HIKVISION

Face Recognition Terminal

Quick Start Guide

Quick Start Guide

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

This manual is applied for face recognition terminal.

Name	Model
Face Recognition Terminal	DS-K5603-Z
	DS-K5603T-Z

Scan the QR code to get *User Manual of DS-K5603 Series Face Recognition Terminal*. Note that mobile data charges may apply if Wi-Fi is unavailable.

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

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.

● Suitable for mounting on concrete or other non-combustible surface only.

● Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
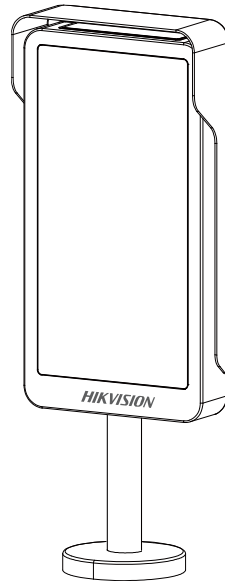
Table of Contents

Chapter 1 Overview

1.1 Introduction

DS-K5603-Z and DS-K5603T-Z face recognition terminal, designed with TX1 system, can be applied in the scenarios of examination hall, railway station, bank, building, hotel, etc., which needs identity verification.

1.2 Main Features

● 10.1-inch and 1280 × 800 resolution capacitive touch screen

● 2 MP wide-angle dual-lens

● Max. 10,000 face pictures, Max. 10,000 face pictures in blacklist, and Max. 50,000 comparing events for DS-K5603-Z face recognition terminal

● Max. 50,000 face pictures, Max. 10,000 face pictures in blacklist, and Max. 100,000 comparing events for DS-K5603T-Z face recognition terminal

● Multiple authentication modes: authentication by card + face picture, by auto mode (card + face picture or face picture)

● Identity authentication by QR code instead of card

  Note: The device should connect an external card reader or the card swiping function cannot be used.

● Two network interfaces

  Each network interface can auto visit the EHome server separately.

● Applies persons in blacklist via iVMS-4200 client software.

● Applies face pictures from the system to the device via EHome protocol

● Uploads blacklist authentication and blacklist event, and displays them on the main screen

- Imports face pictures to the device via the USB interface
- Exports face pictures and events from the device via the USB interface
- Communication with access controller via RS-232 communication mode and communication with the third party devices via RS-485 communication mode
- Uploads offline events
- Audio prompt

Chapter 2Appearance

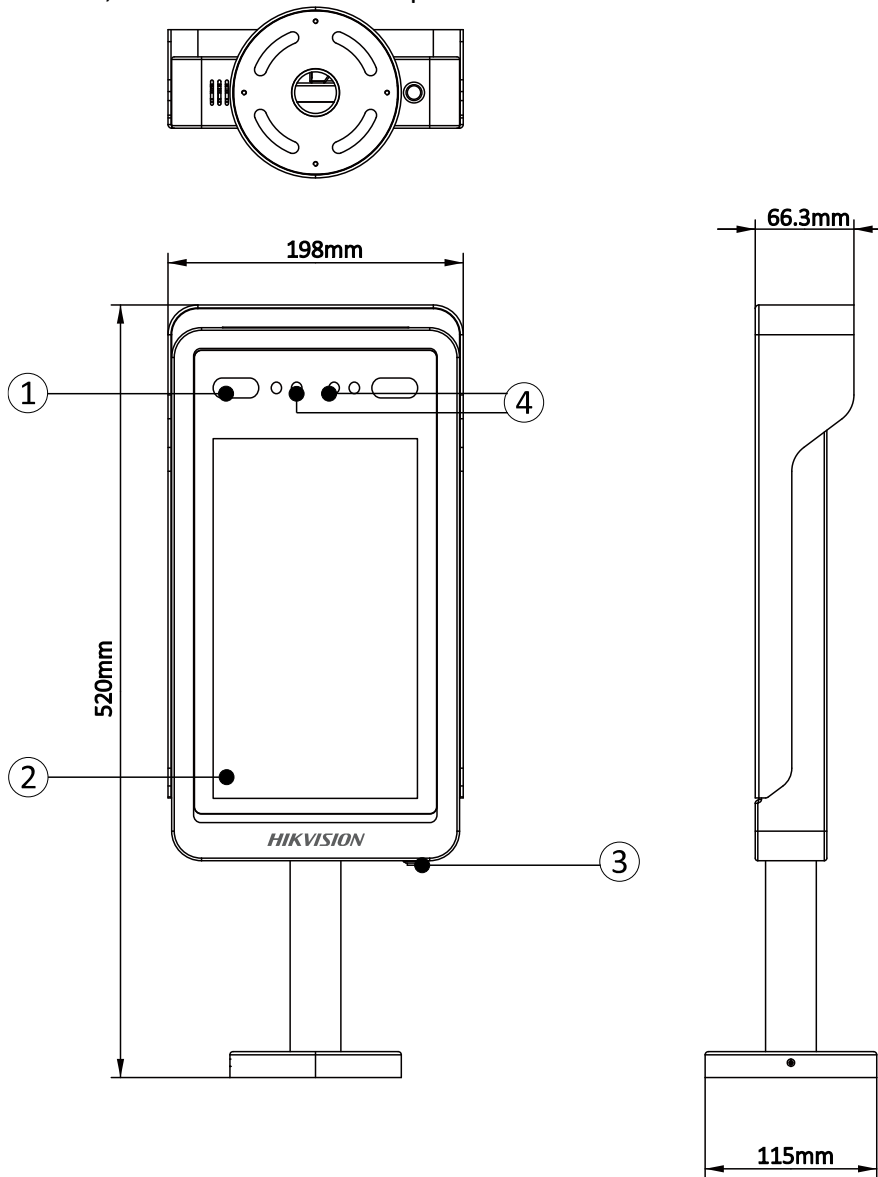The device appearance, dimensions and descriptions are as follows.

Table 2-1 Appearance Description

| No.	Description
1	Supplement Light
2	Display Screen
3	Power Button
4	Cameras

Chapter 3Installation

Installation Environment:

● Avoid backlight and direct sunlight.

● If installing outdoors, install a sun shield over the device.

● The device should be installed on the pedestals of the barriers.

Before you start:

● Drill holes on the barrier pedestal's top panel according to the picture displayed below

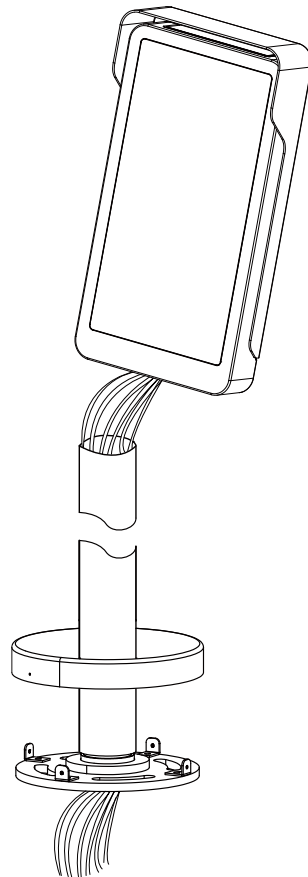● Riveted waterproof nut under the top panel.
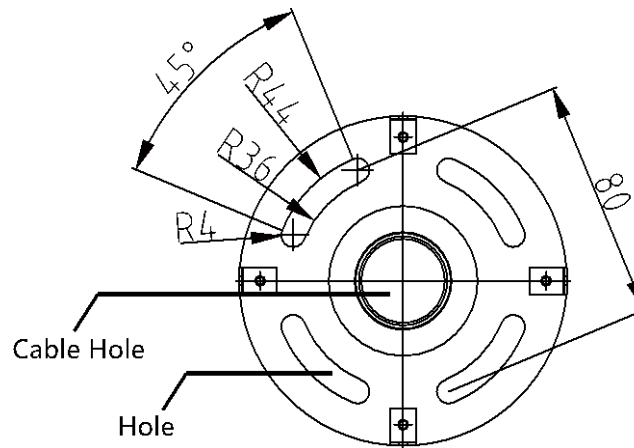
Notes:

● SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.

● The waterproof nut model is BS-M6-1.

Steps:

1. Route the cables through the pipe from top to bottom and thread them through the cable holes on the barrier pedestal's top panel.

2. Wire the cable with the terminals in the barrier pedestal.
3. Raise the pipe and make sure the pipe and the pedestal top panel are vertical.
4. Secure the pipe with hex socket screws.
   1) Rotate the pipe and align the four holes on the round panel with the holes on the pedestal top panel.
   2) Thread the supplied four M6 × 15 socket screws from up to down through the four holes respectively. (Do not tight up.)
   3) Rotate the pipe and make sure the device display screen is in the correct direction.
   4) Tight the four screws to secure the device on the barrier pedestal.
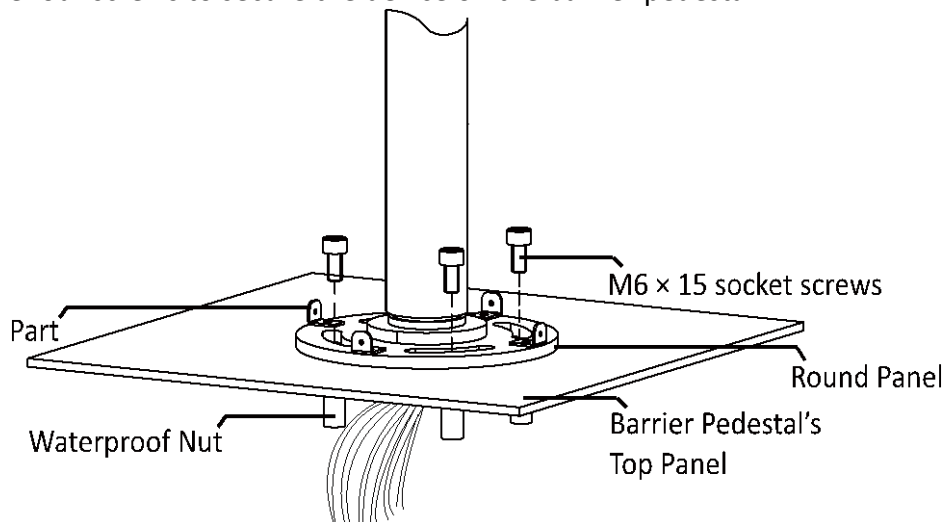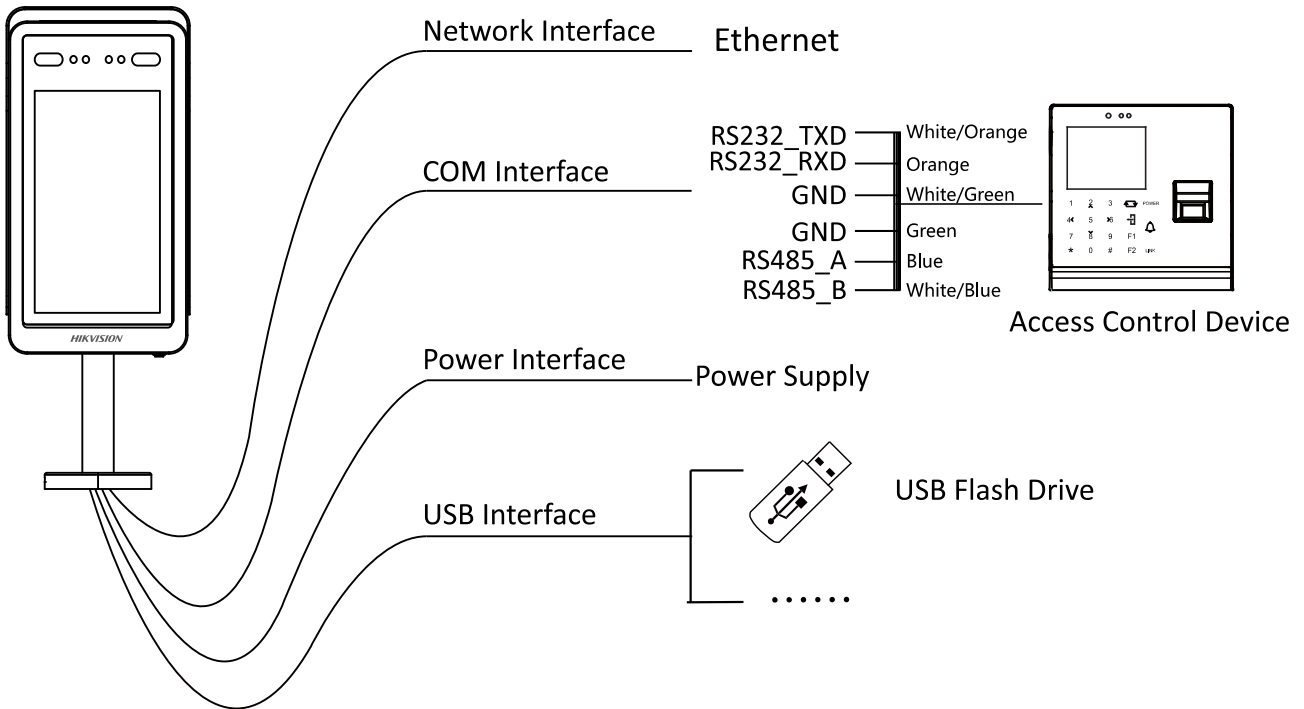

5. Install the cover on the round panel.

1) Move the cover on the round panel.
2) Rotate the cover and hide the hole on the cover and align the hole with one of the four small parts on the round panel.
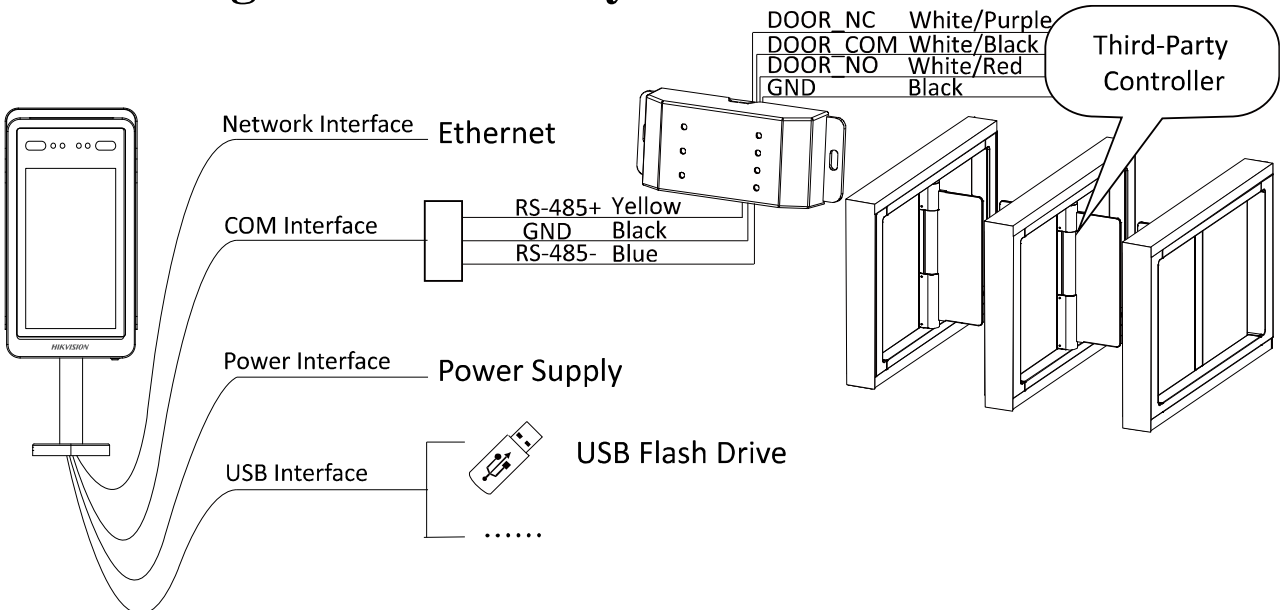3) Secure the cover and the round panel with one supplied M2 screw.

Cover

M2 Screw

Barrier Pedestal's
Top Panel

Waterproof Nut
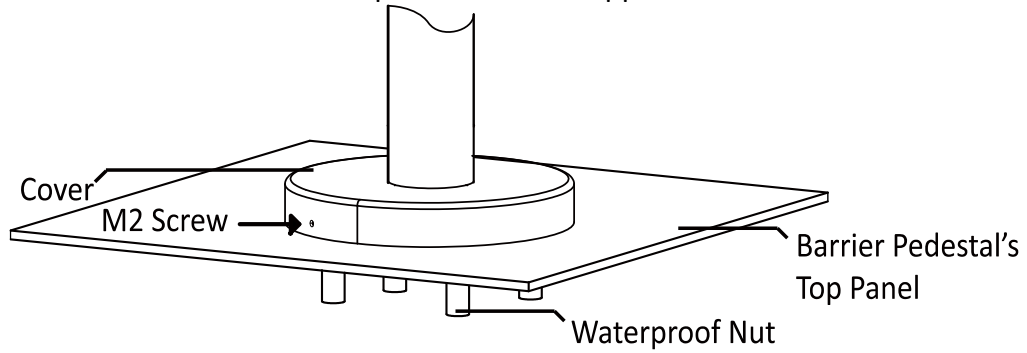
Chapter 4 Wiring

4.1 Wiring Access Control Terminal

The picture displayed below describes the access control terminal's wiring.

Network Interface — Ethernet

COM Interface
- RS232_TXD — White/Orange
- RS232_RXD — Orange
- GND — White/Green
- GND — Green
- RS485_A — Blue
- RS485_B — White/Blue

Access Control Device

Power Interface — Power Supply

USB Interface — USB Flash Drive ......

4.2 Wiring the Third-Party Turnstile

- DOOR_NC — White/Purple
- DOOR_COM — White/Black
- DOOR_NO — White/Red
- GND — Black

Third-Party Controller

Network Interface — Ethernet

COM Interface
- RS-485+ — Yellow
- GND — Black
- RS-485- — Blue

Power Interface — Power Supply

USB Interface — USB Flash Drive ......

Notes:

- For details about I/O output module, see *User Manual of I/O Output Module* or scan the QR code below to view the manual via your mobile device.

- The device can also access to the third-party turnstile via RS-485 to Wiegand module. For details, see User Manual of RS-485 to Wiegand Module or scan the QR Code below to view the manual via your mobile device.

Chapter 5Device Activation

Purpose:

You are required to activate the device first before using it.
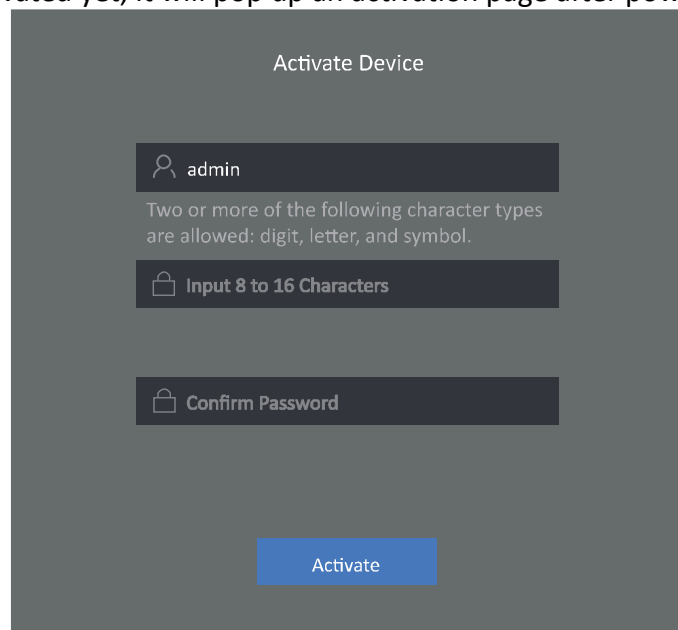
Activation via device, activation via SADP, and activation via client software are supported.

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 Device

If the device is not activated yet, it will pop up an activation page after powering on.

Steps:

1. Create a password for the admin user.
2. Confirm the password.
3. Tap **Activate**.

> ⚠️ **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.*

5.2 Activating via SADP Software

Purpose:

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

password.

Get the SADP software from the supplied disc, 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.
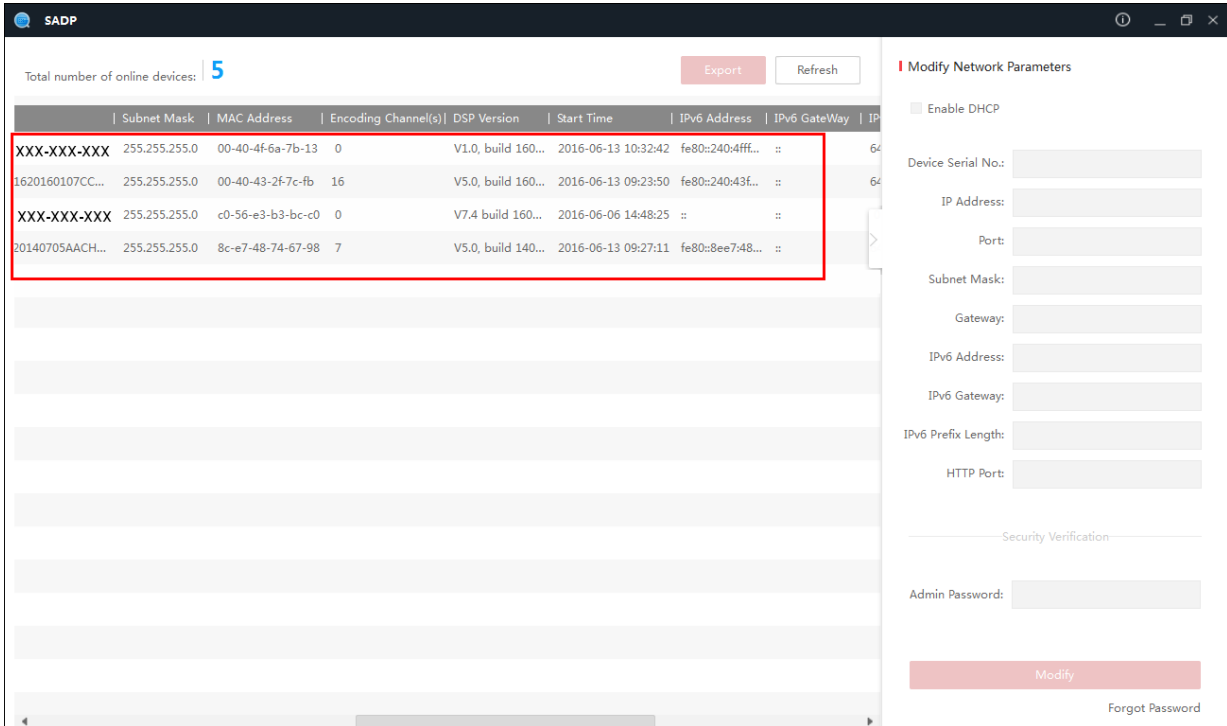
3. Create a password and input the password in the password field, and confirm the password.

> ⚠️ **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.

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

5.3 Activating via Client Software

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

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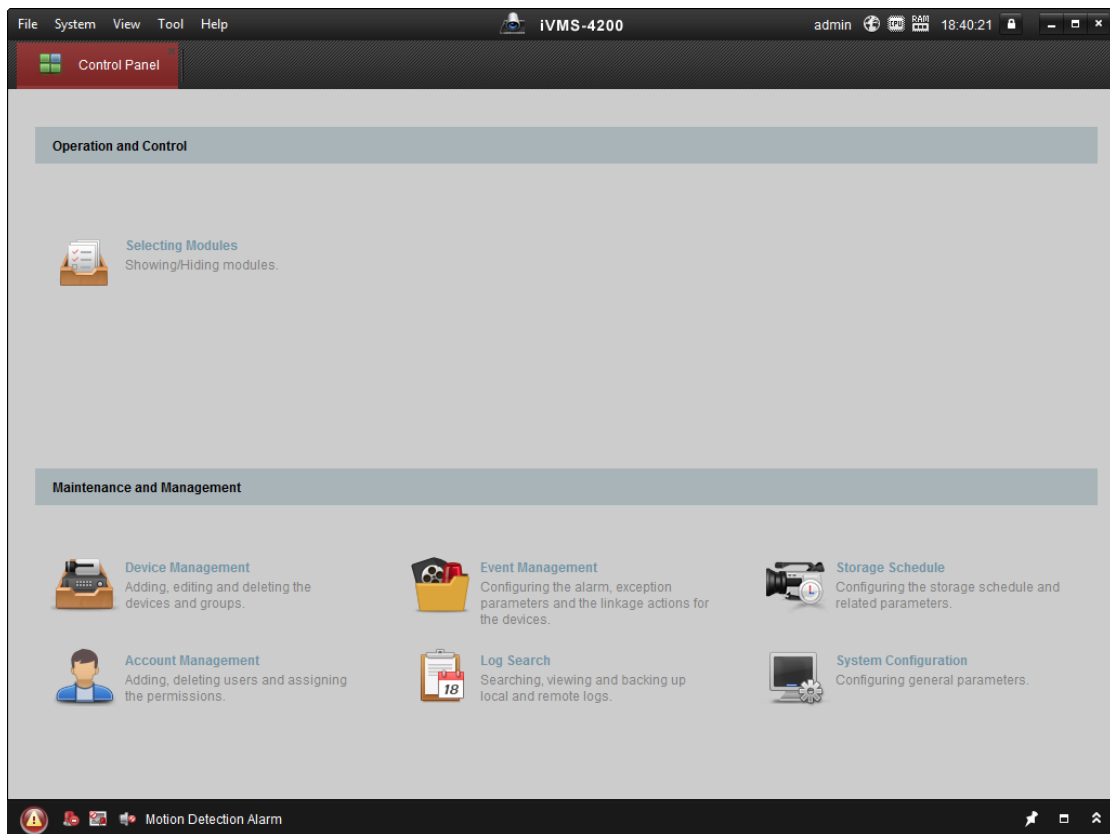
2. Click **Device Management** to enter the Device Management interface.
3. Check the device status from the device list, and select an inactive device.

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.*

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.

After activation, you will enter the initial page.

Chapter 6Basic Operation

Purpose:

After entering the administrative backend, you can manage users, set communication parameters, change device password, manage and maintain data, and view device information.

6.1 Application Mode Settings

Purpose:

After activating the device, you should select an application mode for better device application.

Steps:

1. In the Welcome page, select **Indoor** or **Others** from the drop-down list.
2. Tap **OK** to save the settings.
   Note: You can also change the settings in *Section 6.4 System Settings*.

6.2 Enter Administrative Backend

Purpose:

You should enter the de administrative backend before setting other parameters.

Steps:

1. On the initial page, long tap the screen for 3s to enter the input password page.
2. Input the password in the text box. The password here refers to the activation password.
3. Tap **OK** to enter the backend.
4. (Optional) Tap **Exit** at the lower left corner to exit the backend.

6.3 Communication Settings

Purpose:

You can set the device network parameters and COM parameters.

6.3.1 Setting Network Parameters

Purpose:

The device contains two network interfaces. You can select to enable one of them or both of them, and set the network parameters, including IP address, gateway, and subnet mask. The device can use the network interface to communicate with iVMS-4200 control client.

Steps:

1. In the backend, tap to enter the Communication Settings page.
2. Tap **Network** to enter the Network tab.
3. Set the network interface parameters, including IP address, subnet mask, and gateway.
   Notes:
   ● The device IP address and the PC's IP address should be in the same LAN.
   ● If using both of the network interfaces at the same time, the IP addresses of network interface 1 and 2 should be different to avoid IP address confliction.

4. Tap **Logout** to exit the page and save the parameters.

6.3.2 Setting COM Parameters

Purpose:

The device can be connected to other access control device via the COM interface. After selecting the baud rate, you can connect the device to other access control devices via RS-232 protocol or RS-485 protocol. For details about device linkage, see *6.13 Linking Access Control Device*.

Steps:

1. Tap **COM** in the Communication Settings page to enter the COM tab.
2. Select a baud rate for RS-232 protocol and RS-485 protocol.
   The parameters will be effective as soon as you have selected.

6.4 System Settings

Purpose:

In the System Settings page, you can set the parameters of device ID, voice volume, live view in IR mode, blacklist matching threshold, device authentication mode, QR code scanning, application mode, blacklist authentication mode, power saving mode, ID card reader auto adjust white light brightness, IR light brightness, white light brightness, and Max. white light brightness.

Steps:

1. In the backend, tap to enter the System Settings page.

2. Set the parameters.
   The parameters descriptions are as follows:

Parameter Item	Description
Device ID	Set the device ID for device management. When the device is connected to a peripheral (access controller) via the RS-485 protocol, the device ID is the RS-485 protocol's DIP switch address. **Note:** The device ID should be numbers between 1 and 255.
Live View in IR Mode	The live view on the device screen will enter the IR mode.
Voice Volume	Adjust the voice prompt volume.
Blacklist Matching Threshold	Set the blacklist matching threshold when comparing user with the users in the blacklist. Higher the value, lower the chance a user will be matched in the blacklist.
Device Authentication Mode	You can select the authentication mode. **Auto:** Authenticate via face picture, or face picture and card. When authenticating, if no card swiped, the device only starts 1:N authentication.

Parameter Item	Description
	If swiping card, the device will starts 1:1 authentication according to the face picture on the card.
	Face Picture: Authenticate via face picture only.
	Card + Face Picture: Authenticate via face picture and card
	Note: Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
QR Code Scanning	Enable or disable the QR code scanning function. If enabling, the device camera can scan the QR code to authenticate instead of swiping card. *Notes:* ● By default, the function is disabled. ● You can get the QR code from iVMS-4200 control client. For details about the operation, see the user manual of iVMS-4200 control client.
Application Mode	You can select the device application mode. You can select either others or indoor according to actual environment.
Blacklist Authentication Mode	Enable or disable the function. If enabling, you should apply blacklist via iVMS-4200 control client before operation. After authentication completed, the system will judge whether the user is in the blacklist or not. *Notes:* ● By default, the function is disabled. ● For details about applying users in blacklist, see the user manual of iVMS-4200 control client.
Power Saving Mode	Enable or disable the function. If enabling, the device power will be saved.
ID Card Reader	If the device has connected to an external ID card reader, you should select an ID card reader model. If not, select **None**. *Notes:* ● You should wire the ID card reader to the device USB interface if you want to connect an external ID card reader. ● The available ID card reader model are DS-K1F1110-A and DS-K1F1110-AB.
Auto Adjust White Light Brightness	If enabling the function, the device will adjust the white light brightness automatically according to the actual illumination. And you can set the max. brightness value. If disabling the function, the device supplement white light

Parameter Item	Description
	brightness will not be changed.
IR Light Brightness	Set the IR light's brightness. 0 represents the IR light is turned off.
White Light Brightness	Set the white light's brightness. 100 represents the most brightness, and 1 represents the darkest. 0 represents off.
Max. White Light Brightness	When the auto adjust white light brightness is enabled, you can set the brightness value. 100 represents the most brightness, and 1 represents the darkest. 0 represents off.

3. Click to save the settings.

6.5 User Management

Purpose:

Manually add user information for authentication. You can add user name, card No., and face picture for the user. You can also view, search, and edit the added user.
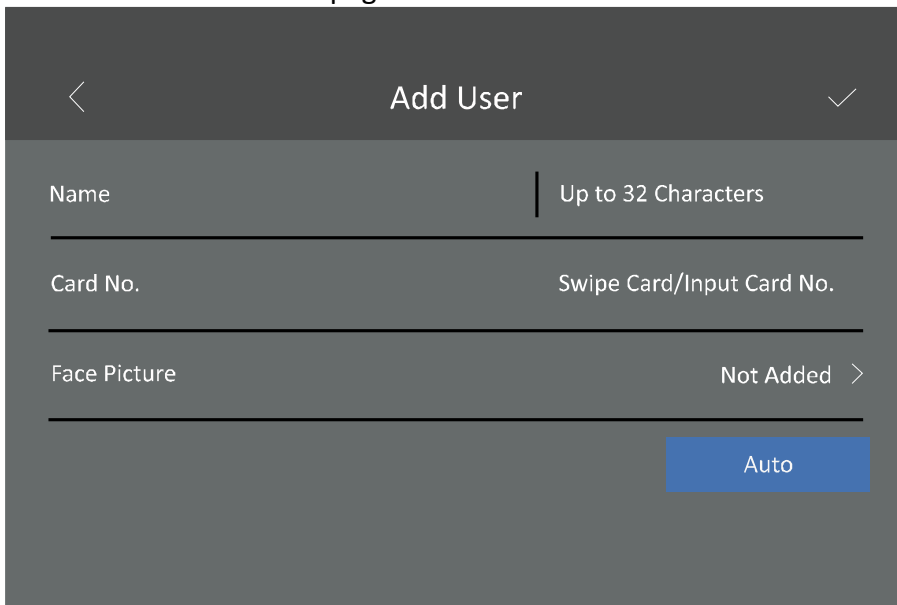
6.5.1 Adding User

Purpose:

You can manually input the user information to add the user.

Steps:

1. In the backend, tap to enter the User Management page.
2. Tap **Add User** to enter the Add User page.

3. Tap the Name text box and input the user name.
   Input the user name via the popped up soft keyboard.
4. Tap the Card No. text box and input your card No.

Or you can swipe card on the device to gain the card No.

Note: Up to 20 digits or letters are allowed in the card No.

5. Add face picture.
    1) Tap **Not Added** on the right of the Face Picture item to enter the face picture adding page.
    2) Position the face looking at the device camera.

       Make sure the face picture is in the blue square on this page and wait for the device recognition.

       After adding the face picture completely, the prompt "Saved" will pop up.
    3) Tap **Save** to save the parameters and go back to the Add User page.

       Or wait for 3s and the system will go back to the Add User page automatically.
    4) (Optional) Tap **Try Again** to delete the saved face picture and start adding face picture again.

       Note: For details about the instructions of adding face pictures, see *Appendix A Tips When Collecting/Comparing Face Picture.*

6. Tap √ to save the parameters.

   The added user will display in the user list.

6.5.2 Searching User

Purpose:

When there are too many users in the user list, you can search for the required one via user name or card No.

Steps:

1. On the User Management page, tap **Name** or **Card No.** at the upper right corner of the page to select the search type.

2. Input the user name or card No. for search.
3. Tap 🔍 to start search.

   The result will display in the user list.

6.5.3 Editing User

Purpose:

You can change the added user information by follow the steps below.

Steps:

1. On the User Management page, tap the user that you want to edit to enter the Edit User page.

2. Refer to *6.5.1 Adding User* to edit the user information.
3. Tap **Save** to save the parameters and go back to the User Management page.

6.6 Setting Face Picture Parameters

Purpose:

You can set the face picture's parameters for recognizing the face. The parameters include 1:N matching threshold, 1:1 matching threshold, Min. detection area (width), Min. detection area (height), Min. detection width (close to), margin (left), margin (top), margin (right), margin (bottom), pitch angle, yaw angle, pupillary distance, and score.

Steps:

1. In the backend, tap to enter the Face Picture page.

2. Set the face picture parameters.
   The description of each parameter item is as follows:

Parameter Item	Description
1:N Matching Threshold	Set the face picture matching threshold when authenticating via 1:N matching mode. Default Value: 83
1:1 Matching Threshold	Set the face picture matching threshold when authenticating via 1:1 matching mode. Default Value: 60
Min. Detection Area (Width)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 14
Min. Detection Area (Height)	When the distance between the camera and the user is long, the parameter represents the minimum percentage of the facial height in the total height of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. Other percentages, distances and angles in this table should also meet their conditions. Recommended Value: 12
Min. Detection Width (Close to)	When the distance between the camera and the user is short, the parameter represents the minimum percentage of the facial width in the total width of the recognition area. The actual percentage should be larger than the configured value when face picture authentication. In this condition, the device will not detect other parameters.
Margin (Left)	The distance from the face left side to the left margin in the recognition area. The actual distance should be larger than the configured value

| Parameter Item	Description
	when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Top)	The distance from the face top side to the top margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Right)	The distance from the face right side to the right margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Margin (Bottom)	The distance from the face bottom side to the bottom margin in the recognition area. The actual distance should be larger than the configured value when face picture authentication. Other percentages, distances, and angles should also meet their conditions.
Pitch Angle	The maximum pitch angle when face authentication. By default, the angle is 30°.
Yaw Angle	The maximum yaw angle when face authentication. By default, the angle is 20°.
Pupillary Distance	The minimum resolution between two pupils when face recognition. The actual resolution should be larger than the configured value. By default, the resolution is 40.
Score	Set the face picture's score when recognition. The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is larger than the configured value, face recognition is failed.

3. Tap $\lhd$ to save the settings and leave the page.

6.7 Changing Password

Purpose:

You can change the device password (activation password).

Steps:

1. In the backend, tap [🔑] to enter the Change Password page.

2. Input the old password, new password, and confirm the new password.

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

> ⚠️ **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.*

6.8 Managing Data

Purpose:

You can export added face pictures, and the authentication events and exception data from the system. You can also import the face information in batch to the system.

Steps:

1. Plug an USB flash drive in the device.

2. On the backend page, tap 🗠 to enter the Data Management page.

3. Tap **Face Picture**, **Event**, **Exception Data**, or **Face Picture** to export the face pictures, events, or exception data to the USB flash drive, and import the face picture from the USB flash drive respectively.

   Notes:
   - The name format of the imported face picture: Card No._Name_Department_Employee ID_Gender
   - The imported face picture should contain the user's frontal face with the format of JPEG or JPG. The face picture's resolution should be 640 × 480 or more. The picture size should be between 60 KB and 200 KB. The pupillary distance of the picture should to more than 60p.
   - The importing and exporting file should be Excel file.

6.9 Maintaining System

Purpose:

You can restore to default settings or factory settings. You can also upgrade the system.

6.9.1 Restoring Device Parameters

Purpose:

You can restoring the device parameters to the default or to the factory.

Steps:

1. In the backend page, tap 🔧 to enter the System Maintenance page.

2. Tap **Default Settings** or **Factory Settings**.
   Default Settings: All parameters will be restored to the default except for the device IP address.
   Factory Settings: All parameters will be deleted. Activation is required the next time you start the device.

6.9.2 Upgrading Firmware

Purpose:
If there is new version available or the current firmware version is too low, you can upgrade the device firmware via the USB interface.

Steps:
1. Plug an USB flash drive in the device USB interface.
   Note: Make sure there are upgrading file in the USB flash drive. The upgrading file's name should be digicap.dav

2. In the backend page, tap to enter the System Maintenance page.

3. Tap **Firmware Upgrade**.
   The device will read the upgrading file in the USB flash drive automatically and start upgrading.
   Note: the upgrading file should be in the root directory.

6.10 Viewing System Information
In the backend page, tap and you can view the total capacity and the capacity usage of the face pictures, card, event, and fingerprint.

6.11 Viewing Device Information
In the backend page, tap and you can view the device name, the software version, the firmware version, and the open source code license.

6.12 Authenticating Identity
Purpose:
After setting network, system parameters and adding user, you can go back to the initial page for identity authentication.
The system will authenticate person according to the configured authentication mode.
You can authenticate identity via 1:1 matching or 1:N matching.
Note: Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

1:N Matching: Compare the captured face picture with all face pictures stored in the terminal.

1: 1 Matching: When swiping card or ID card, compare the captured face picture with the information stored in the card (or ID card).

Before you start:
You should configure the terminal authentication mode. For details, see *6.4 System Settings*.

6.12.1 Authenticating via 1:1 Matching

Steps:
1. If the authentication mode is Card + Face Picture, or Auto, swipe card in the card swiping area.
   Note: The card can be normal IC card, encrypted card, or ID card.
   If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.
2. (Optional) If the Blacklist Authentication Mode function is enabled, the device will compare the authentication information with the blacklist.
   If the user is in the blacklist, a prompt of identity exception will pop up on the auxiliary screen and the device will send a blacklist alarm to the control center.
   Notes:
   ● For details about enabling the Blacklist Authentication Mode function, see *6.4 System Settings.*
   ● You can connect an external HDMI screen as an auxiliary screen.
3. If the authentication mode is Card + Face Picture or Auto, position the face looking at the camera to authenticate face.
   If authentication succeeded, the prompt "Authenticated" will pop up.
   Notes:
   ● For better face picture authentication, the user height should between 140 cm and 190 cm and the distance between the user and the device should be between 30 cm and 100 cm.
   ● For detailed information about authenticating face picture, see *Appendix A Tips When Collecting/Comparing Face Picture.*

6.12.2 Authenticating via 1:N Matching

If the authentication mode is Face Picture or Auto, position the face looking at the camera to start face picture authentication.
If authentication completed, a prompt "Authenticated" will pop up.

6.13 Linking Access Control Device

Purpose:
The face recognition terminal can connect to an access control device via RS-232 protocol and transmit authentication information to the access control device at the same time.
The access control device can control the door status according to authentication result and the access control device authentication mode, and transmit the door events to the control client or other systems.
Before you start:
● Make sure the access control device has connected to the face recognition terminal via RS-232 protocol.
● Make sure the face recognition terminal and the access control device are powered on.

Steps:
1. Set the baud rate of the RS-232 protocol in the COM tab.
   Note: The face recognition terminal's baud rate of RS-232 protocol should be the same as the access control device's. For details about setting the baud rate of the RS-232 protocol, see *6.3.2 Setting COM Parameters*.
2. Authenticate via the face recognition terminal.
   The face recognition terminal will send the authentication result and the card No. to the access control device. The access control device will control the door status according to the result. And it will also send the related events to the client or other systems.
   Note: For details about access control device's authentication mode, see the user manual of the related access control device.

# Appendix ATips When Collecting/Comparing Face Picture

A.1 Expression

● Keep your expression naturally when collecting or comparing face pictures, just like the expression in the picture below.
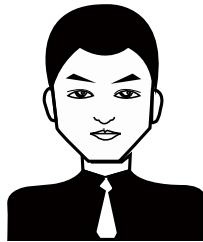
● Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
● Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.
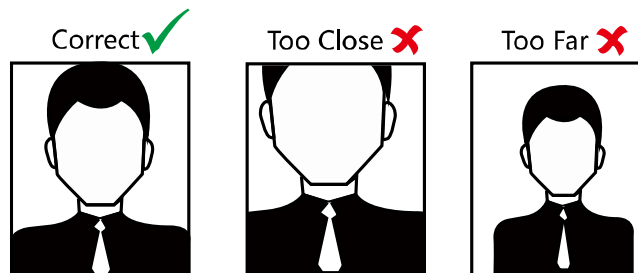
A.2 Posture

In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.
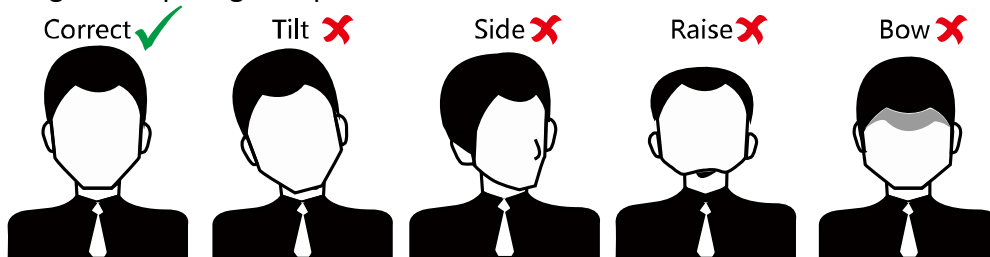
A.3 Size

Make sure your face is in the middle of the collecting window.

010100001080905

See Far, Go Further

UD11040B-B