

# **Fingerprint Access Standalone**

## **User's Manual**








# Foreword

## General

This manual introduces the functions and operations of the Fingerprint Access Standalone (hereinafter referred to as "the Device").

## Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 <b>TIPS</b>	Provides methods to help you solve a problem or save time.
 <b>NOTE</b>	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.1.2	Updated screens.	September 2021

## Privacy Protection Notice

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

## About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the Device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

## Transportation Requirements



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

## Storage Requirements



Store the Device under allowed humidity and temperature conditions.

## Installation Requirements



### **WARNING**

- Connect the Device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the Device.
- Do not connect the Device to more than one power supply. Otherwise, the Device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the Device to direct sunlight or heat sources.
- Do not install the Device in humid, dusty or smoky places.
- Install the Device in a well-ventilated place, and do not block the ventilator of the Device.
- Use the power adapter or case power supply provided by the Device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the Device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause Device to fall off or turnover.

## Operation Requirements



- Make sure that the power supply of the Device works properly before use.

- Do not pull out the power cable of the Device while it is powered on.
- Only use the Device within the rated power range.
- Use the Device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the Device. Make sure that there are no objects filled with liquid on top of the Device to avoid liquids flowing into it.
- Do not disassemble the Device.
- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- If you use power plug or appliance coupler as disconnecting device, please maintain the disconnecting device available to be operated all the time.

# Table of Contents

<b>Foreword</b> .....	<b>i</b>
<b>Important Safeguards and Warnings</b> .....	<b>iii</b>
<b>1 Overview</b> .....	<b>1</b>
<b>2 Structure and Installation</b> .....	<b>2</b>
2.1 Structure and Dimensions .....	2
2.2 Installation .....	4
<b>3 System Structure</b> .....	<b>6</b>
<b>4 Function Settings</b> .....	<b>7</b>
4.1 Login .....	7
4.2 User Management .....	7
4.2.1 Adding Users .....	7
4.2.2 Adding Public Password.....	8
4.2.3 Deleting Users.....	9
4.2.4 Deleting Password.....	10
4.2.5 Adding Main Cards.....	10
4.3 Configuring Access Control.....	11
4.3.1 Setting Period.....	11
4.3.2 Setting Main Card .....	13
4.3.3 Setting Unlock Mode.....	14
4.3.4 Setting Door Lock Time .....	14
4.3.5 Setting Alarms.....	15
4.3.6 Setting Door Status.....	16
4.4 System Settings .....	16
4.4.1 Local Setup.....	16
4.4.2 Configuring Network.....	18
4.4.3 Setting Device Mode .....	19
4.4.4 Restarting Device.....	20
4.4.5 Updating System.....	20
4.5 System Information.....	20
4.5.1 Viewing Unlock Records.....	20
4.5.2 Viewing Alarm Records.....	21
4.5.3 Viewing Device Information .....	22
4.5.4 Exporting/Importing .....	23
<b>Appendix 1 Cybersecurity Recommendations</b> .....	<b>24</b>

# 1 Overview

The Fingerprint Access Standalone integrates card reading, configurations, and other functions. It can be applied in many scenarios, such as commercial building, corporation and intelligent community.

## Main Features

- Touch keyboard + LCD display, TCP/IP protocol.
- Supports unlock through card, fingerprint, password and their combinations.
- Supports a maximum of 3,000 fingerprints (by default) and up to 4,500 fingerprints (customized), 30,000 valid cards and 500 public passwords.
- Supports a maximum of 150,000 card records and 1024 alarm records.
- Supports door timeout alarm, intrusion alarm, duress alarm, and door sensor alarm.
- Supports doorbell input.
- Supports guest card, duress card, blocklist/allowlist and patrol card, while support period of validity or times.
- Supports card reader and single-door controller.
- Supports 128 groups of period and 128 groups of holiday period.



If this product requires external power, please use 12 VDC 0.5 A adapter and the operating temperature must be within -5 °C to 55 °C.

# 2 Structure and Installation

## 2.1 Structure and Dimensions

Figure 2-1 Front view

Unit : mm

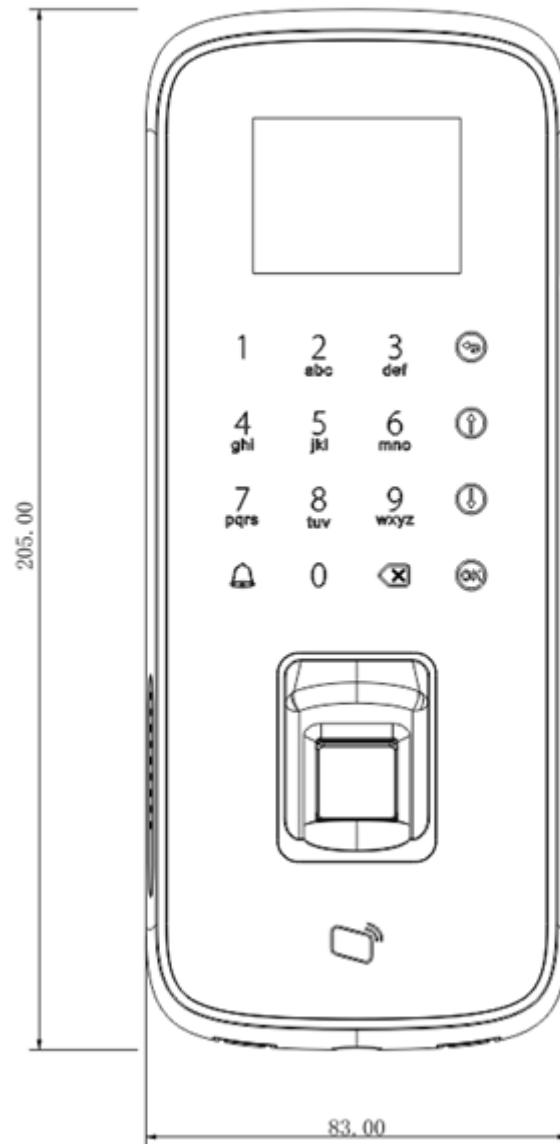
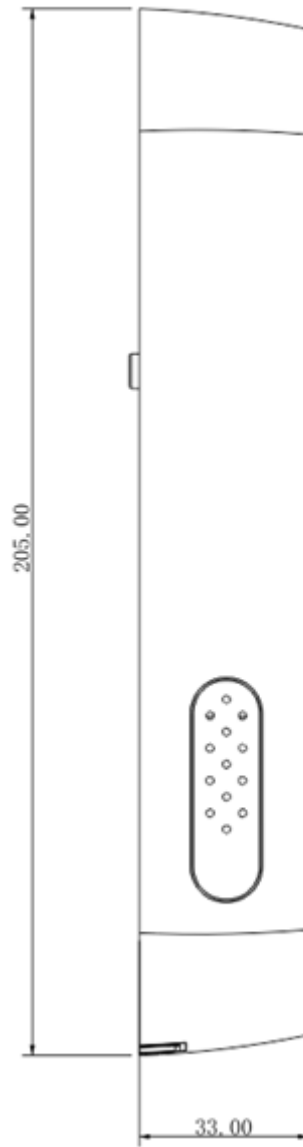




Figure 2-2 Side view

Unit : mm



## 2.2 Installation

Figure 2-3 Wires of the Device

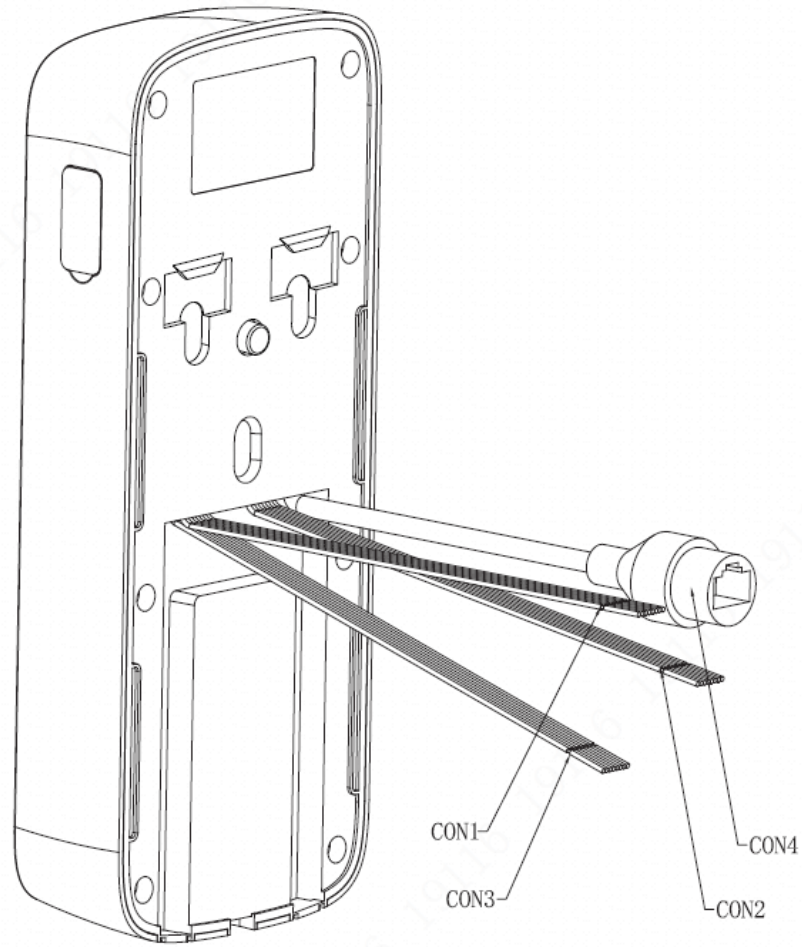


Table 2-1 Description of ports

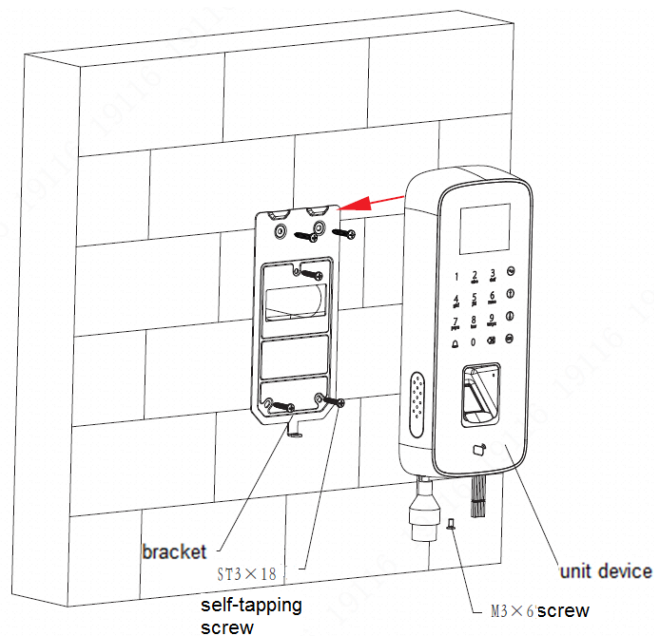
Port	Color	Interface	Note	Protocol	
CON1	Red	+12VI	12 VDC power input	—	
	Black	GND	GND		
	Blue	COM	Lock COM		
	White	NC	Lock NC		
	Green	NO	Lock NO		
	Brown	SR	Door sensor		
	Yellow	GND	GND		
CON2	Purple	PUSH	Unlock button	—	
	Red	+12VO	12 VDC power output		
	Black	GND	GND		
	Blue	CASE	Card reader		
	White	D1	Weigand line 1		Weigand protocol
	Green	D0	Weigand line 0		
	Brown	LED	Weigand card indicator line		
Yellow	B1	RS485B	RS485 protol		
Purple	A1	RS485A			

Port	Color	Interface	Note	Protocol	
CON3	Red	BELL+	Ring	—	
	Black	BELL-			
	Blue	GND	GND		
	White	AOUT	Alarm output		
	Green	AIN	Alarm input		
	Brown	GND	GND		
	Yellow	B2	External RS485B		RS485 protocol
	Purple	A2	External RS485A		
CON4	—	RJ45	Network	—	

## Installation Procedure

- Step 1** Fasten the bracket on installation surface with three ST3×18 self-tapping screws.
- Step 2** Connect the wires, thread the wires through the slots of the bracket, and place wires into the installation surface.
- Step 3** According to the direction of arrow, secure the Device to the bracket.

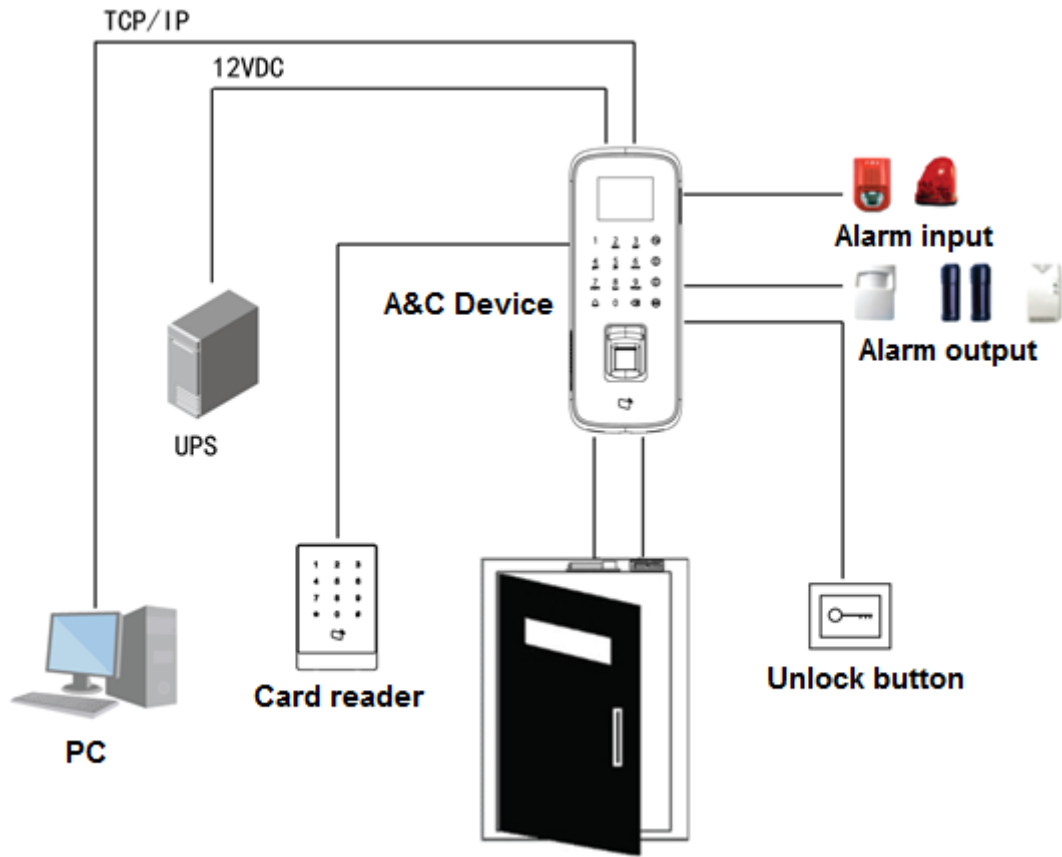
Figure 2-4 Installation of the Device



- Step 4** From the bottom up, and fasten the bracket with a M3×6 screw.

# 3 System Structure

Figure 3-1 System structure



# 4 Function Settings

## 4.1 Login

Step 1 Start the Device and Tap **OK**.

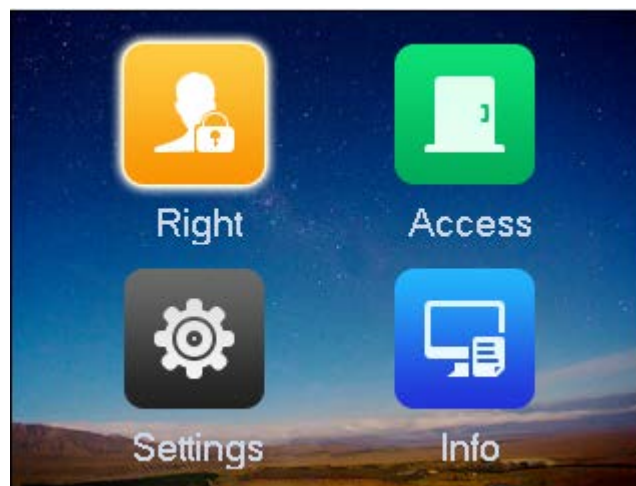
Step 2 Enter the admin password, and tap **OK** to enter the **Main Menu**.



Default password is "88888888". Please change admin password.

- Tap ↑ button to move up.
- Tap ↓ button to move down.
- Tap **OK** to enter or confirm.
- Tap ↶ to return or exit.
- Tap ⌫ to backspace.
- Tap 🔔 to ring.

Figure 4-1 Main menu



## 4.2 User Management

You can add or delete users.

### 4.2.1 Adding Users

Add users to associate the card No. with their fingerprints.

Step 1 On the main page, select **Right** > **OK**.

Step 2 Tap **Add User** > **OK**.

Figure 4-2 Add user

Add User	
Card No.	003D62AC
UserID	1
Card Type	Normal
Use Time	255
Password	123456
Period	0
Validity	2037-12-31

**Step 3** Use the keypad to enter card number or place the card on the swiping area.

**Step 4** Select a card type.

Table 4-1 Card types

Card Type	Description
Normal	People can access the door within configured time and valid period.
VIP card	Service personnel receive notifications when the VIP cardholder enters.
Guest card	Guests can unlock the door for limited times. When the unlocking times runs out, they cannot unlock the door.
Patrol card	Patrol users will have their attendance tracked, but they have no unlocking permissions.
Block list	When users in the blocklist unlock the door, service personnel will receive a notification.
Duress card	Duress card becomes valid after you set duress alarm. You can swipe this card to unlock, but an alarm will be send to the center.

**Step 5** Configure other user parameters.

**Step 6** Tap **OK** and the system prompts whether to enroll the fingerprint.

- Select **YES** and follow the instructions to enroll the fingerprint.
- Select **NO** to complete adding.

## 4.2.2 Adding Public Password

Unlock the door by only entering the public password.



Before use the public password to unlock the door, set the unlock mode to unlocking by password, or unlocking by card or password or fingerprint.

**Step 1** On the **Right** screen, select **Add Public Password**, and then tap **OK**.

Figure 4-3 Public password



Step 2 Enter public password no. and tap ↓.

Step 3 Enter public password and confirmation password.

Step 4 Tap **OK**.

## 4.2.3 Deleting Users

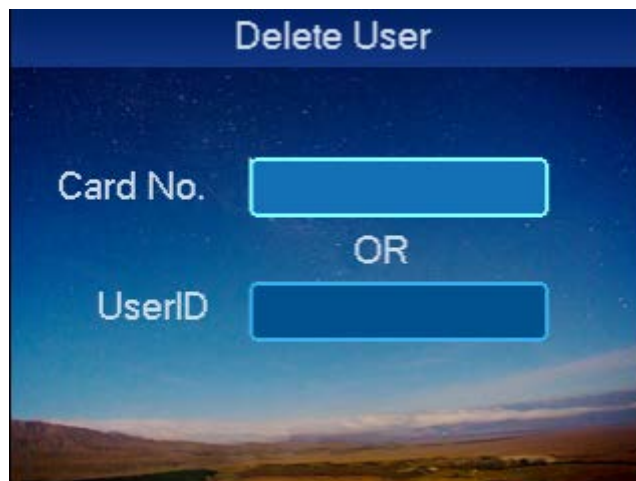
You can delete a single user or all users.

### 4.2.3.1 Deleting Single User

Step 1 On the **Right** screen, select **Delete User** and tap **OK**.

Step 2 Select **Delete Single User** and tap **OK**.

Figure 4-4 Delete user



Step 3 Delete user.

- Enter card number you want to delete and tap **OK**.
- Scan card you want to delete on card swiping area, and then tap **OK**.
- Enter user number you want to delete, and then tap **OK**.

Step 4 Select **OK** and tap **OK**.

### 4.2.3.2 Deleting All Users

Step 1 On delete user screen, select all users, and tap **OK**.

Step 2 Select **OK** and tap **OK**.

### 4.2.4 Deleting Password

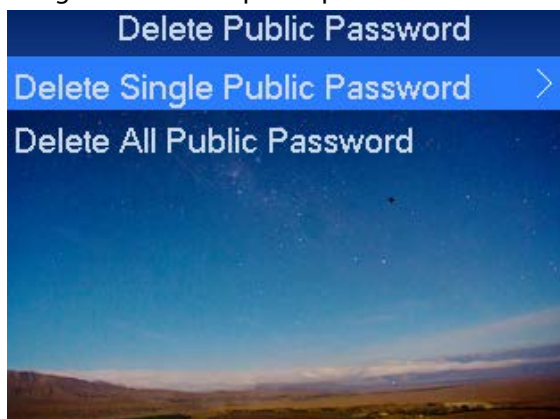
You can delete a single public password or delete all public passwords.

#### 4.2.4.1 Deleting Single Public Password

Step 1 On the **Delete User** screen, select **Delete Public Password**, and tap **OK**.

Step 2 Select **Delete Single Public Password** and tap **OK**.

Figure 4-5 Delete public password



Step 3 Enter number of public password and tap **OK**.

Step 4 Select **OK** and tap **OK**.

#### 4.2.4.2 Deleting All Public Passwords

Step 1 On **Delete Public Password** screen, select **Delete all public passwords**, and tap **OK**.

Step 2 Select **OK** and tap **OK**.

### 4.2.5 Adding Main Cards

You can quickly add card users through main card. Before adding card users, you must add one main card first.

Step 1 On the **Right** screen, select add more main card, and tap **OK**.

Step 2 Place main card on swiping area and scan.

Step 3 Place the added card at the swiping area to scan.



## 4.3 Configuring Access Control

### 4.3.1 Setting Period

You can set unlock period, including card swiping period, holiday period, mode period and NO period.

#### 4.3.1.1 Setting Card Swiping Period

Card swiping period can be 0–127, a total of 128 periods. In each period, you need to set schedules for a week. When a new card is added, and set card swiping period, then user swipe card to unlock. Access control will judge if current time is within set period.

Table 4-2 Card swiping period

Day	Period
Monday	0800-2200 (valid period: 08:00 to 22:00)
Tuesday	0800-2200 (valid period: 08:00 to 22:00)
Wednesday	0800-2200 (valid period: 08:00 to 22:00)
Thursday	0800-2200 (valid period: 08:00 to 22:00)
Friday	0800-2200 (valid period: 08:00 to 22:00)
Saturday	0800-2200 (valid period: 08:00 to 22:00)
Sunday	0800-2200 (valid period: 08:00 to 22:00)

**Step 1** On the main menu, select **Access**, and tap **OK**.

**Step 2** Select time period, and tap **OK**.

**Step 3** Select card swiping period, and tap **OK**.

Figure 4-6 Card swiping period (1)



**Step 4** Enter time period, and tap **OK**. Enter any number between 0–127.

Figure 4-7 Card swiping period (2)



Step 5 Select a day to set periods, and tap **OK**.

Step 6 Set periods for the rest of the week.

Step 7 Tap **OK**.

Step 8 Select **YES**, and tap **OK**.

### 4.3.1.2 Setting Holiday Period

You can set up to 128 holiday periods (from 0 through 127).

Step 1 On the time period setup screen, select holiday period, and then tap **OK**.

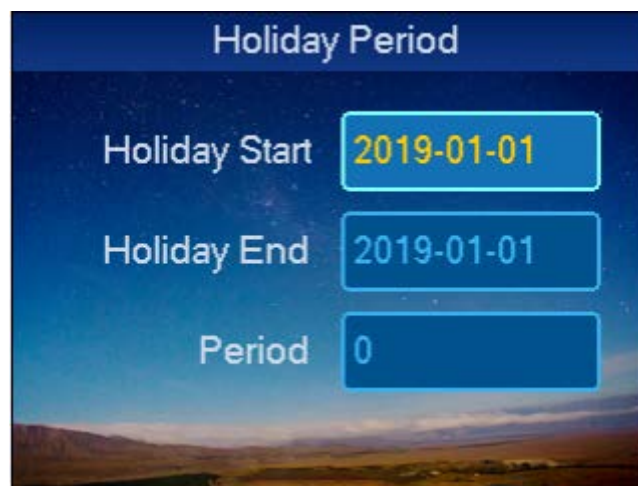
Step 2 Enter period number (0–127).

Step 3 Enter the holiday start time, holiday end time and period, and then tap **OK**.



Period is the period number you set on card period screen.

Figure 4-8 Holiday period



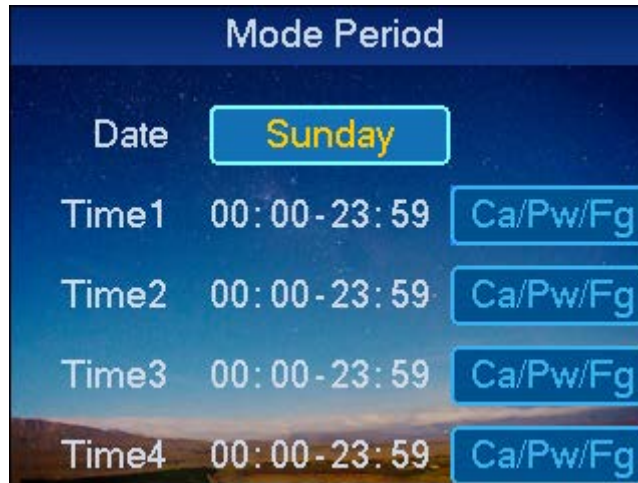
Step 4 Select **YES**, and tap **OK**.

### 4.3.1.3 Setting Mode Period

Mode period has four periods per day from Monday to Sunday.

Step 1 On time period setup screen, select mode period, and tap **OK**.

Figure 4-9 Mode period



Step 2 Select **Monday**, and tap **OK**.

Step 3 Configure period, tap **OK** to select unlock mode of the period.

Step 4 Configure periods from Tuesday through Sunday.

Step 5 Tap **OK**.

Step 6 Select **YES**, and tap **OK**.

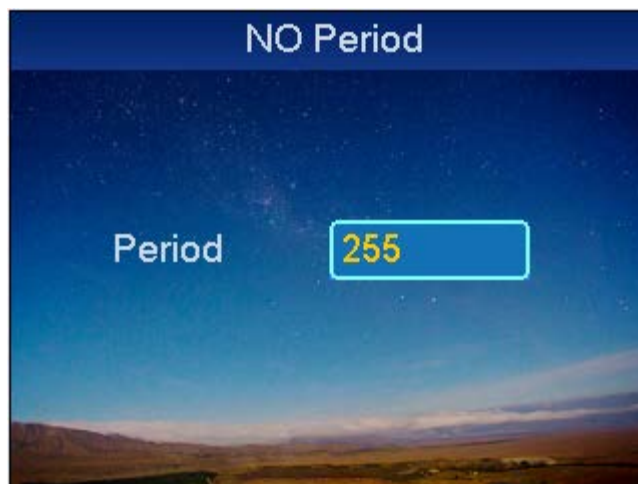
After completion, the unlock methods are managed according to the four periods.

#### 4.3.1.4 Setting NO Period


After you set the NO period, the door will remain unlocked during this period.

Step 1 On the time setup screen, select **NO Period**, and tap **OK**.

Figure 4-10 NO period



Period number is the number you set on the card swiping period screen.

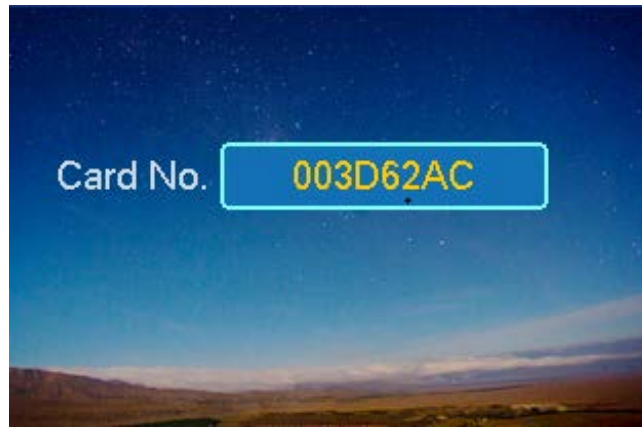
Step 2 Tap  to delete old data, enter period number, and then tap **OK**.


#### 4.3.2 Setting Main Card

You can modify or add main card.

Step 1 On the **Access** screen, select main card setup, and tap **OK**.

Figure 4-11 Main card setup



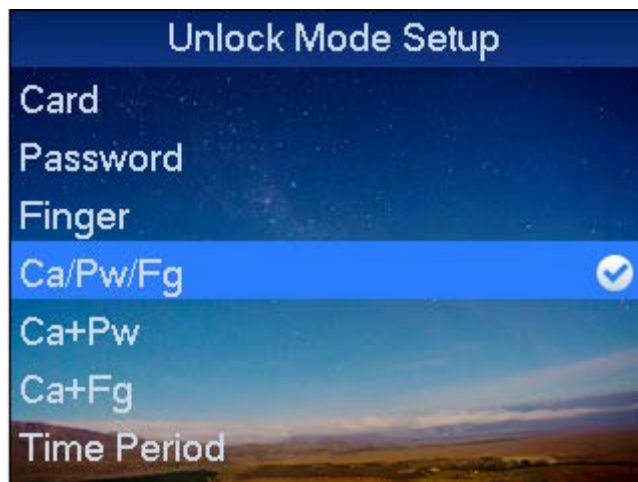
Step 2 Tap  to delete old card number, and enter new card number, or place the card on the swiping area for scanning, and then tap **OK**.

### 4.3.3 Setting Unlock Mode

Unlock modes includes card, password, fingerprint, card and password, card and fingerprint, card or password or fingerprint.

Step 1 On the **Access** screen, select unlock mode, and then tap **OK**.

Figure 4-12 Unlock mode setup



Step 2 Select the unlock mode and tap **OK**.

### 4.3.4 Setting Door Lock Time



Door lock time includes lock hold time and over time.

- Hold Time: After you swipe card, the door remains unlocked for a defined hold time before it close again.
- Over Time: If the door remains unlocked after the defined over time after you swipe card, an alarm is triggered.

Step 1 On the **Access** screen, select door lock time setup and tap **OK**.

Figure 4-13 Door lock time setup



Step 2 Tap  to delete original data, enter hold time and over time, and then tap **OK**.  


Door lock hold time is the time door remains open after a person swipes the card. If the door remains open exceeding "over time", an alarm is triggered.

### 4.3.5 Setting Alarms

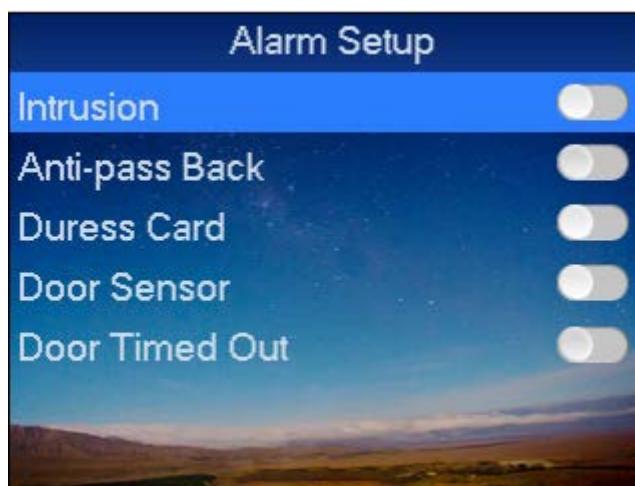
You can enable or disable alarms. System alarm includes intrusion, anti-pass back, duress card, door sensor and door timed out.

Table 4-3 Alarm type

Alarm Type	Note
Intrusion	An alarm is triggered when people enter without valid card swiping or password.
Anti-pass back	If 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 verification and exits without verification, an alarm will be triggered when they attempt to unlock again, and access is denied at the same time.</li> <li>• If a person enters without verification and exits with verification, an alarm will be triggered when they attempt to unlock again, and access is denied at the same time.</li> </ul>
Duress Card	An alarm will be triggered when a duress card or duress password is used to unlock the door.
Door Sensor	When the Device is damaged, an alarm will be triggered.
Door Timed Out	A timeout alarm will be triggered if the door remains unlocked for longer time than the preset time .

Step 1 On the **Access** screen, select alarm setup, and tap **OK**.

Figure 4-14 Alarm setup



Step 2 Select the alarm type to enable alarm function, and then tap **OK**.

## 4.3.6 Setting Door Status

You can set the access control status to normal, NO or NC.

Step 1 On the **Access** screen, select door status setup, and then tap **OK**.

Step 2 Use ↑ and ↓ to select the access control status, and tap **OK**.

is displayed after selection.

## 4.4 System Settings

### 4.4.1 Local Setup

You can set data, admin password and voice mail. You also can export all data, and restore default settings.

#### 4.4.1.1 Setting Date

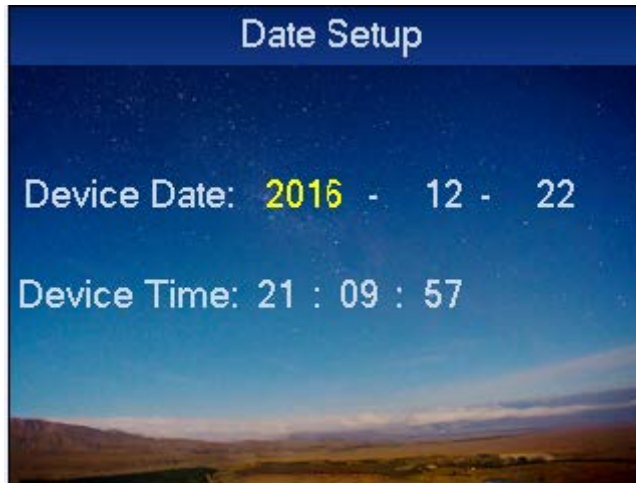
Set system date and time.

Step 1 On the **System** screen, tap ↑ or ↓ to select date setup, and then tap **OK**.

Step 2 Select local setup, and then tap **OK**.

Step 3 Select date setup, and then tap **OK**.

Figure 4-15 Data setup



Step 4 Set the date and time of the Device, and then tap **OK**.

#### 4.4.1.2 Changing Admin Password

You can change admin password.

Step 1 On the local setup screen, select admin password setup, and then tap **OK**.

Figure 4-16 Admin password setup

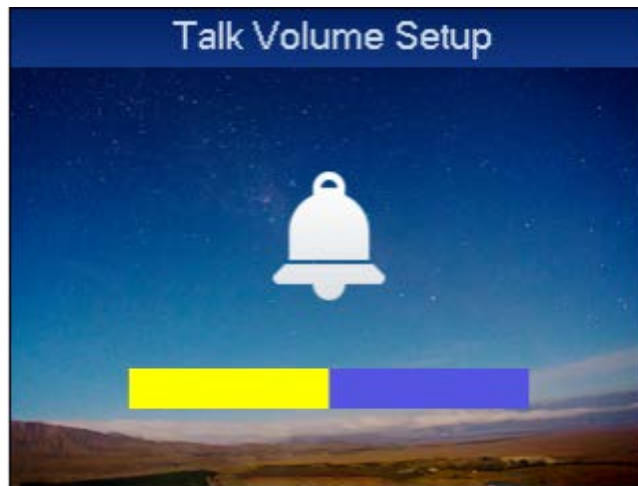


Step 2 Enter old password, new password, confirmation password, and then tap **OK**.

#### 4.4.1.3 Setting Volume

Step 1 On the local setup screen, select **Talk Volume Setup**, and then tap **OK**.

Figure 4-17 Volume setup



Step 2 Tap ↑ or ↓, to adjust volume.

#### 4.4.1.4 Restoring Default Settings

Step 1 On the local setup screen, select default, and then tap **OK**.

Step 2 Select **YES** and then tap **OK** to restore.

### 4.4.2 Configuring Network

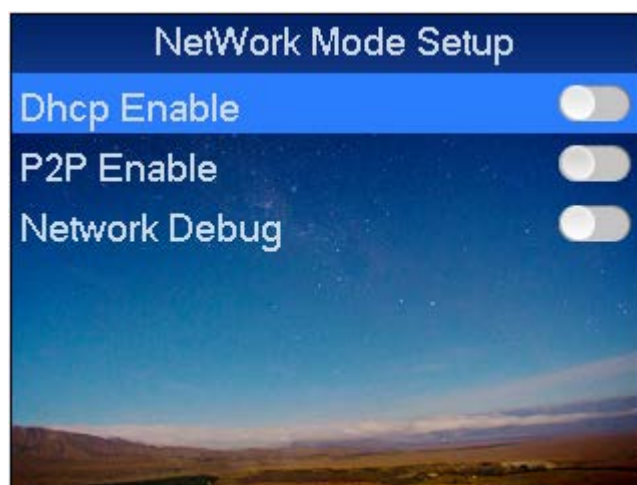
#### 4.4.2.1 Setting Network Mode

Step 1 On the main menu, select **Settings**, and then tap **OK**.

Step 2 Select **Network Setup** and tap **OK**.

Step 3 Select **Network Mode Setup** and tap **OK**.

Figure 4-18 Network mode setup



Step 4 Tap ↑ or ↓, to select network mode and enable it, and then tap **OK**.

Tap **OK** again to close network connection mode.



Network Type	Note
DHCP	Auto gets IP function. When you enable DHCP IP address, subnet mask and default gateway cannot be set.
P2P Enable	No need to apply for dynamic domain, mapping port or deploying server.

### 4.4.2.2 Setting IP

Step 1 On the **Network Setup** screen, select **IP Setup**, and then tap **OK**.

Figure 4-19 IP setup



Step 2 Modify IP, subnet mask and gateway, and then tap **OK**.

### 4.4.3 Setting Device Mode

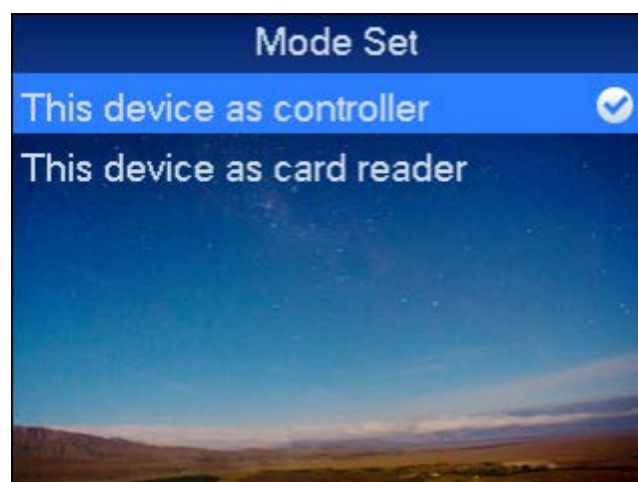
The Device supports two Device modes, which are controller mode and card reader mode.

- **This device as controller:** The Device is used as a controller to control access.
- **This device as card reader:** The Device is used as a card reader. If you need to control door access, it must be connected to a controller.

Step 1 On the **Settings** screen, select mode setup, and then tap **OK**.

Step 2 Select the work mode, and tap **OK**.

Figure 4-20 Mode setup



Step 3 Tap ↑ or ↓ to select work mode, and then tap **OK**.

After selection is successful, a ⚙ will be shown next to work mode.

## 4.4.4 Restarting Device

Step 1 On the main menu, select **Settings** and then tap **OK**.

Step 2 Select **Reboot** and then tap **OK**.

Step 3 Select **YES**, and then tap **OK** to restart the Device.

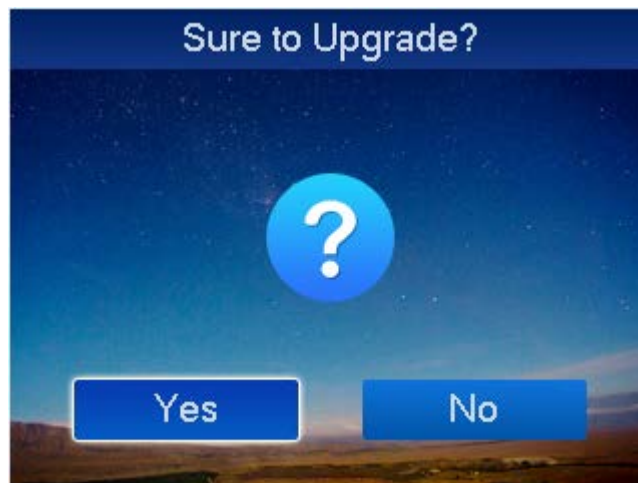
## 4.4.5 Updating System

Step 1 Rename update file as "AutoUpDate.bin", save it in USB root directory, and then insert USB into the Device.

Step 2 On the main menu, select **Settings**, and then tap **OK**.

Step 3 Select **USB Upgrade** and tap **OK**.

Figure 4-21 Update through USB



Step 4 Use ↑ and ↓ to select **Yes**, and then tap **OK**.

The system starts to update, and it will restart automatically when updating is complete.

## 4.5 System Information

You can view card swiping information, alarm information and local information.

### 4.5.1 Viewing Unlock Records

Step 1 On the main menu, select **Info**, and then tap **OK**.

Step 2 Select unlock records, and then tap **OK**.

Figure 4-22 Unlock record



Step 3 Tap ↑ or ↓ to select view method.

- View all unlock history  
Select **View all unlock records**, and then tap **OK**. You can view unlock record information, including time, card number., mode and status.
- View record by period  
1) Select **View record by period**, and then tap **OK**.

Figure 4-23 View records by period



- 2) Enter the start time and end time, and then tap **OK**.



A maximum of 150,000 records can be shown.

## 4.5.2 Viewing Alarm Records

Step 1 On the **Info** screen, select alarm record, and then tap **OK**.

Figure 4-24 Alarm records



Step 2 Tap ↑ or ↓ to select view method.

- View all alarm records  
Select **View all alarm records**, and then tap **OK** to view alarm type, alarm time and more.
- View record by period  
1) Select **View record by period**, and then tap **OK**.

Figure 4-25 View records by period



- 2) Enter start time and end time and tap **OK**.



A maximum of 1024 records can be displayed.

### 4.5.3 Viewing Device Information

You can view basic device information such as device version, MAC and IP.

Step 1 On the main menu, select **Info**, and then tap **OK**.

Step 2 Select **Local Info** and tap **OK**.

## 4.5.4 Exporting/Importing

You can export unlock records and alarm records to USB, and export or import configurations through USB.

**Step 1** On the main menu, select **Info**, and then tap **OK**.

**Step 2** Select **USB Export** and tap **OK**.

Figure 4-26 USB export



**Step 3** Tap  $\uparrow$  or  $\downarrow$  to select the item you want to export or import.

Table 4-4 Description of USB export

Parameter	Description
Export all unlock records	Select <b>Export all unlock records</b> , and tap <b>OK</b> .
Export unlock records by period	1. Select <b>Export unlock records by period</b> , and tap <b>OK</b> . 2. Enter <b>Start time</b> and <b>End time</b> , tap <b>OK</b> .
Export all alarm records	Select <b>Export all alarm records</b> , tap <b>OK</b> .
Export alarm records by period	1. Select <b>Export alarm records by period</b> , and tap <b>OK</b> . 2. Enter <b>Start time</b> and <b>End time</b> , tap <b>OK</b> .
Export configuration	Select <b>Export configuration</b> and tap <b>OK</b> .
Import configuration	Select <b>Import configuration</b> and tap <b>OK</b> .

# Appendix 1 Cybersecurity Recommendations

## **Mandatory actions to be taken for basic device network security:**

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

Please refer to the following suggestions to set passwords:

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

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

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

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

### **1. Physical Protection**

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

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

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

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

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

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

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

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

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

### **6. Enable HTTPS**

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

### **7. MAC Address Binding**

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

the risk of ARP spoofing.

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

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

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

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

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

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

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

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

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

#### **11. Secure Auditing**

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

#### **12. Network Log**

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

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

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

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