Access Control Terminal

Quick Start Guide

UD.6L0206D1079A01

Quick Start Guide

©2015 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-C
	DS-K1T105M-C （with Camera）
Optical IP-based Fingerprint Access Control Terminal	DS-K1T200EF-C
	DS-K1T200MF-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.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES

FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, SECURITY BREACHES, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF OR RELIANCE ON THIS MANUAL, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY OR CERTAIN DAMAGES, SO SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Support

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

0100001050825

Regulatory Information

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.

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.

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.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

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 Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, 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.

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 1

1.1 Introduction 1
1.2 Main Features 2
1.2.1 Main Features of DS-K1T105 Series Model 2
1.2.2 Main Features of DS-K1T200 Series Model 2

2 Appearance 4

2.1 Appearance of DS-KITI05 Series Model 4
2.2 Appearance of DS-KIT200Series Model 5
2.2.1 Description of Components 5
2.3 Appearance of Keys 6
2.3.1 Description of Items 6

3 Terminal Connection 8

3.1 Terminal Description 8

4 Wiring Description 12

4.1 External Device Wiring Overview 12
4.2 The Wiring of External Card Reader 13
4.2.1 The Wiring of External RS485 Card Reader 13
4.3 The Wiring of Electric Lock and Door Magnetic 14
4.3.1 The Wiring of Electric Lock 14
4.3.2 The Wiring of Door Contact 15
4.4 The Wiring of Exit Button 16
4.5 The wiring of Alarm Input 17
4.6 The Wiring of External Alarm Device 17
4.7 Card Reader Connection 18
4.7.1 The Wiring of Wiegand Output 18
4.7.2 The Wiring of RS485 Output 19

5 Activating the Access Control Terminal 21

5.1 Activating via SADP Software 21
5.2 Activating via Client Software 23

6 Basic Operation 27

6.1 User Management 28
6.1.2 Adding User 29
6.1.2 Managing User 31
6.2 Communication Settings 34
6.2.1 Network Settings 34
6.2.2 Serial Port Settings 35
6.2.3 Wiegand Settings 36

6.2.4 Wi-Fi Settings 37
6.3 System Settings 38
6.3.1 Setting System 39
6.3.2 Managing Data 40
6.3.3 Restoring Settings 41
6.3.4 Door Settings 41
6.3.5 Setting the Camera 42
6.4 Time Settings 43
6.5 Upload/Download Settings 44
6.6 Testing 45
6.7 Log Query Settings 46
6.8 System Information 47

1 Overview

1.1 Introduction

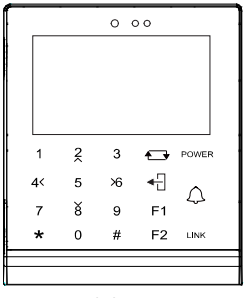

Figure 1-1 DS-K1T105 Series Standalone Access Control Terminal Front Panel

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 two network communication methods (TCP/IP, and Wi-Fi), and supports offline operation.

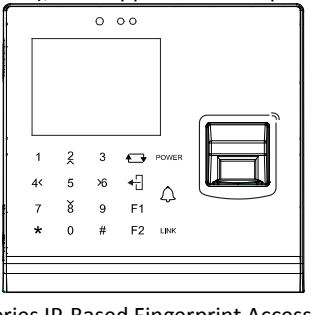

Figure 1-2 DS-K1T200 Series IP-Based Fingerprint Access Control Terminal Front Panel

DS-K1T200 is a series 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/TP) and Wi-Fi.
- Face detection and picture capturing function 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 RS485 communication for connecting to external card reader.
- Supports working as a card reader, and supports Wiegand interface and RS485 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 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 and picture capturing function implemented by built-in camera (2 MP optional, only supports DS-K1T200EF/MF-C)
- Supports RS485 communication for connecting external card reader.
- Supports working as a card reader, and supports Wiegand interface and RS485 interface for accessing the controller.
- Max. 100,000 card No., Max. 300,000 access control events records , and Max. 9500 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)
- Supports Mifare card reading, including card No. reading, and sector reading & writing (DS-K1T200MF/MF-C)
- 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-KITI05 Series Model

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

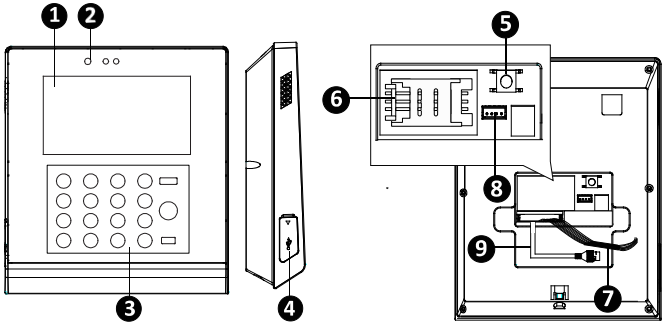

Figure 2-1 Appearance of DS-K1T105 Series Model

Table 2-1 Description of DS-K1T105 Series Model

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

2.2 Appearance of DS-KIT200Series Model

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

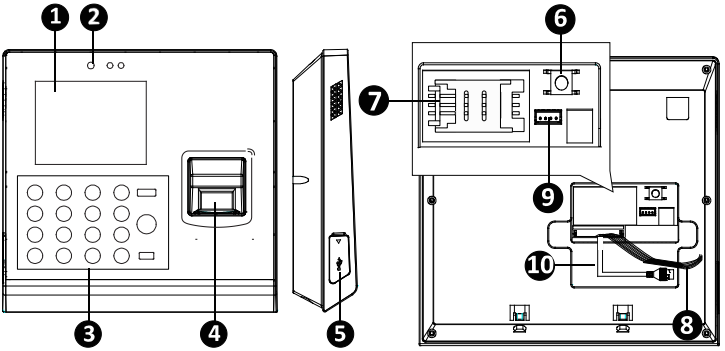

Figure 2-2 Appearance of DS-K1T200 IP-Based Fingerprint Access Control Terminal

2.2.1 Description of Components

Table 2-2 DS-K1T200 IP-Based Fingerprint Access Control Terminal Components

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

No.	Description
10	Ethernet Port

2.3 Appearance of Keys

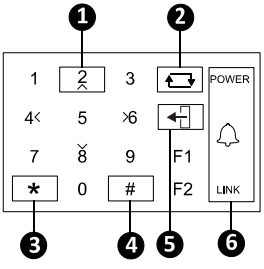

Figure 2-3 Appearance of Keys

2.3.1 Description of Items

Table 2-3 Description of Keys

No.	Description			
1	Numeric Keys: Enter number in the textbox. Direction Keys: Select icons in the menu.			
2	Editing Key: Click the key to enter/exit the editing status.			
3	Exiting Key: Click the key to exit the menu.			
4	Confirming Key: Click the key to confirm operations. Long-click 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/	Normal Card: Solid Blue

No.	Description			
			Illegal Card	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.
				(RS485 Card Reader Mode) Flicker Red: Connection Exception.

3 Terminal Connection

3.1 Terminal Description

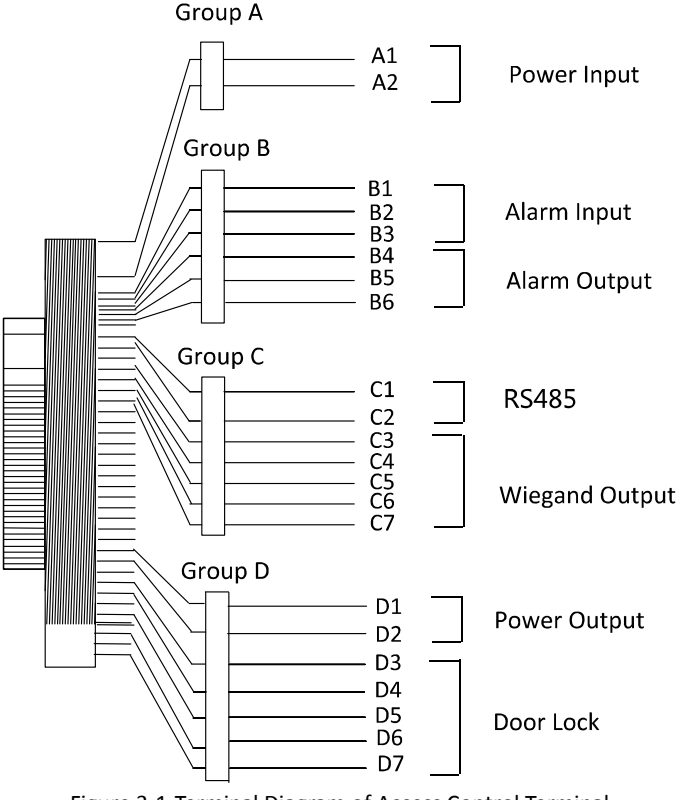

Figure 3-1 Terminal Diagram of Access Control Terminal

Table 3-1 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	RS485 Communication Port	Yellow	485 +	RS485 Wiring
	C2		Blue	485 -	
	C3	Wiegand Output	Green	W0	Wiegand Wiring 0
	C4		White	W1	Wiegand Wiring 1

Line Group	No.	Function	Color	Terminal Name	Description
	C5		Orange	LED-ERR	Error Prompt LED Indicator Wiring
	C6		Purple	BEEP	Beep Siren Wiring
	C7		Grey	TAMPER	Tampering Alarm Wiring
Line Group D	D1	Power Output	Red	+12V	Power Output
	D2		Black	GND	GND
	D3	Door Lock	White/Purple	NC	Lock Wiring
	D4		White/ Yellow	COM	
	D5		White/Red	NO	
	D6		Yellow/Green	SENSOR	Door Contact Signal Input

Line Group	No.	Function	Color	Terminal Name	Description
	D7		Yellow/Grey	BUTTON	Exit Door Wiring

4 Wiring Description

4.1 External Device Wiring Overview

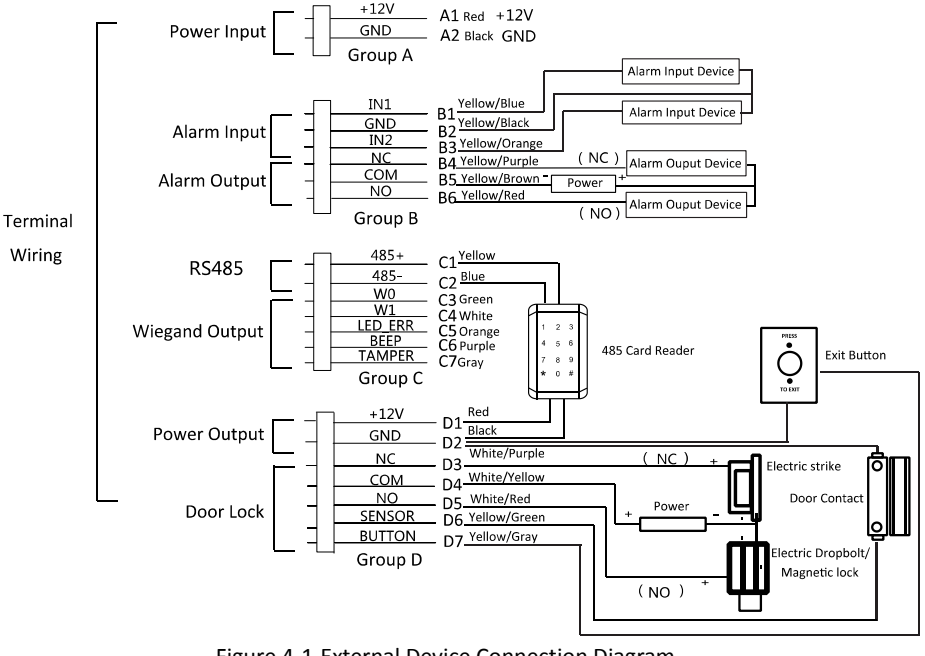

Figure 4-1 External Device Connection Diagram

4.2 The Wiring of External Card Reader

4.2.1 The Wiring of External RS485 Card Reader

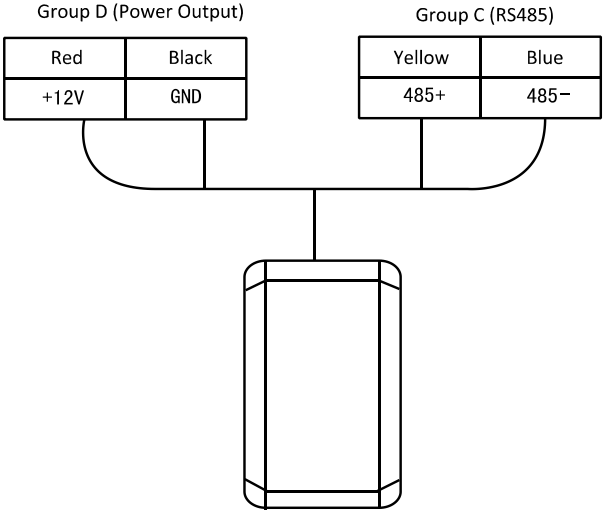

Figure 4-2 External RS485 Card Reader Connection Diagram

NOTE

- When connected to the external card reader, the terminal only supports RS485 communication method (External Wiegand card reader is not supported).
- Set the dial-up of the external card reader as 2 when connected to the access control terminal.

4.3 The Wiring of Electric Lock and Door Magnetic

4.3.1 The Wiring of Electric Lock

Group D (Door Lock)

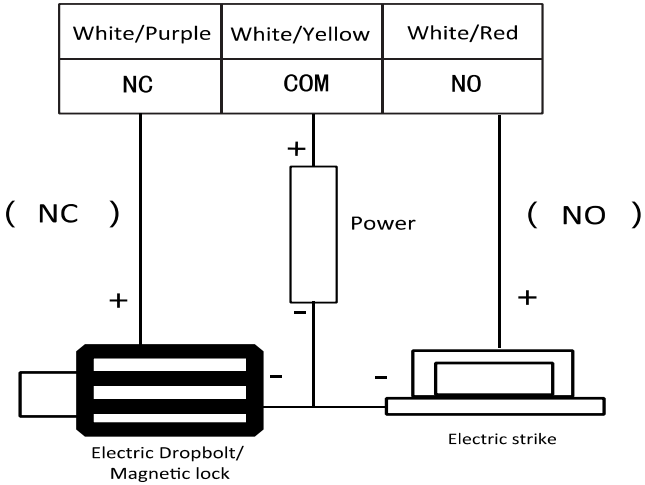

Figure 4-3 The Installation of Electric Dropbolt, Magnetic Lock, and Electric Strike

NOTE

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.

4.3.2 The Wiring of Door Contact

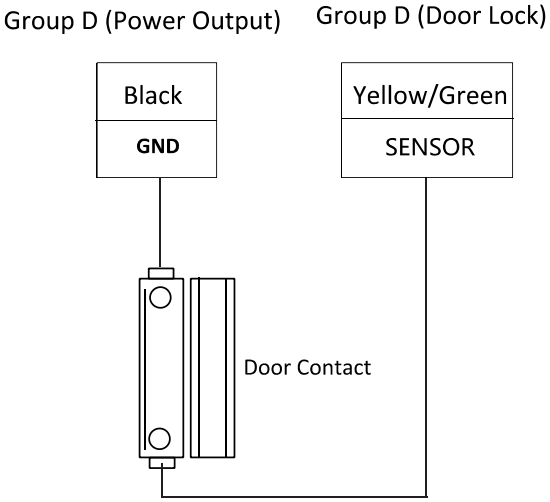

Figure 4-4 The Installation of Door Contact

4.4 The Wiring of Exit Button

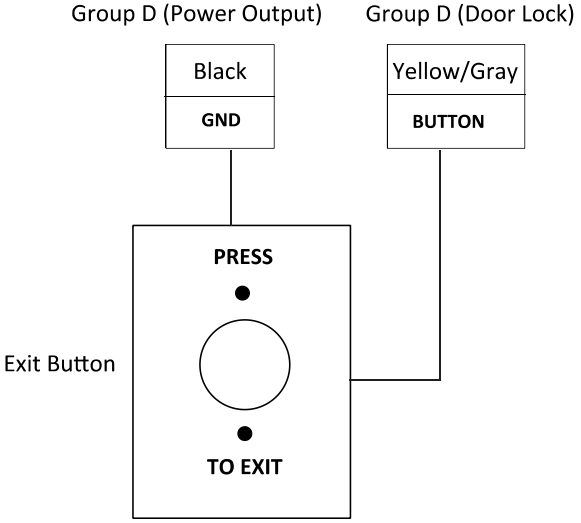

Figure 4-5 The Installation of Exit Button

4.5 The wiring of Alarm Input

Group B (Alarm Input)

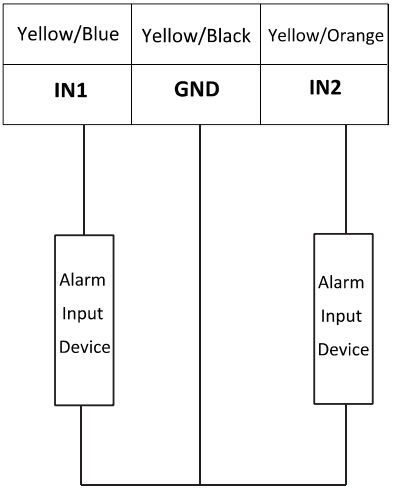

Figure 4-6 Alarm Input Connection

4.6 The Wiring of External Alarm Device

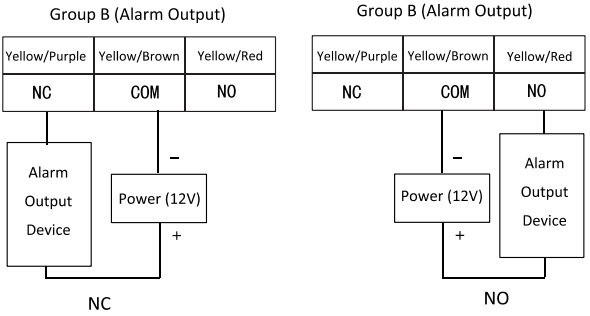

Figure 4-7 The Installation Diagram of External Alarm Device

4.7 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 RS485 communication port.

NOTE

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.

4.7.1 The Wiring of Wiegand Output

Group C (Wiegand Output)

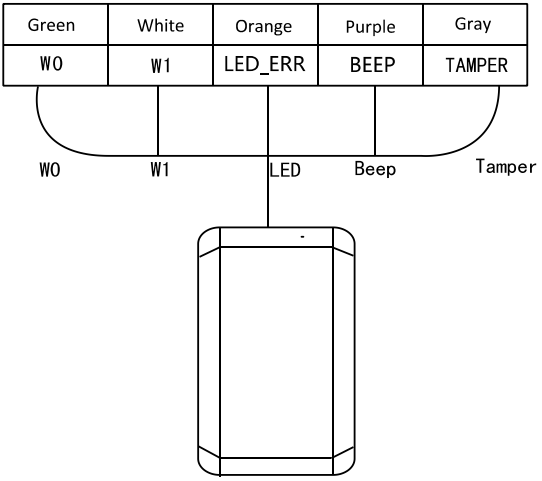

Figure 4-8 Wiegand Connection Diagram

NOTE

- When the access control terminal works as a card reader, you must connect the **LED-ERR and BEEP** 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 Wiegand mode can be configured in **Network Parameter -> Wiegand Mode** (Wiegand 26/Wiegand 34).
- The distance of Wiegand communication should be no longer than 80 m.

4.7.2 The Wiring of RS485 Output

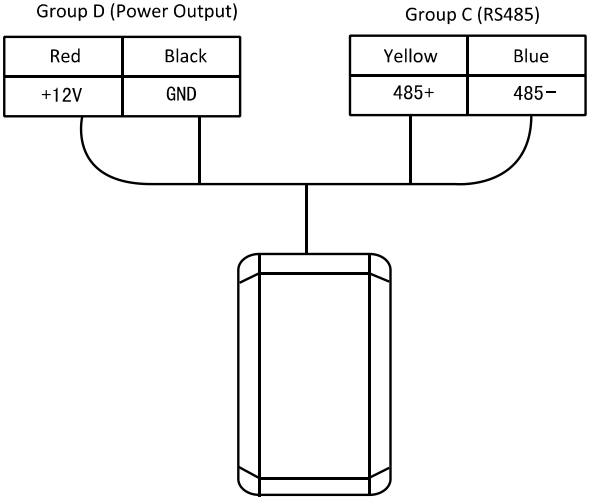

Figure 4-9 RS485 Connection Diagram

NOTE

- 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 RS485 card reader, the default RS485 address is 1. RS485 address can also be configured in **System Parameter -> Serial Port Settings**.

5 Activating the 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.

5.1 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.

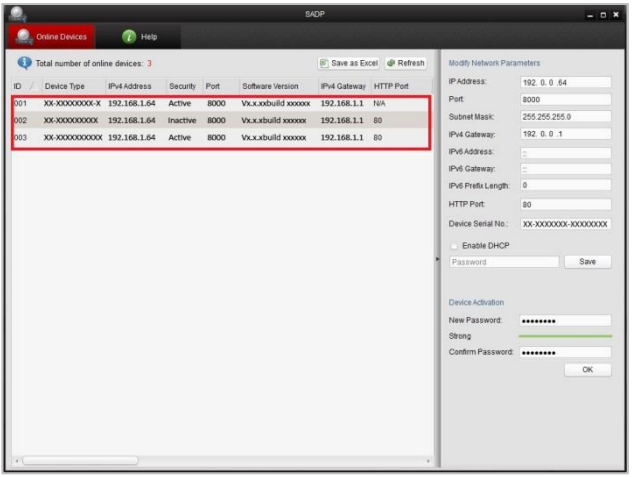

Figure 5-1 SADP Interface

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 **OK** to save the password.

   You can check whether the activation is completed on the pop-up window.

   If activation failed, please make sure that the password meets the requirement and then try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

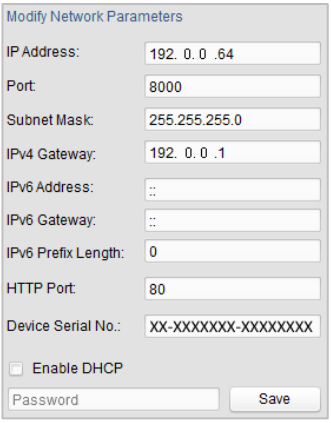

Figure 5-2 Modify Network Parameters Interface

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

5.2 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.
2. Click the icon on the upper-left side of the page, select **Access Control** to enter the control panel.

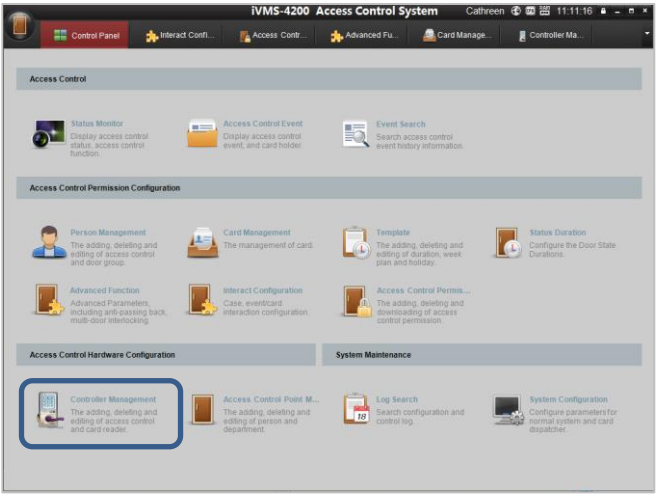

Figure 5-3 Control Panel Interface

3. Click the **Controller Management** icon to enter the Controller Management interface, as shown in the figure below.

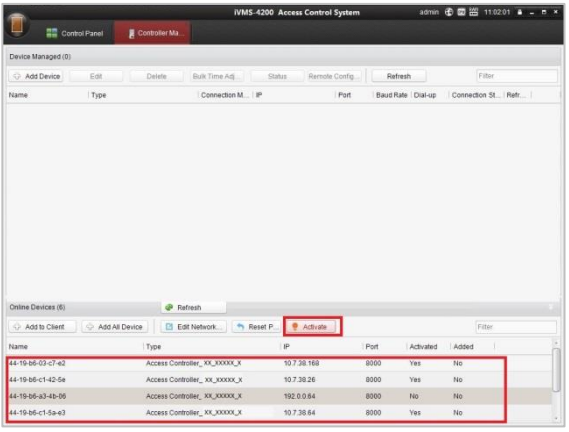

Figure 5-4 Device List

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.

Figure 5-5 List Selecting Interface

6. 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.*

7. Click **OK** button to start activation.
8. Click the Edit Network... button to pop up the Network Parameter Modification interface.
9. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
10. Input the password to activate your IP address modification.

6 Basic Operation

Before You Start:

- You should activate the device before the first login. Otherwise, after powered on, the system will switch into activaon notifying interface. For detailed information about activation, see Chapter 5.

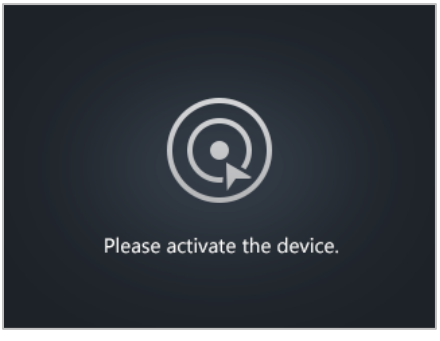

Figure 6-1 Activation Notifying Interface

- You should enter the default password for the first login.

  Enter **System Settings -> System Parameter –> Login Password** to reset the login password.

  The default password is 12345.

Steps:

1. The device enters the initial interface automatically after powered on.

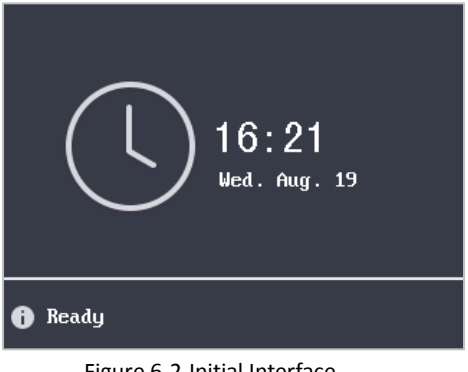

Figure 6-2 Initial Interface

2. Long-click the **#** key to enter the password authentication interface.

Figure 6-3 Password Authentication Interface

3. Enter the default configuration password.

- Click the **#** key to confirm the settings. If the configuration password authentication failed, the system will return to the initial interface, and if the configuration password is successfully authenticated, the system will enter the menu operation interface

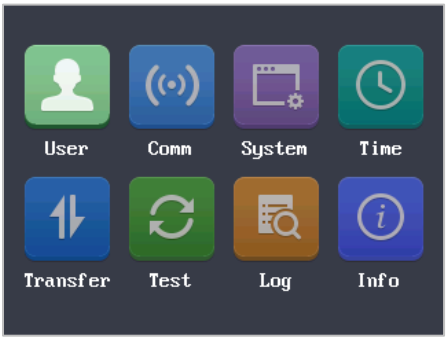

Figure 6-4 Menu Operation Interface

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

6.1 User Management

Purpose:

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

Steps:

1. Move the cursor to **User** (user management) with the direction keys.
2. Click the **#** key to enter the user management interface.

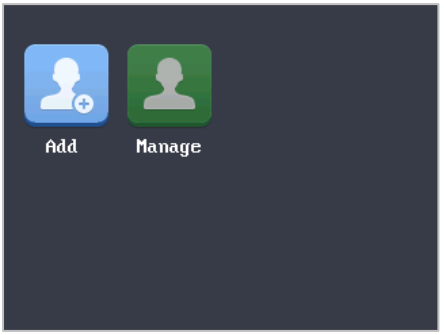

Figure 6-5 User Management Interface

6.1.2 Adding User

Purpose:

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

Steps:

1. Move the cursor to **Add** (add user) by using the direction keys.
2. Click the **#** key to enter the card registration interface.

Figure 6-6 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.

1) Click the key to enter the editing mode.
2) Enter the card number into the textbox.
3) Click the key to exit the editing mode.

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

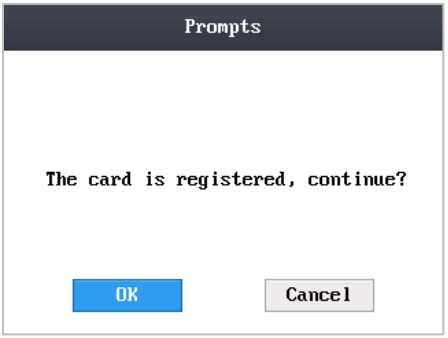

Figure 6-7 Card Registration PoP-Up Window

1) Move the cursor to the **OK** button, and click the **#** key to enter the fingerprint registration interface.

Figure 6-8 Fingerprint Registration Interface

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

NOTE

- 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.

6.1.2 Managing User

1. Move the cursor to **Manage** (edit user) by using direction keys on the user management interface.
2. Click the **#** key to enter the managing user interface.

Searching User

Steps:

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

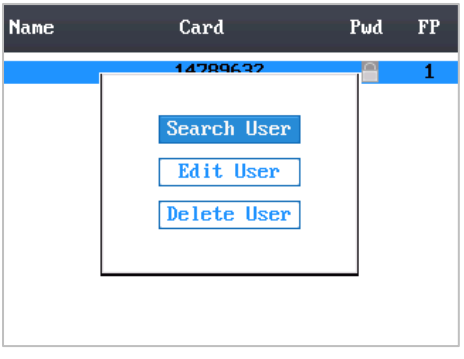

Figure 6-9 Managing User Interface

3. Move the cursor to **Search User**.
4. Click the **#** key to enter the searching interface.

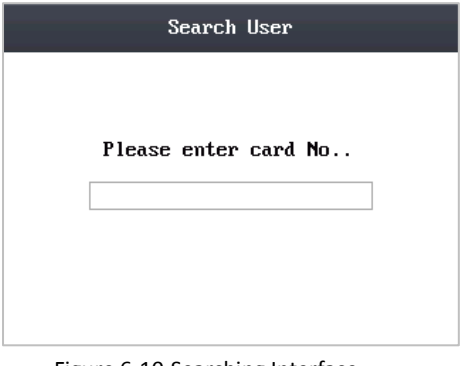

Figure 6-10 Searching Interface

5. Enter the card number into **Please enter card No.** textbox.
6. Click the **#** key to view the basic information about the card holder.

Editing User

Steps:

1. Move the cursor to a user by using direction keys.
2. Click the **#** key to popup an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Editing User**.
4. Click the **#** key to enter the editing interface.

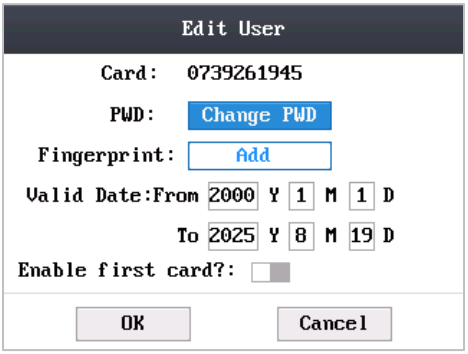

Figure 6-11 Editing Interface

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.

     NOTE

     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) Enter a new password.
     3) Confirm the new password.

Figure 6-12 Password Changing Interface

- Changing the valid date

  You can set the start/end time of the user's permission.

  Click the ⏎ key to enter/exit the editing mode.

- Enabling first card

  Click the **#** key to enable first card.

  NOTE

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

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

Deleting the User

Steps:

1. Move the cursor to the user by using direction keys.
2. Click the **#** key to pop up an interface for selecting corresponding operations. (Figure 6-9)
3. Move the cursor to **Delete User**, and click 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.

   NOTE

   DS-K1T105 series model does not support this function.

5. Click the **#** key to finish the deleting operation.

NOTE

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

6.2 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. Click the **#** key to enter the communication settings interface.

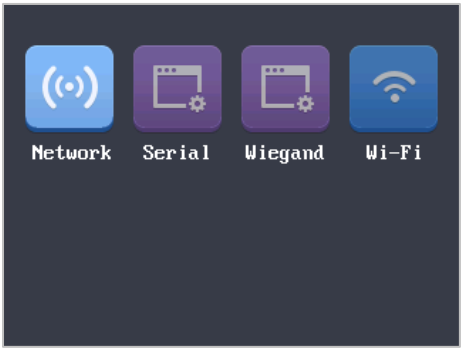

Figure 6-13 Communication Settings Interface

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 RS485 card reader, serial port parameters include working mode, Baud Rate, and RS485 address.

Wiegand Settings: When the access control terminal works as a Wiegand card reader, Wiegand parameters involve whether to enable the Wiegand connection, and the Wiegand mode.

Wi-Fi: You can enable the Wi-Fi function.

6.2.1 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. Click the **#** key to enter the network settings interface.

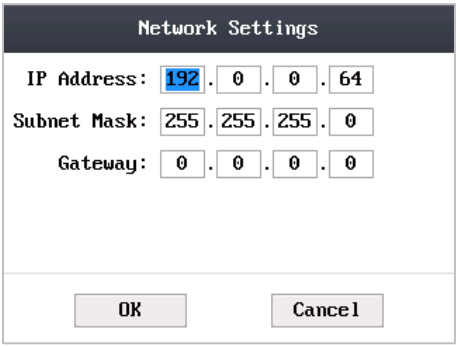

Figure 6-14 Network Settings Interface

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

   NOTE

   Click the key to enter/exit the editing mode.

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

6.2.2 Serial Port Settings

Purpose:

When the access control terminal works as the RS485 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. Click the **#** key to enter the serial port settings interface.

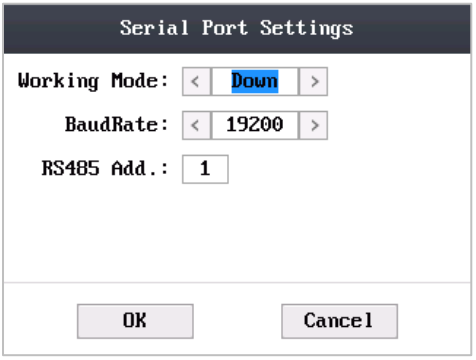

Figure 6-15 Serial Port Settings Interface

3. Modify parameters of the serial port, including working mode, Baud Rate, and RS485 address.

   Working Mode: Up serial port and down serial port are supported.

   NOTE

   Set the working mode of the serial port as **Down** (downstream) if the access control terminal is connected to the external card reader.

   Baud Rate: The current suppoted Baud Rate is 19200.

   RS485 Address: When the access control terminal works as a RS485 card reader, the default RS485 address is 1.

NOTE

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

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

6.2.3 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. Click the **#** key to enter the Wiegand settings interface.

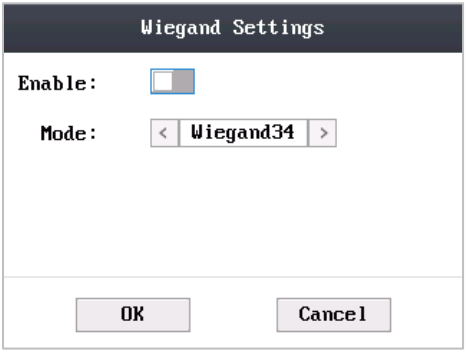

Figure 6-16 Wiegand Settings Interface

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

Enable the Wiegand: Select whether to enable the Wiegand.

NOTE

Click the **#** key to enable first card.

Wiegand Mode: The default Wiegand mode is Wigand 34.

NOTE

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

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

6.2.4 Wi-Fi Settings

Steps:

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

Figure 6-17 Wi-Fi Enabling

3. Move the cursor to and click the **#** key to enable the WLAN.

Figure 6-18 Wi-Fi Selection

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

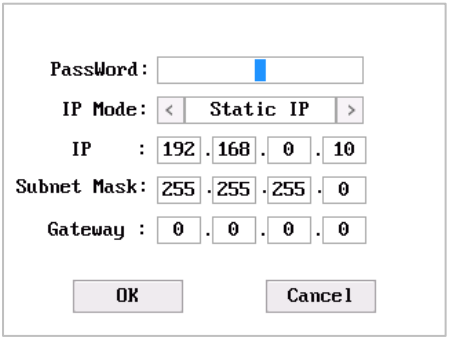

Figure 6-19 Wi-Fi Settings

5. Enter the password of the network.
6. Edit the IP mode, IP address, subnet mask, and gateway address.
7. Move the cursor to the **OK** button, and click the **#** key.

NOTE

Click the key to enter and exit the editing mode.

6.3 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. Click the **#** key to enter the system parameters interface.

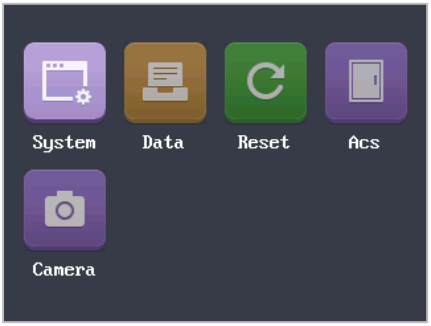

Figure 6-20 System Settings Interface

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).

6.3.1 Setting System

Steps:

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

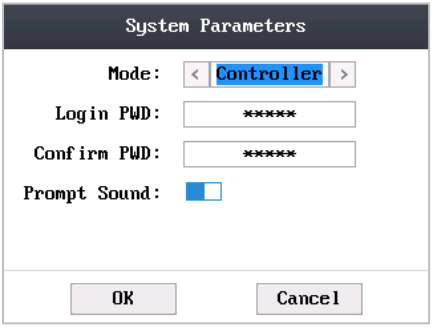

Figure 6-21 System Parameters Interface

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 into the interface of the new mode.

   NOTE

   If the access control terminal works as a card reader, you should configure the serial port settings. See details in 6.2.2.

   Login Password: To reset the login password of the device, you should enter a new password, and confirm it.

   Voice Prompts: 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.

   - Beep three times: legal card.
   - Beep four times: illegal card.

NOTE

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

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

6.3.2 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 managemen**t) by using direction keys in the system settings Interface.
2. Click the **#** key to enter the data management interface.

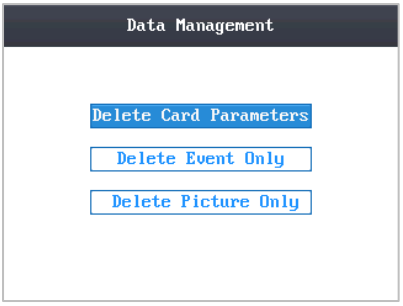

Figure 6-22 Data Management Interface

3. 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.

NOTE

   This function is only supported by terminal with the model of –C.
4. Click the **#** key.

6.3.3 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. Click the **#** key to enter the restore settings interface.

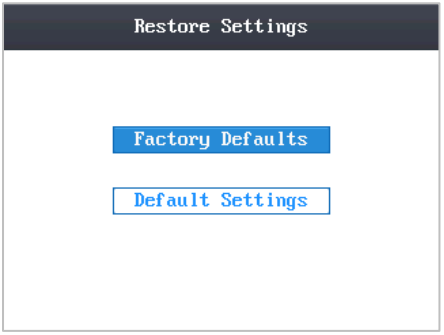

Figure 6-23 Restore Settings Interface

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

6.3.4 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. Click the **#** key to enter the door settings interface.

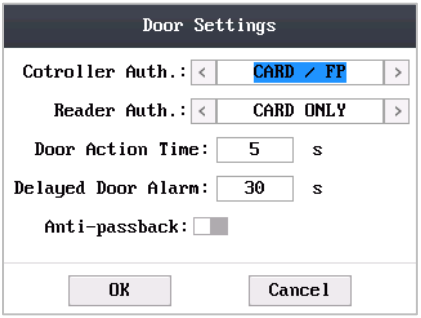

Figure 6-24 Door Settings Interface

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, Password & Fingerprint, Card & Password & Fingerprint.

   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.

NOTE

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

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

6.3.5 Setting the Camera

Purpose:

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

NOTE

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. Click the **#** key to enter the camera settings interface.

Figure 6-25 Camera Settings Interface

3. Edit camera parameters.

   Enable Face Detection: When enabling face detection, the system can detect the face captured by the camera.

   Enable Card No. Overlay: When enabling card No. overlay, captured pictures can be overlaid on the card information.

   Display Picture: When enabling to display the picture, captured pictures can display on the screen.

NOTE

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

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

6.4 Time Settings

Steps:

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

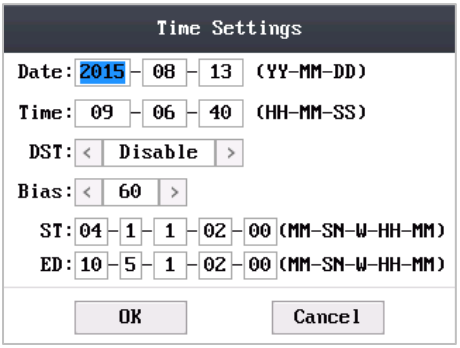

Figure 6-26 Time Settings Interface

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.

NOTE

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

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

6.5 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. Click the **#** key to enter the upload/download interface.

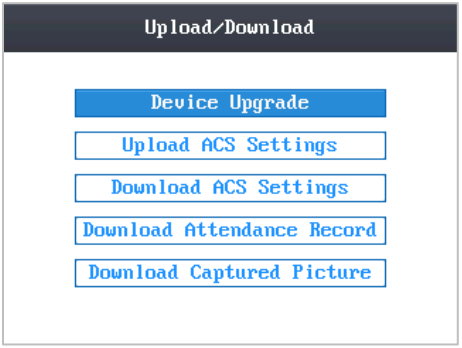

Figure 6-27 Upload/Download Interface

4. Move the cursor to Device Upgrade, Upload Access Settings, Download Access Settings, Download Attendance Record, or Download Captured Picture.
   Device Upgrade: The system can automatically read the upgrading information from the USB, and upgrade the device.
   Upload Access Settings: The system can automatically read the access parameters from the USB, and upload them to the device.
   Download Access Settings: The system can automatically download access parameters into the USB.
   Download Attendance Record: The system can automatically download attendance records into the USB.
5. **Download Captured Picture:** The system can automatically download captured pictures into the USB. Click the **#** key.

6.6 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. Click the # key to enter the test interface.

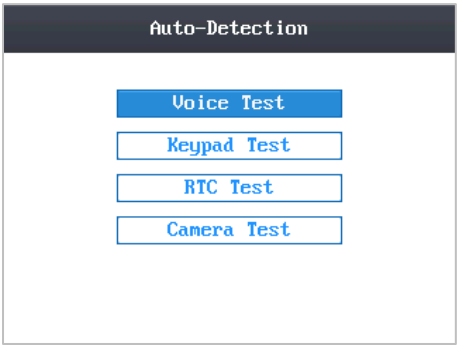

Figure 6-28 Test Interface

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.

   NOTE

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

6.7 Log Query Settings

Steps:

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

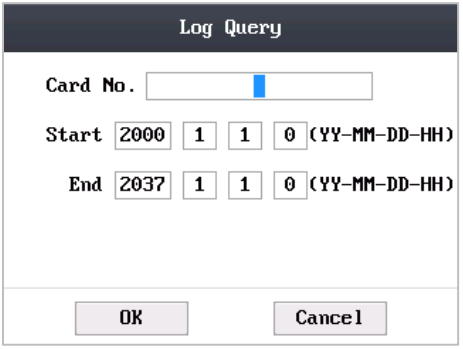

Figure 6-29 Log Query Interface

3. Enter the card number.
   - Enter the card number by swiping the card.
     Place the card close to the screen.
   - Enter the card number manually.
     1) Click the key to enter the text editing mode.
     2) Enter the card number in the textbox.
     3) Click the key to exit the text editing mode.
4. Set the start/end time.
   Click the key to enter and exit the editing mode.
5. Move the cursor to the **OK** button, and click the **#** key.

NOTE

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

6.8 System Information

Steps:

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

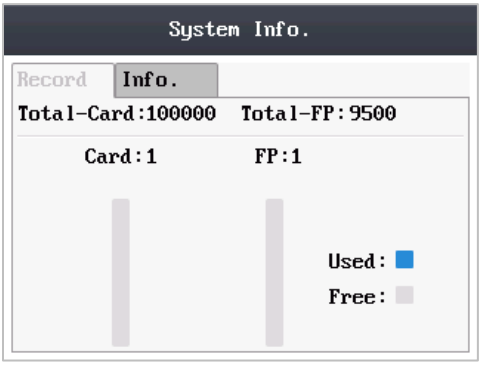

Figure 6-30 System Information Interface

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.

  NOTE

  The default maximum card amount is 100,000.

  Fingerprint Capacity: It refers to the maximum amount of fingerprints.

  NOTE

  - Fingerprint capacity only supports devices with fingerprint registration function.
  - The default maximum fingerprint amounts of devices with fingerprint registering function are as follows.

    Optical device: 9500
  - 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 6-31 Device Information Interface

First Choice for Security Professionals