use-IP

HIKVISION

DS-K1T673 Series
Face Recognition Terminal

Quick Start Guide

UD24653B-K

Quick Guide

1 Installation
1.1 Open the box.
1.2 Check the environment.
1.3 Install the device.

2 Wiring
2.1 Power supply wiring.
2.2 Door lock wiring.
2.3 Door contact wiring.
2.4 Exit button wiring.
2.5 Wiegand wiring.
2.6 RS-485 wiring.
2.7 Alarm in/out wiring.

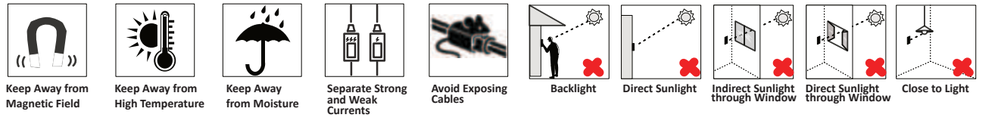
3 Activation
Activate the device.

4 Other Operations
4.1 Quick operation settings.
4.2 Authentication settings.

1 Installation

Install with Mounting Plate

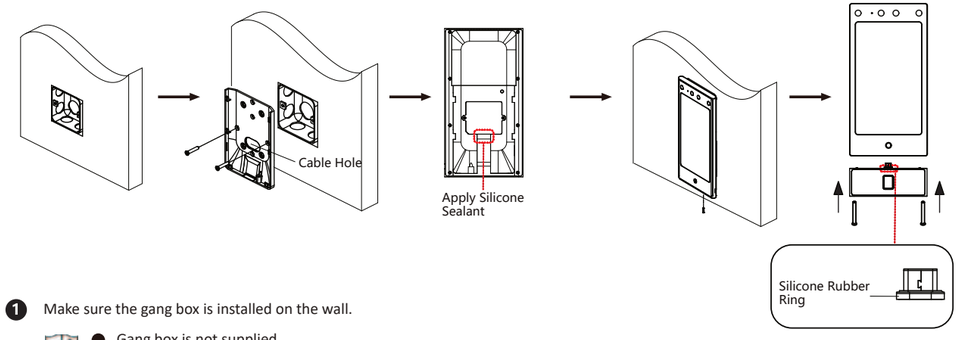
Installation Environment



- Avoid backlight, direct sunlight, and indirect sunlight.
- For Better recognition, there should be light source in or near the installation environment.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

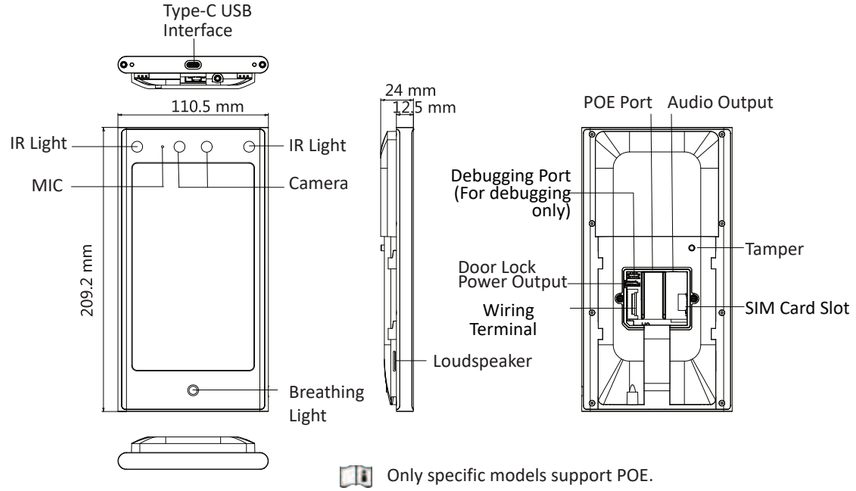
Cable Requirements

Cable Size	18 AWG	15 AWG	12 AWG
Power Supply	12 V Switched-mode	12 V Switched-mode	12 V Switched-mode
Distance Between Power Supply and Device	≤ 20 m	≤ 30 m	≤ 40 m



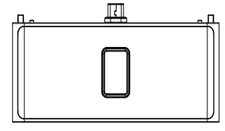
1. Make sure the gang box is installed on the wall.
   - Gang box is not supplied.
   - The height of the Gang box can refer to the wall switch standard, and it is about 1.4 m above the ground.
2. Secure the mounting plate on the gang box with two supplied screws (SC-KM3X8-H2-SUS).
3. Route the cable through the cable hole, wire the cables and insert the cables in the gang box.
   Apply silicone sealant among the cable wiring area to keep the raindrop from entering.
4. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-KM3X8-H2-SUS).
5. (Optional) According to actual needs, you can connect other modules to the USB interface, and secure them with 2 M3 screws.
   When inserting an peripheral module, ensure that the silicone rubber ring is intact to prevent rain and other input.

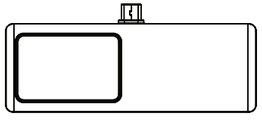
Interfaces and Dimension

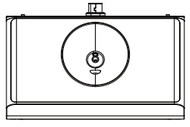


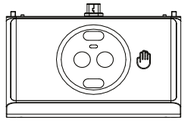
Only specific models support POE.

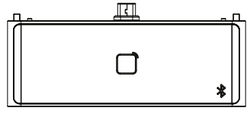
Peripheral Module


Fingerprint + Bluetooth + QR Code Module


Wireless Module (433/868 Mhz)


Alcohol Detection Module

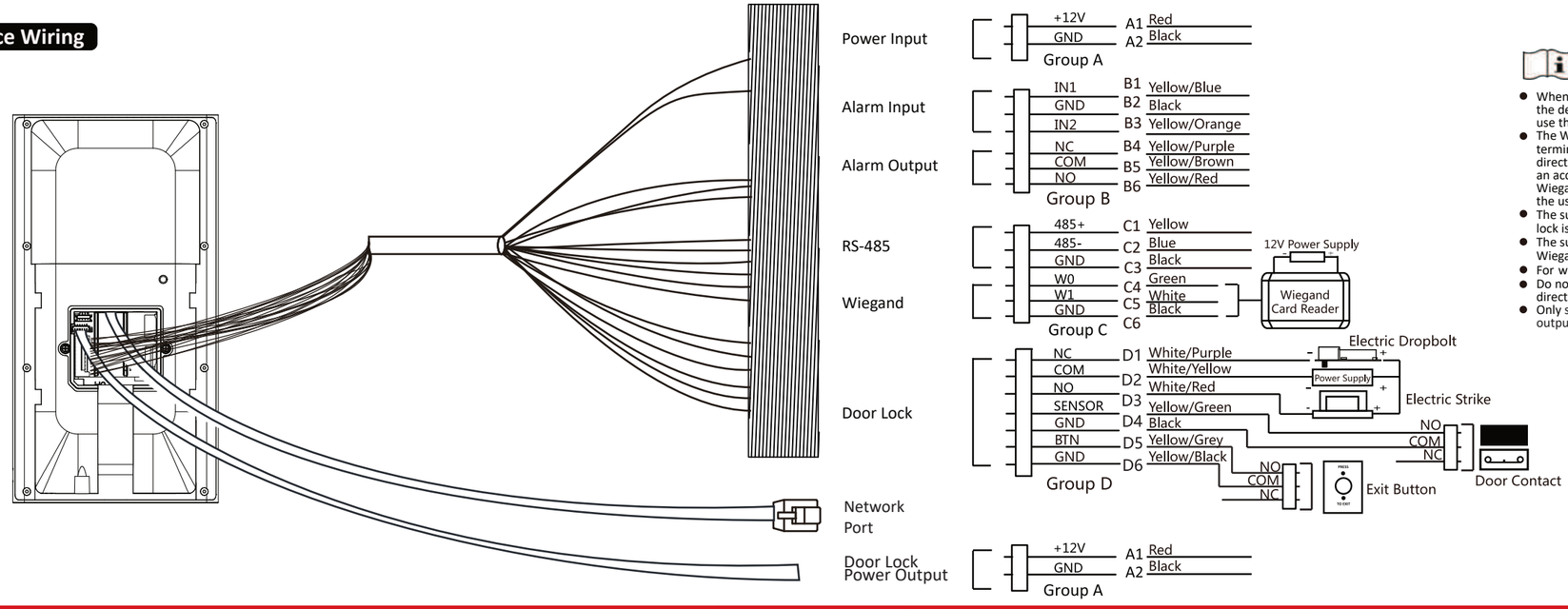

Palm Print and Palm Vein Module


Dual-frequency Card Module (13.56 Mhz and 125 Khz)

- If the audio plug diameter is greater than 8 mm, an external adapter is required.
- The figures are for reference only.
- The device supports multiple modules, which can be accessed according to actual needs.
- Peripheral modules need to be purchased by yourself.
- Avoid frequent insertion and removal of the blow pistol of alcohol detection module . Replace it immediately if it becomes loose or falls off.

2 Wiring

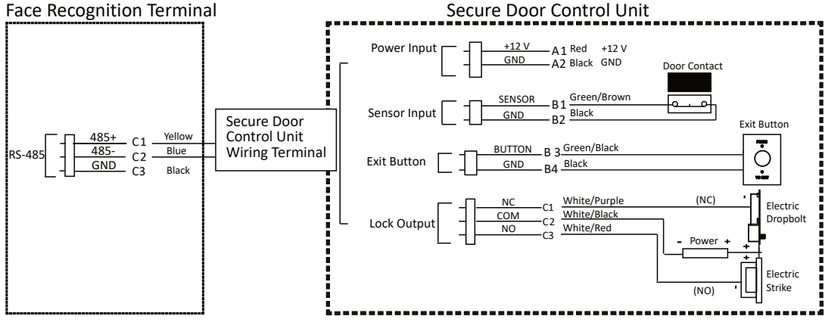
Device Wiring



- When connecting door contact and exit button, the device and the RS-485 card reader should use the same common ground connection.
- The Wiegand terminal here is a Wiegand input terminal. You should set the device's Wiegand direction to "input". If you should connect to an access controller, you should set the Wiegand direction to "Output". For details, see the user manual.
- The suggested external power supply for door lock is 12 V, 1 A.
- The suggested external power supply for Wiegand card reader is 12 V, 1 A.
- For wiring the fire system, see the user manual.
- Do not wire the device to the electric supply directly.
- Only specific models support door lock power output.

2 Wiring

Secure Door Control Unit Wiring



- The secure door control unit should connect to an external power supply separately.
- The suggested external power supply is 12 V, 0.5 A.
- For scenarios with high safety requirement, use the secure door control unit wiring first. You can ask the technical support to purchase for the secure door control unit separately.
- The picture here are parts of the wiring. For details, see the secure door control unit's user manual.

3 Activation

● Activation via Device

After powering on, you will enter the activation page.

Steps:

1. Create a password and confirm the password.
2. Tap **Activate** to activate the device.

Characters containing admin and nimda are not supported to be set as activation 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 Other Operations

● Steps Afterwards

After activating, you can select language, set password change type, set network parameters, access to Hik-Connect, set privacy, and set administrator.

● Log in Home Page

Authenticate face, card, fingerprint, keyfob, palm print or password, and log in the device to enter the home page.

● Restore to Factory

Tap "System Maintenance"-"Restore to Factory". All parameters will be restored to the factory settings. The system will reboot to take effect.

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

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

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- ***HIKVISION*** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

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

Data Protection

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

- If the Type C power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.

Scan the QR code to get the user manual for detailed information.