DS-K1T807 Series Access Control Terminal

User Manual

Legal Information

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.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

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.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

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

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 Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- 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.
- 1. Do not ingest battery. Chemical burn hazard!
  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.

⚠ Cautions:

- At the time of final installation, the user needs to be informed in an obvious position that the device has a face collection function.
- 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.
- 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.
- 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.

Available Models

Product Name	Model
Access Control Terminal	DS-K1T807MX-E1, DS-K1T807MBFWX-E1, DS-K1T807MBWX-QRE1, DS-K1T807MBFWX-QRE1, DS-K1T807EX-E1, DS-K1T807EBFWX-E1, DS-K1T807EBWX-QRE1, DS-K1T807EBFWX-QRE1

Contents

Chapter 1 Appearance

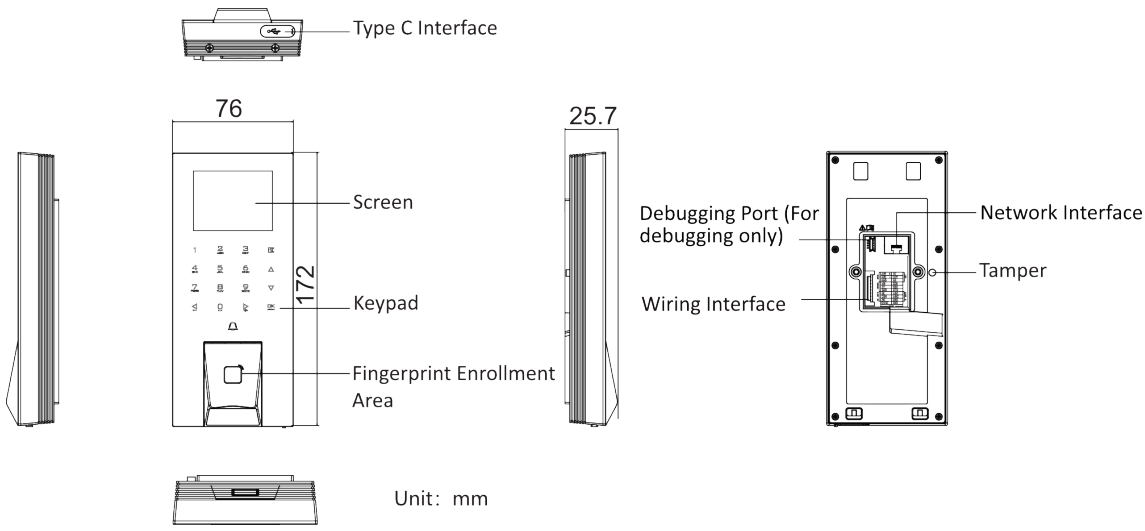


Figure 1-1 Optical Fingerprint Series

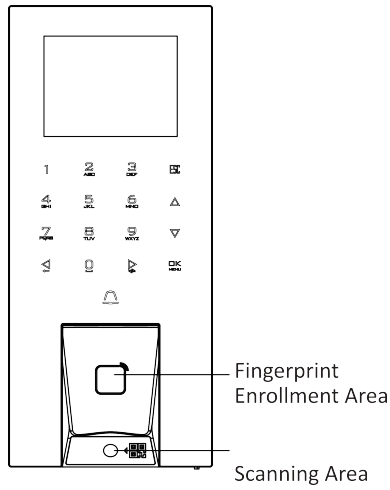


Figure 1-2 Optical Fingerprint+ QR Code Series

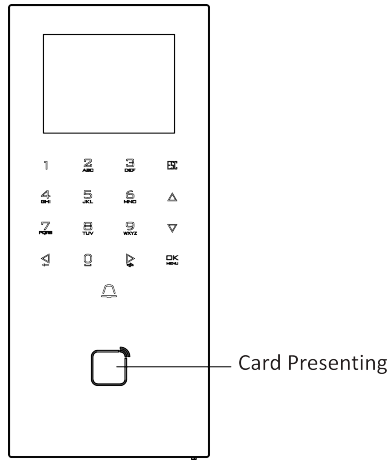


Figure 1-3 Card Series

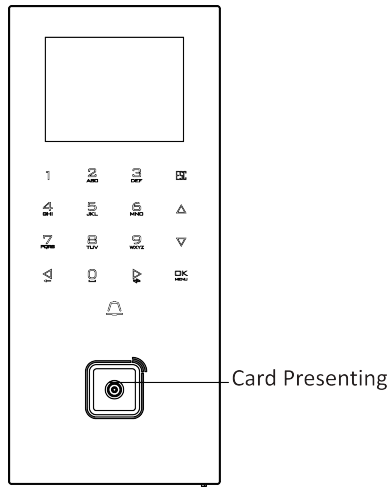


Figure 1-4 Card+QR Code Series

Chapter 2 Installation

2.1 Installation Environment

The minimum bearing weight of the wall or other places should be 3 times heavier than the device weight.

2.2 Install without Gangbox

Steps

1. Make sure the cables are threaded through the hole.

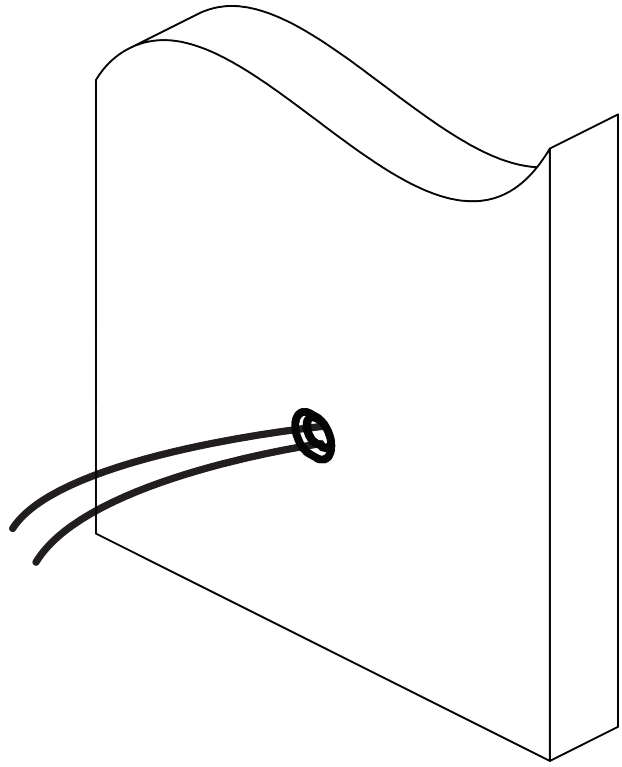


Figure 2-1 Thread Cable

2. Secure the mounting plate on the gang box with two supplied screws (SC-KA4×25).

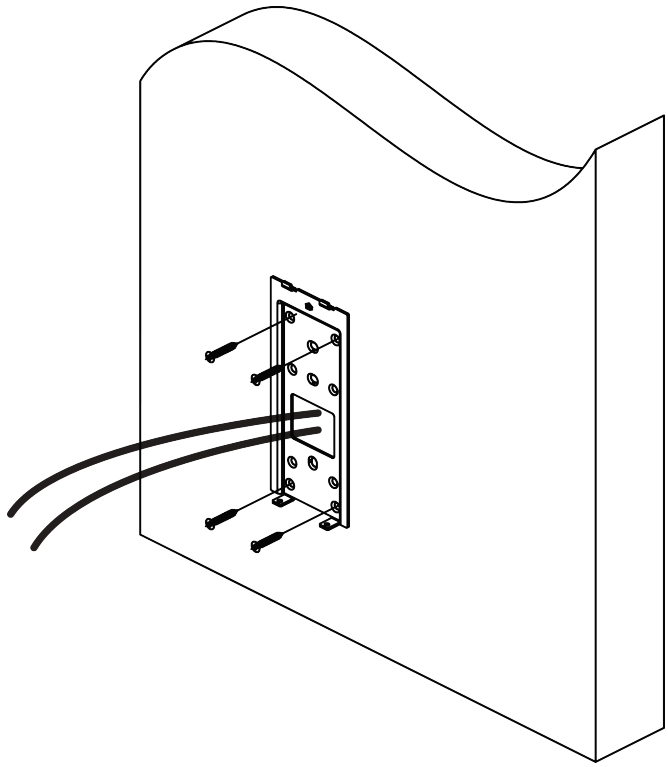


Figure 2-2 Secure Mounting Plate

3. Use a screwdriver to loosen the screws on the back cover of the device and remove the back cover.

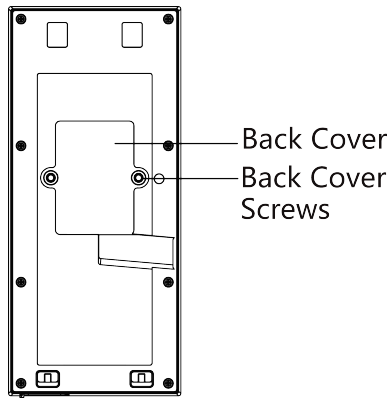


Figure 2-3 Remove Back Cover

4. Complete the wiring. And Fix the back cover.

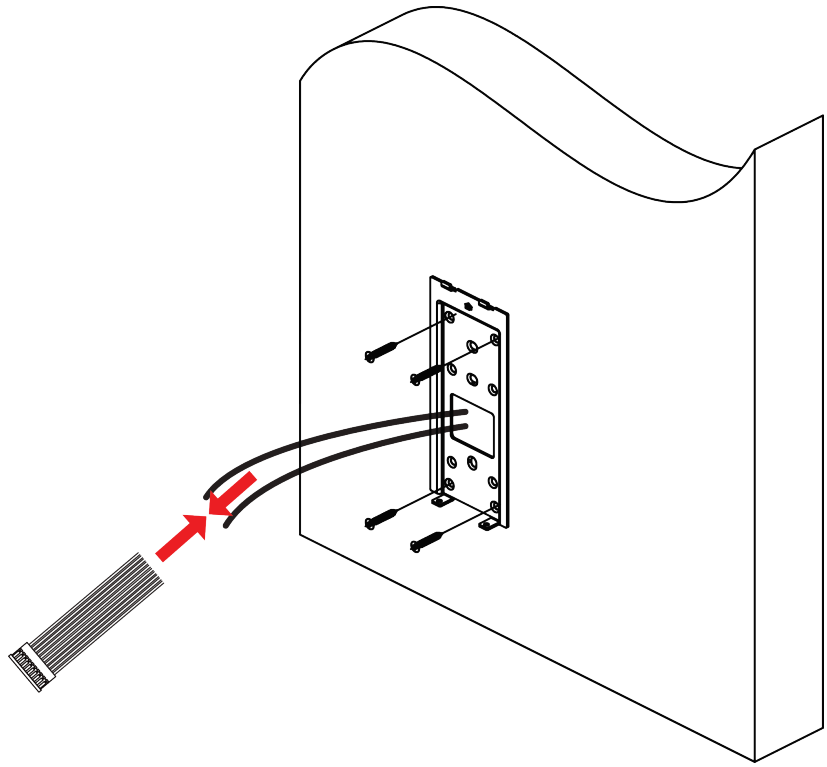


Figure 2-4 Complete Wiring

5. Apply silicone sealant among the cable wiring area to keep the raindrop from entering.

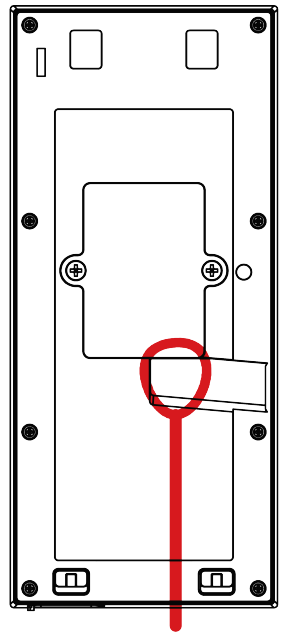


Figure 2-5 Apply Silicone Sealant

6. Hang the device into the plate from top to bottom. Secure the device on the mounting plate with 2 supplied screw (SC-KM3X8-T10-SUS-NL).

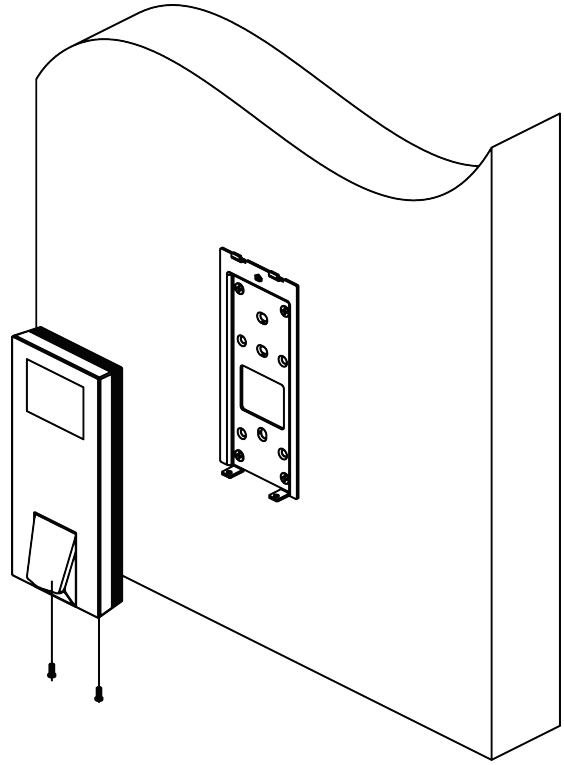


Figure 2-6 Secure Device

7. Complete the installation.

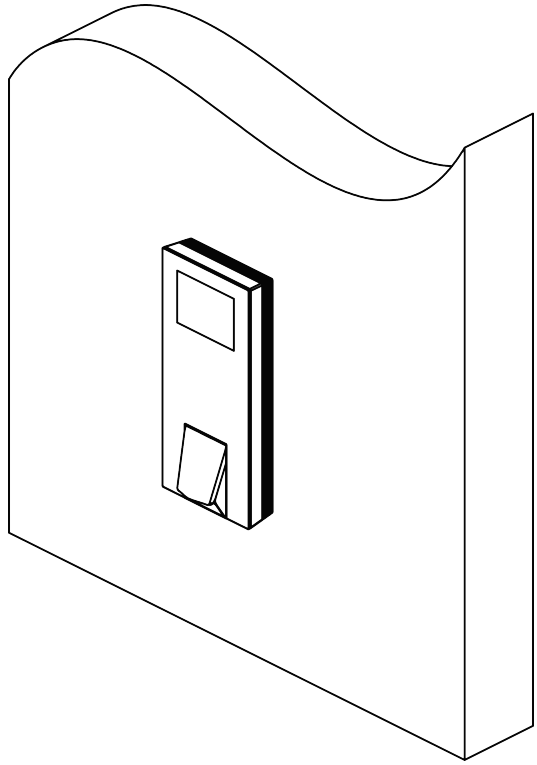


Figure 2-7 Complete Installation

2.3 Install with Gang Box

Steps

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

Note

You should purchase the gang box separately.

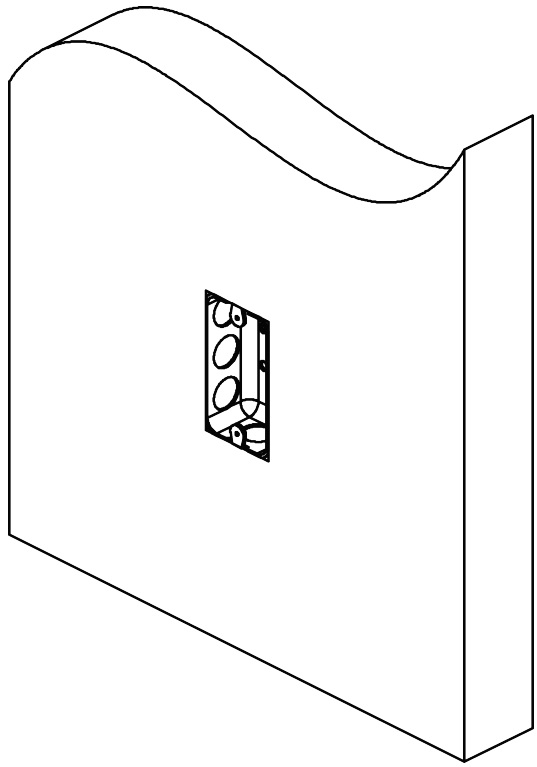


Figure 2-8 Install Gang Box

2. Secure the mounting plate on the gang box with 2 supplied screws (SC-KA4X25). Route the cable through the cable hole, wire the cables and insert the cables in the gang box.

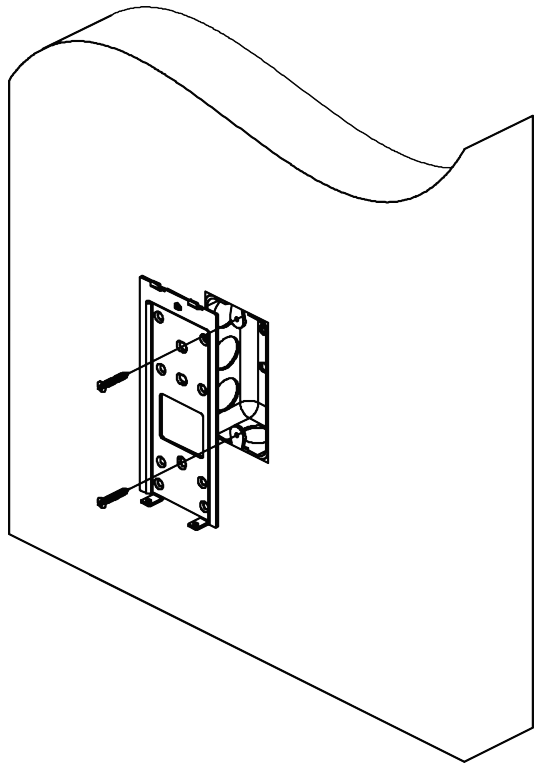


Figure 2-9 Install Mounting Plate

3. Align the device with the mounting plate, and secure the device on the mounting plate with 2 supplied screws (SC-KM3X8-T10-SUS-NL).

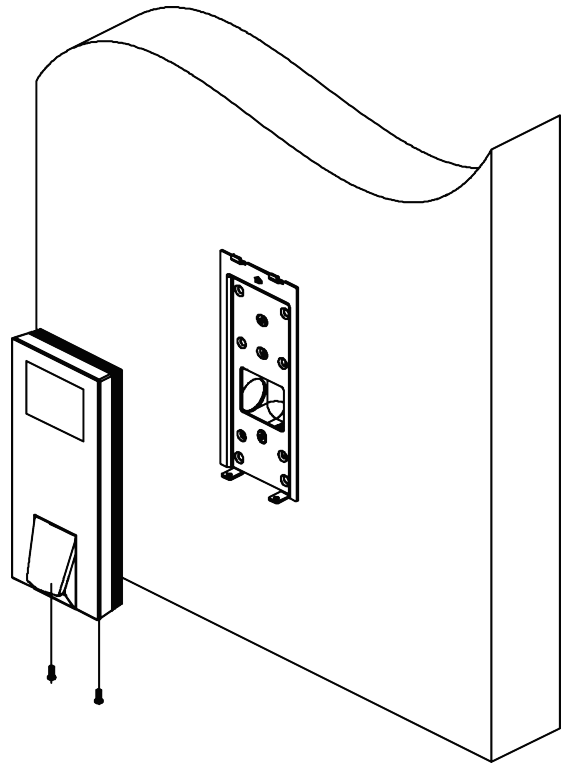


Figure 2-10 Secure Device

4. Complete the installation.

Chapter 3 Wiring

The device supports connecting to the RS-485 terminal, the door lock, the exit button, the alarm output/input devices, the Wiegand card reader, the access controller, and the power supply. You can wire the peripherals according to the descriptions below.

If connect the Wiegand card reader with the access controller, the access control terminal can transmit the authentication information to the access controller and the access controller can judge whether to open the door or not.

Note

- If the cable size is 18 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.
- If the cable size is 15 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
- If the cable size is 12 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 40 m.

3.1 Wire Normal Device

You can connect the terminal with normal peripherals.

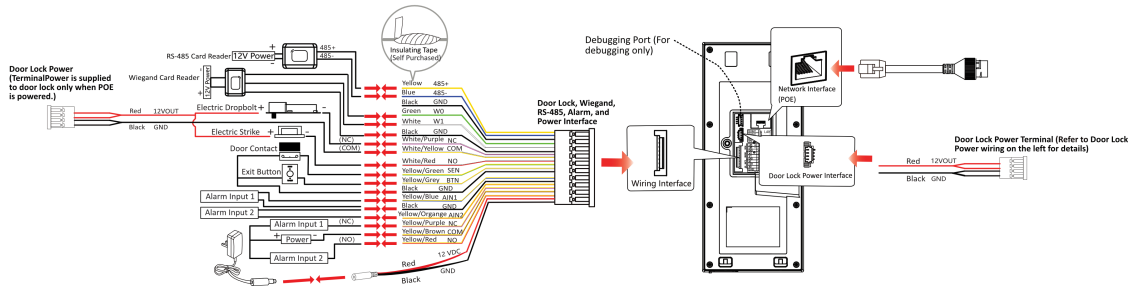


Figure 3-1 Wiring

Note

- Do not wire the device to the electric supply directly.
- When connecting door contact and exit button, the device should use the same common ground connection.
- The suggested external power supply for door lock is 12 V, 1 A

3.2 Wire Secure Door Control Unit

You can connect the terminal with the secure door control unit.

The wiring diagram is as follows.

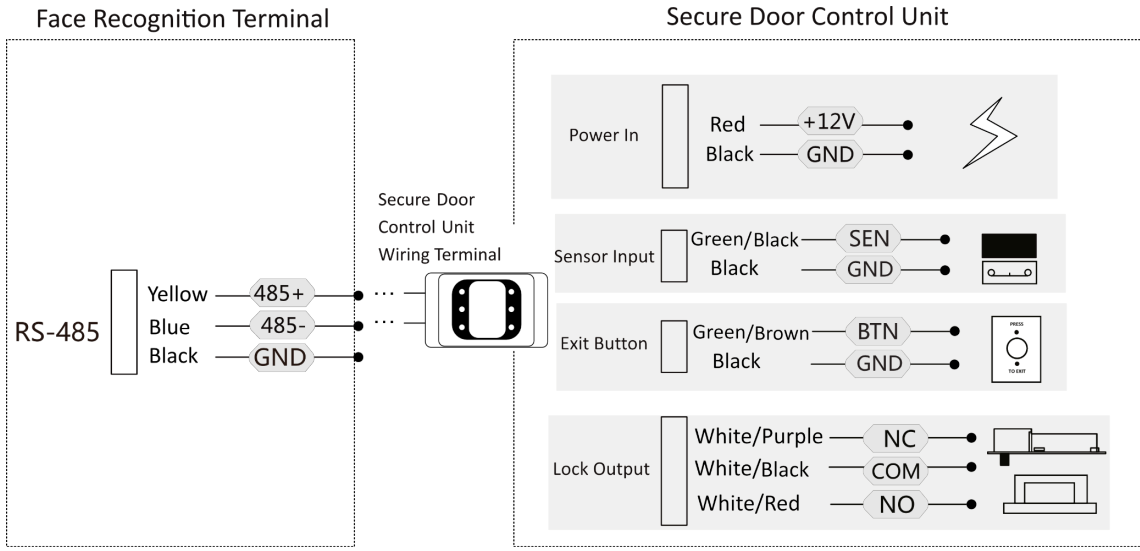


Figure 3-2 Secure Door Control Unit Wiring

Note

- The secure door control unit should connect to an external power supply separately. The suggested external power supply is 12V, 0.5A.
- 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.

Chapter 4 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

4.1 Activate via Device

If the device is not activated, you can activate the device after it is powered on.

On the Activate Device page, create a password and confirm the password. Select **Activate** and the device will activated.

Figure 4-1 Activation Page

- 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.

- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- 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).

4.2 Activate via Mobile Web

You can activate the device via mobile web.

Steps

Note

- After powering on the device for the first time, the hotspot function is enabled by default.
- Only the device with Wi-Fi function supports activation via AP mode.

1. Connect to the device hotspot with your mobile phone by entering the hotspot password. The activation page will pop up.

   Note

   - 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, 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 3 for 5 s to enter the AP mode again.
   - After device activation, the hotspot password will be changed to the device activation password.

2. Create a new password (admin password) and confirm the password.

   Note

   Characters containing admin and nimda are not supported to be set as activation password.

   Caution

   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.

3. Tap **Activate**.

4. Select **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. Edit the device IP address. You can edit the IP address via the SADP tool, PC web browser and the client software.

What to do next

Login the mobile web to configure parameters. For details, see ***Login*** .

4.3 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

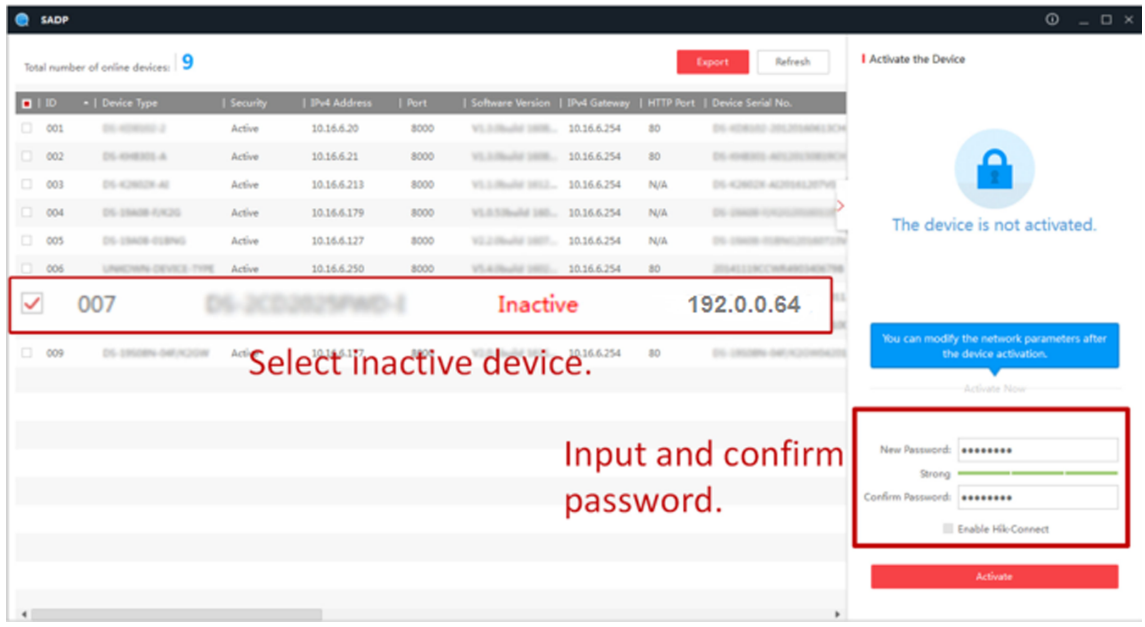
Caution

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.

Note

Characters containing admin and nimda are not supported to be set as activation password.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

4.4 Activate Device via iVMS-4200 Client Software

For some devices, you are required to create the password to activate them before they can be added to the iVMS-4200 software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

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.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Note

Characters containing admin and nimda are not supported to be set as activation password.

7. Click **OK** to activate the device.

Chapter 5 Quick Operation

5.1 Select Language

You can select a language for the device system.

After the device activation, you can select a language for the device system.

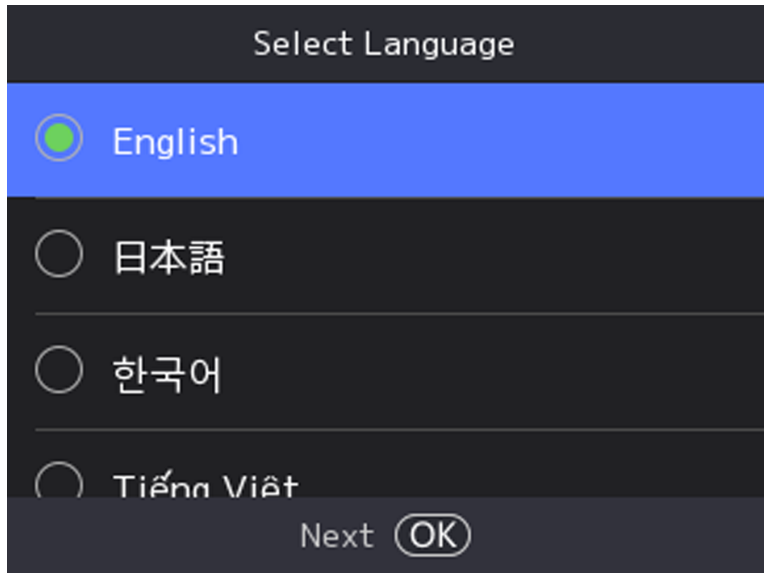


Figure 5-1 Select System Language

By default, the system language is English.

Note

After you change the system language, the device will reboot automatically.

5.2 Set Password Change Type

After activating the device, you can set the password change type as reserved email address or security questions. Once you forgot the device password, you can change the password via the selected change type.

Change Password via Email Address

If you need to change password via reserved email, you can enter an email address, and press **OK**.

Change via Security Questions

If you need to change password via security questions, you can set security questions on Web. Press **ESC**.

Note

You can only select one type to change password. If you need, you can enter the web page to set both of the changing types.

5.3 Set Network Parameters

After activation and select application mode, you can set the network for the device

Steps

1. When you enter the Select Network page, select **Wired Network** or **Wi-Fi** for your actual needs.

Figure 5-2 Select Network

Note

Disconnect the wired network before connecting a Wi-Fi.

2. Select **Next**.

Wired Network

Note

Make sure the device has connected to a network.

If enable **DHCP**, the system will assign the IP address and other parameters automatically.

If disable **DHCP**, you should set the IP address, the subnet mask, and the gateway.

Wi-Fi

Select a Wi-Fi and enter the Wi-Fi's password to get connected.

Or select **Add Wi-Fi** and enter the Wi-Fi's name and the password to get connected.

3. **Optional:** Select **Back** to skip network settings.

Chapter 6 Basic Operation

6.1 Login

Login the device to set the device basic parameters.

6.1.1 Login by Activation Password

You should login the system before other device operations. If you do not configure an administrator, you should follow the instructions below to login.

Steps

1. Long press **OK** to enter the password.
   - If you have added an administrator for the device, you can authenticate the credentials.
   - If you haven't added an administrator for the device, enter the password.
2. Press OK to enter the home page.

Note

The device will be locked for 30 minutes after 5 failed password attempts.

6.2 Communication Settings

6.2.1 Set Wired Network Parameters

You can set the device wired network parameters, including the IP address, the subnet mask, the gateway, and DNS parameters.

Steps

1. Select **System → Communication** to enter the Communication settings page.
2. On the Communication page, select **Wired Network**.
3. Set IP Address, Subnet Mask, and Gateway.
   - Enable **DHCP**, and the system will assign IP address, subnet mask, and gateway automatically.
   - Disable **DHCP**, and you should set the IP address, subnet mask, and gateway manually.

   Note

   The device's IP address and the computer IP address should be in the same IP segment.
4. Set the DNS parameters. You can enable **Auto Obtain DNS**, set the preferred DNS server and the alternate DNS server.

6.2.2 Set Wi-Fi Parameters

You can enable the Wi-Fi function and set the Wi-Fi related parameters.

Steps

Note

The function should be supported by the device.

1. Select **System → Communication** to enter the Communication settings page.
2. On the Communication settings page, select **Wi-Fi**.

Figure 6-2 Wi-Fi Settings

3. Enable the Wi-Fi function.
4. Select a Wi-Fi from the list, and enter the Wi-Fi's password. Select **OK**.

Note

Only digits, letters, and special characters are allowed in the password.

5. Set the Wi-Fi's parameters.
   - By default, DHCP is enable. The system will allocate the IP address, the subnet mask, and the gateway automatically.
   - If disable DHCP, you should enter the IP address, the subnet mask, and the gateway manually.
6. Press ESC to save the network parameters.

6.2.3 Set ISUP Parameters

Set ISUP parameters and the device can upload data via ISUP protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Select **System → Communication** .

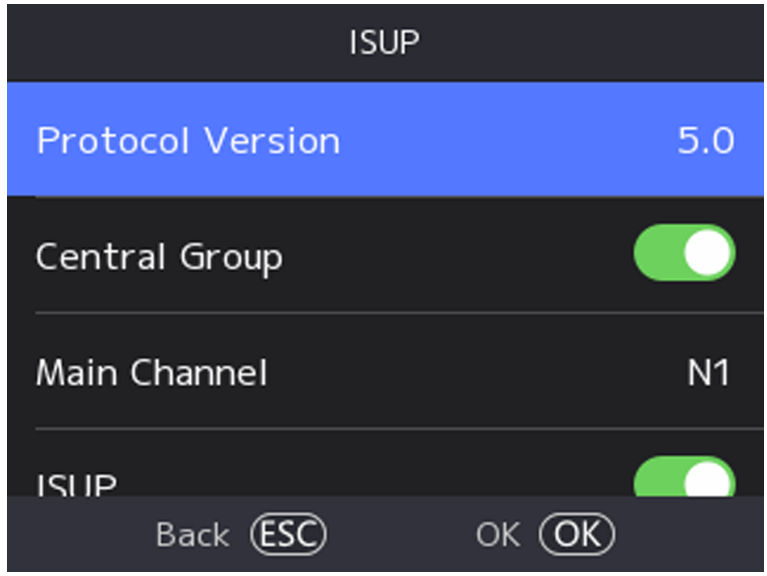


Figure 6-3 ISUP Settings

2. Enable the ISUP function and set the ISUP server parameters.

ISUP Version

Set the ISUP version according to your actual needs.

Central Group

Enable central group and the data will be uploaded to the center group.

Main Channel

Support N1 or None.

ISUP

Enable ISUP function and the data will be uploaded via ISUP protocol.

Address Type

Select an address type according to your actual needs.

IP

Set the ISUP server's IP address.

Port

Set the ISUP server's port No.

Note

Port No. Range: 1 to 65535.

Device ID

Set device serial no.

ISUP Key

If you choose V5.0, you should create an account and ISUP key. If you choose other version, you should create an ISUP account only.

Note

- Remember the ISUP account and ISUP key. You should enter the account name or the key when the device should communicate with other platforms via ISUP protocol.
- ISUP key range: 8 to 16 characters.

6.2.4 Platform Access

You can change the device verification code and set the server address before you add the device to the Hik-Connect mobile client.

Before You Start

Make sure your device has connected to a network.

Steps

1. Select **System → Communication** (Communication) on the Home page to enter the Communication settings page.
2. On the Communication settings page, select **Hik-Connect**.
3. Enable **Hik-Connect**
4. You can view the connection status.
5. Press **ESC**.

6.2.5 Set RS-485 Parameters

The device can connect external access controller, secure door control unit, or card reader via the RS-485 terminal.

Steps

1. Select **System → Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, select **RS-485** to enter the RS-485 tab.
3. Select an peripheral type according to your actual needs.

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

4. Select **ESC** and you should reboot the device if you change the parameters.

6.2.6 Set AP Mode

You can enable AP mode.

Steps

1. Select **System → Communication** on the Home page to enter the Communication Settings page.
2. On the Communication Settings page, select **AP Mode** to enter the settings page.
3. Enable AP mode.
4. You can view the AP name.

6.2.7 Set Wiegand Parameters

You can enable Wiegand function, and select Wiegand direction.

Steps

1. Select **Communication → Wiegand** .
2. Select the Wiegand direction.

6.3 User Management

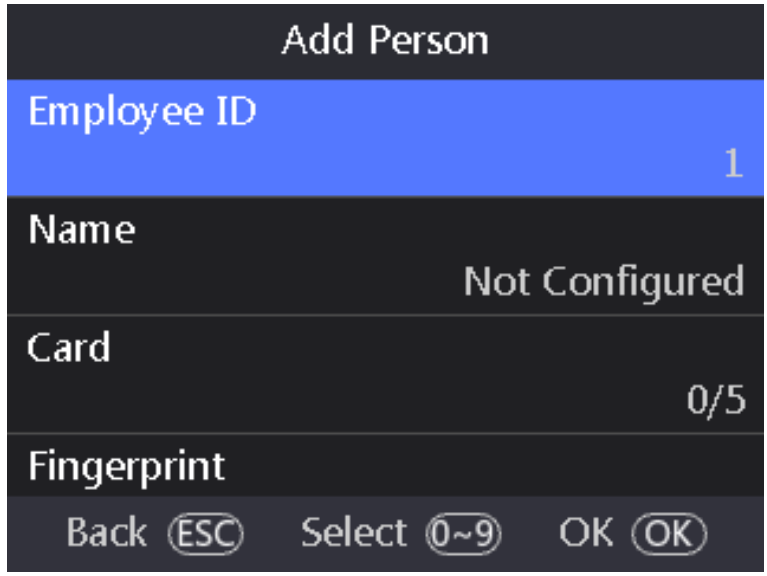
On the user management interface, you can add, edit, delete and search the user.

6.3.1 Add Administrator

The administrator can log in the device backend and configure the device parameters.

Steps

1. Long press OK to enter the admin login page.
2. Select **Person → Add Person** to enter the page.



3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Select the Name field and input the user name on the keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the user name.
- Up to 32 characters are allowed in the user name.

5. **Optional:** Add a fingerprint, or card for the person.

Note

- **Note**

  For details about adding a fingerprint, see ***Add Fingerprint*** .
- For details about adding a card, see ***Add Card*** .

6. **Optional:** Set the user's authentication type.

Note

For details about setting the authentication type, see ***Set Authentication Mode*** .

7. Set the person role.
8. Press ESC and then press OK to save the settings.

6.3.2 Add Fingerprint

Add a fingerprint for the person and the person can authenticate via the added fingerprint.

Steps

Note

The function should be supported by the device.

1. Long press OK and login the device.
2. Press **Person → Add person** to enter the Add person page.
3. Select the Employee ID field and edit the employee ID.

   Note

   - The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
   - The employee ID should not start with 0 and should not be duplicated.
4. Select the Name field and input the person name on the keyboard.

   Note

   - Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
   - The suggested person name should be within 128 characters.
5. Select the Fingerprint field to enter the Fingerprint page.
6. Follow the instructions to add a fingerprint.

   Note

   - The same fingerprint cannot be repeatedly added.
   - Up to 10 fingerprints can be added for one person.
   - You can also use the client software or the fingerprint recorder to record fingerprints. For details about the instructions of scanning fingerprints, see ***Tips for Scanning Fingerprint*** .
7. Set the person role.
8. Press ESC and then press OK to save the settings.

6.3.3 Add Card

Add a card for the person and the person can authenticate via the added card.

Steps

Note

The supported card type varies between different models.

1. Long press OK and login the device.
2. Select **Person → Add Person** to enter the Add person page.
3. Select the Employee ID field and edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Select the Name field and input the person name on the keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 128 characters.

5. Select the Card field and press OK to enter the Add Card page.
6. Configure the card No.
   - Enter the card No. manually.
   - Present the card over the card swiping area to get the card No.

Note

- The card No. cannot be empty.
- Up to 20 characters are allowed in the card No.
- The card No. cannot be duplicated.

7. Configure the card type.
8. Set the person role.
9. Press ESC and then press OK to save the settings.

6.3.4 View PIN code

You can view the person PIN code.

Steps

1. Long press OK and login the device.
2. Select **Person → Add Person** to enter the Add person page.
3. Edit the employee ID.

Note

- The employee ID should be less than 32 characters. And it can be a combination of lower letters, upper letters, and numbers.
- The employee ID should not be duplicated.

4. Select the Name field and input the person name on the keyboard.

Note

- Numbers, upper case letters, lower case letters, and special characters are allowed in the person name.
- The suggested person name should be within 128 characters.

5. View the PIN code.
6. Press ESC and then press OK to save the settings.

6.3.5 Set Authentication Mode

After adding the person's credentials, you should set the authentication mode and the person can authenticate his/her identity via the configured authentication mode.

Steps

1. Long press OK and login the device.
2. Select **Person → Add Person → Authentication Type** .
3. Select Device or Custom as the authentication mode.

   Device

   If you want to select device mode, you should set the terminal authentication mode in Access Control Settings page first. For details see *Setting Access Control Parameters*.

   Custom

   You can combine different authentication modes together according to your actual needs.
4. Press ESC to save the settings.

6.3.6 Edit Person

After adding the person, you can edit it.

Edit Person

On the Person Management page, select a person from the person List to enter the person Information page. Follow the steps in ***User Management*** to edit the person parameters. Press ESC to save the settings.

Note

The employee ID cannot be edited.

6.4 Data Management

You can delete data, import data, and export data.

6.4.1 Delete Data

Delete user data.

On the Home page, select **Data → Delete Data → User Data** . All user data added in the device will be deleted.

6.4.2 Import Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, select **Data → Import Data** .
3. Select **User Data**, or **Access Control Parameters** .

Note

The imported access control parameters are configuration files of the device.

4. Enter the created password when you exported the data. If you do not create a password when you exported the data, leave a blank in the input box and select **OK** immediately.

Note

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB flash drive to Device B. In this case, you should import the user data before importing the profile photo.
- The supported USB flash drive format is FAT32.
- The employee ID should be less than 32 characters. It can be a combination of lower letters, upper letters, and numbers. It should not be duplicated, and should not start with 0.

6.4.3 Export Data

Steps

1. Plug a USB flash drive in the device.
2. On the Home page, select **Data → Export Data** .
3. Select **Face Data**, **Event Data**, **User Data**, or **Access Control Parameters**.

Note

The exported access control parameters are configuration files of the device.

4. **Optional:** Create a password for exporting. When you import those data to another device, you should enter the password.

Note

- The supported USB flash drive format is DB.
- The system supports the USB flash drive with the storage of 1G to 32G. Make sure the free space of the USB flash drive is more than 512M.
- The exported user data is a DB file, which cannot be edited.

6.5 Identity Authentication

After network configuration, system parameters configuration and user configuration, you can go back to the initial page for identity authentication. The system will authenticate person according to the configured authentication mode.

6.5.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Authenticate fingerprint, card or PIN.

Fingerprint

Place the enrolled fingerprint on the fingerprint module and start authentication via fingerprint.

Card

Present the card on the card swiping area and start authentication via card.

Note

The card can be normal IC card, or encrypted card.

PIN Code

Enter the pin code to authenticate via PIN code.

If authentication completed, a prompt "Authenticated" will pop up.

6.5.2 Authenticate via Multiple Credential

Before You Start

Set the user authentication type before authentication. For details, see ***Set Authentication Mode*** .

Steps

1. If the authentication mode is Card and Password, authenticate any credential according to the instructions on the live view page.

   Note

   - The card can be normal IC card, or encrypted card.

2. After the previous credential is authenticated, continue authenticate other credentials.

Note

- For detailed information about scanning fingerprint, see *Tips for Scanning Fingerprint*.

If authentication succeeded, the prompt "Authenticated" will pop up.

6.6 Basic Settings

You can set the voice, time, sleeping, language, and privacy.

Long press OK and login the device. Select **System → Basic** to enter Basic Settings page.

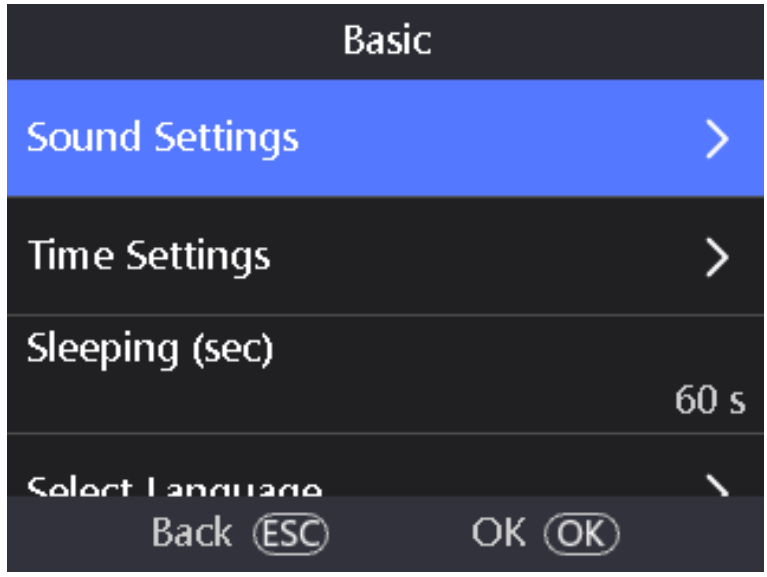


Figure 6-4 Basic Settings Page

Sound Settings

You can enable/disable the sound function.

Time Settings

Set the time zone, the device time and the DST.

Sleeping (sec)

Set the device sleeping waiting time (s). For example, when you are on the initial page and if you set the sleeping time to 30 s, the device will sleep after 30 s without any operation.

Note

20 s to 1800 s are available to configure.

Select Language

Select the language according to actual needs.

Privacy

Name/Employ ID

You can choose to display/not display/desensitize name and Employ ID when authenticating.

6.7 Password Management

You can change device password.

Steps

1. Long press **OK** and login the device. Select **System → Basic → Password** .
2. Select **Change Password**. Enter the old password.
3. Enter the new password and confirm it.
4. Select **OK**.

Note

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 two 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.
Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

6.8 Set Access Control Parameters

You can set the access control permissions, including the functions of authentication mode, authentication interval and password mode.

On the home page, select **ACS** (Access Control Settings) to enter the Access Control Settings page. Edit the access control parameters on this page.

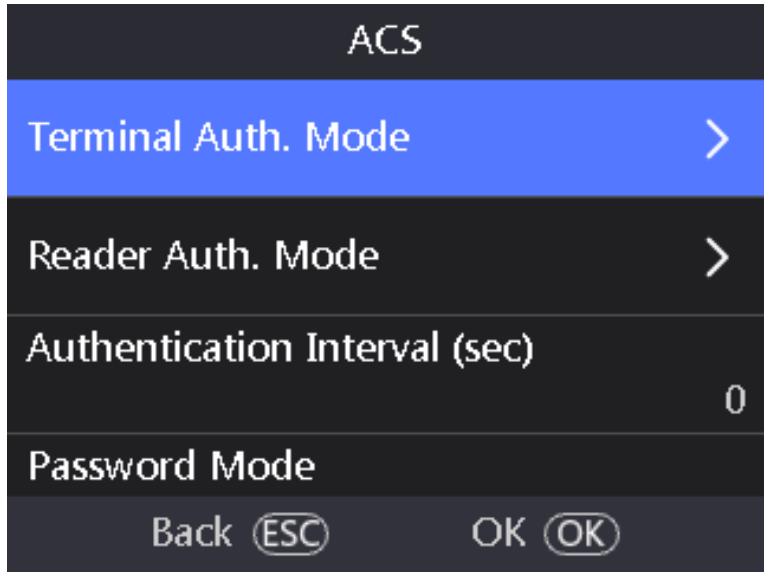


Figure 6-5 Access Control Parameters

The available parameters descriptions are as follows:

Table 6-1 Access Control Parameters Descriptions

Parameter	Description
Terminal/Reader Authentication Mode	Select the authentication mode. You can also customize the authentication mode. **Note** • Only the device with the fingerprint module supports the fingerprint related function. • Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
Authentication Interval	Set the device authenticating interval. Available authentication interval range: 0 to 65535.
Password Mode	**Platform-Applied Personal PIN** The PIN is managed and distributed by the platform. You cannot set the PIN on the device or Web. **Device-Set Personal PIN** The PIN is set on the device or Web. You cannot set the PIN on other platform.

6.9 System Maintenance

You can view the device system information and capacity. You can also upgrade device, view the user manual, restore the system to factory settings, default settings, and reboot the system.

Long press OK and login the device. Select **Maint.** to enter System Maintenance page.

System Information

You can view the device information including device model, serial No., firmware version, MAC address, production data and open source code license.

Note

The page may vary according to different device models. Refers to the actual page for details.

Capacity

You can view the number of user, face picture, card, fingerprint and event.

Note

Parts of the device models support displaying the fingerprint number. Refers to the actual page for details.

Device Upgrade

Online Update

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can select **Device Upgrade → Online Update** to upgrade the device system.

Update via USB

Plug the USB flash drive in the device USB interface. Select **Device Upgrade → Update via USB** , and the device will read the *digicap.dav* file in the USB flash drive to start upgrading.

User Manual

You can scan the QR code to view the user manual.

Restore to Factory Settings

All parameters will be restored to the factory settings. The system will reboot to take effect.

Restore to Default Settings

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.

Reboot

The device will reboot after the confirmation.

Chapter 7 Configure the Device via the Mobile Web

7.1 Login

Log in the mobile browser to configure.

Note

- The device is in AP mode in default.
- Make sure the device is activated.

Enter the device IP address in the address bar of the mobile browser and tap **Enter** to enter the login page.

Enter the device user name and the password. 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.

7.2 Overview

You can view the door status, network status and basic information, and set person management, smart settings, authentication settings, and door parameters via shortcut entry.

Function Descriptions:

Door Status

/ / /

The door status is open/closed/remaining open/remaining closed. You can tap to select open/closed/remaining open/remaining closed status according to your actual needs.

Shortcut Entry

You can set person management, smart settings, authentication settings, and door parameters via shortcut entry.

Network Status

You can view the connected and registered status of wired network, wireless network, ISUP and Hik-Connect.

Basic Information

You can view the model, serial No. and firmware version.

7.3 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, tap **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

7.4 Configuration

7.4.1 View Device Information

View the device name, language, model, serial No., version, IO input number, IO output number,local RS-485 number, number of alarm input and output, Mac address, factory information and device capacity, etc.

Tap → **System Settings** → **Basic Information** to enter the configuration page.

View the device name, language, model, serial No., version, IO input number, IO output number,local RS-485 number, number of alarm input and output, Mac address, factory information and device capacity, etc.

7.4.2 Time Settings

Set the time zone, time sync. mode, and displayed time.

Tap → **System Settings** → **Time Settings** to enter the settings page.

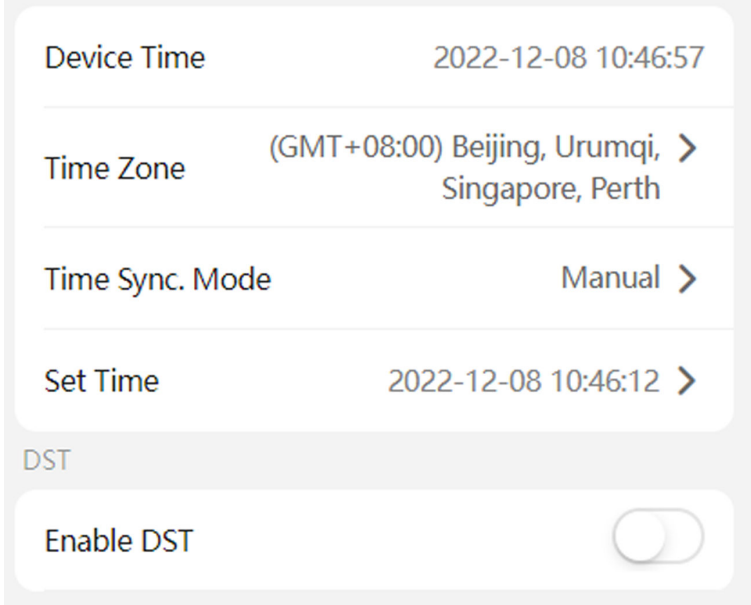


Figure 7-1 Time Settings

Tap **Save** to save the settings.

Time Zone

Select the time zone where the device is located from the drop-down list.

Time Sync. Mode

Manual

By default, the device time should be synchronized manually. You can set the device time manually.

NTP

Set the NTP server's IP address, port No., and interval.

7.4.3 Set DST

Steps

1. Tap → **System Settings** → **Time Settings** , to enter the settings page.

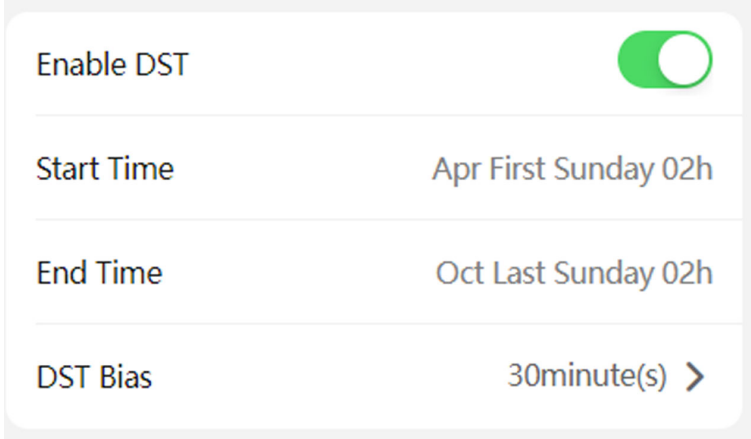


Figure 7-2 DST

2. Tap **Enable DST**.
3. Set the start time, end time, and DST bias.
4. Tap **Save**.

7.4.4 User Management

Steps

1. Tap → **User Management** → **User Management** → **admin** to enter the setting page.
2. Enter the old password and create a new password.
3. Confirm the new password.
4. Tap **Save**.

Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using 8-16 characters, including at least two 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.

7.4.5 Network Settings

Wired Network

Set wired network.

Tap → **Communication Settings** → **Wired Network** to enter the configuration page.

DHCP

If you disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, Mac address, and MTU, Mac address, MTU.

If you enable the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Wi-Fi Parameters

Set the Wi-Fi parameters for device wireless connection.

Steps

Note

The function should be supported by the device.

1. Tap → **Communication Settings** → **Wi-Fi** to enter the settings page.
2. Enable **Wi-Fi**.

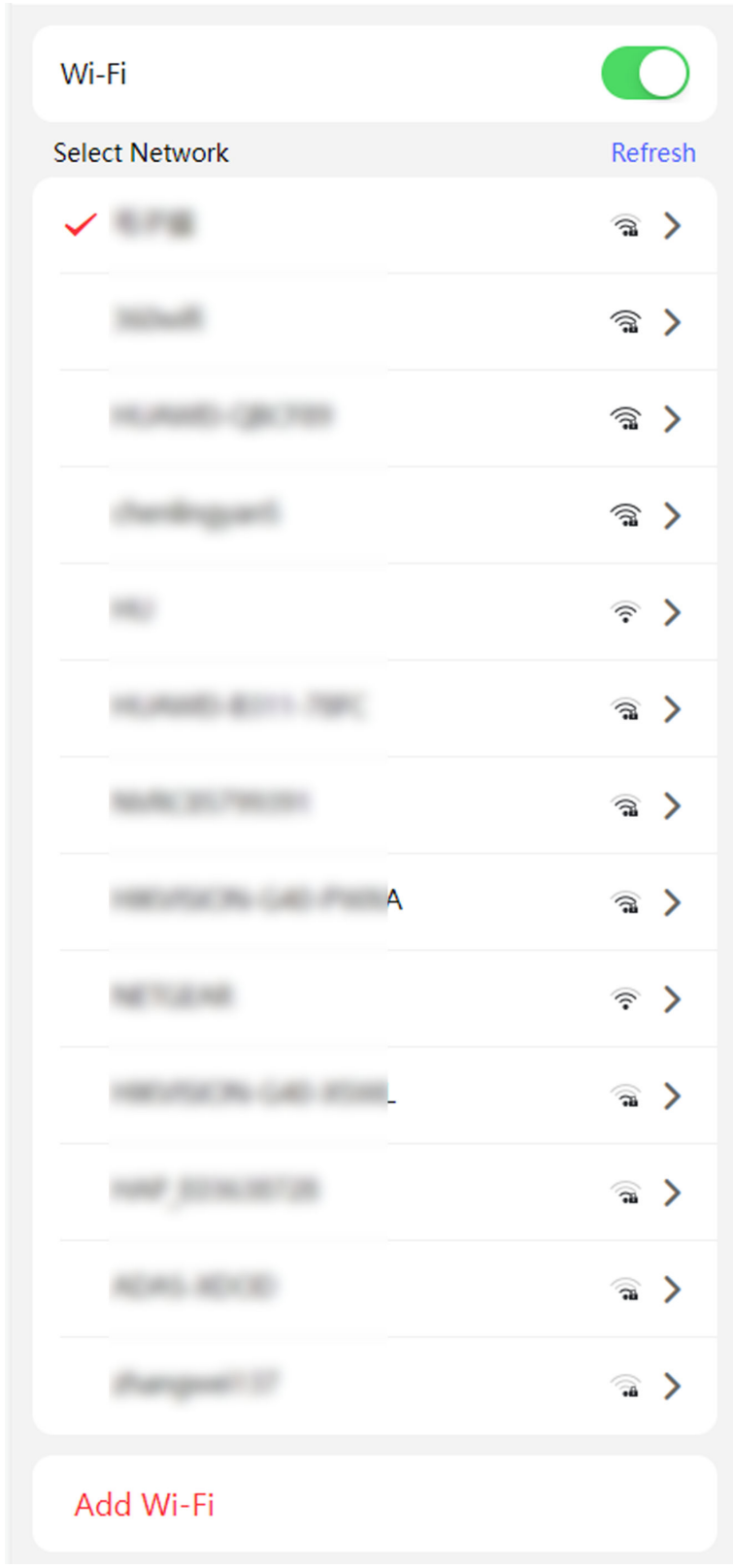


Figure 7-3 Wi-Fi

3. Add Wi-Fi.
   1) Tap **Add Wi-Fi**.
   2) Enter **Wi-Fi Name** and **Wi-Fi Password**, and select **Encryption Type**.
   3) Tap **Save**.
4. Select the Wi-Fi name, and tap **Connect**.
5. Enter the password and tap **Save**.

Set Device Hotspot

Set the device hotspot, and mobile phone can connect to the device to enter the mobile browser.

Steps

1. Tap → **Communication Settings** → **Device Hotspot** .
2. You can enable device hotspot and view the hotspot name.

   Note

   By default, the hotspot name is the AP_Device Serial No.
3. Tap **Save**.

Set Port Parameters

You can set the HTTP and HTTPS according to actual needs when accessing the device via network.

Tap → **Network Service** → **HTTP(S)** , to enter the setting page.

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Tap → **Device Access** → **Hik-Connect** to enter the settings page.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.
2. Check **Enable** to enable the function.
3. You can enable **Custom** to enter the server address.

Note

- 6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.
- The verification code cannot be ***123456*** or ***abcdef*** (case non-sensitive0).

4. You can view **Register Status** and **Binding Status**.
5. Enable **Video Encryption**, and create the password and confirm it.

Note

After adding the device to APP, you need to enter the video encryption password to live view the device.

6. You can tap **Bind An Account → View QR Code** , scan the QR code to bind an acount.
7. Tap **Save** to enable the settings.

Set ISUP Parameters

Set the ISUP parameters for accessing device via ISUP protocol.

Steps

Note

The function should be supported by the device.

1. Tap ≡ → **Device Access → ISUP** to enter the settings page.
2. Enable **ISUP**.
3. Set the ISUP version, server Address, port, device ID and encryption key.

Note

If you select 5.0 as the version, you should set the encryption key as well.

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

7.4.6 Person Management

You can add, edit, delete, and search person via mobile Web browser.

Steps

1. Tap ≡ → **Person Management** to enter the settings page.
2. Add person.
   1) Tap**+**.
   2) Set the following parameters.

Employee ID

Enter the employee ID. The Employee ID cannot be 0 or exceed 32 characters. It can be a combination of uppercase, lowercase letters and numbers.

Name

Enter your name. The name supports numbers, uppercase and lowercase English, and characters. The name is recommended to be within 32 characters.

Long-Term Effective person

Set the person permission as long-term effective.

Start Date/End Date

Set **Start Date** and **End Date** of person permission.

Administrator

If the person needs to be set as administrator, you can enable **Administrator**.

person Role

Select your person role.

Fingerprint

Add fingerprint. Tap **Fingerprint**, then tap **+**, and add fingerprint via the fingerprint module.

Card

Add card. Tap **Card**, then tap **+**, enter the card No. and select card type.

PIN

Note

- Before configuring passwords, it is necessary to clarify whether the password is device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created and edited on Web and cannot be created and edited on the platform; If it is a platform-applied personal PIN, it needs to be configured on the platform and cannot be edited on the Web.
- Make sure **Password Mode** is selected as **Device Password**.

Tap **Person Management → Add** to enter the Add Person page.

Enter the password.

3) Tap **Save**.

3. Tap the person that needs to be edited in the person list to edit the information.
4. Tap the person that needs to be deleted in the person list, and tap to delete the person.
5. You can search the person by entering the employee ID or name in the search bar.

7.4.7 Search Event

Tap **Search** to enter the Search page.

Enter the search conditions, including the employee ID, the name, the card No., the start time, and the end time, and tap **Search**.

Note

Support searching for names within 32 digits.

7.4.8 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

1. Tap → **Access Control** → **Authentication Settings** .
2. Tap **Save**.

Terminal

Select terminal for settings.

Enable Authentication Device

Enable the authentication function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Interval When Entering Password

When you entering the password on the card reader, if the interval between pressing two digits is longer than the set value, the digits you pressed before will be cleared automatically.

Enable Card No. Reversing

The card No. will be in reverse sequence after enabling the function.

Enable Bluetooth

After enabling, you can connect bluetooth.

Set Door Parameters

Tap → **Access Control** → **Door Parameters** .

Tap **Save** to save the settings after the configuration.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remaining Open Duration with First Person (min)

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Door Opening Timeout Alarm

An alarm will be triggered if the door has not been closed within the configured time duration.

Door Lock Status

You can set as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Door Lock Powering off Status

You can set as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Closed**.

Door Opening Duration in Special Scene

The door contact can be enabled with appropriate delay after person with extended access needs swipes her/his card.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Super Password

The specific person can open the door by inputting the super password.

Note

The duress code and the super code should be different. And the digit ranges from 4 to 8.

Set RS-485 Parameters

You can set the RS-485 parameters including the peripheral, address, baud rate, etc.

Tap → **Access Control** → **RS-485** .

Tap **Save** to save the settings after the configuration.

Peripheral Type

Select a peripheral from the drop-down list according the actual situation. You can select from **Card Reader**, **Extension Module**, or **Access Controller**.

Note

After the peripheral is changed and saved, the device will reboot automatically.

RS-485 Protocol

Private

The device can connect with the third party device via RS-485.

OSDP

Standard RS-485 protocol.

RS-485 Address

Set the RS-485 Address according to your actual needs.

Note

If you select **Access Controller**: If connect the device to a terminal via the RS-485 interface, set the RS-485 address as 2. If you connect the device to a controller, set the RS-485 address according to the door No.

Baud Rate

The baud rate when the devices are communicating via the RS-485 protocol.

Data Bit

The data bit when the devices are communicating via the RS-485 protocol.

Stop Bit

The stop bit when the devices are communicating via the RS-485 protocol.

Parity/Flow Ctrl/Communication Mode

Enabled by default.

Set Card Security

Tap → **Card Settings** to enter the configuration page.

Set the parameters and tap **Save**.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Sector

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

EM card is supported when the device connects a peripheral card reader that supports presenting EM card.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Card No. Authentication Mode

You can select **Full card No.**, **3 Bytes** or **4 Bytes**.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

1. Tap → **Access Configuration** → **Wiegand Settings** .
2. Enable **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

Note

The device can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.

4. Tap **More**, and you can set **Time Interval** and **Pulse Width**.
5. Tap **Save** to save the settings.

7.4.9 Fingerprint Parameters Settings

Set fingerprint Parameters.

Note

The function should support by the device.

Fingerprint Parameters

Tap → **Smart** → **Fingerprint Parameters** .

Fingerprint Security Level

You can set the security level of fingerprint. The higher the security level you set, the lower the False Acceptance Rate (FAR) will be. The higher the security level you set, the lower the False Rejection Rate (FRR) will be.

7.4.10 Set Privacy Parameters

Set the storage and authentication result parameters.

Tap → **Configuration** → **Privacy Settings** .

Event Storage

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Authentication Settings

Name Display/Employee ID

You can tap to enable Picture, Name, or Employee ID to display. When authentication is completed, the system will display the selected contents in the result.

Name De-identification

The name information is desensitized with an asterisk.

7.4.11 Password Mode

Before configuring passwords, it is necessary to clarify whether the password is a device-set personal PIN or a platform-applied personal PIN. If it is a device-set personal PIN, it can be created or edited on the device or on the web, and cannot be set on other platforms; If it is a platform-applied personal PIN, it can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

Steps

1. Tap → **Security** → **Password Mode**

Device-Set Personal PIN

It can be created or edited on the device or on the web, and cannot be set on other platforms.

Platform-Applied Personal PIN

It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

2. Tap **Save**.

7.4.12 Upgrade and Maintenance

Restart device, restore device parameters, and upgrade device version.

Restart Device

Tap → **Restart Device** .
Tap **Restart** to restart the device.

Upgrade

Tap → **Upgrade** .
Tap **Upgrade** to upgrade the device.

Note

Do not power off during the upgrading.

Restore Parameters

Tap → **Default** .

Restore to Default Settings

The device will restore to the default settings, except for the device IP address and the user information.

Restore to Factory Settings

All parameters will be restored to the factory settings. You should activate the device before usage.

7.4.13 View Online Document

Tap → **View Online Document** . Tap **View Online Document**, you can scan the QR code with your mobile phone for details.

7.4.14 View Open Source Software License

Tap → **Open Source Software License** , and tap **Open Source Software License** to view the device license.

Chapter 8 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

Click/tap the link to view the client software's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42

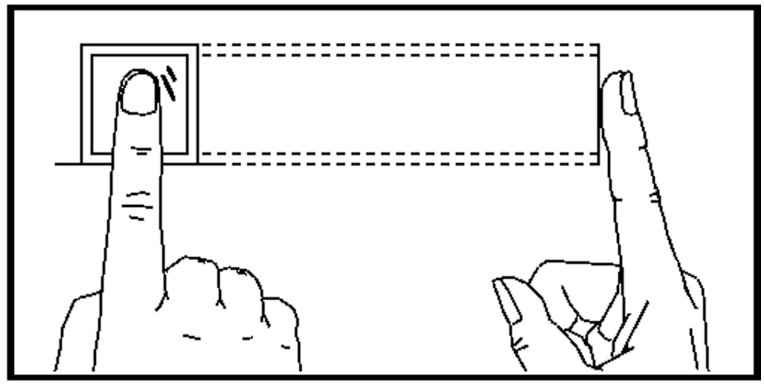
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

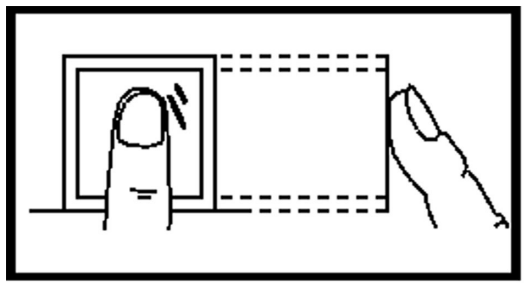
The figure displayed below is the correct way to scan your finger:



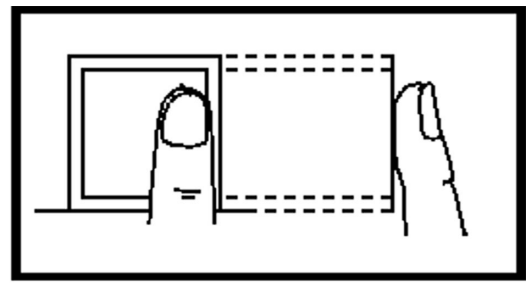
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

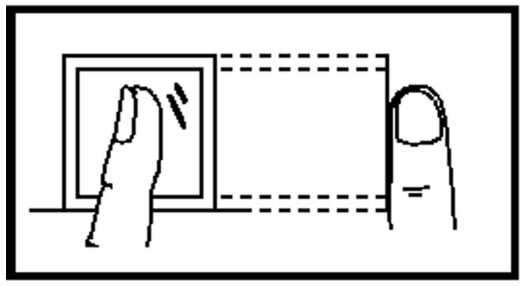
The figures of scanning fingerprint displayed below are incorrect:



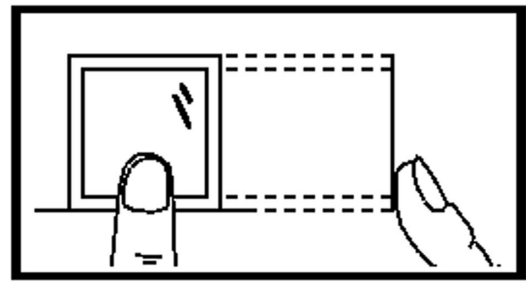
Vertical



Edge I



Side



Edge II

Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. Dimension

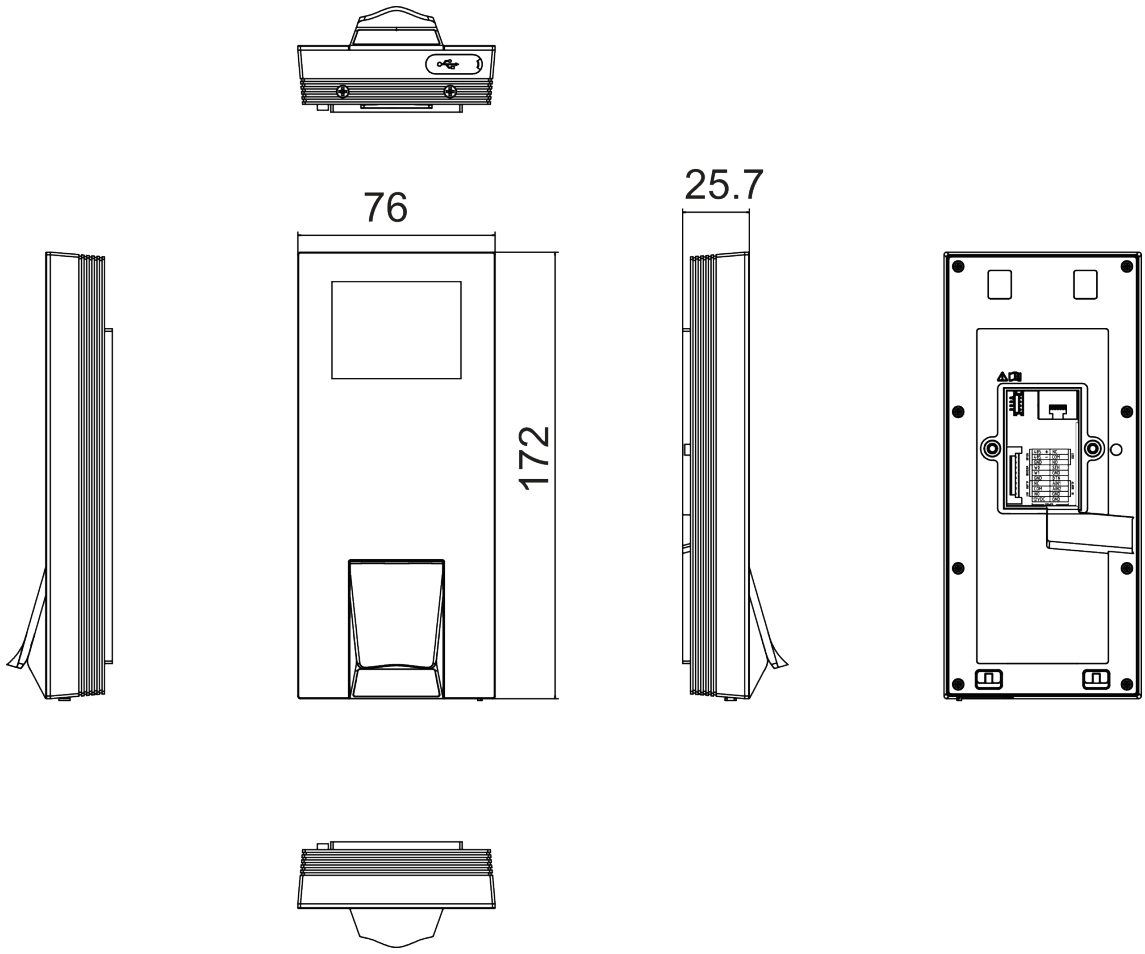


Figure B-1 Dimension

Unit: mm.


See Far, Go Further