

Face Recognition Terminal

Quick Start Guide
UD37555B

Quick Guide

This guide introduces the wiring, installation, usage scenarios and device configuration. You can open the door by following the guide.

1 Installation And Wiring

View typical application, installation environment, installation and wiring, securing door control unit wiring.

2 Quick Configuration

Select screen direction, activate via device, quick operation settings, authentication settings and open door.

3 Appearance and Interface

View the appearance and interface of the device.

4 FAQ

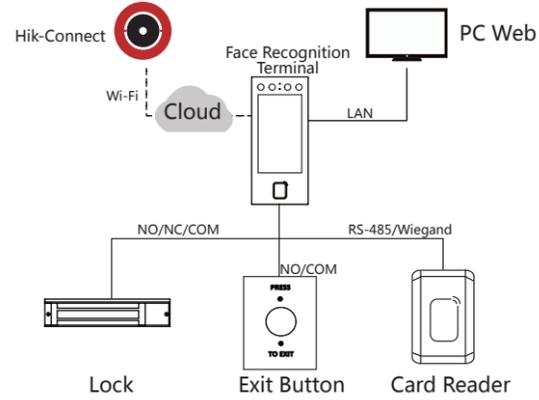
View the FAQ of the device.

Scan the QR code to get the user manual.



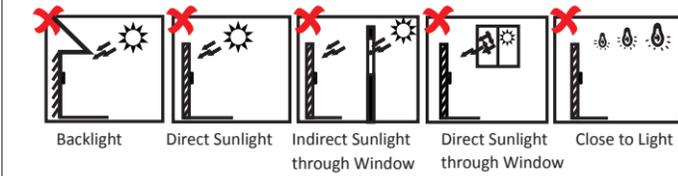
1 Installation and wiring

1.1 Typical Application

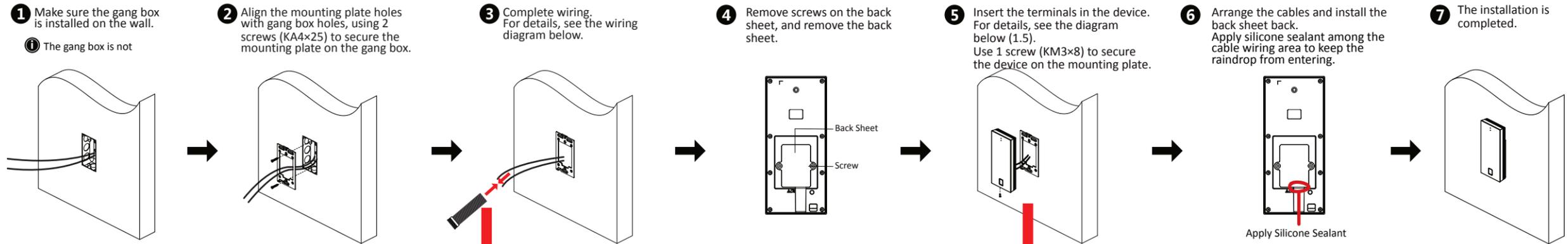


1.2 Installation Environment

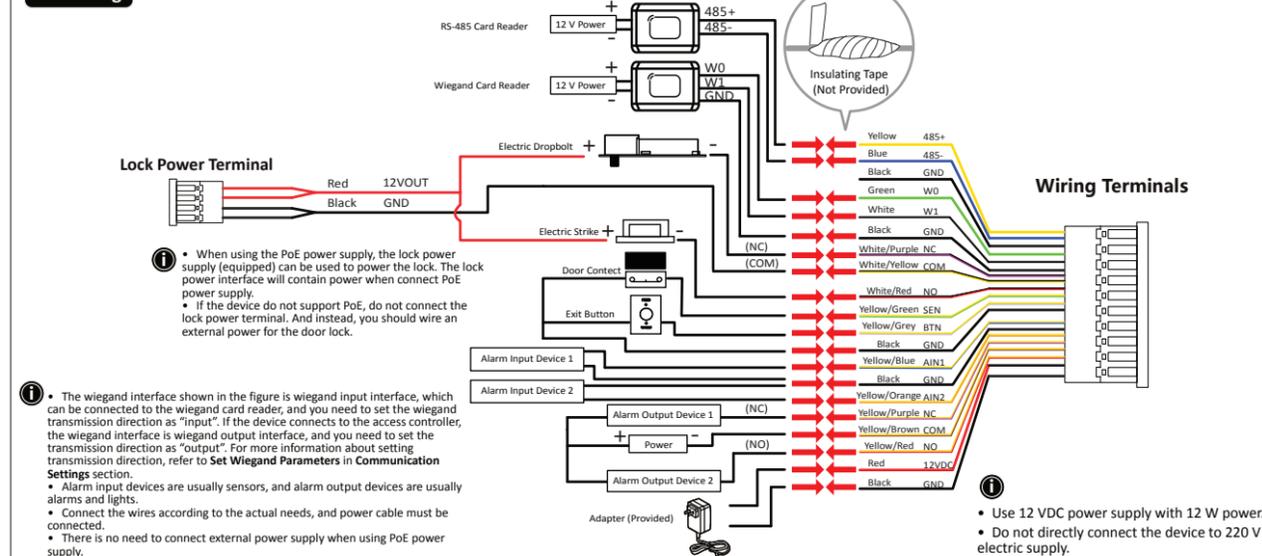
- The installation wall should bear a force that exerts 3 times the weight of the device along the center of gravity of the equipment. The installation device is not damaged and the device does not fall off.
- Prepare for the following tools and accessories: screwdriver (not provided), screws, strands, network cable (not provided), adapter (not provided for non PoE), glass glue and glue gun(not provided).
- Avoid installation environment shown in the figures below.



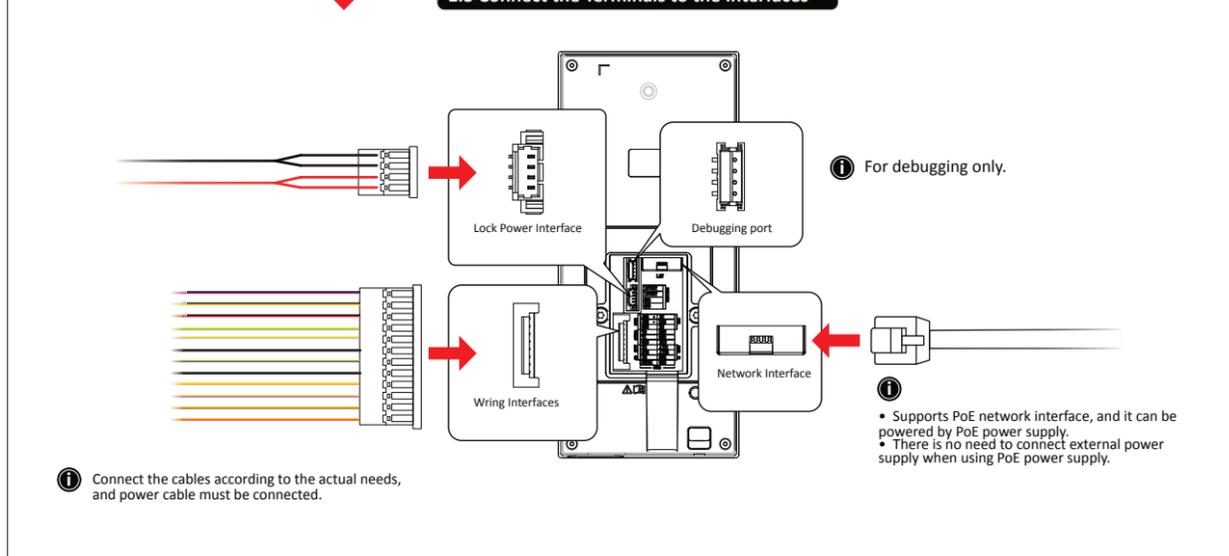
1.3 Installation



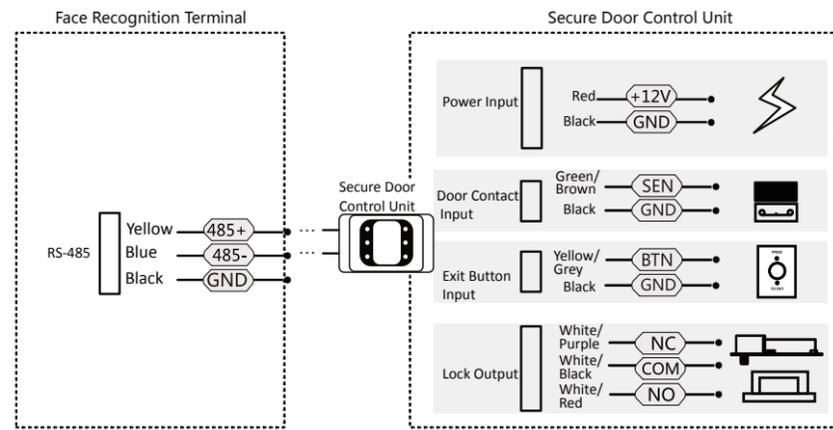
1.4 Wiring



1.5 Connect the Terminals to the Interfaces



1.6 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.



Face recognition terminal supports multi-function wiring: it also supports fire wiring, except basic harness wiring and securing module wiring. Scan the QR code to view other wiring methods and instructions.



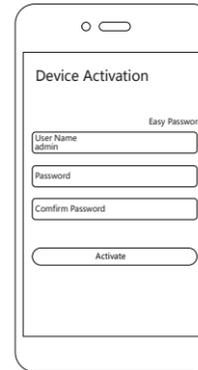
2 Quick Configuration

● Activate Device

—Remote Activation

- If the device is not activated, after powering on, you will enter the activation page.
1. Turn on the Wi-Fi, find the device name and enter the hotspot's password.
 2. It automatically goes to the activation page, tap the edit box to create password.
 3. Tap the confirm password to enter the password again.

- ① Hotspot's password will automatically become the activation password after activation.



—Local Activation

- You can also activate the device by creating local password on the device.
1. Tap local settings to go to the activation page.
 2. Create the password in the edit box.
 3. Tap the confirm password to enter the password again. Other activation methods refer to User Manual.

- Do not contain following characters in the password: the user name, 123, admin (case insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- Password cannot contain words such as hik, hkws, and hikvision (case insensitive).



The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

● Quick Operation Settings

After activating, you can set password change type, set network parameters, enable Cloud service, set privacy, and add administrator.

● Authentication Type Settings

1. Log in to enter the settings page, tap **Personnel Management** →+ to add personnel.
2. Set the authentication type as device mode on **Authentication Settings Page**.
3. Return to the menu, and enter **Access Control Settings** → **Access Controller Authentication Settings** to set the authentication type as **Single Authentication** or **Combined Authentication**, and set the authentication method.

● Open Door

Based on the set authentication method, accordingly you can pass the authentication by face, fingerprint, card password, QR code to open the door.

- ① Different models supports different functions, refers to actual product.



Scan the QR code to view more function settings.



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

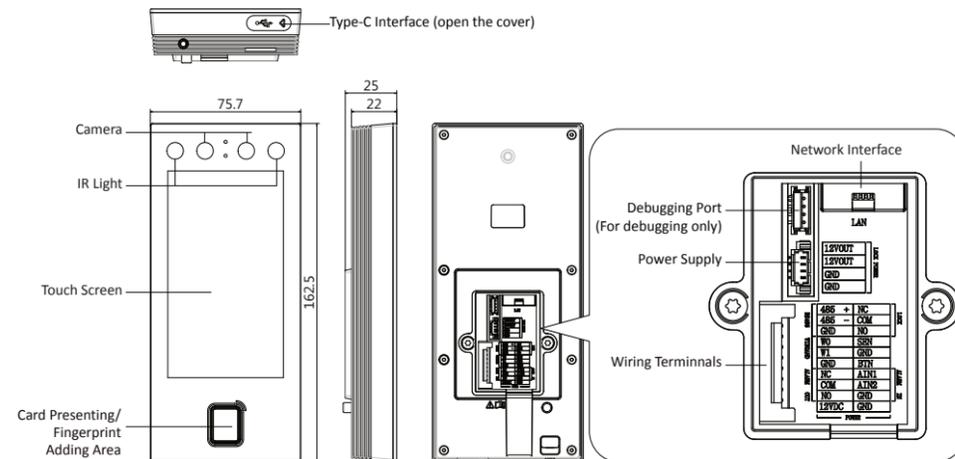
- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may 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

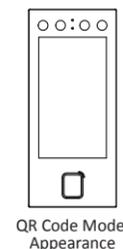
- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY 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.

3 Interfaces and Dimension

Unit : mm



- ① Parts of models support fingerprint function, refers to the actual product.



- ① For different device models, the device will support fingerprint, QR code, and keypad. Refers to actual products for details.

4 FAQ

Question 1: How to change password.

Answer 1:

Make sure that password change type is set after activation.

Step 1: Enter the password login page.

—Administrator added: hold the authentication page and swipe to left or right to go to the administrator authentication page, tap to enter the password page.

—Administrator not added: hold the authentication page and swipe to left or right to go to the administrator password page.

Step 2: Tap **Forget Password** to reset password by answering questions you have set or reserved phone number.

Question 2: How to enter **Settings Page** after activation.

Answer 2: Hold the authentication page and swipe to left or right to go to the administrator authentication page. Log in the device to enter the Settings Page.

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.

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

Symbol Conventions

Symbol	Description
	Note Provides additional information to emphasize or supplement important points of the main text.
	Caution Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
	Danger Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.