

HIKVISION



Access Control Terminal

Quick Start Guide

Quick Start Guide

©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

This quick start guide is intended for users of the models below:

Series	Model
Standalone Access Control Terminal	DS-K1T105E/M
	DS-K1T105E/M-C (with Camera)
Optical IP-Based Fingerprint Access Control Terminal	DS-K1T200EF/MF
	DS-K1T200EF/MF-C (with Camera)
	DS-K1T201EF/MF
	DS-K1T201EF/MF-C (with Camera)

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that Product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. (“Hikvision”) reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

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 RE Directive 2014/53/EU, 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.

Use only power supplies listed in the user instructions:

Model	Manufacturer
KPL-040F-VI	Channel Well Technology Co Ltd.



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 **Warnings** and **Cautions**:

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

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

	
Warnings Follow these safeguards to prevent serious injury or death.	Cautions Follow these precautions to prevent potential injury or material damage.



Warnings

- 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.
- 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

- 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.

Table of Contents

1 Overview	3
1.1 Introduction	3
1.2 Main Features	3
1.2.1 Main Features of DS-K1T105 Series Model.....	3
1.2.2 Main Features of DS-K1T200/201 Series Model	4
2 Appearance	5
2.1 Appearance of DS-K1T105 Series Model	5
2.2 Appearance of DS-K1T200/201 Series Model.....	5
2.3 Appearance of Keys.....	6
3 Installation	8
3.1 Installation of DS-K1T105 Series Device	8
3.2 Installation of DS-K1T200/201 Series Device	9
4 Terminal Connection	11
5 Wiring Description	13
5.1 External Device Wiring Overview.....	13
5.2 The Wiring of External Card Reader.....	14
5.2.1 The Wiring of External RS-485 Card Reader.....	14
5.2.2 The Wiring of External Wiegand Card Reader	14
5.3 The Wiring of Electric Lock and Door Contact	15
5.3.1 The Wiring of Electric Lock.....	15
5.3.2 The Wiring of Door Contact	15
5.4 The Wiring of Exit Button.....	16
5.5 The Wiring of Alarm Input.....	16
5.6 The Wiring of External Alarm Device	17
5.7 Card Reader Connection	17
5.7.1 The Wiring of Wiegand	17
5.7.2 The Wiring of RS-485 Output	18
6 Activating Access Control Terminal	19
6.1 Activating via Device	19
6.2 Activating via SADP Software	20
6.3 Activating via Client Software	21
7 Basic Operation	24
7.2 User Management	25
7.2.1 Adding User.....	26

7.2.2 Managing User	27
7.3 Communication Settings	29
7.3.1 Network Settings	30
7.3.2 Serial Port Settings	30
7.3.3 Wiegand Settings	31
7.3.4 Wi-Fi Settings	32
7.4 System Settings	33
7.4.1 Setting System	34
7.4.2 Managing Data	35
7.4.3 Restoring Settings.....	36
7.4.4 Door Settings.....	37
7.4.5 Setting Camera	37
7.5 Time Settings.....	38
7.6 Upload/Download Settings	39
7.7 Testing	40
7.8 Log Query Settings	41
7.9 System Information	41
Appendix: Tips for Scanning Fingerprint.....	43

1 Overview

1.1 Introduction

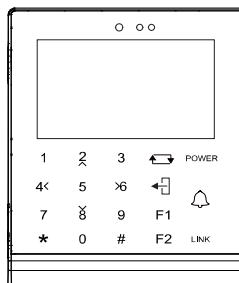


Figure 1-1 DS-K1T105 Series Standalone Access Control Terminal Front Panel

DS-K1T105 is a series of standalone access control terminal with picture capturing function. DS-K1T105 is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It supports face detection, smart card recognition TCP/IP communication method, Wi-Fi communication method, and supports offline operation.

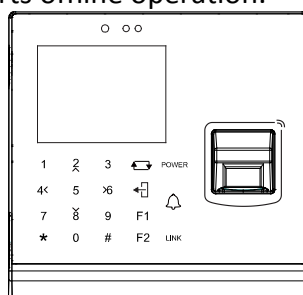


Figure 1-2 DS-K1T200/201 Series Fingerprint Access Control Terminal Front Panel

DS-K1T200/201 series are optical IP-based fingerprint access control terminal with multiple advanced technologies including fingerprint recognition, face detection, Wi-Fi, smart card recognition, LCD display screen, and picture capturing technology. It is designed with a 2.8-inch LCD display screen, and HD camera (2 MP optional). It is equipped with optical fingerprint recognition module (supporting 1:1 mode and 1:N mode), and supports offline operation.

1.2 Main Features

1.2.1 Main Features of DS-K1T105 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/IP) and Wi-Fi
- Face detection, picture capturing function and QR code authentication implemented by built-in camera (2 MP optional, only supports DS-K1T105E/M -C)
- Supports multiple door opening modes (card, card + password, exit button, etc.)

- Supports RS-485 communication for connecting to external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 valid card No., and Max. 300,000 access control events records storage
- Supports EM card reading (DS-K1T105E/E-C)
- Supports Mifare card reading, including card No. reading, & writing function (DS-K1T105M/M-C)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, and duress card alarm
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Data can be permanently saved after power-off

1.2.2 Main Features of DS-K1T200/201 Series Model

- Doorbell ringtone settings function
- Touch mode and blue light display technique for keypad
- Stand-alone settings for the terminal
- 2.8-inch LCD display screen
- Transmission modes of wired network (TCP/TP) and Wi-Fi
- Face detection, picture capturing function and QR code authentication implemented by built-in camera (2 MP optional, only supports DS-K1T200EF/MF-C and DS-K1T201EF/MF-C)
- Supports RS-485 communication for connecting external card reader
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller
- Max. 100,000 cards No., Max. 300,000 access control events records
- DS-K1T200 series device supports up to 9500 fingerprints storage; DS-K1T201 series device supports up to 5000 fingerprints storage
- Adopts the optical fingerprint module, supporting 1:N mode (fingerprint, card + fingerprint) and 1:1 mode (card + fingerprint)
- Supports multiple authentication modes (card, fingerprint, card + fingerprint, card + password, fingerprint + password, card + fingerprint + password, and so on.)
- Supports EM card reading (DS-K1T200EF/EF-C and DS-K1T201EF/EF-C support the function)
- Supports Mifare card reading, including card No. reading, and sector reading & writing (DS-K1T200MF/MF-C and DS-K1T201MF/MF-C support the function)
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, duress card alarm, and so on
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal
- Data can be permanently saved after power-off

2 Appearance

2.1 Appearance of DS-K1T105 Series Model

Please refer to the following content for detailed information of the DS-K1T105 series model.

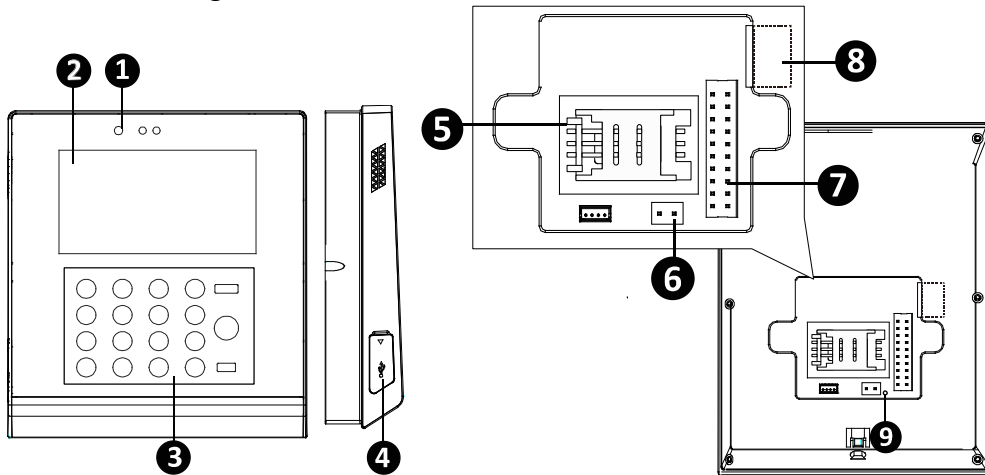


Figure 2-1 Appearance of DS-K1T105 Series Model

Table 2-1 Description of DS-K1T105 Series Model

No.	Description
1	HD Camera with 2 MP (only DS-K1T105E/M/ -C support)
2	2.8-Inch LCD Display Screen
3	Keypad
4	USB 2.0 Interface
5	PSAM Card Slot
6	Power Interface
7	External Wiring Terminals
8	Ethernet Port
9	Tampering Prevention Switch

2.2 Appearance of DS-K1T200/201 Series Model

Please refer to the following content for detailed information of DS-K1T200 series model

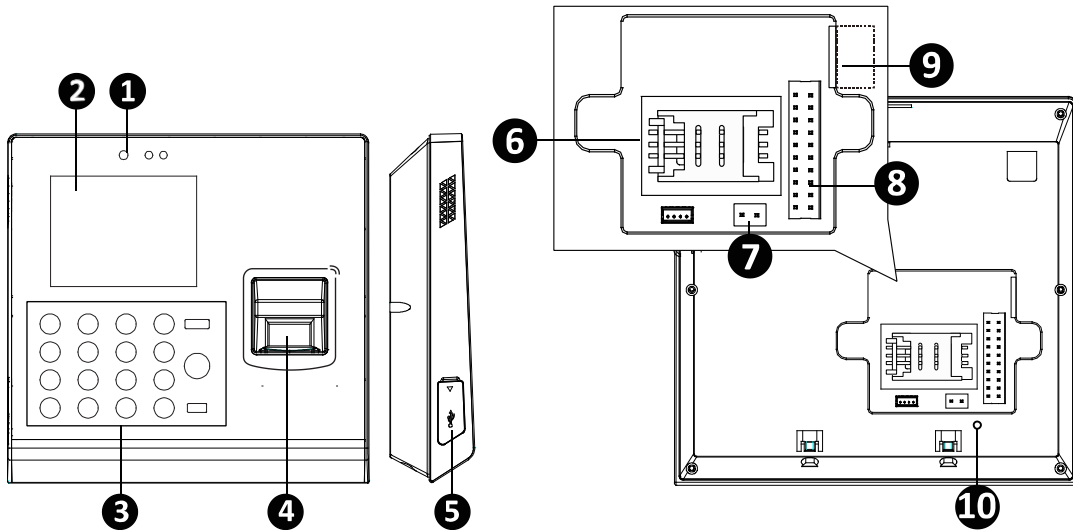


Figure 2-2 Appearance of DS-K1T200/201 Series Fingerprint Access Control Terminal

Table 2-2 DS-K1T200/201 Series Fingerprint Access Control Terminal Components

No.	Description
1	HD Camera with 2 MP (only DS-K1T200EF/MF -C support)
2	2.8-Inch LCD Display Screen
3	Keypad
4	Optical Fingerprint Reading Module
5	USB 2.0 Interface
6	PSAM Card Slot
7	Power Interface
8	External Wiring Terminals
9	Ethernet Port
10	Tampering Prevention Switch

2.3 Appearance of Keys

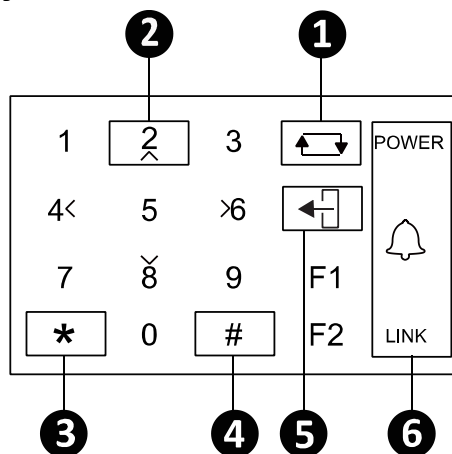



Figure 2-3 Appearance of Keys

Table 2-3 Description of Keys

No.	Description				
1	Editing Key: Click the key to enter/exit the editing status.				
2	Numeric Keys: Enter number in the textbox. Direction Keys: Select icons in the menu.				
3	Exiting Key: Click the key to exit the menu.				
4	Confirming Key: Click the key to confirm operations. Long-press the key to enter the login interface.				
5	Deleting Key: Click the key to delete contents in the textbox.				
6	Status Indicator: Indicator for power, ring, and connection status	POWER	Power Status	Solid Blue: Normal Power. Off : Power Exception.	
			Doorbell Ring		
		LINK	Normal Card/ Illegal Card	Normal Card: Solid Blue Illegal Card: Solid Red	
			Connection Status	Off: Network or Wi-Fi Disconnected.	
Solid Blue: Network or Wi-Fi connected, but client unarmed. Flicker Blue: Network or Wi-Fi connected, but client armed.					
		Flicker blue in the card reader mode.			
F1	Long-press the F1 key to enter the QR code authentication mode.				



In the Event Card Interact interface in the iVMS-4200 Client Software, choose the alarm output of Event Bell. You can connect a bell at the alarm output terminal. For details about configuring the Event Bell alarm output, see the *User Manual of iVMS- 4200 Client Software*.

3 Installation



Make sure that the wall is strong enough to withstand three times the weight of the device.

3.1 Installation of DS-K1T105 Series Device

Steps:

1. Install the 86 gang box into the wall.

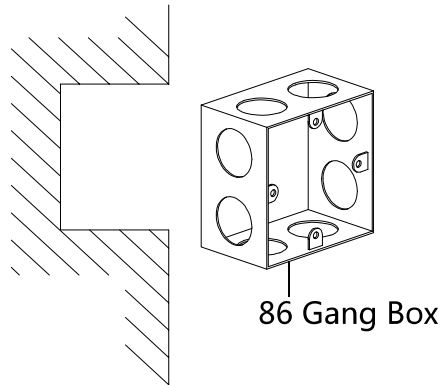


Figure 3-1 Install 86 Gang Box

2. Secure the device mounting plate on the gang box with two screws (supplied).

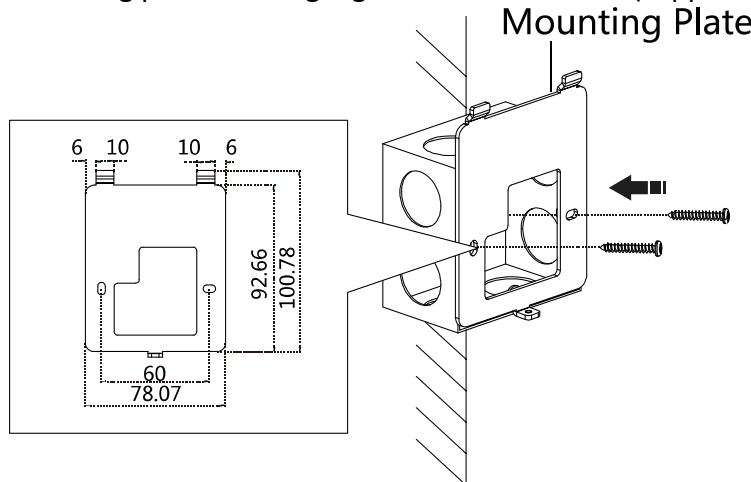


Figure 3-2 Secure Mounting Plate

3. Align the terminal with mounting plate.
4. Buckle the terminal on the plate.

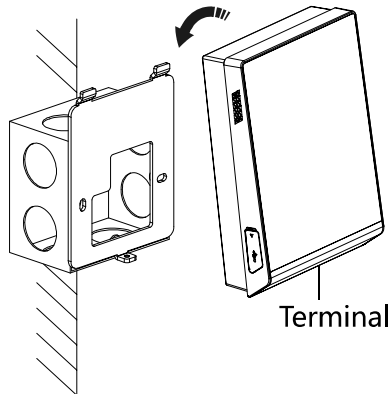


Figure 3-3 Buckle on Plate

5. Tighten the screw to fix the terminal on the mounting plate and complete the installation.

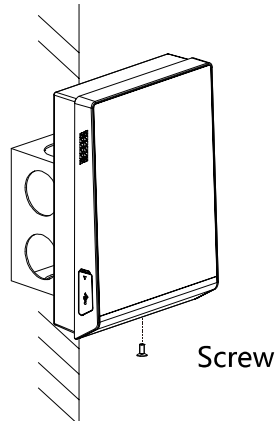


Figure 3-4 Tighten Screw

3.2 Installation of DS-K1T200/201 Series Device

Steps:

1. Install the 86 gang box into the wall.

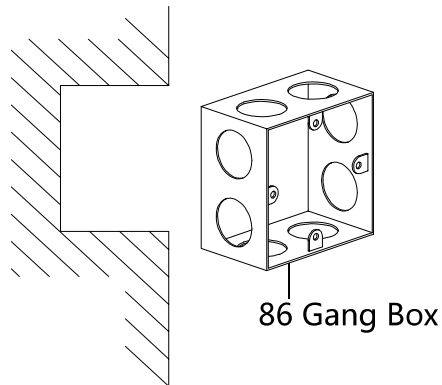


Figure 3-5 Install 86 Gang Box

2. Secure the device mounting plate on the gang box with two screws (supplied).

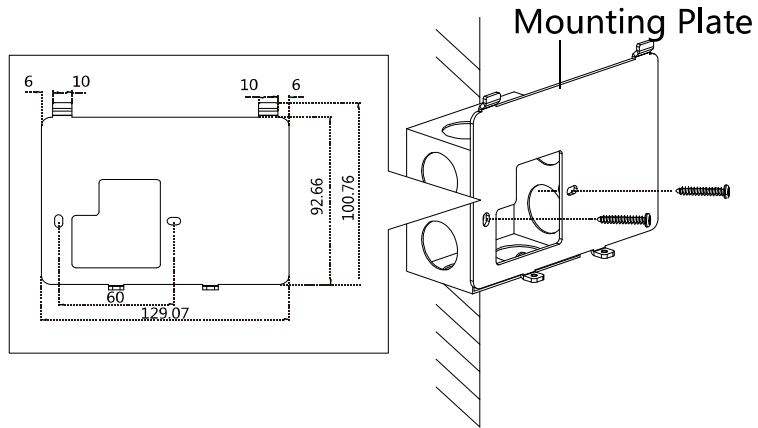


Figure 3-6 Secure Mounting Plate

3. Align the terminal with mounting plate.
4. Buckle the terminal on the plate.

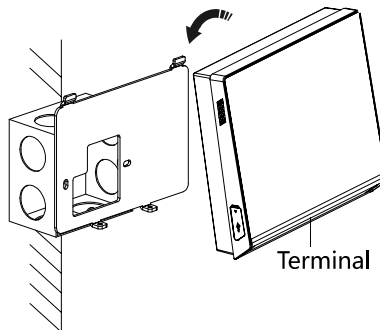


Figure 3-7 Buckle on Plate

5. Tighten the screws to fix the terminal on the mounting plate and complete the installation.

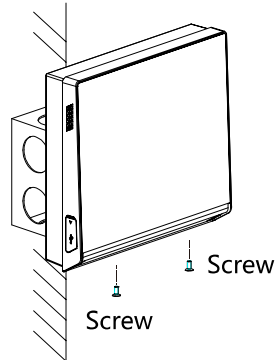


Figure 3-8 Tighten Screws

4 Terminal Connection

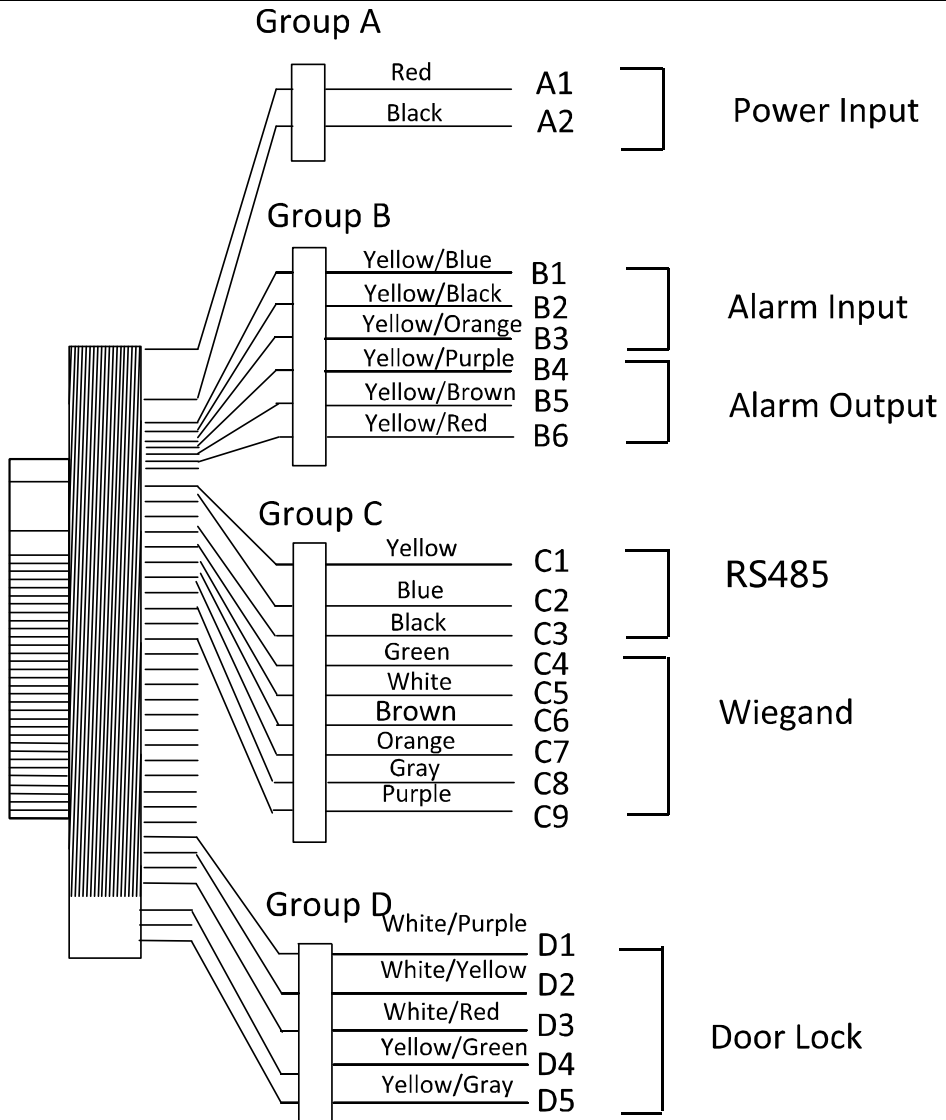


Figure 4-1 Terminal Diagram of Access Control Terminal

Table 4-1 Terminal Description

Line Group	No .	Function	Color	Terminal Name	Description
Line Group A	A1	Power Input	Red	+12V	12V DC Power Supply
	A2		Black	GND	GND
Line Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	GND
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Line Group C	C1	RS-485 Communication Port	Yellow	485 +	RS-485 Wiring
	C2		Blue	485 -	
	C3		Black	GND	
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Indicator of Card Reader Control Output (Valid Card Output)
	C7		Orange	WG_ERR	Indicator of Card Reader Control Output (Invalid Card Output)
	C8		Grey	TAMPER	Tampering Alarm Wiring
	C9		Purple	BUZZER	Buzzer Wiring
Line Group D	D1		Lock	White/Purple	NC
	D2	White/Yellow		COM	
	D3	White/Red		NO	
	D4	Yellow/Green		SENSOR	Door Contact Signal Input
	D5	Yellow/Grey		BUTTON	Exit Door Wiring

5 Wiring Description

5.1 External Device Wiring Overview

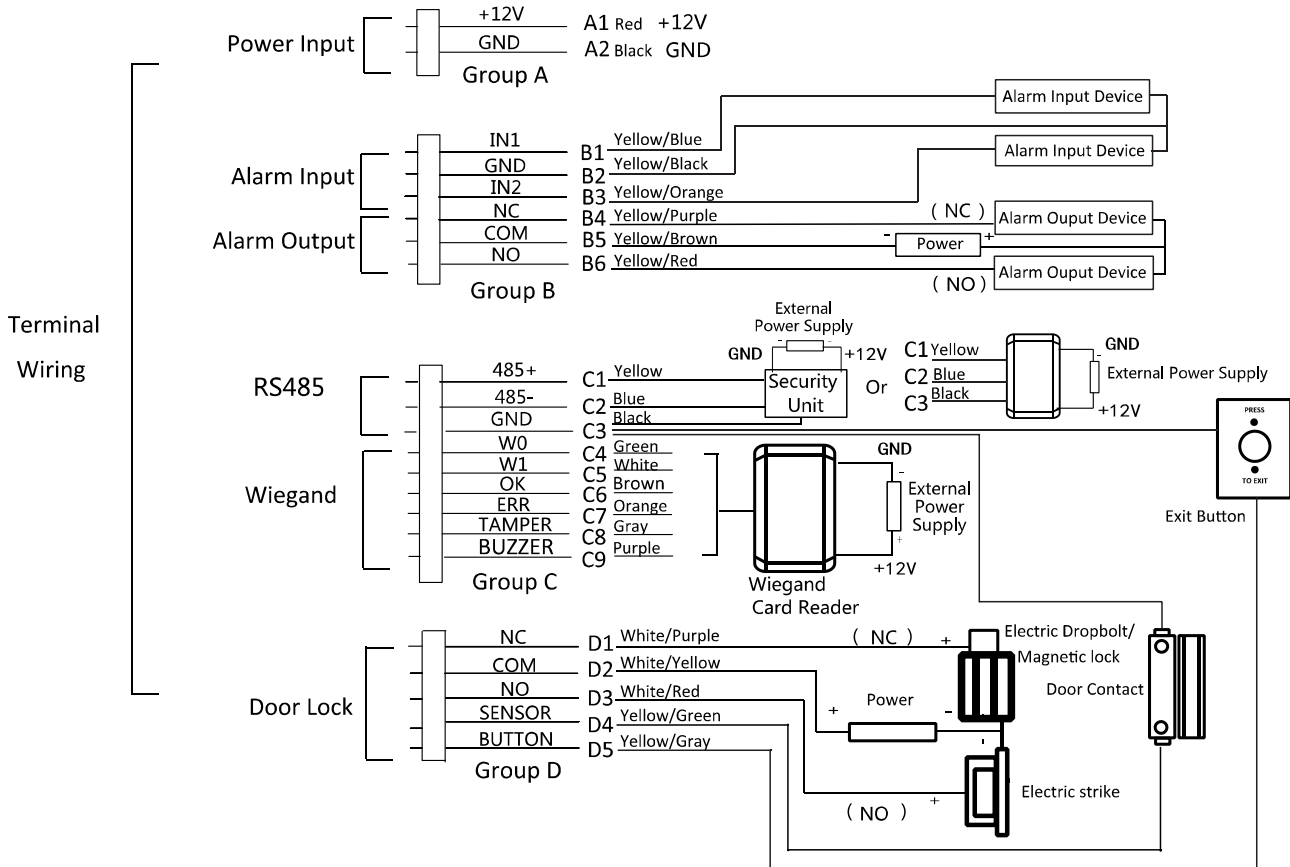


Figure 5-1 External Device Connection Diagram

5.2 The Wiring of External Card Reader

5.2.1 The Wiring of External RS-485 Card Reader

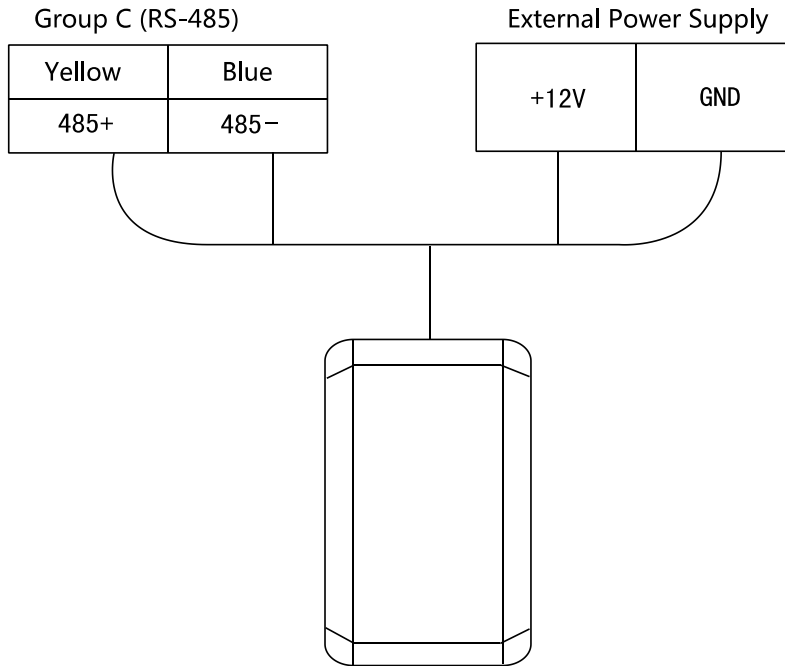


Figure 5-2 External RS-485 Card Reader Connection Diagram

5.2.2 The Wiring of External Wiegand Card Reader

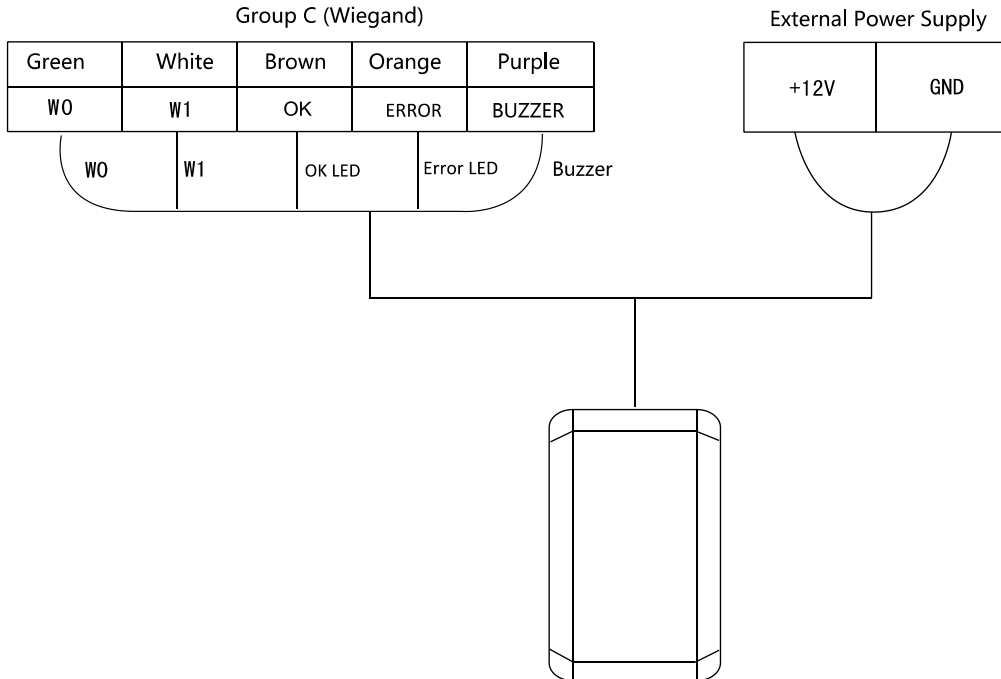


Figure 5-3 External Wiegand Card Reader Connection Diagram



- Set the dial-up of the external card reader as 2 when connected to the access control terminal.
- The external power supply and the access control terminal should use the same GND cable.

5.3 The Wiring of Electric Lock and Door Contact

5.3.1 The Wiring of Electric Lock

Group D (Door Lock)

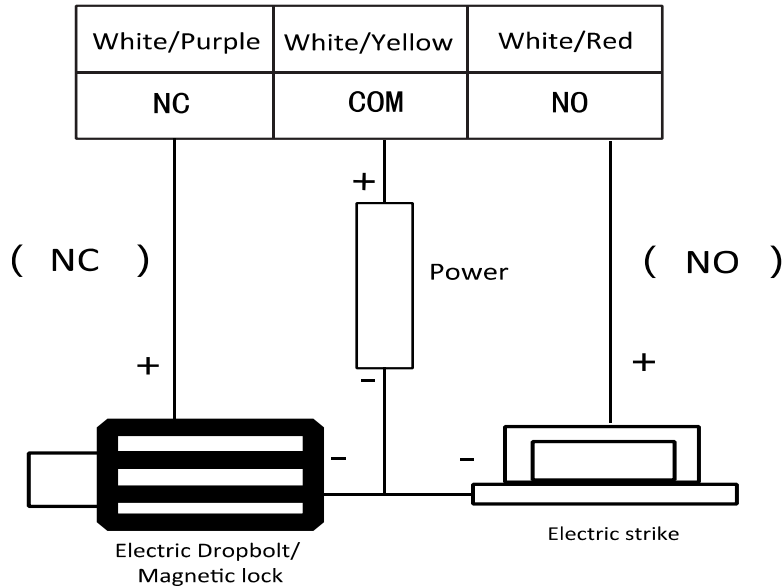


Figure 5-4 The Installation of Electric Dropbolt, Magnetic Lock, and Electric Strike



Signal input interface of the door status (DOOR_NC, DOOR_COM, DOOR_NO) is used to recognize whether the door is locked. If the NC interface is connected for opening door, the NO interface can only be connected for locking door.

5.3.2 The Wiring of Door Contact

Group C Group D (Door Lock)

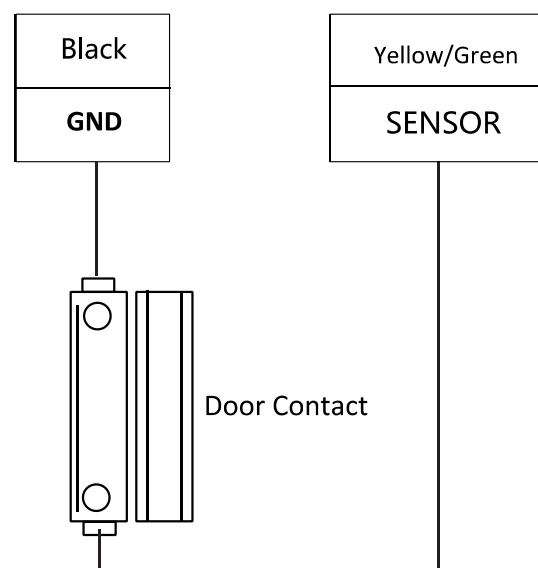


Figure 5-5 The Installation of Door Contact

5.4 The Wiring of Exit Button

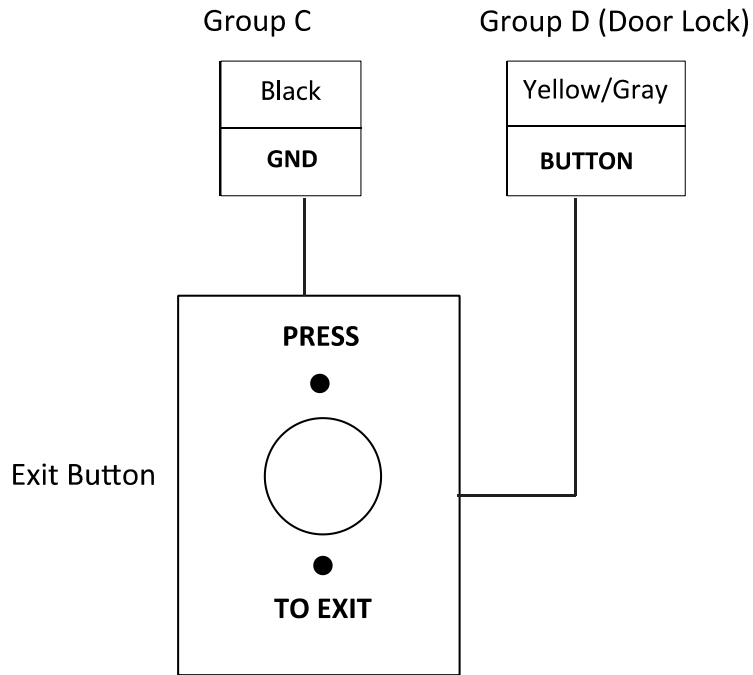


Figure 5-6 The Installation of Exit Button

5.5 The Wiring of Alarm Input

Group B (Alarm Input)

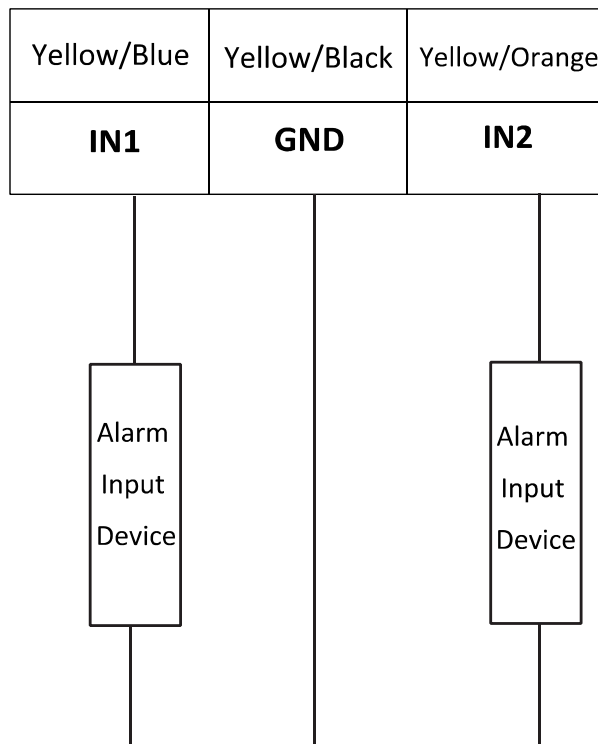


Figure 5-7 Alarm Input Connection

5.6 The Wiring of External Alarm Device

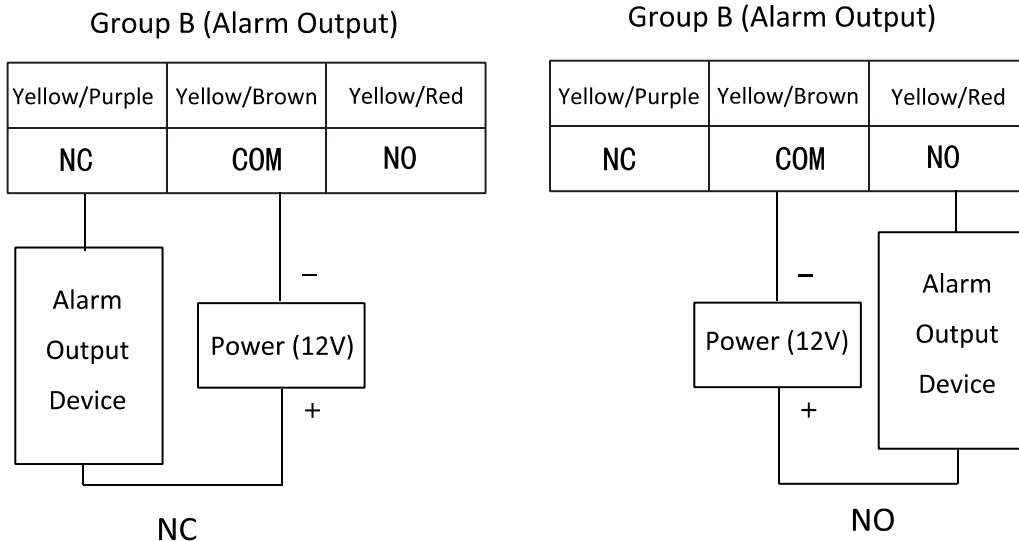


Figure 5-8 The Installation Diagram of External Alarm Device

5.7 Card Reader Connection

The access control terminal can be switched into the card reader mode. It can access to the access control as a card reader, and supports Wiegand communication port and RS-485 communication port.



When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.

5.7.1 The Wiring of Wiegand

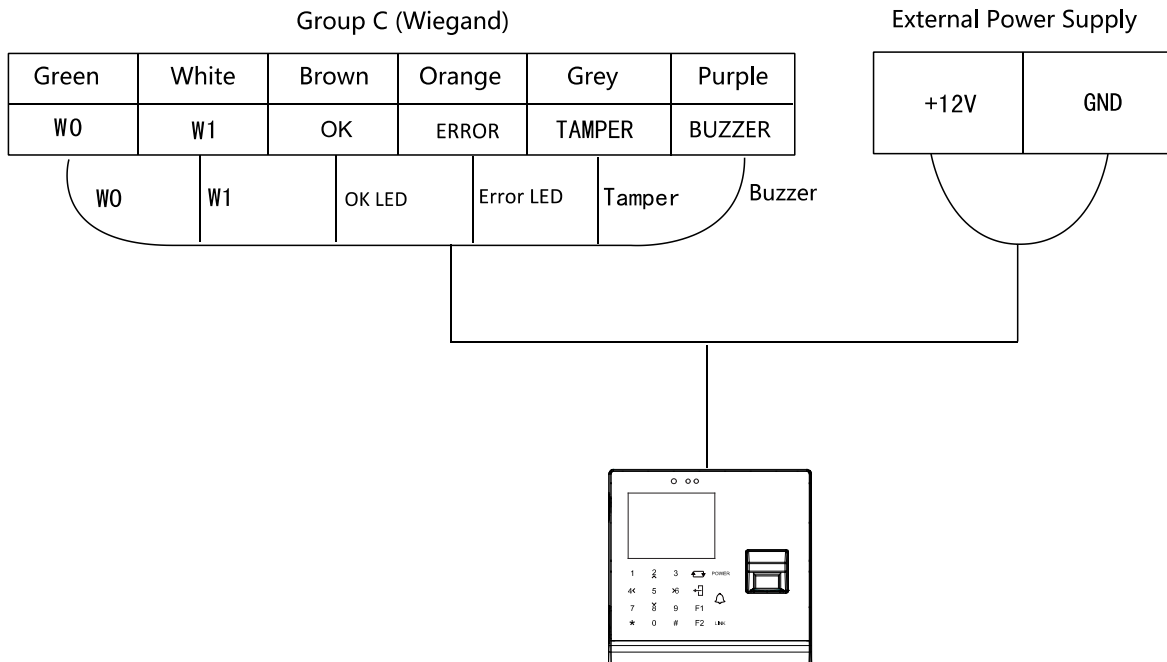


Figure 5-9 Access Control Terminal Wiegand Connection Diagram



- When the access control terminal works as a card reader, you must the **WG_ERR**, **BUZZER** and **WG_OK** interfaces if you want to control the LED and buzzer of the Wiegand card reader.
- Set the working mode of the terminal as card reader, which can be configured in **System Parameter** → **Mode Switch**, if the terminal is required to work as a card reader. The card reader mode support to communicate by Wiegand or RS-485.
- The distance of Wiegand communication should be no longer than 80 m.
- The external power supply and the access control terminal should use the same GND cable.

5.7.2 The Wiring of RS-485 Output

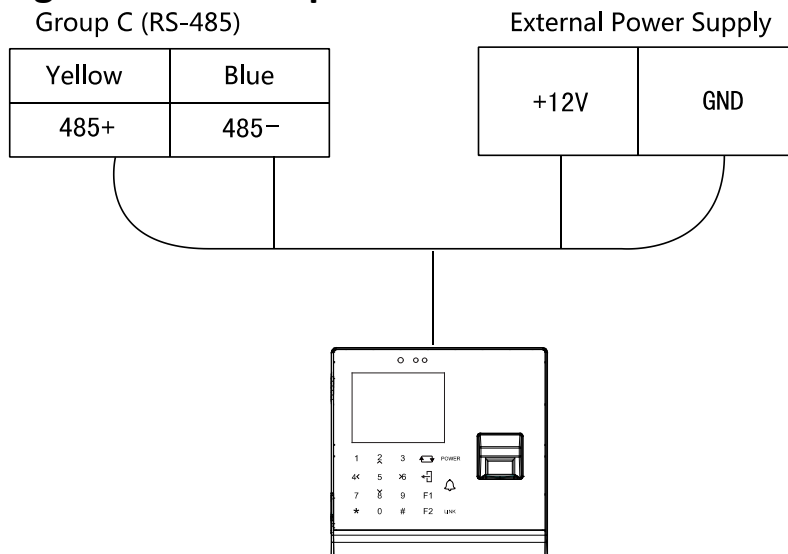


Figure 5-10 Access Control Terminal RS-485 Connection Diagram



- Set the working mode of the terminal as card reader, which can be configured in **System Parameter** → **Mode Switch**, if the terminal requires working as a card reader.
- When the access control terminal works as a RS-485 card reader, the default RS-485 address is 1. RS-485 address can also be configured in **System Parameter** -> **Serial Port Settings**.
- The external power supply and the access control terminal should use the same GND cable.

6 Activating Access Control Terminal

Purpose:

You are required to activate the terminal first before using it. Activation via SADP, and Activation via client software are supported. The default values of the control terminal are as follows.

- The default IP address: 192.0.0.64.
- The default port No.: 8000.
- The default user name: admin.

6.1 Activating via Device

If the device is not activated, you can activate the device after it is powering on.

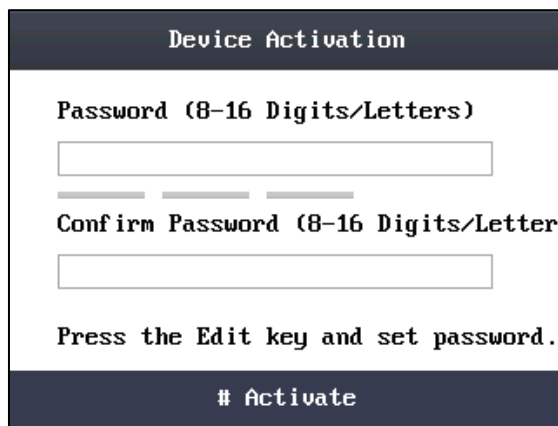


Figure 6-1 Device Activation Interface

Steps:

1. Use the Up, Down, Left, Right key to move the cursor to the Password textbox and create the password for device activating.
 - 1) Tap the ↵ key (Edit key) to enter the editing mode.

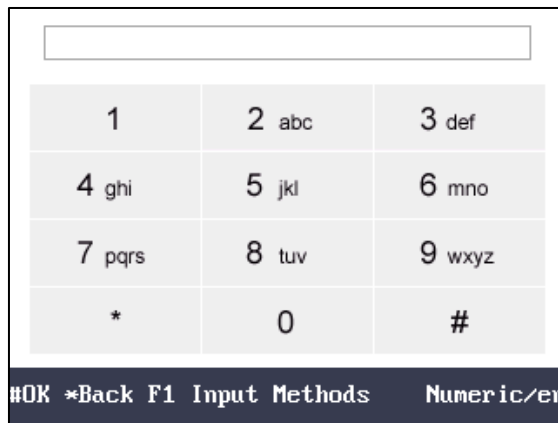


Figure 6-2 Input Text

- 2) Tap F1 key to switch the input method.
 - 3) Enter the card number into the textbox.
 - 4) Tap the ↵ key to exit the editing mode.
2. Move the cursor to the Confirm Password textbox and input the password again.
3. Move the cursor to **# Activate** and tap the # key to active the device.



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

6.2 Activating via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the SADP software to search the online devices.
2. Check the device status from the device list, and select an inactive device.

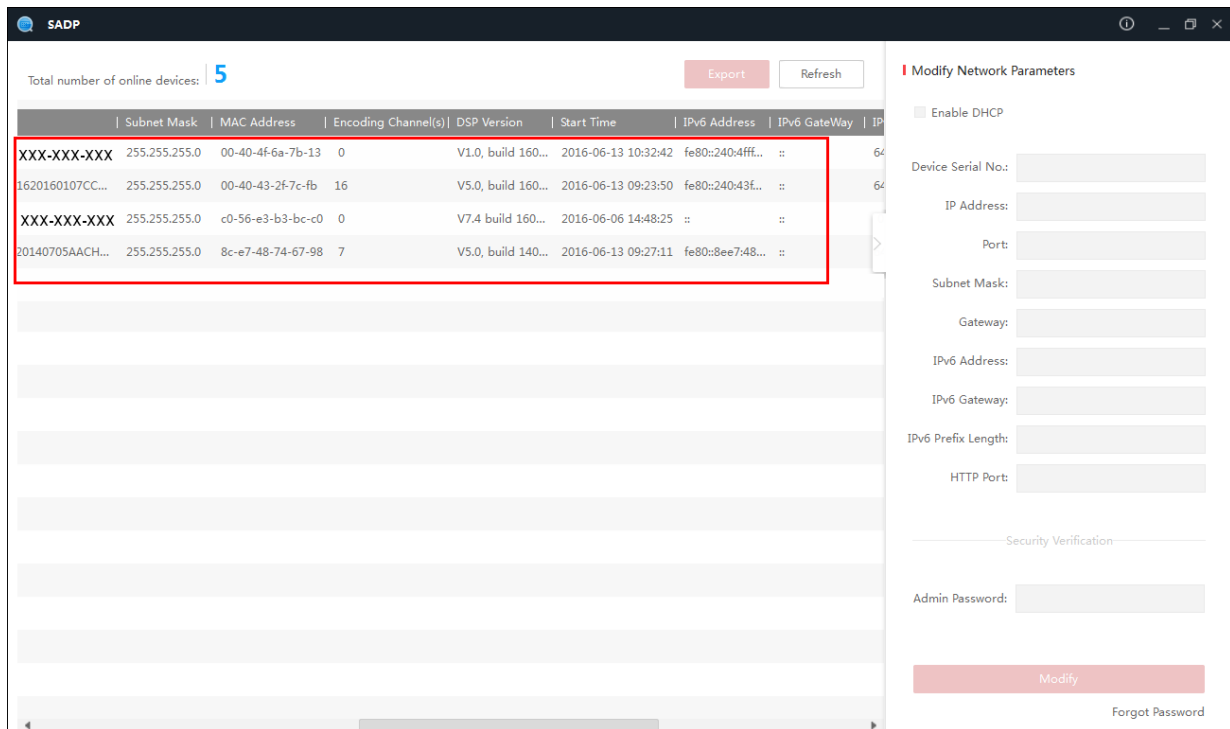


Figure 6-3 SADP Interface

3. Create a password and input the password in the password field, and confirm the password.



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **Activate** to save the password.

5. Check the activated device. You can change the device IP address to the same network segment with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Modify Network Parameters

Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

Security Verification

Admin Password:

[Forgot Password](#)

Figure 6-4 Modify Network Parameters Interface

6. Input the password and click the **Modify** button to activate your IP address modification.

6.3 Activating via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

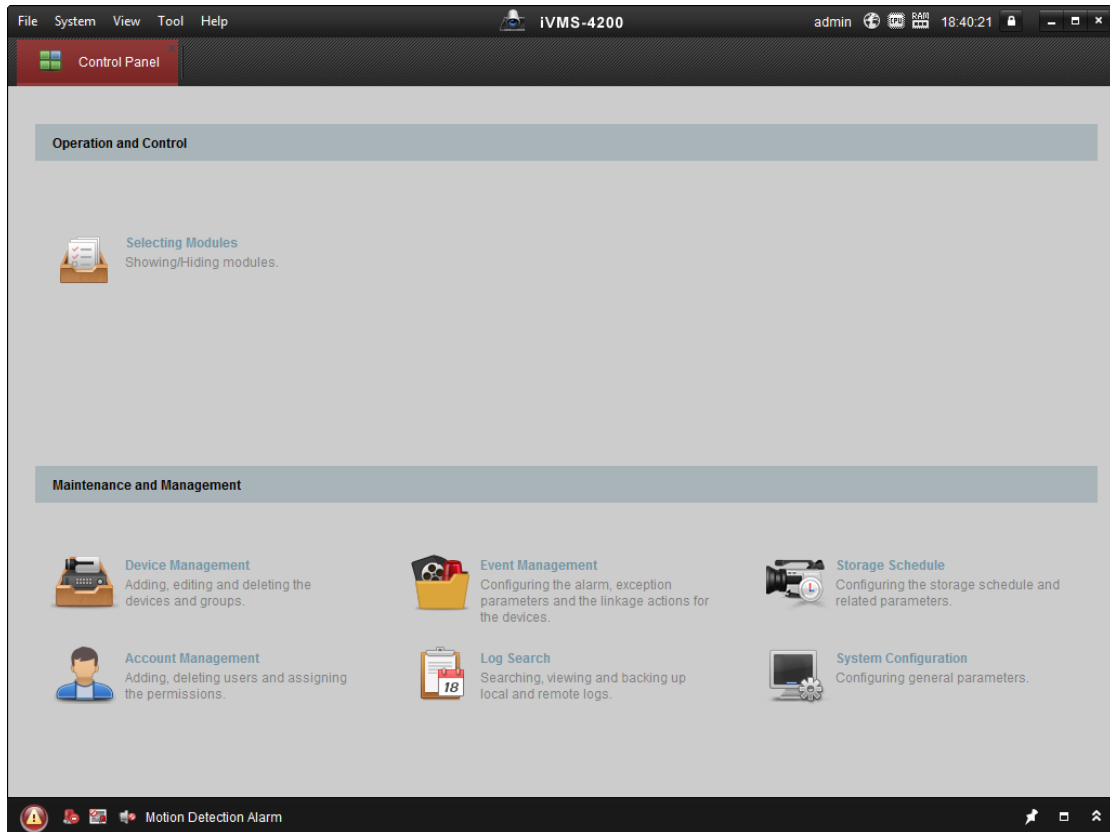


Figure 6-5 Control Panel Interface

2. Click **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.

IP	Device Type	Firmware Version	Security	Server Port	Device Serial No.	Start Time
192.0.0.64			Active	8000		2017-01
192.168.1.64			Inactive	8000		2017-01

Figure 6-6 Device List

4. Check the device status from the device list, and select an inactive device.
5. Click the **Activate** button to pop up the Activation interface
6. In the pop-up window, create a password in the password field, and confirm the password.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.



Figure 6-7 List Selecting Interface

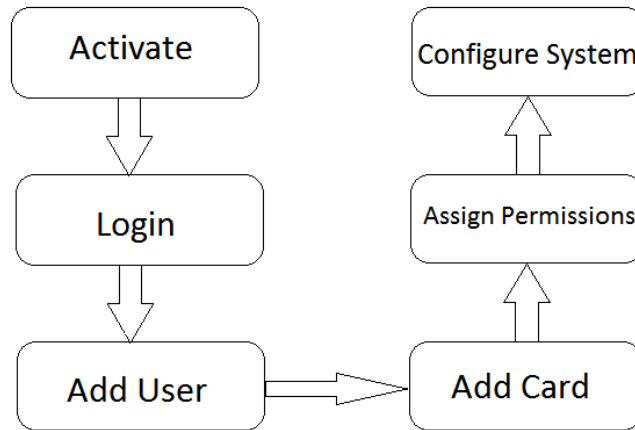
7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same network segment with your computer by either modifying the IP address manually.
10. Input the password and click the **OK** button to save the settings.

7 Basic Operation

Before You Start:

You should activate the device before the first login. Otherwise, after powered on, the system will switch into the Device Activation interface. For detailed information about activation, see *Chapter 6 Activating Access Control Terminal*.

The working flow is as follows:



Steps:

1. Power on the device to enter the initial interface.

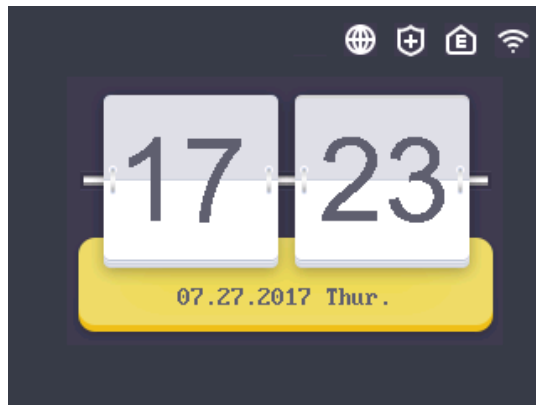


Figure 7-1 Initial Interface

2. Long-tap the # key for 3s to enter the password authentication interface.

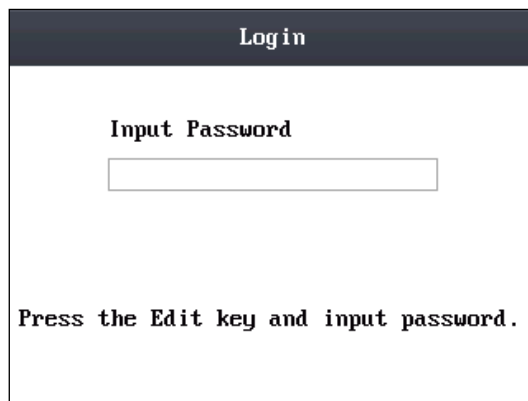


Figure 7-2 Password Authentication Interface

3. Enter the device password.
 - 1) Tap the ↵ key (Edit key) to enter the editing mode.
 - 2) Tap F1 key to switch the input method.
 - 3) Enter the (activation) password into the textbox.
 - 4) Tap the ↵ key to exit the editing mode.
4. Tap the # key to confirm the settings. The system will enter the menu operation interface.

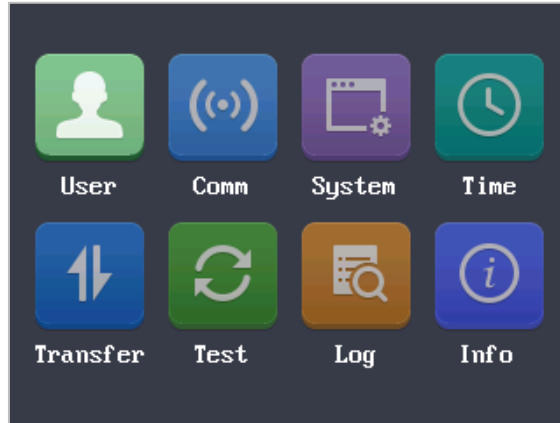







Figure 7-3 Menu Operation Interface

On the menu operation interface, you can manage users, set communication parameters, set system parameters, and so on.



In the initial interface, the icon , , , and  on the upper-right corner represents network is online, network is armed, EHome is online, and Wi-Fi is connected respectively. If there is  on the first three icons, it represents network is offline, network is not armed, and EHome is offline respectively. When the Wi-Fi is not connected, the Wi-Fi icon will have no color inside.

7.2 User Management

Purpose:

On the user management interface, you can add and manage users.

Use the Up, Down, Left, Right key to move the cursor to **User** (user management) by using the direction keys.

Tap the # key to enter the User interface.

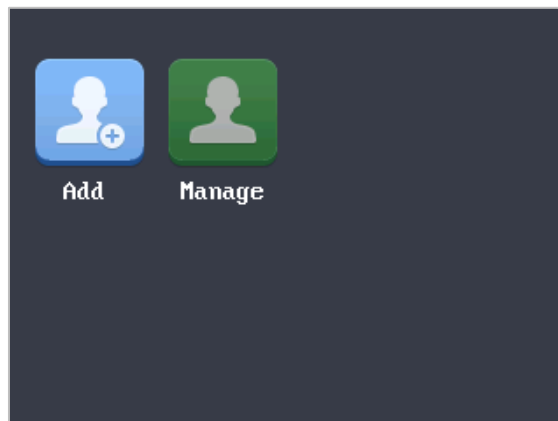


Figure 7-4 User Management Interface

7.2.1 Adding User

Purpose:

In the **Adding User** menu, you can add users, register card, and record fingerprints optionally for the corresponding person.

Steps:

1. Use the Up, Down, Left, Right key to move the cursor to **Add** (add user) by using the direction keys.
2. Tap the # key to enter the Add interface.



Figure 7-5 Card Registration Interface

3. Register the card.
 - Register the card by swiping the card.
 - 1) Place the card on the induction area.
 - 2) The system displays the card No. in the textbox automatically with a beep sound if the card No. has been recognized. .
 - Register the card by entering the card number into the **or enter the Card No.** textbox directly.

After registering the card, a dialog box about whether to register the fingerprint pops up.

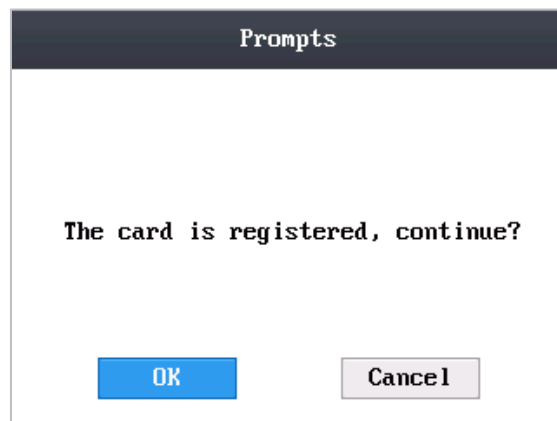


Figure 7-6 Card Registration Pop-up Window

4. Register the fingerprint.
 - 1) Move the cursor to the **OK** button, and tap the # key to enter the fingerprint registration interface.



Figure 7-7 Fingerprint Registration Interface

- 2) Place the finger on the fingerprint scanner, rise and rest your finger by following the corresponding voice prompts.



- The fingerprint registration function only supports device with fingerprint module.
- The same fingerprint cannot be repeatedly registered.
- For the optical access control terminal, you should place your finger twice to register the fingerprint. For details about scanning fingerprints, refer to *Appendix*.

7.2.2 Managing User

Move the cursor to the **Manage** (edit user) by using the direction keys.

Tap the # key to enter the Management interface.

Searching User

Steps:

1. Move the cursor to a user by using the direction keys.
2. Tap the # key to pop up an interface for selecting corresponding operations.

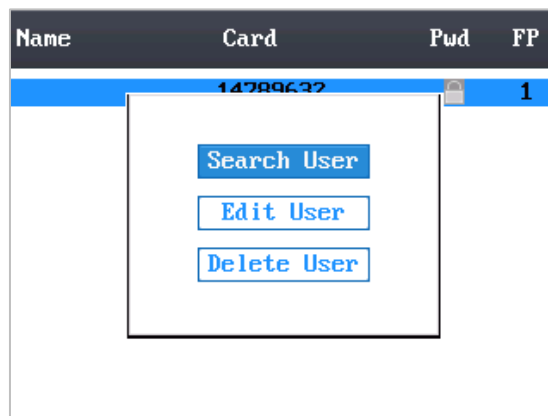


Figure 7-8 Managing User Interface

3. Move the cursor to **Search User** by using the direction keys.
4. Tap the # key to enter the searching interface.

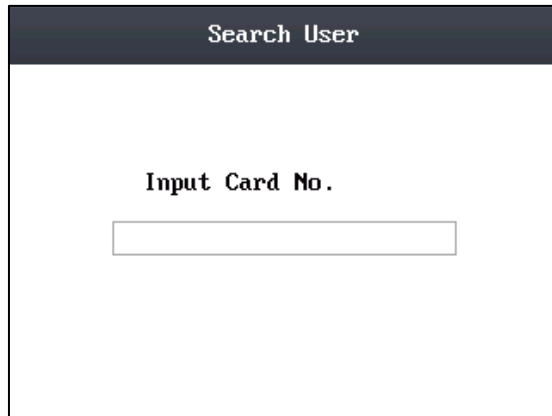


Figure 7-9 Searching Interface

5. Input the card number to **Input Card No.** textbox.
6. Tap the # key to view the basic information about the card holder.

Editing User

Steps:

1. Move the cursor to a user by using the direction keys.
2. Tap the # key to pop up an interface for selecting corresponding operations.
3. Move the cursor to **Edit User**.
4. Tap the # key to enter the editing interface.

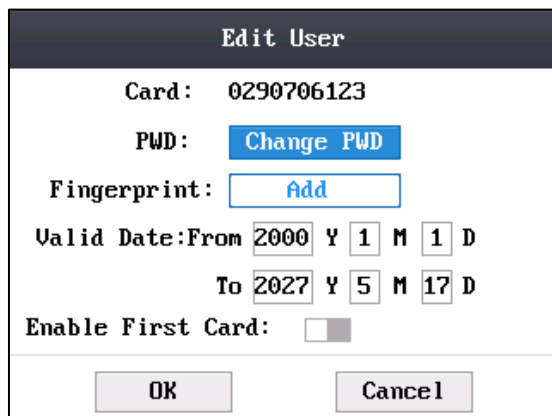


Figure 7-10 Editing Interface

5. Edit the user information.
 - Adding the Fingerprint.
Move the cursor to **Add** to enter the fingerprint registration interface. See details in step 4 of adding user.



DS-K1T105 series model does not support this function.

- Changing the Password.
 - 1) Move the cursor to **Change PWD** to enter the password changing interface.
 - 2) Input a new password.
 - 3) Confirm the new password.



Figure 7-11 Password Changing Interface

- Changing the valid date.
You can set the start/end time of the user’s permission.
Tap the ↵ key to enter/exit the editing mode.
- Enabling first card
Tap the # key to enable first card.



After enabling first card, the door remains open during the pre-defined valid duration.

6. Move the cursor to the **OK** button, and tap the # key to confirm the settings.

Deleting User

Steps:

1. Move the cursor to a user by using direction keys.
2. Tap the # key to pop up an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Delete User**, and tap the # key to enter the deleting interface.
4. Move the cursor to **Delete User**, **Delete PWD only** or **Delete FP only**,

Delete User: Delete the user and the overall information.

Delete PWD only: Only delete the password set by the user.

Delete FP only: Only delete the fingerprint information of the user.



DS-K1T105 series model does not support this function.

5. Tap the # key to finish the deleting operation.



You can tap the * key to return to the main menu.

7.3 Communication Settings

Purpose:

On the communication settings interface, you can set network parameters, the serial port, Wiegand parameters, and Wi-Fi.

Steps:

1. Move the cursor to **Comm** (communication settings) by using direction keys.
2. Tap the # key to enter the communication settings interface.

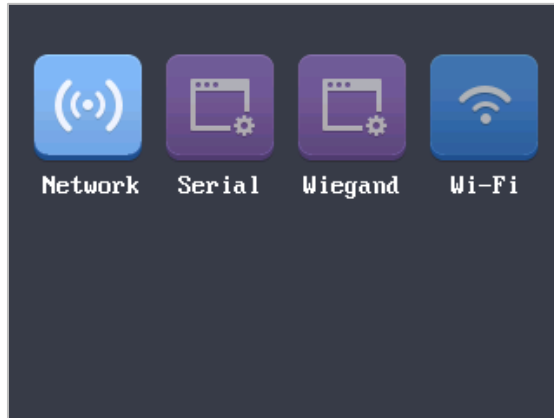


Figure 7-12 Communication Settings Interface

Network Settings:	It refers to network parameters of the device, including IP address, subnet mask, and gateway address.
Serial Port Settings:	When the access control terminal works as a RS-485 card reader, serial port parameters include working mode, Baud Rate, and RS-485 address.
Wiegand Settings:	When the access control terminal works as a Wiegand card reader, Wiegand parameters involve the Wiegand direction, and the Wiegand mode.
Wi-Fi:	You can enable the Wi-Fi function.

7.3.1 Network Settings

Purpose:

On the network settings interface, you can set network parameters of the device.

Steps:

1. Move the cursor to **Network** (network settings) by using direction keys.
2. Tap the # key to enter the network settings interface.

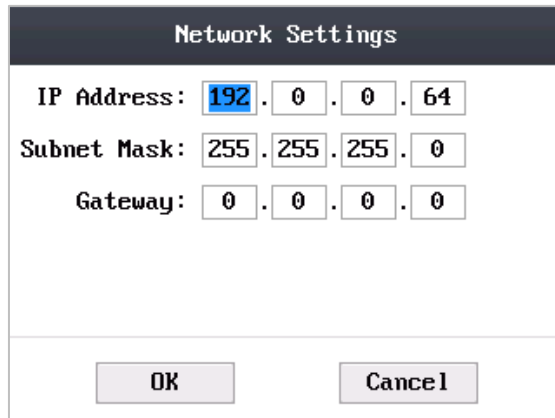


Figure 7-13 Network Settings Interface

3. Modify network parameters of the device, including IP address, subnet mask, and gateway address.



Tap the ↵ key to enter/exit the editing mode.

4. Move the cursor to the **OK** button, and tap the # key.

7.3.2 Serial Port Settings

Purpose:

When the access control terminal works as the RS-485 card reader, you should set serial port parameters.

Steps:

1. Move the cursor to **Serial** (serial port settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the serial port settings interface.

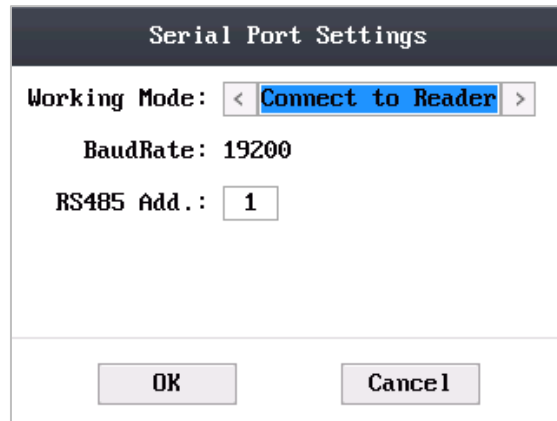


Figure 7-14 Serial Port Settings Interface

3. Modify parameters of the serial port, including working mode, Baud Rate, and RS-485 address.

Working Mode:	<ul style="list-style-type: none"> ● When the access control terminal working as the terminal, set the working mode of the serial port to Connect to Reader, Connect to Client or Connect to Unit. ● If the terminal is worked as the card reader, the serial port is connected to the terminal by default. There is no need to configure the serial port working mode.
Baud Rate:	It will display the Baud Rate configured on the client software.
RS-485 Address:	When the access control terminal works as a card reader, the RS-485 address should be configured.



- Tap the ↵ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.



Reboot the device after changing the working mode.

7.3.3 Wiegand Settings

Purpose:

When the access control terminal works as the Wiegand card reader, you should set Wiegand parameters.

Steps:

1. Move the cursor to **Wiegand** (Wiegand settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the Wiegand settings interface.

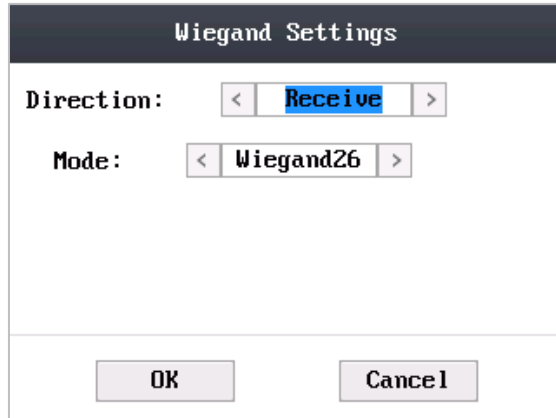


Figure 7-15 Wiegand Settings Interface

3. Edit parameters of the serial port, including the Wiegand direction and the Wiegand mode.

Wiegand Direction:	1) In the terminal mode, select whether to Receive or to Send . In the Receive mode, the mode is self-adaptive and the mode cannot be edited. 2) In the card reader mode, only Send is supported.
Wiegand Mode:	The default Wiegand mode is Wiegand 34



- Tap the ↵ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.



Reboot the device after changing the Direction.

7.3.4 Wi-Fi Settings

Steps:

1. Move the cursor to **Wi-Fi** (Wi-Fi settings) by using direction keys on the communication settings interface.
2. Tap the # key to enter the Wi-Fi settings interface.

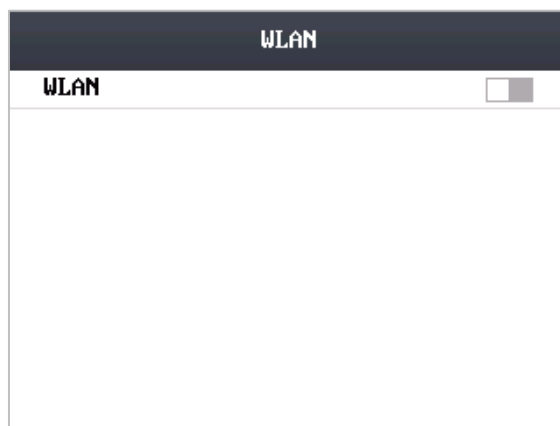


Figure 7-16 Wi-Fi Enabling

3. Move the cursor to and tap the # key to enable the WLAN.

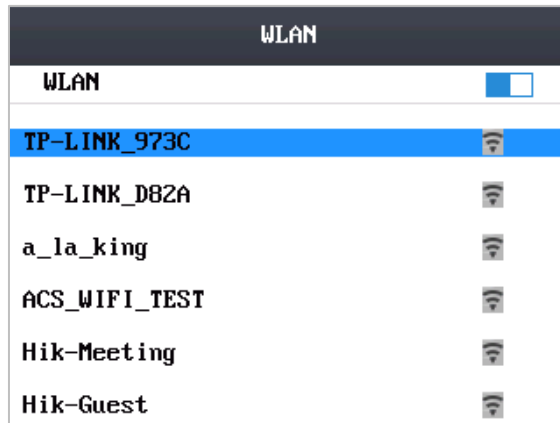


Figure 7-17 Wi-Fi Selection

4. Move the cursor to a network, and tap # key to enter the network connection interface.

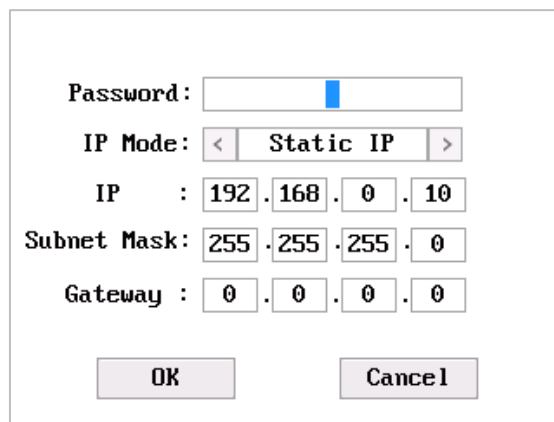


Figure 7-18 Wi-Fi Settings

5. Input the password of the network. The password supports numbers, letters (uppercase and lowercase) and symbols.
6. Edit the IP mode, IP address, subnet mask, and gateway address.
7. Move the cursor to the **OK** button, and tap the # key.



Tap the ↵ key to enter and exit the editing mode.

7.4 System Settings

Purpose:

On the system settings interface, you can set system parameters, manage the data, restore default settings, set access control parameters, and set cameras.

Steps:

1. Move the cursor to **System** (system parameters) by using direction keys.
2. Tap the # key to enter the system parameters interface.

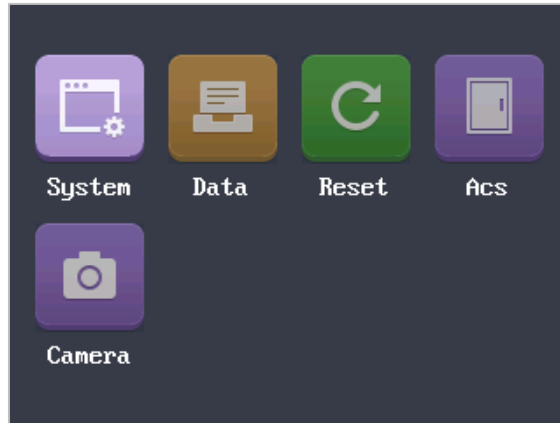


Figure 7-19 System Settings Interface

System Parameters:	System parameters of the device include the device running mode, login password, and prompt sound.
Data Management:	It is used to manage the storage data of the device, including Delete Card Parameters, Delete Event Only, and Delete Picture Only.
Restore Settings:	The device can be restored into factory defaults or default settings.
Access Control Settings:	You can set parameters of the access control terminal, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.
Camera Settings:	You can set the camera for the access control terminal (only supported by terminal with the model of -C).



Camera Settings will be displayed on the screen when the access control terminal has the function.

7.4.1 Setting System

Steps:

1. Move the cursor to **System** (system parameters) by using direction keys on the system settings interface.
2. Tap the # key to enter the system parameters interface.

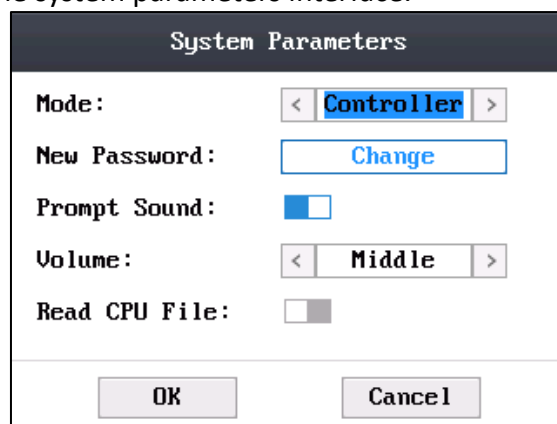





Figure 7-20 System Parameters Interface

3. Modify system parameters, including switching the mode, entering the login password, and enabling voice prompts.

Mode:	The device mode can be switched between Controller and Card Reader . After switching the mode, the system can automatically reboot and enter
--------------	--

	<p>into the interface of the new mode.</p> <p> NOTE</p> <ul style="list-style-type: none"> ● If the access control terminal works as a card reader, you should configure the serial port setting and the Wiegand setting. See details in <i>Chapter 7.3.2 Serial Port Settings</i> and <i>Chapter 7.3.3 Wiegand Settings</i>. ● If the access control terminal is in the card reader mode, the terminal works as a card reader to access to the access controller or another access control terminal via RS-485 and Wiegand. ● If the access control terminal is in the card reader mode, the terminal will apply the fingerprint via RS-485, the client software and the local. (The fingerprint application function should be supported by the device) ● If the access control terminal is in the card reader mode, the terminal supports swiping card and scanning fingerprint. When scan the fingerprint, the bound card No. should contain 10 numbers. Or the fingerprint scanning will be failed.
Login Password:	To change the login password of the device, you should input the old password, create a new password, and confirm it.
Voice Prompts:	<p>After enabling voice prompts, you can hear the voice prompts to notify you the card status when you swipe the card. Otherwise, you will hear the beeper in place of the voice prompts.</p> <ul style="list-style-type: none"> ● Beep three times: legal card. ● Beep four times: illegal card.
Volume:	You can adjust the device volume. High, Middle, and Low are available.
Read CPU File:	<p>If the device can be swiped by the CPU card, when enable the function, the device can read the CPU card information.</p> <p> NOTE</p> <ul style="list-style-type: none"> ● Only device can recognize CPU card supports the function. ● Tap the  key to enter and exit the editing mode. ● Tap the Right/Left direction keys to choose contents. ● Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.

7.4.2 Managing Data

Purpose:

On the data management interface, you can delete the storage data of the device.

Steps:

1. Move the cursor to **Data** (data management) by using direction keys in the system settings Interface.
2. Tap the # key to enter the data management interface.

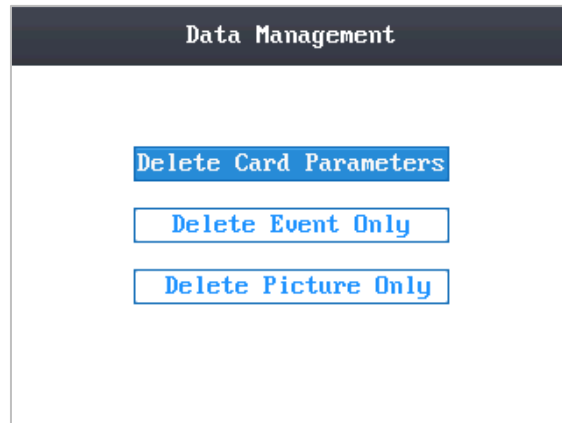


Figure 7-21 Data Management Interface

Move the cursor to Delete Card Parameters, Delete Event Only, or Delete Picture Only.

Delete Card Parameters: Delete all cards parameters registered in the device.

Delete Event Only: Delete all access events in the system.

Delete Picture Only: Delete all captured pictures in the system.



This function is only supported by terminal with the model of -C.

3. Tap the # key.

7.4.3 Restoring Settings

Purpose:

On the restore settings interface, you can restore Factory Defaults or Default Settings.

Steps:

1. Move the cursor to **Reset** (restore settings) by using direction keys on the system settings interface.
2. Tap the # key to enter the restore settings interface.

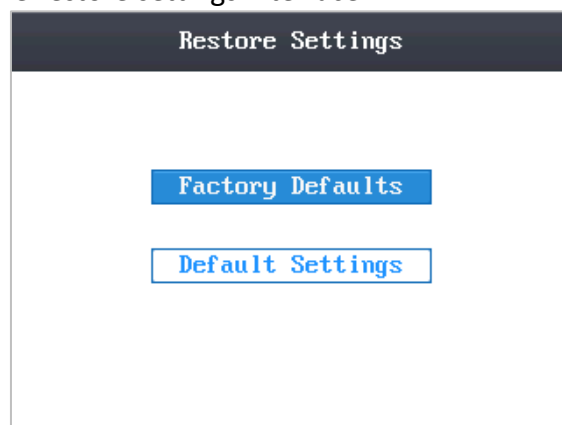


Figure 7-22 Restore Settings Interface

3. Move the cursor to Factory Defaults or Default Settings.

Factory Defaults: After restoring factory defaults, all parameters of the device are returned to the factory defaults.

Default Settings: After restoring defaults settings, parameters, excluding network parameters and event parameters, are returned to the factory defaults.

4. Tap the # key.

5. Move the cursor to the **OK** button, and tap the # key.

7.4.4 Door Settings

Purpose:

On the door settings interface, you can set door parameters, including Controller Authentication, Card Reader Authentication, Door Action Time, Delayed Door Alarm, and Anti-passing Back.

Steps:

1. Move the cursor to **ACS** (door settings) by using direction keys in the system settings interface.
2. Tap the # key to enter the door settings interface.

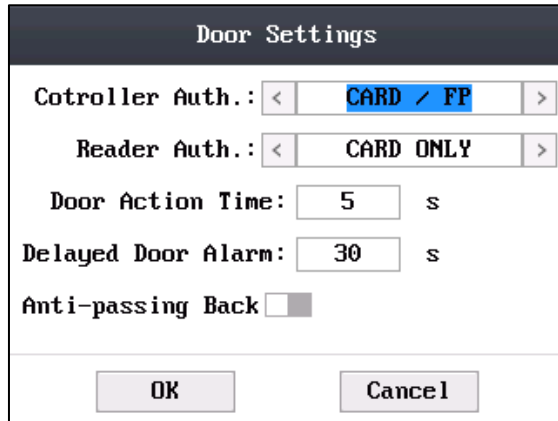


Figure 7-23 Door Settings Interface

3. Edit door parameters.

Controller Authentication:	Set the controller authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Fingerprint & Password, Card & Fingerprint & Password.
Card Reader Authentication:	Set the card reader authentication mode for opening the door, that is, Card Only, Fingerprint Only, Card/Fingerprint, Card & Fingerprint, Card & Password, Password & Fingerprint, Card & Password & Fingerprint.
Door Action Time:	Set the door action time: 1 ~ 255 s.
Delayed Door Alarm:	Set the delayed door alarm threshold: 1 ~ 255 s.
Anti-Passing Back:	Set whether to enable the function of anti-passing back.



- Tap the ↵ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.

7.4.5 Setting Camera

Purpose:

On the camera settings interface, you can set camera parameters.



This function is only supported by terminal with the model of -C.

Steps:

1. Move the cursor to **Camera** (camera settings) by using direction keys in the system settings Interface.
2. Tap the # key to enter the camera settings interface.



Figure 7-24 Camera Settings Interface

3. Edit camera parameters.

Enable Face Detection:	If enabling face detection, the device should detect the face when authenticating. Or authentication will be failed.
Overlay User Info. On Picture:	When enabling card No. overlay, captured pictures can be overlaid on the card information.
Display Detected Face Picture:	When enabling to display the picture, captured pictures can display on the screen.
Enable QR Code Authentication:	<p>You can authenticate via QR code. When enabling the function, long-press the F1 key to enter the QR code authentication mode. Place the QR code picture in front of the device camera to authenticate.</p> <p>NOTE</p> <ul style="list-style-type: none"> ● You can generate the card QR code when adding the card to the person. For details, see <i>Adding User (Card)</i> in <i>User Manual of iVMS-4200 Client Software</i>. ● The function should be supported by the device with camera.

NOTE

- Tap the ↵ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.
- The captured pictures can be saved in the SD card.

4. Move the cursor to the **OK** button, and tap the # key.

7.5 Time Settings

Steps:

1. Move the cursor to **Time** (time settings) by using direction keys.
2. Tap the # key to enter the time settings interface.

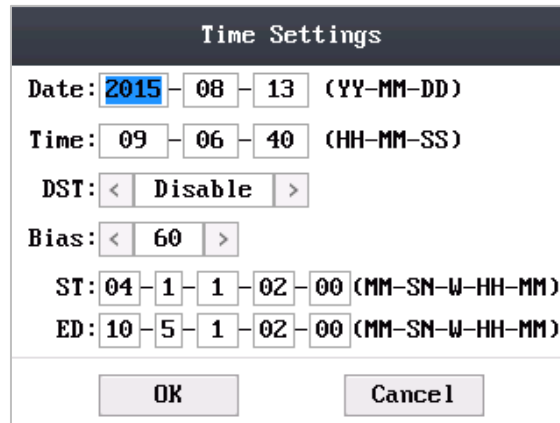


Figure 7-25 Time Settings Interface

3. Edit time parameters.

Date/Time: Edit the data and the time of the device.

DST (Daylight Saving Time): When enabling DST, you should set the bias time, the start time, and the end time of DST.



- Tap the ↵ key to enter and exit the editing mode.
- Tap the Right/Left direction keys to choose contents.
- Tap the # key to switch the mode between “Yes” mode and “No” mode.

4. Move the cursor to the **OK** button, and tap the # key.

7.6 Upload/Download Settings

Purpose:

On the upload/download interface, you can upgrade the device, upload the door parameters, download access parameters, download captured pictures, and download attendance record.

Steps:

1. Plug a USB disk into the access control terminal.
2. Move the cursor to **Transfer** (upload/download) by using direction keys.
3. Tap the # key to enter the upload/download interface.

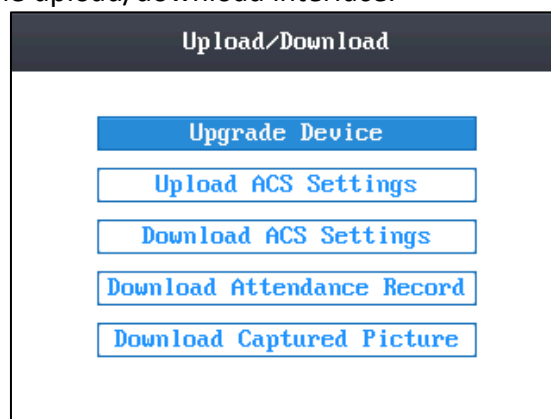



Figure 7-26 Upload/Download Interface

4. Move the cursor to Device Upgrade, Upload Access Settings, Download Access Settings, Download Attendance Record, or Download Captured Picture.

Upgrade Device:	The system can automatically read the upgrading
------------------------	---

	information from the USB, and upgrade the device.  The upgrading file should be put in the root directory.
Upload ACS Settings:	The system can automatically read the access parameters from the USB, and upload them to the device.
Download ACS Settings:	The system can automatically download access parameters into the USB.
Download Attendance Record:	The system can automatically download attendance records into the USB.
Download Captured Picture:	The system can automatically download captured pictures into the USB. Click the # key.



The supported USB format is FAT32.

7.7 Testing

Purpose:

On the test interface, you can do voice test, keypad test, RTC test, and camera test.

Steps:

1. Move the cursor to **Test** by using direction keys.
2. Tap the # key to enter the test interface.

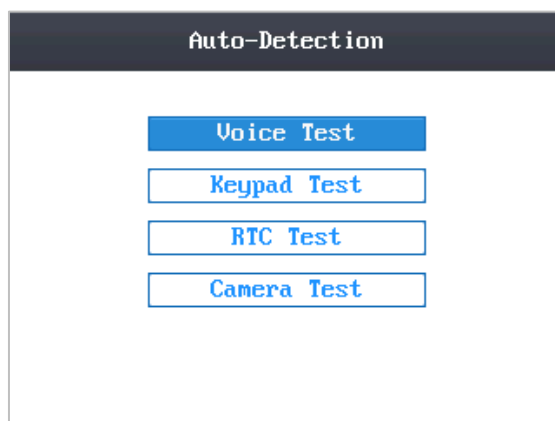



Figure 7-27 Test Interface

3. Move the cursor to select Voice Test, Keypad Test, RTC Test, or Camera Test to do corresponding test.

Voice Test:	You can hear a voice prompt “Voice prompt succeeds” after click the # key.
Keypad Test:	On the keypad test interface, if the keypad test succeeds, the screen will display corresponding numbers or functions of the keypad you click.
RTC Test:	On the RTC test interface, if the test succeeds, the screen will display the synchronization time.
Camera Test:	On the camera test, if the camera test succeeds, the screen will display the real-time picture the camera captures.  This function is only supported by terminal with the model of –C.

7.8 Log Query Settings

Steps:

1. Move the cursor to **Log** (log query settings) by using direction keys.
2. Tap the # key to enter the log query interface.

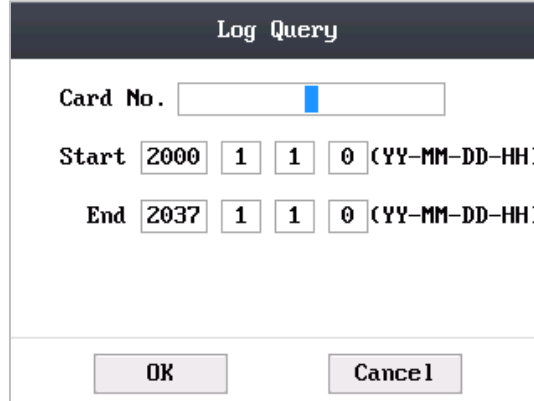


Figure 7-28 Log Query Interface

3. Enter the card number.
 - Enter the card number by swiping the card.
Place the card close to the screen.
 - Input the card number manually.
4. Set the start/end time.
Tap the ↔ key to enter and exit the editing mode.
5. Move the cursor to the **OK** button, and tap the # key.



On the log query display interface, you can view the card number, swiping time, and card reader ID.

7.9 System Information

Steps:

1. Move the cursor to **Info** (system information) by using direction keys.
2. Tap the # key to enter the system information interface.

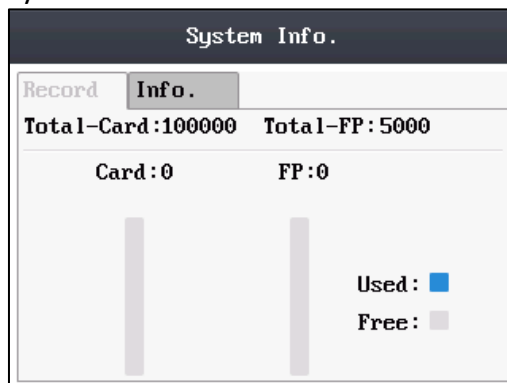




Figure 7-29 System Information Interface

3. Move the cursor to **Record Capacity** or **Information** by using Left/Right direction keys.
 - **Record Capacity**

Card Capacity:	It refers to the maximum amount of cards.
-----------------------	---

	 <p>The default maximum card amount is 100,000.</p>
Fingerprint Capacity:	<p>It refers to the maximum amount of fingerprints.</p>  <ul style="list-style-type: none"> ● Fingerprint capacity only supports devices with fingerprint registration function. ● The default maximum fingerprint amounts of devices with fingerprint registering function are as follows. ● DS-K1T200 series optical device: 9500; ● DS-K1T201 series optical device: 5000 ● DS-K1T105 series model does not support this function.

- **Device Information**

In the device information interface, you can view the device name, the serial No., Mac address, and so on.



Figure 7-30 Device Information Interface

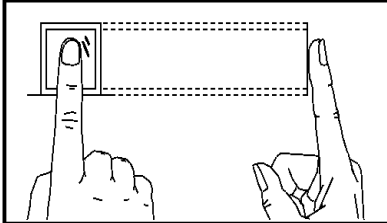
Appendix: Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

The figure displayed below is the correct way to scan your finger:

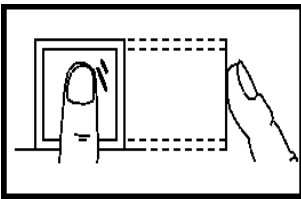


You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

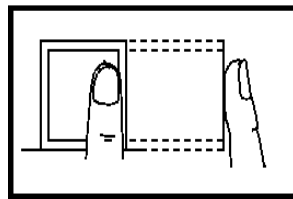
Incorrect Scanning

The figures of scanning fingerprint displayed below are wrong:

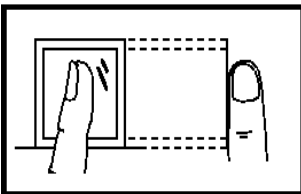
Vertical



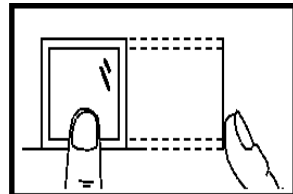
Edge I



Side



Edge II



Environment

The scanner should avoid direct high light, high temperature, humid conditions and rain.

When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again after drying the finger.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

0200001071027



UD05666B-C

www.hikvision.com