

# **Face Recognition Access Controller**

## **User's Manual**




# Foreword

## General

This manual introduces the installation and basic operations of the Face Recognition Access Controller (hereinafter referred to as "access controller").

## Safety Instructions

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

Signal Words	Meaning
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Revision History

Version	Revision Content	Release Date
V1.0.0	First Release.	May 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 access controller, hazard prevention, and prevention of property damage. Read these contents carefully before using the access controller, comply with them when using, and keep them well for future reference.

## Operation Requirement

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

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>II</b>
<b>1 Overview</b> .....	<b>1</b>
1.1 Introduction .....	1
1.2 Features .....	1
1.3 Application.....	1
1.4 Dimension and Component .....	2
<b>2 Connection and Installation</b> .....	<b>3</b>
2.1 Cable Connections.....	3
2.2 Installation Notes.....	4
2.3 Installation .....	6
<b>3 System Operations</b> .....	<b>9</b>
3.1 Basic Configuration Procedure .....	9
3.2 Common Icons .....	9
3.3 Initialization .....	9
3.4 Standby Interface .....	10
3.5 Main Menu .....	11
3.6 Unlocking Methods .....	13
3.6.1 Cards .....	13
3.6.2 Face .....	13
3.6.3 User Password .....	13
3.6.4 Administrator Password.....	14
3.7 User Management .....	14
3.7.1 Adding New Users .....	14
3.7.2 Viewing User information.....	16
3.8 Access Management.....	16
3.8.1 Period Management .....	16
3.8.2 Unlock .....	18
3.8.3 Alarm Configuration .....	21
3.8.4 Door Status.....	22
3.8.5 Lock Holding Time .....	22
3.9 Network Communication.....	22
3.9.1 IP Address.....	22
3.9.2 Serial Port Settings .....	24
3.9.3 Wiegand Configuration .....	24
3.10 System .....	25
3.10.1 Time .....	25
3.10.2 Face Parameter .....	26
3.10.3 Image Mode.....	28
3.10.4 Fill Light Mode Setting.....	28
3.10.5 Fill Light Brightness Setting.....	28
3.10.6 Volume Adjustment.....	28
3.10.7 IR Light Brightness Adjustment .....	28
3.10.8 Restore to Factory Settings .....	29

3.10.9 Reboot .....	29
3.11 USB .....	29
3.11.1 USB Export .....	29
3.11.2 USB Import.....	30
3.11.3 USB Update .....	31
3.12 Features .....	31
3.12.1 Privacy Setting.....	33
3.12.2 Result Feedback.....	34
3.13 Record.....	36
3.14 Auto Test.....	37
3.15 System Info .....	38
<b>4 Web Operations .....</b>	<b>39</b>
4.1 Initialization .....	39
4.2 Login.....	41
4.3 Resetting the Password .....	41
4.4 Alarm Linkage .....	43
4.4.1 Setting Alarm Linkage.....	43
4.4.2 Alarm Log.....	45
4.5 Data Capacity.....	45
4.6 Video Setting.....	46
4.6.1 Data Rate.....	46
4.6.2 Image .....	47
4.6.3 Exposure.....	48
4.6.4 Motion Detection.....	49
4.6.5 Volume Setting.....	50
4.6.6 Image Mode .....	51
4.7 Face Detect.....	51
4.8 Network Setting.....	54
4.8.1 TCP/IP .....	54
4.8.2 Port .....	55
4.8.3 Register.....	56
4.8.4 P2P .....	56
4.9 Date Setting .....	57
4.10 Safety Management.....	58
4.10.1 IP Authority.....	58
4.10.2 Systems .....	59
4.11 User Management.....	60
4.11.1 Adding Users.....	60
4.11.2 Modifying User Information.....	60
4.11.3 Onvif User .....	60
4.12 Maintenance.....	61
4.13 Configuration Management .....	61
4.13.1 Config Mgmt. ....	62
4.13.2 Features.....	62
4.13.3 Wiegand Serial Port Setting .....	62
4.14 Upgrade .....	63
4.15 Version Information .....	63

4.16 Online User .....	63
4.17 System Log .....	64
4.17.1 Querying Logs .....	64
4.17.2 Backup Logs .....	65
4.17.3 Admin Log.....	65
4.18 Exit .....	65
<b>5 FAQ .....</b>	<b>66</b>
<b>Appendix 1 Notes of Temperature Monitoring.....</b>	<b>67</b>
<b>Appendix 2 Notes of Face Recording/Comparison .....</b>	<b>68</b>
<b>Appendix 3 Cybersecurity Recommendations .....</b>	<b>71</b>

# 1 Overview

## 1.1 Introduction

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

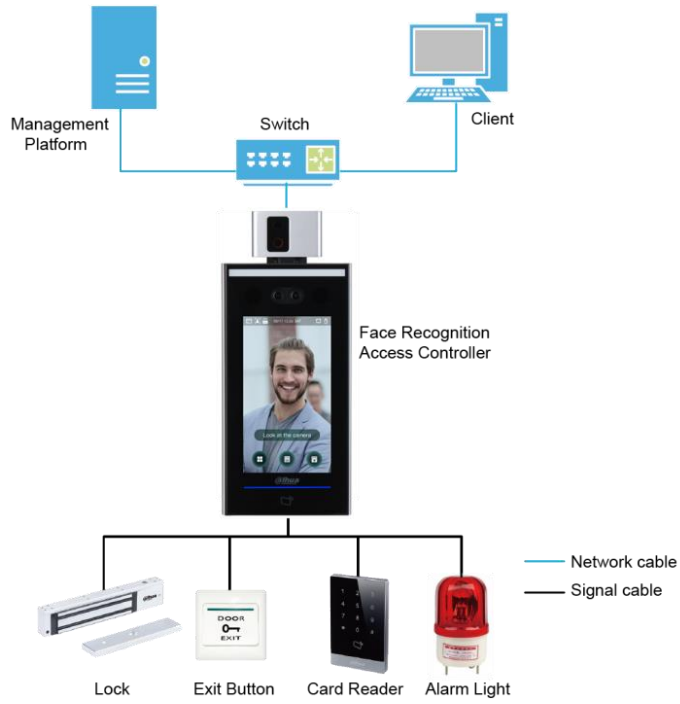
## 1.2 Features

- LCD display, the resolution of 7-inch access controller is 1024 × 600.
- Support face unlock, IC card 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 access controller 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, tamper alarm, intrusion alarm, door contact timeout alarm, and illegal card exceeding threshold alarm
- Support general 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 access controller 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 1-1 Dimensions and components (mm [inch])

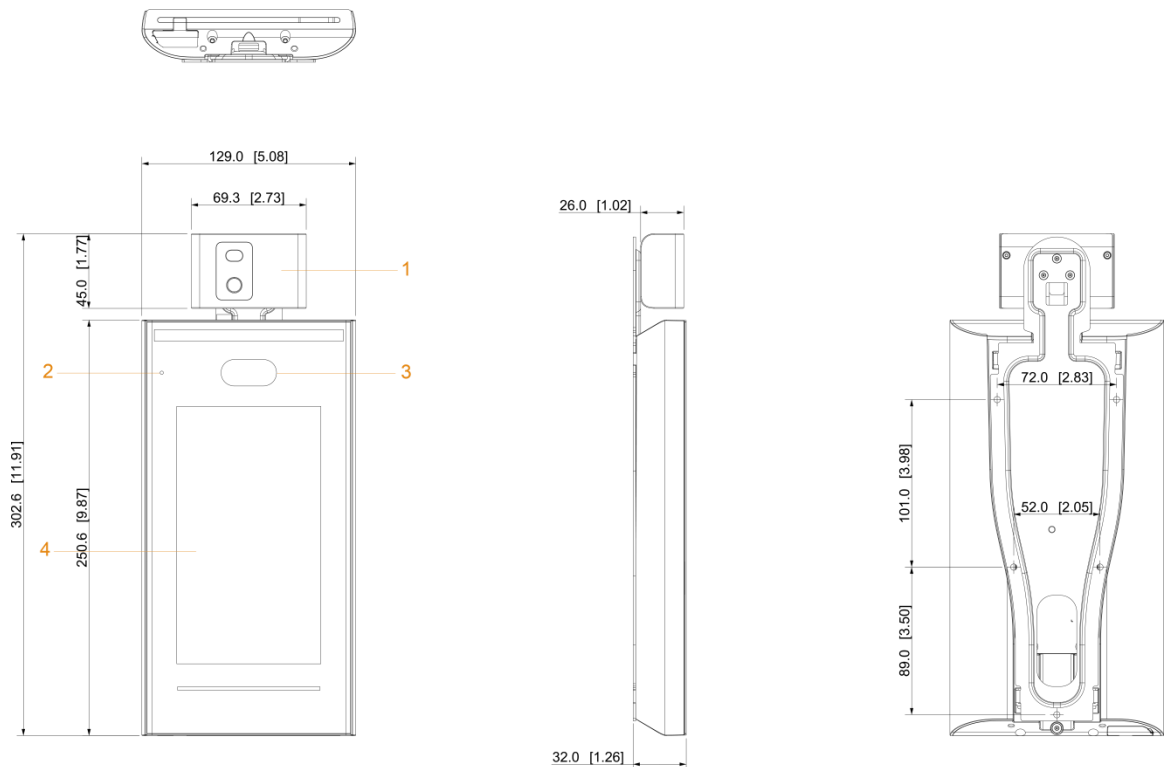


Table 1-1 Component description (3)

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





# 2 Connection and Installation

## 2.1 Cable Connections

The access controller needs to be connected to devices like sirens, readers, and door contacts. For cable connection, see Table 2-1.

Table 2-1 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).  <ul style="list-style-type: none"> <li>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.</li> <li>Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.</li> </ul>
Purple	A	RS-485 positive electrode input (connected to external card reader)/output (connected to controller, or connected to door control security module).  <ul style="list-style-type: none"> <li>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.</li> <li>Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.</li> </ul>	
CON2	White and red	ALARM1_NO	Alarm 1 normally open output port.
	White and orange	ALARM1_COM	Alarm 1 common output port.

Port	Cable color	Cable name	Description
	White and blue	ALARM2_NO	Alarm 2 normally open output port.
	White and gray	ALARM2_COM	Alarm 2 common output port.
	White and green	GND	Connected to the common GND port.
	White Brown	ALARM1	Alarm 1 input port.
	White and yellow	GND	Connected to the common GND port.
	White and purple	ALARM2	Alarm 2 input port.
CON3	Black and red	RX	RS-232 receiving port.
	Black and orange	TX	RS-232 sending portk.
	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 brown	DOOR1_COM	Lock control common port.
	Black and yellow	DOOR1_NO	Lock control normally open port.
	Black and purple	DOOR1_NC	Lock control normally closed port.

## 2.2 Installation Notes



- If there is light source 0.5 meters away from the access controller, the minimum illumination should be no less than 100 Lux.
- It is recommended that the access controller 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 2-1 Ambient illumination requirement



Candle: 10Lux



Light bulb: 100Lux–850Lux



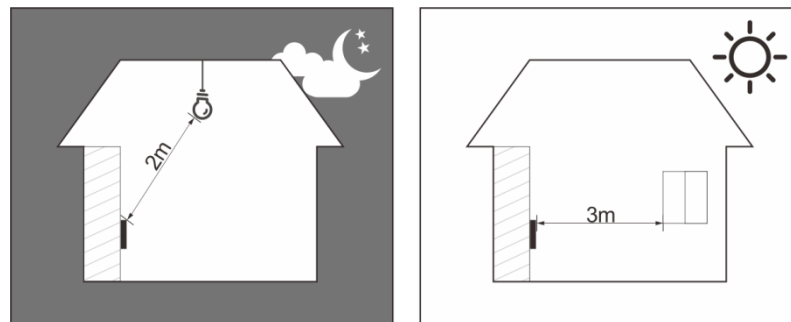
Sunlight:  $\geq 1200$ Lux

## 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 access controller, 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.

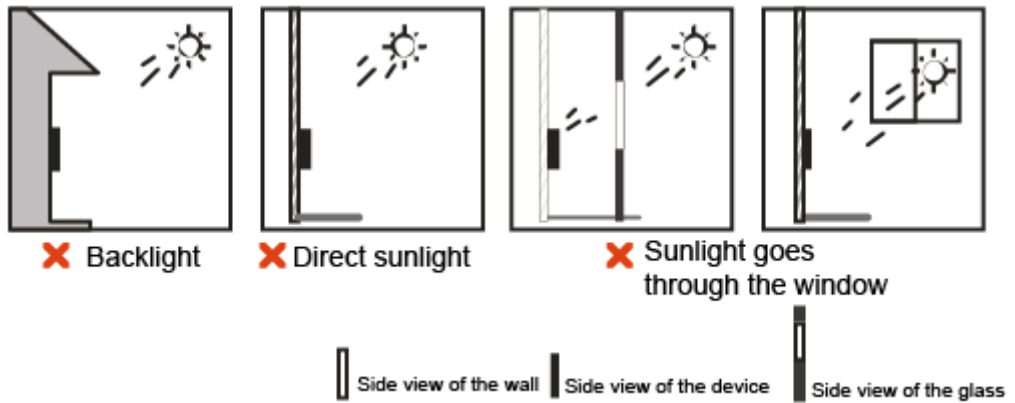
## Places Recommended

Figure 2-2 Places recommended



## Places Not Recommended

Figure 2-3 Places not recommended



## 2.3 Installation

Make sure that the distance between the camera and ground is 1.4 meters.

Figure 2-4 Installation height

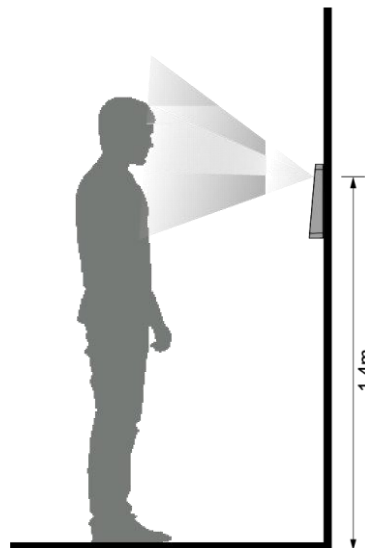
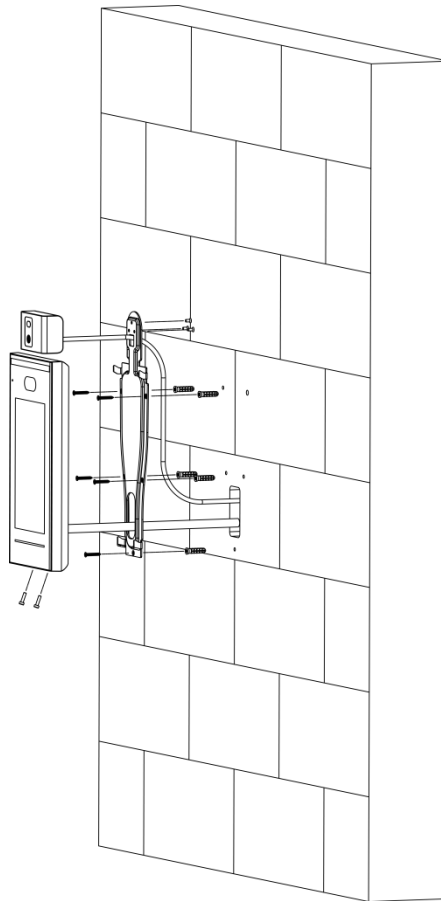


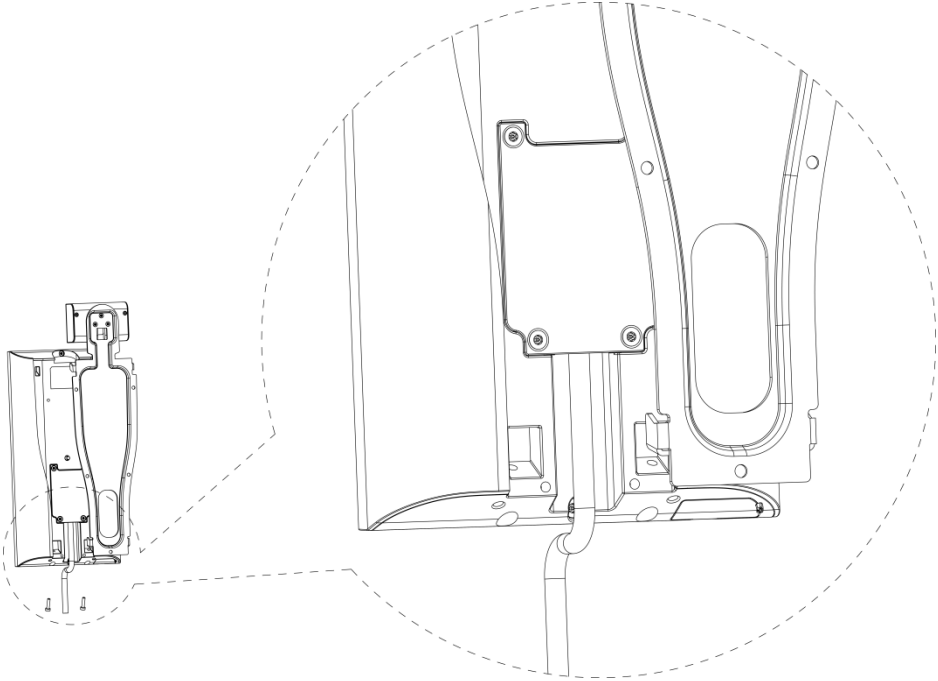
Figure 2-5 Installation diagram



## Installation Procedure

- Step 1 Fix the temperature monitoring unit to the bracket with 3 screws.
- Step 2 Drill six holes (five bracket installation holes and one cable entry) in the wall according to holes in the bracket.
- Step 3 Fix the bracket on the wall by installing the expansion screws into the six bracket installation holes.
- Step 4 Connect cables for access controller. See "2.1 Cable Connections."
- Step 5 Hang the access controller on the bracket hook.
- Step 6 Tighten the screws at the bottom of the access controller.
- Step 7 Apply silicon sealant to the cable outlet of the access controller.

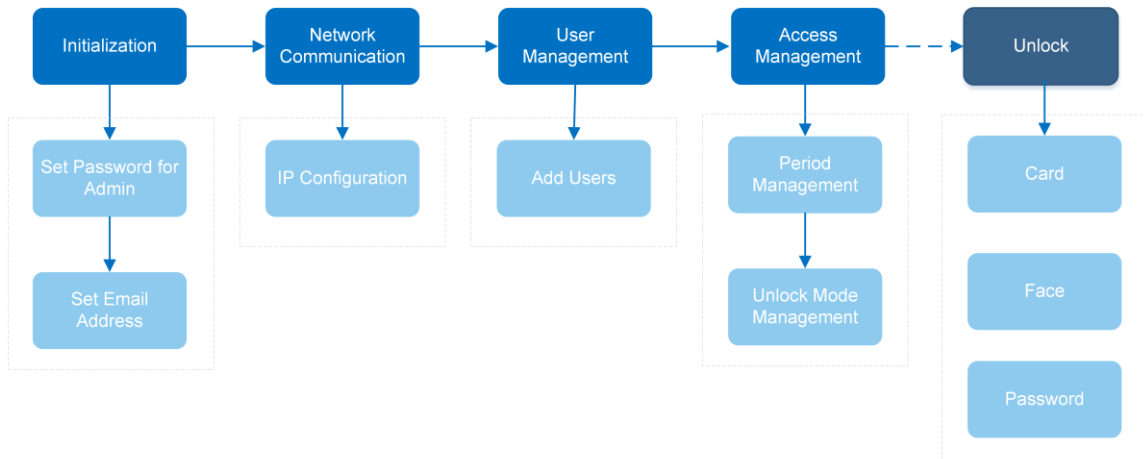
Figure 2-6 Applying silicon sealant



# 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.
	Enable.
	Disable.

## 3.3 Initialization

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

Figure 3-2 Initialization

The screenshot shows a dark-themed web interface for device initialization. At the top, the text 'Device Initialization' is centered. Below this, there are four input fields arranged vertically. The first field is labeled 'Admin' and contains the text 'admin'. The second field is labeled 'PWD' and is empty. The third field is labeled 'PWD Confirm' and is empty. The fourth field is labeled 'E-mail' and is empty. At the bottom of the form, there are two buttons: 'Yes' on the left and 'Clear' on the right.



- 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 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, passwords and cards. See Table 3-2.



- If there are no operations in 30 seconds, the access controller will go to the standby mode.
- The standby interface might vary with versions, and the actual interface shall prevail.



Figure 3-3 Homepage

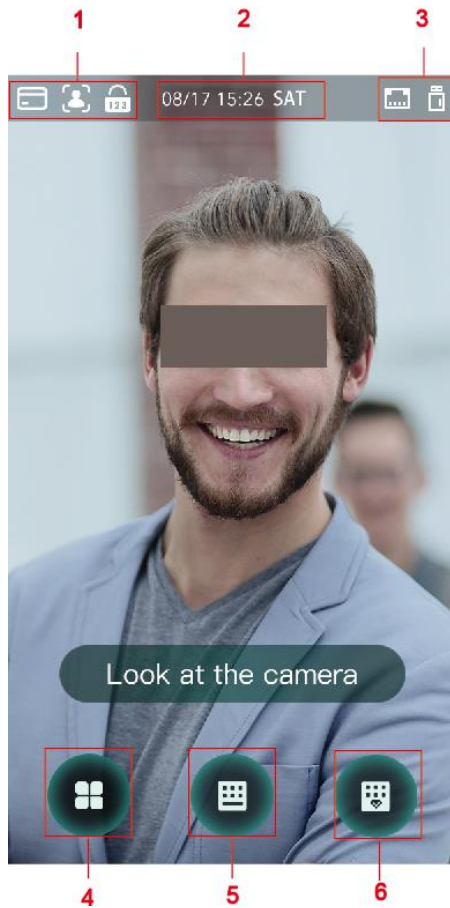





Table 3-2 Homepage description

No.	Description
1	Unlock methods: Card, face and password.  When card, face, and password are all set as unlock mode, the password icon will not be displayed at the top left corner of the access controller.
2	Date & Time. Displays the current date and time.
3	Display the network status and USB status.
4	Main menu icon.  Only users with the administrator permission can enter the main menu.
5	Password unlock icon.
6	Administrator password unlock icon.

## 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.

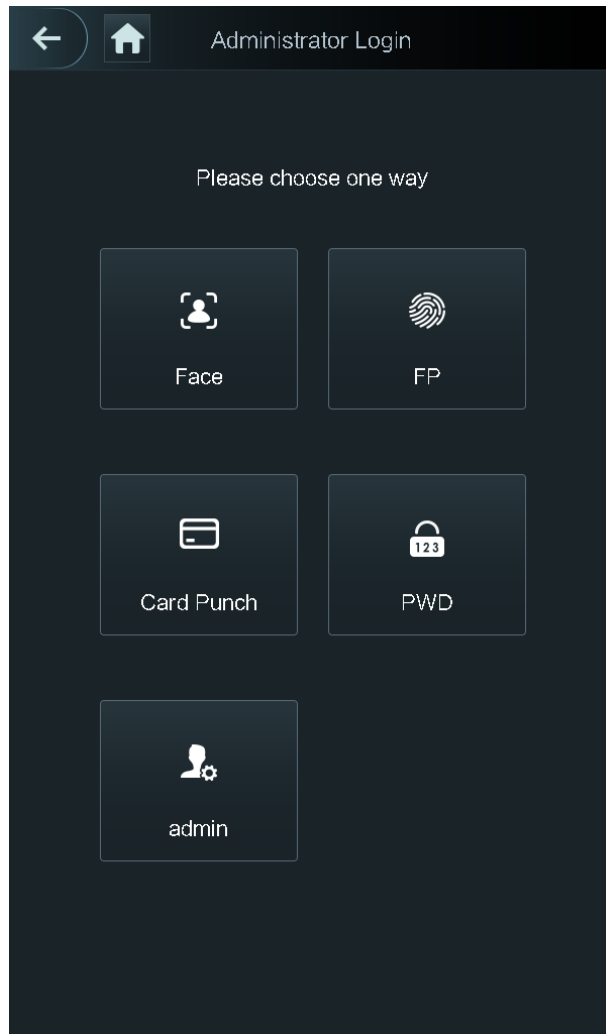
**Step 1** Tap  on the standby interface.

**Step 2** Select a main menu entering method.



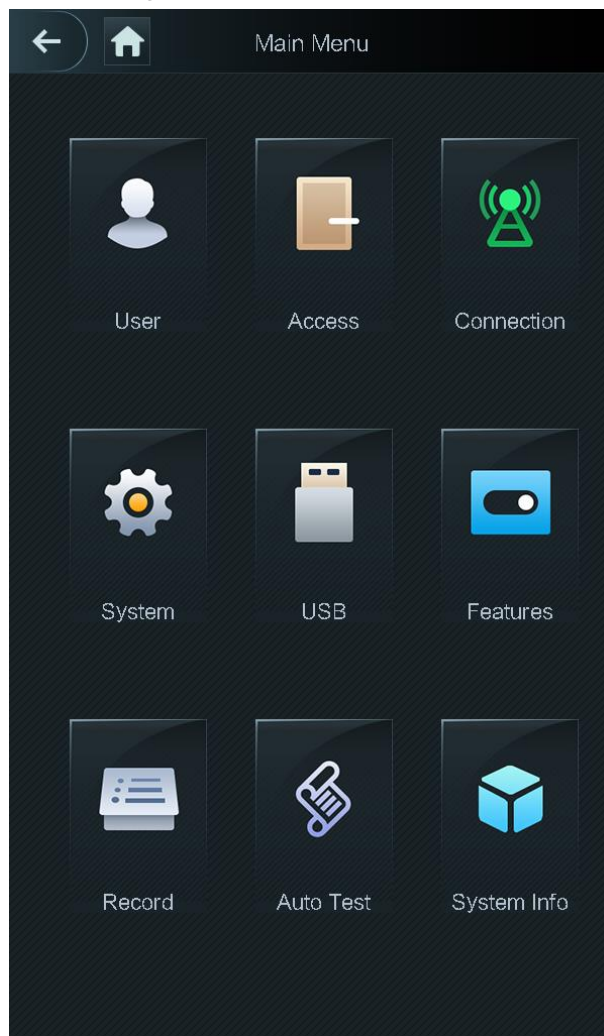
Different modes support different unlock methods, and the actual interface shall prevail.

Figure 3-4 Administrator login



The main menu interface is displayed.

Figure 3-5 Main menu



## 3.6 Unlocking Methods

You can unlock the door through faces, passwords, and cards.

### 3.6.1 Cards


Put the card at the card swiping area to unlock the door.

### 3.6.2 Face

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

### 3.6.3 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 .
- The door is unlocked.

### 3.6.4 Administrator Password

Enter the administrator password, and then you can unlock the door. There is only one administrator password for one access controller. 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 "3.8.1.5 NC Period."

- Step 1 Tap  on the homepage.
- Step 2 Tap **Please Enter Administrator PWD.**
- Step 3 Enter the administrator password, and then tap .
- The door is unlocked.

## 3.7 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 user IDs, names, face images, cards, passwords, selecting user levels, and more.



The following figures are for reference only, and the actual interface shall prevail.



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


Figure 3-6 New User Info




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 the access controller will take a picture of the new user's face automatically.
Card	<p>You can register five cards at most for each user. On the card registration interface, enter your card number or swipe your card, and then the card information will be read by the access controller.</p> <p>You can enable the <b>Duress Card</b> function on the card registration interface. Alarms will be triggered if a duress card is used to unlock the door.</p> <p> Only certain models support card unlock.</p>
PWD	<p>The door unlocking password. The maximum length of the password is 8 digits.</p> <p> If the access controller is without touch screen, you need to connect the access controller to a peripheral card reader. There are buttons on the card reader.</p>

Parameter	Description
User Level	<p>You can select a user level for new users. There are two options:</p> <ul style="list-style-type: none"> <li>• User: Users only have door unlock permission.</li> <li>• Admin: Administrators can unlock the door and also have parameter configuration permission.</li> </ul>  <p>No matter whether there is an administrator in the access controller, administrator identity authentication is needed.</p>
Period	You can set a period in which the user can unlock the door.
Holiday Plan	You can set a holiday plan in which the user can unlock the door.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Level	<p>There are six levels:</p> <ul style="list-style-type: none"> <li>• General: General users can unlock the door normally.</li> <li>• Blacklist: When users in the blacklist unlock the door, service personnel will get a prompt.</li> <li>• Guest: Guests are allowed to unlock the door certain times. Once they exceed the maximum times, they cannot unlock the door again.</li> <li>• Patrol: Paroling users can get their attendance tracked, but they have no unlock permission.</li> <li>• VIP: When VIP unlocks the door, service personnel will get a prompt.</li> <li>• Special: When special people unlock the door, there will be a delay of 5 seconds before the door is closed.</li> </ul>
Use Time	When the user level is Guest, you can set the maximum number of times that the user 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 on periods, door normally closed periods, and remote verification periods.


### 3.8.1.1 Period Config

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

### 3.8.1.2 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 is normally open in 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 is normally closed in 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

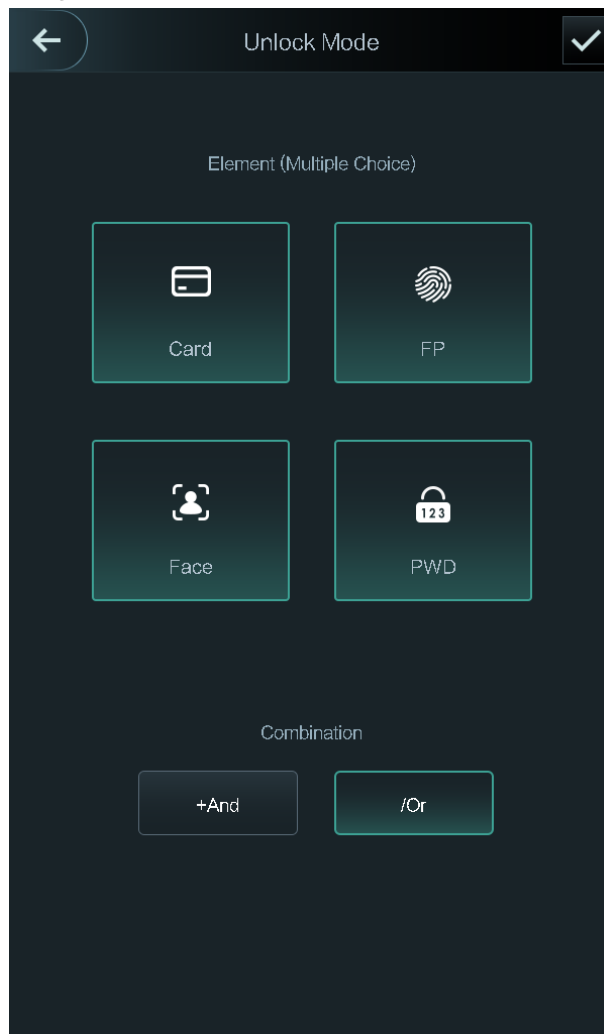
There are three unlock modes: unlock mode, unlock by period, and group combination. Unlock modes vary with controller access models, and the actual controller access shall prevail.

### 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 unlock mode(s).



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

Step 3 Select a combination mode.



- **+ And** means "and". For example, if you select card + PWD, it means, to unlock the door, you need to swipe your card first, and then enter 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 password.

Step 4 Tap  to save the settings.



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

**Step 5** Enable the Unlock Mode.

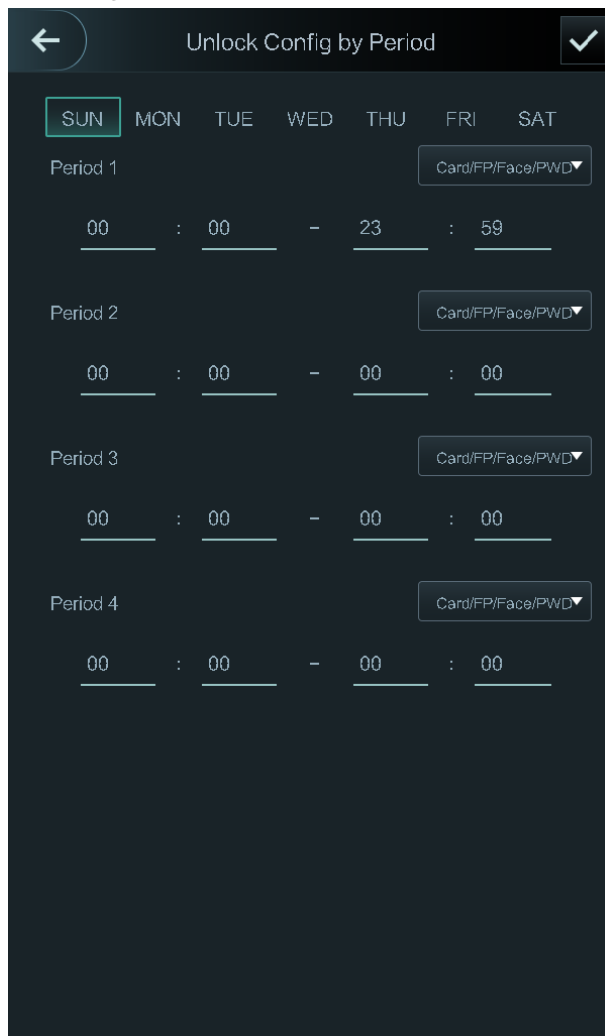
-  means enabled.
-  means not enabled.

### 3.8.2.2 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 cards; and in period 2, doors can only be locked through faces.

**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 a unlock mode.

**Step 3** Tap  to save the settings.

The **Unlock Mode** interface is displayed.

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

-  means enabled.

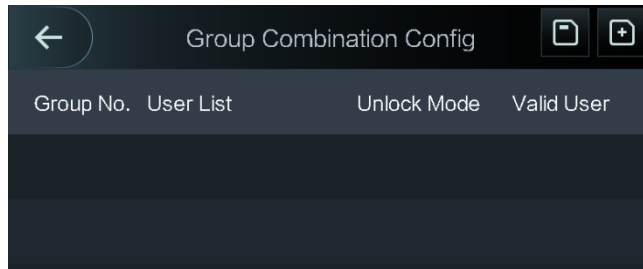
-  means not enabled.

### 3.8.2.3 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

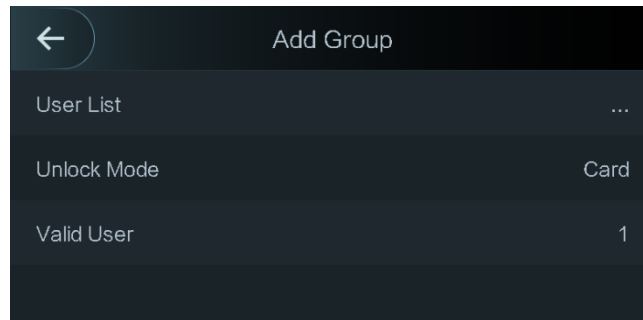






Table 3-4 Group parameter

Parameter	Description
User List	<p>Add users to the newly created group.</p> <ol style="list-style-type: none"> <li>1. Tap <b>User List</b>. The <b>User List</b> interface is displayed.</li> <li>2. Tap , and then enter a user ID.</li> <li>3. Tap  to save the settings.</li> </ol>
Unlock Mode	There are three options: <b>Card</b> , <b>PWD</b> and <b>Face</b> .
Valid User	<p>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.</p> <ul style="list-style-type: none"> <li>• Valid users cannot exceed the total number of users in a group.</li> <li>• If valid users equal total user numbers in a group, doors can only be unlocked by all the users in the group.</li> <li>• 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.</li> </ul>

**Step 3** Tap  to go back to the previous interface.

**Step 4** Tap  to save the settings.

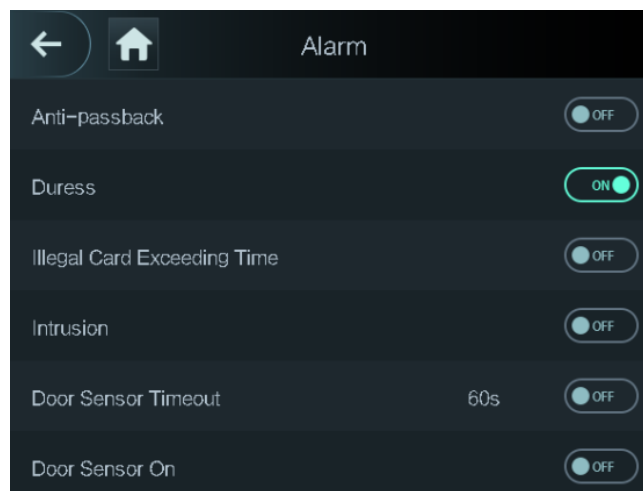
**Step 5** Enable the **Group Combination**.

-  means enabled.
-  means not enabled.

### 3.8.3 Alarm Configuration

Administrators can manage visitors' unlock permission through alarm configuration. Select **Access > Alarm**. The Alarm interface is displayed.

Figure 3-11 Alarm





-  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. <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>
Duress	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Illegal Card Exceeding	After an unauthorized card is used to unlock the door more than 5 times in 50 seconds, an alarm will be triggered.

Parameter	Description
Time	
Intrusion	An intrusion alarm will be triggered if a door is unlocked without having the door contact released.
Door Sensor Timeout	A timeout alarm will be triggered if the time that a user takes to unlock the door exceeds the Door Sensor Timeout time. The Door Sensor Timeout time range is 1–9999 seconds.
Door Sensor On	Only when the <b>Door Sensor On</b> is enabled can the intrusion alarm and door sensor timeout alarm be triggered.

### 3.8.4 Door Status

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

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

### 3.8.5 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 access controller 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 access controller to make it be connected to the network. See Figure 3-12 and Table 3-6.

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 access controllers of have dual NICs. The default management address for 1000M network port is 192.168.1.108, and for 100M network port is 192.168.2.108.

### 3.9.1.2 Active Register

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



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

For active register parameter, see Table 3-7.

Table 3-7 Active register

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

### 3.9.1.3 Wi-Fi

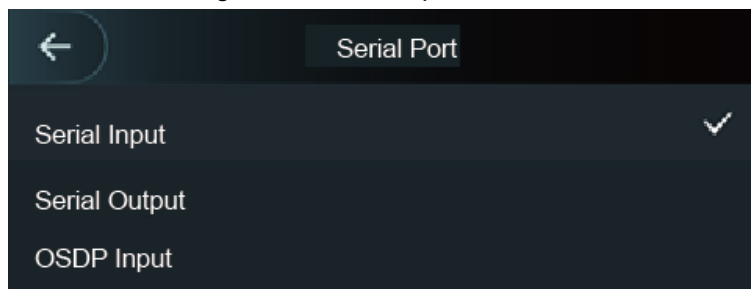
You can connect the access controller to the network through Wi-Fi if the access controller has Wi-Fi function.

## 3.9.2 Serial Port Settings

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

Select **Connection > Serial Port**, and then the **Serial Port** interface is displayed.

Figure 3-13 Serial port



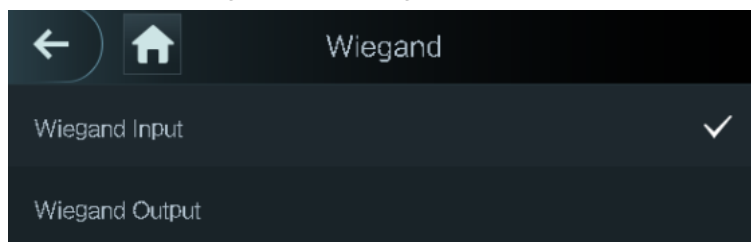
- Select **Serial Input** when external devices that are with card reading and writing functions are connected to the access controller. **Serial Input** is selected to enable access card information to be sent to the access controller and the management platform.
- For access controllers with face recognition, card reading and writing functions, if you select **Serial Output**, access controller will send lock/unlock information to the access controller. 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 access controller. The access controller can send card information to the management platform.

## 3.9.3 Wiegand Configuration

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

Select **Connection > Wiegand**, and then the Wiegand interface is displayed.

Figure 3-14 Wiegand



- Select **Wiegand Input** when an external card swipe mechanism is connected to the access controller.

- Select **Wiegand Output** when the access controller works as a reader that can be connected to the controller. See Table 3-8.

Table 3-8 Wiegand output

Parameter	Description
Wiegand Output Type	<p>The <b>Wiegand Output Type</b> determines the card number or the digit of the number that can be recognized by the access controller.</p> <ul style="list-style-type: none"> <li>• Wiegand26, three bytes, six digits.</li> <li>• Wiegand34, four bytes, eight digits.</li> <li>• Wiegand66, eight bytes, sixteen digits.</li> </ul>
Pulse Width	You can set pulse width and pulse interval.
Pulse Interval	
Output Data Type	<p>You can select the types of output data.</p> <ul style="list-style-type: none"> <li>• User ID: If User ID is selected, and then user ID will be output.</li> <li>• Card No.: If Card No. is selected, and then card number will be output.</li> </ul>

## 3.10 System

### 3.10.1 Time

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



- When you select **Network Time Protocol (NTP)**, you need to enable the **NTP Check function** first. **Server IP Address:** enter the IP address of the time server, time of the access controller 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	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.
Recognition Interval	When a person who has the access permission stands in front of the access controller and gets the face recognized, the controller will prompt that face recognition succeeded. The prompt interval is the recognition interval.
Invalid Face Prompt Interval	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. The larger the value is, the more difficult face images can unlock the door. The recommended value range is above 80.
Temperature Monitoring	<p>Set whether to enable the body temperature monitoring.</p> <ul style="list-style-type: none"> <li>● Temp Unit: Select a temperature unit.</li> <li>● Temp Rect: Set whether to display the temperature monitoring box or not.</li> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> </ul> <p> Only the access controller with a temperature monitoring unit supports this parameter.</p>

Name	Description
Mask Mode	<ul style="list-style-type: none"> <li>• No detect: Mask is not detected during face recognition.</li> <li>• 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.</li> <li>• 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.</li> </ul>

### 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 is normally off; otherwise, the fill light will be on.
- NO: The fill light is normally on.
- NC: The fill light is normally closed.

### 3.10.5 Fill Light Brightness Setting

You can select fill light brightness according to your needs.

### 3.10.6 Volume Adjustment

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 unclearer the images will be.

## 3.10.8 Restore to Factory Settings



- Data will be lost if you restore the access controller to the factory settings.
- After the access controller 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 access controller to the factory settings with all user information and device information deleted.
- You can select to restore the access controller to the factory settings with user information and device information retained.

## 3.10.9 Reboot

Select **Setting > Reboot**, tap **Reboot**, and the access controller 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 access controller to the USB before using USB to import information to another access controller.
- USB can also be used to update the program.

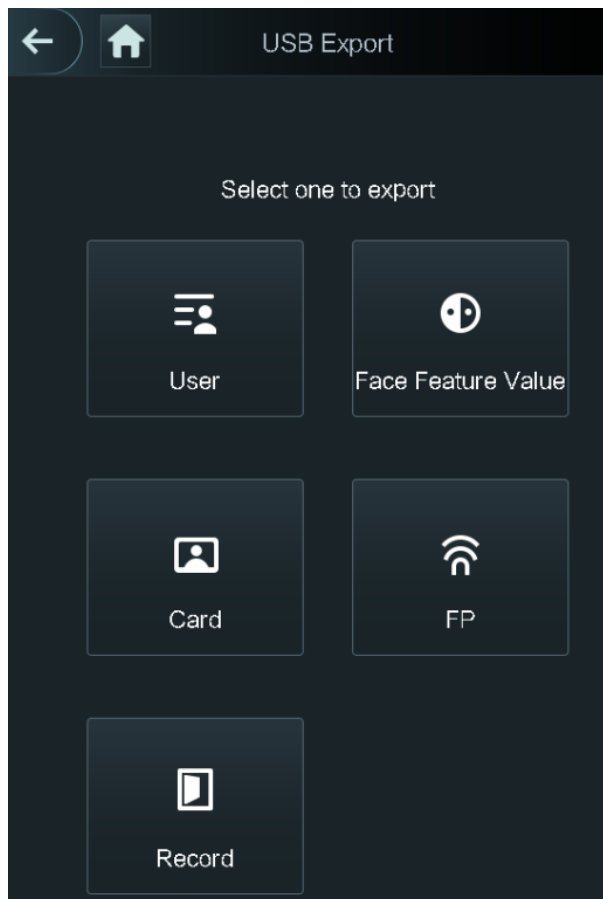
### 3.11.1 USB Export

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

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

The **USB Export** interface is displayed.

Figure 3-16 USB export



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

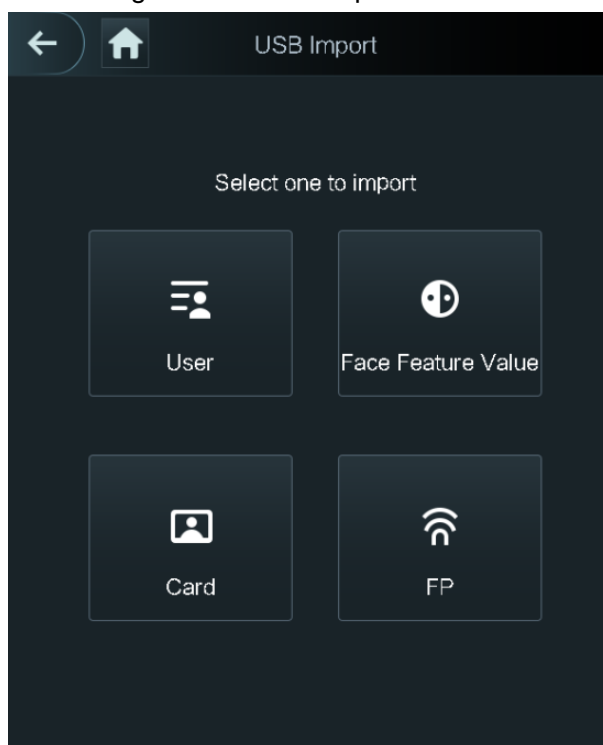
**Step 3** Tap **OK**.  
Data exported will be saved in the USB.

### 3.11.2 USB Import

Only data in the USB that was exported from one access controller can be imported into another access controller.

**Step 1** Select **USB > USB Import**.  
The **USB Import** interface is displayed.

Figure 3-17 USB Import



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

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

Step 3 Tap **OK**.

Data in the USB flash drive will be imported into the access controller.

### 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 flash drive.



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

Step 2 Select **USB > USB Update**.

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

Step 3 Tap **OK**.

The update starts, and the access controller reboots after the update is finished.

## 3.12 Features

You can do settings about privacies, card number reverse, security module, door sensor type, and result feedback. For details of the functions mentioned, see Figure 3-18 and Table 3-10.

Figure 3-18 Features

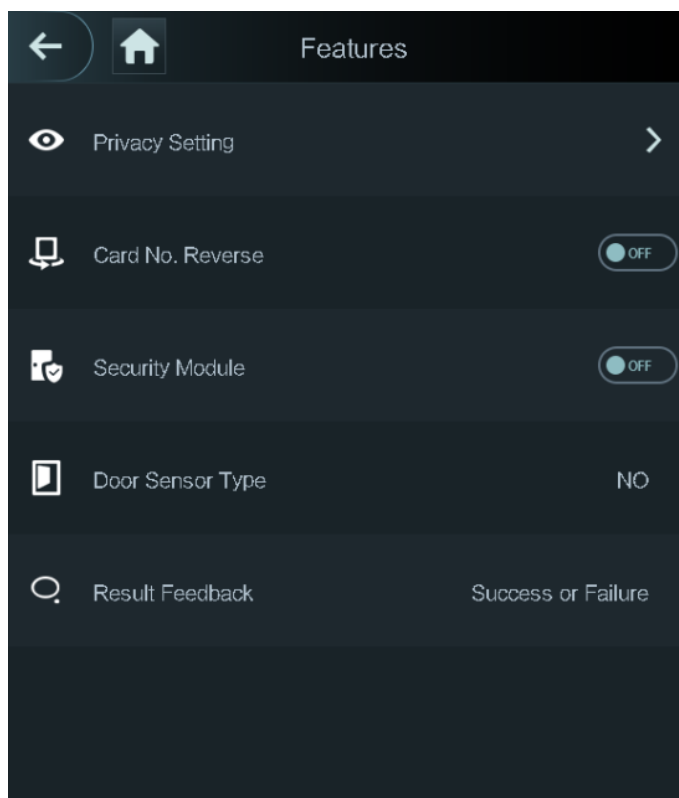


Table 3-10 Feature description

Parameter	Description
Privacy Setting	See "3.12.1 Privacy Setting" 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	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Once the security module is enabled, the exit button, lock control and firefighting linkage will be invalid.</li> </ul>
Door Sensor Type	There are two options: <b>NO</b> and <b>NC</b> .
Result Feedback	Displays whether the unlock succeeded or failed.

### 3.12.1 Privacy Setting

Figure 3-19 Privacy setting

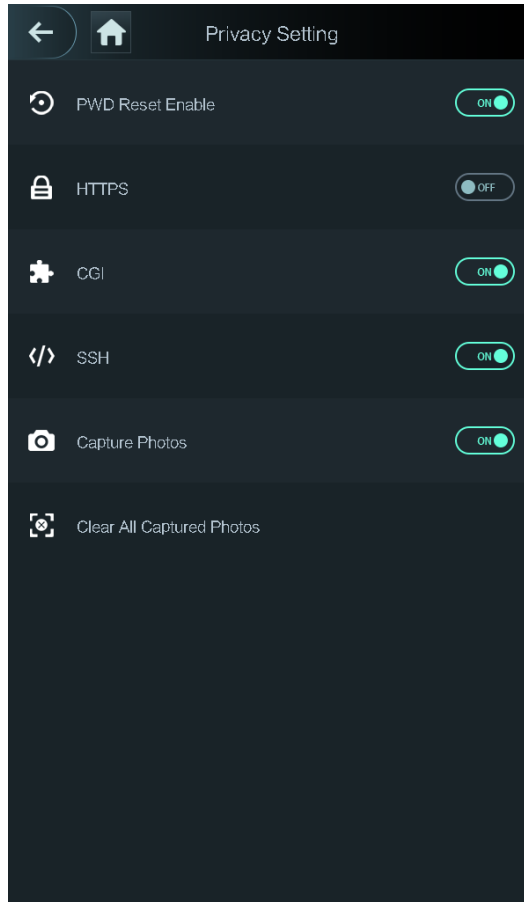



Table 3-11 Features

Parameter	Description
PWD Reset Enable	If the <b>PWD Reset Enable</b> 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.
Capture photo	If you select ON, when a user unlocks the door, the user's photo will be

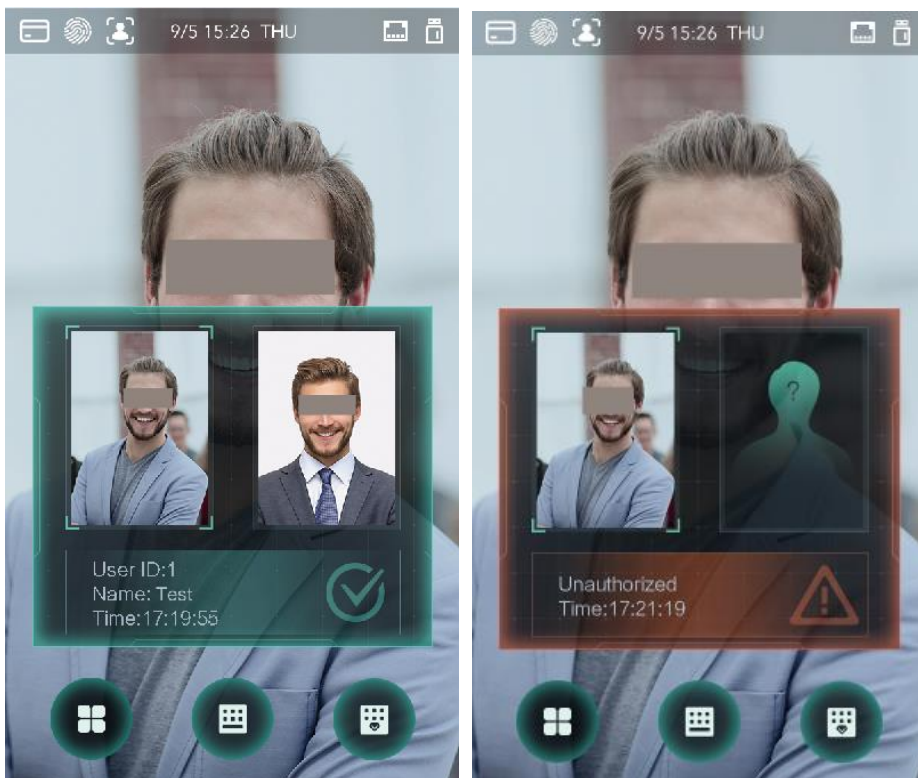
Parameter	Description
	automatically taken. This function is ON by default.
Clear all captured photos	Tap the icon, and you can delete all captured photos.

### 3.12.2 Result Feedback

You can select a result feedback mode as needed.

#### Mode 1

Figure 3-20 Mode 1





## Mode 2

Figure 3-21 Mode 2



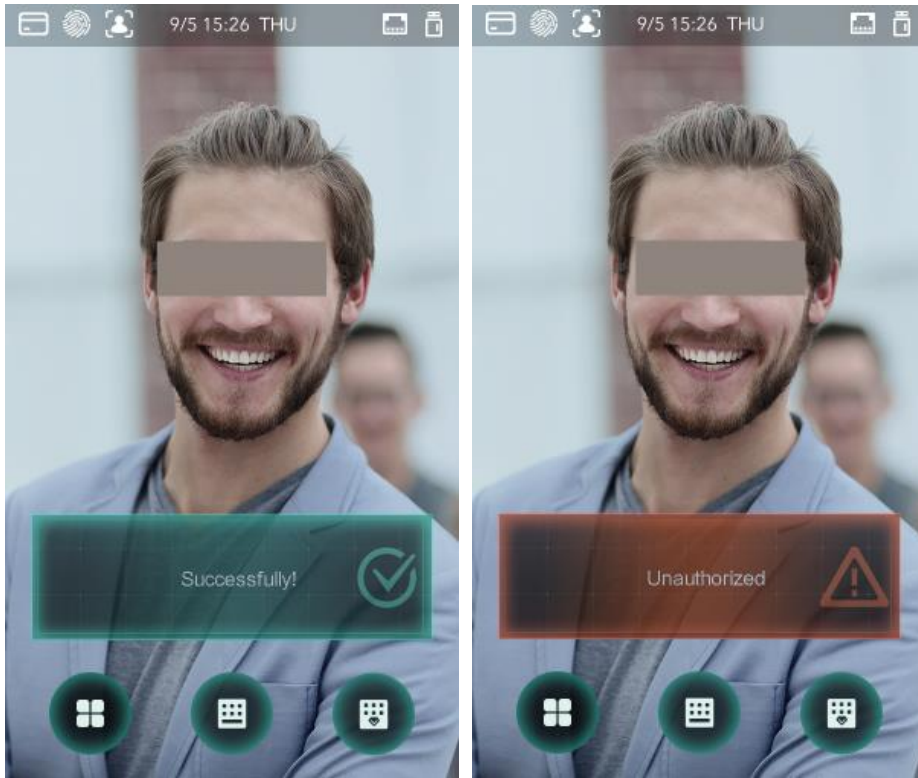
## Mode 3

Figure 3-22 Mode 3



## Mode 4

Figure 3-23 Mode 4



### 3.13 Record

You can query all unlocking records.

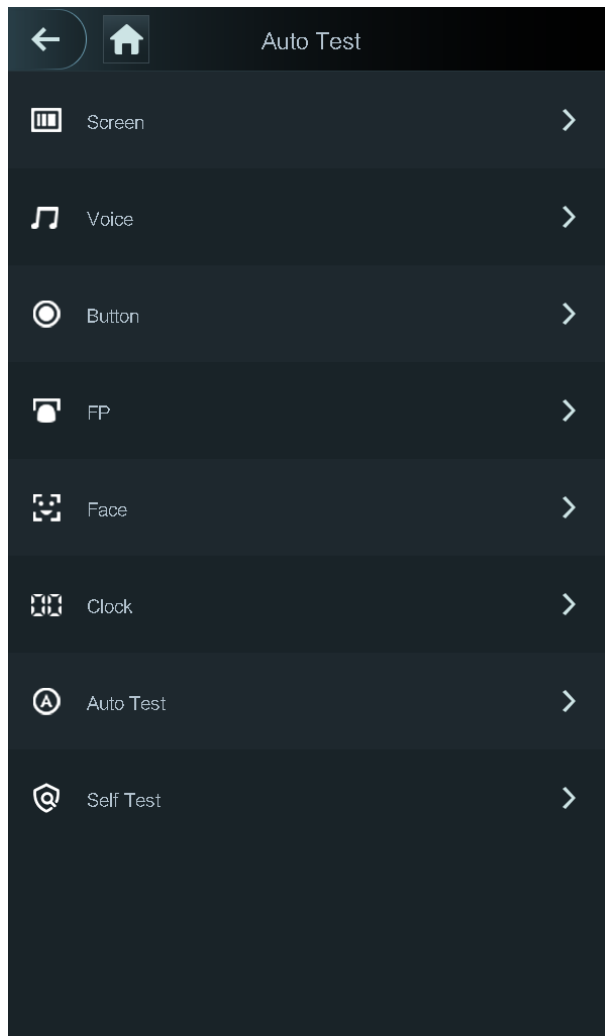
Figure 3-24 Search punch records

User ID.	Name	Time	Status	Verify Mode
		09-05 17:21	Failed	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face

### 3.14 Auto Test

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

Figure 3-25 Auto test



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

## 3.15 System Info

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

# 4 Web Operations

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

## 4.1 Initialization

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

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



- 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 access controllers of have dual NICs. The default IP address for 1000M network port is 192.168.1.108, and for 100M network port is 192.168.2.108.

Figure 4-1 Initialization

Boot Wizard

① Device Initialization      ② Auto Check

Username admin

New Password

Low Medium High

Confirm Password

Password shall be at least 8 digits, and shall at least include two types, including number, letter and common character

Bind Email

(It will be used to reset password. Please fill in or complete it timely)

Next

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

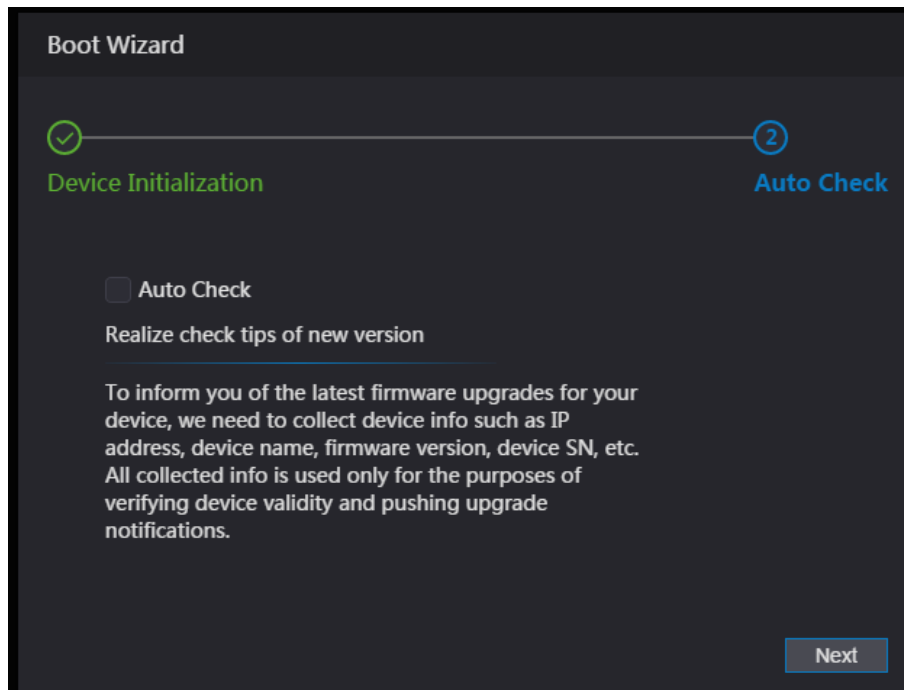


- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' ' ; : &). Set a password of high security level according to the password strength prompt.

- 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



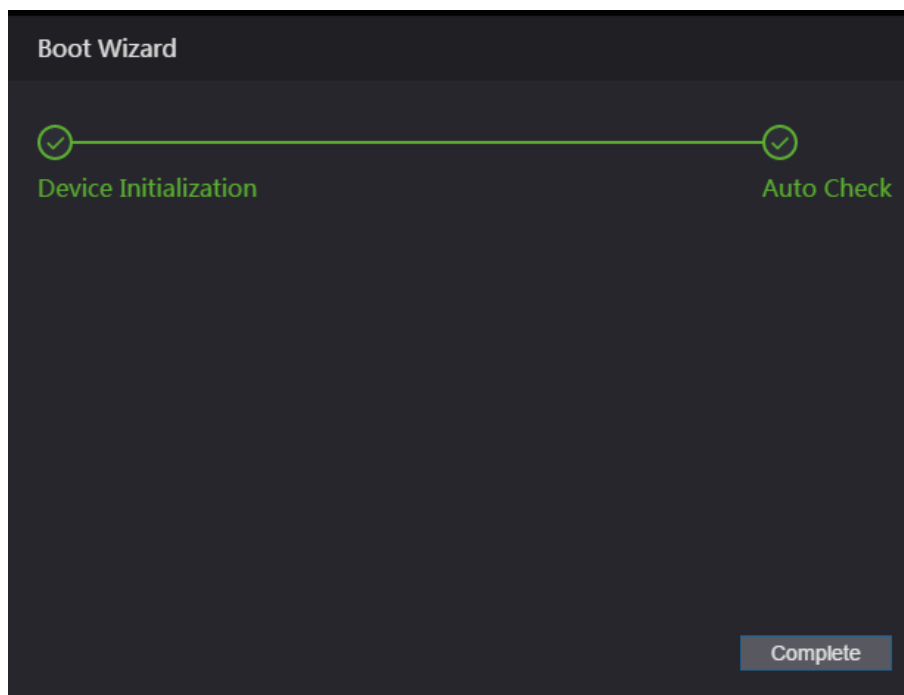
Step 4 You can decide whether to select **Auto Check** or not.



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

Step 5 Click **Next**.

Figure 4-3 Finished configuration



Step 6 Click **Complete**, and the initialization is completed. The web login interface is displayed.

## 4.2 Login

Step 1 Open IE web browser, enter the IP address of the access controller 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 computer used to log in to the web is in the same LAN with the device.
- 7-inch model X access controllers of have dual NICs. The default management address for 1000M network port is 192.168.1.108, and for 100M network port is 192.168.2.108.

Figure 4-4 Login

**WEB SERVICE**

Username:

Password:

[Forget Password?](#)

**Login**

Step 2 Enter the user name and password.



- The default administrator name is admin, and the password is the login password after initializing the access controller. Modify the administrator regularly and keep it properly for the sake of security.
- If you forget the administrator login password, you can click **Forgot password?** to reset it. See "4.3 Resetting the Password."

Step 3 Click **Login**.

The web interface is logged in.

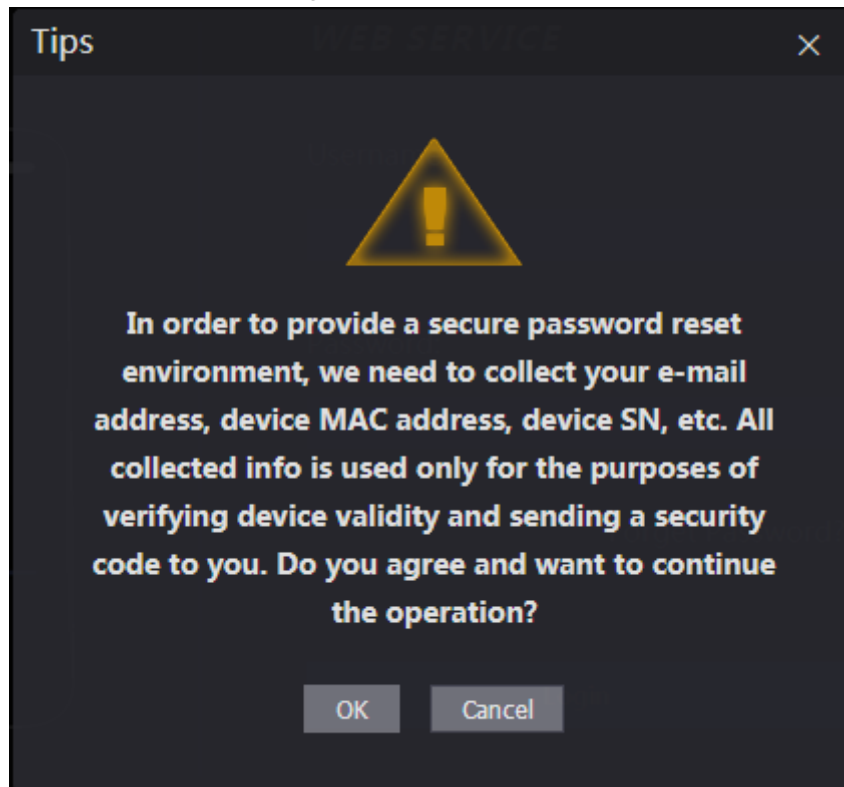
## 4.3 Resetting the Password

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

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

The **Tips** interface is displayed.

Figure 4-5 Tips

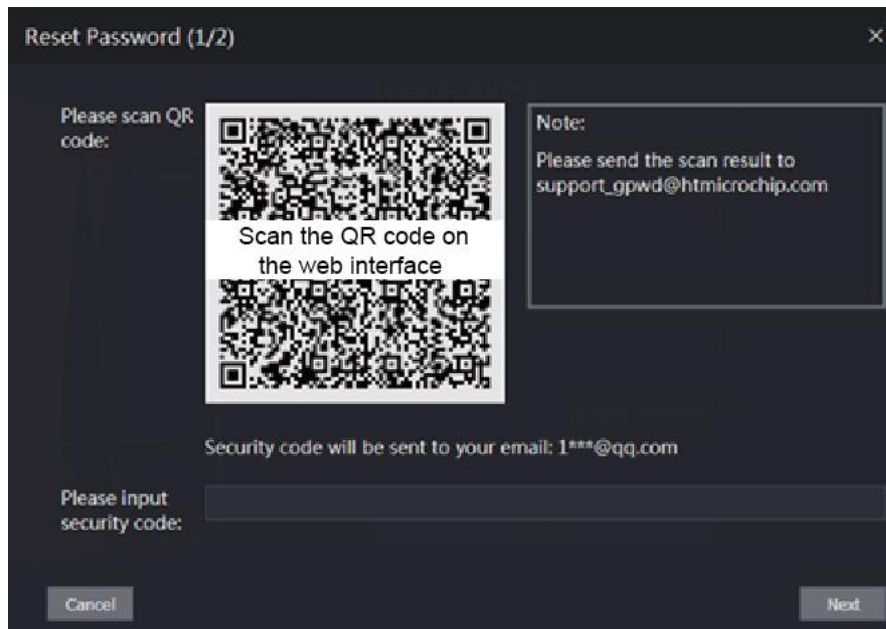


Step 2 Read the tips.

Step 3 Click **OK**.

The **Reset Password** interface is displayed.

Figure 4-6 Reset Password



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



- At most two security codes will be generated by scanning the same QR code. If security codes become invalid, to get more security codes, refresh the QR code.



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

**Step 5** Enter the security code you have received.

**Step 6** Click **Next**.

The **Reset Password** interface is displayed.

**Step 7** Reset and confirm the new password.



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

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

## 4.4 Alarm Linkage

### 4.4.1 Setting Alarm Linkage

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

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

The **Alarm Linkage** interface is displayed.

Figure 4-7 Alarm linkage

Alarm Input	Name	Alarm Input Type	Alarm Output Channel	Modify
1	Zone1	NO	1	
2	Zone2	NO	1	

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

Figure 4-8 Modifying alarm linkage parameter

The screenshot shows a 'Modify' dialog box with the following parameters:

- Alarm Input: 1
- Name: Zone1
- Alarm Input Type: NO
- Fire Link Enable:
- Alarm Output Enable:
- Duration (Sec.): 30 (range 1~300)
- Alarm Output Channel:  1,  2
- Access Link Enable:
- Channel Type: NO

Buttons: OK, Cancel

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. 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 access controller 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 <b>Alarm Output</b> is enabled.
Duration (Sec.)	The alarm duration, and the range is 1–300 seconds.
Alarm Output Channel	You can select an alarm output channel according to the alarming device that you have installed. Each alarm device can be regarded as a channel.
Access Link Enable	After the Access Link is enabled, the access controller will be normally on 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 access controller is added to a client.

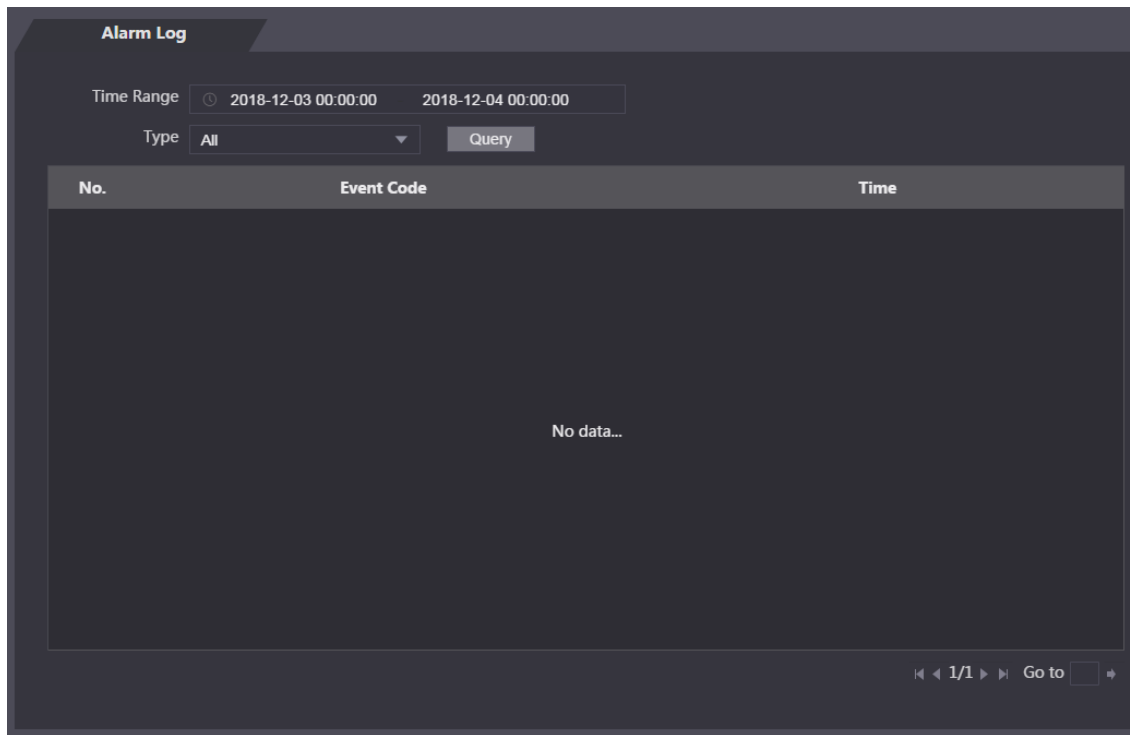
## 4.4.2 Alarm Log

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

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

The **Alarm Log** interface is displayed.

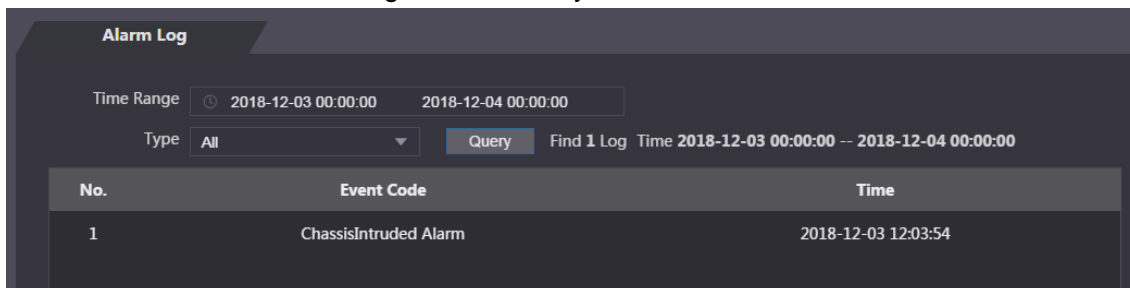
Figure 4-9 Alarm log



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

The query results are displayed.

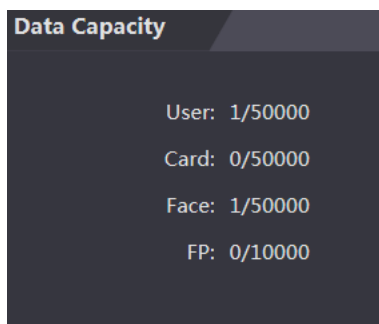
Figure 4-10 Query results



## 4.5 Data Capacity

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

Figure 4-11 Data capacity



## 4.6 Video Setting

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

### 4.6.1 Data Rate

Figure 4-12 Data rate

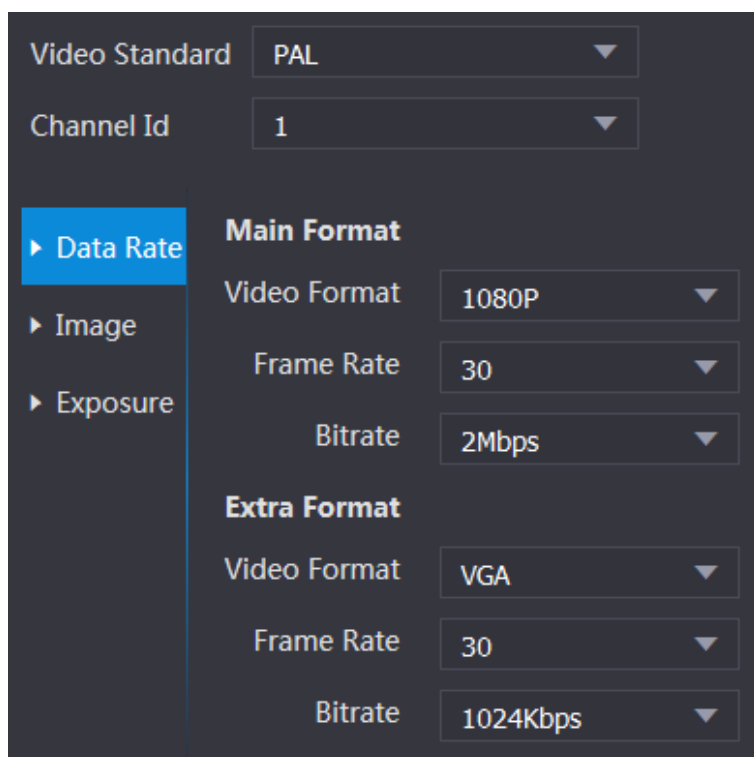


Table 4-2 Data rate parameter description

Parameter	Description
Video Standard	There are two options: NTSC and PAL. Select a standard according to the video standard of your region.
Channel	There are two options: 1 and 2. 1 is white light camera and 2 is IR light camera.

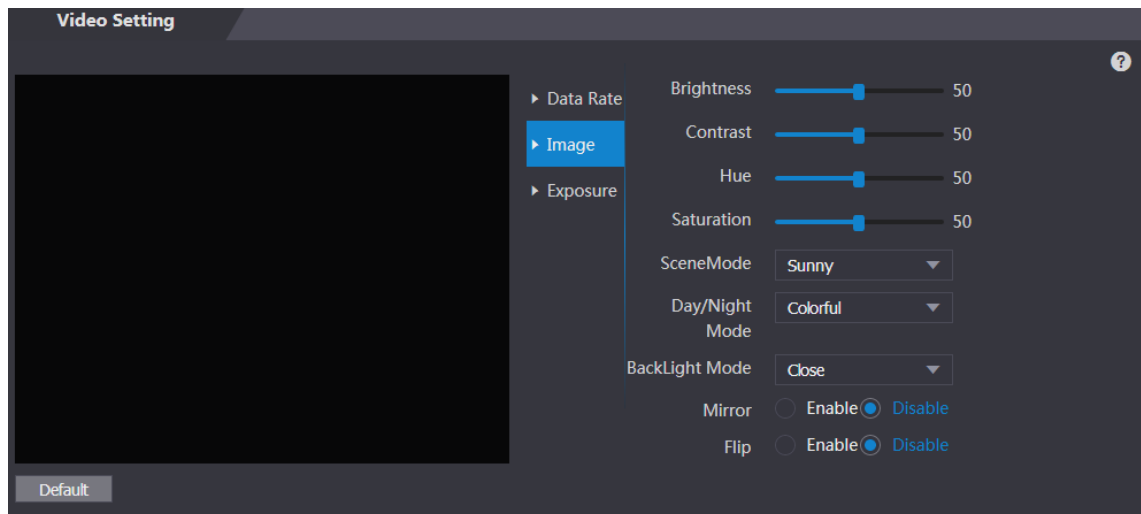
Parameter		Description
Main Format	Video Format	There are four options: D1, VGA, 720p and 1080p. Select an option according to the video quality you want.
	Frame Rate	The rate at which consecutive frames appear on a display. The frame rate range is 1–30fps.
	Bit Rate	The number of bits that are conveyed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

## 4.6.2 Image

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


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



Figure 4-13 Image



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


Table 4-3 Image parameter description

Parameter	Description
Brightness	The larger the value is, the brighter the images will be.
Contrast	Contrast is the difference in luminance or color that makes an object distinguishable. The larger the contrast value is, the greater the brightness and color contrast will be.
Hue	The larger the value is, the deeper the color will be.
Saturation	The larger the value is, the brighter the colors will be.  The value does not change image brightness.

Parameter	Description
Scene Mode	<ul style="list-style-type: none"> <li>● Close: Without modes.</li> <li>● Auto: The system automatically adjusts scene modes.</li> <li>● Sunny: In this mode, image hue will be reduced.</li> <li>● Night: In this mode, image hue will be increased.</li> </ul>  <p><b>Sunny</b> is selected by default.</p>
Day/Night Mode	<p>Day/Night mode decides the working status of the fill light.</p> <ul style="list-style-type: none"> <li>● Auto: The system automatically adjusts the day/night modes.</li> <li>● Colorful: In this mode, images are with colors.</li> <li>● Black and white: In this mode, images are in black and white.</li> </ul>
Back Light Mode	<ul style="list-style-type: none"> <li>● Close: Without backlight compensation.</li> <li>● 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.</li> <li>● 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.</li> </ul>  <p>When human faces are in the backlight, you need to enable WDR.</p> <ul style="list-style-type: none"> <li>● 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.</li> </ul>
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.

### 4.6.3 Exposure

Table 4-4 Exposure parameter description

Parameter	Description
Anti-flicker	<ul style="list-style-type: none"> <li>● 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.</li> <li>● 60Hz: When the utility frequency of alternating current is 60Hz, the exposure is automatically adjusted to make sure that there are no stripes on images.</li> <li>● Outdoor: When <b>Outdoor</b> is selected, the exposure mode can be switched.</li> </ul>
Exposure Mode	 <ul style="list-style-type: none"> <li>● When you select <b>Outdoor</b> in the Anti-flicker drop-down list, you can select <b>Shutter Priority</b> as the exposure mode.</li> <li>● Exposure modes of different devices might vary, and the actual product shall prevail.</li> </ul>

Parameter	Description
	<p>You can select from:</p> <ul style="list-style-type: none"> <li>• Auto: The access controller will automatically adjust brightness of images.</li> <li>• Shutter Priority: The access controller 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 access controller will adjust gain value automatically to get ideal brightness.</li> <li>• Manual: You can configure gain and shutter value manually to adjust image brightness.</li> </ul>
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 <b>Customized Range</b> , 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.

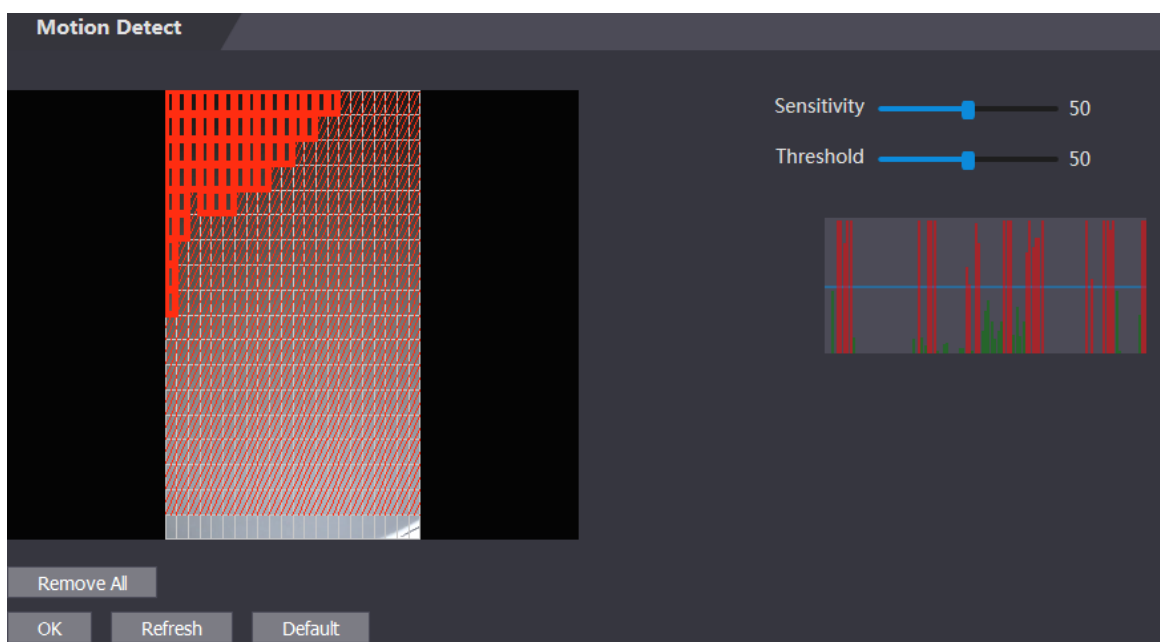
## 4.6.4 Motion Detection

Set a range in which moving objects can be detected.

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

The **Motion Detection** interface is displayed.

Figure 4-14 Motion detection

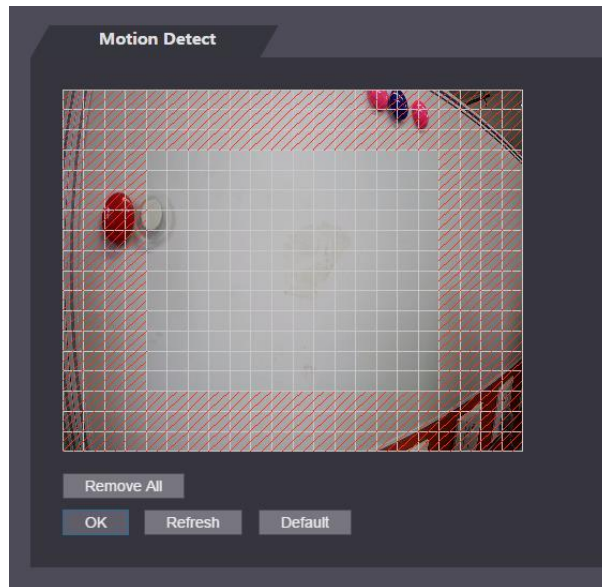


**Step 2** Press and hold the left mouse button, and then drag the mouse in the red area. The **Motion Detection** area is displayed.



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

Figure 4-15 Motion detection area



**Step 3** Set sensitivity and threshold.



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

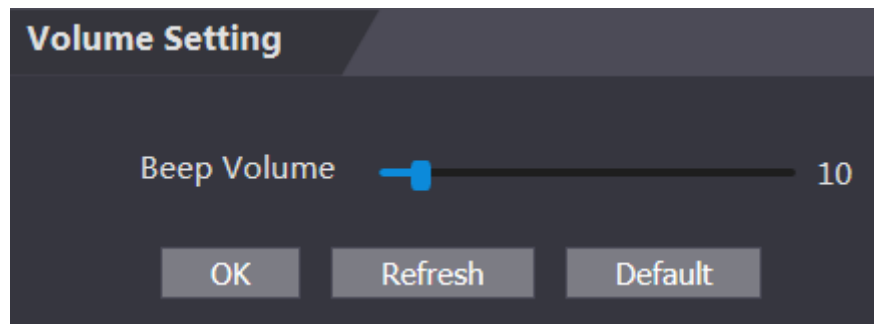
**Step 4** Click **OK** to finish the setting.

## 4.6.5 Volume Setting

You can adjust volume of the access controller speaker.



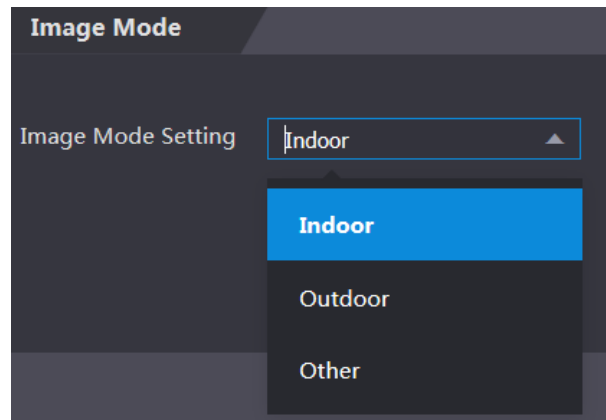
Figure 4-16 Volume setting



## 4.6.6 Image Mode

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

Figure 4-17 Image mode

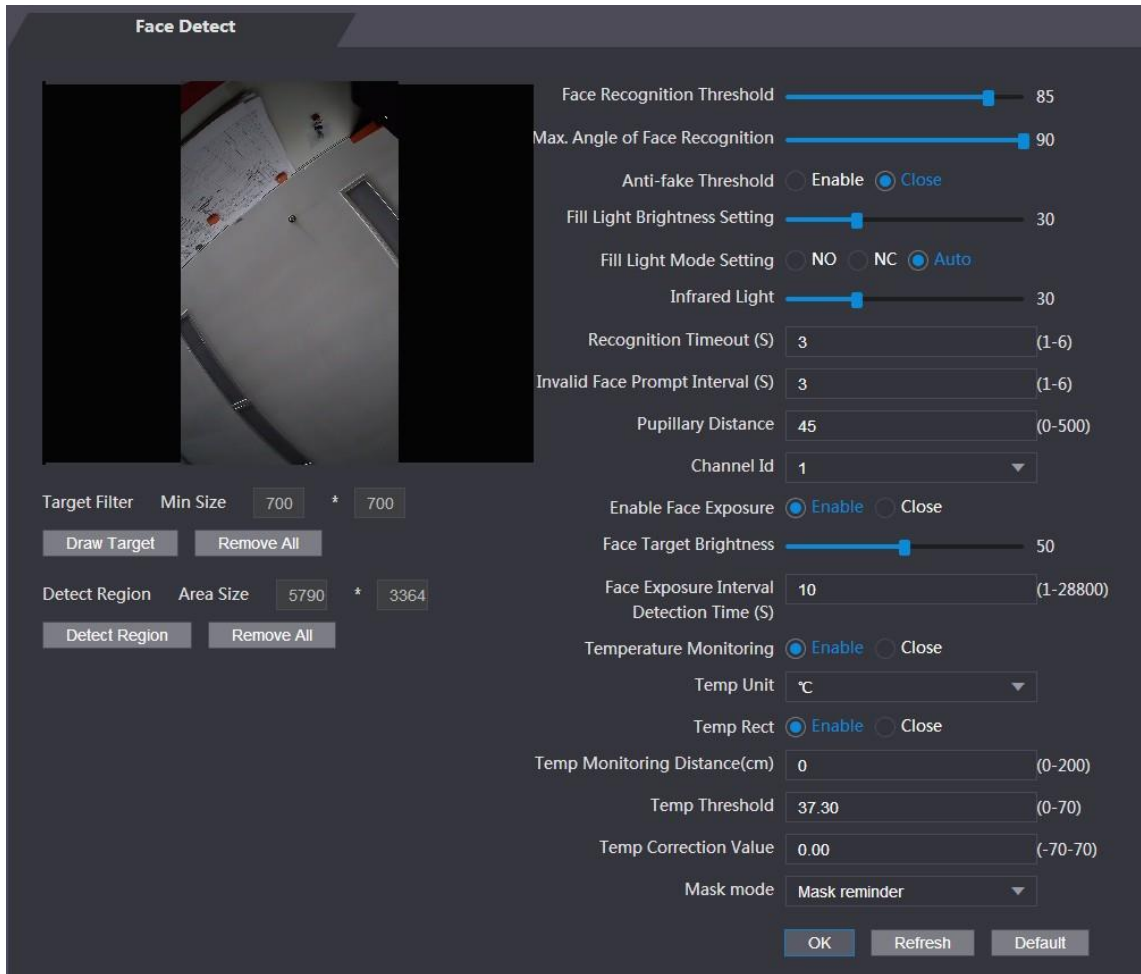


## 4.7 Face Detect

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


Step 1 Select **Face Detect**.

Figure 4-18 Face detect




Step 2 Configure parameters.

Table 4-5 Face detect parameter description

Parameter	Description
Face Recognition Threshold	The larger the value is, the higher the accuracy will be.
Max. Angle of Face Recognition	The larger the angle is, the wider range of the profiles will be recognized.
Anti-fake Threshold	This function prevents people from unlocking by human face images or face models. There are two options: <b>Enable</b> and <b>Close</b> .
Fill Light Brightness Setting	You can set fill light brightness.
Fill Light Mode Setting	There are three fill light modes. <ul style="list-style-type: none"> <li>• NO: Fill light is normally on.</li> <li>• NC: Fill light is normally closed.</li> <li>• Auto: Fill light will be automatically on when a motion detection event is triggered.</li> </ul>  When <b>Auto</b> is selected, the fill light will not be on even if Infrared Light value is greater than 19.
Infrared Light	Adjust IR brightnees by dragging the scroll bar.

Parameter	Description
Recognition Timeout	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	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.
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.
Enable Face Exposure	After face exposure is enabled, human face will be clearer when the access controller 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 <b>Draw Target</b> , and then you can draw the minimum face detection frame. Click <b>Remove All</b> , and you can remove all the frames you drew.
Detect Region	Click <b>Detect Region</b> , move your mouse, and you can adjust the face detection region. Click <b>Remove All</b> , and you can remove all the detection regions.
Face Target Brightness	The default value is 50. Adjust the brightness as needed.
Face Exposure Interval	After a face is detected, the access controller will give out light to illuminate the face, and the access controller will not give out light again until the interval you set has passed.
Temperature Monitoring	Set whether to enable the body temperature monitoring. <ul style="list-style-type: none"> <li>Temp Unit: Select a temperature unit.</li> <li>Temp Rect: Set whether to display the temperature monitoring box or not.</li> <li>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.</li> <li>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.</li> <li>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</li> </ul>

Parameter	Description
	<p>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.</p> <p></p> <p>Only the access controller with a temperature monitoring unit supports this parameter.</p>
Mask Mode	<ul style="list-style-type: none"> <li>• No detect: Mask is not detected during face recognition.</li> <li>• 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.</li> <li>• 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.</li> </ul>

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

## 4.8 Network Setting

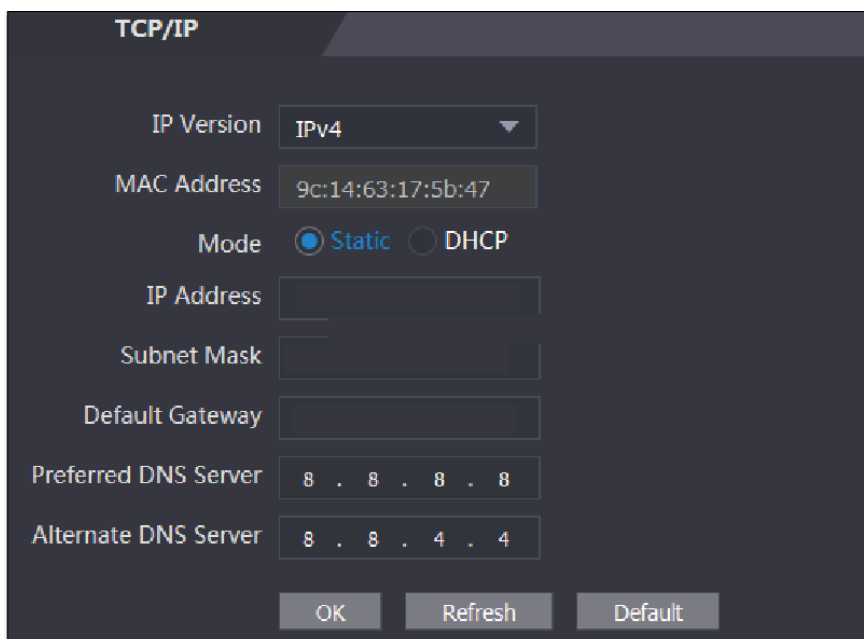
### 4.8.1 TCP/IP

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

Make sure that the access controller is connected to the network correctly.

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

Figure 4-19 TCP/IP




The screenshot displays the TCP/IP configuration screen. At the top, the title 'TCP/IP' is shown. Below it, several configuration options are listed:

- IP Version:** A dropdown menu currently set to 'IPv4'.
- MAC Address:** A text field containing the value '9c:14:63:17:5b:47'.
- Mode:** Two radio buttons are present; 'Static' is selected (indicated by a blue dot), and 'DHCP' is unselected.
- IP Address:** An empty text input field.
- Subnet Mask:** An empty text input field.
- Default Gateway:** An empty text input field.
- Preferred DNS Server:** A text field with the value '8 . 8 . 8 . 8'.
- Alternate DNS Server:** A text field with the value '8 . 8 . 4 . 4'.

At the bottom of the screen, there are three buttons: 'OK', 'Refresh', and 'Default'.

Step 2 Configure parameters.

Table 4-6 TCP/IP

Parameter	Description
IP Version	There is one option: IPv4.
MAC Address	MAC address of the access controller is displayed.
Mode	<ul style="list-style-type: none"> <li>• Static Set IP address, subnet mask, and gateway address manually.</li> <li>• DHCP <ul style="list-style-type: none"> <li>◇ After DHCP is enabled, IP address, subnet mask, and gateway address cannot be configured.</li> <li>◇ 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.</li> <li>◇ If you want to see the default IP when DHCP is effective, you need to disable DHCP.</li> </ul> </li> </ul>
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.
Subnet Mask	
Default Gateway	IP address and gateway address must be in the same network segment.
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.

## 4.8.2 Port

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

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


The **Port** interface is displayed.

**Step 2** Configure port numbers. See the following table.



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

Table 4-7 Port description

Parameter	Description
Max Connection	<p>You can set the maximum connections of clients that the access controller can be connected to.</p> <p></p> <p>Platform clients like Smart PSS are not counted.</p>
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.

### 4.8.3 Register

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

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

The **Auto Register** interface is displayed.

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

Table 4-8 Auto register description

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

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

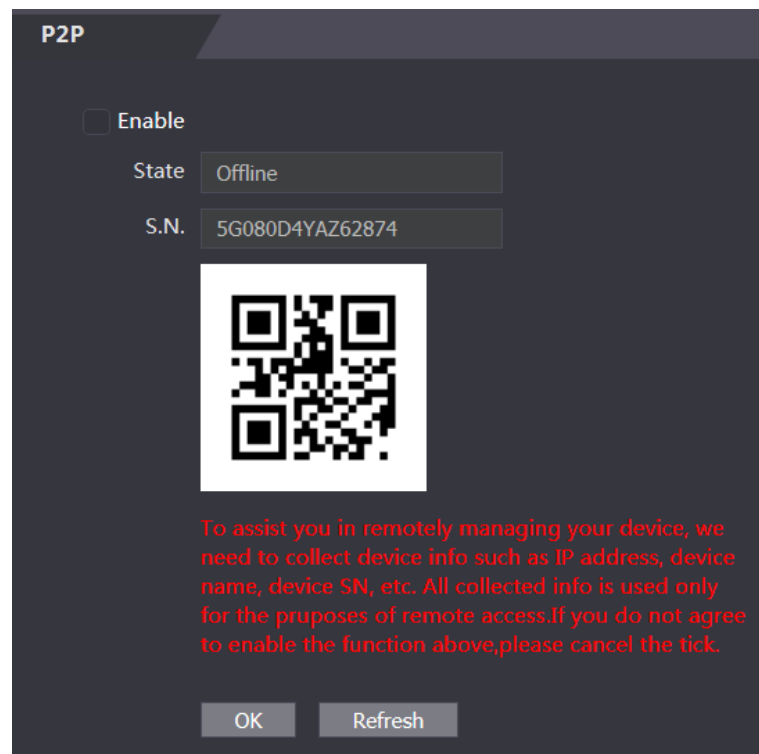
### 4.8.4 P2P

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 access controller 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 access controller to external network; otherwise the access controller cannot be used.

Figure 4-20 P2P



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

The **P2P** interface is displayed.

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

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



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

## 4.9 Date Setting

You need to set time zone, time, DST, and NTP for the access controller.



Only access controllers of certain models support this function.

**Step 1** Select **Date Setting**.

The **Date Setting** interface is displayed.

Figure 4-21 Date Setting

The screenshot shows a 'Date Setting' window with the following configuration:

- Time Zone: GMT+08:00
- System Time: 2019-12-07 15 : 15 : 39
- DST:  Enable  Close
- Date Setting:  Date  Week
- Starting Time: January 1 00 : 00
- Ending Time: January 2 00 : 00
- NTP Setting:  NTP Setting
  - Server: clock.isc.org
  - Port: 123
  - Update Cycle: 60 Min.

Buttons: OK, Refresh, Default

Step 2 Set parameters.

Table 4-9 Date setting

Parameter	Description
Time Zone	Select time zone as needed.
System Time	You can set system time manually, or you can click <b>Sync with PC</b> , to scynchronize access controller time with the computer time.
DST	<ol style="list-style-type: none"> <li>1. Enable DST.</li> <li>2. Select <b>Date</b> or <b>Week</b> in <b>Date Setting</b>.</li> <li>3. Set <b>Starting Time</b> and <b>Ending Time</b>.</li> </ol>
NTP Setting	<ol style="list-style-type: none"> <li>1. Enable <b>NTP Setting</b>.</li> <li>2. Configure parameters.                             <ul style="list-style-type: none"> <li>◇ Server: Enter domain name of the NTP server. The access controller time will be synchronized with the NTP server.</li> <li>◇ Port: Enter port number of the NTP server.</li> <li>◇ Update Cycle: Set an update cycle, and then access controller time will be updated accordingly.</li> </ul> </li> <li>3. Click <b>OK</b>.</li> </ol>

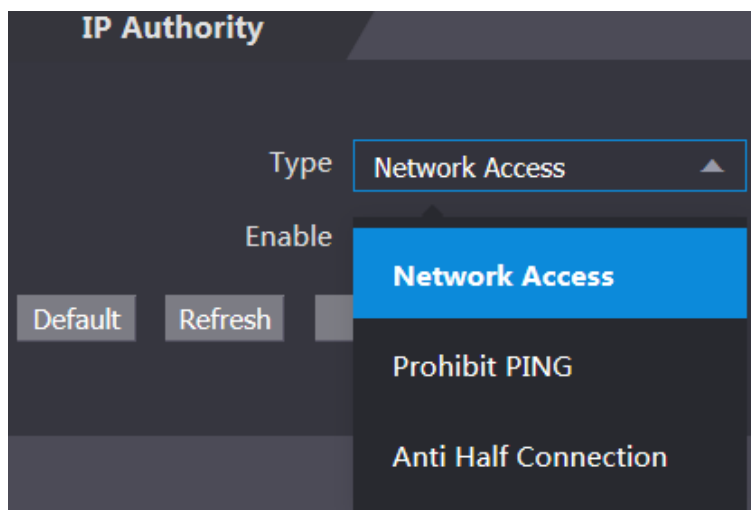
## 4.10 Safety Management

### 4.10.1 IP Authority

Select a cyber security mode as needed.



Figure 4-22 IP authority



## 4.10.2 Systems

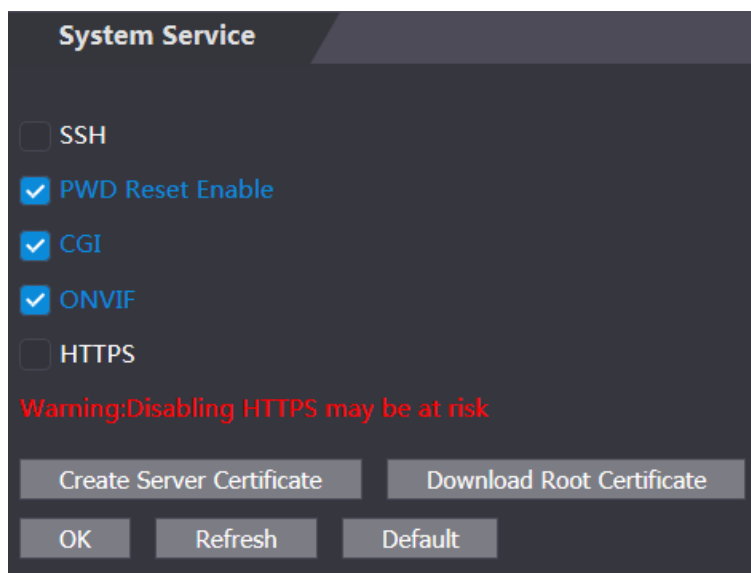
### 4.10.2.1 System Service

There are four options: SSH, PWD Reset Enable, CGI, and HTTPS. Refer to "3.12 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 access controller will be synchronized.

Figure 4-23 System service



### 4.10.2.2 Creating Server Certificate

Click **Create Server Certificate**, enter needed information, click **Save**, and then the access controller 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 on the **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.

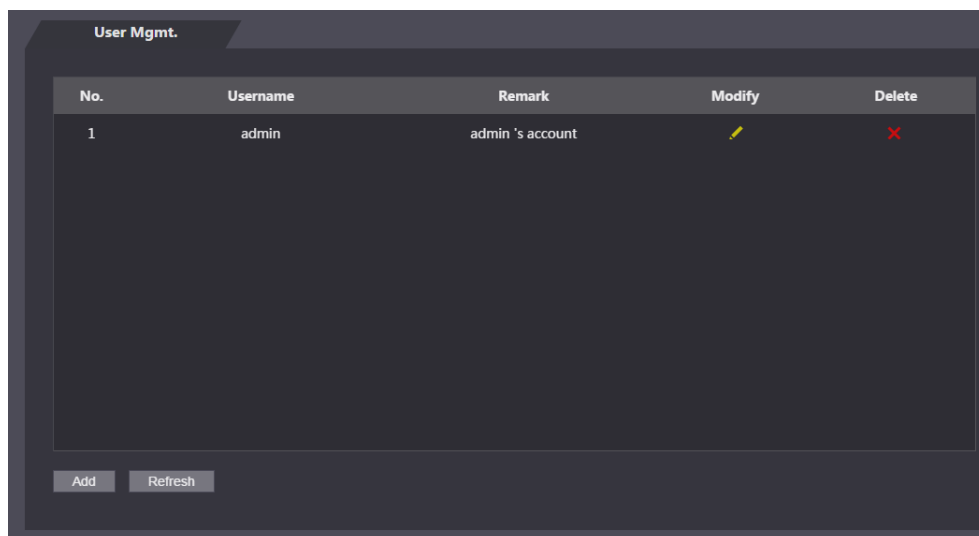
### 4.11.1 Adding Users

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.

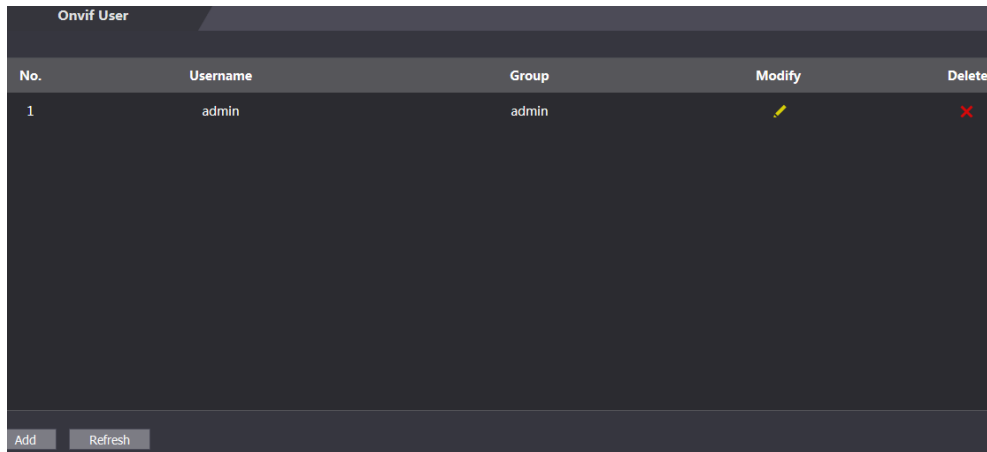
Figure 4-24 User management



### 4.11.3 Onvif User

Open Network Video Interface Forum (ONVIF), a global and open industry forum with the goal of facilitating the development and use of a global open standard for the interface of physical IP-based security products. When ONVIF is used, administrator, operator, and user have different permission of ONVIF server. Create onvif users as needed.

Figure 4-25 Onvif user



No.	Username	Group	Modify	Delete
1	admin	admin		

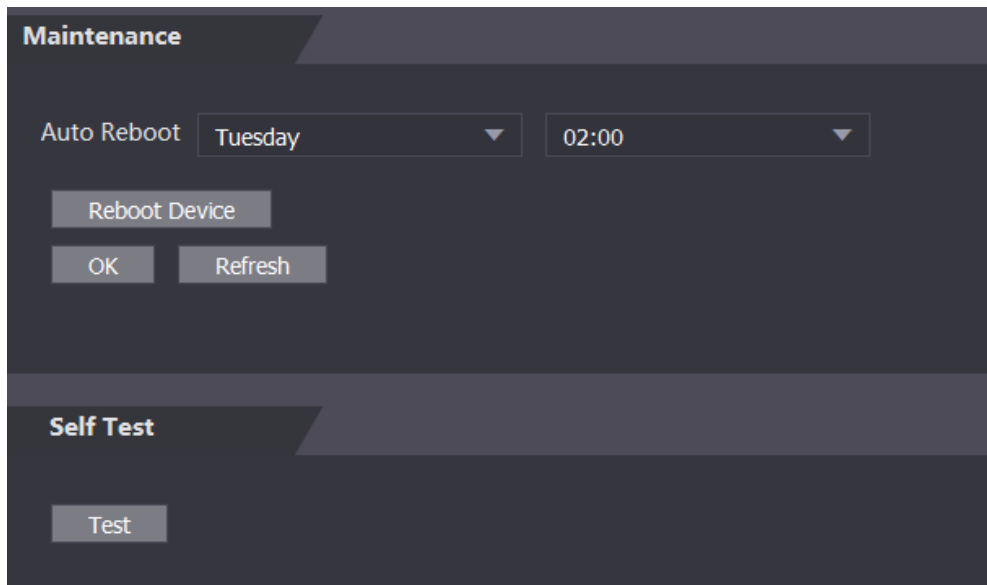
Buttons: Add, Refresh

## 4.12 Maintenance

You can make the access controller reboot itself in idle time to improve the running speed of the access controller. You need to set the auto reboot date and time.

The default reboot time is at 2 O'clock in the morning on Tuesday. Click **Reboot Device**, the access controller will reboot immediately. Click **OK**, the access controller will reboot at 2 O'clock in the morning every Tuesday.

Figure 4-26 Maintenance



**Maintenance**

Auto Reboot: Tuesday (dropdown), 02:00 (dropdown)

Buttons: Reboot Device, OK, Refresh

**Self Test**

Button: Test

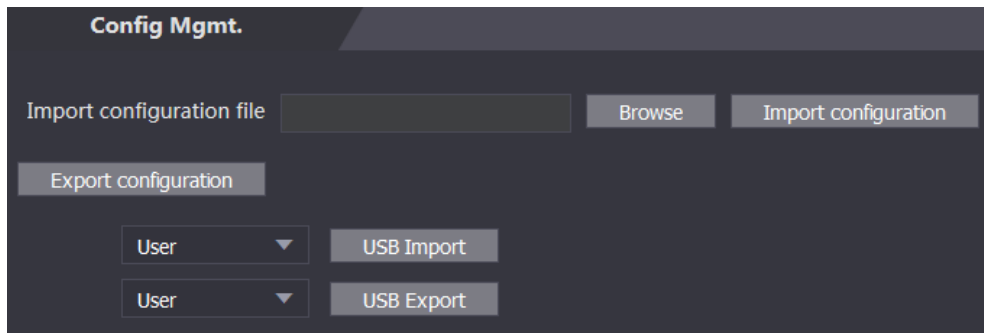
## 4.13 Configuration Management

You need to do configuration management, select unlock result feedback, Wiegand and serial settings for the access controller.

### 4.13.1 Config Mgmt.

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

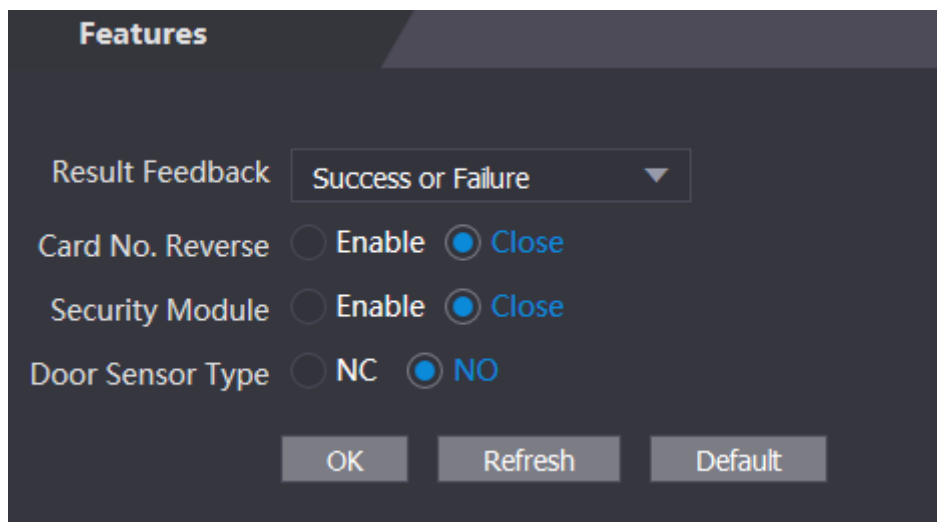
Figure 4-27 Configuration management



### 4.13.2 Features

Select result feedback mode as needed. For details, see "3.12.2 Result Feedback."

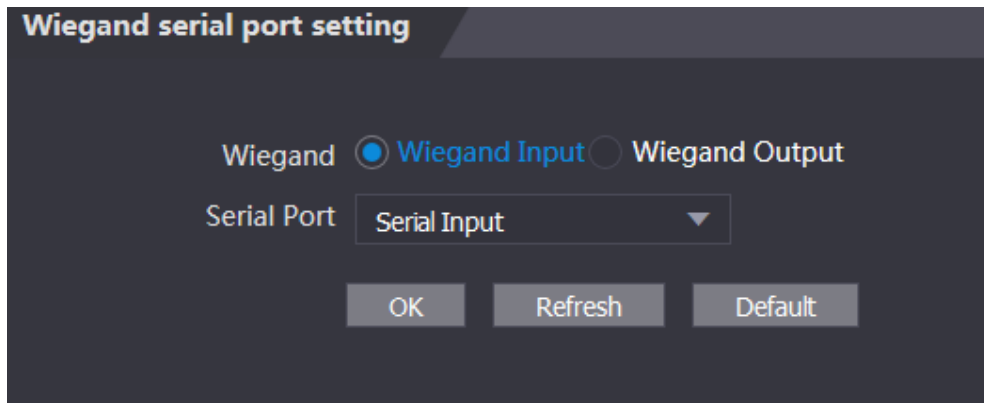
Figure 4-28 Features



### 4.13.3 Wiegand Serial Port Setting

Select Wiegand/serial port setting as needed. For details, see "3.9.2 Serial Port Settings" and "3.9.3 Wiegand Configuration."

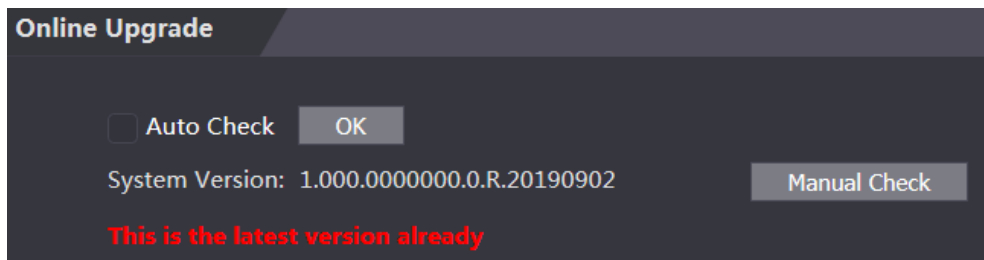
Figure 4-29 Wiegand serial port setting



## 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 4-30



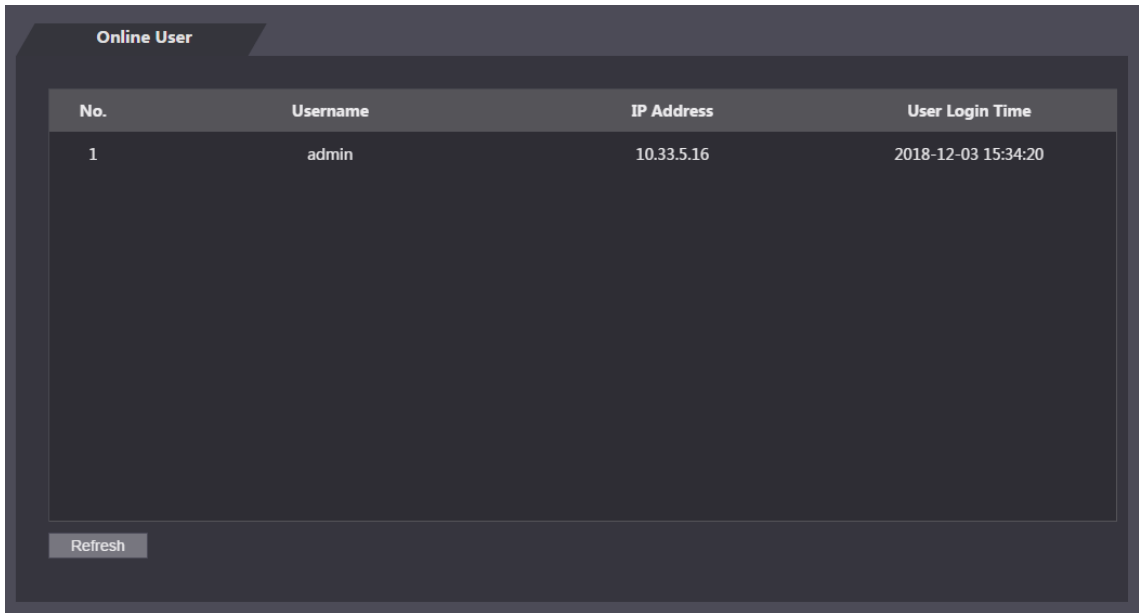
## 4.15 Version Information

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 4-31 Online user



The screenshot shows a web interface titled "Online User". It contains a table with the following data:

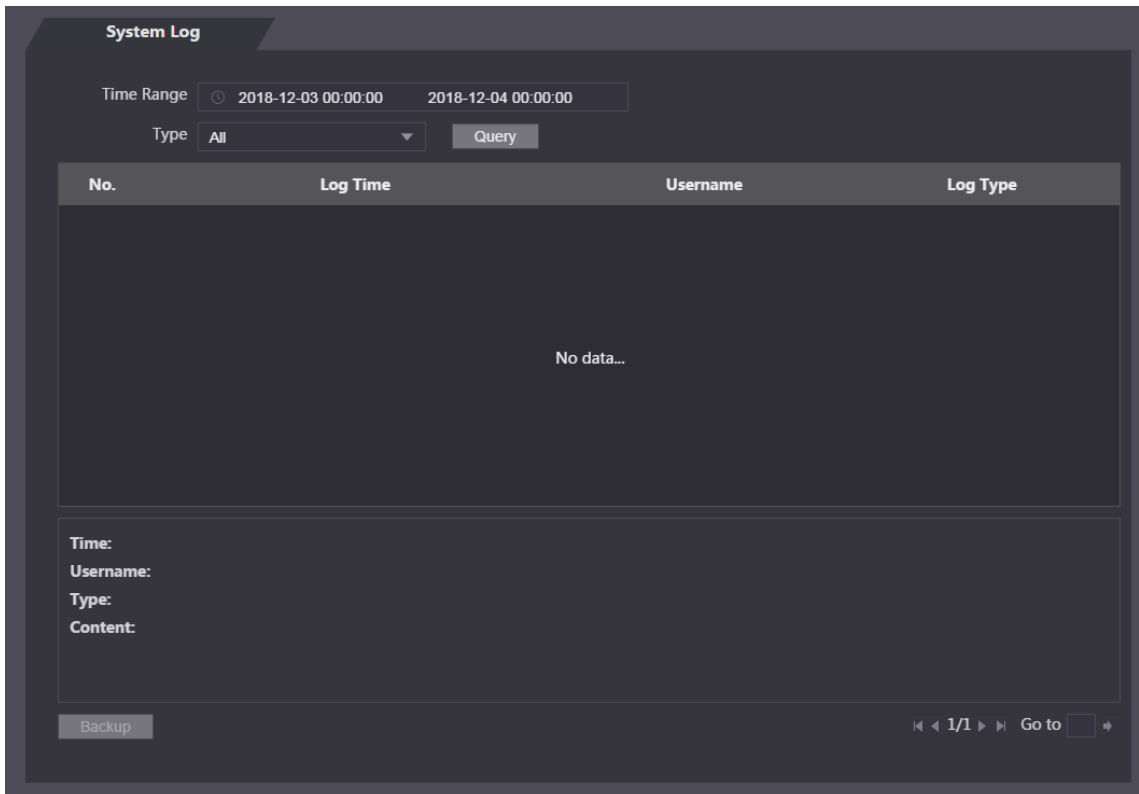
No.	Username	IP Address	User Login Time
1	admin	10.33.5.16	2018-12-03 15:34:20

Below the table is a "Refresh" button.

## 4.17 System Log

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

Figure 4-32 System log



The screenshot shows a web interface titled "System Log". It includes search filters for "Time Range" (2018-12-03 00:00:00 to 2018-12-04 00:00:00) and "Type" (All). A "Query" button is present. Below the filters is a table with the following headers: "No.", "Log Time", "Username", and "Log Type". The table content is empty, displaying "No data...". At the bottom, there is a "Backup" button and a pagination control showing "1/1" and a "Go to" field.

### 4.17.1 Querying Logs

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

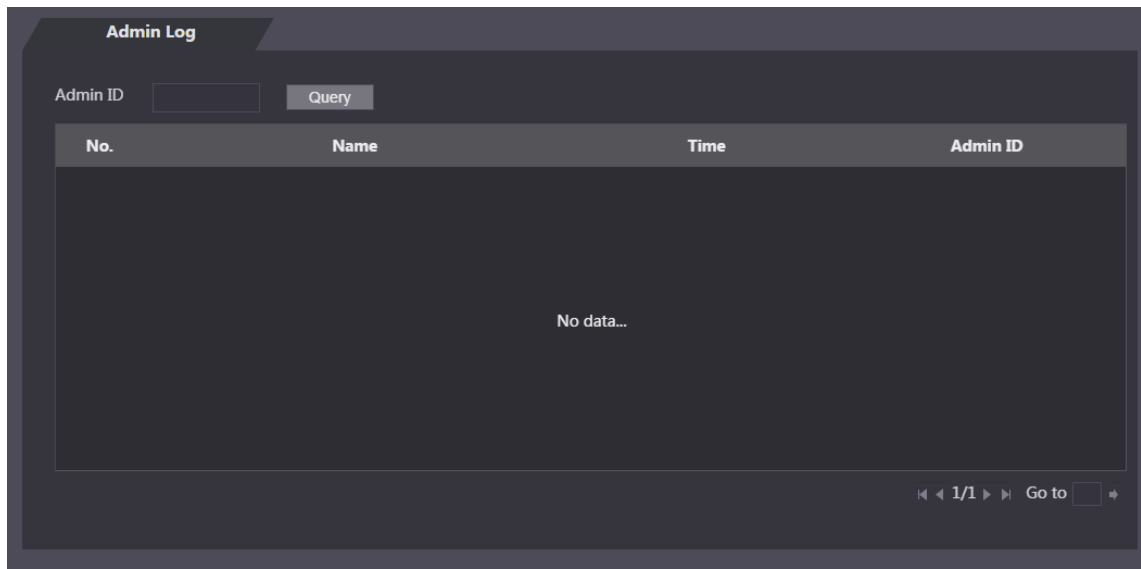
## 4.17.2 Backup Logs


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 4-33 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 access controller 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 access controller 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 access controller and the external controller are connected to the Wiegand port.**

Check whether the GND cable of access controller 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 access controller remotely.
- 5 User information, and face images cannot be imported into the access controller.**

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

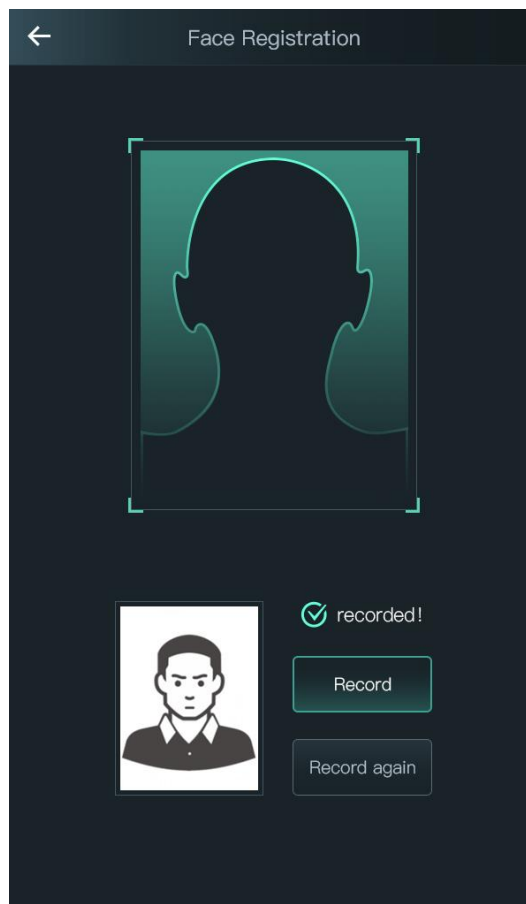
- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you will use the device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the device at least two meters away from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

## During Registration

You can register faces through the access controller 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



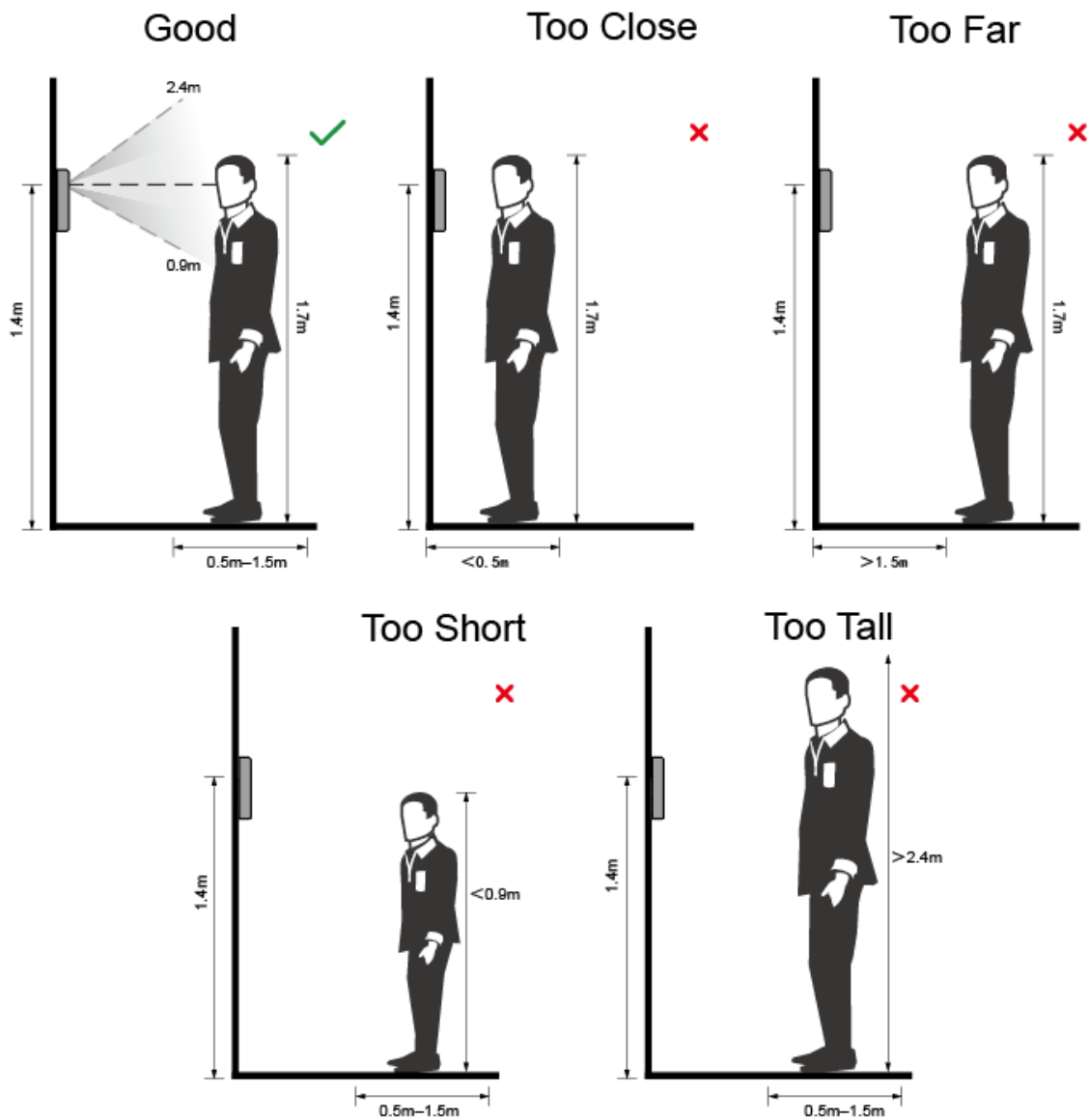


- Do not shake your head or body, otherwise the registration might fail.
- Avoid two faces appear in the capture frame at the same time.

## Face Position

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

Appendix Figure 2-2 Appropriate face position

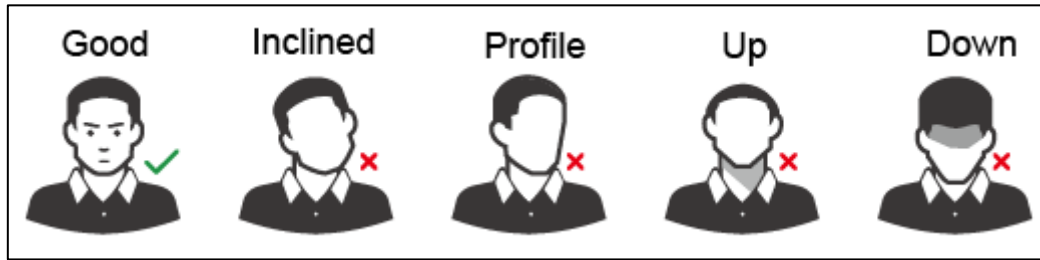


## Requirements of Faces

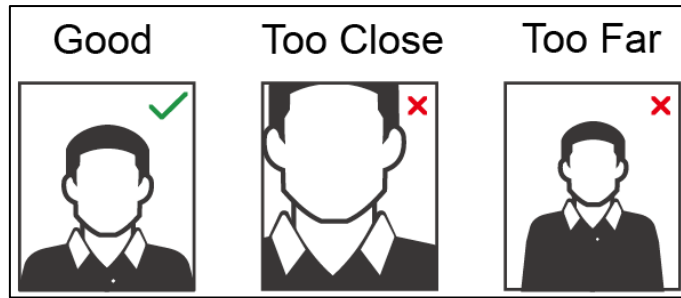
- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during 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 face does not take 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 equipment network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

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

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

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

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

### **1. Physical Protection**

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

### **2. Change Passwords Regularly**

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

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

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

### **4. Enable Account Lock**

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

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

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

#### **6. Enable HTTPS**

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

#### **7. Enable Whitelist**

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

#### **8. MAC Address Binding**

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

#### **9. Assign Accounts and Privileges Reasonably**

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

#### **10. Disable Unnecessary Services and Choose Secure Modes**

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

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

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

#### **11. Audio and Video Encrypted Transmission**

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

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

#### **12. Secure Auditing**

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

#### **13. Network Log**

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

#### **14. Construct a Safe Network Environment**

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

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is

suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.