Access Control Terminal

User Manual

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope

rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Dangers

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions

- This equipment is not suitable for use in locations where children are likely to be present.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).

- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Available Models

The access control terminal contains the following models:

Product name: Access control terminal

Contents

Chapter 1 Appearance

Refer to the following contents for detailed information of the access control terminal:

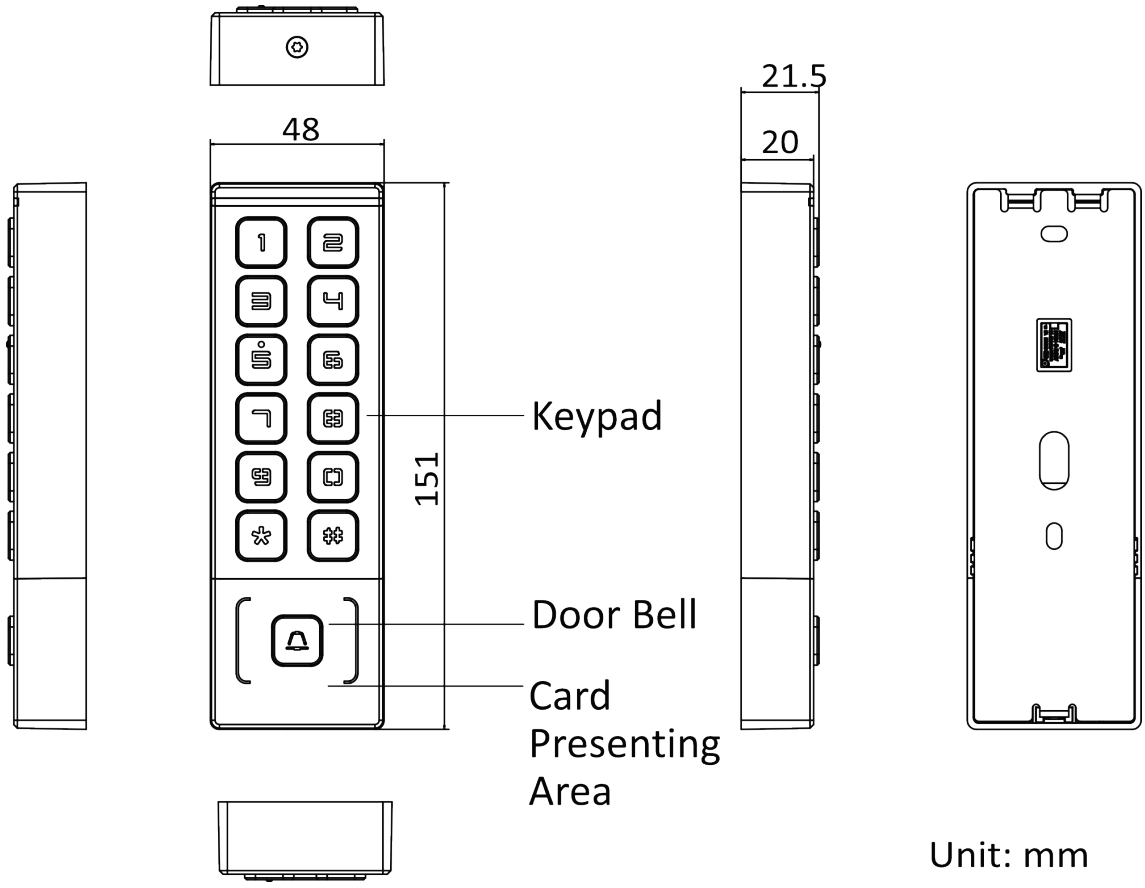

Figure 1-1 Access Control Terminal

Note

The pictures here are for reference only.

Chapter 2 Installation

2.1 Installation Environment

- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.
- • Please prepare the following tools and accessories: screwdriver (self purchased), screws, cables, and adapters (self purchased).

2.2 Surface Mounting

Steps

1. Attach the installation sticker to the wall about 1.45 m from the ground or the location where the device needs to be installed, and punch the hole according to the hole location (hole 1 and hole 2) on the sticker and wall.

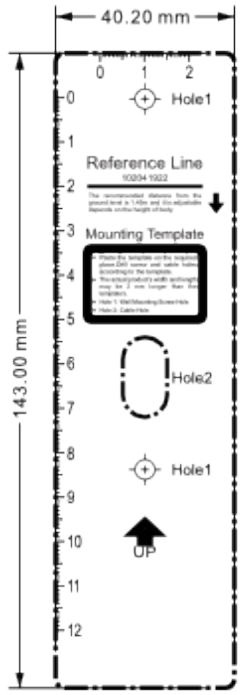

Figure 2-1 Installation Sticker

2. Insert the plastic sleeve of the provided expansion screw into the punched hole.

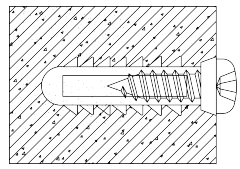

Figure 2-2 Insert Plastic Sleeve

3. Make sure the cables are threaded through the hole.

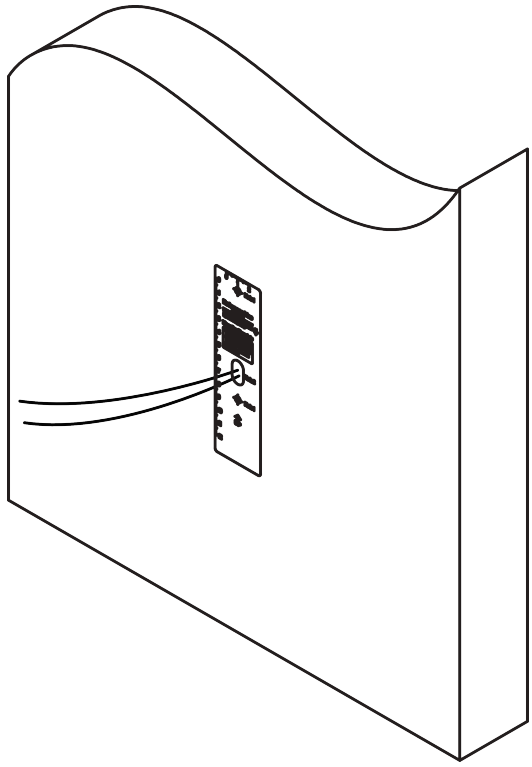

Figure 2-3 Thread Cables

4. Secure the mounting plate on the gang box with two supplied screws (PA4X25-SUS).

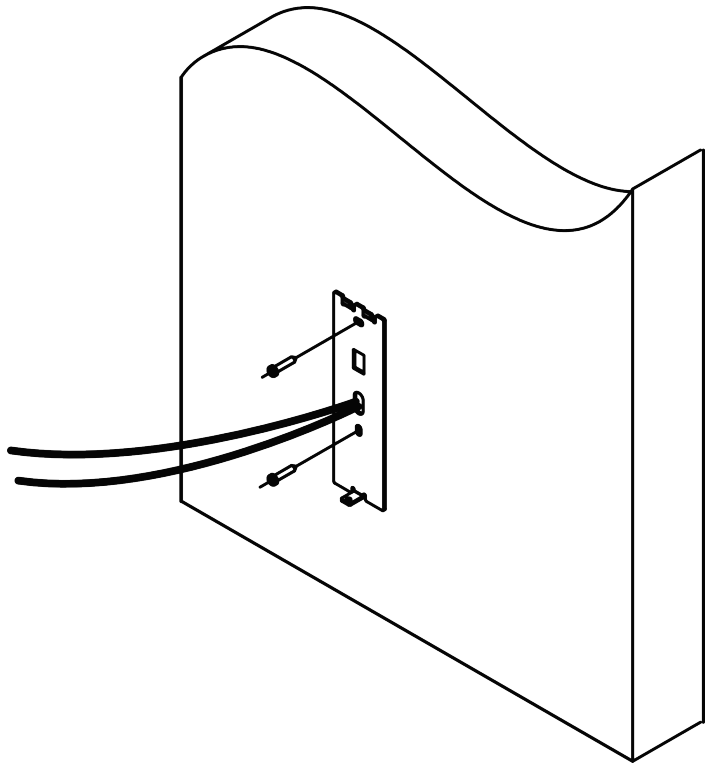

Figure 2-4 Secure Mounting Plate

5. Complete the wiring. See the wiring diagram for details.

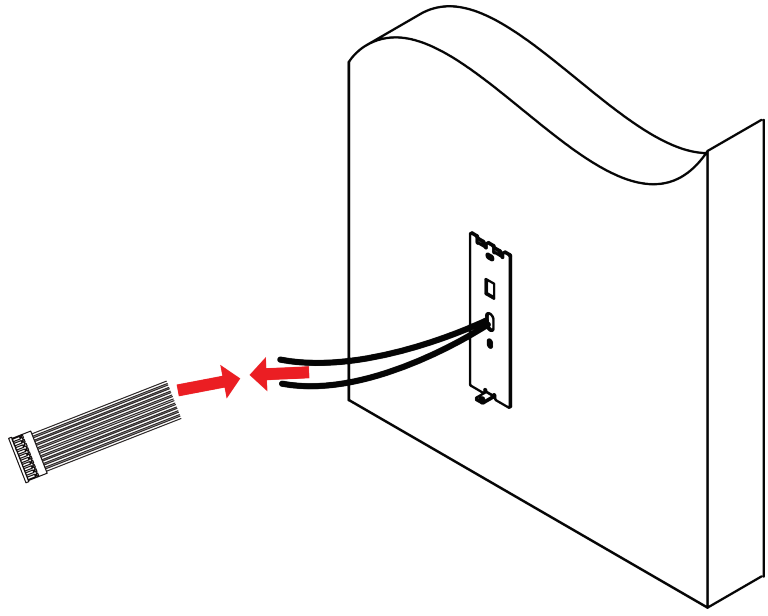

Figure 2-5 Complete Wiring

6. Hang the device into the plate from top to bottom. Secure the device on the mounting plate with 1 supplied screw (SC-KM3X6-T10-SUS).

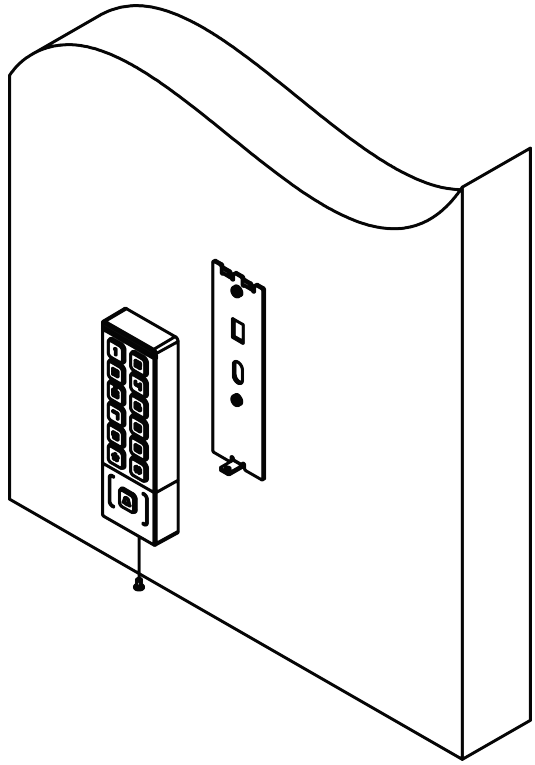

Figure 2-6 Secure Device

Chapter 3 Device Wiring

3.1 External Device Wiring

Wire the external device.

The wiring diagram is as follows.

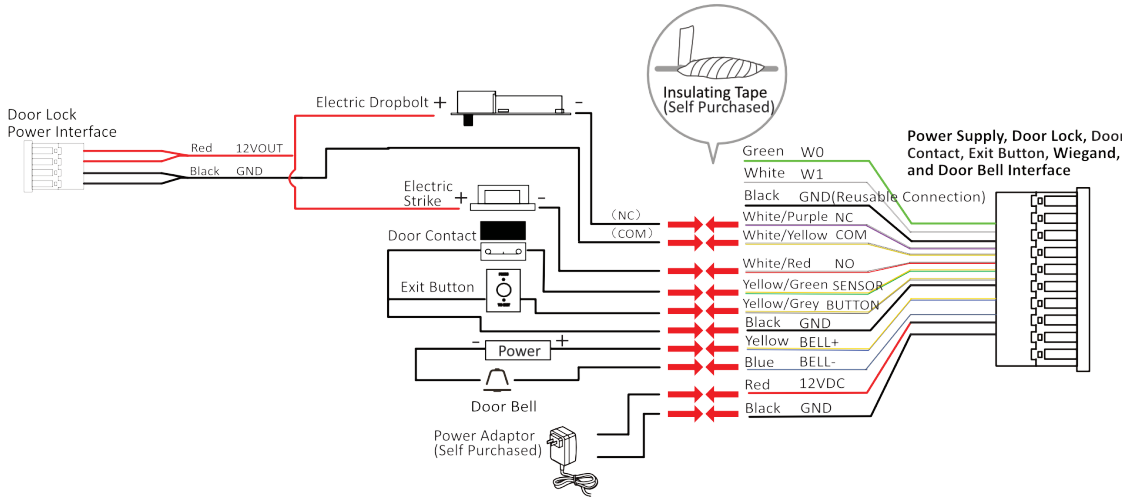

Figure 3-1 External Device Wiring

Note

- Use a DC 12 V power supply. Do not connect the device directly to the 220 V mains.
- The suggested external power supply for door lock is 12 V, 1 A.

Chapter 4 Operate on the Device

4.1 Common Commands

Table 4-1 Common Commands Description

Module	Operation	Command	Description
Activate Device	Activate	[*][0][#] [Programming Password (6 to 8 Digits)] [Repeat Programming Password (6 to 8 Digits)] [#]	The 6 to 8 digits programming password cannot all be 0.
Programming Mode	Enter Programming Mode	[Programming Password (6 to 8 Digits)] [*][0][#]	/
	Go back to Programming Mode	[*]	/
	Exit Programming Mode	[*] [#]	The device will automatically exit the programming mode after 30s of no operation.
	Change Programming Password	[00] [New Programming Password (6 to 8 Digits)] [Repeat New Programming Password (6 to 8 Digits)] [#]	/
Add Door Opening Credential	Set Door Opening Password	[03] [Door Opening Password (4 to 8 Digits)] [Repeat Door Opening Password (4 to 8 Digits)] [#]	/
	Add User Card	[01] [User Code (4 Digits)](Optional) [Swipe Card]...	If you choose to add a user code, you can

Module	Operation	Command	Description
			save the added card to the user code location.
	Delete User Card	[02] [Swipe Card]...	/
	Add User Cards in Batch	[01] [User Code (4 Digits)](Optional) [Swipe Card 1][Swipe Card 2][Swipe Card 3]...	/
	Delete User Cards in Batch (Method 1)	[02] [Swipe Card 1] [Swipe Card 2][Swipe Card 3]...	/
	Delete User Cards in Batch (Method 2)	[15] [Programming Password (6 to 8 Digits)] [#]	/
	Delete User Code	[02] [User Code] [#]	/
	Delete User Codes in Batch	[02] [User Code] [#] [User Code] [#]...	/

4.2 Basic Commands

The device needs to be activated before it can be used. After activating, the device can be at two modes: normal mode and programming mode. After entering programming mode, the device can be operated by commands.

4.2.1 Activation

Command

Activate: [*][0][#] [Programming Password (6 to 8 Digits)] [Repeat Programming Password (6 to 8 Digits)] [#].

Note

The 6 to 8 digits programming password cannot all be 0.

Prompts Description

Indicator	Prompt Audio	Description
Light is solid green.	The buzzer rings for 3 s.	Activated , and in normal mode (not programming mode).
Light flashes red slowly for 3 times.	The buzzer rings for 5 times quickly.	Activating failed.
Light flashes orange slowly.	/	Inactivated

4.2.2 Enter and Exit Programming Mode

There are two ways to enter the programming mode: enter the command , or directly swipe the functional card (including management card, adding card and deleting card).

Programming Mode Command

Enter Programming Mode: [Programming Password (6 to 8 Digits)] [*][0][#].
Exit Programming Mode: [*] [#].
Change Programming Password: [00] [New Programming Password (6 to 8 Digits)] [Repeat New Programming Password (6 to 8 Digits)] [#].

Table 4-2 Prompts Description

Indicator	Prompt Audio	Description
Light is solid green for 2 s.	The buzzer rings 2 times quickly.	Enter Programming Mode
Light is solid red for 2 s.	The buzzer rings 3 times slowly.	Entering Programming Mode failed
/	The buzzer beeps 1 sound.	Swipe Card and Press Button Prompt Audio
/	The buzzer rings 2 times.	Exit due to timeout.

Note

- After 5 consecutive programming password input errors, the device will enter a locked status. After waiting for 1800 s or after the device losing power time cleared, you can enter the programming password again to enter the programming mode. Enter the programming password in the locked status, the indicator will be solid orange for 2 s, and the buzzer will ring 5 times quickly, indicating that it cannot enter the programming mode.
- In programming mode, "*" represents a fallback to programming mode without entering a command, and "# "Indicates the end or completion of a command.
- In programming mode, you need to press "*" to exit the batch addition and deletion mode.

Swipe Functional Card

After swiping the functional card in the card swiping area, you can directly enter the programming mode. See ***Set Functional Card*** for adding details.

4.3 Other Common Commands

4.3.1 Open Door

There are two ways to open door: enter the password, or swipe user card.

Prompts Description

Indicator	Prompt Audio	Description
Light is solid green for 2 s.	The buzzer rings 2 times quickly.	Authenticated
Light is solid red for 2 s.	The buzzer rings 3 times slowly.	Authentication failed.
/	The buzzer beeps 1 sound.	Swipe Card and Press Button Prompt Audio
/	The buzzer rings 2 times.	Exit due to timeout.

Set Door Opening Password

You can set the door opening password and open door by entering the door opening password.

Command

Command of Setting Door Opening Password: [03] [Door Opening Password (4 to 8 Digits)] [Repeat Door Opening Password (4 to 8 Digits)] [#].

Note

The 4 to 8 door opening password cannot all be 0. If all of them are 0, the door opening password function will be disabled.

Add/Delete User Card

Command

Add User Card: [01] [User Code (4 Digits)] (Optional)[Swipe Card]...

Add User Card in Batch:[01] [User Code (4 Digits)](Optional) [Swipe Card 1][Swipe Card 2][Swipe Card 3]...

Note

- If you enter a user code before adding a card, the location of the added user card is under this code ID, and if you do not enter the user code, the added card has no fixed position.
- The user code format is 4 digits and the range is from1 to 1000. If the entered code content and format is incorrect, the addition fails, and the current adding command ends.

Delete User Code: [02] [User Code] [#].
Delete User Code in Batch: [02] [User Code] [#][User Code] [#]...
Delete User Card: [02] [Swipe Card].
Delete User Card in Batch (Method 1): [02] [Swipe Card 1] [Swipe Card 2][Swipe Card 3]...
Delete User Card in Batch (Method 2): [15] [Programming Password (6 to 8 Digits)] [#].

4.3.2 Set Functional Card

Functional cards include management card, adding card and deleting card.

Note

Functional cards cannot be used to open door, but are only equivalent to a certain command.

Management Card

Swipe the management card in the standby status: it means that the device directly enters the programming mode, and there is no need to enter the command to enter the programming mode.
Command of Adding Management Card: [04] [Swipe Card].
Command of Deleting Management Card: [05][#].
Command of Adding Management Card, Adding Card and Deleting Card at Once: [10] [Swipe Management Card][Swipe Adding Card] [Swipe Deleting Card].

Note

After swiping the management card to enter the programming mode, if the device is not operated for 30 s, it will exit programming mode. Swipe twice in 3 seconds to switch door contact settings. When switching the door contact, the buzzer ringing 8 times slowly means that the mode is switched to remain closed, and the buzzer ringing 8 times quickly means that the mode is switched to remain open.

Adding Card

Swipe the adding card in the standby status: it means that the device directly enters the programming mode, and enters the [01] command (adding command).
For example, if you need to add a user card, you can swipe the adding card and then swipe a user card when the device is in standby status.

Command of Adding Adding Card: [06] [Swipe Card].
Command of Deleting Adding Card: [07][#].

Note

After swiping the adding card to enter the programming mode, if the device is not operated for 30 s, it will exit programming mode.

Delete Card

Swipe the deleting card in the standby status: it means that the device directly enters the programming mode, and enters the [02] command (deleting command).
For example, if you need to delete a user card, you can swipe the deleting card and then swipe a user card when the device is in standby status.
Command of Adding Deleting Card: [08] [Swipe Card].
Command of Deleting Deleting Card: [09][#].

Note

After swiping the deleting card to enter the programming mode, if the device is not operated for 30 s, it will exit programming mode.

4.4 Advanced Commands

4.4.1 Set Door Parameters

The door opening time, door opening timeout, door contact type and exit button type can be set by command.

Command: [11] [Data Bit 1] [Data Bit 2] [Data Bit 3] [Data Bit 4] [#].

Data Bit 1: Indicates the door opening time, which is a three digits number from 000 to 255. The unit is second. If the door opening time is 3 s, the data bit 1 is set to 003. The default door opening time is 5 s.

Data Bit 2: Indicates the door opening timeout, which is a two digits number. The unit is second. If the door is opened beyond this setting time, the device will alarm and ring for 10 s. If you enter "50", the alarm time for door opening timeout will be 50 s. The default door opening timeout is 30 s.

Data Bit 3: Indicates the type of door contact, which is a one digit number. "0" means remaining closed, and "1" means remaining open. It is remaining closed by default.

Data Bit 4: Indicates the type of exit button, which is a one digit number. "0" means remaining closed, and "1" means remaining open. It is remaining closed by default.

4.4.2 Set Voice Parameters

You can set whether to enable the button sound and authentication prompt audio through the command.

Command: [12] [Data Bit 1] [Data Bit 2] [#].

Data Bit 1: Indicates whether to enable the button sound, which is a one digit number. "0" means the button sound is disabled, and "1" means the button sound is enabled. It is enabled by default.

Indicates whether to enable the authentication prompt audio, which is a one digit number. "0" means the authentication prompt audio is disabled, and "1" means the authentication prompt audio is enabled. It is enabled by default.

Note

The disabling only takes effect in the normal mode, not in the programming mode.

4.4.3 Set NFC

You can set whether to enable NFC function through the command.

Command: [13] [Data Bit 1] [#].

Data Bit 1: “0" means disabling NFC function, and "1" means enabling NFC function. It is enabled by default.

Note

Only some models support this function, please refer to the actual product.

4.4.4 Set Card Reader Wiegand Mode

The Wiegand mode of card reader can be set by command.

Command: [14] [Data Bit 1] [#].

Data Bit 1: "0" means Wiegand 26 mode, and "1" means Wiegand 34 mode. The default mode is Wiegand 34.

4.4.5 Restore to Default Settings

You can perform commands or press button to restore to default settings.

Command 1: [16] [Programming Password (6 to 8 Digits)]] [#] (Only Restore Data Except User Cards Data).
Command 2: Press and hold the "*" button for 5 seconds within 30 seconds of powering on.

4.4.6 Restart Device

You can restart the device by command.

Command: [17] [Programming Password (6 to 8 Digits)] [#].

4.4.7 Restore to Factory Settings

You can restore the device to factory settings by command.

Command: [18] [Programming Password (6 to 8 Digits)]] [#] (Restore All User and Default Data).

Chapter 5 Configure the Device via the Mobile Web

The device supports activation and operation through device-side commands. It also supports activation and operation on the mobile phone by connecting to the device hotspot. (If it is activated through the mobile phone, it cannot be operated through the device. If it is activated through the device, you can operate on the mobile phone.）

5.1 Activate via Mobile Web

You can activate the device via mobile web.

Steps

1. After the device is powered on, the hotspot is enabled by default. Search for and connect to the device hotspot on your phone.

   Note

   - Device hotspot name is AP_ Serial No., and initial password of device hotspot is Serial No. After restarting or switching from non-AP mode to AP mode after activation (press and hold the number button 5 to switch AP mode), the hotspot password will be changed to the activation password.
   - You can log in to the mobile web client only when the device is in AP mode.

2. Open the browser address bar of the mobile phone and enter 192.168.8.1 to enter the activation interface.
3. Set the activation password and confirm it.

   Note

   - The password must be 8 to 16 characters long.
   - The password must be composed of two or more combinations of numbers, lowercase letters, uppercase letters, and special characters.
   - The password cannot contain the user name, 123, admin, 4 or more consecutive digits in increments or decrement, or the same symbol.

4. Tap **Activate Device**.

5.2 Login

You can log in via mobile browser.

Note

- Parts of the device models support this function.
- Make sure the device is activated.

Enter the device IP address in the address bar of the mobile browser and press **Enter** to enter the login page.

Enter the device user name and the password. Tap **Login**.

5.3 Quick Operation via Web Browser

5.3.1 Time Settings

You can set the time zone, time synchronization mode, and the displayed time.

Device Time

Display the device time in real time.

Time Zone

Select the device located time zone from the drop-down list.

Time Synchronization Mode

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Phone Time** to synchronize the device time with the phone's time.

DST

You can enable DST, set and view the DST start time, end time and bias time.

Click **Next** to save the settings.

5.4 Overview

You can view the door status, network status and basic information, and set person management, authentication settings, and door parameters via shortcut entry.

Function Descriptions:

Door Status

/ / /

The door status is open/closed/remaining open/remaining closed. You can tap to select open/closed/remaining open/remaining closed status according to your actual needs.

Shortcut Entry

You can set person management, authentication settings, and door parameters via shortcut entry.

Network Status

You can view the connected status of wireless network and Guarding Vision.

Basic Information

You can view the model, serial No. and firmware version.

5.5 Configuration

5.5.1 View Device Information

View the device name, language, model, serial No., version, number of channels, IO input number, number of alarm input and output, Mac address, factory information and device capacity, etc.

Tap → **System Settings** → **Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, number of channels, IO input number, number of alarm input and output, Mac address, factory information and device capacity, etc.

5.5.2 Time Settings

Set the time zone, time sync. mode, and displayed time.

Tap → **System Settings** → **Time Settings** to enter the settings page.

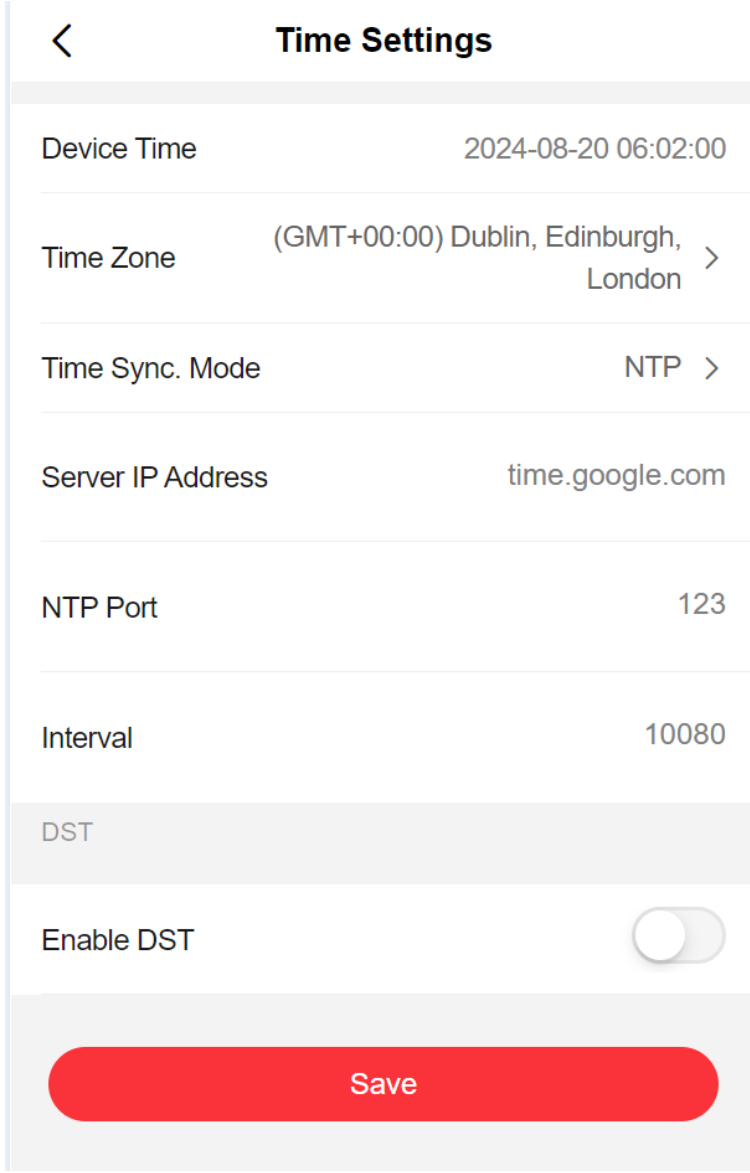

Figure 5-1 Time Settings

Tap **Save** to save the settings.

Time Zone

Select the time zone where the device is located from the drop-down list.

Time Sync. Mode

Manual

You can set the device time manually, or enable **Sync. with Phone Time**.

NTP

Set the NTP server's IP address, port No., and interval.

5.5.3 Set DST

Steps

1. Tap ☰ → **System Settings** → **Time Settings** , to enter the settings page.

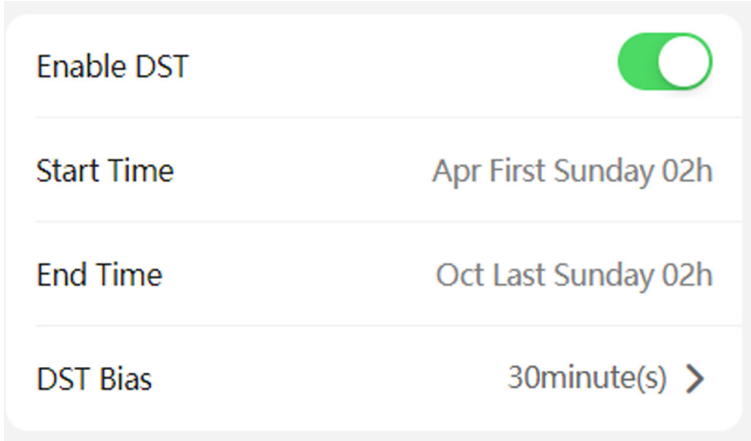

Figure 5-2 DST

2. Tap **Enable DST**.
3. Set the start time, end time, and DST bias.
4. Tap **Save**.

5.5.4 Change Administrator's Password on Mobile Web

You can change administrator's password.

Steps

1. Tap ☰ → **User Management** → **admin** to enter the settings page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. Tap **Save**.

Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using 8 to 16 characters, including at least two kinds of following characters: upper case letters, lower case letters, numbers, and special characters, and do not contain following characters in the password: the user name, 123, admin (case insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters) in order to increase the security of your product. We recommend you

change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5.5.5 Network Settings

Set Device Hotspot

Set the device hotspot, and mobile phone can connect to the device to enter the mobile browser.

Steps

1. Tap → **Network Settings** → **Device Hotspot** .
2. You can enable device hotspot and view the hotspot name.

   Note

   By default, the hotspot name is the AP_Device Serial No.
3. Tap **Save**.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Tap → **Device Access** → **Guarding Vision** to enter the settings page.

   Note

   Guarding Vision is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.
2. Check **Enable** to enable the function.
3. You can view **Network Connection Status** and **Account Linkage Status**.
4. Tap **Save** to enable the settings.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap → **Access Configuration** → **Wiegand Settings** .

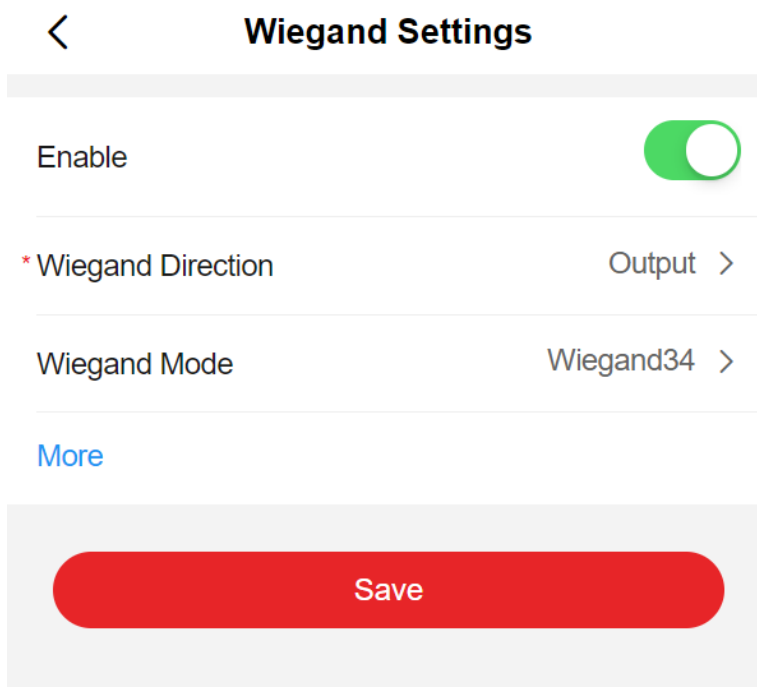

Figure 5-3 Wiegand Page

2. Enable **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

Note

The device can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.

4. Tap **More**, and you can set **Time Interval** and **Pulse Width**.
5. Tap **Save** to save the settings.

5.5.6 User Management

You can add, edit, delete, and search users via mobile Web browser.

Steps

1. Tap → **Person Management** to enter the settings page.

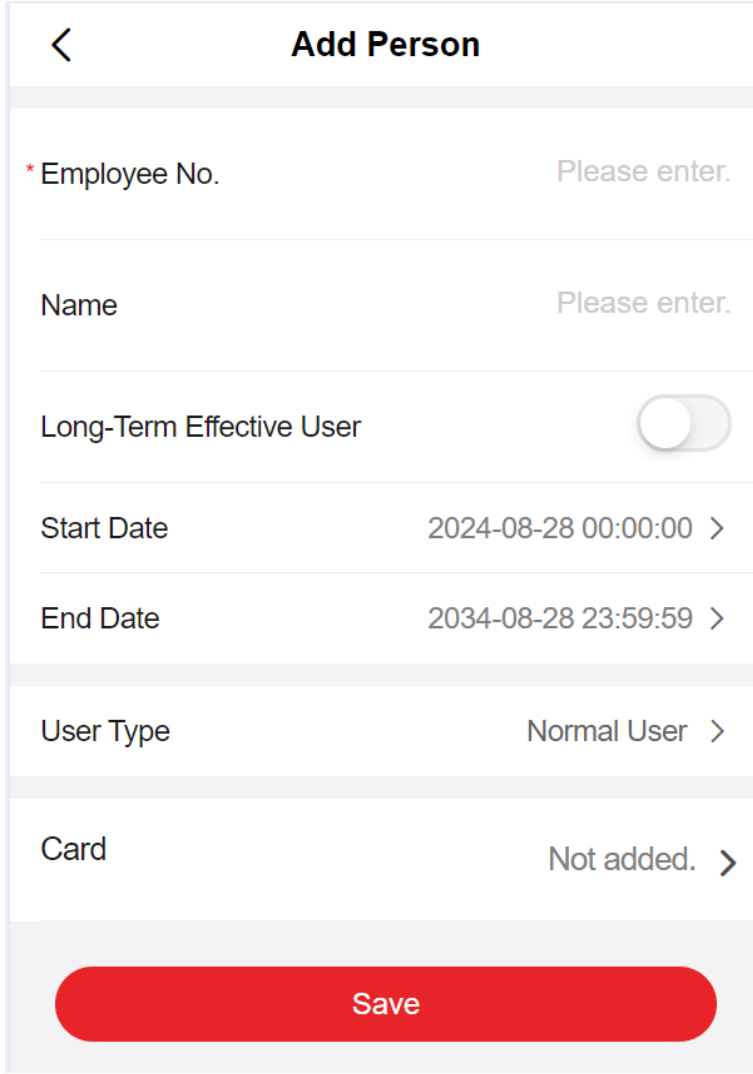

Figure 5-4 User Management

2. Add user.

1) Tap**+**.

2) Set the following parameters.

Employee No.

Enter the employee No. The Employee No. cannot be 0 or exceed 32 characters. It can be a combination of uppercase letters, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, English uppercase and lowercase letters and Chinese characters. The name is recommended to be within 32 characters.

Long-Term Effective User

Set the user permission as long-term effective, or set the start date and end date of user permission.

User Type

Select your user role.

Card

Add card. Tap **Card**, then tap **+**. Enter the card No. or swipe the card to read card No., and then select **Card Type**.

3) Tap **Save**.

3. **Optional:** Tap the user that needs to be edited in the user list to edit the information.
4. **Optional:** Tap the user that needs to be deleted in the user list, and tap to delete the user.
5. **Optional:** You can search the user by entering the employee ID in the search bar.

5.5.7 Search Event

Tap → **Search** to enter the page.

Enter the search conditions, including the event type, major type, sub type, employee No., card No., start time, and end time, and tap **Search**.

Note

Support searching for names within 32 digits.

5.5.8 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap → **Access Control** → **Authentication Settings** .

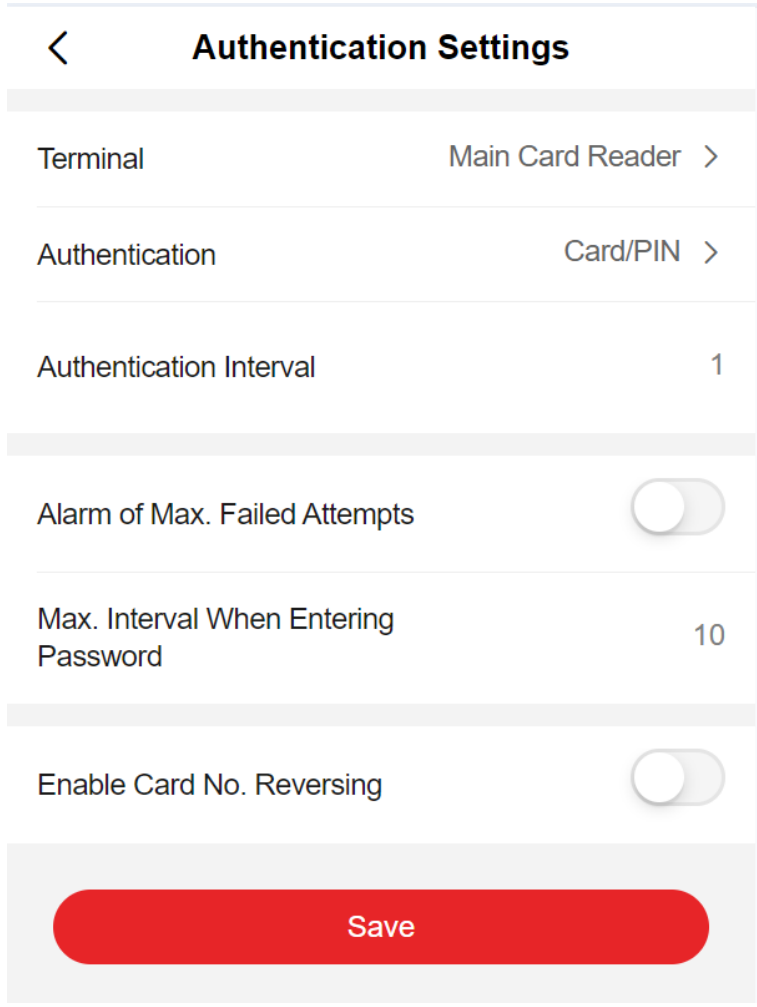

Figure 5-5 Set Authentication Parameters

2. Tap **Save**.

Terminal

Select the terminal.

Authentication Type

Select an authentication type according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Max. Authentication Failed Attempts Alarm/Max. Authentication Failed Attempts

After you enable **Max. Authentication Failed Attempts Alarm**, you can set **Max. Authentication Failed Attempts**. The device will automatically generate and report alarm events after the authentication failures exceed the configured attempts.

Max. Interval When Entering Password

You can set the Max. timeout period for password entry, after which the password input will be invalid.

Enable Card No. Reversing

If this function is enabled, the card reader will reverse the order of the card No. after reading them.

Set Door Parameters

Tap → **Access Control** → **Door Parameters** .

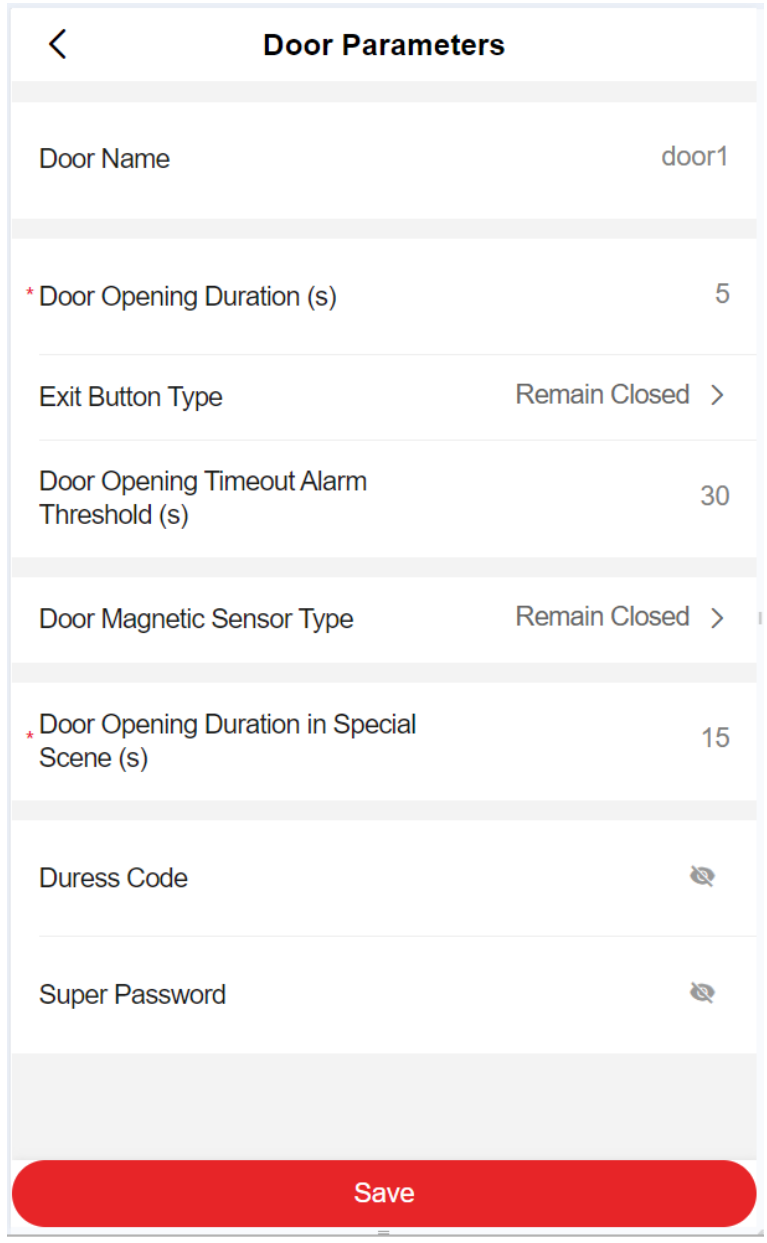

Figure 5-6 Door Parameters Settings

Tap **Save** to save the settings after the configuration.

Door Name

You can create a name for the door.

Door Opening Duration(s)

Set the door open duration.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Door Opening Timeout Alarm Threshold

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Magnetic Sensor Type

You can set the Door Magnetic Sensor Type as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Door Opening Duration in Special Scene(s)

The door contact can be enabled with appropriate delay after person with extended access needs swiping her/his card.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Note

The duress code and the super code should be different. And the digit ranges from 4 to 8.

Set Card Security

Tap → **Card Settings** to enter the settings page.

Set the parameters and tap **Save**.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

5.5.9 Upgrade and Maintenance

You can restart device, restore device parameters, and upgrade device.

Restart Device

Tap → **Restart** .

Tap **Restart** to restart the device.

Upgrade

Tap → **Upgrade** .

Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Default** .

Restore to Default Settings

The device will restore to the default settings, except for the device network parameters and the user information.

Restore to Factory Settings

All parameters will be restored to the factory settings. You should activate the device before usage.

5.5.10 View Online Document

Tap → **View Online Document** . Tap **View Online Document**, you can scan the QR code with your mobile phone for details.

Appendix A. Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the company website. Unless otherwise agreed, our company makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Trademarks Acknowledgment

All trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL OUR COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF

PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Appendix B. Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Note	Provides additional information to emphasize or supplement important points of the main text.

Appendix C. Dimension

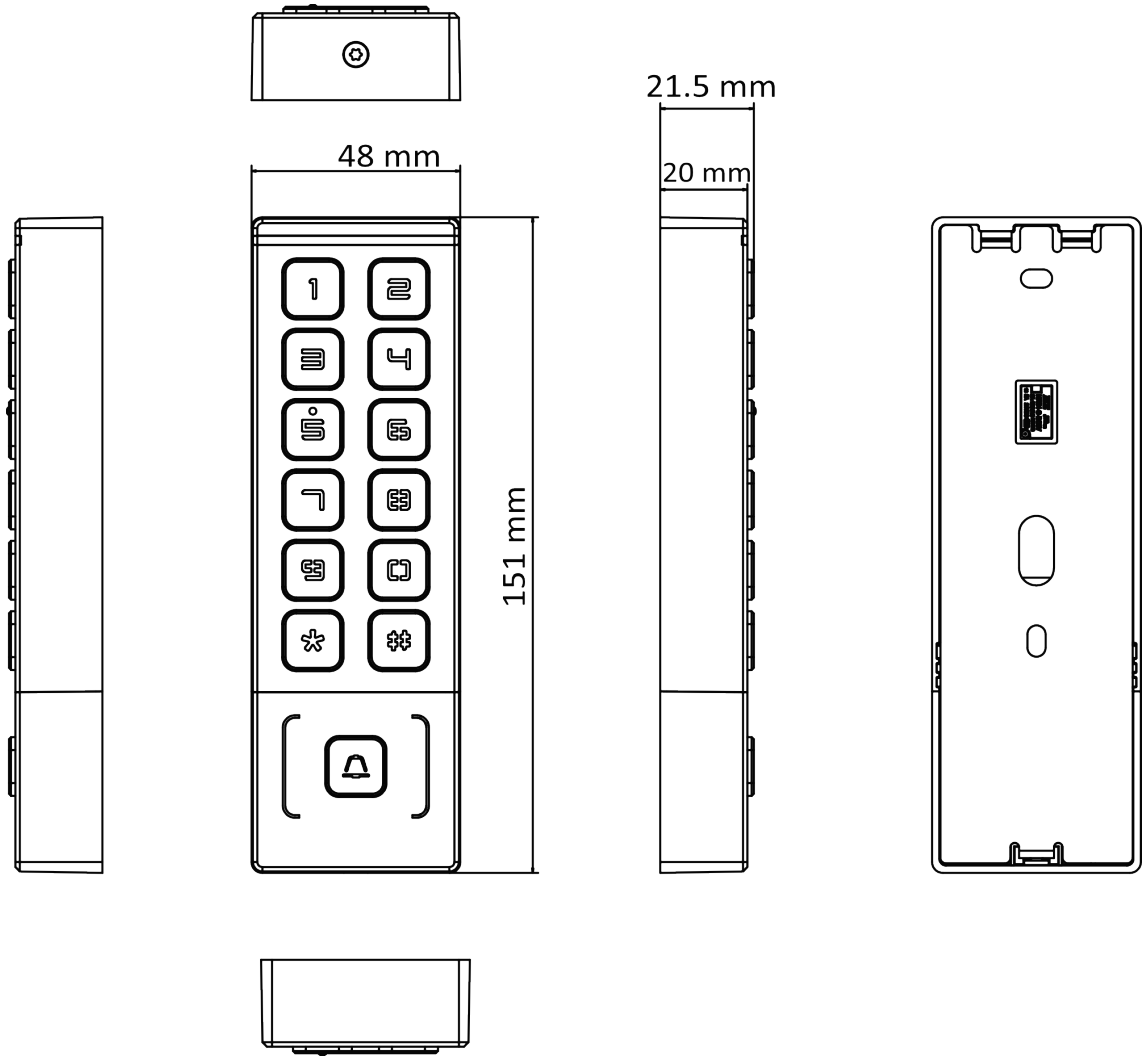

Figure C-1 Dimension

Note

The pictures here are for reference only.