DS-K1T805 Series
Access Control Terminal

Quick Start Guide

UD32453B

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Quick Guide

1 Installation
1.1 Check the environment.
1.3 Install the device.

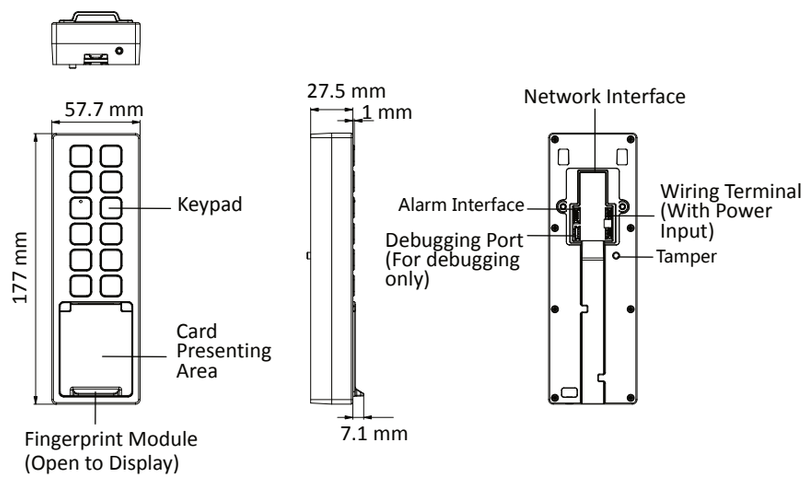
2 Wiring
2.1 Normal device wiring.
2.2 Wiring with secure door control unit.

3 Quick Operation
3.2 Activate the device.
3.3 Log in.

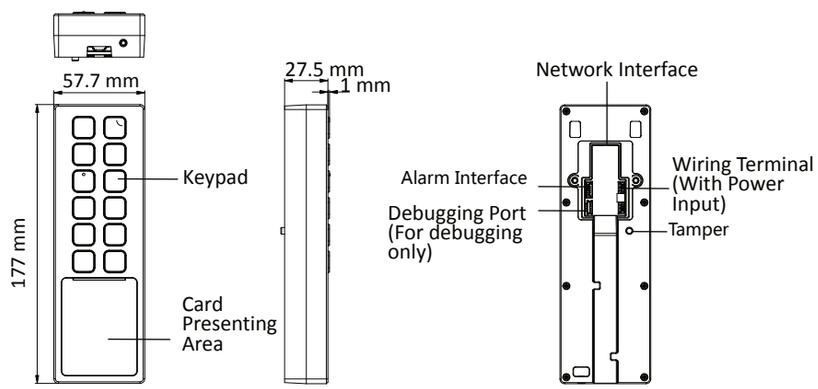
Appearance

The pictures here are for reference only.

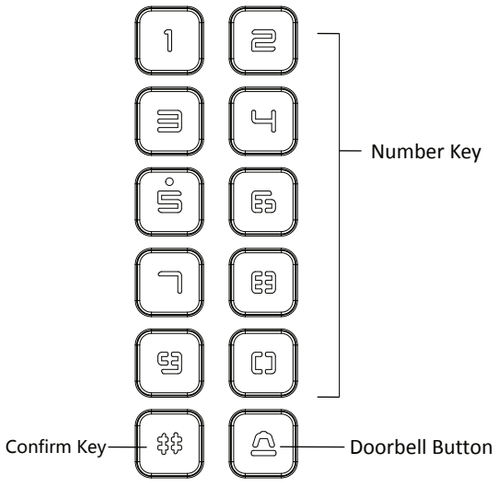
Fingerprint + Card Series



Card Series



Keypad

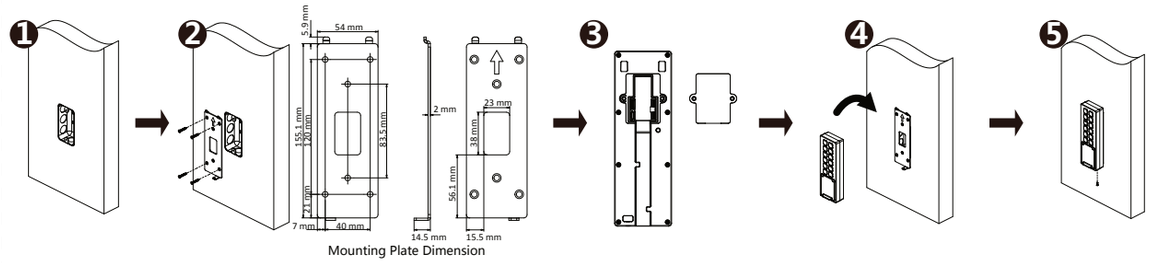


Key 5: Hold to enable AP mode
#: Press # to confirm PIN entering.

1 Installation

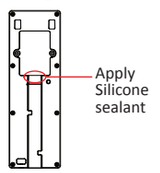
Before Installation:

- Supports indoor and outdoor use.
- The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

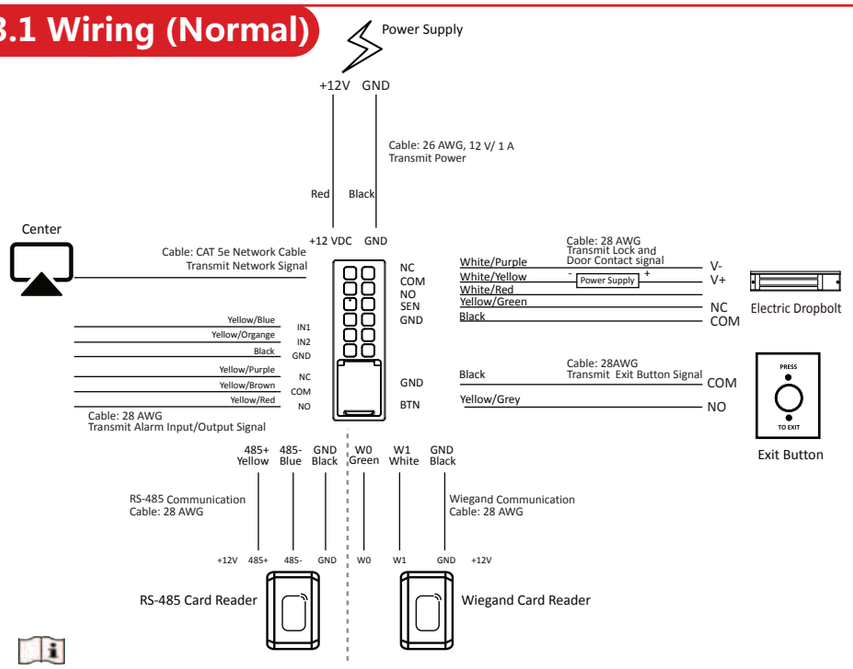


Mounting Plate Dimension

1. Make sure the gang box is installed on the wall. Gang box is not supplied.
2. Secure the mounting plate on the wall with 4 supplied screws (SC-KA4X22). Make sure the cables are through the cable hole.
3. Remove the back panel to display the wiring area. Wire the cables and install the back panel back.
   Apply Silicone sealant among the cable wiring area to keep the raindrop from entering.
4. Align and hang the device with the mounting plate.
5. Secure the device on the mounting plate with 1 supplied screw (SC-KM3X8-T10-SUS-NL).
   For more installation methods, see the user manual.

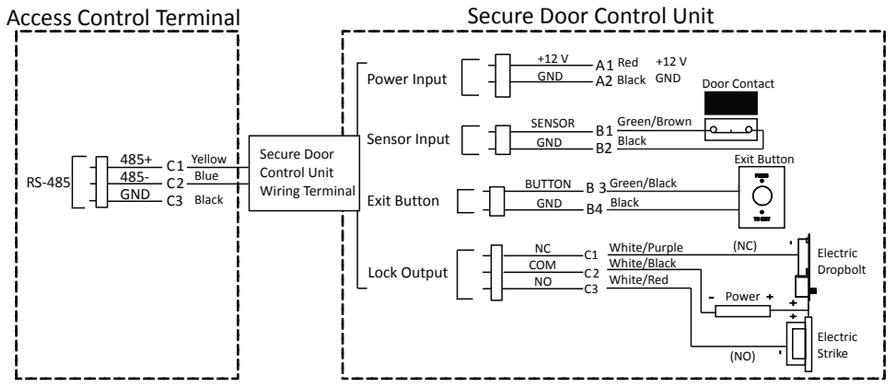


3.1 Wiring (Normal)



- When connecting door contact and exit button, the device and the RS-485 card reader should use the same common ground connection.
- You should set the device's Wiegand direction as **Input** to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction as **Output** to transmit authentication information to the access controller. For details about Wiegand direction settings, see *Set Wiegand Parameters* in web configuration.
- The device and the door lock should use separate power supply.
- 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.
- Do not wire the device to the electric supply directly.

3.2 Device Wiring (With Secure Door Control



- 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.

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.

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.

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.

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

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

Warning
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- CAUTION: To reduce the risk of fire, replace only with the same type and rating of fuse.
- CAUTION: This equipment is for use only with Hikvision's bracket. Use with other (carts, stands, or carriers) may result in instability causing injury. To prevent possible hearing damage, do not listen at high volume levels for long periods.
- 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.)

Caution
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The USB port of the equipment is used for connecting to a USB flash drive only. The serial port of the equipment is used for debugging only.
- Burned fingers when handling the fingerprint sensor metal. Wait one-half hour atier switching off before handling the parts.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instruations.
- 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 soti and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers atier 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.
- Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Please make sure that the biometric recognition accuracy will be affected by the collected pictures' quality and the light in the environment, which cannot be 100% correct.

4 Quick Operation

Activate Device

Select one of the following methods to activate the device.
--Activate via Mobile Web (With Wi-Fi Function Device Supported)
1. Connect to the device hotspot with your mobile phone by entering the hotspot password. The activation page will pop up.
   - If automatic pop-up failed. Enter the device default IP or enter www.acsvis.com in the browser to enter the activation page.
   - For inactive devices, device hotspot is enabled by default. The device hotspot name is *AP_Serial Number*, and the hotspot password is the device serial number.
   - The device is in the AP mode by default. The AP mode will be disabled after 30 min. Hold key 5 for 10 s to enter the AP mode again.
2. Create a new password (admin password) and confirm the password.
3. Click **Activate**.
4. Enter **Configuration** -> **Communication Settings** -> **Wi-Fi**. And connect to a Wi-Fi. Or edit the IP address via the mobile web, PC web browser and the client software.
   - The device hotspot is enabled and is in the AP mode by default and it will be disabled after 30 min.
   - If the AP mode is disabled, hold keypad number 5 for 10 s to enable the AP mode again.

--Activate via PC Web
1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.
   Make sure the device IP address and the computer's should be in the same IP segment.
2. Create a new password (admin password) and confirm the password.
3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool or the client software.

--Activate via HikCentral Access Control (HCAC) Web Client
1. Login the HCAC and activate license.
2. Select **Device** -> **Device and Server**.
3. In the Online Device area, view the device status and select inactive devices.
4. Click **Activate** to open the device activation window.
5. Create a password in the password field, and confirm the password.
6. Click **Save** to activate the device.
   If you have not set security questions, the window of setting security questions will pop up, and you should select the method of resetting password and set the security questions as needed.
7. Click the edit icon in the Operation column to change the device's IP address, subnet mask, gateway, and so on if needed.

Characters containing admin and nimda are not supported to be set as activation password. For details, please refer to the user

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.

Login

--Login Mobile Web
1. Connect the mobile phone to the Wi-Fi the same as the device's.
   Make sure the device and the PC are in the same IP segment.
2. Open the browser on the mobile phone and enter the device IP address in the address bar and press **Enter** to enter the login page.
3. Enter the device user name and the password.
4. Tap **Login**.
Or hold key 5 for 10 s to enter the AP mode. Enter the mobile phone's Wi-Fi page. Select the device hotspot and enter the hotspot's password (the activation password). The mobile phone will pop up the login page automatically.

--Login PC Web
1. Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
   Make sure the device and the PC are in the same IP segment.
2. Enter the device user name and the password.
3. Click **Login**.

For more configuration and operation of HCAC, scan the QR code.

Authentication via Single Credential

1. Set the user authentication type before authentication in via Web.
2. Authenticate fingerprint or card.
Fingerprint: Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.
Authentication via fingerprint should be supported by the device.
Card: Present the card on the card presenting area and start authentication via card.

Scan the QR code to get the user manual for more configuration and operation details.