



DS-K1A340 Series Face Recognition Terminal

Quick Start Guide

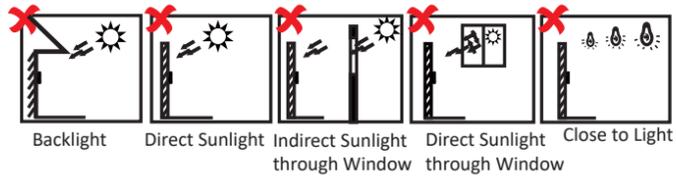
UD24079B-D

1 Installation

Installation Environment:

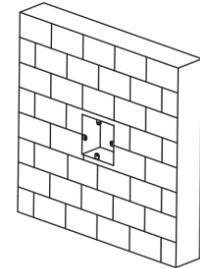
Indoor use only.
Avoid backlight, direct sunlight, and indirect sunlight.

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.



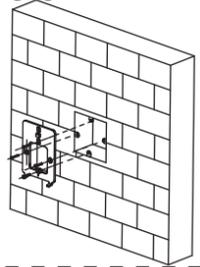
Wall Mounting

1 Make sure the gang box is installed on the wall.

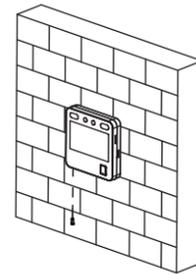


Gang box is not supplied.

2 Secure the mounting plate on the gang box with the supplied screws (M4).
Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

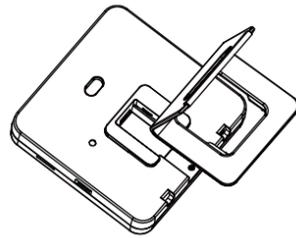


3 Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (M3).

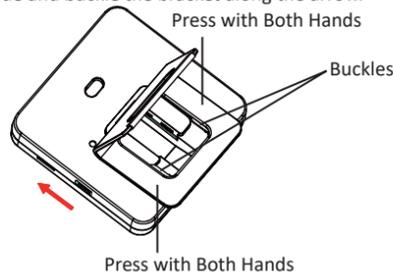


Base Mounting

1 Route the cable through the cable hole of the bracket.
Align the bracket with the device rear panel.



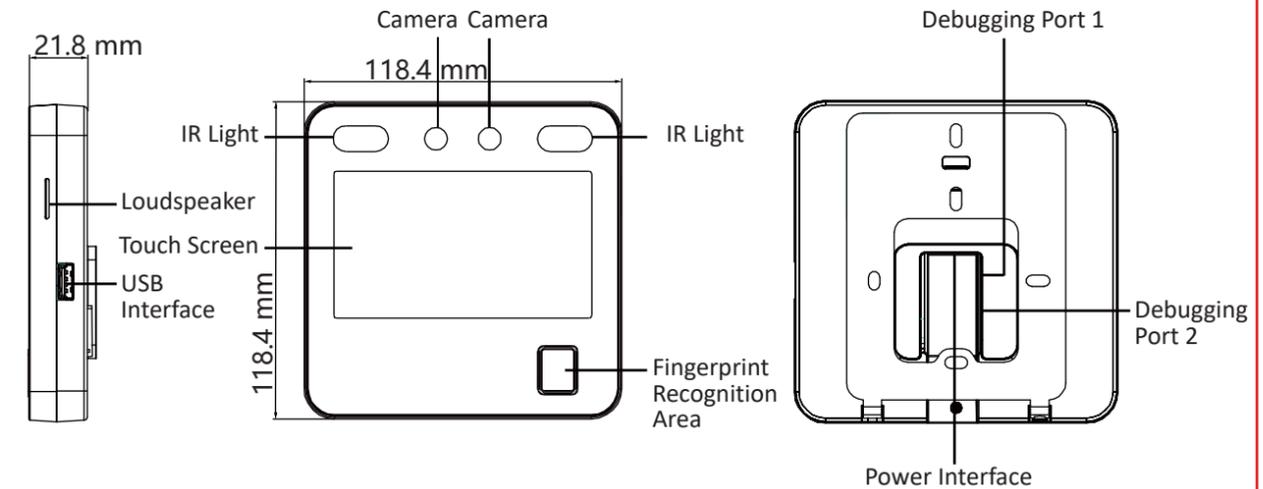
2 Press the bracket with both hands. Make sure the rear panel of the device and the buckles of the bracket are aligned with each other. Slide and buckle the bracket along the arrow.



3 Slide to the end to complete the installation.

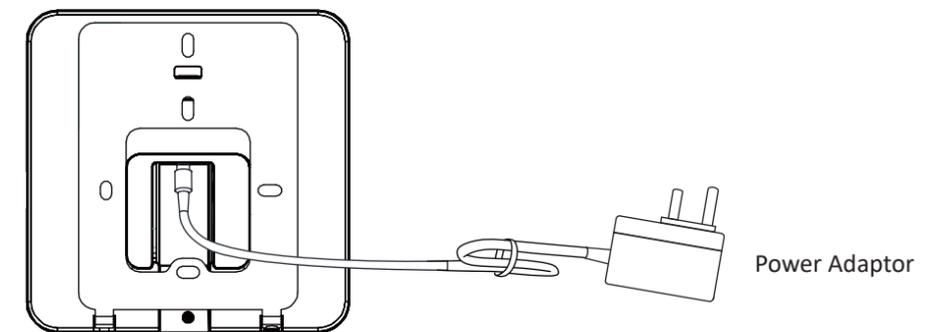


2 Appearance



The figures are for reference only.

3 Wiring (Normal)



Power on the device to operate.

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.
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 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.

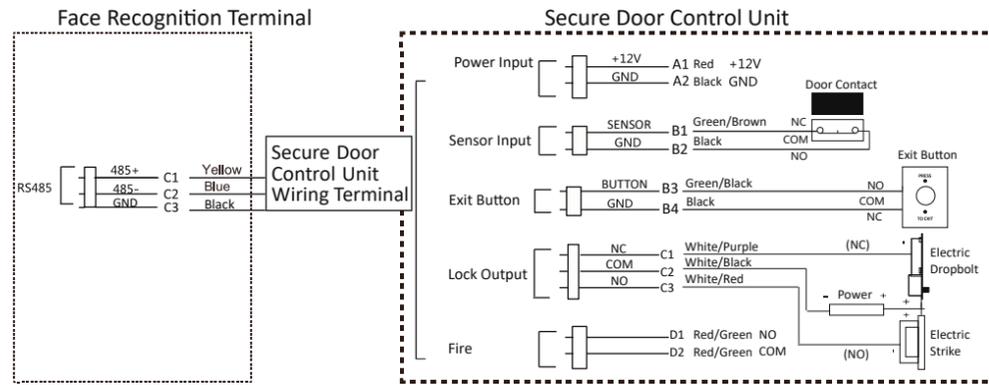
Data Protection
During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption 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.

Scan the QR code to get the user manual for detailed information. Use only power supplies listed in the user instructions:



Model	Manufacturer	Standard
ADS-26FSG-12 12024EPG	Shenzhen Honor Electronic Co.,Ltd	PG
MSA-C2000IC12.0-24P-DE	MOSO Technology Co.,Ltd	PDE
ADS-245-12 1224GPG	Shenzhen Honor Electronic Co., Ltd.	PB

3.2 Device Wiring (With Secure Door Control Unit)



- 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 pictures here are parts of the wiring. For details, see the secure door control unit's user manual.

4 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—

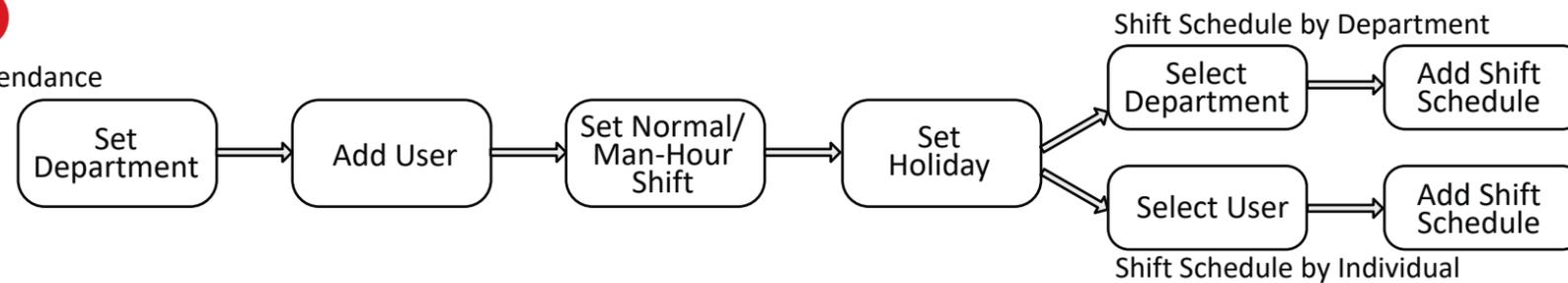
We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially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

● Device Quick Operation

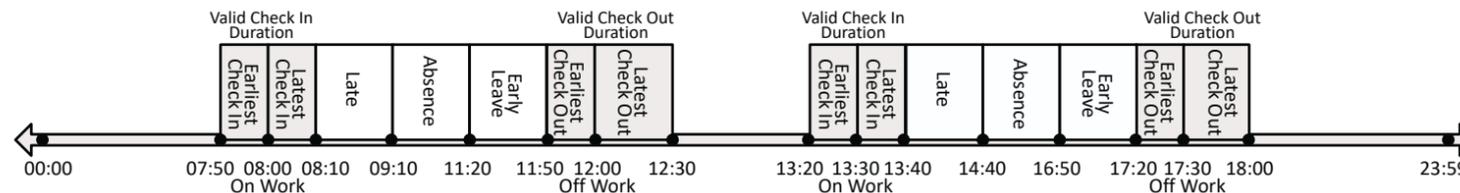
After activating, you can select language, set password change type, set reserved questions, set application mode, set network parameters, access to Hik-connect, set privacy, link to app, and set administrator.

5 Basic Operation

● Local Time and Attendance



- ▶ **Set Department:** After logging in the device, tap **Department Management** and you can see the default department. Tap + to create a department. Select a department, and you can edit or delete it.
- ▶ **Add User:** After logging in the device, tap **User** -> +. Enter the user name, select a department, add face and fingerprint information, etc.
- ▶ **Set Normal Shift:** It is applicable to the normal attendance situation. You can set the attendance rule and the attendance checking times. After logging in the device, tap **Local T&A** -> **Shift Management** -> **Normal Shift Management**. Attendance Rule: Tap **Attendance Rule** to enter the page. Take the following picture as an example to describe the rules.



Advanced Check In Time: Set the earliest check in time. For example, if set the on work time as 8:00, and set the parameter as 10 min, the earliest check in time will be 7:50. Checking in at and earlier than 7:49 will be marked as invalid.

By default, if set as 0 min, the valid check in time starts from 00:00.

Latest Check In Time: Set the latest check in time. For example, if set the on work time as 8:00, and set the parameter as 10 min, the latest check in time will be 8:10. Checking in at and later than 8:11 will be marked as late or absence.

Late Time: The late time is N min after the latest check in time. For example, if set the latest check in time as 8:10, and set the parameter as 60 min, checking in at and later than 9:11 will be marked as absence. 8:10 to 9:10 will be marked as late.

Earliest Check Out Time: Set the earliest check out time. For example, set the off work time as 17:30 and set the parameter as 10 min, the earliest check out time will be 17:20. Checking out at or earlier than 17:19 will be marked as invalid.

Latest Check Out Time: Set the latest check out time. For example, set the off work time as 17:30 and set the parameter as 30 min, the latest check out time will be 18:00. Checking out at or later than 18:01 will be marked as invalid.

By default, if set as 0 min, the valid check out time ends at 23:59:59.

Absence Time (Early Leave): The early leave time is N min earlier than the check out time. For example, if set the earliest check out time as 17:20, and set the parameter as 30 min, checking out between 16:50 and 17:20 will be marked as early leave.

- ▶ **Set Man-Hour Shift:** It is applicable to the situation with flexible working hours. After logging in the device, Tap **Local T&A** -> **Shift Management** -> **Man-Hour Shift Management** -> +. Edit the shift name, work duration, latest on-work time, and break time.
- ▶ **Set Holiday:** After logging in the device, tap **Local T&A** -> **Holiday Management** -> +. Create a holiday name and set a holiday duration. Select a holiday and you can edit or delete it.
- ▶ **Shift Schedule by department:** All persons in the department use the same shift schedule to take attendance. After logging in the device, Tap **Local T&A** -> **Shift Schedule by Department**. Select a department, add shift schedule, and select holiday. Shift Schedule by individual: Take attendance according to individual's conditions. Tap **Local T&A** -> **Shift Schedule by Individual**. Tap + to add shift schedule and select holiday.

● Other Settings

- ▶ **Restore to Default:** All parameters, except for the communication settings, remotely imported user information, will be restored to the default settings. The system will reboot to take effect.
- ▶ **Restore to Factory:** All parameters will be restored to the factory settings. The system will reboot to take effect.
- ▶ **Forgot Password (Via Device):** Long tap on the initial page for 3 s and slide to the left/right by following the gesture and log in the page. Tap in the pop-up admin authentication page. Tap **Forgot Password** in the upper right corner of the page. Plug USB flash drive into the USB interface. Tap **Export File**, and contact the technician to get the key, and enter the key in the export file. Tap **Import File** to import the file with the key to the device. Follow the prompts to reset the password.
- ▶ **Forgot Password (Via iVMS-4200 Client Software):** Make sure the device IP address and the PC's are in the same IP segment. Enter **Maintenance and Management** and click **Online Device**. Find the device and click . Click **Generate** and click **Download** to send the QR code to technical support. Receive a new code and import it to the client software. Create a new password and confirm it. Click **Save**.

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 equipment 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 EMC Directive 2014/30/EU, RE Directive 2014/53/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

Safety Instruction



Warning

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- 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.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Do not ingest battery. Chemical burn hazard!
- 1. This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- 2. This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- 3. Keep new and used batteries away from children.
- 4. If the battery compartment does not close securely, stop using the product and keep it away from children.
- 5. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- 6. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- 7. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- 8. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- 9. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- 10. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- 11. Dispose of used batteries according to the instructions



Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetic 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.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger). 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). Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- The serial port of the equipment is used for debugging only.
- Wall Mounting: 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 instructions.
- 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.
- This bracket is intended for use only with equipped devices. Use with other equipment may result in instability causing injury.
- This equipment is for use only with equipped bracket. Use with other (carts, stands, or carriers) may result in instability causing injury.