Access Control Terminal

User Manual

Legal Information

©2023 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

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

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

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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.

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
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
FCC Conditions
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

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, the RoHS Directive 2011/65/EU

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

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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.
Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope

rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.
This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.
Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

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.

⚠ Dangers

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Do not ingest battery, Chemical Burn Hazard.
  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.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions

- This equipment is not suitable for use in locations where children are likely to be present.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).

- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- You can view the device License via the website: *http://opensource.hikvision.com/Home/List?id=46*.

Available Models

The access control terminal contains the following models:

Product Name	Model	Wireless
Access Control Terminal	DS-K1T805MBWX	13.56 MHz Card Presenting Frequency, Wi-Fi, Bluetooth
	DS-K1T805MBFWX	13.56 MHz Card Presenting Frequency, Wi-Fi, Bluetooth
	DS-K1T805EBWX	125 KHz Card Presenting Frequency, Wi-Fi, Bluetooth
	DS-K1T805EBFWX	125 KHz Card Presenting Frequency, Wi-Fi, Bluetooth

Contents

Chapter 1 Features **1**

Chapter 2 Appearance **2**

Chapter 3 Installation **4**

3.1 Installation Environment 4

3.2 Surface Mounting 4

3.3 Flush Mounting with Gang Box 7

Chapter 4 Device Wiring **13**

4.1 External Device Wiring 13

4.2 Wire Secure Door Control Unit 14

Chapter 5 Activation **15**

5.1 Activate via Mobile Web 15

5.2 Activate via Web Browser 16

5.3 Activate via SADP 16

5.4 Activate Device via iVMS-4200 Client Software 18

Chapter 6 Identity Authentication **19**

6.1 Authenticate via Single Credential 19

6.2 Authenticate via Multiple Credential 19

Chapter 7 Quick Operation via Web Browser **20**

7.1 Set Security Question 20

7.2 Select Language 20

7.3 Time Settings 20

7.4 Administrator Settings 21

Chapter 8 Operation via Web Browser **22**

8.1 Login 22

8.2 Forget Password 22

8.3 Overview 22

8.4 Person Management 24
8.5 Search Event 25
8.6 Configuration 25
8.6.1 View Device Information 25
8.6.2 Set Time 25
8.6.3 Set DST 26
8.6.4 Change Administrator's Password 26
8.6.5 Account Security Settings 27
8.6.6 Online Users 27
8.6.7 View Device Arming/Disarming Information 27
8.6.8 Network Settings 27
8.6.9 Event Linkage 31
8.6.10 Access Control Settings 32
8.6.11 Card Settings 37
8.6.12 Set Privacy Parameters 38
8.6.13 Set Smart Parameters 38
8.6.14 Upgrade and Maintenance 38
8.6.15 Device Debugging 39
8.6.16 Log Query 39
8.6.17 Security Mode Settings 40
8.6.18 Certificate Management 40
Chapter 9 Configure the Device via the Mobile Browser 42
9.1 Login 42
9.2 Overview 42
9.3 Forget Password 43
9.4 Configuration 43
9.4.1 View Device Information 43
9.4.2 Time Settings 43

9.4.3 Set DST 44
9.4.4 User Management 45
9.4.5 Network Settings 45
9.4.6 User Management 49
9.4.7 Search Event 51
9.4.8 Access Control Settings 51
9.4.9 Fingerprint Parameters Settings 57
9.4.10 Upgrade and Maintenance 58
9.4.11 View Online Document 58
9.4.12 View Open Source Software License 58
Chapter 10 Other Platforms to Configure 59
Appendix A. Tips for Scanning Fingerprint 60
Appendix B. Dimension 62

Chapter 1 Features

- High protective level: IP65 and IK08
- Slim and flexible design with metal
- Built-in card reader for M1/EM card

Note

Device supports M1 card or EM card according to different device models.

- Supports operation by mobile App (Hik-Connect)
- Supports AP mode, configuration via PC web and mobile web are available

Note

Only device supporting Wi-Fi function supports AP mode.

- Supports multiple authentication types: card, fingerprint, PIN, and bluetooth

Note

Fingerprint and bluetooth functions should be supported by the device.

Chapter 2 Appearance

Refer to the following contents for detailed information of the access control terminal:

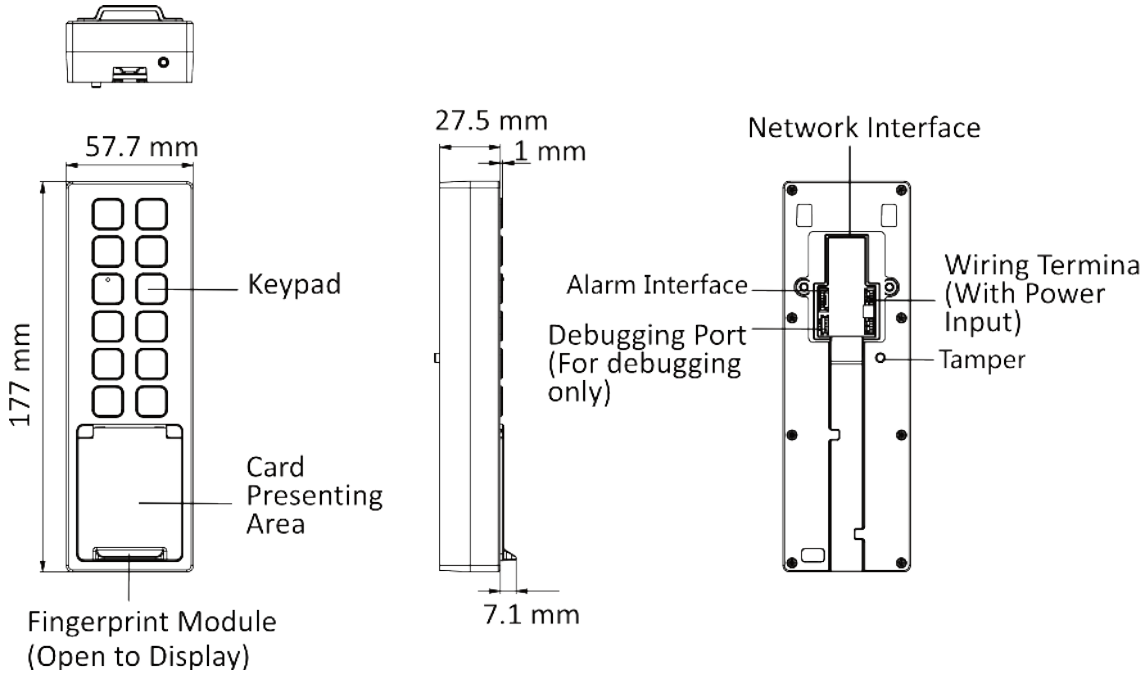


Figure 2-1 Access Control Terminal (Fingerprint + Card Series)

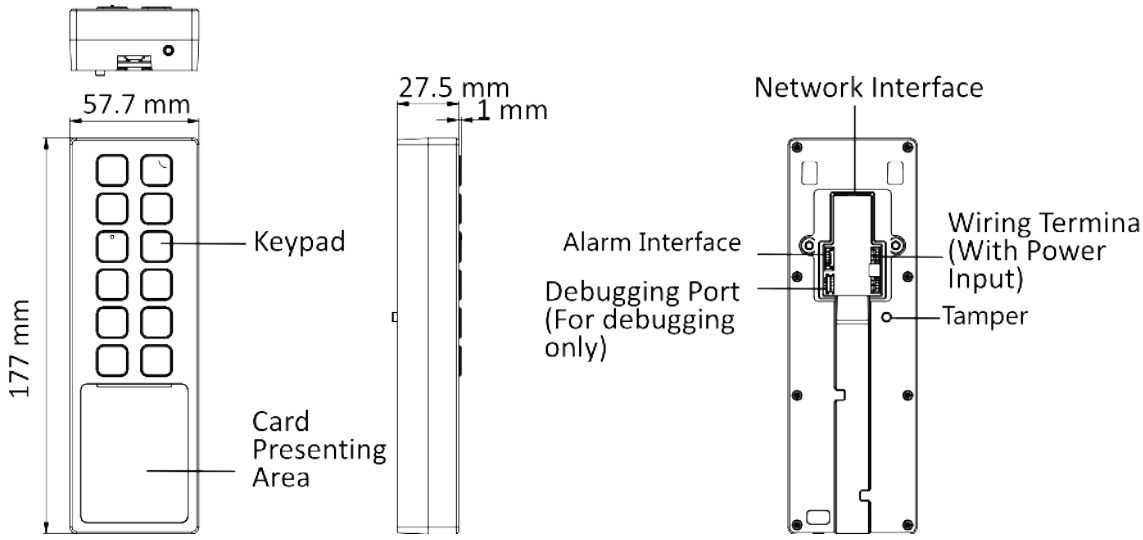


Figure 2-2 Access Control Terminal (Card Series)

Note

The pictures here are for reference only.

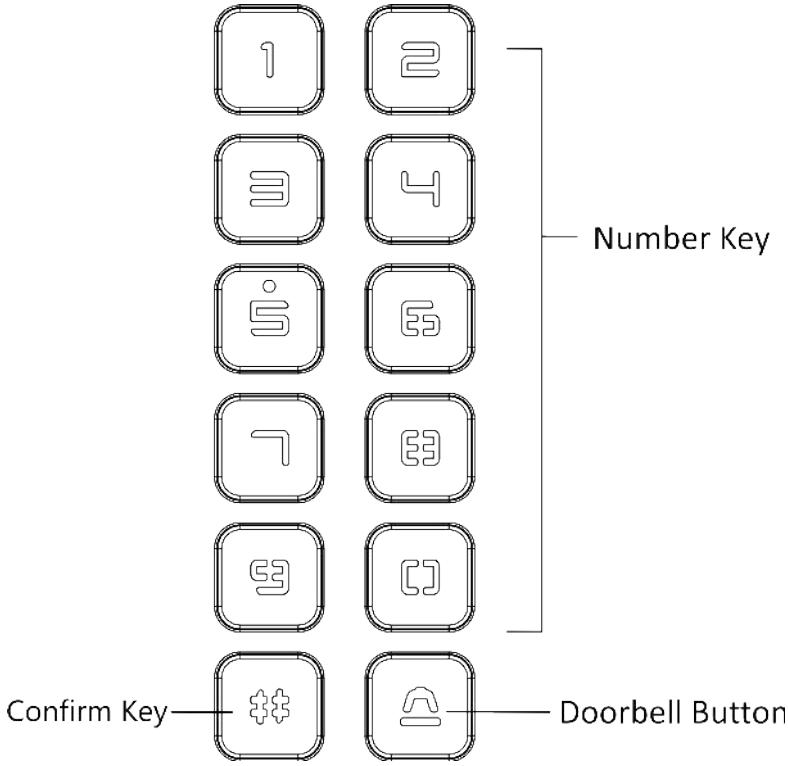


Figure 2-3 Keypad

Note

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

Chapter 3 Installation

3.1 Installation Environment

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

3.2 Surface Mounting

Steps

Note

The additional force shall be equal to three times the weight of the equipment. The equipment ad its associated mounting means shall remain secure during the installation. After the installation, the equipment, including any associated mounting plate, shall not be damaged.

1. Install the mounting plate on the wall with 4 supplied screws (SC-KA4X22). Make sure the cables are through the cable hole.

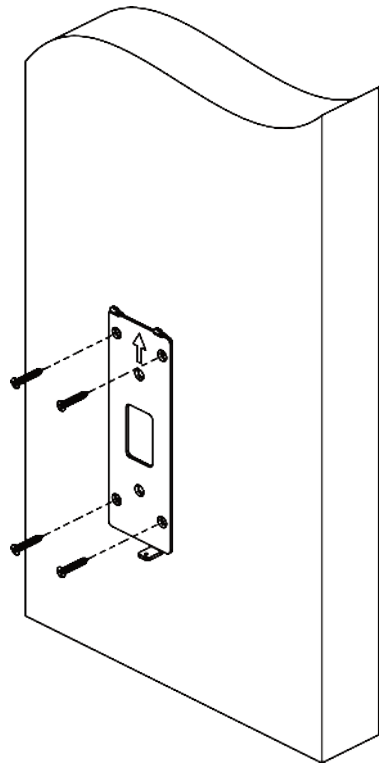


Figure 3-1 Install Mounting Plate

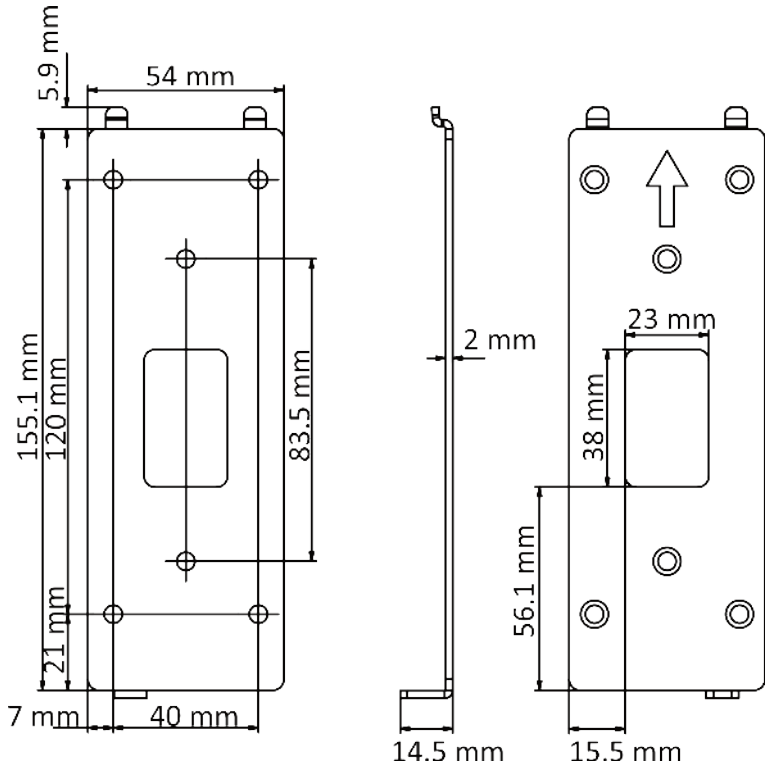


Figure 3-2 Mounting Plate Dimension

2. Remove the back panel to display the wiring area. Wire the cables and install the back panel back.

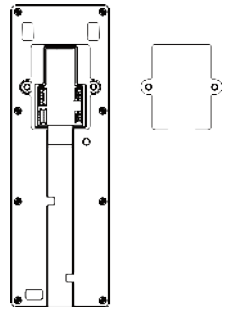


Figure 3-3 Remove Back Panel

Note

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

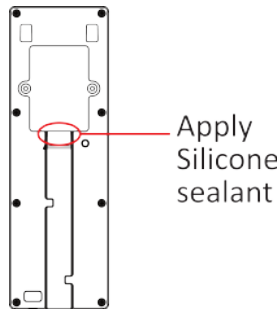


Figure 3-4 Apply Silicone Sealant

3. AAlign and hang the device with the mounting plate.

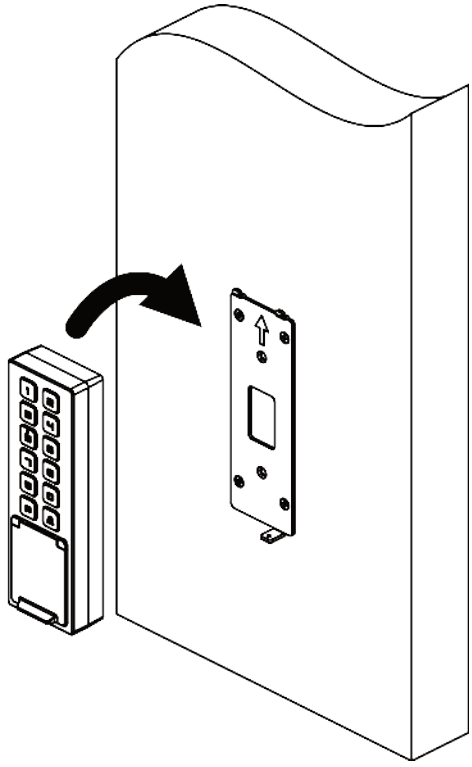


Figure 3-5 Align and Hang Device

4. Use 1 supplied screw (SC-KM3×8-T10-SUS-NL) to secure the device and the mounting plate.

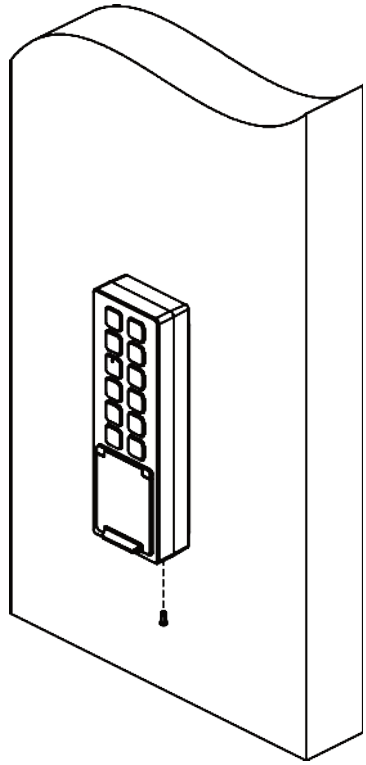


Figure 3-6 Secure Device

3.3 Flush Mounting with Gang Box

Steps

Note

The gang box is optional. You should purchase it separately.

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

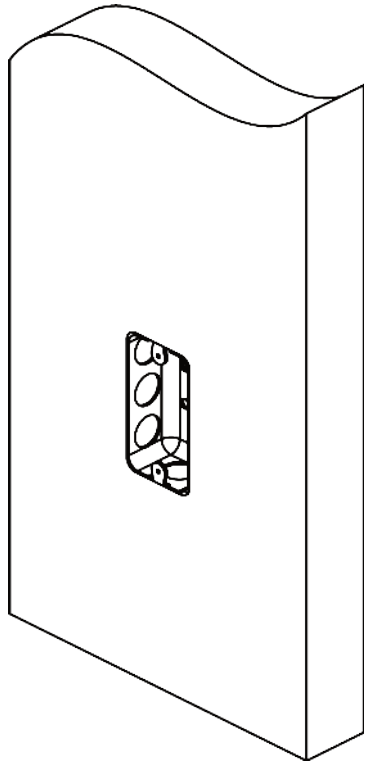


Figure 3-7 The Gang Box on the Wall

Note

Gang box is not supplied.

2. Secure the mounting plate on the wall with 4 supplied screws (SC-KA4X22). Make sure the cables are through the cable hole.

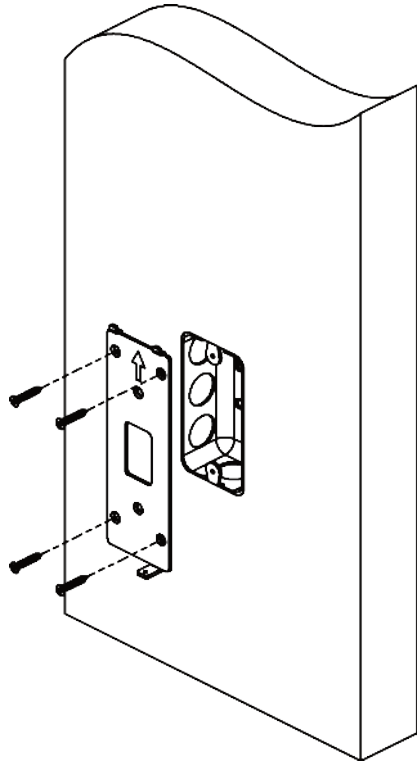


Figure 3-8 Install Mounting Plate

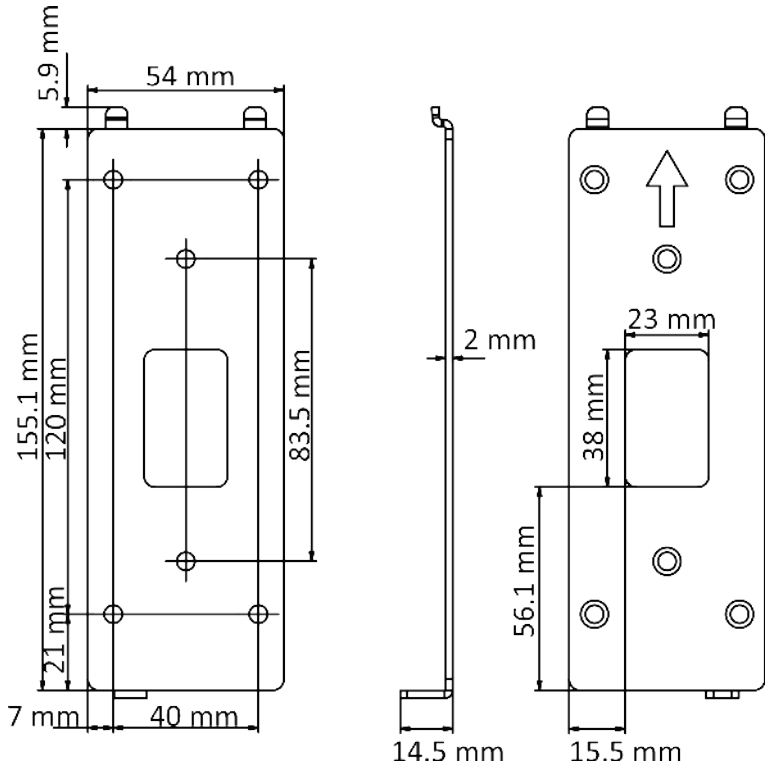


Figure 3-9 Mounting Plate Dimension

3. Remove the back panel to display the wiring area. Wire the cables and install the back panel back.

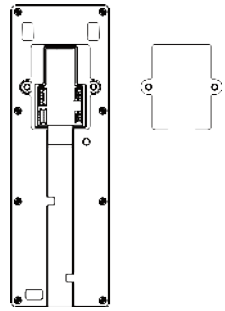


Figure 3-10 Remove Back Panel

Note

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

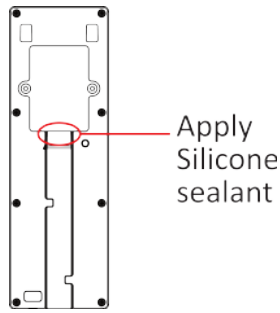


Figure 3-11 Apply Silicone Sealant

4. Align and hang the device with the mounting plate.

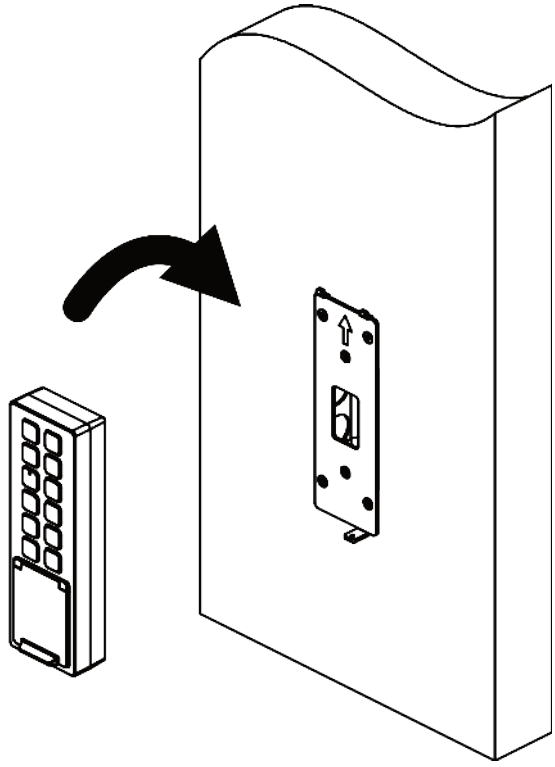


Figure 3-12 Align Device

5. Secure the device on the mounting plate with 1 supplied screw (SC-KM3X8-T10-SUS-NL).

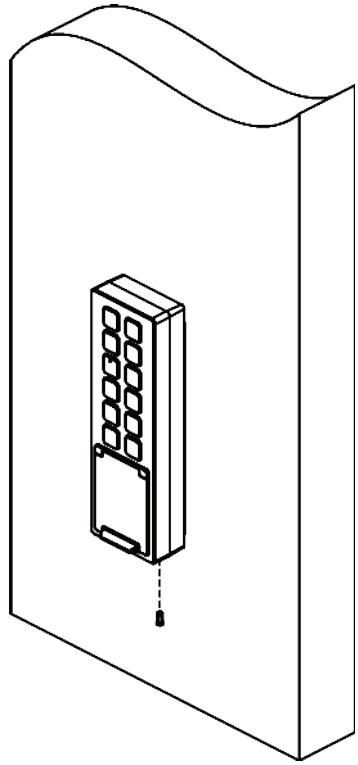


Figure 3-13 Secure Device

Chapter 4 Device Wiring

4.1 External Device Wiring

Wire the external device.

The wiring diagram is as follows.

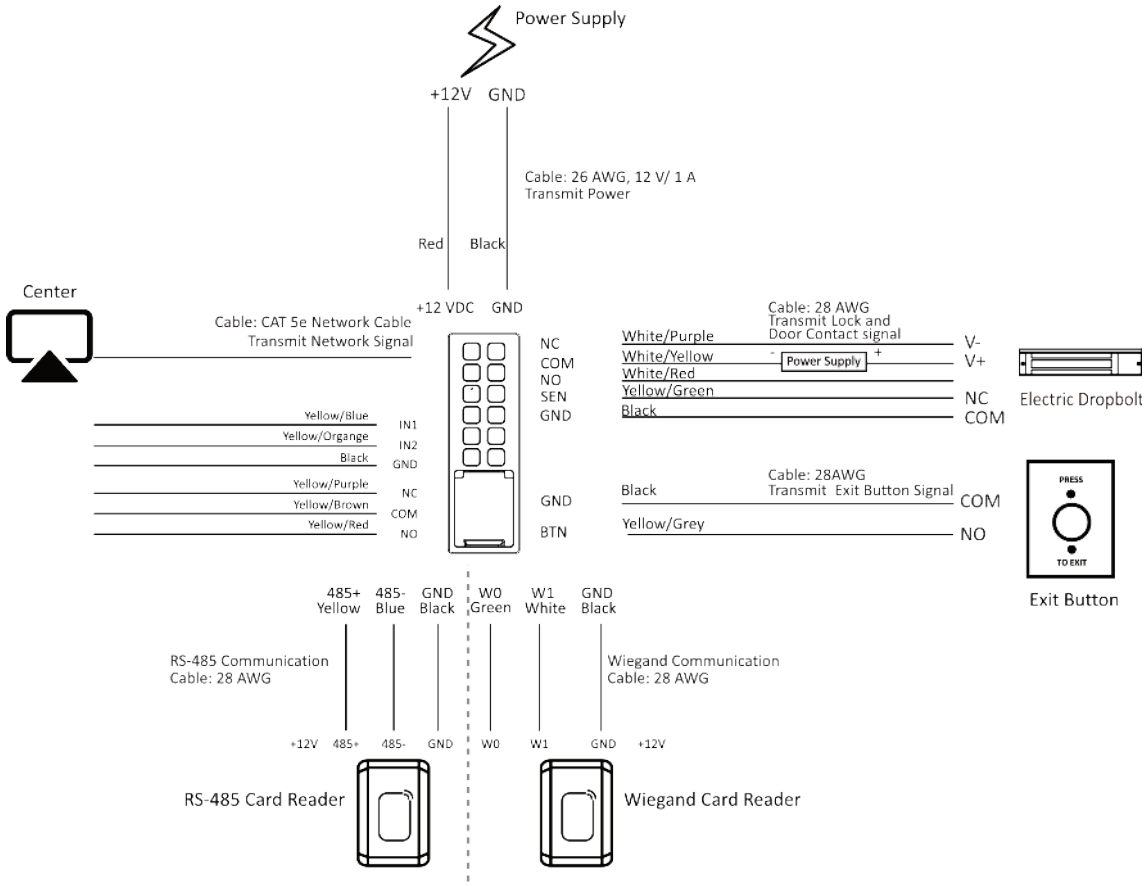


Figure 4-1 External Device Wiring

Note

- When connecting door contact and exit button, the device and the RS-485 card reader should use the same common ground connection.
- You should set the face recognition terminal's Wiegand direction as **Input** to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction as **Output** to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see ***Set Wiegand Parameters*** .
- The device and the door lock should use separate power supply.

- The suggested external power supply for door lock is 12 V, 1 A.
- The suggested external power supply for Wiegand card reader is 12 V, 1 A.
- Do not wire the device to the electric supply directly.

4.2 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

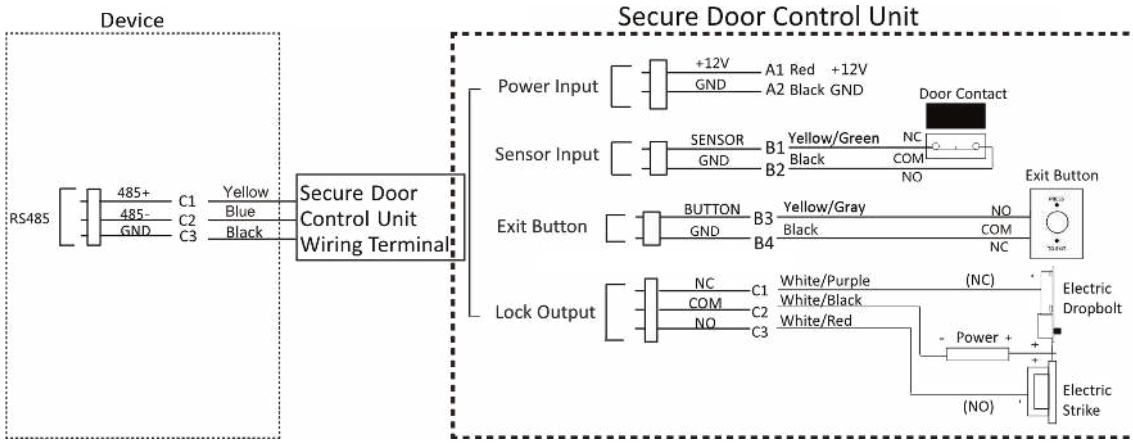


Figure 4-2 Secure Door Control Unit Wiring

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 5 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.: 80
- The default user name: admin

5.1 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 5 for 10 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. Click **Activate**.
4. Enter **Configuration → Communication Settings → Wi-Fi** and connect to a Wi-Fi. Or edit the IP address via the mobile web, PC web browser and the client software. 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*** .

5.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

   Note

   Make sure the device IP address and the computer's should be in the same IP segment.

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

   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.

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

5.3 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.

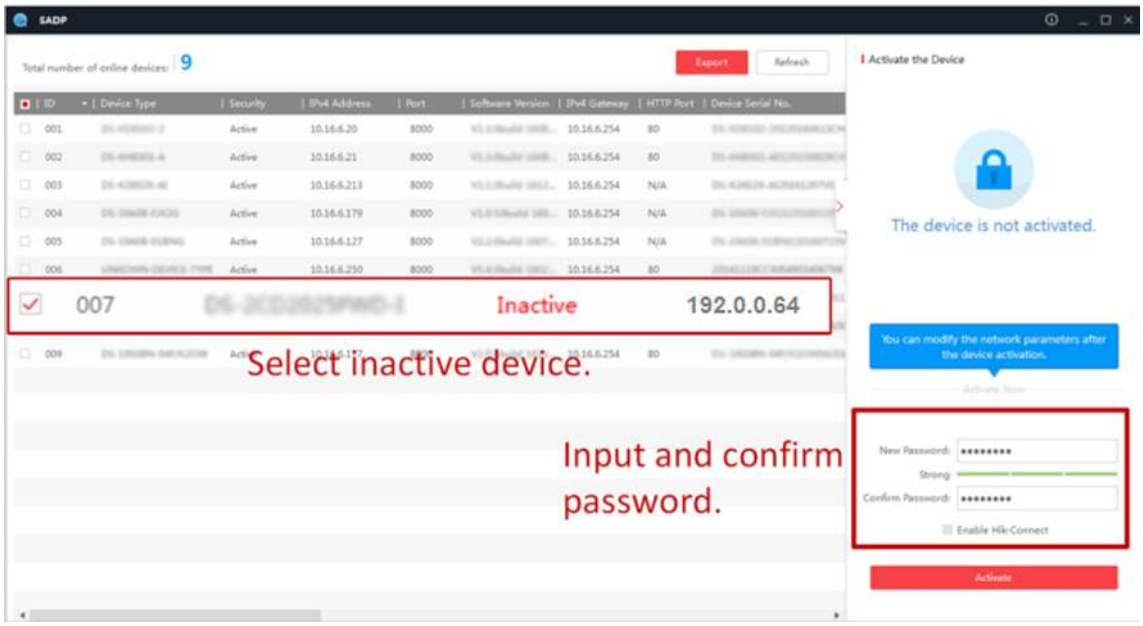
Caution

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.

5.4 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 6 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.

6.1 Authenticate via Single Credential

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

Authenticate fingerprint, or card.

Fingerprint

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

Card

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

Note

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

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

6.2 Authenticate via Multiple Credential

Before You Start

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

Steps

1. 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.

Chapter 7 Quick Operation via Web Browser

7.1 Set Security Question

If you forget the device activation password, you can change the password via security questions and E-mail. Set the security questions before configuration.

Click in the top right of the web page to enter the **Change Password** page.

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**. Or you can click **Skip** to skip the step.

7.2 Select Language

You can select a language for the device system.

Click in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.

Note

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

Click **Next** to complete the settings.

7.3 Time Settings

Click in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

Time Zone

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

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

DST

Enable DST. Set the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

7.4 Administrator Settings

Steps

1. Click in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

   Note

   You should select at least one credential.

   1) Click **Add Card** to enter the Card No. and select the property of the card.

      Note

      Up to 5 cards can be supported.

   2) Click **Add Fingerprint** to add fingerprints.

      Note

      Up to 10 fingerprints are allowed.
4. Click **Complete**.

Chapter 8 Operation via Web Browser

8.1 Login

You can login via the web browser.

Note

Make sure the device is activated. For detailed information about activation, see ***Activation*** .

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

8.2 Forget Password

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

Note

The function is supported when the PC/mobile phone is in the same network segment with the device.

On the login page, click **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.

8.3 Overview

You can view real-time event, person information, network status, basic information, and device capacity.

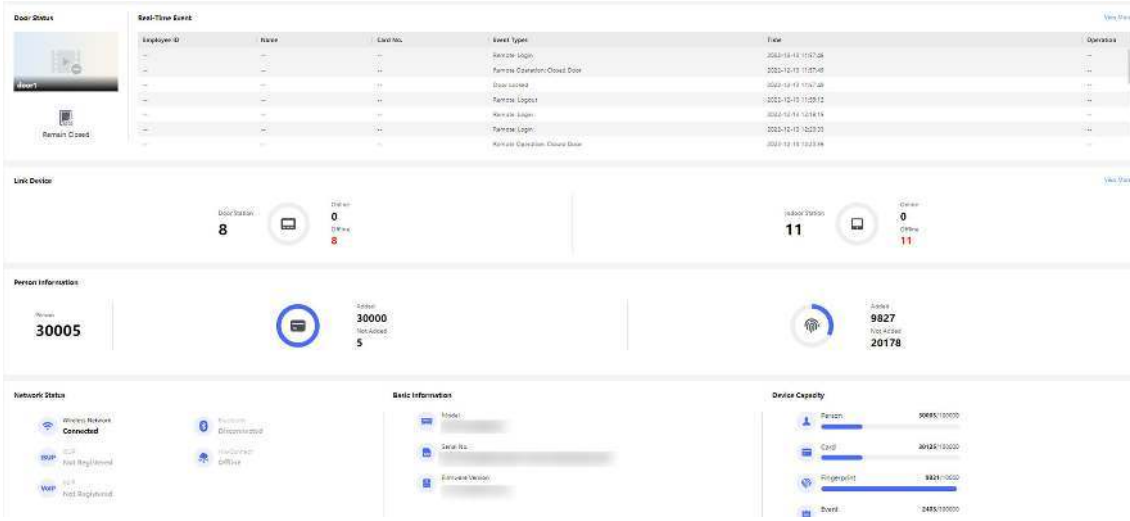


Figure 8-1 Overview Page

Function Descriptions:

Door Operation

/ / /

The door operation is open/closed/remaining open/remaining closed.

Door Status

You can click / / / , and the door status will be controlled/controlled/remaining open/remaining closed.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the start time, and the end time, and click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person, card, and fingerprint.

Network Status

You can view the connected and registered status of wired network, wireless network, bluetooth, ISUP, and cloud service.

Basic Information

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

Device Capacity

You can view the person, card, event and fingerprint capacity.

Note

Only devices supporting fingerprint function can display the fingerprint capacity.

View More

You can click **View More** to view the event details.

8.4 Person Management

Click **Add** to add the person's information, including the basic information, certificate, and authentication settings.

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.
Add the person's basic information, including the employee ID, the person's name, gender and person type.
If you select **Visitor** as the person type, you can set the visit times.
Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.
Enable **Long-Term Effective User**, or set **Validity Period** and the person can only has the permission within the configured time period according to your actual needs.
Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set the authentication type.
Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **Save** to add the card.
Click **Save** to save the settings.

Add Fingerprint

Note

Only devices supporting the fingerprint function can add the fingerprint.

Click **Person Management → Add** to enter the Add Person page.
Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.

Click **Save** to save the settings.

8.5 Search Event

Click **Event Search** to enter the Search page.

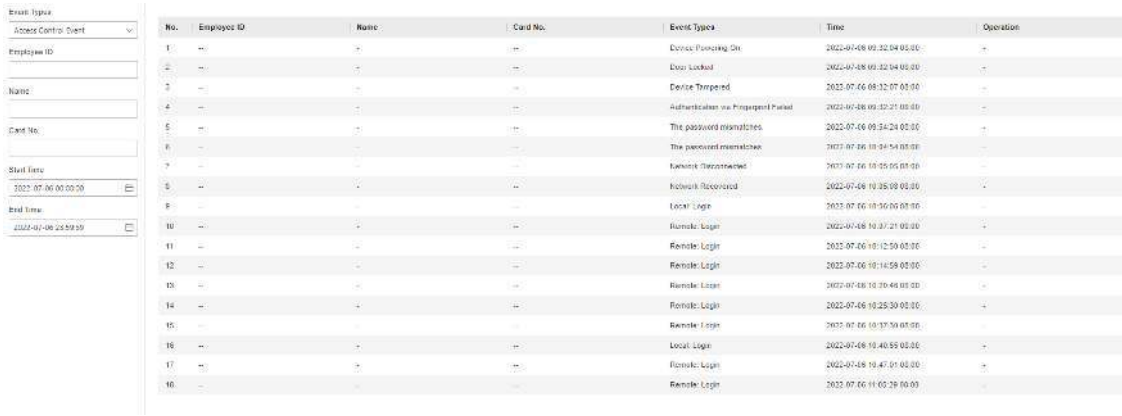


Figure 8-2 Search Event

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

The results will be displayed on the right panel.

8.6 Configuration

8.6.1 View Device Information

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

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

You can view the device name, language, model, serial No., version, IO input number, IO output number, local RS-485, number of alarm input, number of alarm output, device capacity, etc.

8.6.2 Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **Configuration → System → System Settings → Time Settings** .

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

Time Zone

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

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

8.6.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.6.4 Change Administrator's Password

Steps

1. Click **Configuration → User Management** .
2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **OK**.

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.

8.6.5 Account Security Settings

You can change the security questions and answers, or the email address for the device. After change the settings, once you forgot the device password, you should answer the new questions or use the new email address to reset the device password.

Steps

1. Click **Configuration → System → User Management → Account Security Settings** .
2. Change the security questions or email address according your actual needs.
3. Enter the device password and click **OK** to confirm changing.

8.6.6 Online Users

The information of users logging into the device is shown.

Go to **Configuration → User Management → Online Users** to view the list of online users.

8.6.7 View Device Arming/Disarming Information

View device arming type and arming IP address.

Go to **Configuration → User Management → Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

8.6.8 Network Settings

Set TCP/IP, port, Wi-Fi parameters, device hotspot, bluetooth, ISUP, and platform access.

Note

Some device models do not support Wi-Fi or mobile data settings. Refer to the actual products when configuration.

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Auto**.

DHCP

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

If you check 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. Click **Configuration → Network → Network Settings → Wi-Fi** .

Figure 8-3 Wi-Fi Settings Page

2. Check **Wi-Fi**.
3. Add Wi-Fi.
   - Click **Manual Add**, and enter **SSID** and **Security Mode**.
4. Select a Wi-Fi
   - Click **Connect** of a Wi-Fi in the list and enter the Wi-Fi password.
   - Click **Manual Add**, and enter **SSID** and **Security Mode**. Click **OK**.
5. **Optional:** Set the WLAN parameters.

1) Set the IP address, subnet mask, and default gateway. Or enable **DHCP** and the system will allocate the IP address, subnet mask, and default gateway automatically.

6. Click **Save**.

Device Hotspot

Set the device hotspot.

Click **Configuration → Network → Network Settings → Device Hotspot** .

Click **Enable Device Hotspot** to enable the function and view the device hotspot name.

Note

By default, the hotspot name is the AP_Device Serial No.

Click **Save**.

Bluetooth Settings

You can enable bluetooth function.

Click **Configuration → Network → Network Settings → Bluetooth** .

Open

Enable **Open** to enable the bluetooth function.

Device Name

You can edit the device name connected to the bluetooth.

Connection Status

You can view the connection status.

Open Door via Bluetooth

After enabling this function, you can open doors via or HikCentral Access Control (HCAC).

Note

You should add devices to the HCAC before opening door via bluetooth. Via HCAC, you can also realize the auto door open function. for details, scan the QR code to view HCAC's user manual.

Set Port Parameters

Set the HTTP, HTTPS, HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .

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.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

Platform Access

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

Steps

1. Click **Configuration → Network → 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. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the verification code.
5. Click **View** to view device QR code. Scan the QR code to bind the account.

   Note

   8 to 32 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.

6. Click **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. Click **Configuration → Network → Device Access → ISUP** .
2. Check **Enable**.
3. Set the ISUP version, server address, device ID, and the ISUP status.

   Note

   If you select 5.0 as the version, you should set the encryption key as well.
4. Set the ISUP listening parameters, including ISUP alarm center IP address/domain name, ISUP alarm center URL, and ISUP alarm center port.
5. Click **Save**.

8.6.9 Event Linkage

Set linked actions for events.

Steps

1. Click **Configuration → Event → Event Detection → Linkage Settings** to enter the page.
2. Set event source.
   - If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.
   - If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
   - If you choose **Linkage Type** as **Employee ID Linkage**, you need to enter the employee ID and select the card reader.
3. Set linked action.

   Buzzer Linkage

   Enable **Buzzer Linkage**, and check **Start Buzzing** or **Stop Buzzing**.

   Door Linkage

   Enable **Linked Door**, check **Door 1** or **Door 2**, and set the door status for the target event.

   Linked Alarm Output

   Enable **Linked Alarm Output**, check **Alarm Output 1** or **Alarm Output 2**, and set the alarm output status for the target event.

Note

Equip the device with an SD card to use video recording function. To view the recorded videos, see ***Search Event*** .

8.6.10 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

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

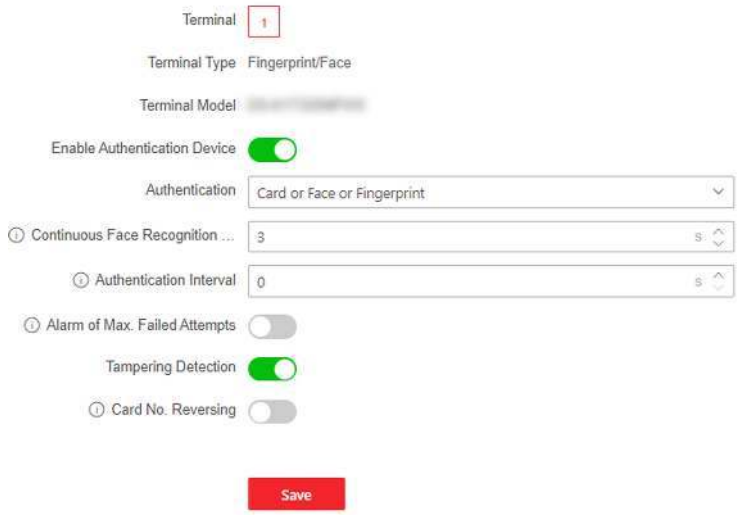


Figure 8-4 Set Authentication Parameters

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

Terminal

Select terminal for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

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.

Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

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.

OK LED Polarity/Error LED Polarity

Set OK LED Polarity/Error LED Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .

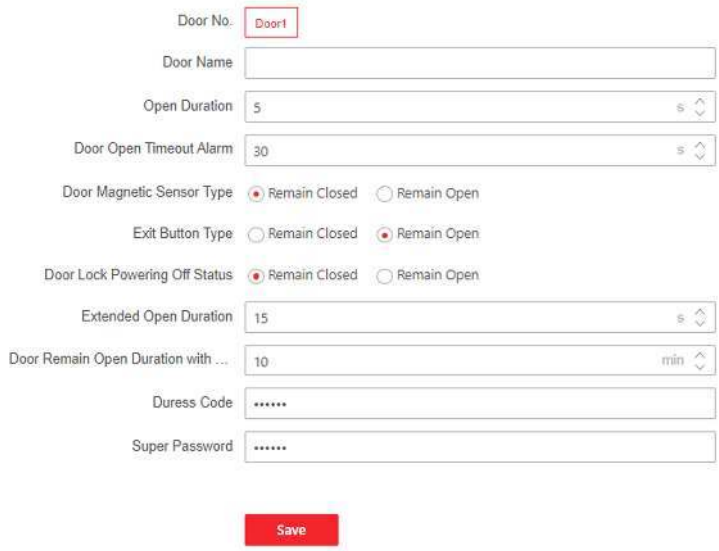


Figure 8-5 Door Parameters Settings Page

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

Door No.

Select the device corresponded door No.

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.

Door Open Timeout Alarm

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

Door Contact

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

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 Lock Powering Off Status

You can set the door lock status when the door lock is powering off. By default, it is **Remain Closed**.

Extended Open Duration

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

Door Remain Open Duration with First Person

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.

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.

Set RS-485 Parameters

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

Click **Configuration → Access Control → RS-485 Settings** .

Check **Enable RS-485**, and set the parameters.

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

No.

Set the RS-485 No.

Peripheral Type

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

Note

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

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.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **Configuration → Access Control → Wiegand Settings** .
2. Check **Wiegand** to enable the Wiegand function.
3. Set a transmission direction.

   Input

   The device can connect a Wiegand card reader.

   Output

   The can connect an external access controller. And the two devices will transmit the card No. via Wiegand 26 or 34.
4. Drag the block to set the time interval and pulse width.

   Note

   - The time interval ranges from 1 ms to 20 ms.
   - The pulse width ranges from 1 us to 100 us.
5. Click **Save** to save the settings.

   Note

   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Set Terminal Parameters

You can set terminal parameters for accessing.

Click **Configuration → Access Control → Terminal Parameters** .

You can set **Working Mode** as **Access Control Mode**. The access control mode is the device normal mode. You should authenticate your credential for accessing.

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

8.6.11 Card Settings

Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable DESFire Card

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

Set Card No. Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Configuration → Card Settings → Card No. Authentication Settings** .

Select a card authentication mode and click **Save**.

Full Card No.

All card No. will be read.

Wiegand 26 (3 bytes)

The device will read card via Wiegand 26 protocol (read 3 bytes).

Wiegand 34 (4 bytes)

The device will read card via Wiegand 34 protocol (read 4 bytes).

8.6.12 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**.

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.

8.6.13 Set Smart Parameters

Set Basic Parameters

Click **Configuration → Smart → Smart** .
Select **Fingerprint Security Level** according to your actual needs.

8.6.14 Upgrade and Maintenance

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

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .
Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .
Select an upgrade type from the drop-down list. Click and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.
If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.

Note

- Do not power off during the upgrading.
- You can click **Check for Updates** to check the newer version.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

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

Restore

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

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click and select the file to import. Click **Import** to start import configuration file.

8.6.15 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

8.6.16 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

8.6.17 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **Maintenance and Security → Security → Security Service** .

Select a security mode, and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

8.6.18 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.

2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Install**.

Chapter 9 Configure the Device via the Mobile Browser

9.1 Login

Login the mobile browser to configure.

Note

- Parts of the models supports Wi-Fi settings.
- Make sure the device is activated.
- Make sure the device and the mobile phone are in the same IP segment.

Connect the mobile phone to the Wi-Fi the same as the device's.

Enter the device IP address in the address bar of the mobile browser and press **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. (The function should be supported by the device with Wi-Fi function.)

9.2 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.

9.3 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.

9.4 Configuration

9.4.1 View Device Information

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

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

You can view the device name, language, model, serial No., version, number of channels, IO input number, local RS-485 number, number of alarm input and output, Mac address, and device capacity, etc.

9.4.2 Time Settings

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

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

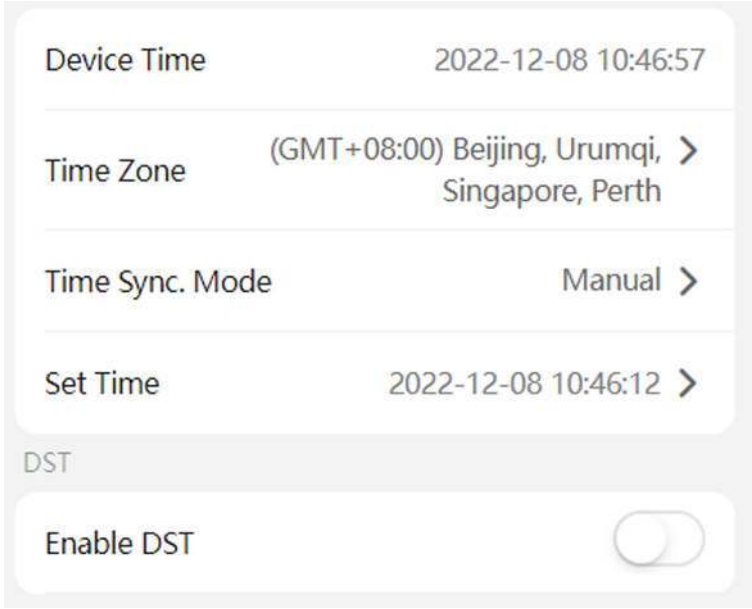


Figure 9-1 Time Settings

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.

9.4.3 Set DST

Steps

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

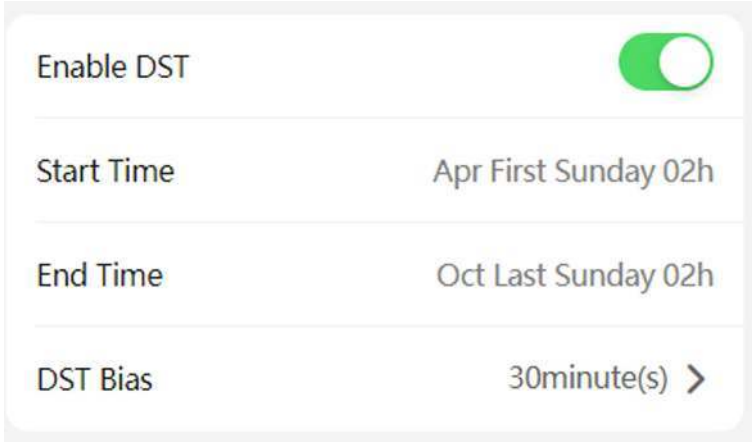


Figure 9-2 DST

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

9.4.4 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.

9.4.5 Network Settings

You can set the wired network, Wi-Fi parameters and device port.

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**.

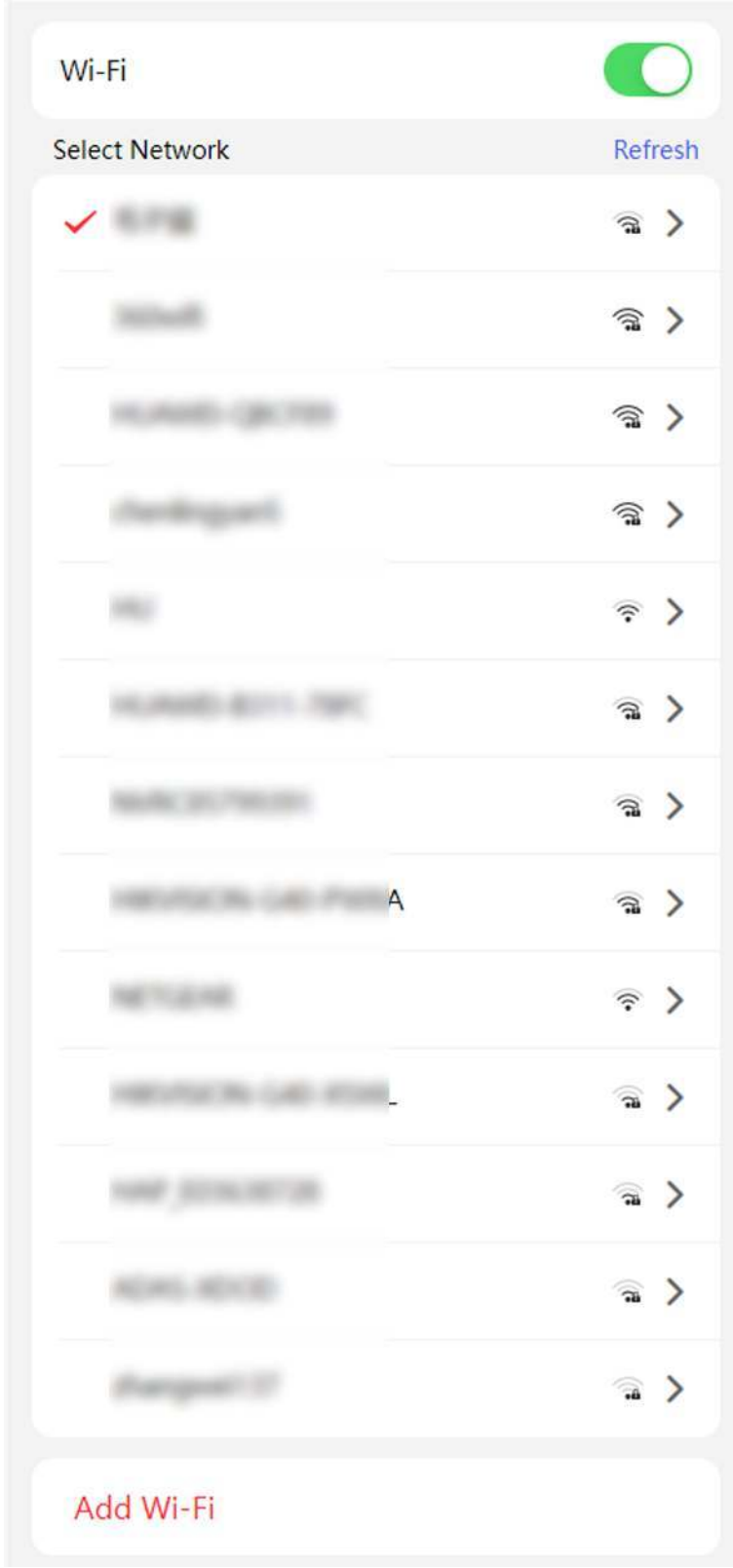


Figure 9-3 Wi-Fi

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

9.4.6 User Management

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

Steps

1. Tap ≡ → **Person Management** to enter the settings page.
2. Add user.
   1) Tap**+**.

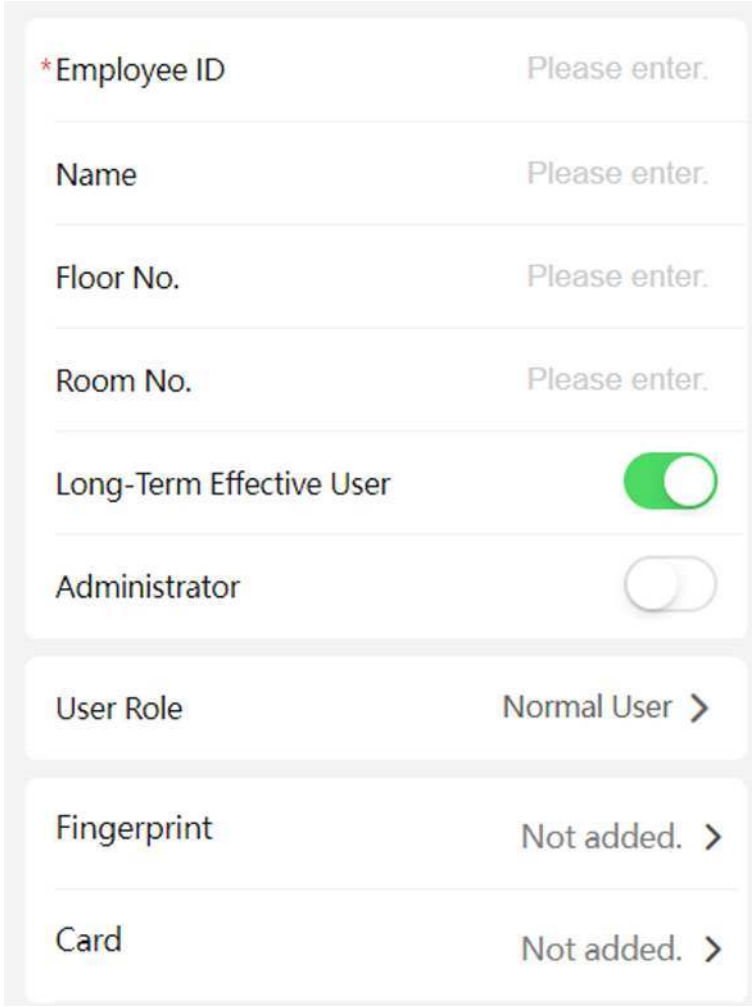


Figure 9-4 Add User

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 User

Set the user permission as long-term effective.

Start Date/End Date

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

Administrator

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

User Role

Select your user 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.

3) Tap **Save**.

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

9.4.7 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.

9.4.8 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

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

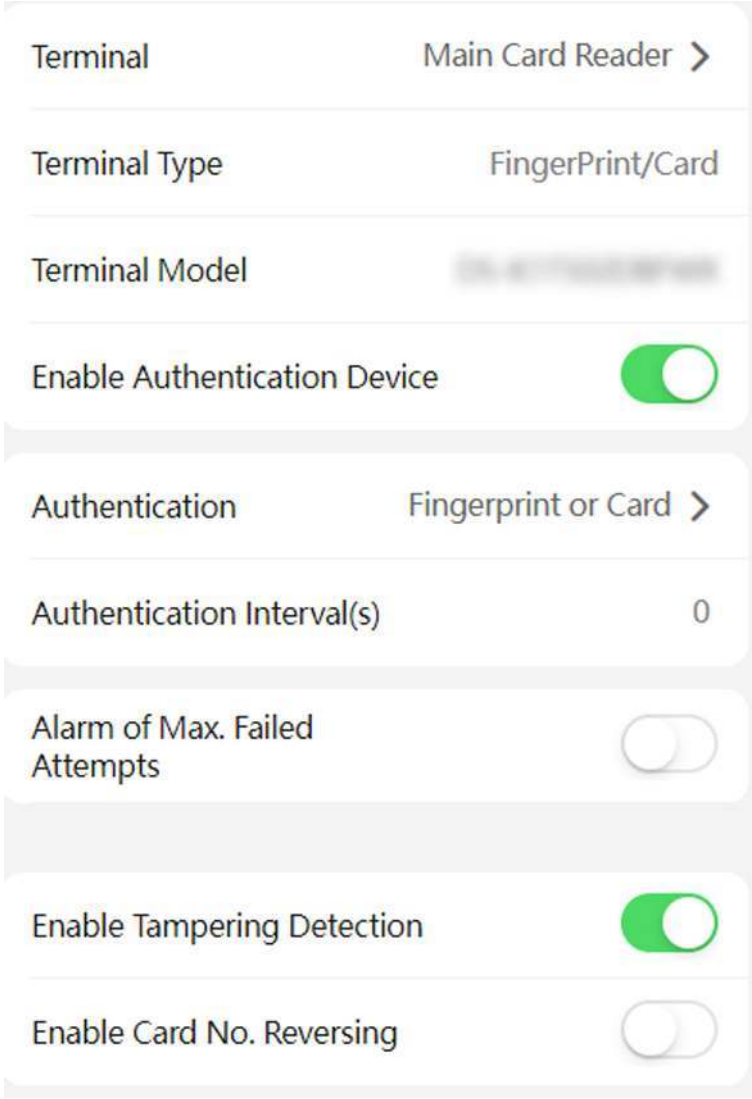


Figure 9-5 Authentication Settings

2. Tap **Save**.

Terminal

Select terminal for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

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.

Max. Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts

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

Enable Tampering Detection

Enable the anti-tamper detection for the card reader.

Enable Card No. Reversing

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

Communication with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

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.

OK LED Polarity/Error LED Polarity

Set OK LED Polarity/Error LED Polarity of the access control device according to the card reader parameters. Generally, adopts the default settings.

Set Door Parameters

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

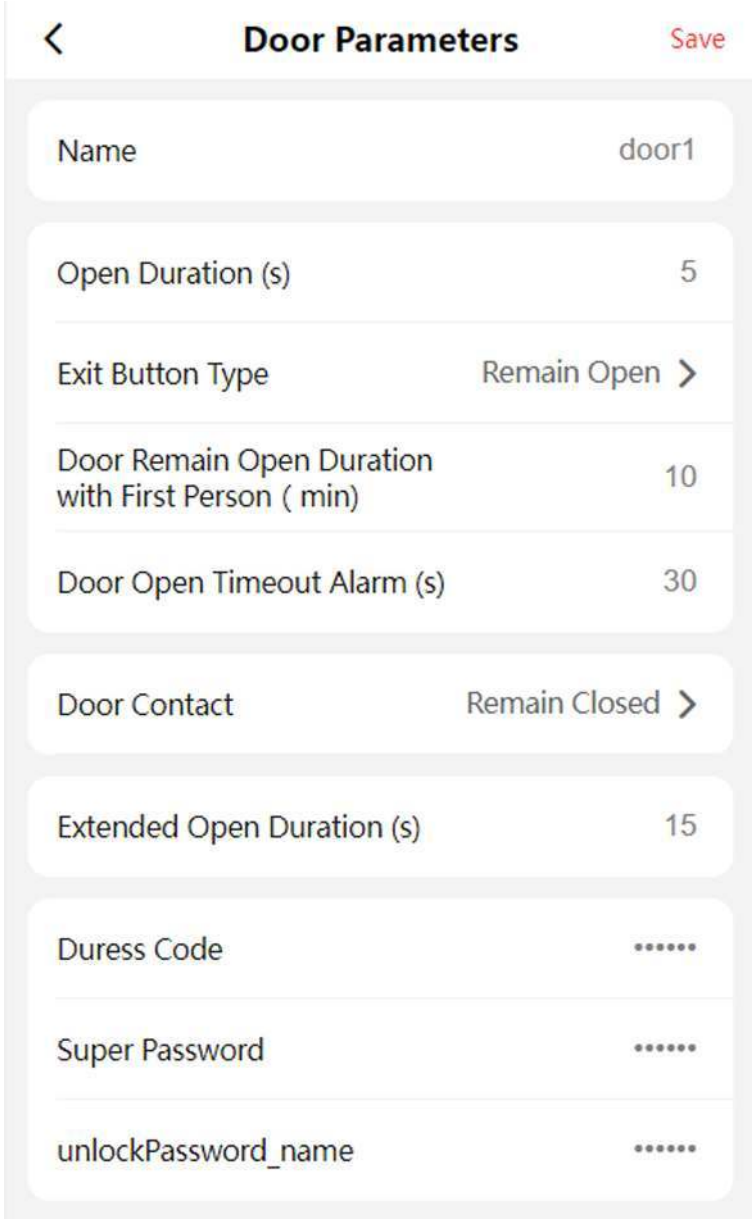


Figure 9-6 Door Parameters Settings Page

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

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 Remain 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 Open Timeout Alarm

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

Door Contact

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

Extended Open Duration

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.

Unlock Password

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

Note

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

Terminal Parameters

You can set terminal parameters for accessing.

Tap → **Access Control** → **Terminal Parameters** .

You can set **Working Mode** as **Access Control Mode**. The access control mode is the device normal mode. You should authenticate your credential for accessing.

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

Set Card Security

Tap → **Access Control** → **Card Security** to enter the configuration page.

Set the parameters and tap **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can enable NFC card to increase the security level of the data.

Enable M1 Card

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

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

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.

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.

Output Type

Set the output type according to your actual needs.

9.4.9 Fingerprint Parameters Settings

Set fingerprint security level.

Tap → **Smart** .

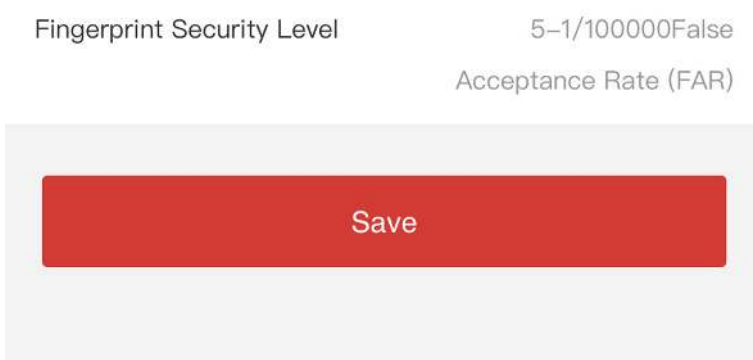


Figure 9-7 Fingerprint Security Level

Note

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

Select the security level according to actual needs. Tap **Save** to save the settings.

9.4.10 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.

9.4.11 View Online Document

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

9.4.12 View Open Source Software License

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

Chapter 10 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.

https://pinfo.hikvision.com/hkwsen/unzip/20230109110406_14606_doc/UD31348B_iVMS-4200%20AC%20Client_User%20Manual_V1.9.0_PDF1-TEST_en-US_20221226.PDF

HikCentral Access Control (HCAC)

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

https://pinfo.hikvision.com/hkwsen/unzip/20230207191241_72415_doc/index.html

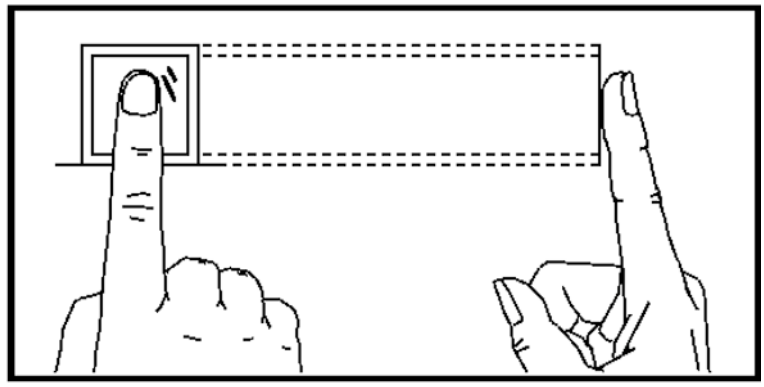
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

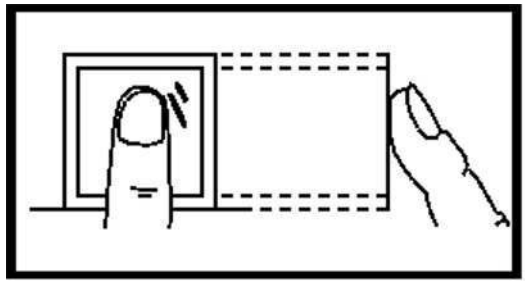
The figure displayed below is the correct way to scan your finger:



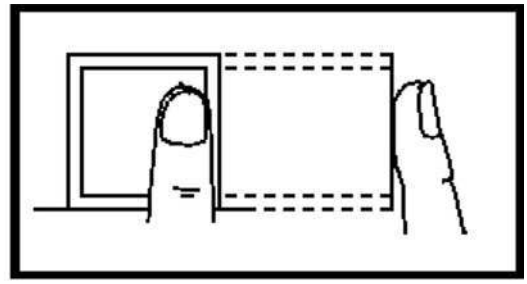
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

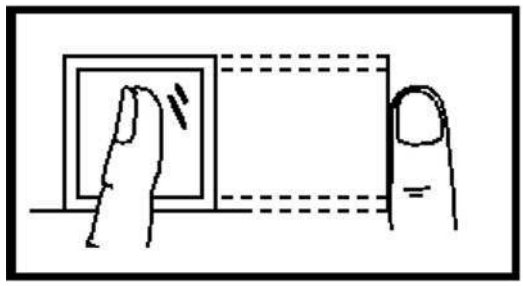
The figures of scanning fingerprint displayed below are incorrect:



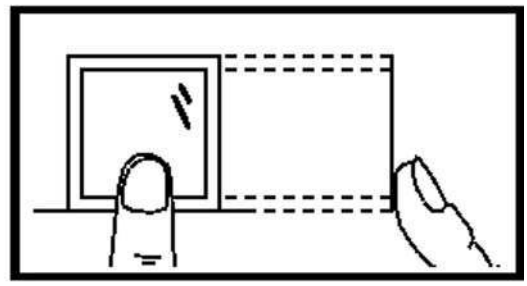
Vertical



Edge I



Side



Edge II

Environment

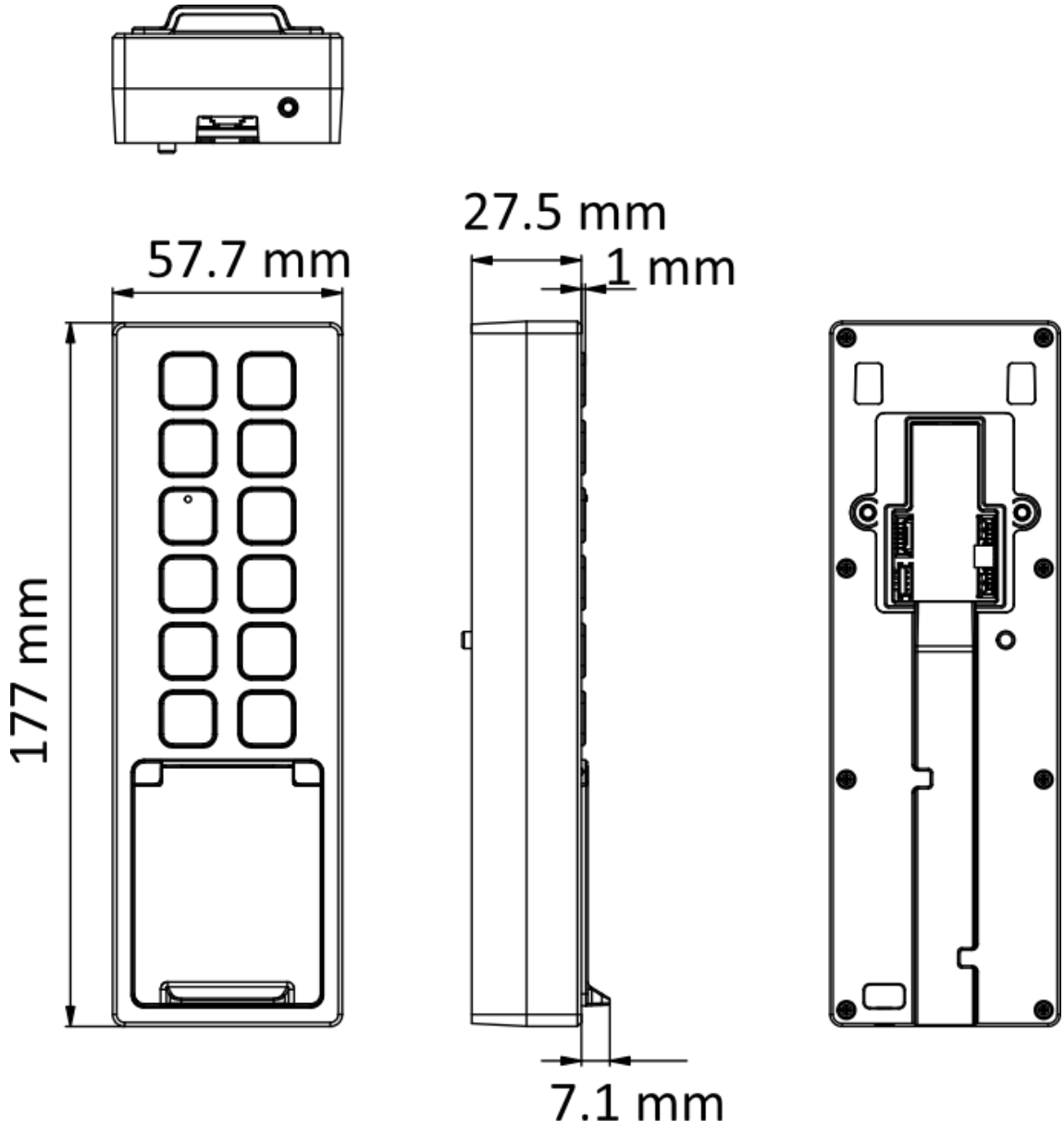
The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

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

Dimension of Device (Fingerprint + Card Series)



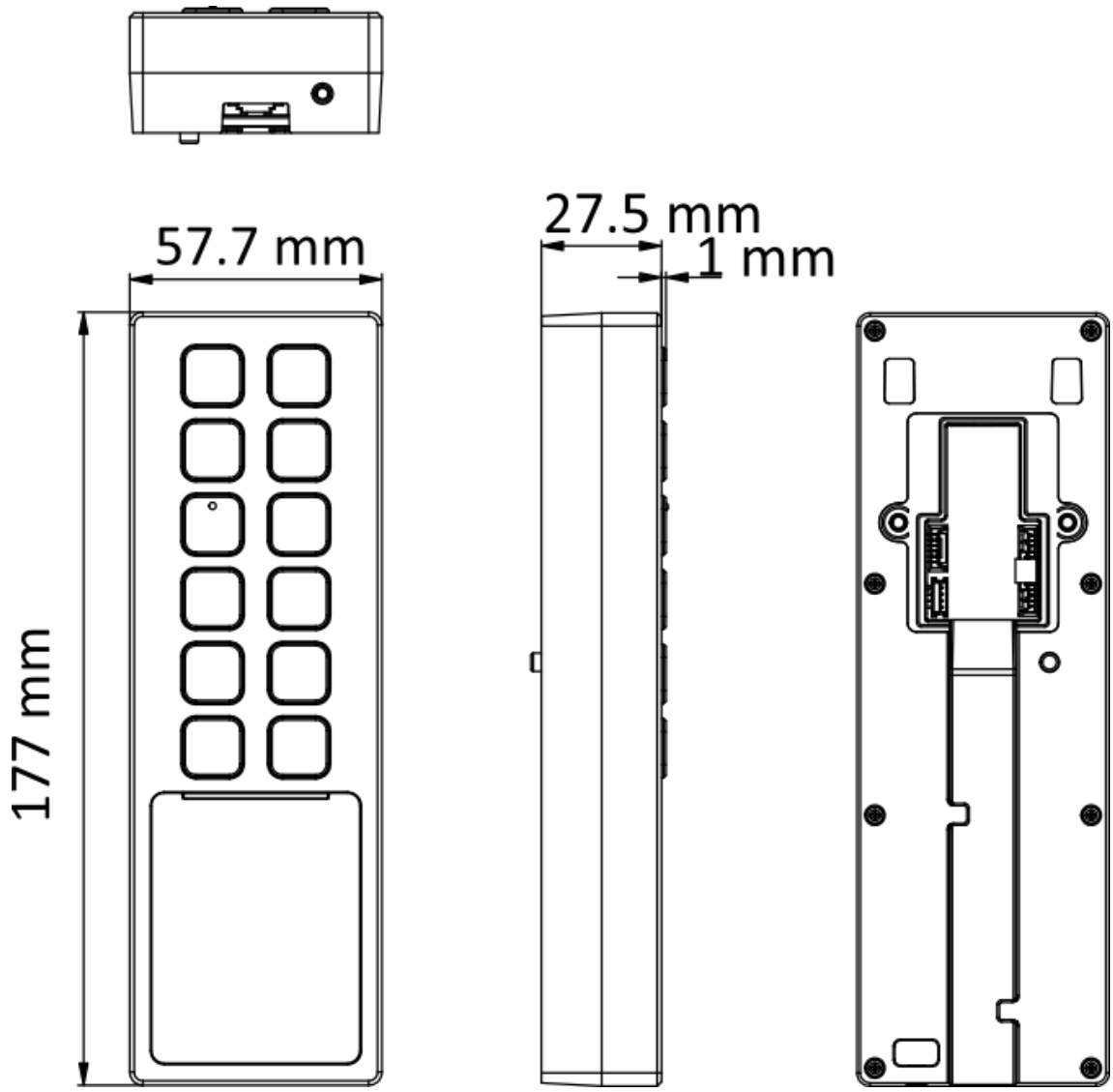


Figure B-1 Dimension of Device (Card Series)

Note

The pictures here are for reference only.

See Far, Go Further