALARM1_COM	Alarm 1 common output port.
	White and blue	DOOR2_NO	Lock control normally open port.
	White and gray	DOOR2_COM	Lock control common port.
	White and yellow	GND	Connected to the common GND port.

Port	Cable color	Cable name	Description
	White and purple	PUSH2	Door open button of door No.2
	White and green	GND	Connected to the common GND port.
	White and brown	ALARM1	Alarm 1 input port.
CON3	Black and blue	GND	Connected to the common GND port.
	Black and gray	SR1	Used for door contact detection.
	Black and green	PUSH1	Door open button of door No.1
	Black and purple	DOOR1_NC	Lock control normally closed port.
	Black and brown	DOOR1_COM	Lock control common port.
	Black and yellow	DOOR1_NO	Lock control normally open port.

2.2 Installation Notes

- If there is light source 0.5 meters away from the device, the minimum illumination should be no less than 100 Lux.
- 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 backlight and direct sunlight.

Ambient Illumination Requirement

Figure 2-2 Ambient illumination requirement

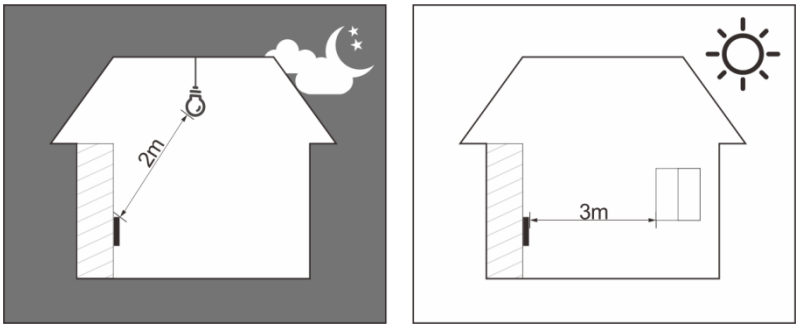
Temperature Monitoring Requirement

- It is recommended to install the temperature monitoring unit in an indoor windless environment (a relatively isolated area from the outdoor), and maintain the ambient temperature at 15°C to 32°C.

- Warm up the temperature monitoring unit for more than 20 minutes after power-on to enable the temperature monitoring unit to reach thermal equilibrium.
- If there is no suitable indoor environment (including areas directly facing indoor and outdoor areas, and outdoor doorways), set up a temporary passage with stable ambient temperature for temperature monitoring.
- The factors such as sunlight, wind, cold air, and air conditioning cold and warm air can easily affect the surface temperature of human body and the working status of the terminal, which will cause the temperature deviation between the monitored temperature and the actual temperature.
- Influencing factors of temperature monitoring
  - ◇ Wind: Wind will take away the heat from the forehead, which will affect the accuracy of temperature monitoring.
  - ◇ Sweating: Sweating is a way for the body to automatically cool down and dissipate heat. When the body sweats, the temperature will also decrease.
  - ◇ Room temperature: If the room temperature is low, the surface temperature of human body will decrease. If the room temperature is too high, the human body will start to sweat, which will affect the accuracy of temperature monitoring.
  - ◇ The temperature monitoring unit is sensitive to light waves with a wavelength of 10um to 15um. Avoid using it in the sun, fluorescent light sources, air conditioning outlets, heating, cold air outlets, and glass surfaces.

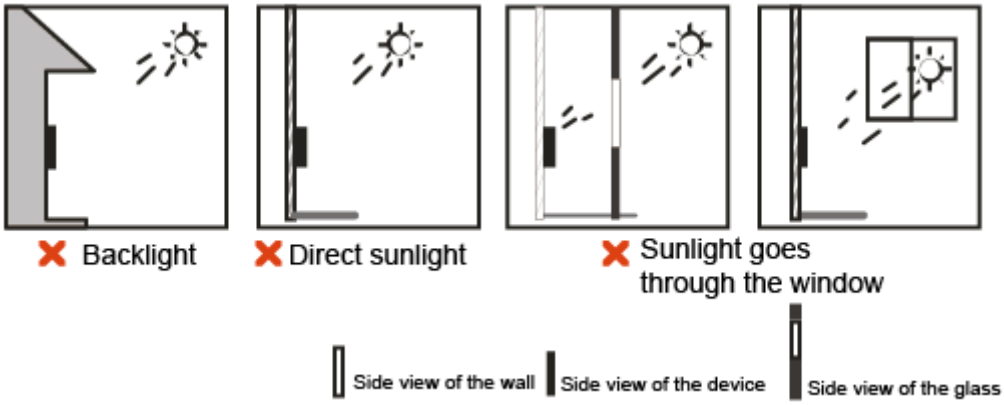
Places Recommended

Figure 2-3 Places recommended



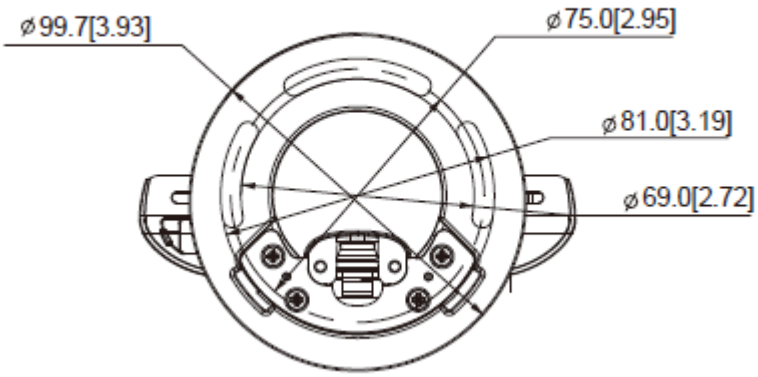
Places Not Recommended

Figure 2-4 Places not recommended



2.3 Installation Drawings

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



2.4 Installation

The installation of model X and model Y is the same. This section takes model X as an example.

Figure 2-6 Installation of the terminal

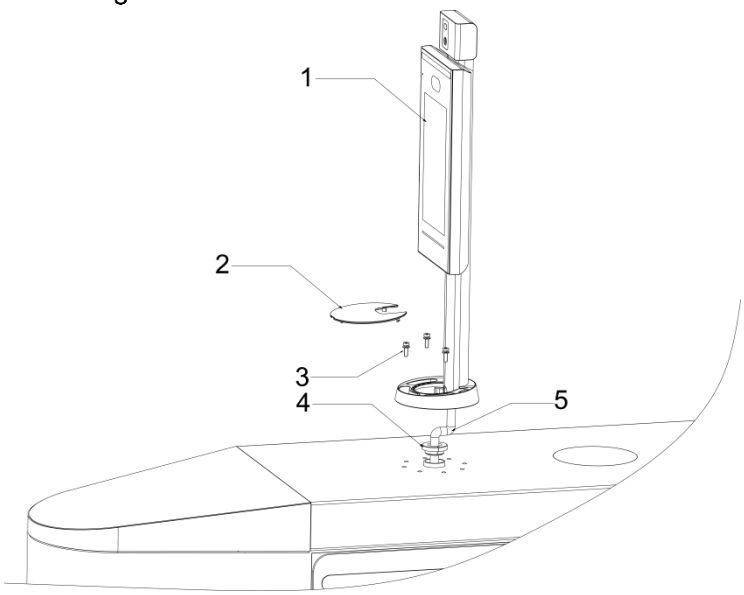


Figure 2-7 Applying silicon sealant to the terminal

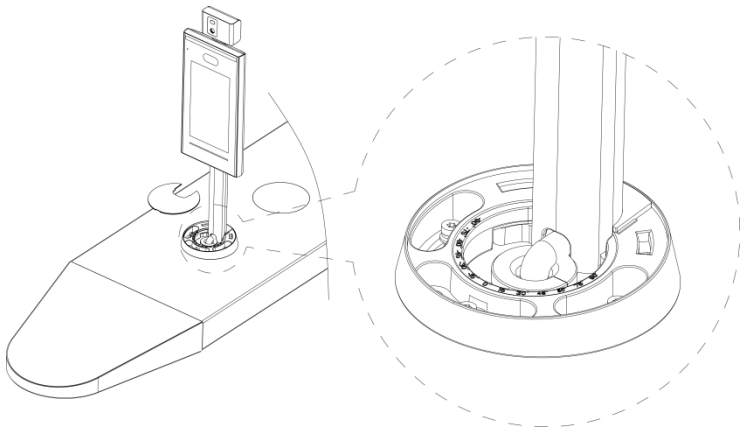


Table 2-3 Component description

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

Step 4 Connect cables for terminal. See "2.1 Cable Connections."

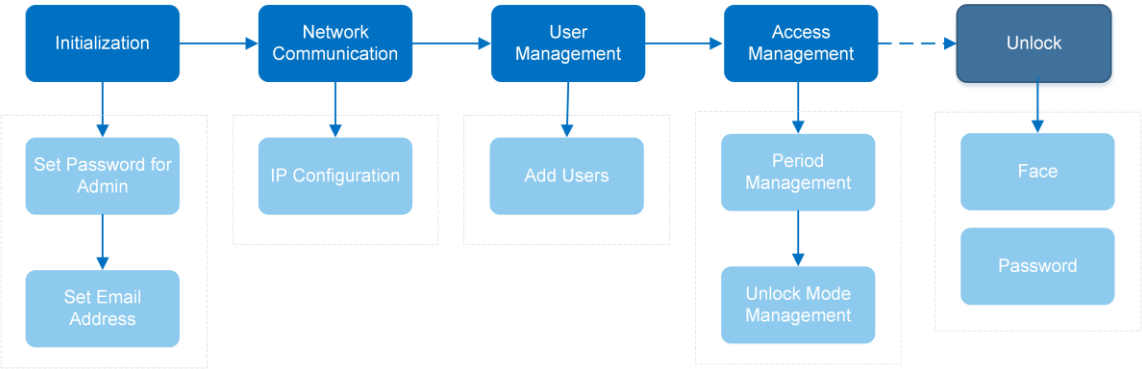
Step 5 Apply sealant to gaps between the waterproof silica gel plug and turnstile. See Figure 2-7.

Step 6 Install the ornamental cover on the base of the terminal.

3 System Operations

3.1 Basic Configuration Procedure

Figure 3-1 Basic configuration procedure



3.2 Common Icons

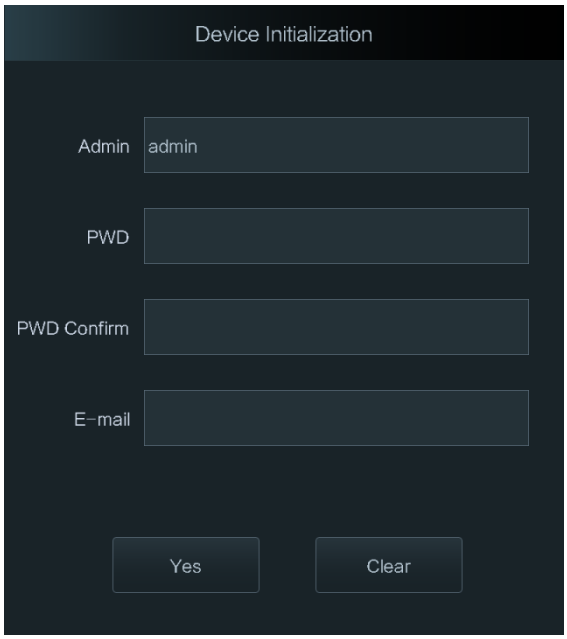
Table 3-1 Icon description

Icon	Description
	Main menu icon.
	Confirm icon.
	Turn to the first page of the list.
	Turn to the last page of the list.
	Turn to the previous page of the list.
	Turn to the next page of the list.
	Return to the previous menu.
ON	Enable.
OFF	Disable.

3.3 Initialization

Administrator password and an email should be set the first time the terminal is turned on or after reset; otherwise the terminal cannot be used.

Figure 3-2 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 must 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 ' " ; : &).

3.4 Standby Interface

You can unlock the door through faces and passwords.

- If there are no operations in 32 seconds, the terminal will go to the standby mode.
- The following figures are for reference only, and the actual interface shall prevail.

Figure 3-3 Homepage

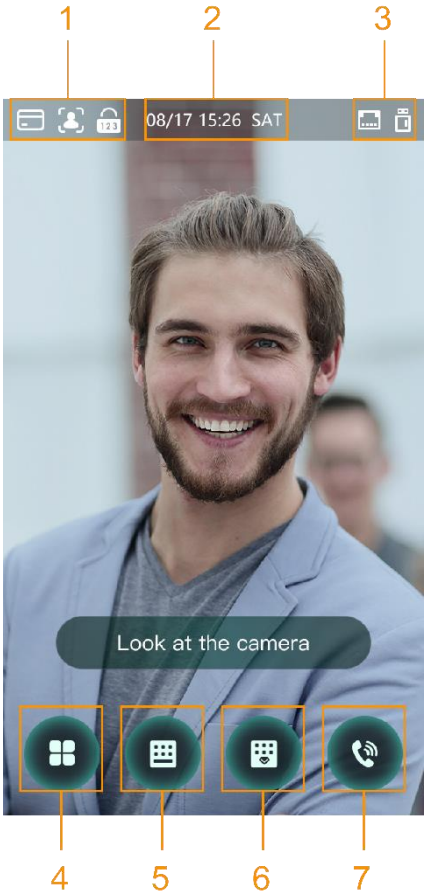


Table 3-2 Homepage description

No.	Description
1	Unlock methods: Card, face, fingerprint, and password. When card, face, fingerprint, and password are all set as unlock mode, the password icon will not be displayed at the upper-left corner of the access controller.
2	Date & Time: Current date and time.
3	Network status and USB status.
4	Main menu. Only administrators can enter the main menu.
5	Password unlock.
6	Administrator password unlock.
7	Tap to call other devices.

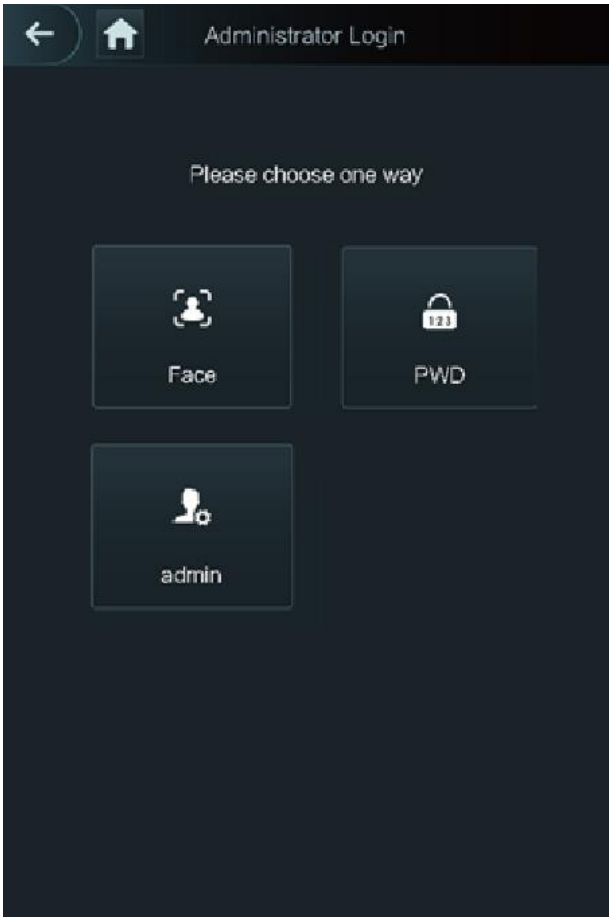
3.5 Main Menu

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.

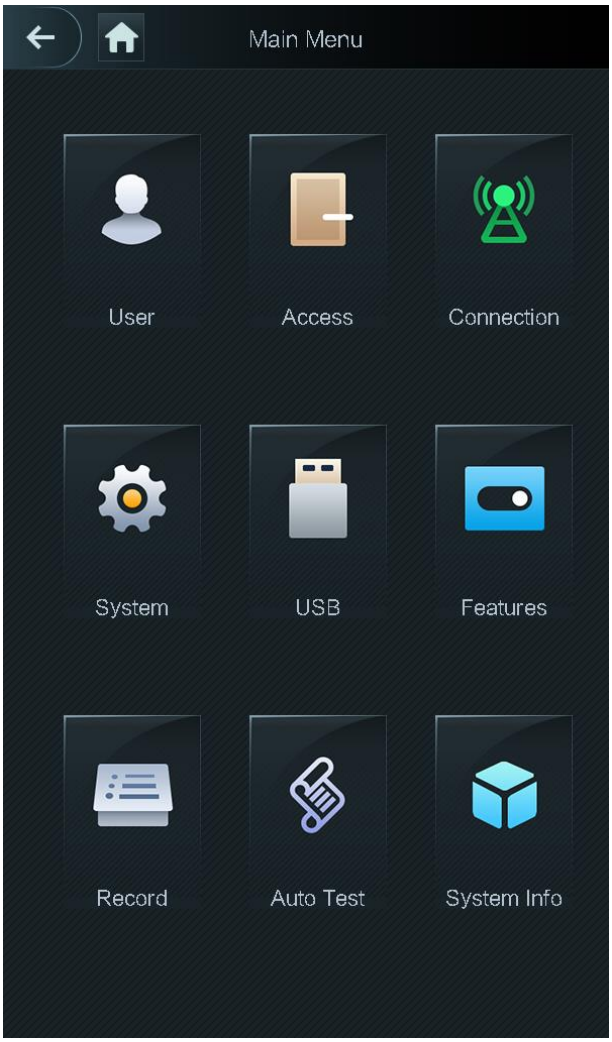
Different modes support different unlock methods, and the actual interface shall prevail.

Figure 3-4 Administrator login



Step 2 Select a main menu entering method.

Figure 3-5 Main menu



3.6 Unlocking Methods

You can unlock the door through faces and passwords.

3.6.1 Face

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

3.6.2 User Password

Enter the user password, 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 .

3.6.3 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 ☑.

3.7 User Management

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

3.7.1 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 1 Select **User > New User**.

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

Figure 3-6 New user

Step 2 Configure parameters on the interface.

Table 3-3 New user parameter description

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter 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.
PWD	The door unlocking password. The maximum length of the password is 8 characters.
Level	You can select a user level for new users. There are two options. ● User: Users only have door unlock permission. ● Admin: Administrators can not only unlock the door but also have parameter configuration permission. 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 permission. ● 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 Tap ☑ to save the configuration.

3.7.2 Viewing User Information

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

3.8 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.

3.8.1 Period Management

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

3.8.1.1 Period Configuration

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.

3.8.1.2 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.

3.8.1.3 Holiday Plan

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

3.8.1.4 NO Period

If a period is added to the **NO** period, then the door stays open during that period.

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

3.8.1.5 NC Period

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

3.8.1.6 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**.

- means enabled.
- means not enabled.

3.8.2 Unlock

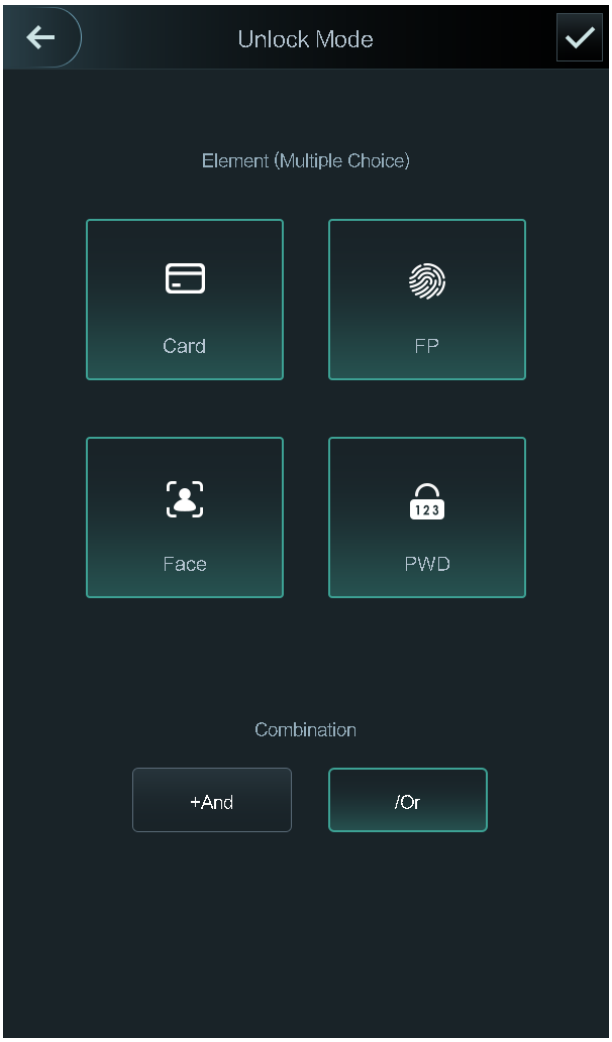
There are three unlock modes: unlock mode, unlock by period, and group combination. Unlock modes vary with terminal models, and the actual terminal shall prevail.

3.8.2.1 Unlock Mode

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

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

Figure 3-7 Element (multiple choice)



Step 2 Select one or more unlock modes.

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 select card + PWD, it means, to unlock the door, you need to swipe your card first, and then get the password.
- **/ Or** means "or". For example, if you select card/PWD, it means, to unlock the door, you can either swipe your card or enter the password.

Step 4 Tap to save the settings.

Step 5 Enable the **Unlock Mode**.

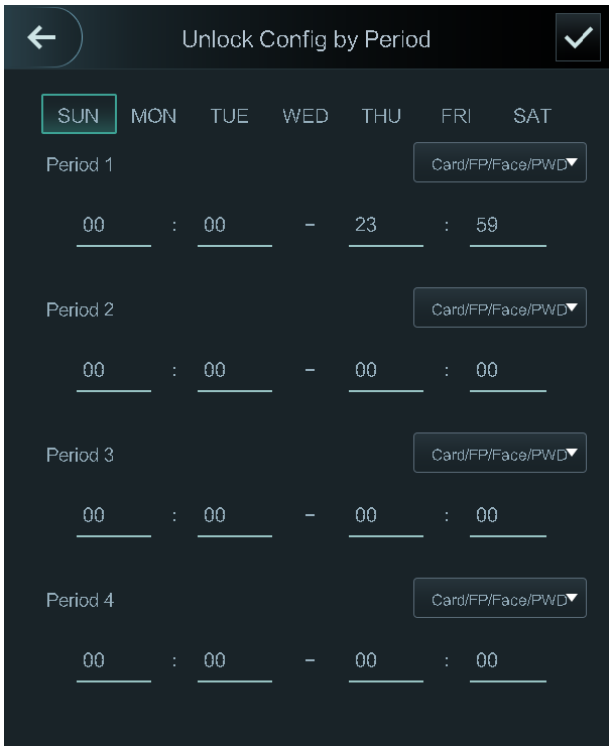
- means enabled.
- means not enabled.

3.8.2.2 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 password.

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

Figure 3-8 Unlock by period



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

Step 3 Tap ☑ to save the settings.

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

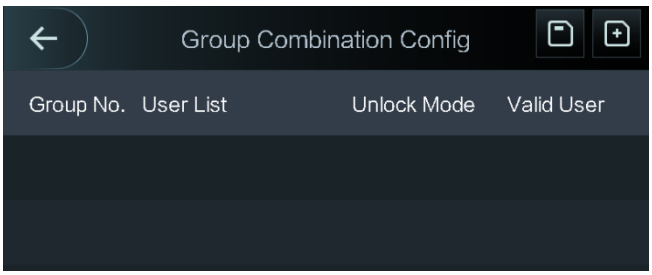
- ON means enabled.
- OFF means not enabled.

3.8.2.3 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**.

Figure 3-9 Group combination



Step 2 Tap ⊞ to create a group.

Figure 3-10 Add a group

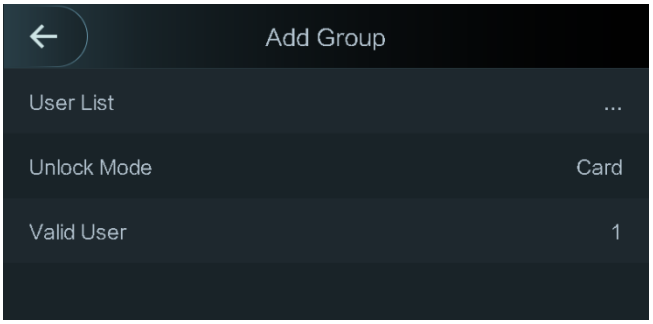


Table 3-4 Group parameter

Parameter	Description
User List	Add users to the newly created group. 1. Tap **User List**. 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 permission. 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.

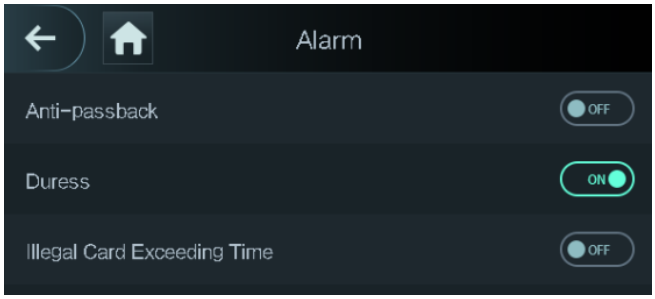
- ON means enabled.
- OFF means not enabled.

3.8.3 Alarm Configuration

Administrators can manage visitor unlock permission through alarm configuration.

Select **Access > Alarm**.

Figure 3-11 Alarm



- ON means enabled.

- means not enabled.

Table 3-5 Parameters on the alarm interface

Parameter	Description
Anti-passback	After the anti-passback is enabled, users need to verify identities both for entry and exit; otherwise an alarm will be triggered. ● If a person enters with the identity checked and exits without the identity checked, an alarm will be triggered when the person tries to enter again and the person will have no permission to unlock the door any more. If a person enters without the identity checked, an alarm will be triggered when the person tries to exit with the identity checked, and the person will have no permission to unlock the door any more.
Duress	After enabling the duress function, an alarm will be triggered when a duress card or duress password 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.

3.8.4 Door Status

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

- NO: If **NO** is selected, the door stays open, which means the door will never be closed.
- NC: If **NC** is selected, the door stays 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.

3.8.5 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.

3.9 Network Communication

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

3.9.1 IP Address

3.9.1.1 IP Configuration

Configure an IP address for the terminal to make it be connected to the network.

Figure 3-12 IP address configuration

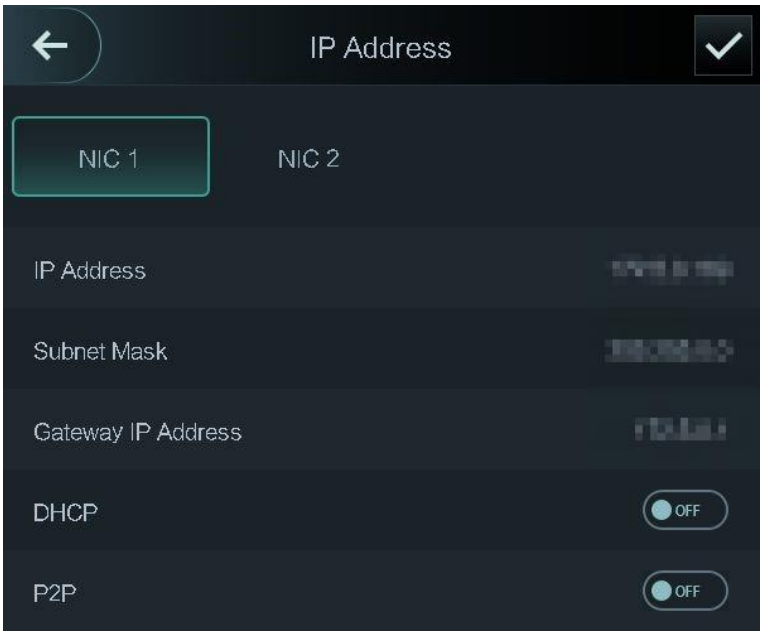


Table 3-6 IP configuration parameters

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 X terminals of have dual NICs. The default management address for ETH1 is 192.168.1.108, and for ETH2 is 192.168.2.108.

3.9.1.2 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 permission in case of data loss caused by improper operation.

Table 3-7 Active register parameter

Parameter	Description
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.

3.9.1.3 Wi-Fi

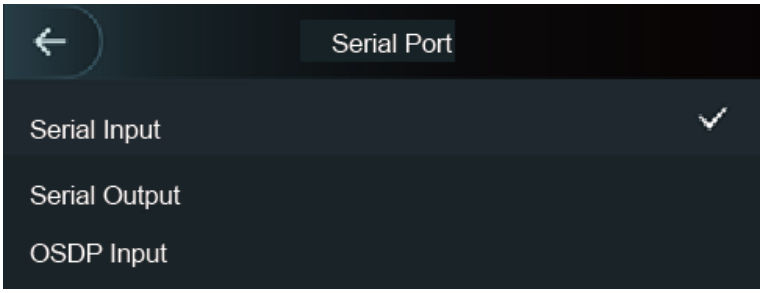
You can connect the terminal to the network through Wi-Fi if the terminal has Wi-Fi function.

3.9.2 Serial Port Settings

Select serial input or serial output according to the use of the external devices.

Select **Connection > Serial Port**.

Figure 3-13 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, 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.

3.9.3 Wiegand Configuration

Select **Wiegand Input** or **Wiegand Output** accordingly.

Select **Connection > Wiegand**.

Figure 3-14 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.

Table 3-8 Wiegand output

Parameter	Description
Wiegand Output Type	The Wiegand Output Type determines the card number or the digit of the number that 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.

3.10 System

3.10.1 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.

3.10.2 Face Parameter

Figure 3-15 Face parameter

Tap a parameter and do configuration, and then tap .

Table 3-9 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	Set the control panel shooting angle of profiles. The larger the value

Name	Description
Recognition	is, the wider range of the profiles will be recognized.
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 access controller 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 Timeout (S)	When a person who does not have the access permission stands in front of the access controller and gets the face recognized, the controller will prompt that face recognition failed. The prompt interval is called recognition timeout.
Invalid Face Prompt Interval (S)	When a face has no access permission stands in front of the access controller, the controller will prompt that the face is invalid. The prompt interval is invalid face prompt interval.
Anti-fake Threshold	This function prevents people from unlocking by human face images or face models.
Temp Parameters	Set whether to enable the body temperature monitoring. ● Temp Unit: Select a temperature unit. ● Temp Rect: Set whether to display the temperature monitoring box or not. ● Temp Monitoring Distance (cm): The value is 0 by default. Set other values to enable temperature monitoring within a defined distance. 80 cm is recommended. ● Temp Threshold (°C): Set the temperature threshold. The monitored body temperature will be judged as high temperature if it is greater than or equal to the set value. ● Temp Correction Value: This parameter is for testing. The difference of the temperature monitoring environment might cause the temperature deviation between the monitored temperature and the actual temperature. You can select multiple monitored samples for testing, and then correct the temperature deviation by this parameter according to the comparison between the monitored temperature and the actual temperature. For example, if the monitored temperature is 0.5°C lower than the actual temperature, the correction value is set to 0.5°C; if the monitored temperature is 0.5°C higher than the actual temperature, the correction value is set to -0.5°C. Only the access controller with a temperature monitoring unit supports this parameter.
Mask Parameters	● No detect: Mask is not detected during face recognition. ● Mask reminder: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is allowed. ● Mask intercept: Mask is detected during face recognition. If the

Name	Description
	person is detected without wearing a mask, the system will prompt mask reminder and passage is not allowed.

3.10.3 Image Mode

There are three options:

- Indoor: Select **Indoor** when the access controller is installed indoors;
- Outdoor: Select **Outdoor** when the access controller is installed outdoors;
- Other: Select **Other** when the access controller is installed at places with backlights like corridors and hallways.

3.10.4 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 stays off; otherwise, the fill light will be on.
- NO: The fill light stays open.
- NC: The fill light stays closed.

3.10.5 Fill Light Brightness Setting

You can select fill light brightness according to your needs.

3.10.6 Volume Adjustment

You can adjust the beeping and voice volume.

Step 1 Select **System > Volume**.

Step 2 Select **Beep Volume** or **Mic Volume** as needed.

Step 3 Tap  or  to adjust the volume.

3.10.7 IR Light Brightness Adjustment

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

3.10.8 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.

3.10.9 Reboot

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

3.11 USB

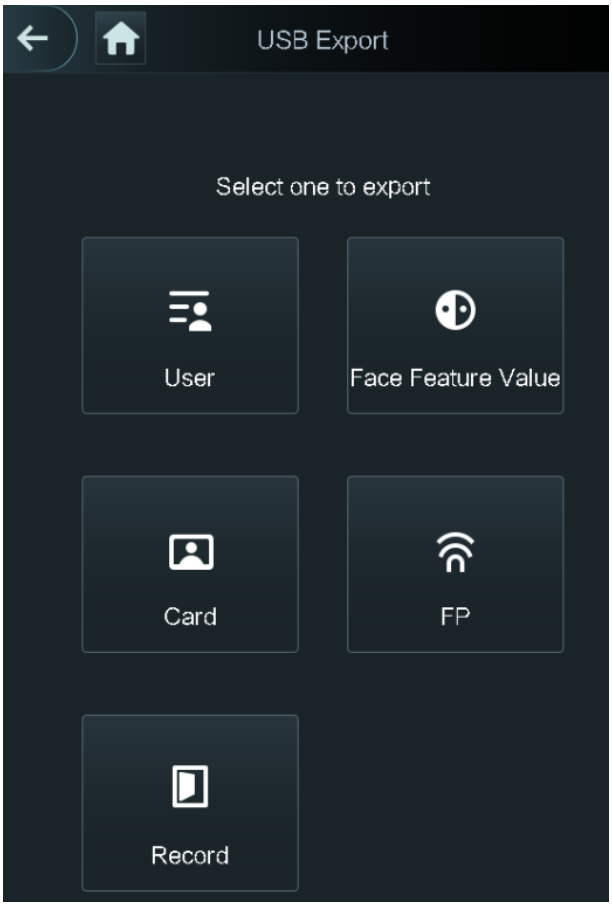
- Make sure that the USB is inserted before exporting user information and updating. During exporting or updating, do not pull out the USB or do other operations; otherwise the exporting or updating will fail.
- You need to import information from one terminal to the USB before using USB to import information to another terminal.
- USB can also be used to update the program.

3.11.1 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**.

Figure 3-16 USB export



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

Step 3 Tap **OK**.

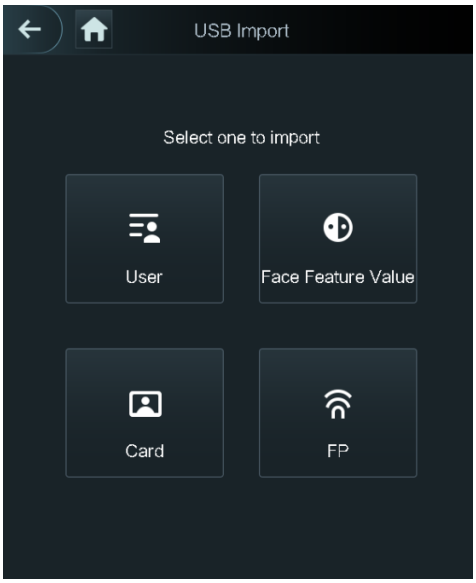
Data exported will be saved in the USB.

3.11.2 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**.

Figure 3-17 USB Import



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

Step 3 Tap **OK**.

Data in the USB flash drive will be imported into the terminal.

3.11.3 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**.

Step 3 Tap **OK**.

The update starts, and the terminal will restart after the update is finished.

3.11.4 Features

You can do settings about privacies, card number reverse, security module, door sensor type, and result feedback. For details of the functions mentioned.

Figure 3-18 Features

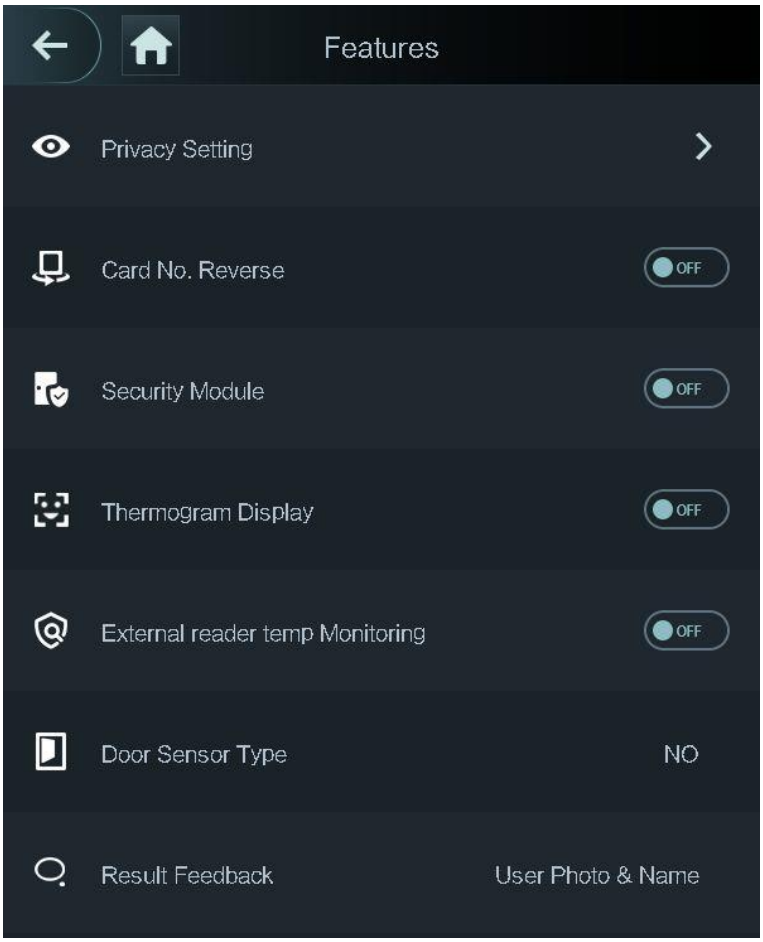


Table 3-10 Feature description

Parameter	Description
Privacy Setting	See Figure 3-19 for details.
Card No. Reverse	If the third-party card reader needs to be connected to the access controller through the wiegand output port, you need to enable the Card No. Reverse function; otherwise the communication between the access controller 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.
Thermogram Display	Display a heat map at the upper-left corner.
External Reader Temp Monitoring	Turn it on and the temperature of the person will be monitored when he/she swipes the card.
Door Sensor Type	There are two options: **NO** and **NC**.
Result Feedback	Displays whether the unlock succeeded or failed.

Privacy Setting

Figure 3-19 Privacy setting

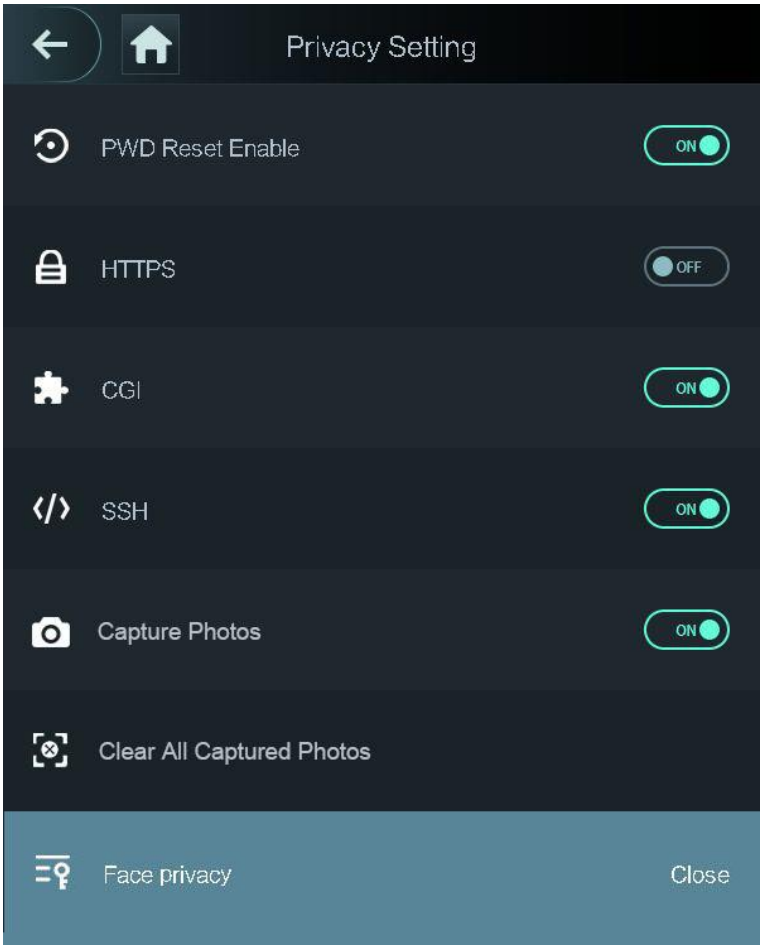


Table 3-11 Features

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. When HTTPS is enabled, the access controller will restart automatically.
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.

Parameter	Description
FP	If you select OFF for Fingerprint (FP), users' fingerprint information will not be displayed when they get fingerprints recorded or when they use fingerprints to unlock the door.
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.
Face Privacy	Set different levels to blur the standby interface.

When HTTPS is enabled, the terminal will restart automatically.

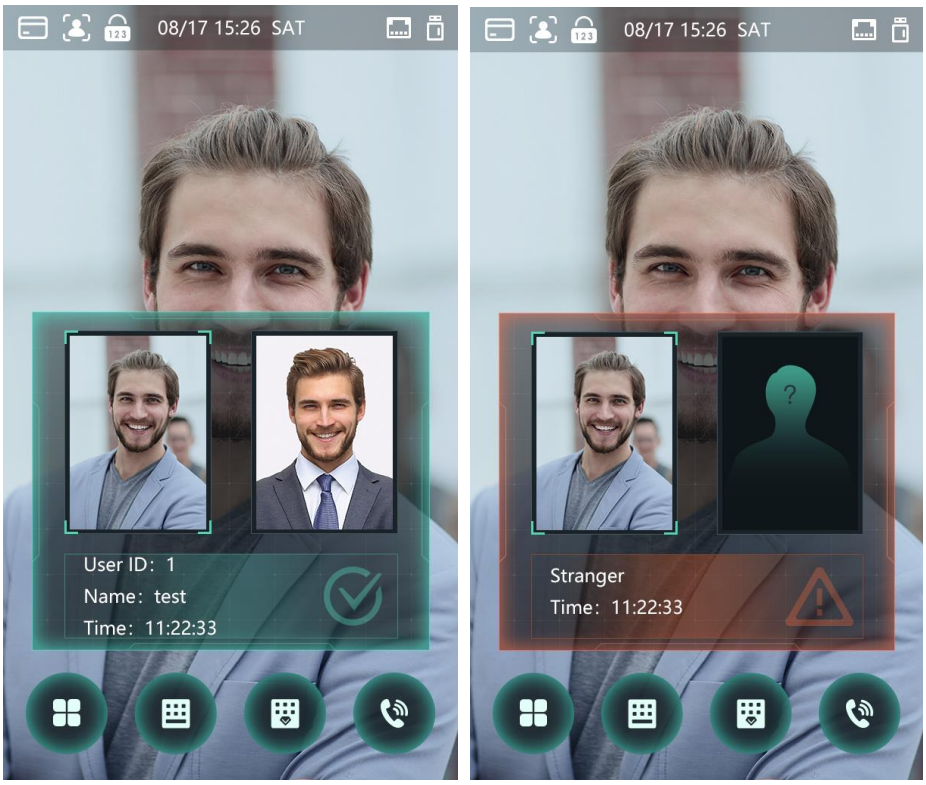
3.11.5 Result Feedback

You can select a result feedback mode as needed.

Select **Features > Result Feedback**.

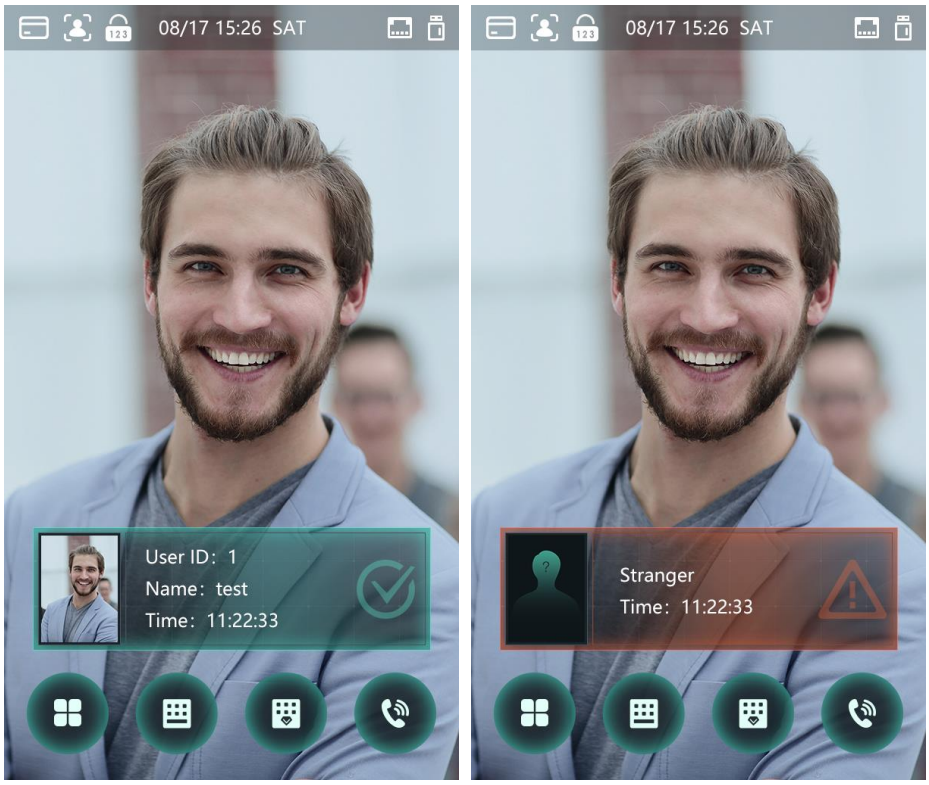
Photo & Name

Figure 3-20 Photo & name



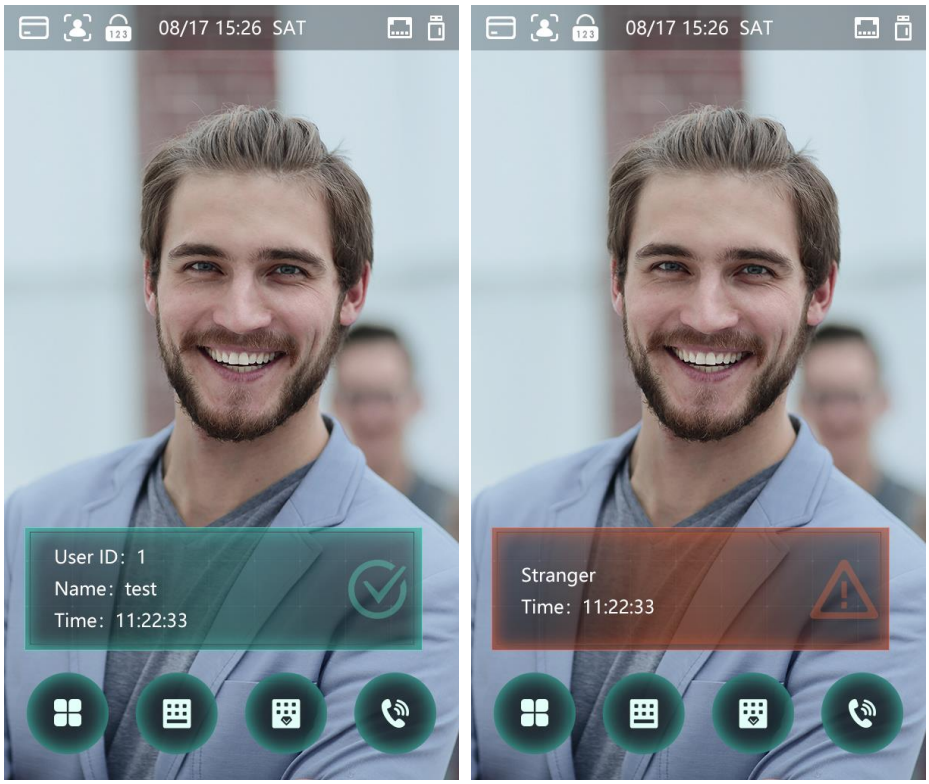
User Photo & Name

Figure 3-21 User photo & name



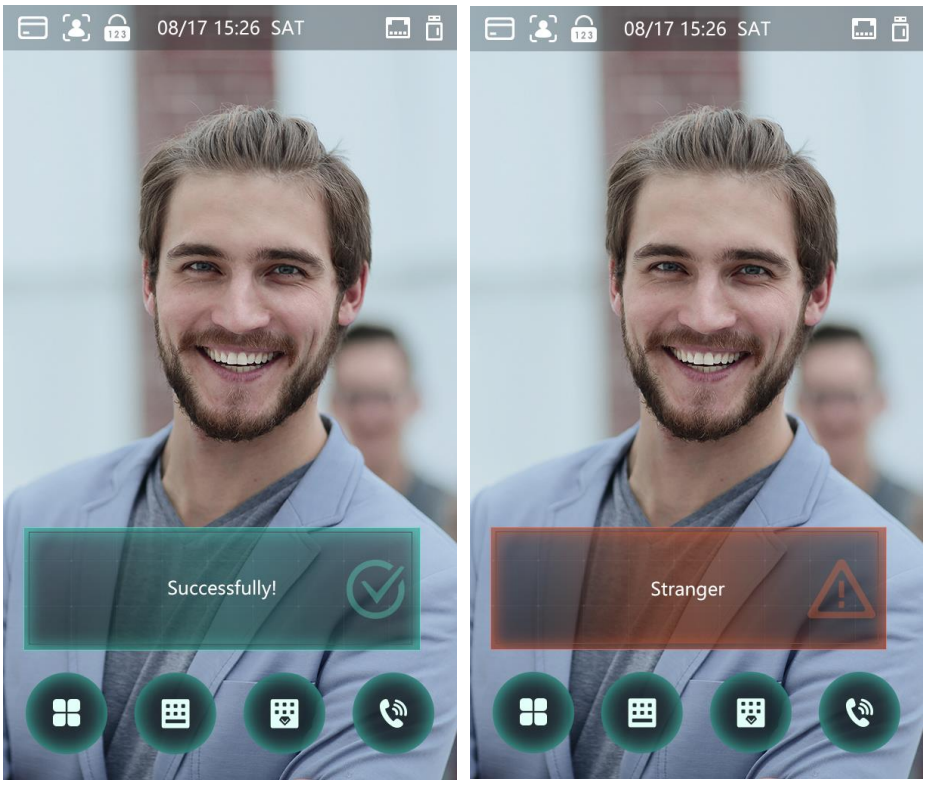
Only Name

Figure 3-22 Only name



Success or Failure

Figure 3-23 Success or failure



3.12 Record

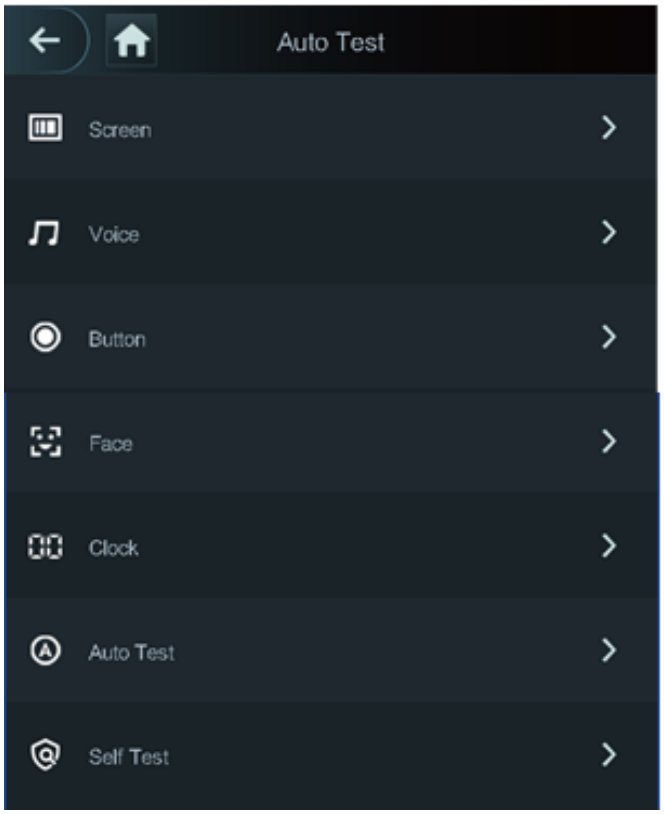
You can query all unlocking records.

Figure 3-24 Search punch records

3.13 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 3-25 Auto test



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

3.14 System Info

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

4 Web Operations

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.

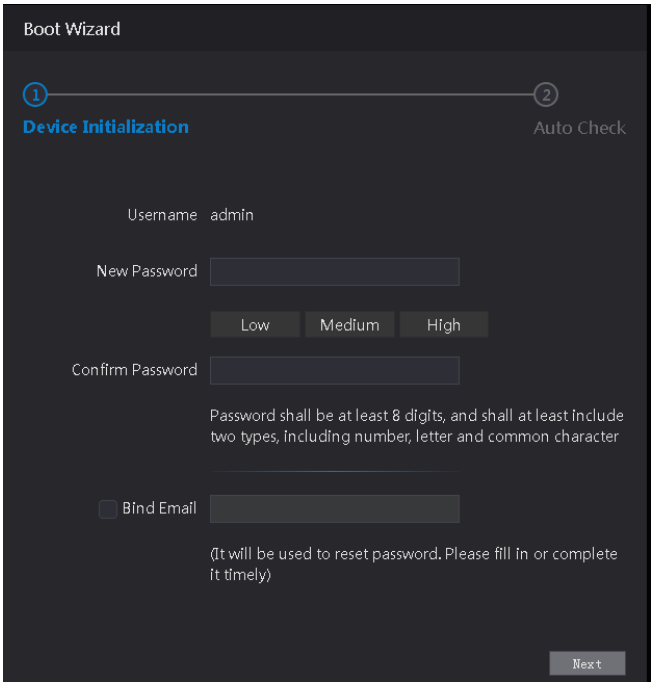
4.1 Initialization

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 terminal in the address bar, and then press Enter.

- 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 X terminals have dual NICs. The default IP address for ETH1 is 192.168.1.108, and for ETH2 is 192.168.2.108.

Figure 4-1 Initialization



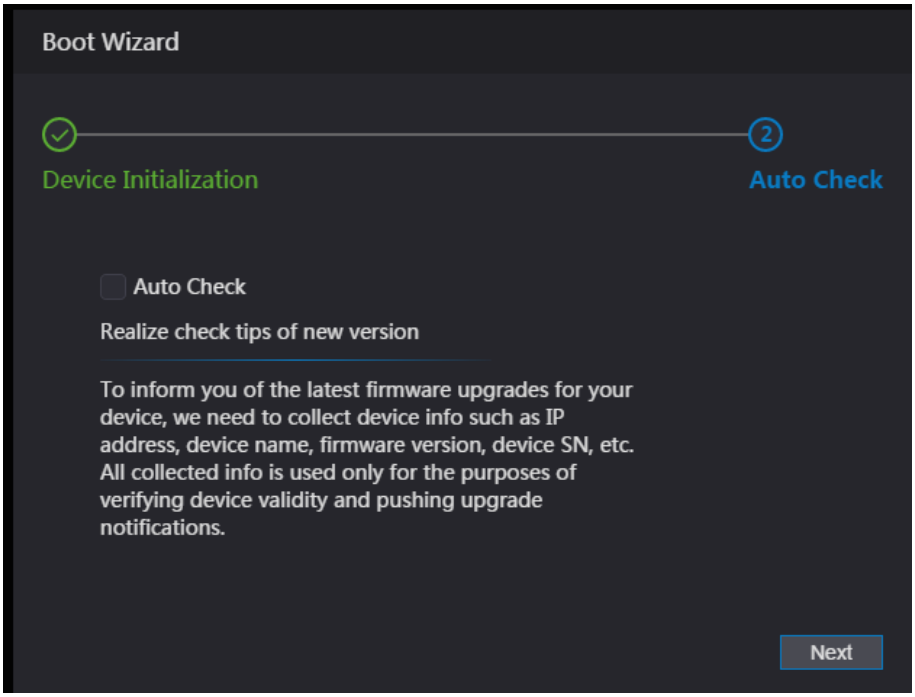
Step 2 Enter the new password, confirm password, enter an email address, and then click **Next**.

- The password must 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 ' " ; : &). Set a password of high security level according to the password strength prompt.
- For security, keep the password properly after initialization and change the password regularly.

- When you need to reset the administrator password by scanning the QR code, you need an email address to receive the security code.

Step 3 Click **Next**.

Figure 4-2 Auto check

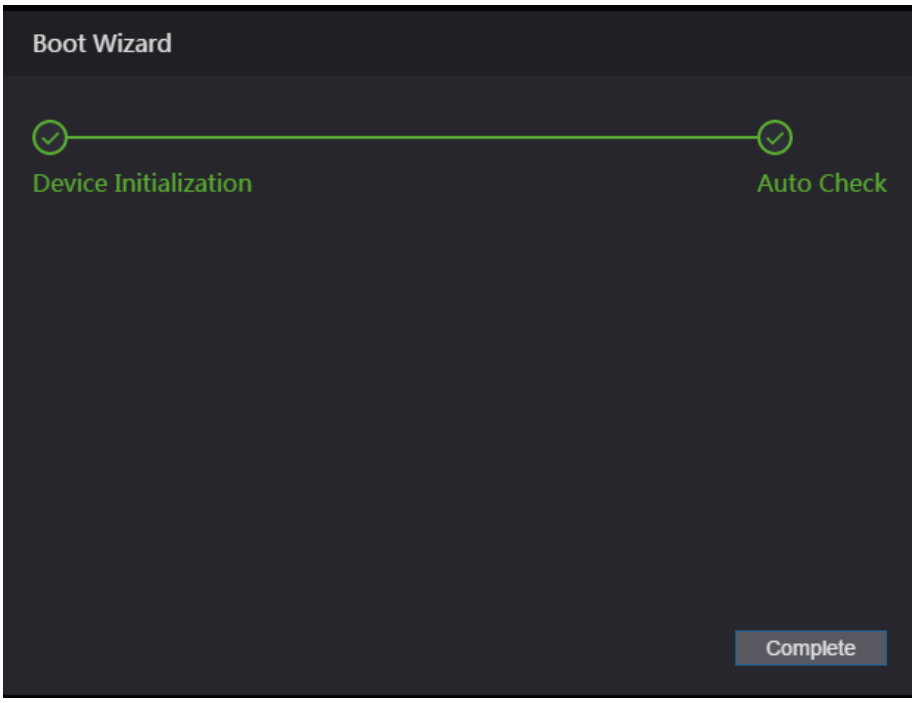


Step 4 You can decide whether to select **Auto Check** or not.

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

Step 5 Click **Next**.

Figure 4-3 Auto check completed



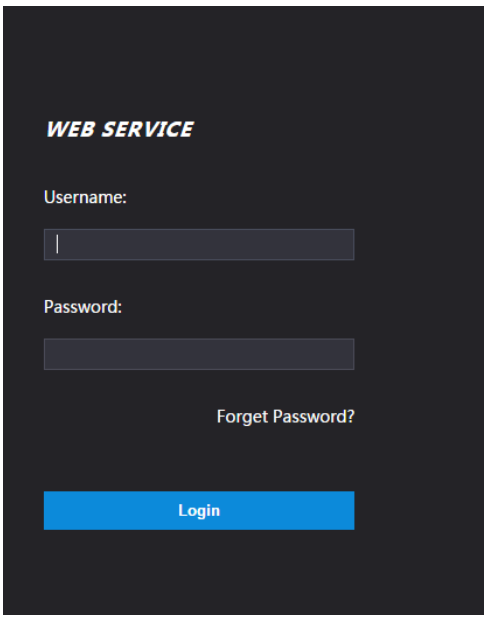
Step 6 Click **Complete**, and the initialization is completed.

4.2 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 X terminals have dual NICs. The default IP address for ETH1 is 192.168.1.108, and for ETH2 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 "4.3 Resetting the Password."

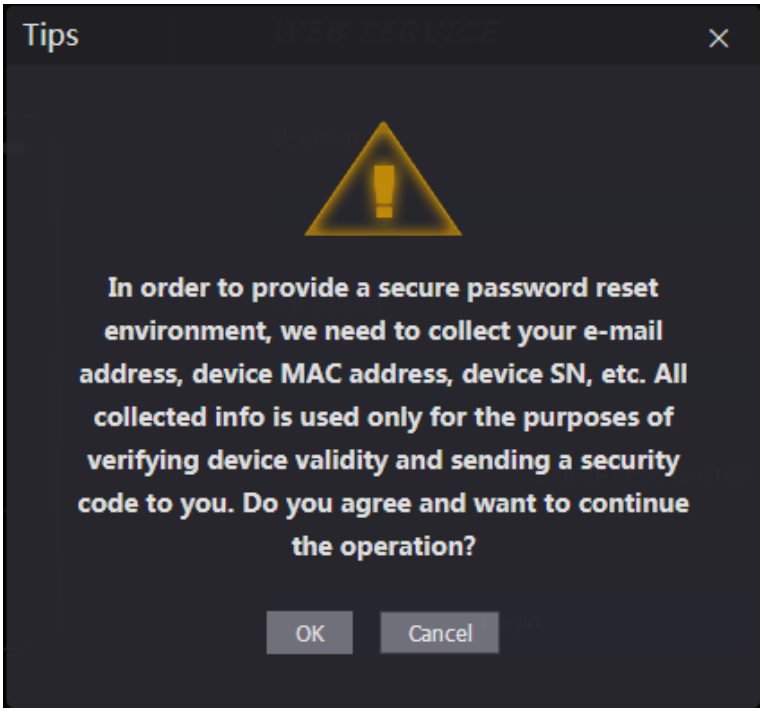
Step 3 Click **Login**.

4.3 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.

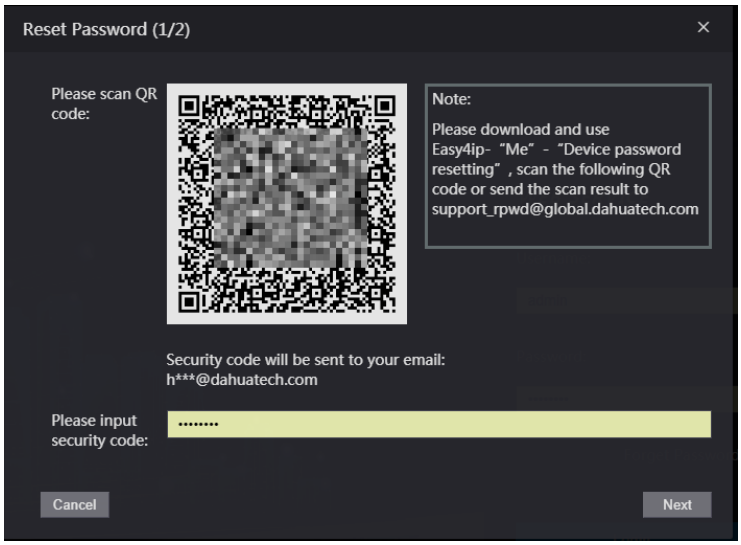
Figure 4-5 Tips



Step 2 Read the tips.

Step 3 Click **OK**.

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**.

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.

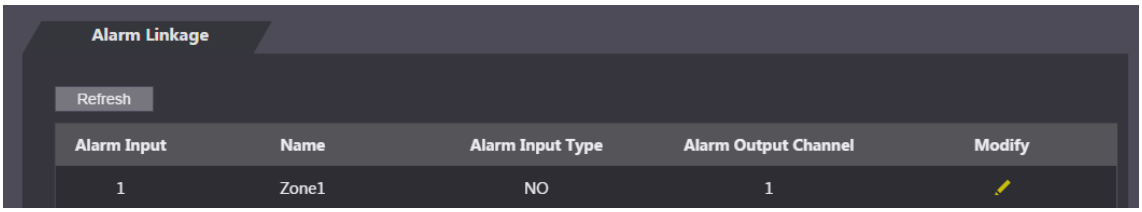
4.4 Alarm Linkage

4.4.1 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.

Figure 4-7 Alarm linkage



Step 2 Click , and then you can modify alarm linkage parameters.

Figure 4-8 Modifying alarm linkage parameter

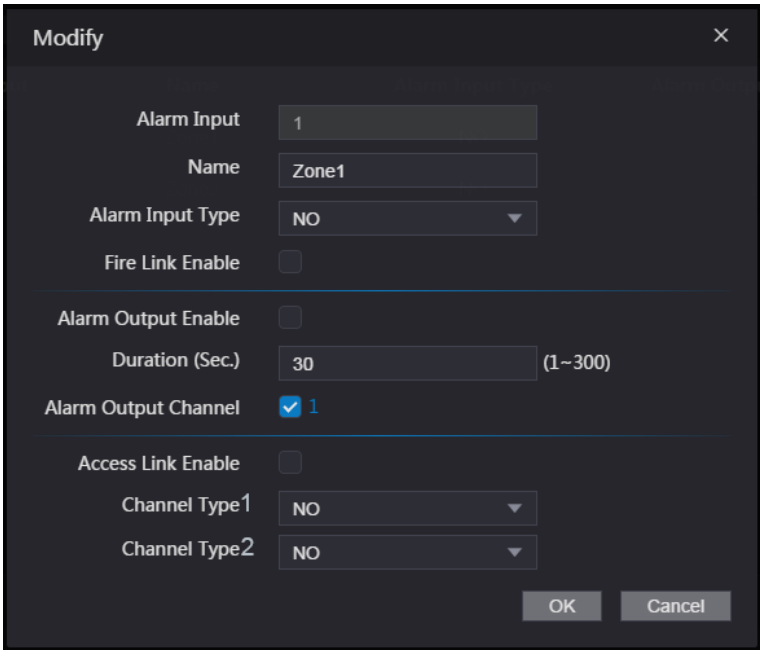


Table 4-1 Alarm linkage parameter description

Parameter	Description
Alarm Input	You cannot modify the value. Keep it default.
Name	Enter a zone name.
Alarm Input Type	There are two options: NO and NC.

Parameter	Description
	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.
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.

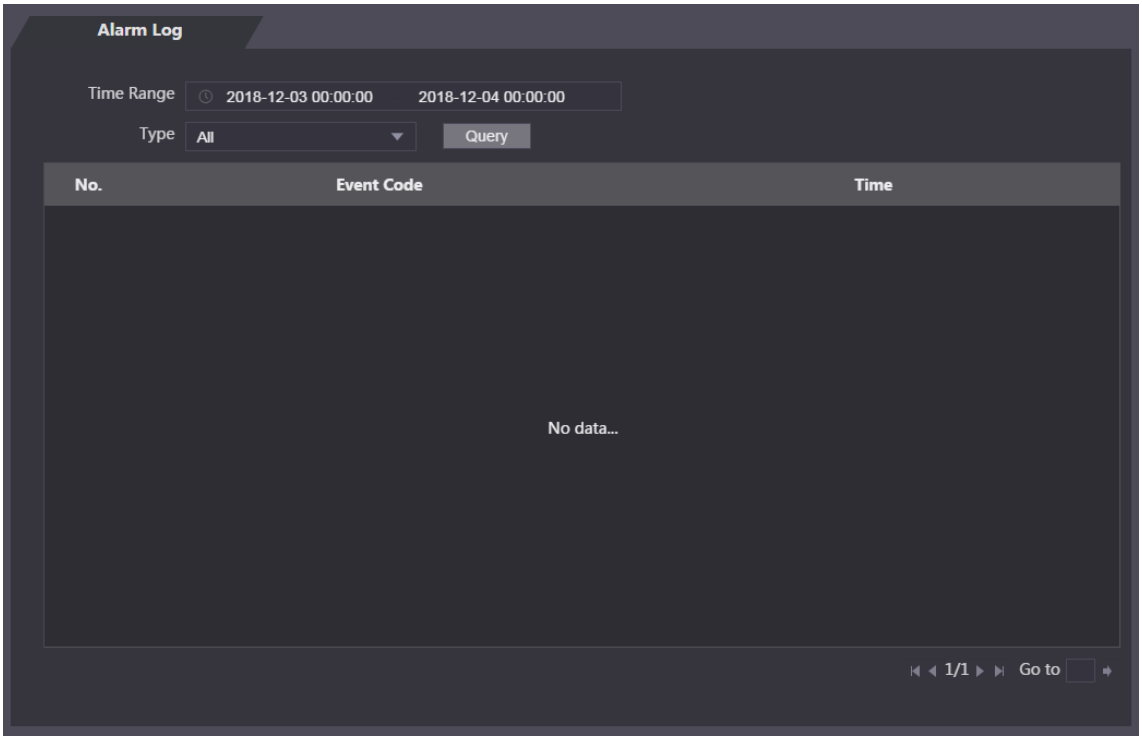
The configuration on the web will be synchronized with the configuration in the client if the terminal is added to a client.

4.4.2 Alarm Log

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

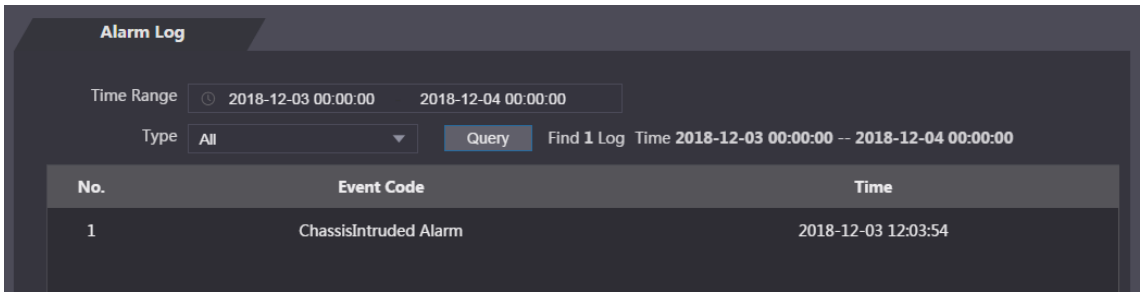
Step 1 Select **Alarm Linkage > Alarm Log**.

Figure 4-9 Alarm log



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

Figure 4-10 Query results



4.5 Call Configuration

The access controller can work as a door station and call other devices.

4.5.1 Configuring the Access Controller

Set the device type and number.

4.5.1.1 Access Controller as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Local**.

Step 3 Configure the parameters.

Figure 4-11 Local (1)

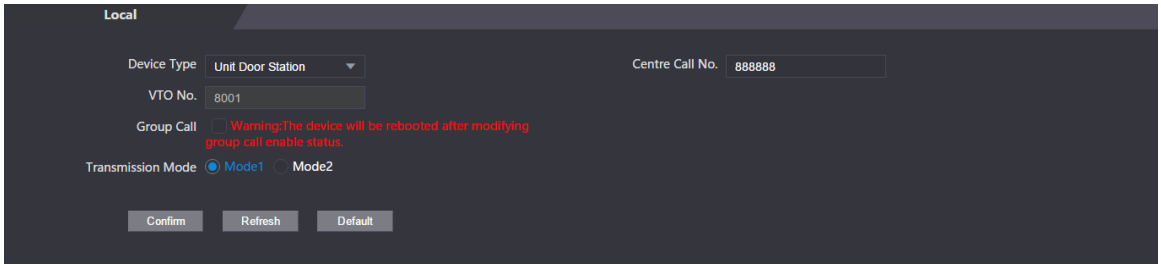


Table 4-2 Parameter description

Parameter	Description
Device Type	The access controller can only work as a unit door station.
Centre Call No.	Enter a number to be identified by the management center. It should be "888888" plus three numbers.
VTO No.	Cannot be configured.
Group Call	When enabled, a call from the access controller to a master indoor station will also be sent to all its extention indoor stations.
Transmission Mode	● Mode1: Real-time call but the video and sound may be lagging with poor network. ● Mode2: Not real-time call but ensures smooth video and sound.

Step 4 Click **Confirm**.

4.5.1.2 Other Device as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Local**.

Step 3 Configure the parameters.

Figure 4-12 Local (2)

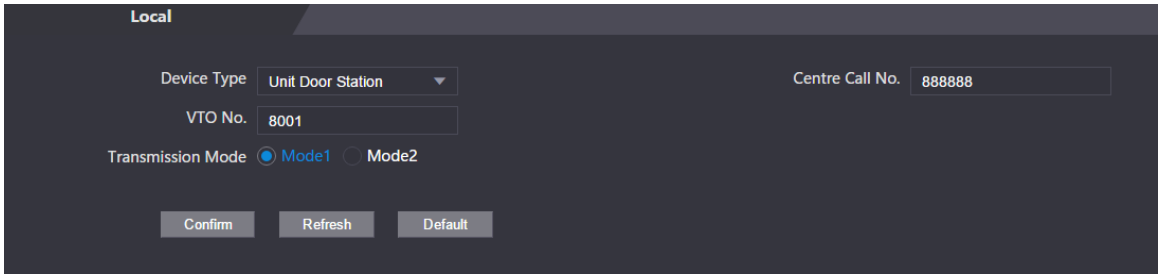


Table 4-3 Parameter description

Parameter	Description
Device Type	The access controller can work as a unit door station or fence station.
Centre Call No.	Enter a number to be identified by the management center. It should be "888888" plus three numbers.
VTO No.	Enter a number for the access controller. ● It should be four digits. The first two should be 80 and the last two starts with 01, such as 8001. ● If there are multiple door stations, VTO numbers cannot be the same.
Transmission Mode	● Mode1: Real-time call but the video and sound may be lagging with poor network. ● Mode2: Not real-time call but ensures smooth video and sound.

4.5.2 SIP Server

On the web, you can add door stations and indoor stations to the SIP server so that they can talk to each other. The SIP server can be the access controller or other door stations.

When the access controller works as the SIP server, it can connect up to 50 other access controllers and indoor monitors combined.

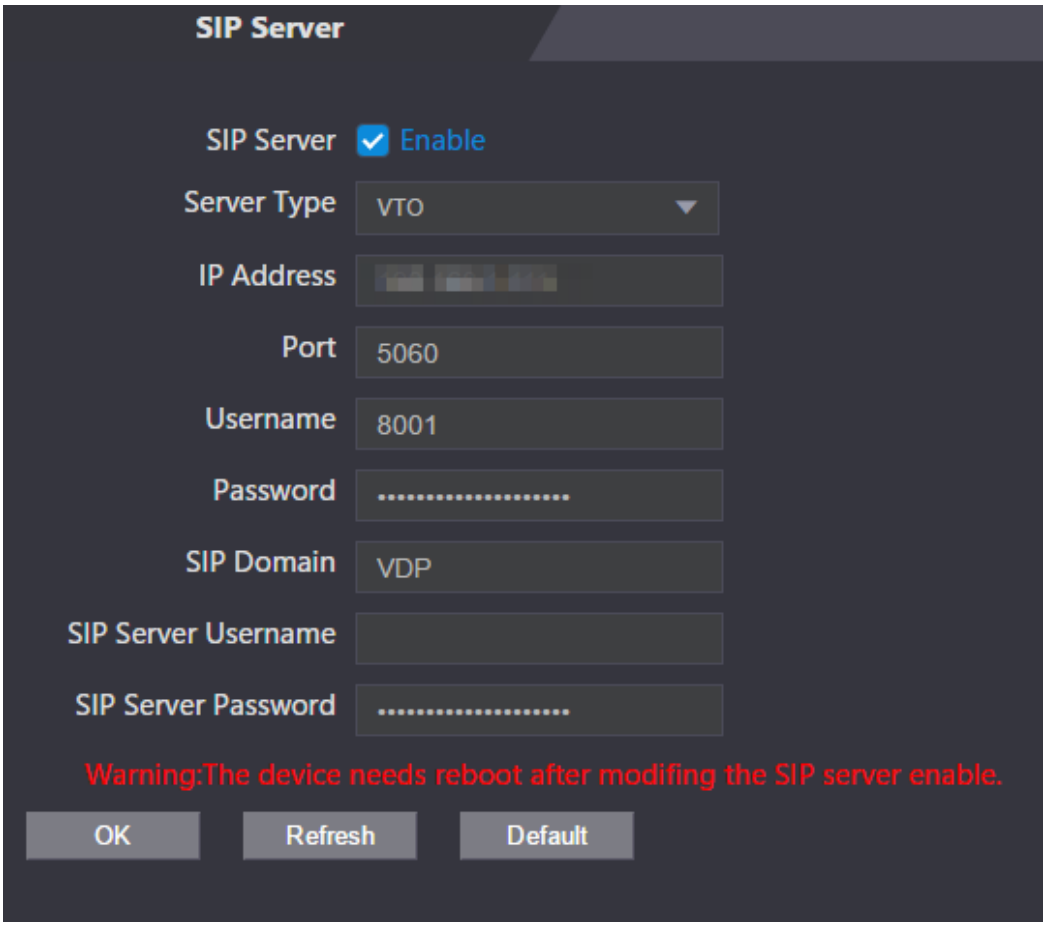
4.5.2.1 Access Controller as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > SIP Server**.

Step 3 Enable **SIP Server** and keep other parameters as default.

Figure 4-13 SIP server (1)



Step 4 Click **OK** and the access controller will restart.

4.5.2.2 Other Device as SIP Server

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > SIP Server**.

Step 3 Do not enable **SIP Server** and select **Server Type** as VTO.

Step 4 Configure the parameters.

Figure 4-14 SIP server (2)

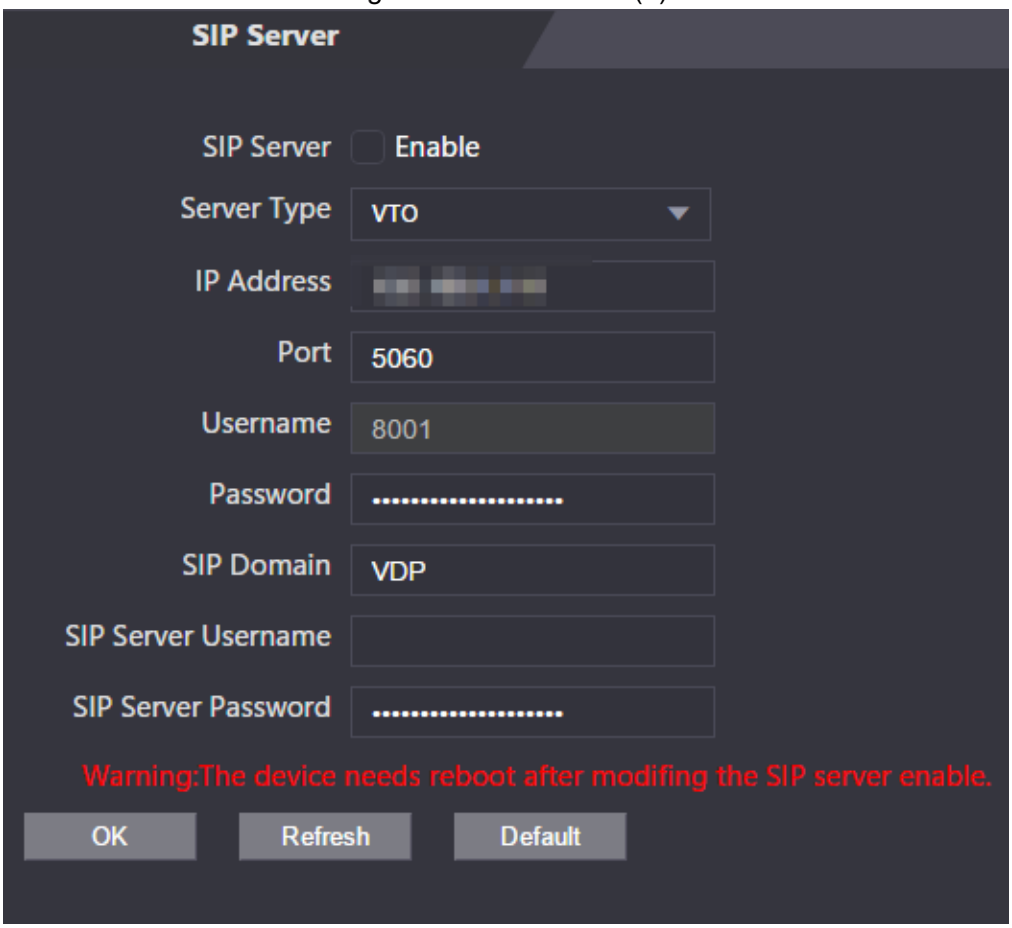


Table 4-4 SIP server parameter description (1)

Parameter	Description
IP Address	The IP address of the door station working as the SIP server.
Port	5060 by default.
Username	Keep the default values.
Password	
SIP Domain	Must be VDP.
SIP Server Username	SIP server login username and password.
SIP Server Password	

Step 5 Click **OK**.

4.5.3 Door Station Management

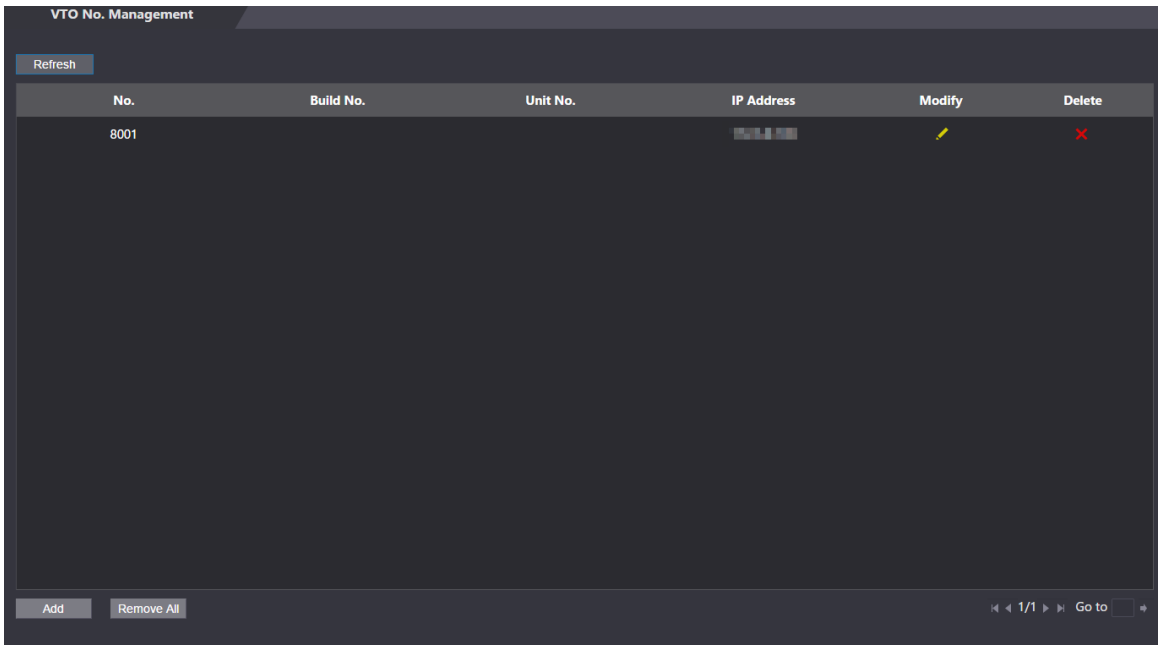
When the access controller works as the SIP server, add other door stations to call them.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > VTO No. Management**.

Step 3 Click **Add**.

Figure 4-15 VTO No. management



Step 4 Configure the parameters.

Figure 4-16 Add a door station

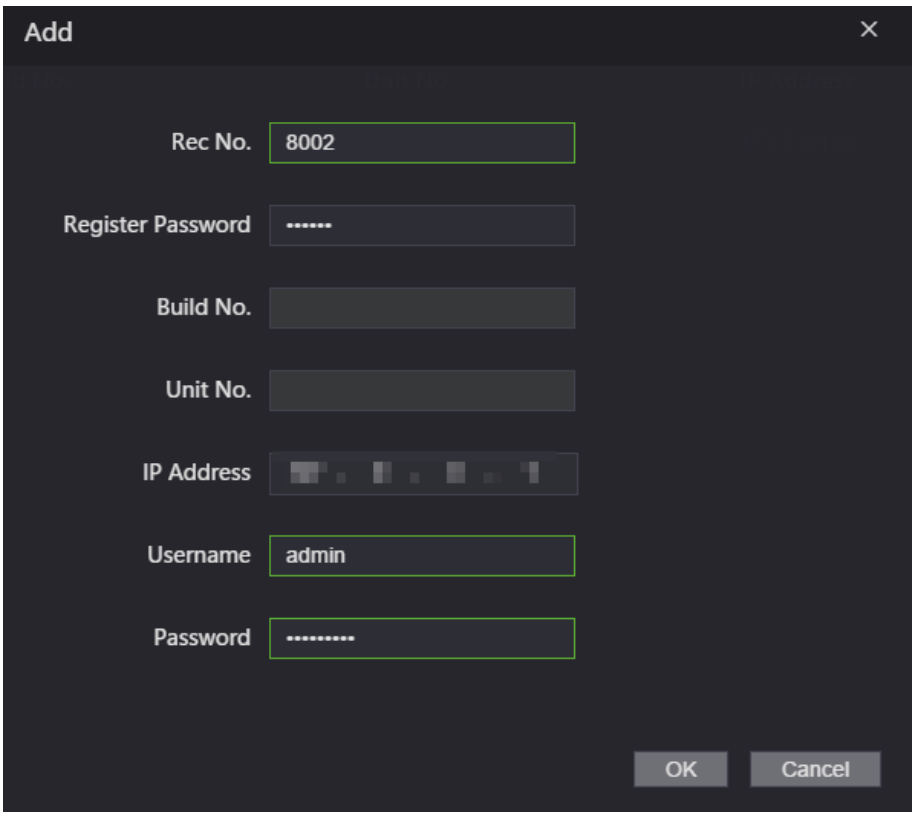


Table 4-5 Parameter description

Parameter	Description
Rec No.	Number of the door station.
Register Password	Keep the default value.
Build No.	Cannot be configured.
Unit No.	Cannot be configured.
IP Address	IP address of the door station.

Parameter	Description
Username	Web login username and password for the door station.
Password	

Step 5 Click **OK**.

4.5.4 Indoor Monitor Management

When the access controller works as the SIP server, add all relevant indoor monitors to call them.

When there are master and extension indoor monitors, you need to enable group call function first before adding them.

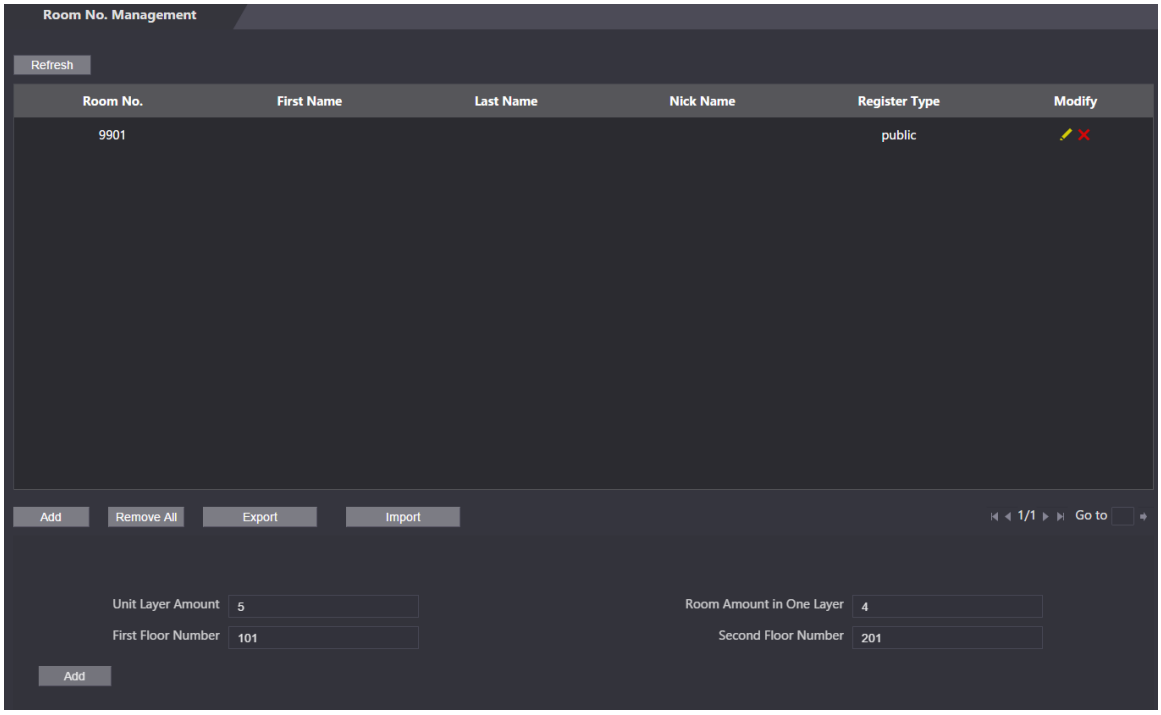
4.5.4.1 Add One Indoor Monitor

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Room No. Management**.

Step 3 Click **Add**.

Figure 4-17 Room No. Management



Step 4 Enter the information.

Figure 4-18 Add one indoor monitor

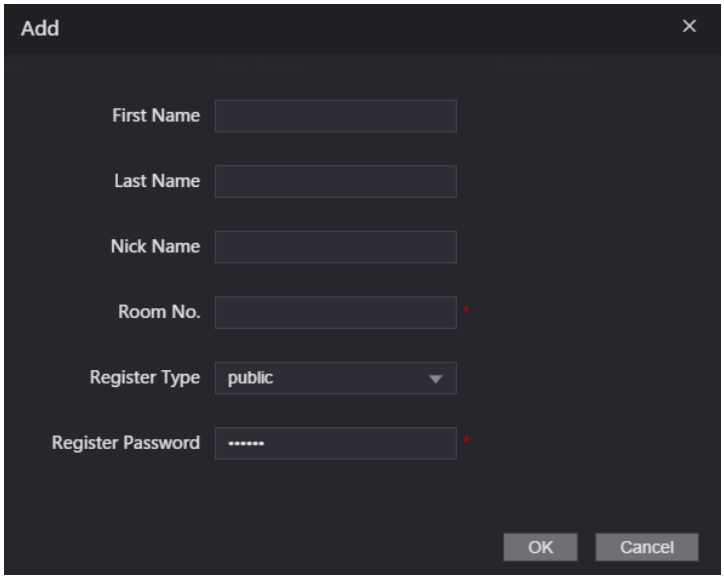


Table 4-6 Parameter description

Parameter	Description
First Name	To differentiate each indoor monitor.
Last Name	
Nick Name	
Room No.	Room number of the indoor monitor. ● It can contain up to five digits and must be the same as the one configured on the indoor monitor. ● When there are master and extension indoor monitors, the room number of master indoor monitor should end with "-0", and that of extension indoor monitors with "-1", "-2", "-3"…For example, the master indoor monitor is 101-0, extension monitors are 101-1, 101-2 and 101-3.
Register Type	Keep the default value.
Register Password	

Step 5 Click **OK**.

You can also click **Export** to export the room number and import to other devices.

4.5.4.2 Add Indoor Monitors in Batches

You can add up to 1024 indoor monitors.

Step 1 Log in to the web.

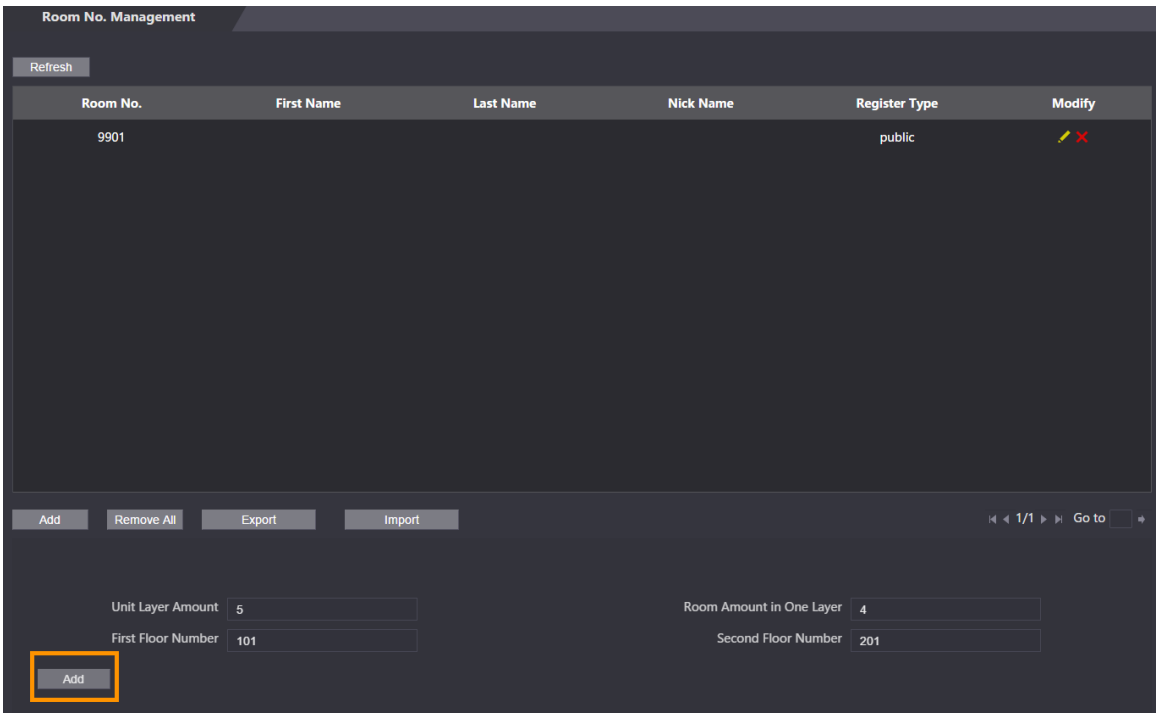
Step 2 Select **Talkback Setting > Room No. Management**.

Step 3 At the bottom, enter numbers for Unit Layer Amount, Room Amount in One Layer, First Floor Number and Second Floor Number.

- Unit layer amount can be 1–99, room amount in one layer 1–99, and floor number 1–99999.

Step 4 Click **Add**.

Figure 4-19 Add indoor monitors in batches



4.5.5 Configuring the Managing Device

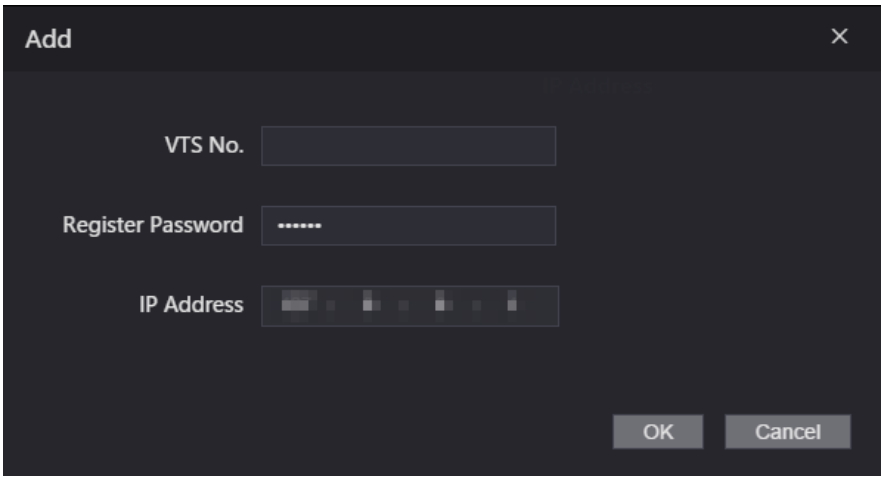
When the access controller works as the SIP server, add other managing devices to call them.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > VTS Management**.

Step 3 Click **Add**.

Figure 4-20 Add managing devices

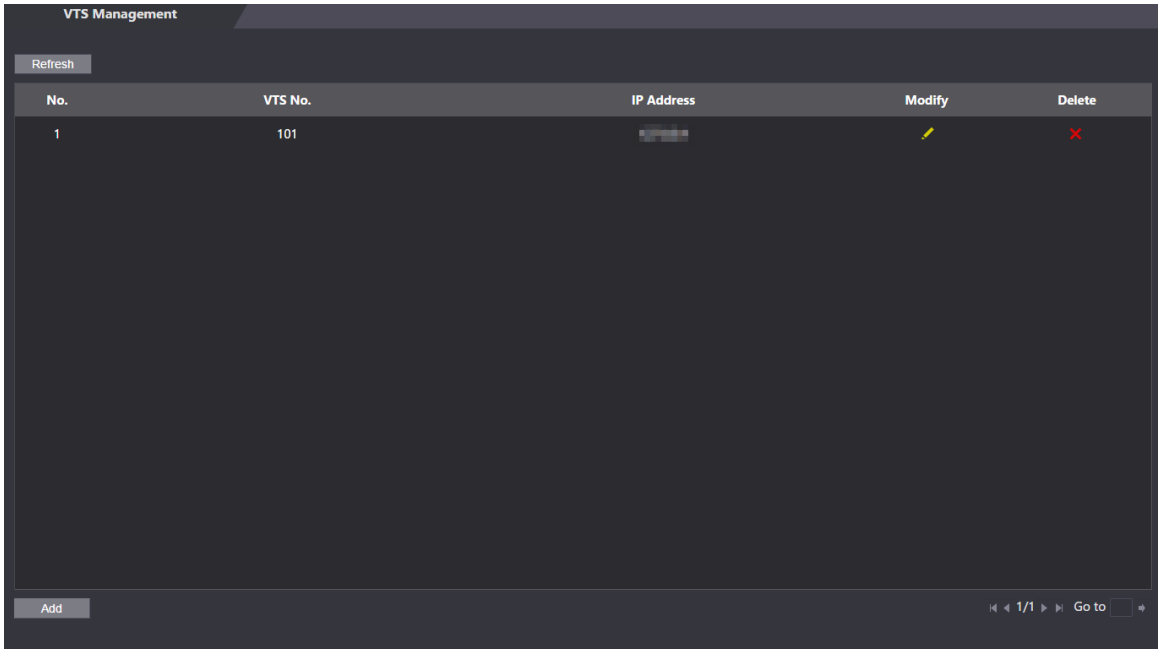


Step 4 Enter the information.

- VTS No. can contain up to 9 digits.
- Login password for the managing device. Keep the default value.

Step 5 Click **OK**.

Figure 4-21 Added a managing device



- Modify a managing device.
  You need to update the information when the register password or IP address of the managing device changes. Click and enter the new password or IP address, and then click **OK**.
- Delete a managing device.
  Click .

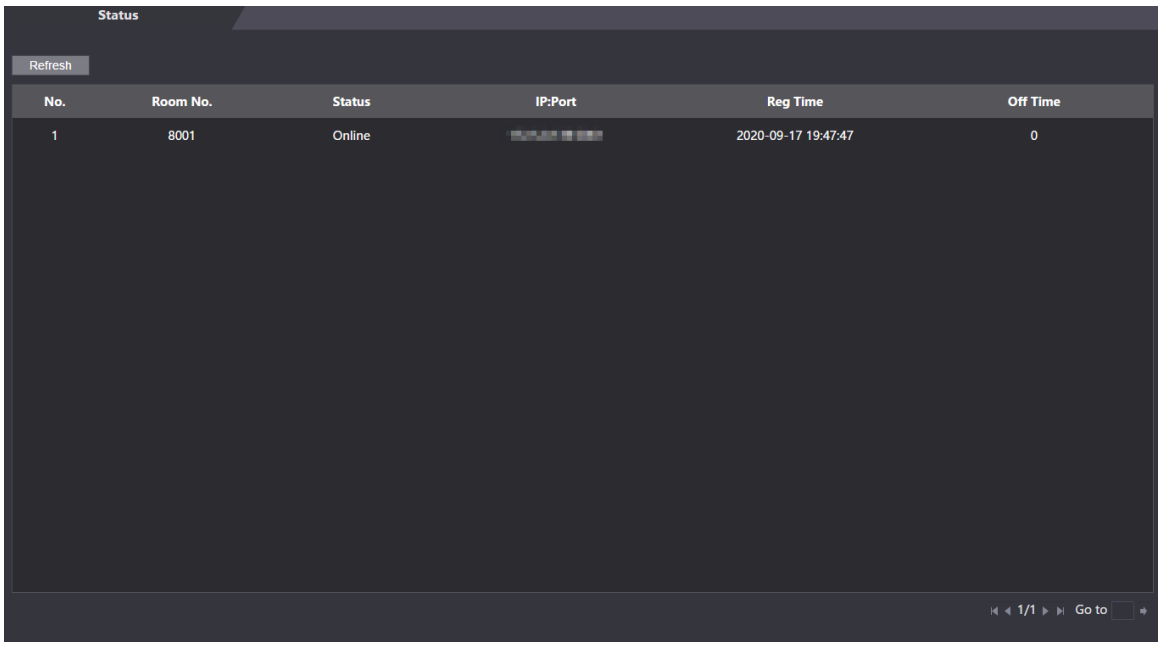
4.5.6 Online Status

When the access controller works as the SIP server, administrators can log in to the web and check the information of online devices.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Status**.

Figure 4-22 Status



4.5.7 Call Logs

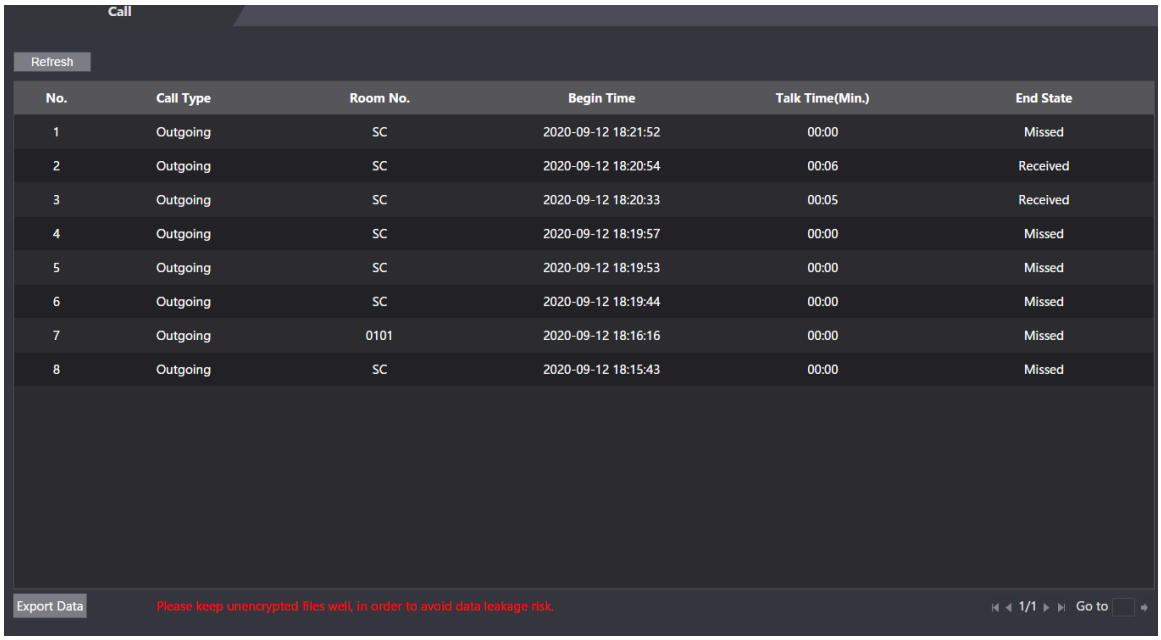
You can check up to 1024 call logs.

Step 1 Log in to the web.

Step 2 Select **Talkback Setting > Call**.

Step 3 (Optional) Click **Export Data** to export all the logs.

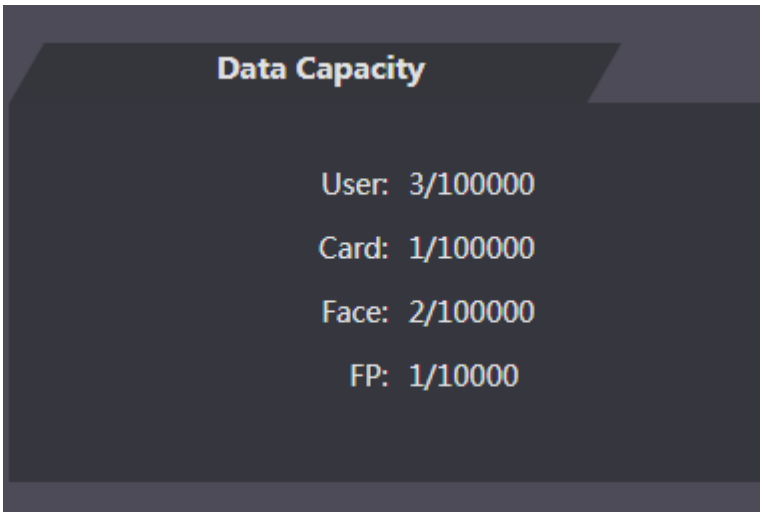
Figure 4-23 Call logs



4.6 Data Capacity

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

Figure 4-24 Data capacity



4.7 Video Setting

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

4.7.1 Data Rate

Figure 4-25 Data rate

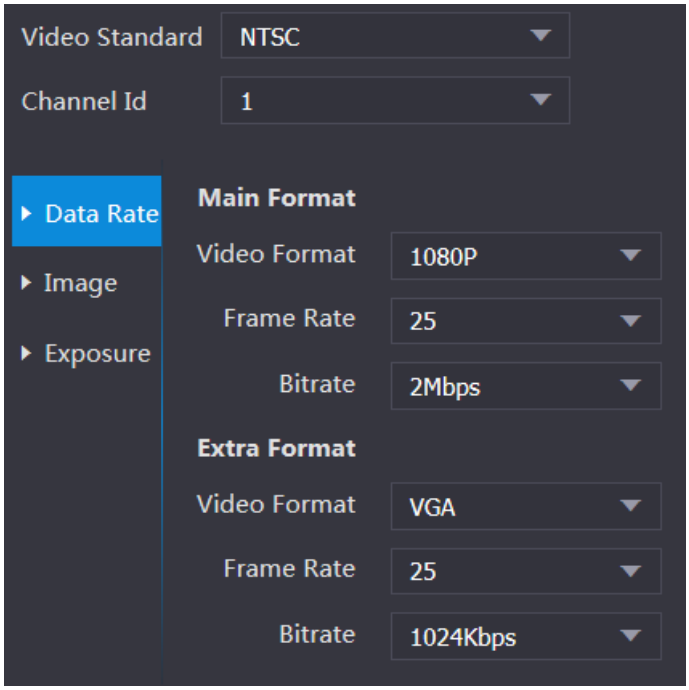


Table 4-7 Data rate parameter description

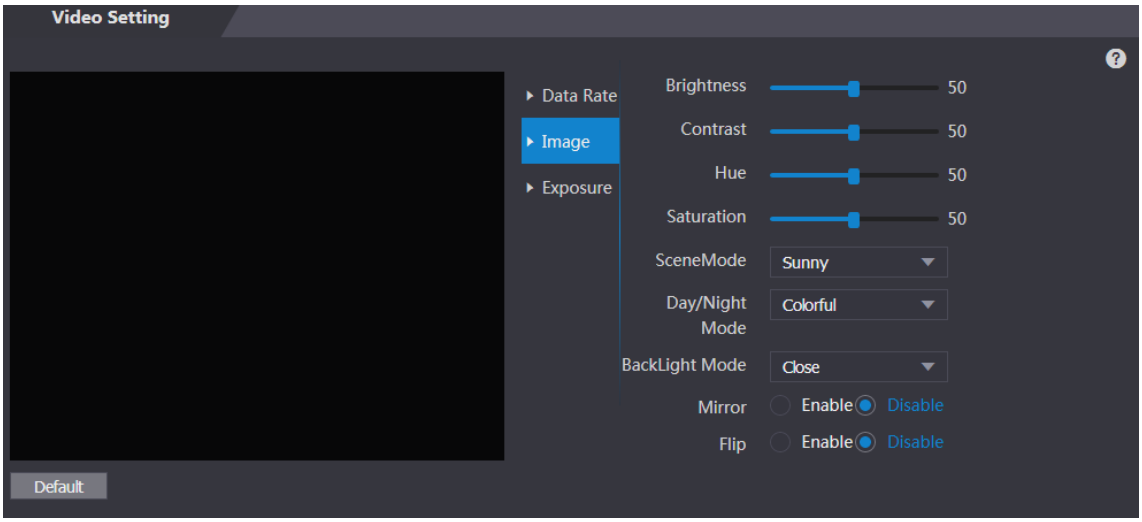
Parameter		Description
Video Standard		There are two options: NTSC and PAL. Select a standard according to the video standard of your region.
Channel		There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.
Main Format	Video Format	There are four options: D1, VGA, 720p and 1080p. Select an option according to the video quality you want. 720p is set by default. If you need the call function, do not set it to 1080p.
	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.

4.7.2 Image

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

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

Figure 4-26 Image



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

Table 4-8 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.
Back Light Mode	● Close: Without backlight. ● 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 WDR. ● 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, images can be flipped over.

4.7.3 Exposure

Table 4-9 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

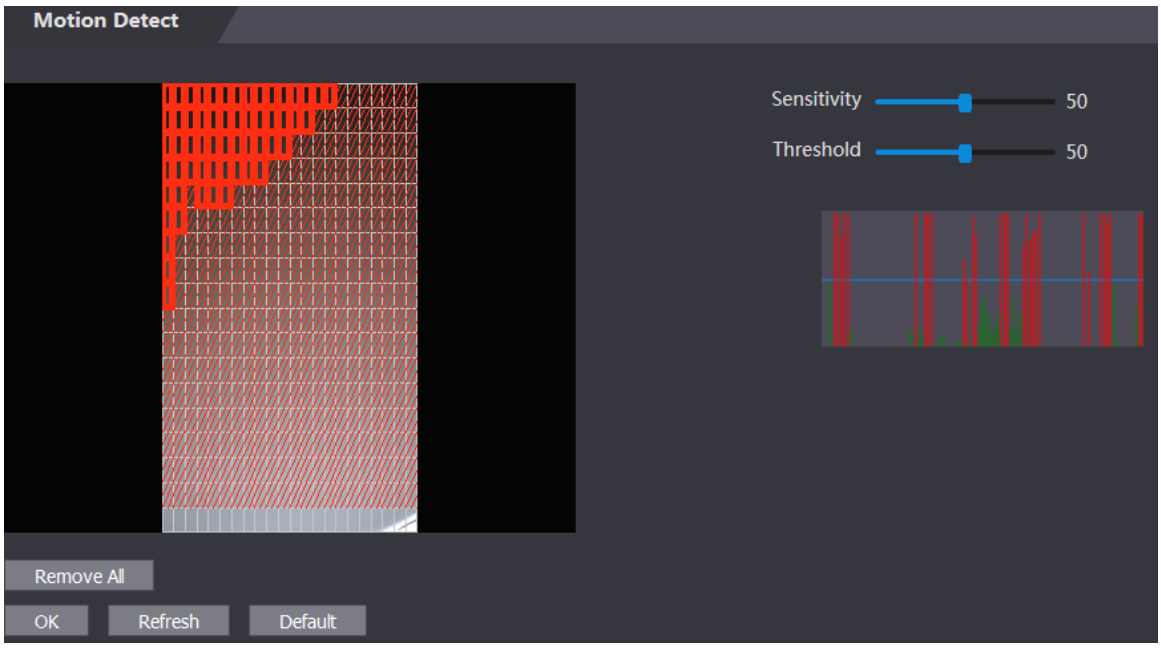
Parameter	Description
	stripes on images. ● Outdoor: When **Outdoor** is selected, the exposure mode can be switched.
Exposure Mode	 ● When you select **Outdoor** in the **Anti-flicker** drop-down list, you can select **Shutter Priority** as the exposure mode. ● Exposure modes of different devices might 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.
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.

4.7.4 Motion Detection

Set a range in which moving objects can be detected.

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

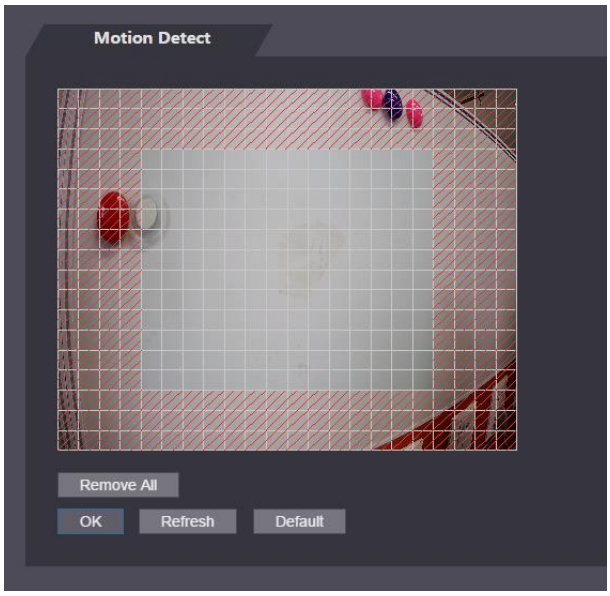
Figure 4-27 Motion detection



Step 2 Press and hold the left mouse button, and then drag the mouse in the red area.

- 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 4-28 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.

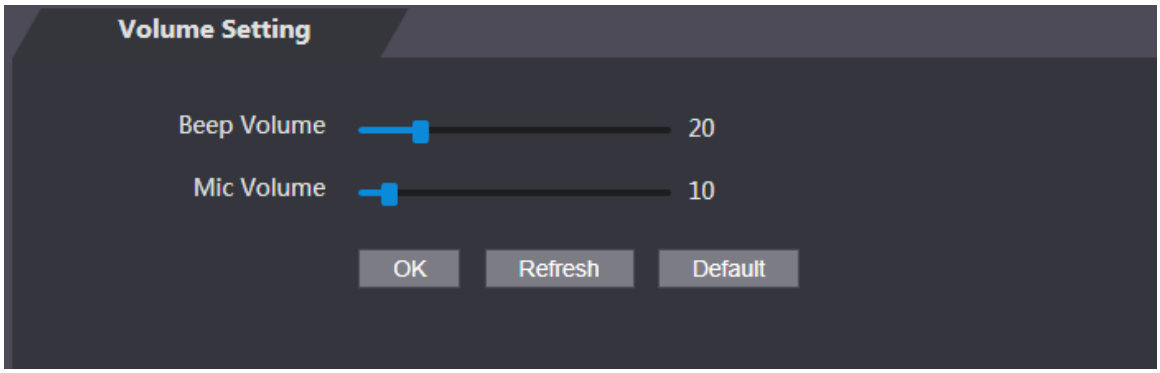
- When grid number is smaller than the threshold, green line will appear; when grid number is more than the threshold, red line will appear. See Figure 4-27.

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

4.7.5 Volume Setting

You can adjust volume of the terminal speaker.

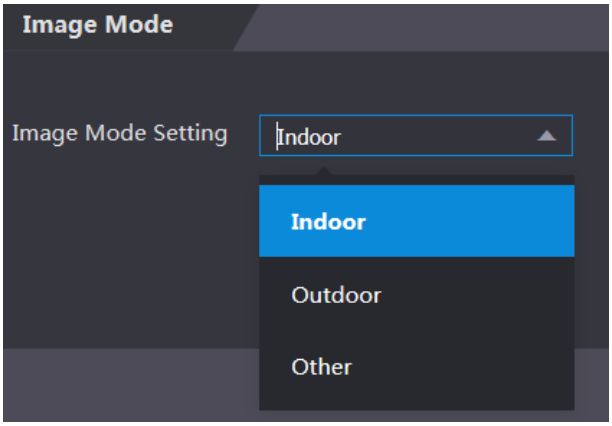
Figure 4-29 Volume setting



4.7.6 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 4-30 Image mode



4.7.7 Local Coding

Set up the area to be displayed on the indoor monitors.

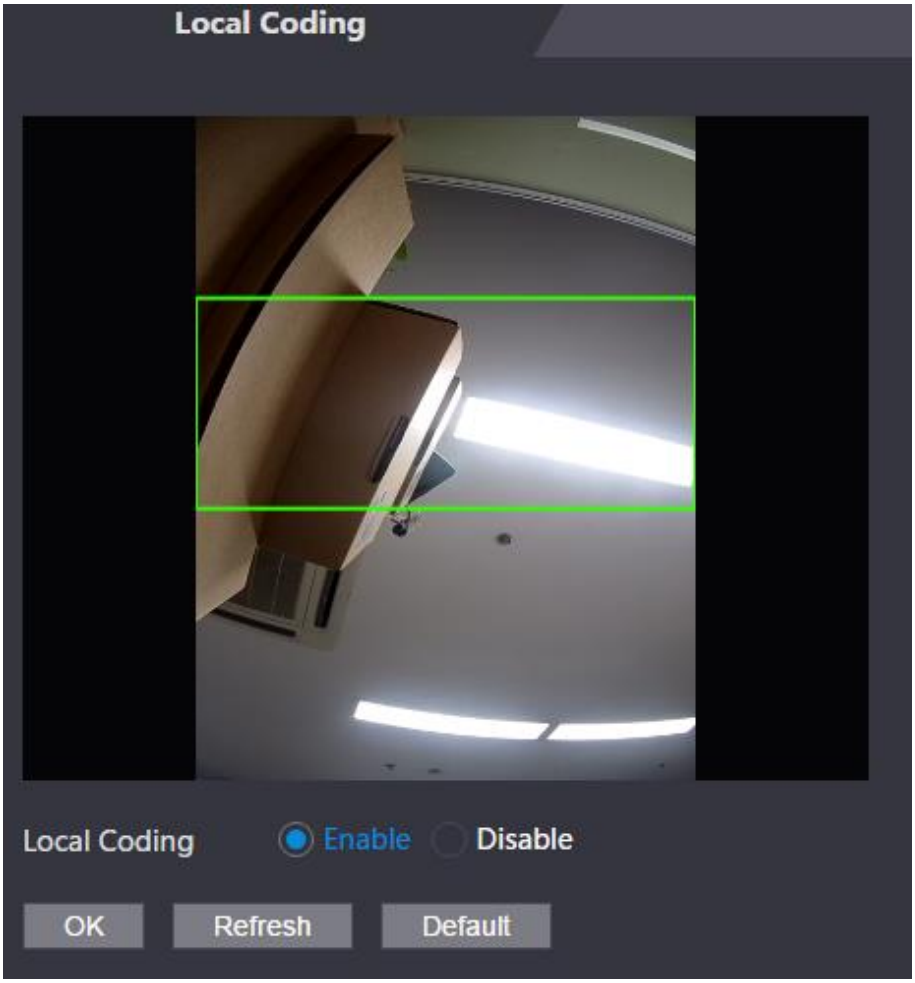
Step 1 Log in to the web.

Step 2 Select **Video Setting > Local Coding**.

Step 3 Enable the function.

Step 4 Drag the box as needed.

Figure 4-31 Local coding



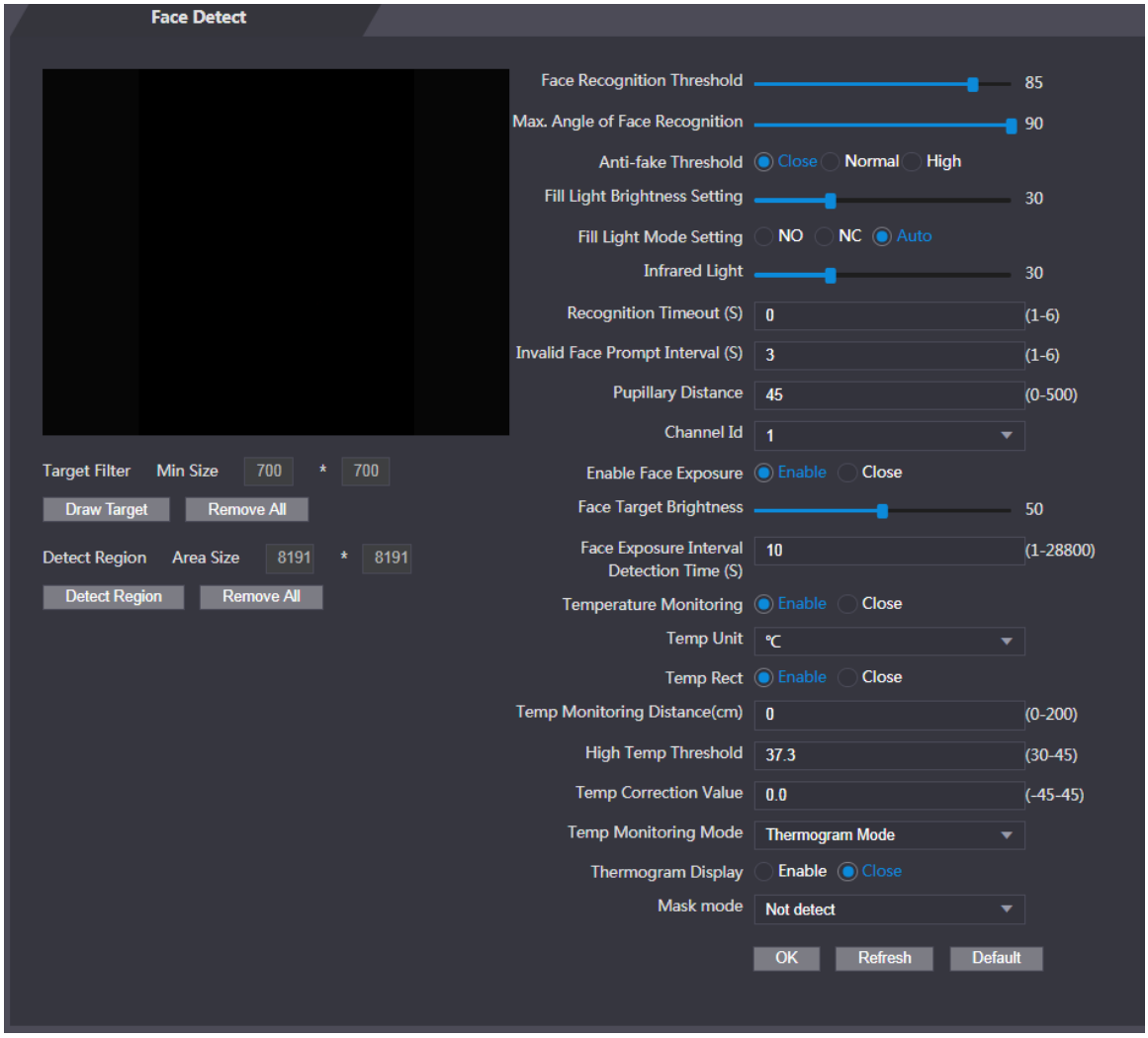
Step 5 Click **OK**.

4.8 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**.

Figure 4-32 Face detect



Step 2 Configure the parameters.

Table 4-10 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. There are two options: **Enable** and **Close**.
Fill Light Brightness Setting	You can set fill light brightness.
Fill Light Mode Setting	There are three fill light modes. ● NO: Fill light stays open. ● NC: Fill light stays 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

Parameter	Description
	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 permission 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 permission 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.
Temperature Monitoring	Set whether to enable the body temperature monitoring. ● Temp Unit: Select a temperature unit. ● Temp Rect: Set whether to display the temperature monitoring box or not. ● Temp Monitoring Distance (cm): The value is 0 by default. Set other values to enable temperature monitoring within a defined distance. 80 cm is recommended. ● Temp Threshold (°C): Set the temperature threshold. The monitored body temperature will be judged as high temperature if it is greater than or equal to the set value. ● Temp Correction Value: This parameter is for testing. The difference of the temperature monitoring environment might cause the temperature deviation between the monitored temperature and the actual temperature. You can select multiple monitored samples for testing. According to the comparison between the monitored temperature and the actual temperature, you can correct the temperature deviation by this parameter. For example, if the monitored temperature is 0.5°C lower than the actual temperature, the correction value is set to 0.5°C; if the measured temperature is 0.5°C

Parameter	Description
	higher than the actual temperature, the correction value is set to -0.5°C. Only the terminal with a temperature monitoring unit supports this parameter.
Mask Mode	● No detect: Mask is not detected during face recognition. ● Mask reminder: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is allowed. ● Mask intercept: Mask is detected during face recognition. If the person is detected without wearing a mask, the system will prompt mask reminder and passage is not allowed.

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

4.9 Network Setting

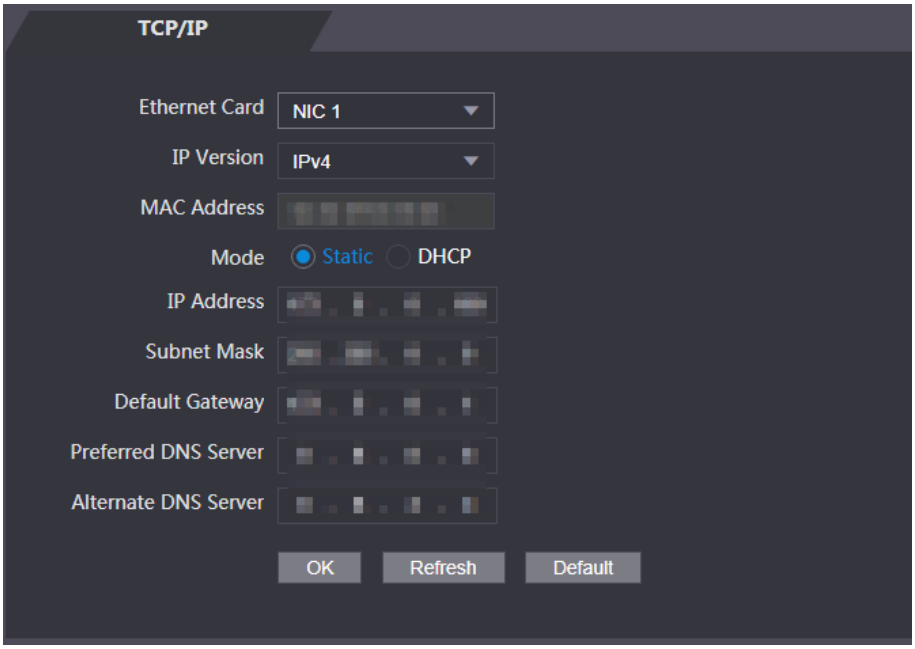
4.9.1 TCP/IP

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 4-33 TCP/IP



Step 2 Configure the parameters.

Table 4-11 TCP/IP

Parameter	Description
Ethernet Card	Select to configure parameters of the card.
IP Version	There is one option: IPv4.
MAC	MAC address of the terminal.
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.

4.9.2 Port

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

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

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 4-12 Port description

Parameter	Description
Max Connection	You can set the maximum connections of clients that the terminal can be connected to. Platform clients like Smart PSS 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.

4.9.3 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.**

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

Table 4-13 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.

4.9.4 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 4-34 P2P

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

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

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

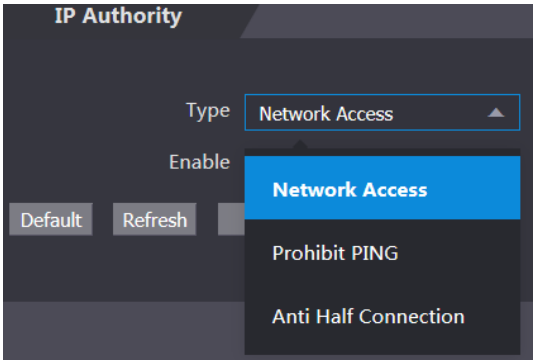
Scan the QR code on your web interface to get the serial number of the terminal.

4.10 Safety Management

4.10.1 IP Authority

Select a cybersecurity mode as needed.

Figure 4-35 IP authority



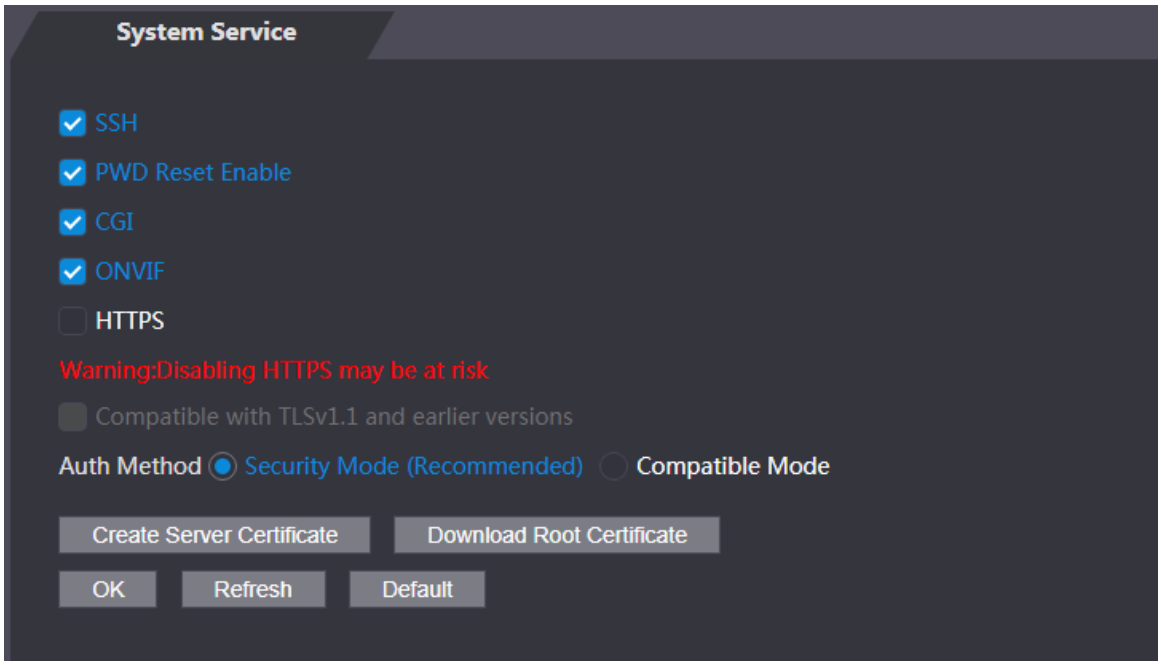
4.10.2 Systems

4.10.2.1 System Service

There are four options: SSH, PWD Reset Enable, CGI, and HTTPS. Refer to "3.11.4 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 4-36 System service



4.10.2.2 Creating Server Certificate

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

4.10.2.3 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.

4.11 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.

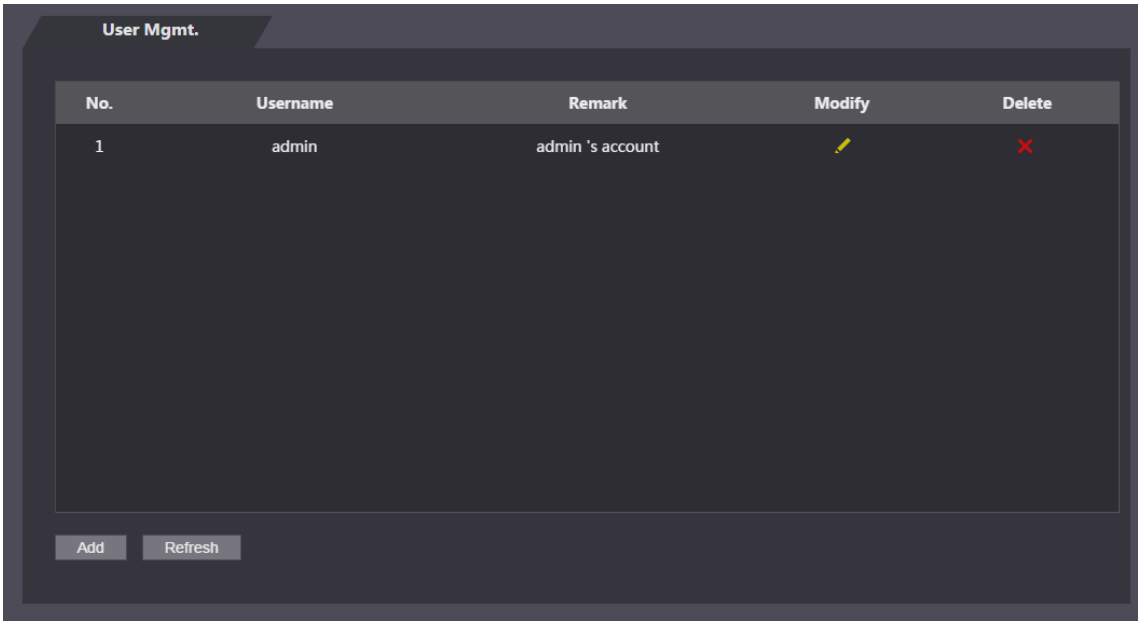
4.11.1 Adding Users

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.

4.11.2 Modifying User Information

You can modify user information by clicking on the **User Mgmt.** interface.

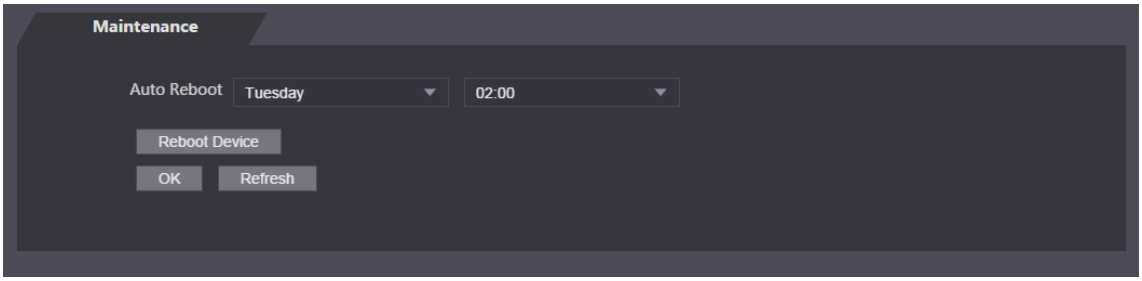
Figure 4-37 User management



4.12 Maintenance

You can make the terminal reboot itself in idle time to improve the running speed of the terminal.

Figure 4-38 Maintenance

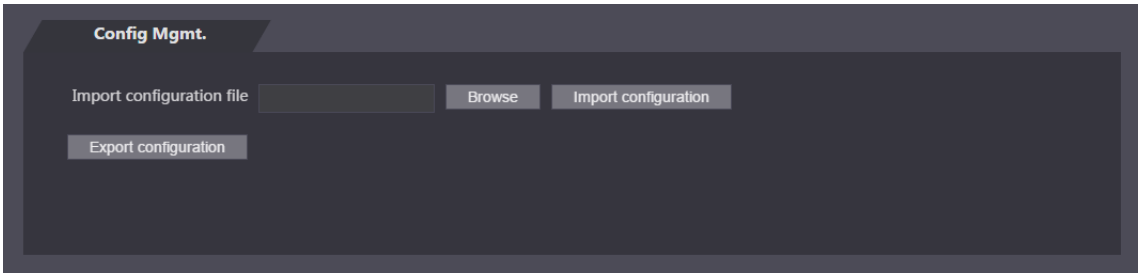


Select the auto reboot date and time. The default reboot time is at 2 O'clock in the morning on Tuesday. Click **Reboot Device**, the terminal will reboot immediately. Click **OK**, the terminal will reboot at 2 O'clock in the morning every Tuesday.

4.13 Configuration Management

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

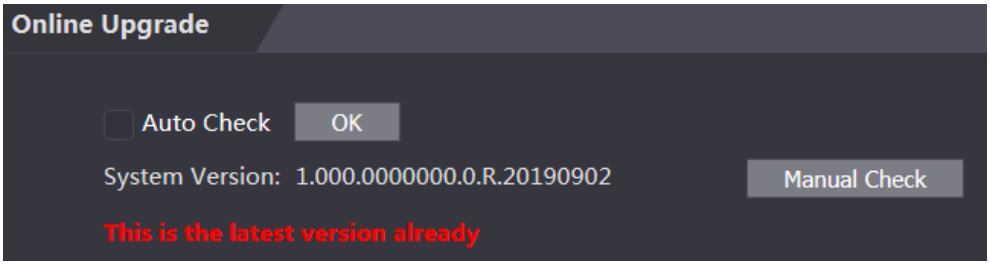
Figure 4-39 Configuration management



4.14 Upgrade

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

Figure 4-40 Upgrade



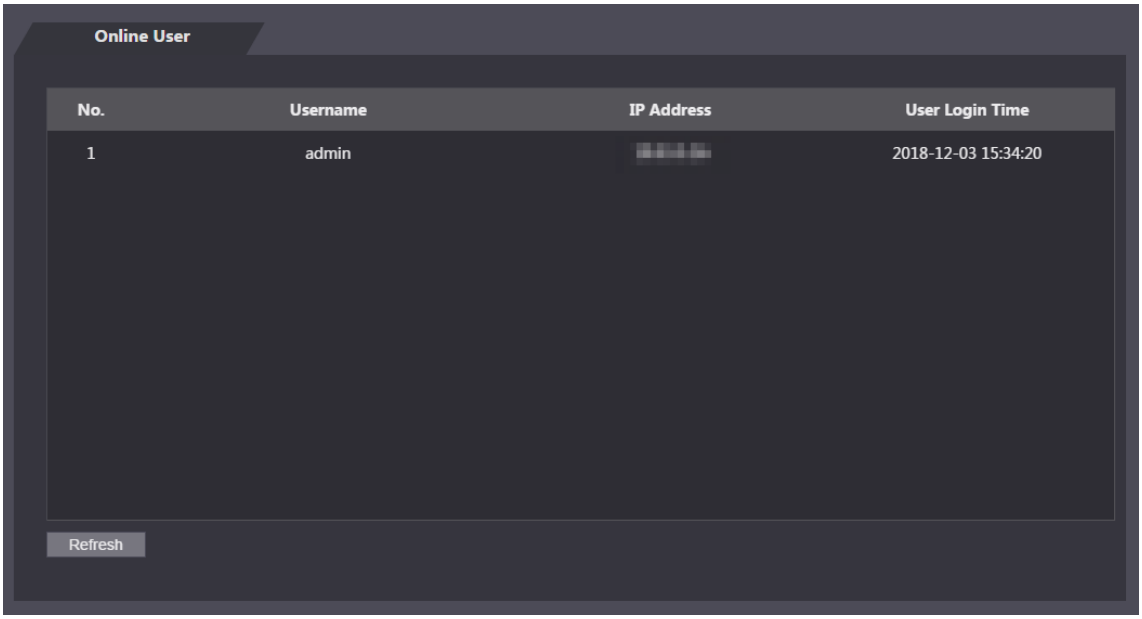
4.15 Version Information

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

4.16 Online User

You can view username, IP address, and user login time on the **Online User** interface.

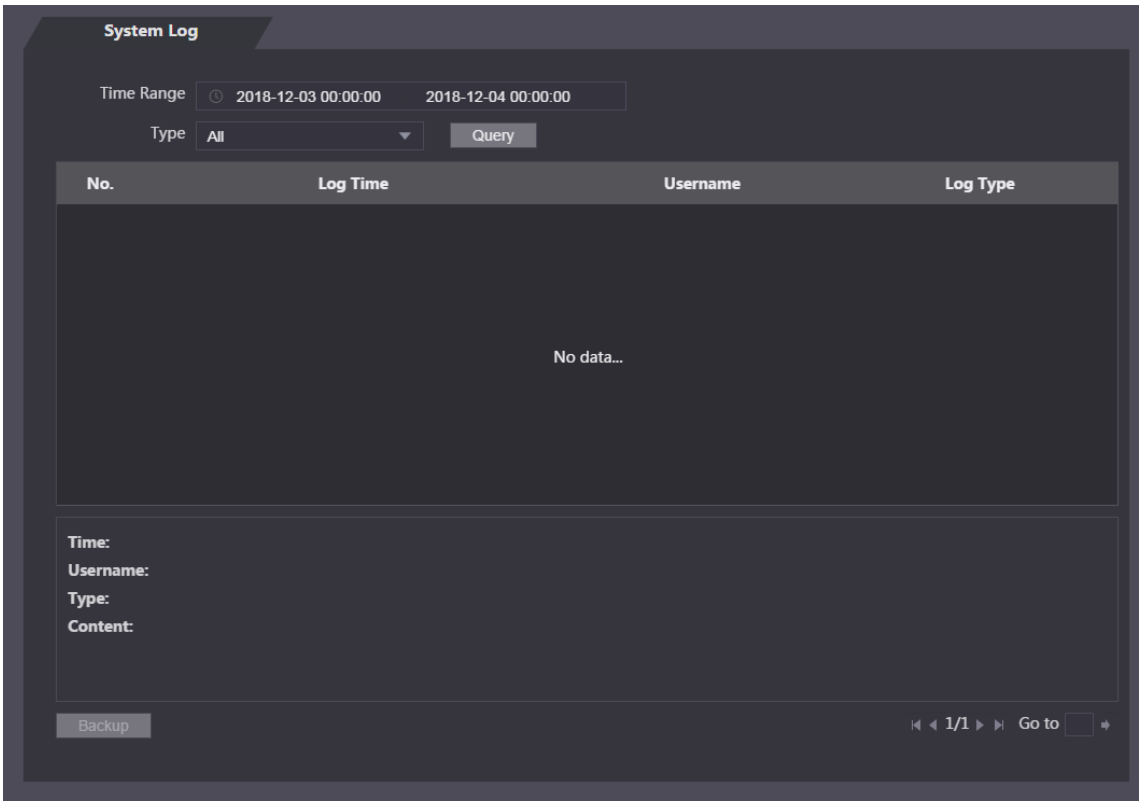
Figure 4-41 Online user



4.17 System Log

You can view and backup the system log on the **System Log** interface.

Figure 4-42 System log



4.17.1 Querying Logs

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

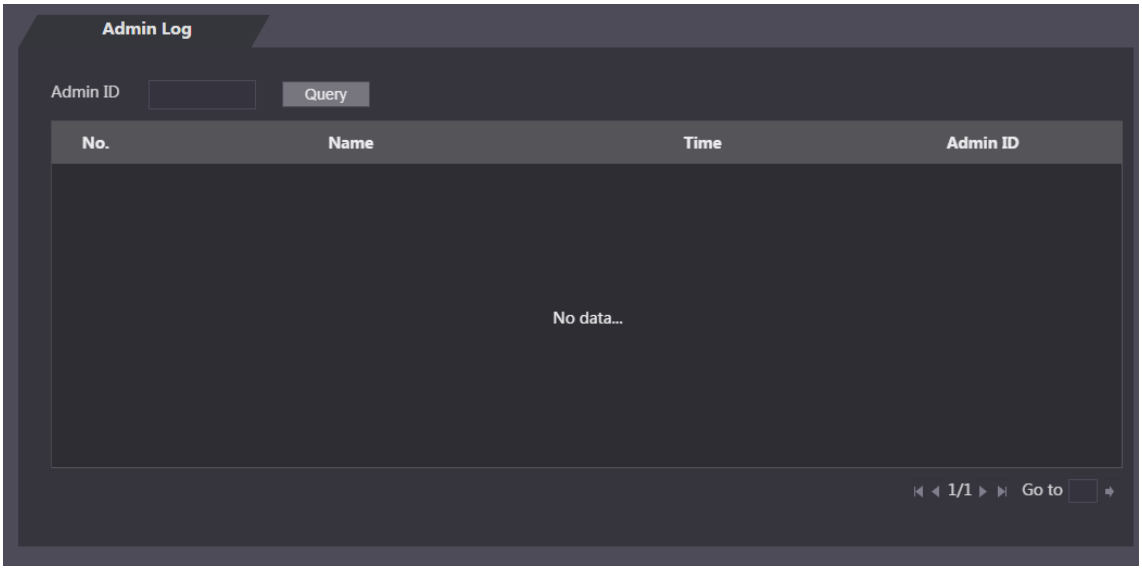
4.17.2 Backing up Logs

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

4.17.3 Admin Log

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

Figure 4-43 Admin log



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

4.18 Exit

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

5 FAQ

1 **The terminal fails to start after power-on.**
Check whether the 12V power supply is correctly connected, and whether the power button is pressed.

2 **Faces cannot be recognized after the terminal powers on.**
Make sure that Face is selected in the unlock mode. See “3.8.2 Unlock”.
Make sure that Face is selected as unlock mode in **Access > Unlock Mode > Group Combination**. See “3.8.2.3 Group Combination”.

3 **There is no output signal when the terminal and the external controller are connected to the Wiegand port.**
Check whether the GND cable of terminal and the external controller are connected.

4 **Configurations cannot be made after the administrator and password are forgotten.**
Delete administrators through the platform, or contact technical support to unlock the terminal remotely.

5 **User information, and face images cannot be imported into the terminal.**
Check whether names of XML files and titles of tables were modified because the system will identify the files through their titles.

6 **When a user’s face is recognized, but other users’ information is displayed.**
Make sure that when importing human faces, there are no other people around. Delete the original face, and import it again.

Appendix 1 Notes of Temperature Monitoring

- Warm up the temperature monitoring unit for more than 20 minutes after power-on to enable the temperature monitoring unit to reach thermal equilibrium.
- Install the temperature monitoring unit in an indoor windless environment, and maintain the indoor ambient temperature at 15°C to 32°C.
- Avoid direct sunlight on the temperature monitoring unit.
- Avoid installing the temperature monitoring unit facing at the light source and glass.
- Keep the temperature monitoring unit away from sources of thermal interference.
- The factors such as sunlight, wind, cold air, and air conditioning cold and warm air will affect the surface temperature of human body, which will cause the temperature deviation between the monitored temperature and the actual temperature.
- Sweating is also a way for the body to automatically cool down and dissipate heat, which will also cause the temperature deviation between the monitored temperature and the actual temperature.
- Maintain the temperature monitoring unit regularly (every 2 weeks). Use a soft dust-free cloth to gently wipe the dust on the surface of the temperature sensor and the distance sensor to keep it clean.

Appendix 2 Notes of Face Recording/Comparison

Before Registration

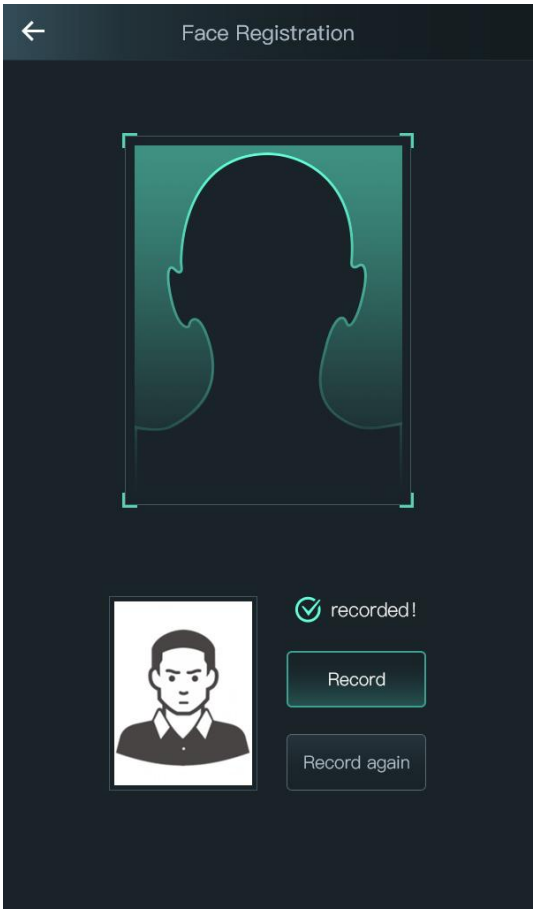
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eye brows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from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

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 2-1 Registration

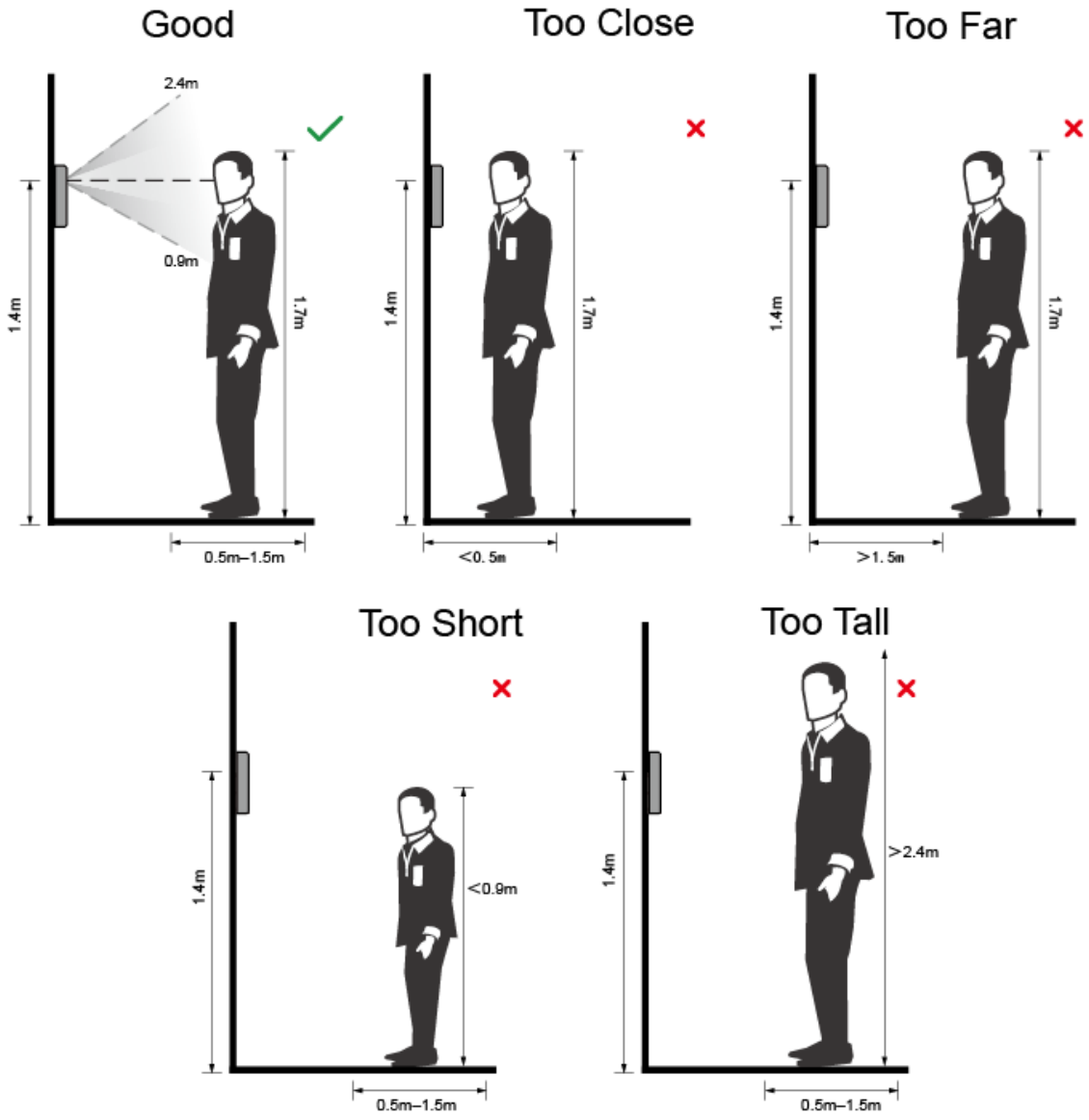


- Do not shake your head or body, or the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

Face Position

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

Appendix Figure 2-2 Appropriate face position

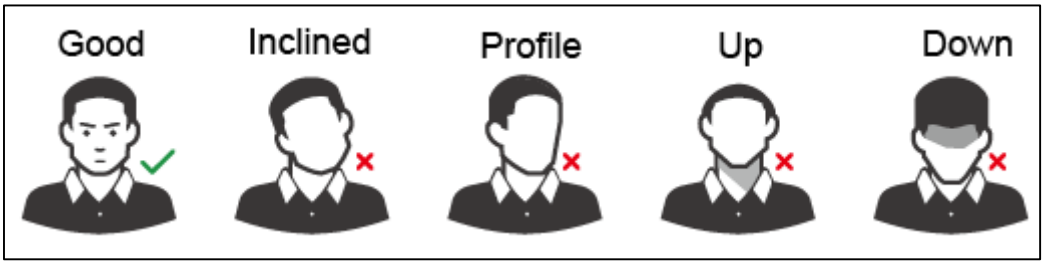


Requirements of Faces

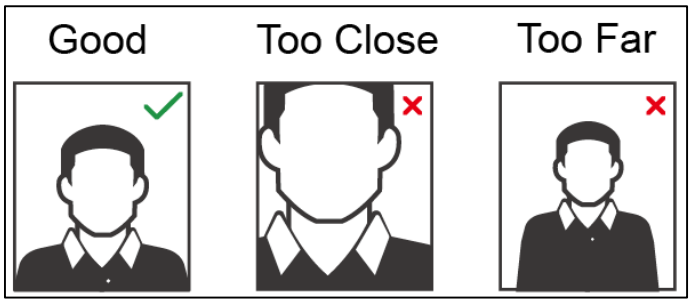
- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during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

too far from the camera.

Appendix Figure 2-3 Head position



Appendix Figure 2-4 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 the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 3 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 device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.