



Access Control Terminal

User Manual

Legal Information

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

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

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

Trademarks

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-K1T502DBWX-C	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G,Bluetooth
	DS-K1T502DBFWX-C	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G,Bluetooth
	DS-K1T502DBFWX	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G,Bluetooth
	DS-K1T502DBWX	13.56 MHz Card Presenting Frequency, Wi-Fi, 2.4G,Bluetooth

Table 1-1 Available Mobile Web Browsers

Operation System	Browser	Version	Available
Android	Xiaomi 12, default browser	16.6.6	Yes
	Huawei P30, default browser	12.1.1.321	Yes
	Xiaomi 5s plus, default browser	14.2.22	Yes
	Huawei P30 Pro, default browser	12.1.2.301	Yes
	Redmi k40, default browser	16.5.12	Yes
IOS	Safari	15.4	Yes

Contents

Chapter 1 Overview	1
1.1 Overview	1
1.2 Features	1
1.2.1 Appearance Description	1
Chapter 2 Installation	4
2.1 Installation Environment	4
2.2 Install without Gang Box	4
Chapter 3 Device Wiring	8
3.1 Terminal Description	8
3.2 External Device Wiring	9
3.3 Wire Secure Door Control Unit	10
Chapter 4 Activation	12
4.1 Activate via Mobile Web	12
4.2 Activate via Web Browser	13
4.3 Activate via SADP	13
4.4 Activate Device via iVMS-4200 Client Software	14
Chapter 5 Identity Authentication	16
5.1 Authenticate via Single Credential	16
5.2 Authenticate via Multiple Credential	16
Chapter 6 Call and Video Intercom	18
Chapter 7 Quick Operation via Web Browser	19
7.1 Set Security Question	19
7.2 Select Language	19
7.3 Time Settings	19
7.4 Privacy Settings	20
7.5 Administrator Settings	20

7.6 No. and System Network	20
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	26
8.6.1 Set Local Parameters	26
8.6.2 View Device Information	26
8.6.3 Set Time	26
8.6.4 Set DST	27
8.6.5 Change Administrator's Password	27
8.6.6 Account Security Settings	28
8.6.7 Online Users	28
8.6.8 View Device Arming/Disarming Information	28
8.6.9 Network Settings	28
8.6.10 Set Audio Parameters	33
8.6.11 Set Image Parameters	34
8.6.12 Access Control Settings	34
8.6.13 Video Intercom Settings	38
8.6.14 Card Settings	41
8.6.15 Set Privacy Parameters	42
8.6.16 Time and Attendance Settings	43
8.6.17 Set Smart Parameters	45
8.6.18 Set Preference	45
8.6.19 Upgrade and Maintenance	46
8.6.20 Device Debugging	47

8.6.21 Log Query	47
8.6.22 Security Mode Settings	47
8.6.23 Certificate Management	48
Chapter 9 Configure the Device via the Mobile Browser	50
9.1 Login	50
9.2 Overview	50
9.3 Forget Password	51
9.4 Configuration	51
9.4.1 View Device Information	51
9.4.2 Time Settings	51
9.4.3 Set DST	52
9.4.4 User Management	53
9.4.5 Network Settings	53
9.4.6 User Management	57
9.4.7 Set Audio	59
9.4.8 Search Event	59
9.4.9 Access Control Settings	59
9.4.10 Intercom	65
9.4.11 Fingerprint Parameters Settings	68
9.4.12 Upgrade and Maintenance	68
9.4.13 View Online Document	69
9.4.14 View Open Source Software License	69
Chapter 10 Client Software Configuration	70
10.1 Configuration Flow of Client Software	70
10.2 Device Management	71
10.2.1 Add Device	71
10.2.2 Reset Device Password	73
10.2.3 Manage Added Devices	74

10.3 Group Management	75
10.3.1 Add Group	75
10.3.2 Import Resources to Group	75
10.4 Person Management	76
10.4.1 Add Organization	76
10.4.2 Configure Basic Information	76
10.4.3 Issue a Card by Local Mode	78
10.4.4 Collect Fingerprint via Client	80
10.4.5 Collect Fingerprint via Access Control Device	81
10.4.6 Configure Access Control Information	82
10.4.7 Customize Person Information	83
10.4.8 Configure Additional Information	84
10.4.9 Import and Export Person Identify Information	84
10.4.10 Import Person Information	84
10.4.11 Export Person Information	85
10.4.12 Get Person Information from Access Control Device	85
10.4.13 Move Persons to Another Organization	86
10.4.14 Issue Cards to Persons in Batch	87
10.4.15 Report Card Loss	87
10.4.16 Set Card Issuing Parameters	88
10.5 Configure Schedule and Template	88
10.5.1 Add Holiday	89
10.5.2 Add Template	90
10.6 Set Access Group to Assign Access Authorization to Persons	91
10.7 Configure Advanced Functions	93
10.7.1 Configure Device Parameters	93
10.7.2 Configure Remaining Unlocked/Locked	98
10.7.3 Configure Custom Wiegand Rule	100

10.7.4 Configure Card Reader Authentication Mode and Schedule	101
10.7.5 Configure Device Parameters	103
10.8 Configure Linkage Actions for Access Control	106
10.8.1 Configure Client Actions for Access Event	107
10.8.2 Configure Device Actions for Access Event	108
10.8.3 Configure Device Actions for Card Swiping	108
10.8.4 Configure Device Actions for Person ID	109
10.9 Door Control	110
10.9.1 Control Door Status	110
10.9.2 Check Real-Time Access Records	111
Appendix A. Tips for Scanning Fingerprint	112
Appendix B. Dimension	114
Appendix C. Communication Matrix and Device Command	115

Chapter 1 Overview

1.1 Overview

Access control terminal is a kind of access control terminal for authentication. It supports two-way audio, remote live view, picture capture, video recording through NVR, and so on.

1.2 Features

- Manage access control, video intercoms, and video security with one device
- IP65 & IK09 protections, as well as increased stability with zinc alloy materials
- Multiple authentication methods, including fingerprint, card, etc.

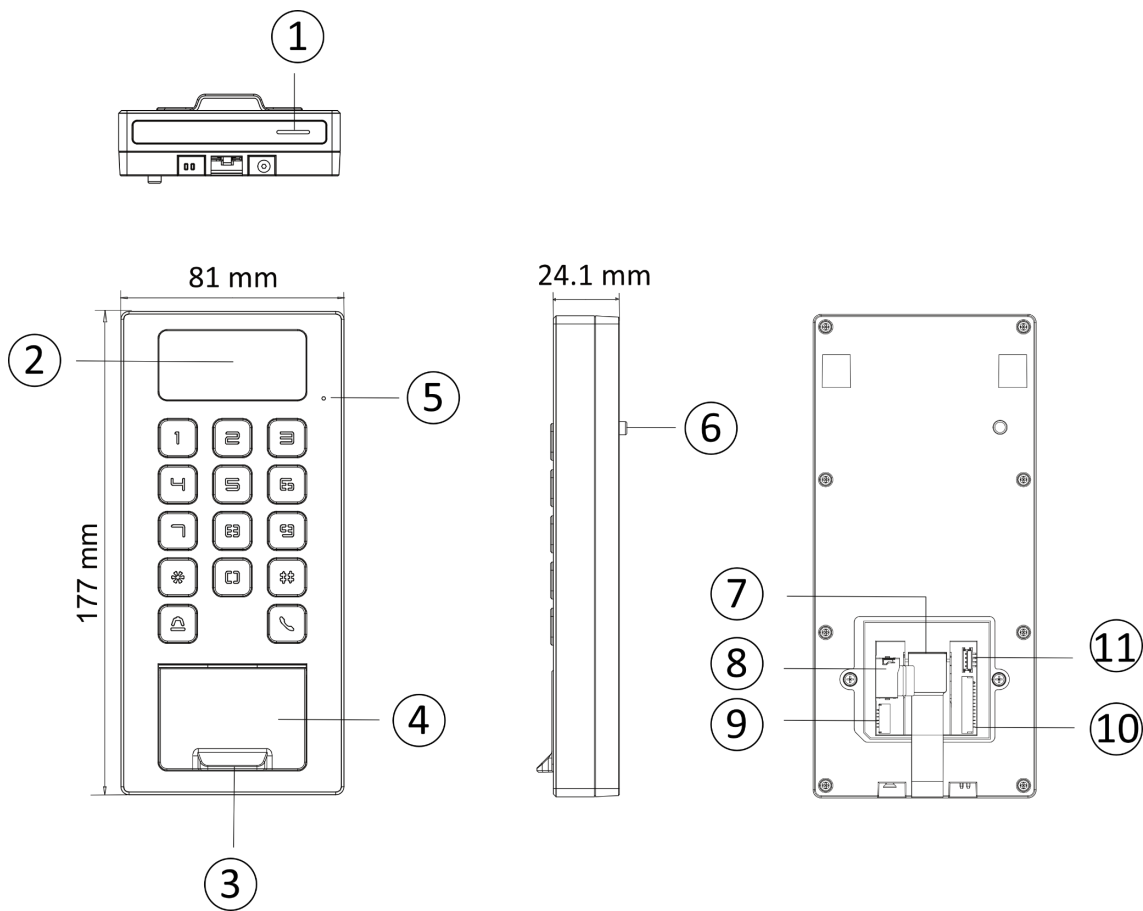


Fingerprint function is supported by parts of the device modules.

- Remote control via the Hik-Connect mobile app
- Connects to external access controller via Wiegand protocol
- Two-way audio via SIP 2.0 protocol
- RS-485 communication for connecting external card reader
- Supports network connection via AP
- Supports H.265 video encoding format

1.2.1 Appearance Description

View the device appearance description.



Note

The pictures here are for reference only.

Table 1-1 Appearance Description

No.	Description
1	Camera (Supported by parts of Device Models)
2	Fingerprint Module (Supported by parts of Device Models)
3	Card Presenting Area
4	MIC
5	Loudspeaker
6	Tamper
7	Network Interface
8	SD Card Slot
9	Wiring Terminal for Alarm Input/ Output

Access Control Terminal User Manual

No.	Description
10	Wiring Terminal
11	Debugging Port (For debugging only)

Chapter 2 Installation

2.1 Installation Environment

- Install the device at least 2 meters away from the light, and at least 3 meters away from the window or the door.
- Make sure the environment illumination is more than 100 Lux.



For details about installation environment, see *Tips for Installation Environment*.

2.2 Install without Gang Box

Steps



The additional force shall be equal to three times the weight of the equipment. The equipment and 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. Secure the mounting plate on the wall with 4 supplied screws (SC-KA4X25-SUS).

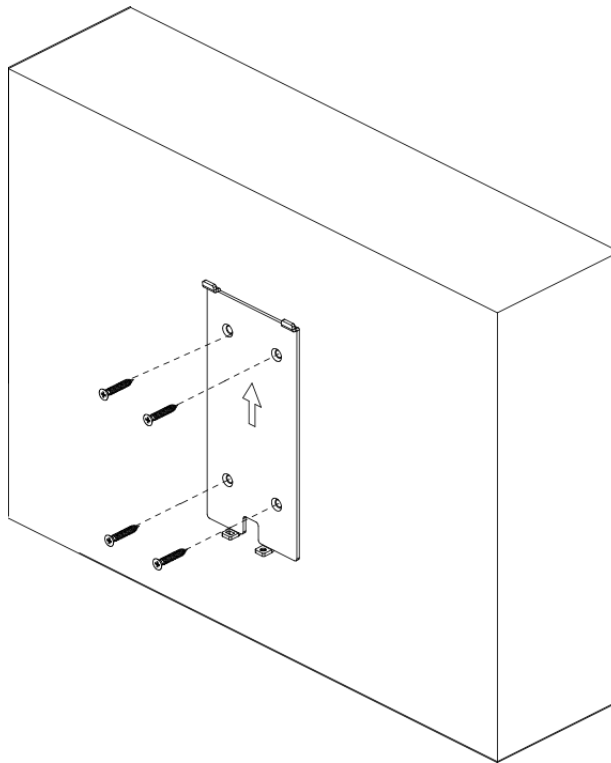
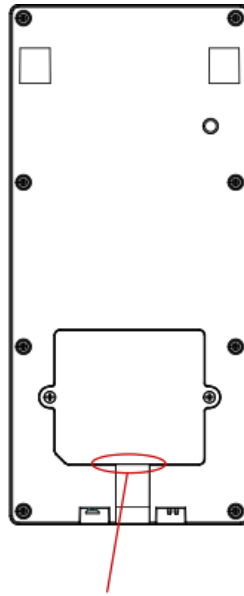


Figure 2-1 Secure Mounting Plate

2. Route the cable through the cable hole of the mounting plate, and connect to corresponding external devices' cables.
3. Apply Silicone sealant among the joints between the device rear panel and the wall (except the lower side) to keep the raindrop from entering.



Apply
Silicone
Sealant

Figure 2-2 Apply Silicone Sealant on the Side

4. Align the device with the mounting plate, and secure the device on the mounting plate with 1 supplied screw (SC-KM3X6-T10-SUS).

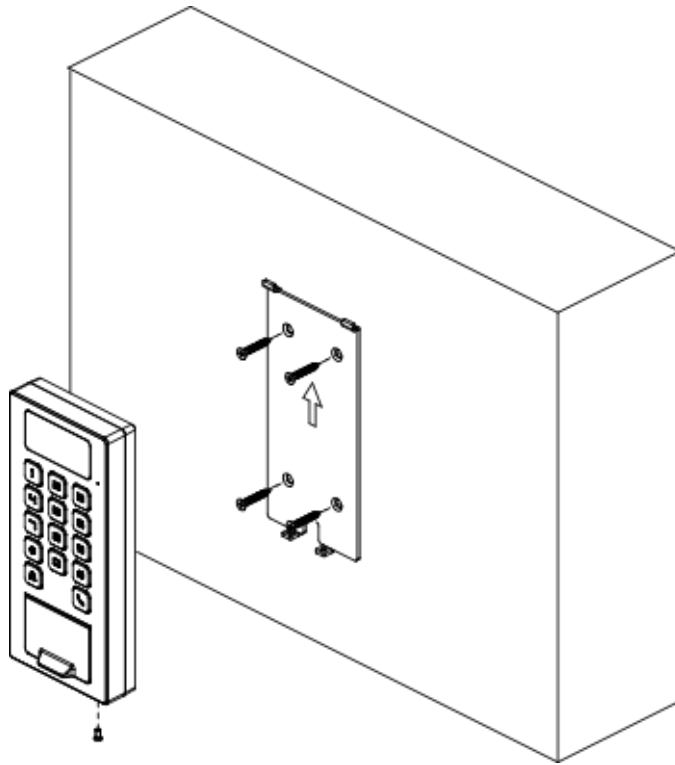


Figure 2-3 Secure Device

Chapter 3 Device Wiring

3.1 Terminal Description

The terminals contains power input, alarm input, alarm output, RS-485, Wiegand output, and door lock.

The terminal's diagram is as follows:

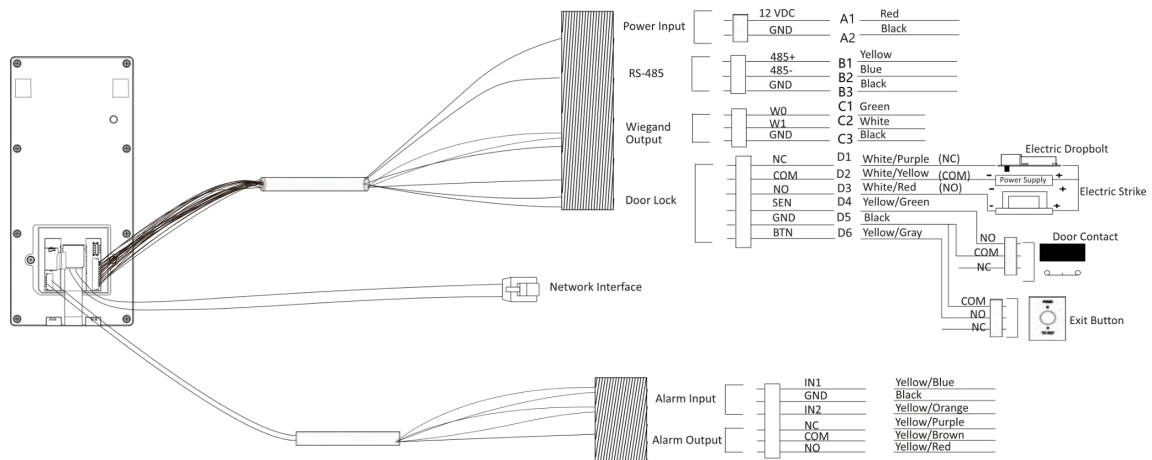


Figure 3-1 Terminal Diagram

The descriptions of the terminals are as follows:

Table 3-1 Terminal Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	Ground
Group B	B1	RS-485	Yellow	485+	RS-485 Wiring
	B2		Blue	485-	
	B3		Black	GND	Ground
Group C	C1	Wiegand	Green	W0	Wiegand Wiring 0
	C2		White	W1	Wiegand Wiring 1
	C3		Black	GND	Ground

Group	No.	Function	Color	Name	Description
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Common
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Contact
	D5		Black	GND	Ground
	D6		Yellow/Gray	BTN	Exit Door Wiring

3.2 External Device Wiring

Wire the external device.

The wiring diagram is as follows.

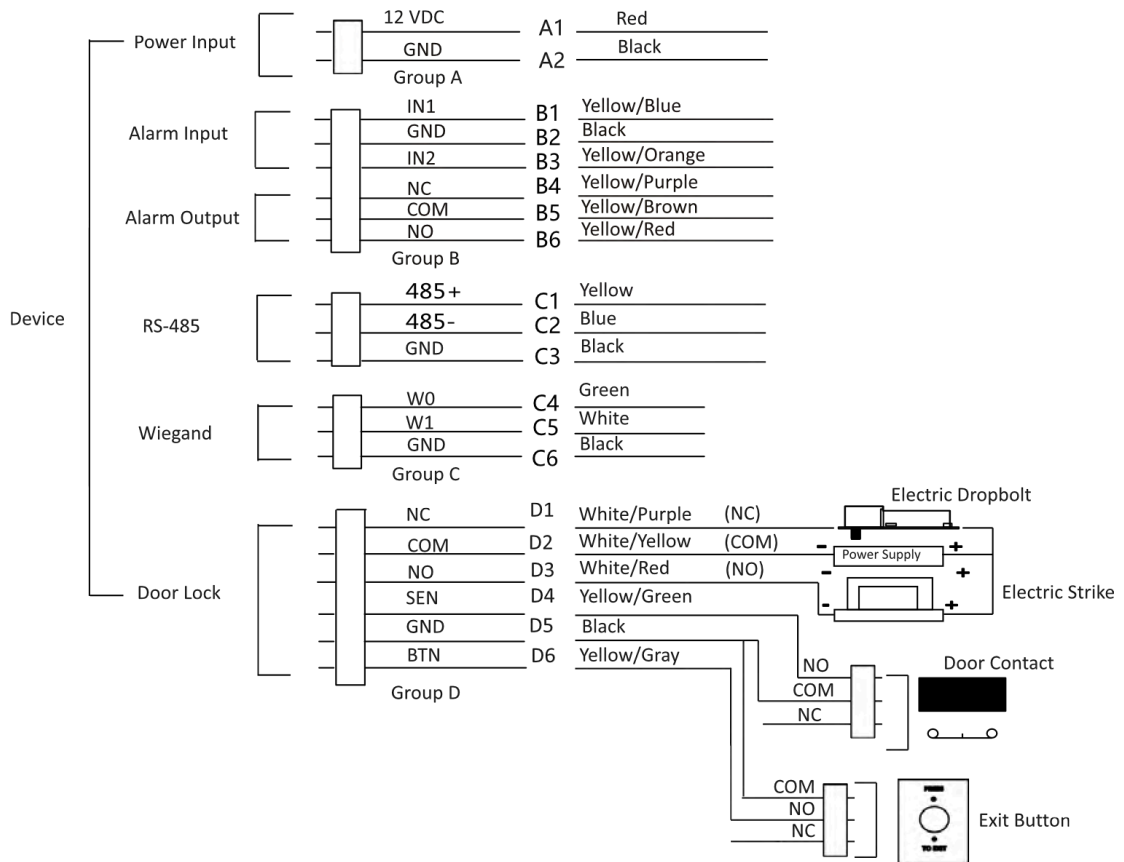


Figure 3-2 External Device Wiring

3.3 Wire Secure Door Control Unit

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

The wiring diagram is as follows.

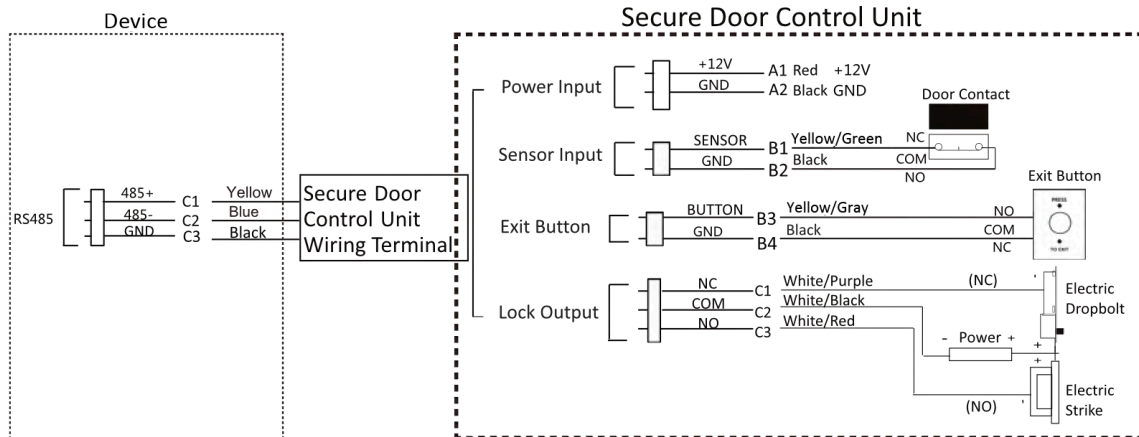


Figure 3-3 Secure Door Control Unit Wiring

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 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.

1. Enable the mobile phone's Wi-Fi function. Search and add the device hotspot (hotspot name: AP_Serial No.).
-

Note

- Hotspot name/password: AP_Serial No.
 - Hold key 5 on the device keypad for 10 s to enable/disable the hotspot function.
 - After 30 min after device powering on, the hotspot function will be disabled automatically.
 - After device activation, the hotspot password will be changed to the device activation password.
-

2. The mobile phone will jump to the web browser page. 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. Edit the device IP address. You can edit the IP address via the SADP tool, PC web browser and the client software.

4.2 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**.



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.



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.



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.

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

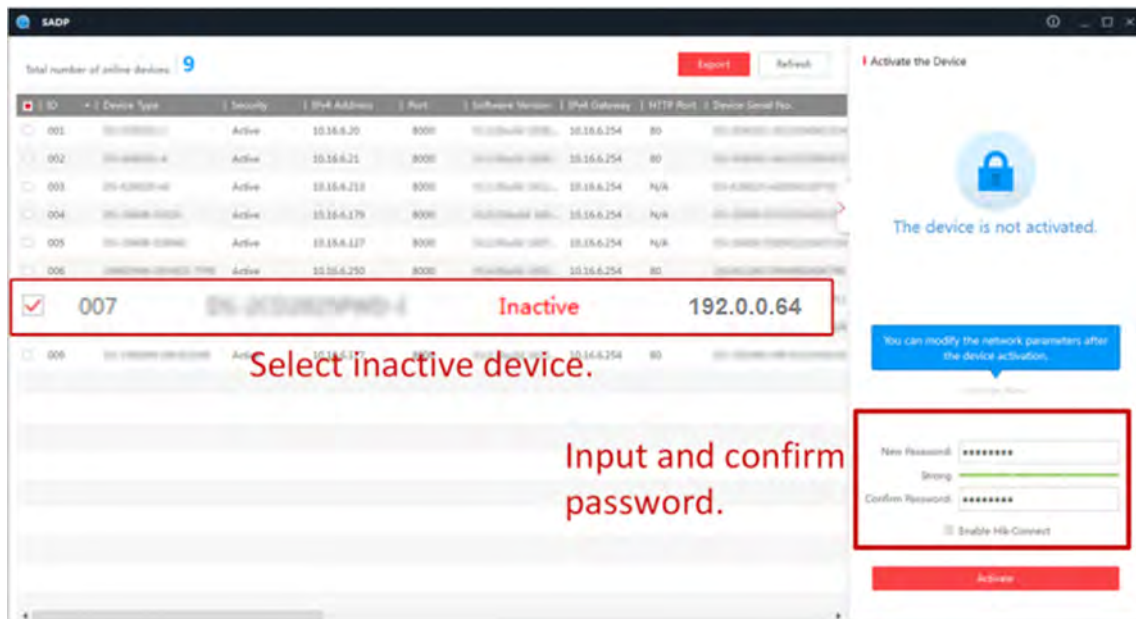
1. Run the SADP software and search the online devices.

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.

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 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.

5.1 Authenticate via Single Credential

Set the user authentication type before authentication. For details, see [**Set Authentication Parameters**](#).

Authenticate fingerprint, card, PIN, or QR code.

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.



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

QR Code

Put the QR code in front of the device camera to authenticate via QR code.



Authentication via QR code should be supported by the device.

PIN

Enter the PIN to authenticate via PIN.

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

5.2 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.
- If the QR Code Scanning function is enabled, you can put the QR code in front of the device camera to authenticate via QR code.

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 6 Call and Video Intercom

Set the SIP server IP, calling and video intercom between devices are available.

Set Device A as SIP server, and set Device A's IP as SIP server IP. For details, see **Session Settings** .
All other devices that need to call each other should be registered to the server.


Set device room number. For details, see **Set Video Intercom Parameters** .

On the device main page, enter the device room No. to call. When the other device is answered, video intercom can be performed.

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. Set the security questions before configuration.

Click  in the top right of the web page to enter the **Change Password** page. You can click **Skip** to skip the step. Or select three questions to answer and click **Next**.

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.


Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

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

7.4 Privacy Settings

Set the picture uploading and storage parameters.

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

Picture Uploading and Storage

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically.


Save Pictures After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

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

7.5 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting device language, time, environment and privacy, you can click **Next** to enter the **Administrator Settings** 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.

7.6 No. and System Network

Steps

1. Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and System Network** settings page.
2. Set the device type.

If set the device type as **Door Station** or **Outer Door Station**, you can set the **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**

If set the device type as **Outer Door Station**, you can set outer door station No., and community No.

3. Set **Registration Password**, **Main Station IP** and **Private Server IP**.
4. **Optional**: Click to **Enable Protocol 1.0**.
5. Click **Complete** to save the settings after the configuration.

Chapter 8 Operation via Web Browser

8.1 Login

You can login via the web browser or the remote configuration of the client software.




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**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click  to enter the Configuration page.

8.2 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, 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 the live video of the device, real-time event, person information, network status, basic information, and device capacity.

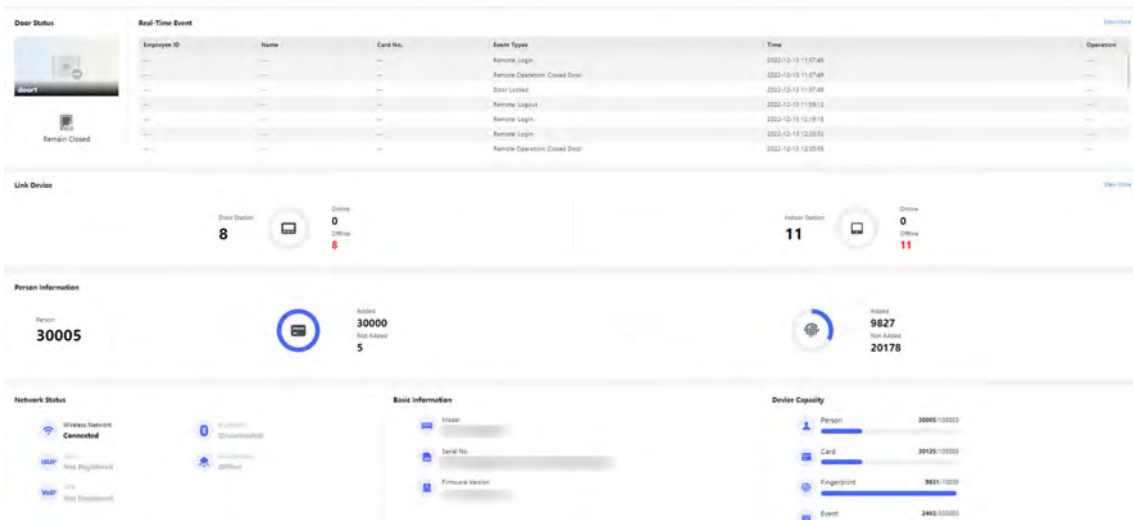


Figure 8-1 Overview Page

Function Descriptions:

Door Status

Click  to view the device live view.



Set the volume when starting live view.

Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.



You can capture image when starting live view.



Select the streaming type when starting live view. You can select from the main stream and the sub stream.



Full screen view.



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

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

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, VoIP 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, authentication and 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, 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.

Set Room No.

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

Click **Add** to add the **Floor No.** and **Room No.**

Click  to delete it.

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.

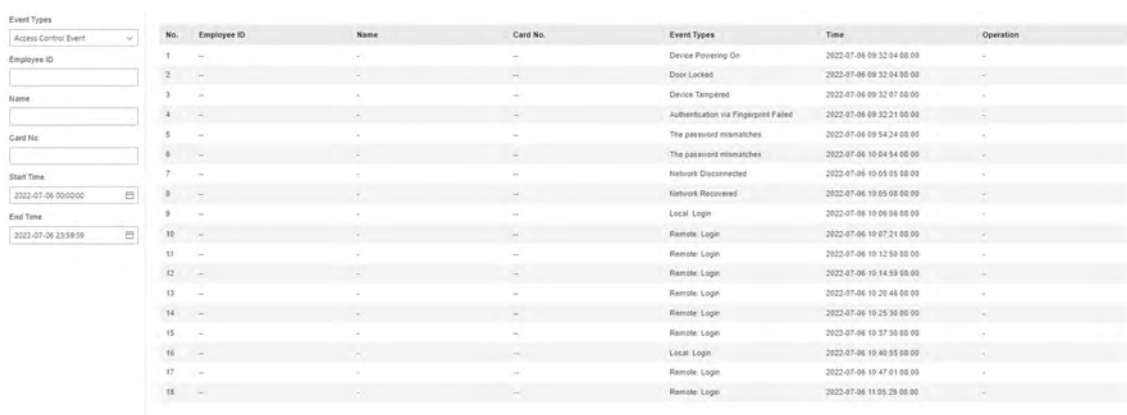
Click **Person Management** → **Add** to enter the Add Person page.

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.



No.	Employee ID	Name	Card No.	Event Types	Time	Operation
1	--	--	--	Device Powering On	2022-07-06 09:32:04.00.00	--
2	--	--	--	Door Locked	2022-07-06 09:32:04.00.00	--
3	--	--	--	Device Tampered	2022-07-06 09:32:07.00.00	--
4	--	--	--	Authentication via Fingerprint Failed	2022-07-06 09:32:21.00.00	--
5	--	--	--	The password mismatches	2022-07-06 09:54:24.00.00	--
6	--	--	--	The password mismatches	2022-07-06 10:04:54.00.00	--
7	--	--	--	Network Disconnected	2022-07-06 10:05:05.00.00	--
8	--	--	--	Network Recovered	2022-07-06 10:05:08.00.00	--
9	--	--	--	Local Login	2022-07-06 10:06:08.00.00	--
10	--	--	--	Remote Login	2022-07-06 10:07:21.00.00	--
11	--	--	--	Remote Login	2022-07-06 10:12:50.00.00	--
12	--	--	--	Remote Login	2022-07-06 10:14:59.00.00	--
13	--	--	--	Remote Login	2022-07-06 10:20:48.00.00	--
14	--	--	--	Remote Login	2022-07-06 10:25:30.00.00	--
15	--	--	--	Remote Login	2022-07-06 10:37:38.00.00	--
16	--	--	--	Local Login	2022-07-06 10:40:55.00.00	--
17	--	--	--	Remote Login	2022-07-06 10:47:01.00.00	--
18	--	--	--	Remote Login	2022-07-06 11:05:29.00.00	--

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 Set Local Parameters

Set the live view parameters, record file saving path, and captured pictures saving path.

Set Live View Parameters

Click **Configuration** → **Local** to enter the Local page. Configure the stream type, the play performance, auto start live view, and the image format and click **Save**.

Set Record File Saving Path

Click **Configuration** → **Local** to enter the Local page. Select a record file size and select a saving path from your local computer and click **Save**.

You can also click **Open** to open the file folder to view details.

Set Captured Pictures Saving Path

Click **Configuration** → **Local** to enter the Local page. Select a saving path from your local computer and click **Save**.

You can also click **Open** to open the file folder to view details.

8.6.2 View Device Information

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

8.6.3 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.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

8.6.4 Set DST

Steps

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

DST

DST

Start Time April First Sun 02

End Time October Last Sun 02

DST Bias 30minute(s)


Save

Figure 8-3 DST Page

2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.6.5 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.

8.6.6 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.

8.6.7 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.

8.6.8 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.

8.6.9 Network Settings

Set TCP/IP, port, Wi-Fi parameters, 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** .

The screenshot shows the TCP/IP Settings page. At the top, there is a dropdown menu for 'NIC Type' set to 'Self-Adaptive'. Below it is a 'DHCP' toggle switch that is turned on. The IPv4 configuration section includes input fields for 'IPv4 Address', 'IPv4 Subnet Mask', and 'IPv4 Default Gateway'. The IPv6 configuration section has radio buttons for 'Manual', 'DHCP', and 'Route Advertisement', with 'Route Advertisement' selected. Below these are input fields for 'IPv6 Address', 'IPv6 Subnet Prefix Length', and 'IPv6 Default Gateway'. The 'Mac Address' is displayed as 'ac:b9:2f:df:84:7d' and the 'MTU' is set to '1500'. There is a 'DNS Server' section with a 'DHCP' toggle switch that is turned off, and input fields for 'Preferred DNS Server' and 'Alternate DNS Server'. A red 'Save' button is located at the bottom of the form.

Figure 8-4 TCP/IP Settings Page

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, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 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, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 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




The function should be supported by the device.

1. Click **Configuration** → **Network** → **Network Settings** → **Wi-Fi** .



Figure 8-5 Wi-Fi Settings Page

2. Check **Wi-Fi**.
3. Select a Wi-Fi
 - Click  of a Wi-Fi in the list and enter the Wi-Fi password.
 - Click **Add** and enter a Wi-Fi's name, password, and encryption type. Click **Connect**. When the Wi-Fi is connected, click **OK**.
4. **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.
5. 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**.

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 server IP address, and verification code.
-

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).
-

5. 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**.

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 HikCentral Connect or HikCentral Access Control.



Note

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

Serial Port Configuration

Set serial port.

Tap **Configuration** → **Communication Settings** → **Serial Port Configuration** to enter the configuration page.

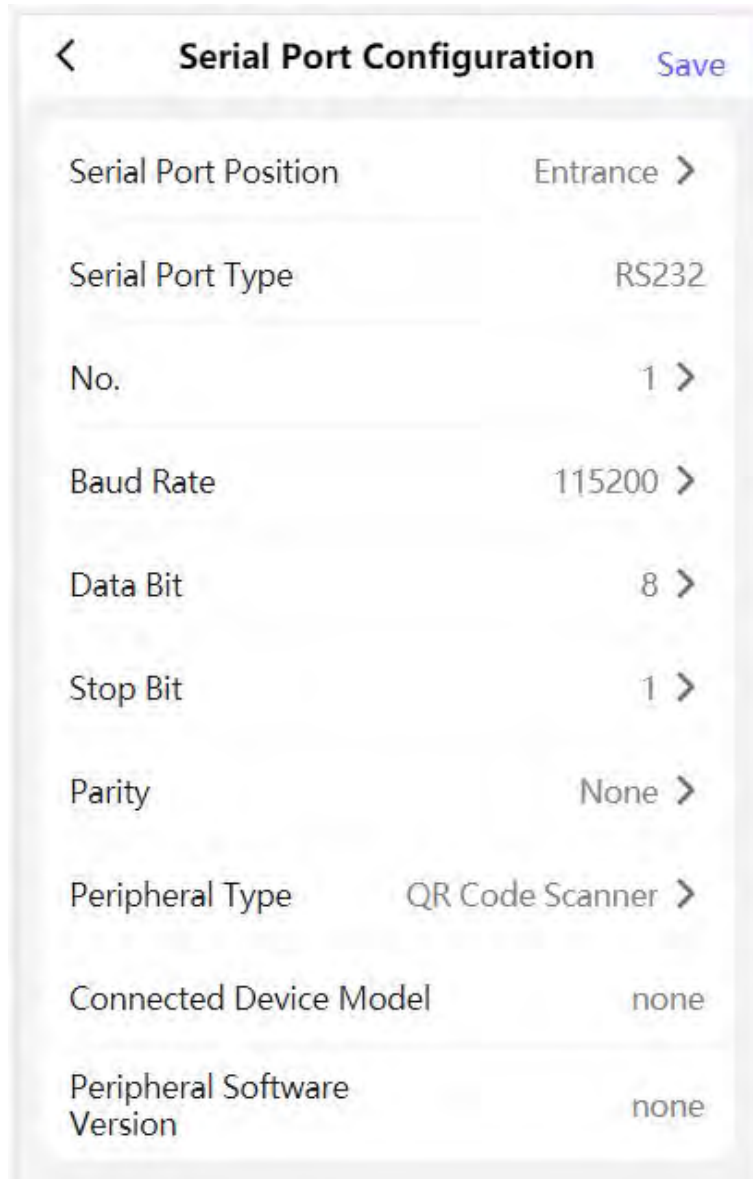


Figure 8-6 Serial Port Configuration

Set **Serial Port Position** as **Entrance** or **Exit**.

Select the port **No.**, and set **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.

Set the **Peripheral Type** as **Card Receiver**, **QR Code Scanner** or **Disable**.

Tap **Save**.

8.6.10 Set Audio Parameters

Set the audio parameters.

Set the input volume, output volume and enable voice prompt according to your actual needs. Click **Save** to save the settings after the configuration.

Note

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

8.6.11 Set Image Parameters

You can adjust the image parameters, video parameters, supplement parameters and capture interval.

Steps

1. Click **Configuration → Image** .
2. Configure the parameters to adjust the image.

Video Adjust(Video Standard)

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Supplement Light Parameters

Set the supplement light type, mode, start time and end time. You can also set the brightness.

Capture Interval

You can select the capture interval according to your actual needs.

3. Click **Default** to restore the parameters to the default settings.

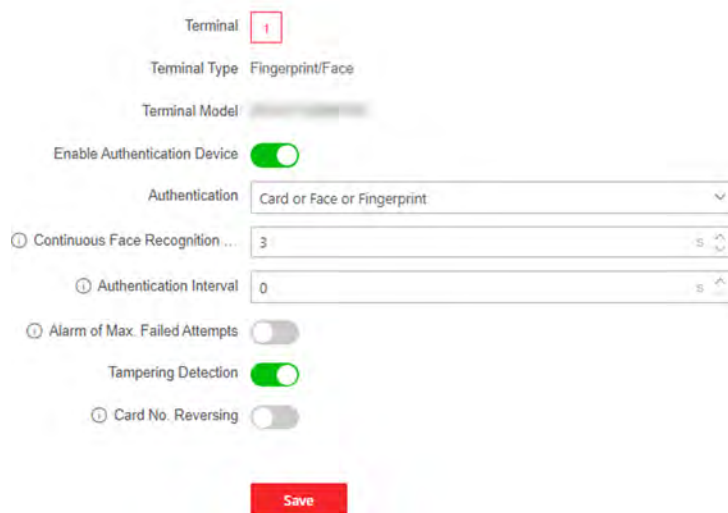
8.6.12 Access Control Settings

Set Authentication Parameters

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

Note

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



The screenshot shows a configuration page for a terminal. At the top, there is a 'Terminal' dropdown menu with a red box around the number '1'. Below it, 'Terminal Type' is set to 'Fingerprint/Face' and 'Terminal Model' is a blurred field. The 'Enable Authentication Device' toggle is turned on (green). The 'Authentication' dropdown is set to 'Card or Face or Fingerprint'. Below that, 'Continuous Face Recognition...' is set to '3' and 'Authentication Interval' is set to '0'. There are three more toggle options: 'Alarm of Max. Failed Attempts' (off), 'Tampering Detection' (on), and 'Card No. Reversing' (off). A red 'Save' button is at the bottom.

Figure 8-7 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.

QR Code

Enable the function and the user can use QR code to open the door.



Note

- Disable the IR light if enabling the QR code function. For details, see **Set Image Parameters** . The picture in low illumination environment may be affected due to disabling the IR light.
 - Set QR code function via HCC or HCEC, you should select compatible to 1.0 or 2.0. 2.0 is recommended.
-

Set Door Parameters

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

Door No.

Door Name

Open Duration

Door Open Timeout Alarm

Door Magnetic Sensor Type Remain Closed Remain Open

Exit Button Type Remain Closed Remain Open

Door Lock Powering Off Status Remain Closed Remain Open

Extended Open Duration

Door Remain Open Duration with ... min

Duress Code

Super Password

Figure 8-8 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 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.

8.6.13 Video Intercom Settings

Set Video Intercom Parameters

The device can be used as a door station, or outer door station. You should set the device No. before usage.

Click **Configuration** → **Intercom** → **Device No.** .

If set the device type as **Door Station**, you can set the floor No., door station No., and click **More** to set **Community No.**, **Building No.**, and **Unit No.** You can press any digit button to enter the calling page, and enter the room No. and press call button to call the resident.

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

Device Type	Door Station
Period No.	1
Building No.	1
Unit No.	1
Floor No.	1
Door Station No.	0
Community No.	0

Save

Figure 8-9 Device No. Settings

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

 **Note**

If you change the device type, you should reboot the device.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.

 **Note**

- If you change the No., you should reboot the device.
 - The main door station No. is 0, and the sub door station No. ranges from 1 to 16.
-

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

 **Note**

If you change the No., you should reboot the device.

If set the device type as **Outer Door Station**, you can set outer door station No., and community No. You can press call button to enter the calling page, and enter **【Community No. + Building No. + # + Unit No. + # + Room No.】** and press call button to call resident.

Outer Door Station No.

If you select outer door station as the device type, you should enter a number between **1** and **99**.

 **Note**

If you change the No., you should reboot the device.

Community No.

Set the device community No.

Session Settings

Enable the communication between door station, main station, and video intercom server.

Steps

1. Click **Configuration** → **Intercom** → **Session Settings** to enter the settings page.

2. Set registration password, main station IP, private server IP and enable Protocol 1.0.

Registration Password

Create a registration password for communication via SIP

Main Station IP

IP address of the main station.

Private Server IP

Enter the IP address of the device that need to communicate via SIP. The device will be the SIP server. Other devices should register to the SIP server, or the video intercom between devices will be failed.

Enable Protocol 1.0

After enabling, the device is registered to the main station through the previous protocol. If disabled, the device is registered to the main station through the new protocol.

3. Click **Save**.

Time Duration Settings

Set the Max. call duration.

Go to **Configuration → Intercom → Call Settings** .

Drag the block to set the Max. call duration. Click **Save**.



Note

The Max. call duration range is 90 s to 120 s.

Number Settings

You can call the room SIP to call the room.

Steps

1. Click **Configuration → Intercom → Number Settings** to enter the settings page.
2. Click **+ Add**, enter the **Room No.** and **SIP**.
3. Click **Save**.

Press Button to Call

Steps

1. Click **Configuration → Intercom → Press Button to Call** to enter the settings page.
2. Check **Call Indoor Station**, **Call Specified Indoor Station**, **Call Management Center** or **APP** at your needs.

Note

If you check **Call Specified Indoor Station**, you need to enter the number of the indoor station.

3. Click **Save**.

8.6.14 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.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card content.

Enable FeliCa Card

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

8.6.15 Set Privacy Parameters

Set the event storage type, picture upload and storage parameters, and the picture clearing parameters.

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.

Picture Uploading and Storage

Upload Picture After Linked Capture

Upload the pictures captured by linked camera to the platform automatically.

Save Pictures After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Clear All Pictures in Device



All pictures cannot be restored once they are deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

8.6.16 Time and Attendance Settings

If you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the shift group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the shift group to define the attendance parameters for the persons in the shift group.

Disable Attendance Mode via Web

Disable the attendance mode and the system will not display the attendance status on the initial page.

Steps

1. Click **Configuration** → **T&A Status** to enter the settings page.
2. Disable the **Time and Attendance**.

Result

You will not view or configure the attendance status on the initial page. And the system will follow the attendance rule that configured on the platform.

Time Settings

Steps

1. Click **Configuration** → **T&A Status** to enter the settings page.
2. Select **Schedule Template**.
3. Drag mouse to set the schedule.



Set the schedule from Monday to Sunday according to the actual needs.

4. You can enable **On/off Work, Break, Overtime** according to your actual needs and set the custom name.
5. **Optional:** Select a timeline and click **Delete**. Or click **Delete All** to clear the settings.

6. Click **Save**.

Set Manual Attendance via Web

Set the attendance mode as manual, and you should select a status manually when you take attendance.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **Configuration → T&A Status** to enter the settings page.
2. Set the **Attendance Mode** as **Manual**.
3. Enable the **Attendance Status Required** and set the attendance status lasts duration.
4. Enable a group of attendance status.



The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

Result

You should select an attendance status manually after authentication.



If you do not select a status, the authentication will be failed and it will not be marked as a valid attendance.

Set Auto Attendance via Web

Set the attendance mode as auto, and you can set the attendance status and its available schedule. The system will automatically change the attendance status according to the configured schedule.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **Configuration → T&A Status** to enter the settings page.
2. Set the **Attendance Mode** as **Auto**.
3. Enable the **Attendance Status Required** function.
4. Enable a group of attendance status.



The Attendance Property will not be changed.

5. **Optional:** Select an status and change its name if required.

6. Set the status' schedule. Refers to [Time Settings](#) for details.

Set Manual and Auto Attendance via Web

Set the attendance mode as **Manual and Auto**, and the system will automatically change the attendance status according to the configured schedule. At the same time you can manually change the attendance status after the authentication.

Before You Start

Add at least one user, and set the user's authentication mode. For details, see *User Management*.

Steps

1. Click **Configuration** → **T&A Status** to enter the settings page.
2. Set the **Attendance Mode** as **Manual and Auto**.
3. Enable the **Attendance Status Required** function.
4. Enable a group of attendance status.



Note

The Attendance Property will not be changed.

-
5. **Optional:** Select an status and change its name if required.
 6. Set the status' schedule. Refers to [Time Settings](#) for details.

Result

On the initial page and authenticate. The authentication will be marked as the configured attendance status according to the schedule. If you tap the edit icon on the result tab, you can select a status to take attendance manually, the authentication will be marked as the edited attendance status.

Example

If set the **Break Out** as Monday 11:00, and **Break In** as Monday 12:00, the valid user's authentication from Monday 11:00 to 12:00 will be marked as break.

8.6.17 Set Smart Parameters

Set Basic Parameters

Click **Configuration** → **Smart** → **Smart** .

Select **Fingerprint Security Level** according to your actual needs.

8.6.18 Set Preference

You can set the display theme and the sleep time for the device.

Set Theme

Click **Configuration** → **Preference** .

Sleep

Enable **Sleep** and the device will enter the sleep mode when no operation within the configured sleep time.

Display Mode

You can select display theme for device authentication. You can select **Display Mode** as **Default** or **Simple**. When you select **Simple**, the information of name, ID, face picture will be not displayed.

8.6.19 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.

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.

8.6.20 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.

8.6.21 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.

8.6.22 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.

8.6.23 Certificate Management

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



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

You can login via mobile browser.



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

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**.

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, bluetooth, 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, IO input number, local RS-485 number, number of alarm output, register number, 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, IO input number, local RS-485 number, number of alarm output, register number, 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.

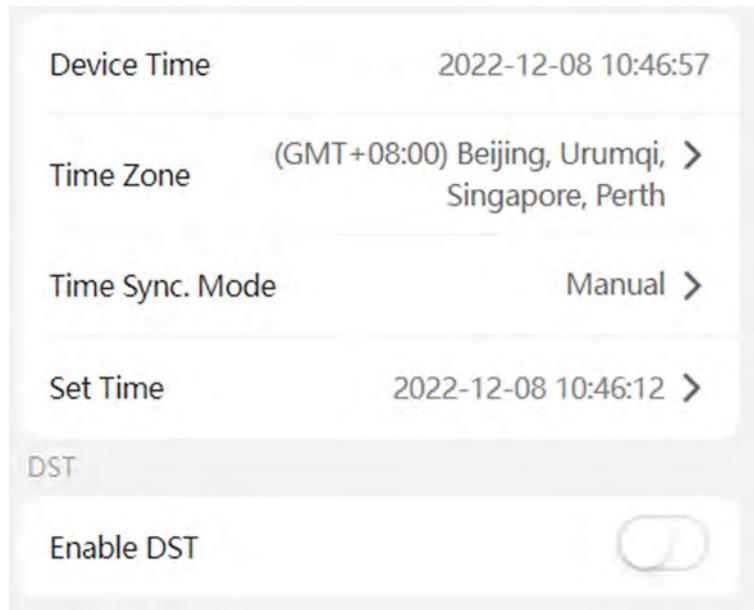


Figure 9-1 Time Settings

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.

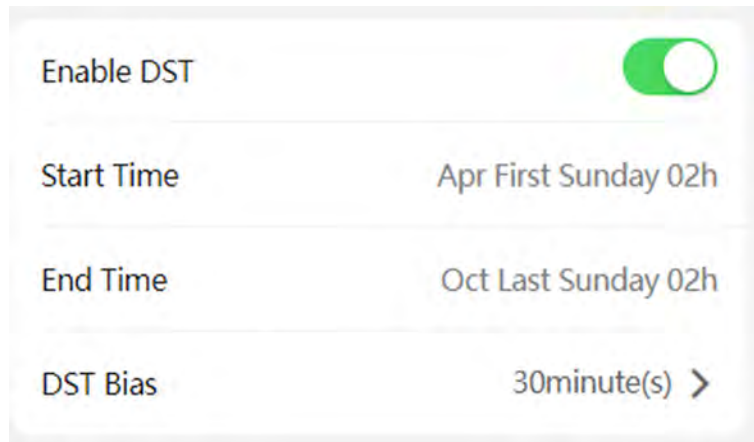



Figure 9-2 DST

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, IPv6 mode, IPv6 address, IPv6 subnet prefix length, IPv6 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, IPv6 mode, IPv6 address, IPv6 subnet prefix length, and IPv6 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**.

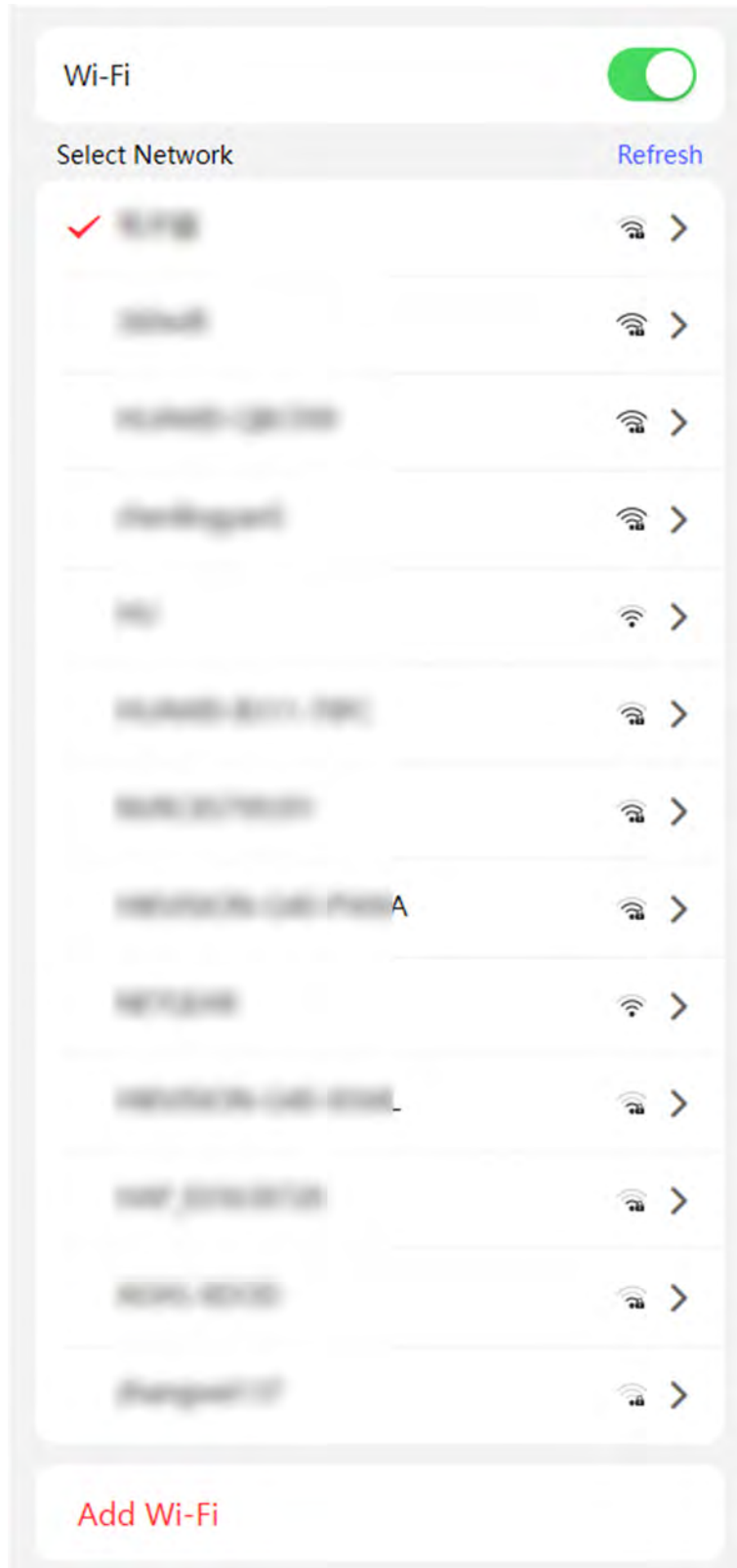


Figure 9-3 Wi-Fi

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.



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.



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 account.
 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.

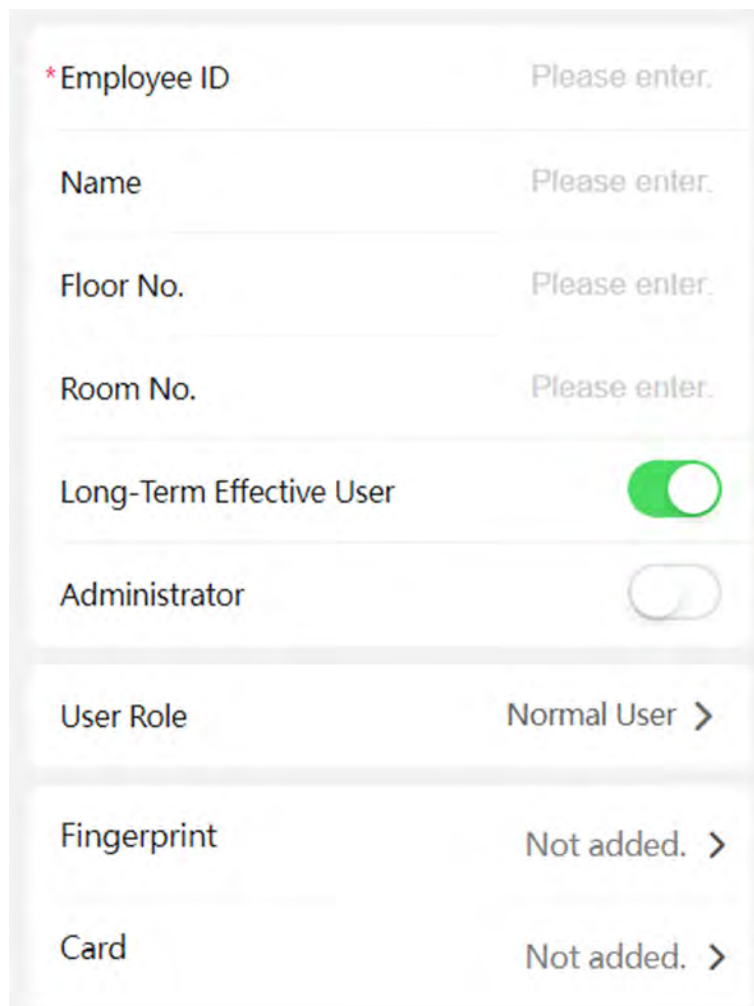
-
4. Tap **Save** to save the settings.

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+.



The screenshot shows a form for adding a user. It contains the following fields and options:

- *Employee ID**: Please enter.
- Name**: Please enter.
- Floor No.**: Please enter.
- Room No.**: Please enter.
- Long-Term Effective User**:
- Administrator**:
- User Role**: Normal User >
- Fingerprint**: Not added. >
- Card**: Not added. >

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.

Floor No./Room No.

Enter the floor No./room No.

Long-Term Effective

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 Set Audio

Set the device volume.

Steps

1. Tap  → **Audio** to enter the settings page.
2. You can adjust the device input and output volume according to your actual needs.
3. You can enable voice prompt according to your actual needs.

9.4.8 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.

9.4.9 Access Control Settings

Set Authentication Parameters

Set Authentication Parameters.

Steps

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

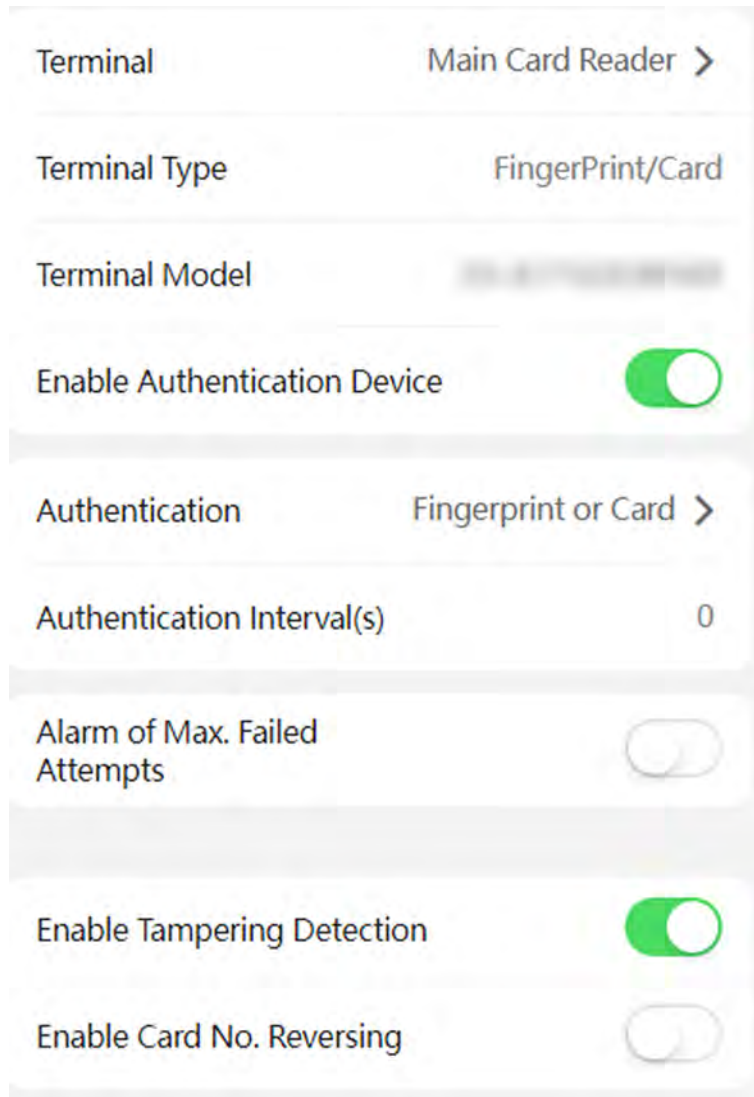


Figure 9-5 Authentication Settings

2. Tap **Save**.

Terminal

Main Card Reader

You can configure the device card reader's parameters. If you select main card reader, you need to configure the following parameters: **Terminal Type**, **Terminal Model**, **Enable Card Reader**, **Authentication**, **Recognition Interval (s)**, **Minimum Card Swiping Interval (s)**, **Max. Authentication Failed Attempts Alarm/Alarm of Max. Failed Attempts**, **Enable Tampering Detection** and **Enable Card No. Reversing**.

Card Reader Type

Get card reader type.

Card Reader Description

Get card reader description. It is read-only.

Enable Card Reader

Enable the card reader's 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.

QR Code

Enable the function and the user can use QR code to open the door.



Note

- Disable the IR light if enabling the QR code function. For details, see ***Set Image Parameters***. The picture in low illumination environment may be affected due to disabling the IR light.
 - Set QR code function via HCC or HCEC, you should select compatible to 1.0 or 2.0. 2.0 is recommended.
-

Set Door Parameters

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

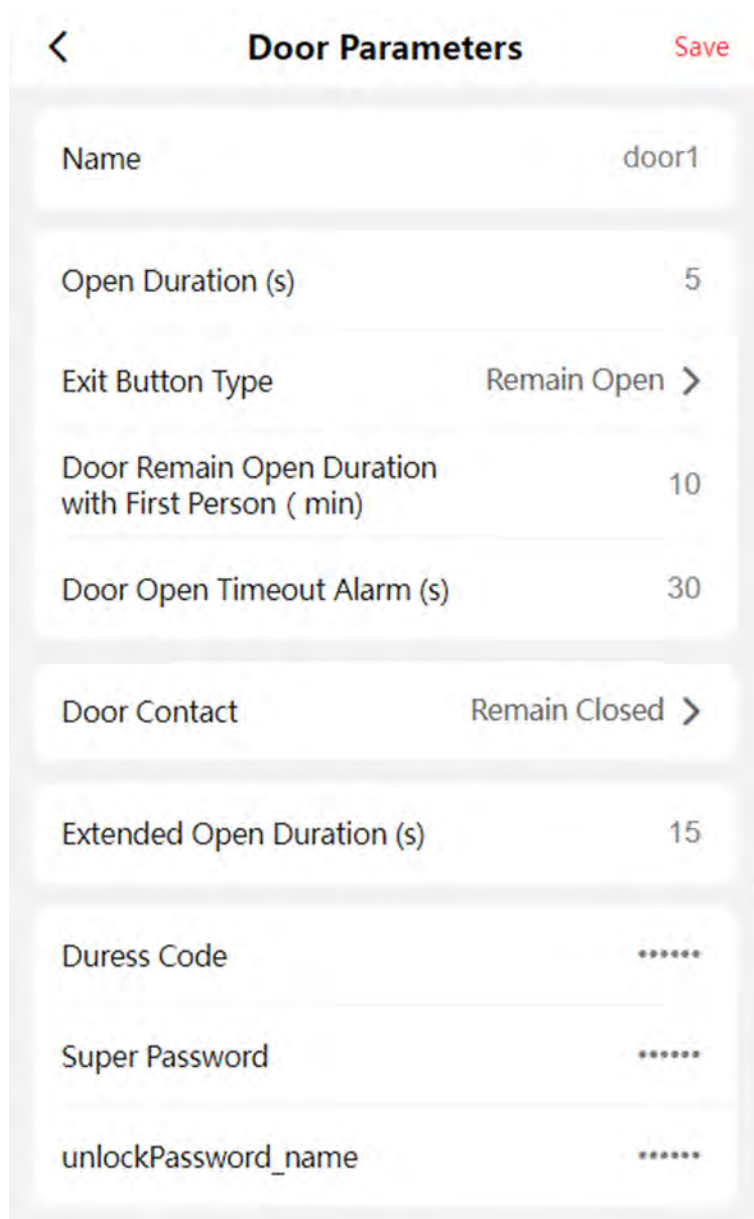


Figure 9-6 Door Parameters Settings Page

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.

Elevator Control Parameters


Tap  → **Access Control** → **Elevator Control Parameters** to enter the configuration page.

Enable **Elevator Control**. Select main elevator controller model and interface type.

Tap **Save**.

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.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card content.

Enable FeliCa Card

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

9.4.10 Intercom

Device ID Settings

The device can be used as a door station, or outer door station. You should set the device No. before usage.

Steps

1. Tap  → **Intercom** → **Device ID Settings** .
2. Set the following parameters.

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

 **Note**

If you change the device type, you should reboot the device.

Period No.

Set the device period No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

 **Note**

If you change the No., you should reboot the device.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed floor No.

 **Note**

- If you change the No., you should reboot the device.
 - The main door station No. is 0, and the sub door station No. ranges from 1 to 16.
-

If set the device type as **Outer Door Station**, you can set outer door station No., and community No.

Outer Door Station No.

If you select outer door station as the device type, you should enter a number between **1** and **99**.

 **Note**

If you change the No., you should reboot the device.


Period No.

Set the device period No.

Session Settings

Enable the communication between door station, main station, and video intercom server.

Steps

1. Tap  → **Intercom** → **Session Settings** .
2. Set registration password, main station IP, private server IP and enable Protocol 1.0.

Registration Password

Activation password of the main station.

Main Station IP

IP address of the main station.

Private Server IP

IP address of the private server.

Enable Protocol 1.0

After enabling, the device is registered to the main station through the previous protocol. If disabled, the device is registered to the main station through the new protocol.

3. Tap **Save**.

Time Duration Settings

Set the Max. call duration.

Tap  → **Intercom** → **Call Settings** .

Set the Max. communication time. Tap **Save**.




Note

The Max. call duration range is 90 s to 120 s.

Number Settings


You can call the room SIP to call the room.

Steps

1. Tap  → **Intercom** → **Number Settings** .
2. Tap +, enter the **Room No.** and **SIP Number**.
3. Tap **Save**.

Press Button to Call

Steps


1. Tap  → **Intercom** → **Press Button to Call** .
2. Select the No. Select **Call Indoor Station**, **Call Specified Indoor Station**, **Call Management Center** or **APP** at your needs.

 **Note**

If you check **Call Specified Indoor Station**, you need to enter the number of the indoor station.

9.4.11 Fingerprint Parameters Settings

Set fingerprint security level.

Tap  → **Smart** .

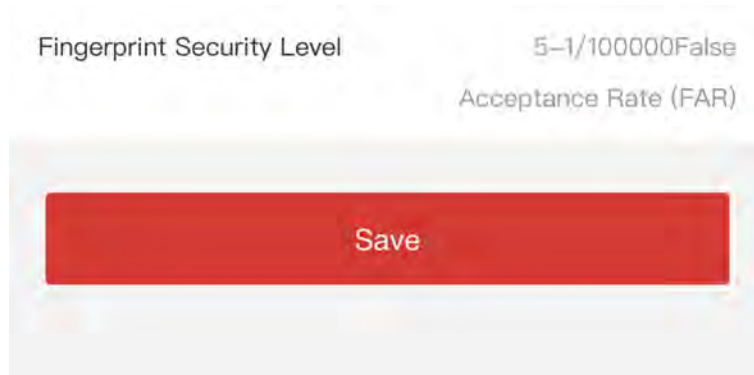


Figure 9-7 Fingerprint Security Level

 **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.

9.4.12 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.

9.4.13 View Online Document

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

9.4.14 View Open Source Software License

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

Chapter 10 Client Software Configuration

You can call the hotline to get the iVMS-4200 client software installation package.

10.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

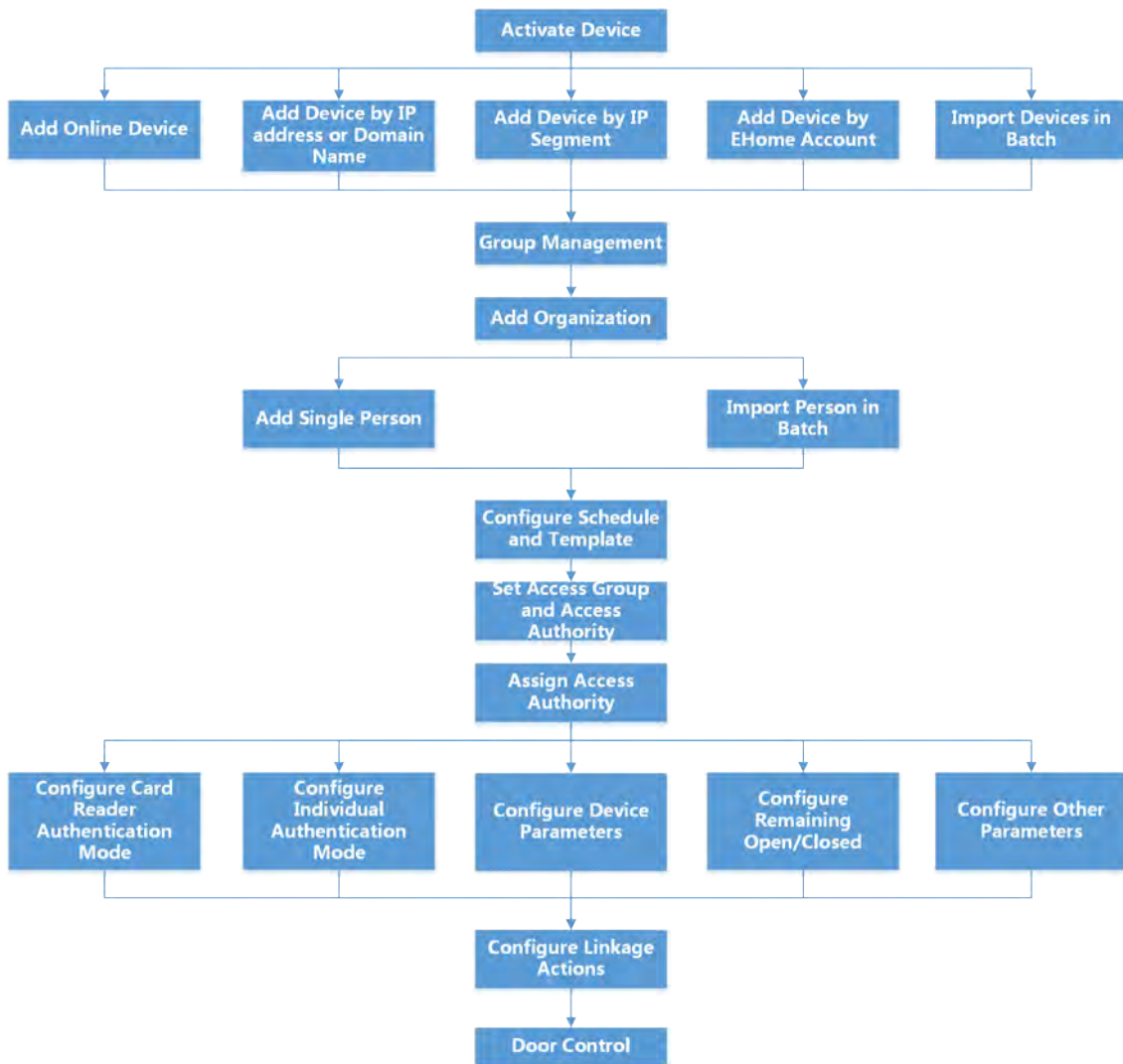


Figure 10-1 Flow Diagram of Configuration on Client Software

10.2 Device Management

The client supports managing access control devices and video intercom devices.

Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

10.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.
The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

Name

Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

Address

The IP address or domain name of the device.

Port

The devices to add share the same port number. The default value is **80**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device 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.

-
5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.
-



Note

- This function should be supported by the device.
 - If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security. See for details about enabling certificate verification.
 - You can log into the device to get the certificate file by web browser.
-
6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

Example

For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.

8. Finish adding the device.
- Click **Add** to add the device and back to the device list page.
 - Click **Add and New** to save the settings and continue to add other device.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

 **Note**

For detailed description of the required fields, refer to the introductions in the template.

Adding Mode

Enter **0** or **1** or **2**.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is **80**.

User Name

Enter the device user name. By default, the user name is **admin**.

Password

Enter the device 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.

Import to Group


Enter **1** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter **0** to disable this function.

6. Click  and select the template file.
7. Click **Add** to import the devices.

10.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.
All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click  on the Operation column.

4. Reset the device password.

- Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

 **Note**

For the following operations for resetting the password, contact our technical support.

 **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.

10.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 10-1 Manage Added Devices

Edit Device	Click  to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click Delete to delete the selected devices.
Remote Configuration	Click  to set remote configuration of the corresponding device. For details, refer to the user manual of device.
View Device Status	Click  to view device status, including door No., door status, etc.  Note For different devices, you will view different information about device status.
View Online User	Click  to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click  to refresh and get the latest device information.

10.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example

For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

10.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Create a group.
 - Click **Add Group** and enter a group name as you want.
 - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.



The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

10.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.



Before You Start

Add a group for managing devices. Refer to [Add Group](#) .

Steps

1. Enter the Device Management module.
2. Click **Device Management** → **Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

Note

You can click  or  to switch the resource display mode to thumbnail view or to list view.

6. Click **Import** to import the selected resources to the group.

10.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

10.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a subordinate organization for the added one.


Steps


1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

Note

Up to 10 levels of organizations can be added.

4. **Optional:** Perform the following operation(s).

Edit Organization Hover the mouse on an added organization and click  to edit its name.

Delete Organization Hover the mouse on an added organization and click  to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

Show Persons in Sub Organization Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

10.4.2 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, email, phone number, etc.

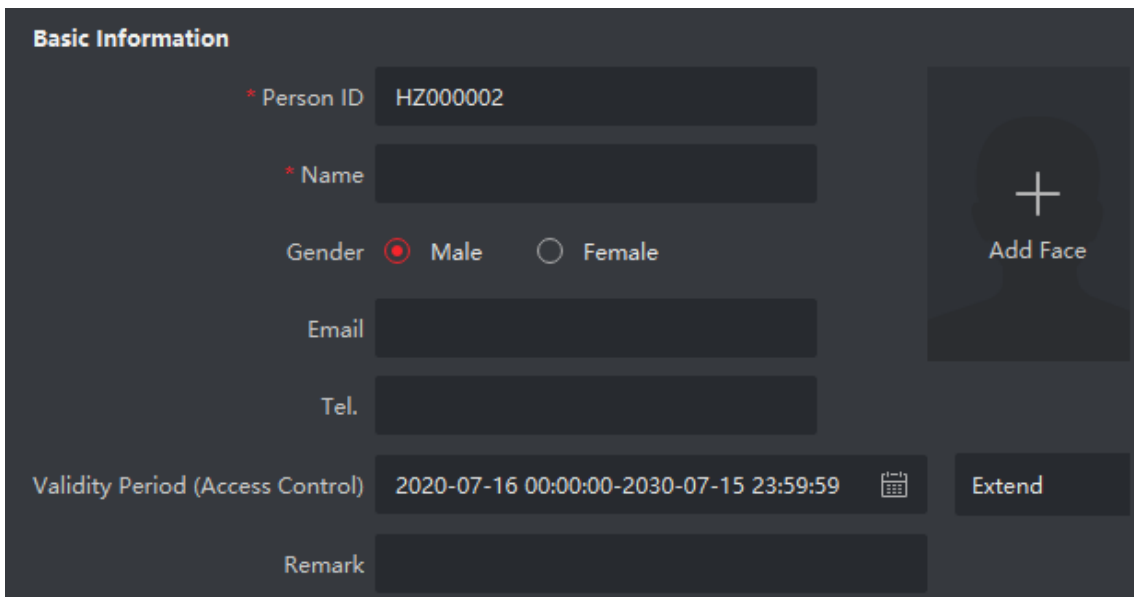
Steps

1. Enter **Person** module.

Note

For the first time you enter **Person** module, a window pops up, and you can set the rules to generate person ID (letters and numbers supported) when adding person. When getting person information from device, if there are no person IDs, the person IDs will be generated according to the rule.

2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.
The Person ID will be generated automatically.
4. Enter the basic information including person name, telephone number, email address, validity period, etc.



The screenshot shows a dark-themed form titled "Basic Information". It contains the following fields and controls:

- * Person ID: HZ000002
- * Name: [Empty text field]
- Gender: Male Female
- Email: [Empty text field]
- Tel.: [Empty text field]
- Validity Period (Access Control): 2020-07-16 00:00:00-2030-07-15 23:59:59 (with a calendar icon) and an "Extend" button.
- Remark: [Empty text field]
- An "Add Face" button with a plus sign icon is located on the right side of the form.

Figure 10-2 Configure Basic Information

Note

Once validity period expired, the credentials and access control settings of the person will be invalid and the person will have no authorization to access the doors\floors. You can click **Extend** to extend the person's validity period for 1 month, 3 months, 6 months, or 1 year.

5. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.
6. Delete Registered Face Picture

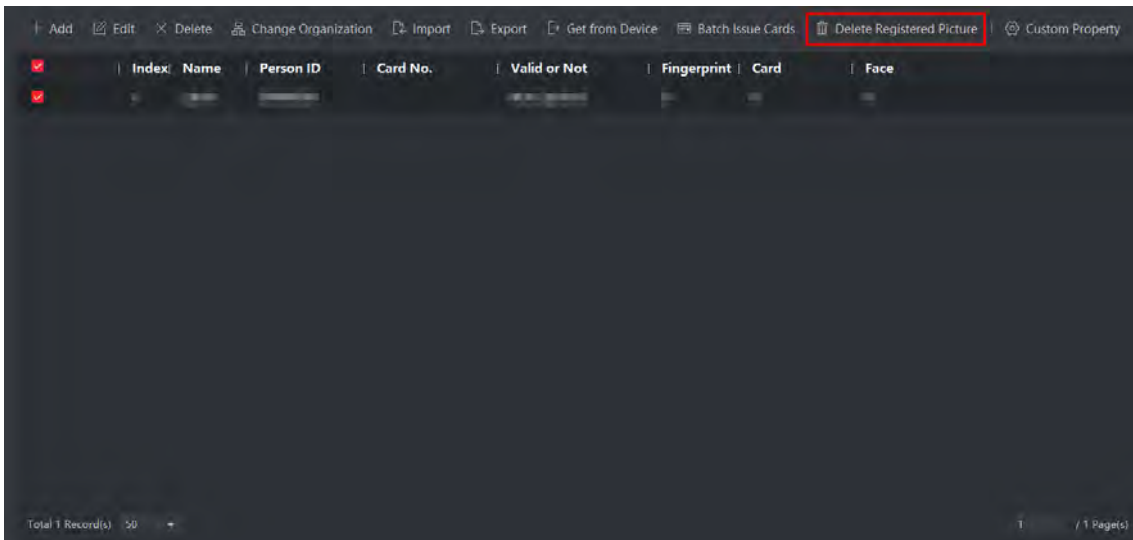


Figure 10-3 Delete Registered Picture

 **Note**

If **Save Pictures in Structure Data Format** is enabled, the **Delete Registered Picture** button will be added to the **Person** page. In general, the registered face picture will be deleted automatically once the person's information is applied to the device. By double clicking the person, the **Edit Person** window will pop up, and you can check whether the registered face picture has been deleted. If not, you can select this person and click **Delete Registered Picture** to delete the picture manually.

10.4.3 Issue a Card by Local Mode

If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential** → **Card** area, click **+**.
4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.

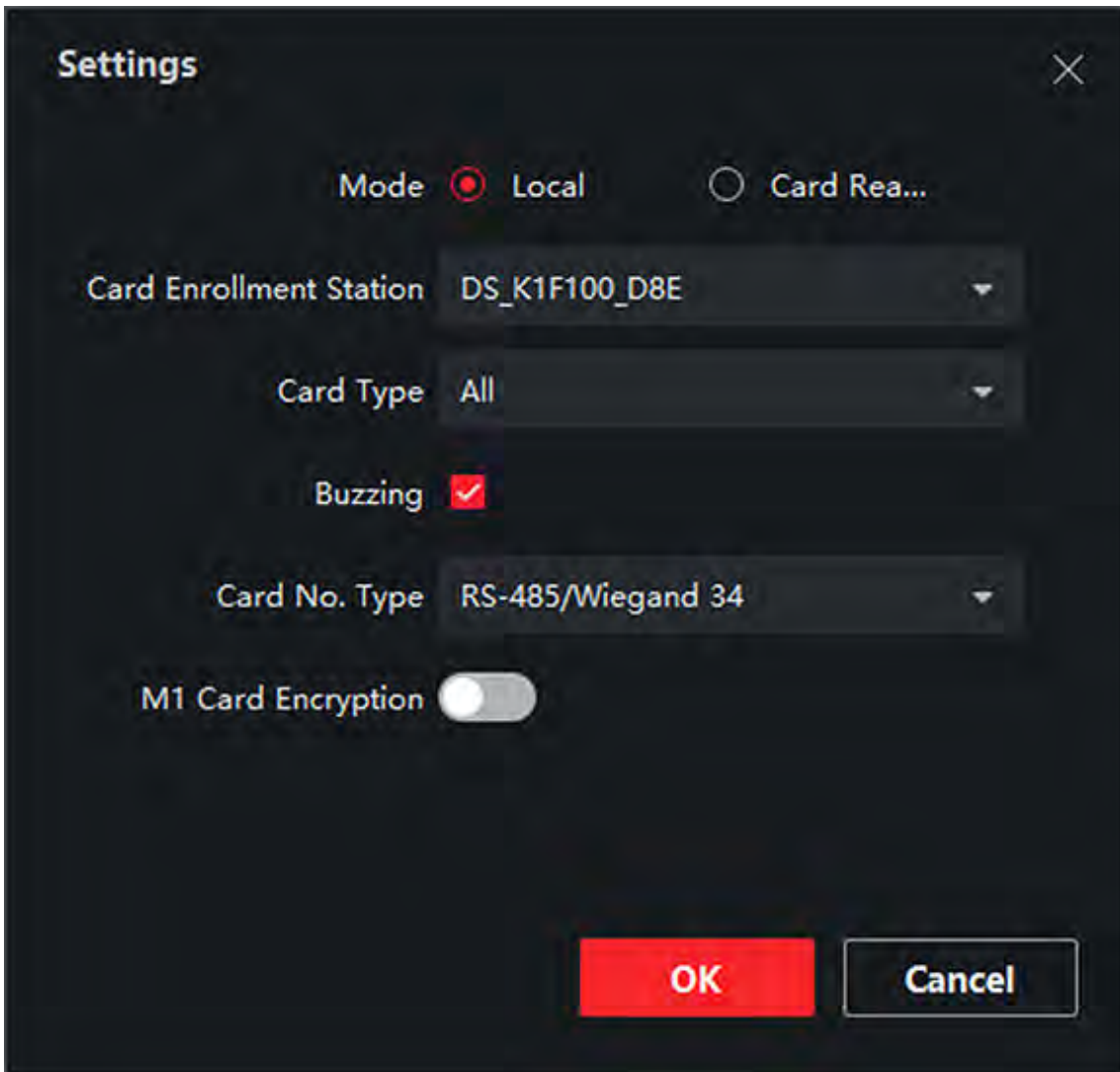


Figure 10-4 Issue a Card by Local Mode

6. Set other related parameters.

Card Enrollment Station

Select a model of card enrollment station from the drop-down list. You can connect the card enrollment station to the PC, and transfer the basic information about the added person between the two devices through USB.

 **Note**

The currently supported models of card enrollment station: DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, DS-K1F180-D8E, DS-K1F100A-D8E, and enrollment station.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E. Select the card type as EM card or Mifare card according to the actual card type.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E. If the card is M1 card, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.
The card number will display in the Card No. field automatically.
9. Click **Add**.
The card will be issued to the person.

10.4.4 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#).

3. In the **Credential** → **Fingerprint** panel, click +.
4. In the pop-up window, select the collection mode as **Local**.
5. Select the model of the connected fingerprint recorder.



Note

If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
 - 1) Click **Start**.
 - 2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.

3) Click **Add** to save the recorded fingerprint.

7. Confirm to add the person.

- Click **Add** to add the person and close the Add Person window.
- Click **Add and New** to add the person and continue to add other persons.



Note

Once the fingerprint is added, the fingerprint type cannot be changed.

10.4.5 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.



Note

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#) .

3. In the **Credential → Fingerprint** panel, click +.
4. In the pop-up window, select the collection mode as **Remote**.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
 - 1) Click **Start**.
 - 2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
 - 3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .




Note

Once the fingerprint is added, the fingerprint type cannot be changed.

10.4.6 Configure Access Control Information

When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.
3. In the **Access Control** area, click  to select access group(s) for the person.

Note

For details, refer to [***Set Access Group to Assign Access Authorization to Persons***](#) .

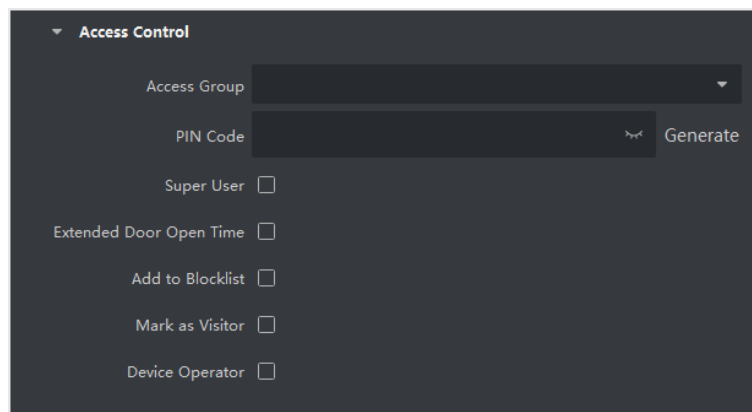


Figure 10-5 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
 - Manually enter a PIN code containing 4 to 8 digits.

Note

Persons' PIN codes cannot be repeated.

- Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.

Note

If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.

5. Check the person's operation permissions.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

For details about setting the door's open duration, refer to [***Configure Parameters for Door***](#) .

Add to Blocklist

Add the person to the blocklist and when the person tries to access doors/floors, an event will be triggered and sent to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.



Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.



Note

The Super User, Extended Door Open Time, Add to Blocklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blocklist, or set her/him as visitor.

6. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons.

10.4.7 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
 - 1) Click **Custom Property**.
 - 2) Click **Add** to add a new property.
 - 3) Enter the property name.
 - 4) Click **OK**.
3. Set the custom information when adding a person.
 - 1) Select an organization in the organization list to add the person and click **Add**.

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#) .

- 2) In the **Custom Information** panel, enter the person information.
- 3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

10.4.8 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
 2. Select an organization in the organization list to add the person and click **Add**.
-

 **Note**

Enter the person's basic information first. For details about configuring person's basic information, refer to [***Configure Basic Information***](#) .

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
 - Click **Add** to add the person and close the Add Person window.
 - Click **Add and New** to add the person and continue to add other persons .

10.4.9 Import and Export Person Identify Information

You can import the information of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and save them in your PC.

10.4.10 Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps


1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.

6. Enter the person information in the downloaded template.



Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

7. Click  to select the CSV/Excel file with person information from local PC.

8. Click **Import** to start importing.



Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.

10.4.11 Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start

Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.



Note

All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel.
4. Check **Person Information** as the content to export.
5. Check desired items to export.
6. Click **Export** to save the exported file in CSV/Excel file on your PC.

10.4.12 Get Person Information from Access Control Device

If the access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the added device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
 - Persons will be **Male** by default.
 - If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.
-

1. Enter **Person** module.
 2. Select an organization to import the persons.
 3. Click **Get from Device**.
 4. Select an added access control device or the enrollment station from the drop-down list.
-

Note

If you select the enrollment station, you should click **Login**, and enter IP address, port No., user name and password of the device.

5. Select the **Getting Mode**.
-

Note

The getting mode varies according to different devices. The access control device supports getting the person information by employee ID. Up to 5 employee IDs can be specified each time.

6. Click **Import** to start importing the person information to the client.
-

Note

Up to 2,000 persons and 5,000 cards can be imported.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

10.4.13 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
 2. Select an organization in the left panel.
The persons under the organization will be displayed in the right panel.
 3. Select the person to move.
-

4. Click **Change Organization**.
5. Select the organization to move persons to.
6. Click **OK**.

10.4.14 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps



1. Enter **Person** module.
2. Click **Batch Issue Cards**.
All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
 - Place the card on the card enrollment station.
 - Swipe the card on the card reader.
 - Manually enter the card number and press the **Enter** key.

The person(s) in the list will be issued with card(s).

10.4.15 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click  on the added card to set this card as lost card.
After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click  to cancel the loss.
After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

10.4.16 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station



Note

Currently, the supported card enrollment station model is DS-K1F180-D8E.

Card Type

Select the card type as EM card or IC card according to the actual card type.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

10.5 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to **Set Access Group to Assign Access Authorization to Persons** .

10.5.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control** → **Schedule** → **Holiday** to enter the Holiday page.
 2. Click **Add** on the left panel.
 3. Create a name for the holiday.
 4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
 5. Add a holiday period to the holiday list and configure the holiday duration.
-






Note

Up to 16 holiday periods can be added to one holiday.

- 1) Click **Add** in the Holiday List field.
 - 2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.
-

Note

Up to 8 time durations can be set to one holiday period.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
6. Click **Save**.
-

10.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control** → **Schedule** → **Template** to enter the Template page.
-

Note

There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

All-Day Authorized

The access authorization is valid in each day of the week and it has no holiday.



All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
 3. Create a name for the template.
 4. Enter the descriptions or some notification of this template in the Remark box.
 5. Edit the week schedule to apply it to the template.
 - 1) Click **Week Schedule** tab on the lower panel.
 - 2) Select a day of the week and draw time duration(s) on the timeline bar.
-

Note

Up to 8 time duration(s) can be set for each day in the week schedule.

- 3) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.
-

Note


Up to 4 holidays can be added to one template.

- 1) Click **Holiday** tab.

- 2) Select a holiday in the left list and it will be added to the selected list on the right panel.
- 3) **Optional:** Click **Add** to add a new holiday.

Note

For details about adding a holiday, refer to [***Add Holiday***](#).

- 4) **Optional:** Select a selected holiday in the right list and click  to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.

10.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to [***Group Management***](#).
- Add template.

Steps

When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control** → **Authorization** → **Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

Note

You should configure the template before access group settings. Refer to [***Configure Schedule and Template***](#) for details.

5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

You can view the selected person(s) and the selected access point(s) on the right side of the interface.

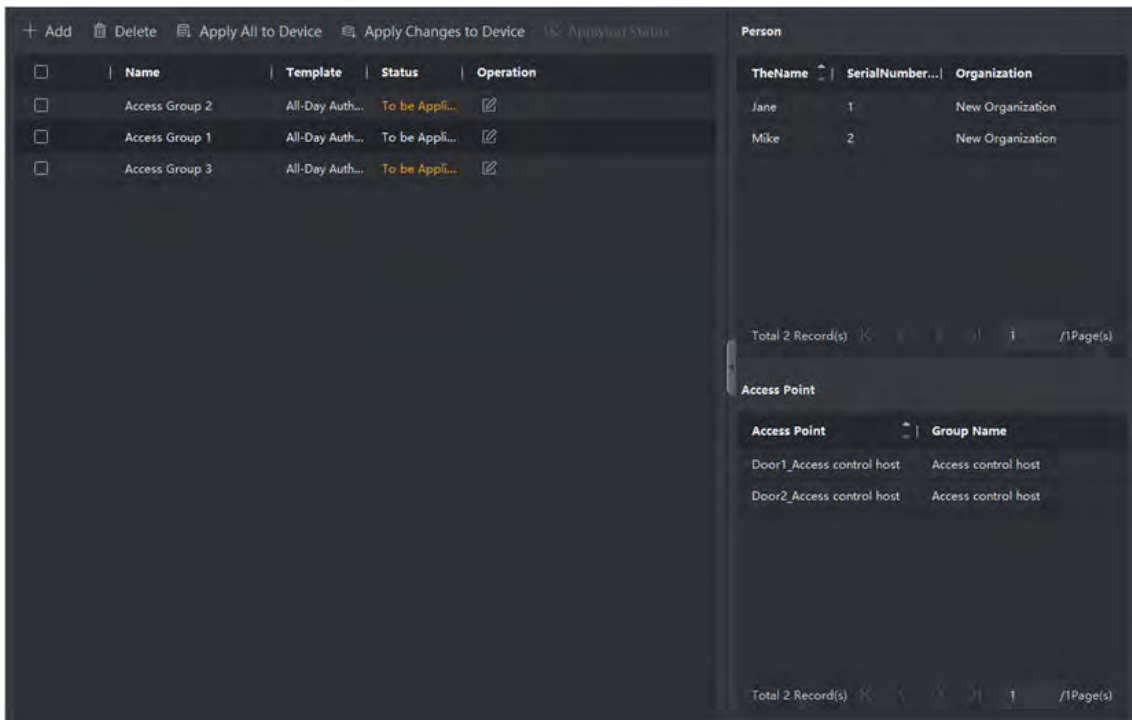


Figure 10-6 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
 - 1) Select the access group(s) to apply to the access control device.
 - 2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
 - 3) Click **Apply All to Devices** or **Apply Changes to Devices**.

Apply All to Devices

This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

Apply Changes to Devices


This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).

- 4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

Note

You can check **Display Failure Only** to filter the applying results.

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click  to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client. You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.

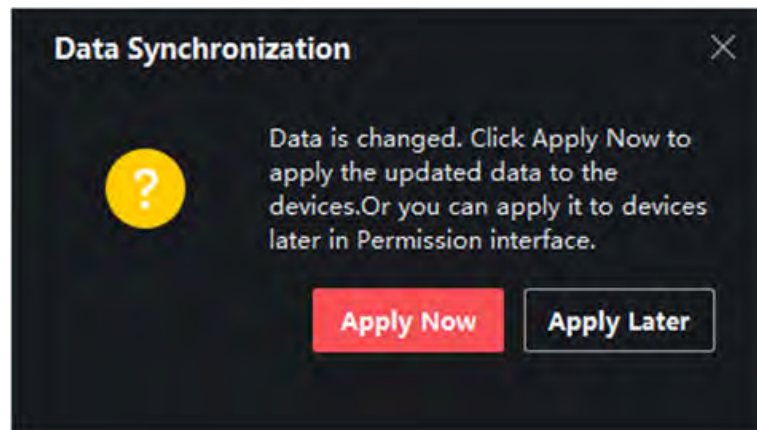



Figure 10-7 Data Synchronization

10.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), only the card(s) with access group applied will be listed when adding cards.
 - The advanced functions should be supported by the device.
 - Hover the cursor on the Advanced Function, and then Click  to customize the advanced function(s) to be displayed.
-

10.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters, including overlaying user information on picture, uploading pictures after capturing, saving captured pictures, etc.


Before You Start

Add access control device to the client.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .



If you can not find Device Parameter in the Advanced Function list, hover the cursor on the Advanced Function, and then Click  to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.



- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

RS-485 Comm. Redundancy

You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

If you enable this function, the voice prompt is enabled in the device. You can hear the voice prompt when operating in the device.

Upload Pic. After Linked Capture

Upload the pictures captured by linked camera to the system automatically.

Save Pic. After Linked Capture

If you enable this function, you can save the picture captured by linked camera to the device.

Press Key to Enter Card Number

If you enable this function, you can input the card No. by pressing the key.

Wi-Fi Probe

If you enable this function, the device can probe the surrounding communication devices' MAC address and upload the MAC address to the system. If the MAC address match the specified MAC address, the system can trigger some linkage actions.

3G/4G

If you enable this function, the device can communicate in 3G/4G network.

NFC Anti-Cloning

If you enable this function, you cannot use the cloned card for authentication and further enhance security.


4. Click **OK**.

5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door

After adding the access control device, you can configure its access point parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. Select an access control device on the left panel, and then click  to show the doors of the selected device.
3. Select a door to show its parameters on the right page.
4. Edit the door or floor parameters.



Note

- The displayed parameters may vary for different access control devices.
- Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.

Name

Edit the card reader name as desired.

Door Contact

You can set the door sensor as remaining closed or remaining open. Usually, it is remaining closed.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Door Locked Time

After swiping the normal card and relay action, the timer for locking the door starts working.

Door Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Super Password

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

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.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).



Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

5. Click **OK**.

6. **Optional:** Click **Copy to** , and then select the door to copy the parameters in the page to the selected doors.




Note

The door's status duration settings will be copied to the selected door as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** .
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.



Note

- The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.
 - Some of the following parameters are not listed in the Basic Information page, click **More** to edit the parameters.
-

Name

Edit the card reader name as desired.

Minimum Card Swiping Interval

If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

Alarm of Max. Failed Attempts

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

Max. Times of Card Failure

Set the max. failure attempts of reading card.

Card Reader Type/Card Reader Description

Get card reader type and description. They are read-only.

Default Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

4. Click **Advanced** and you can configure more parameters.

Enable Card Reader

Enable the function and you can operate the functions below on the card reader.

OK LED Polarity/Error LED Polarity/Buzzer Polarity

Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

Max. Interval When Entering PWD

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

Tampering Detection

Enable the anti-tamper detection for the card reader.

Fingerprint Recognition Level

Select the fingerprint recognition level from the drop-down list.

Fingerprint Recognition Interval

Select the fingerprint recognition interval from the drop-down list.

5. Click **OK**.

6. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).


Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control** → **Advanced Function** → **Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click  to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

Name

Edit the card reader name as desired.

Alarm Output Active Time

How long the alarm output will last after triggered.

4. Click **OK**.

5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

10.7.2 Configure Remaining Unlocked/Locked

You can set the status of the door as unlocked or locked and set the elevator controller as free and controlled. For example, you can set the door remaining locked in the holiday, and set the door remaining unlocked in the specified period of the work day.

Before You Start

Add the access control devices to the system.



Steps

1. Click **Access Control** → **Advanced Function** → **Remain Locked/Unlocked** to enter the Remain Locked/Unlocked page.
2. Select the door or elevator controller that need to be configured on the left panel.
3. To set the door or elevator controller status during the work day, click the **Week Schedule** and perform the following operations.
 - 1) For door, click **Remain Unlocked** or **Remain Locked**.

- 2) For elevator controller, click **Free** or **Controlled**.
- 3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to each day in the week schedule.

- 4) **Optional:** Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
- 5) Click **Save**.






Related Operations

- | | |
|---------------------------|---|
| Copy to Whole Week | Select one duration on the time bar, click Copy to Whole Week to copy all the duration settings on this time bar to other week days. |
| Delete Selected | Select one duration on the time bar, click Delete Selected to delete this duration. |
| Clear | Click Clear to clear all the duration settings in the week schedule. |

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
 - 1) Click **Remain Unlocked** or **Remain Locked**.
 - 2) Click **Add**.
 - 3) Enter the start date and end date.
 - 4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

Note

Up to 8 time durations can be set to one holiday period.

- 5) Perform the following operations to edit the time durations.
 - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .
 - Click the time duration and directly edit the start/end time in the appeared dialog.
 - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 6) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
 - 7) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
 - 8) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.
 - 9) Click **Save**.
5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

10.7.3 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
 - Up to 5 custom Wiegands can be set.
 - For details about the custom Wiegand, see Custom Wiegand Rule Descriptions.
-

1. Click **Access Control** → **Advanced Function** → **Custom Wiegand** to enter the Custom Wiegand page.
 2. Select a custom Wiegand on the left.
 3. Create a Wiegand name.
-

Note

Up to 32 characters are allowed in the custom Wiegand name.

4. Click **Select Device** to select the access control device for setting the custom wiegand.
 5. Set the parity mode according to the property of the third party card reader.
-

Note

- Up to 80 bits are allowed in the total length.
 - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
 - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
-
6. Set output transformation rule.
 - 1) Click **Set Rule** to open the Set Output Transformation Rules window.

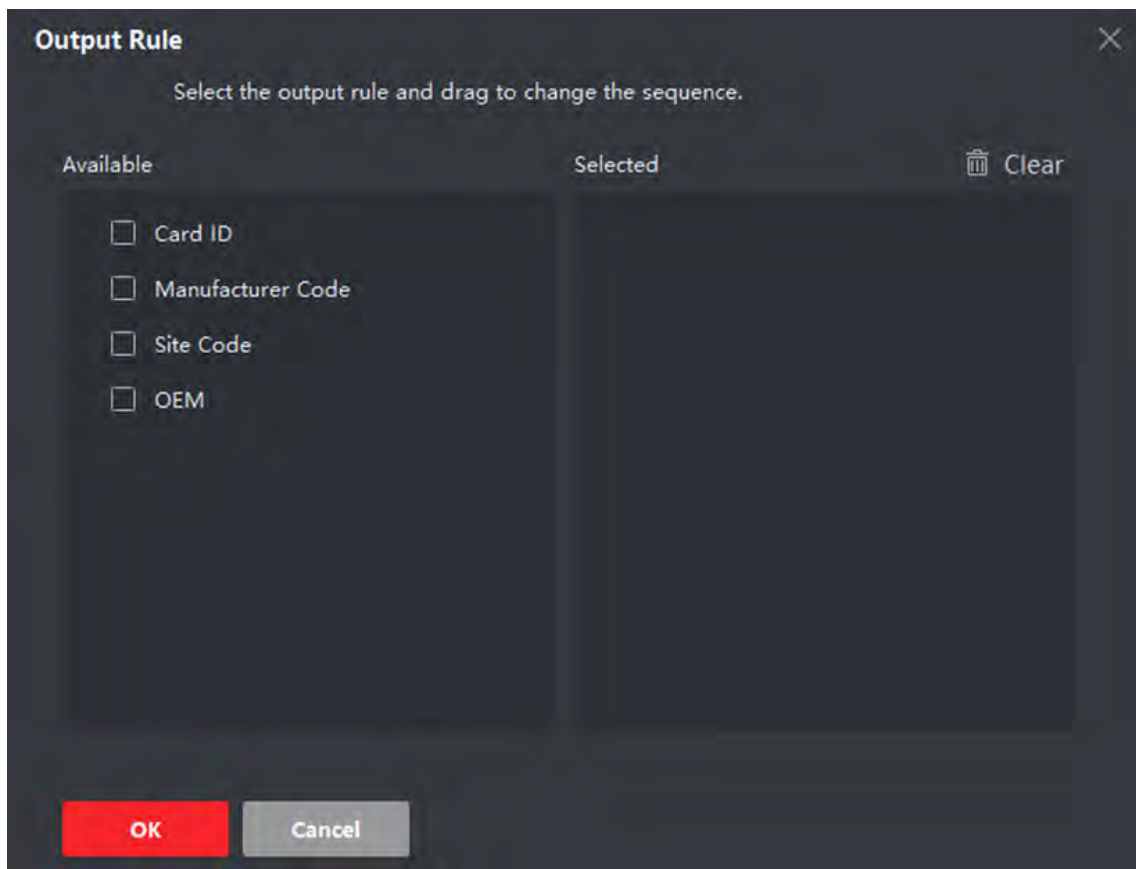


Figure 10-8 Set Output Transformation Rule

2) Select rules on the left list.

The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.

4) Click **OK**.

5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

10.7.4 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control** → **Advanced Function** → **Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.
 - 1) Click **Configuration**.

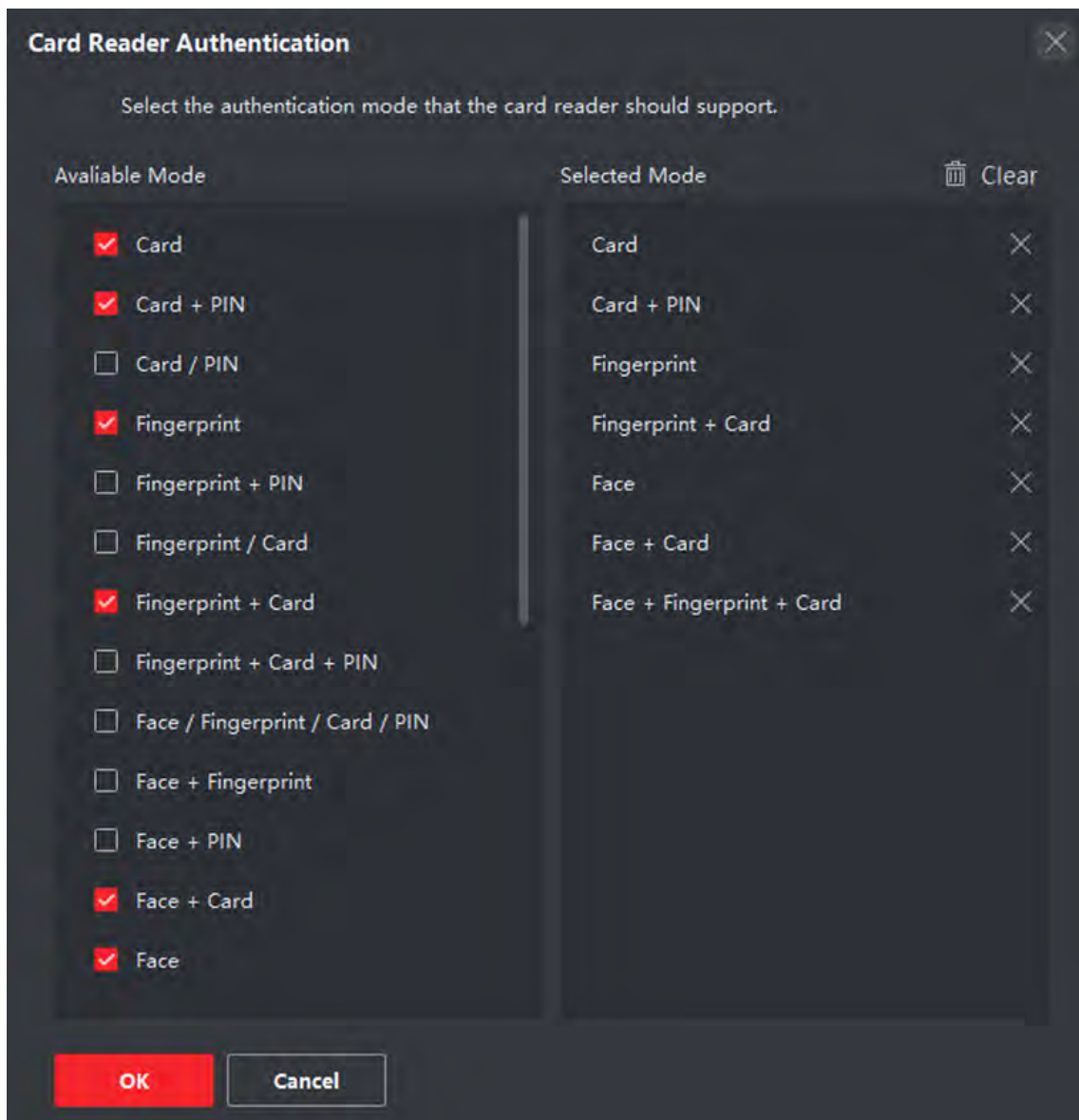


Figure 10-9 Select Card Reader Authentication Mode

 **Note**

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information*** .

- 2) Check the modes in the Available Mode list and they will be added to the selected modes list.
- 3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

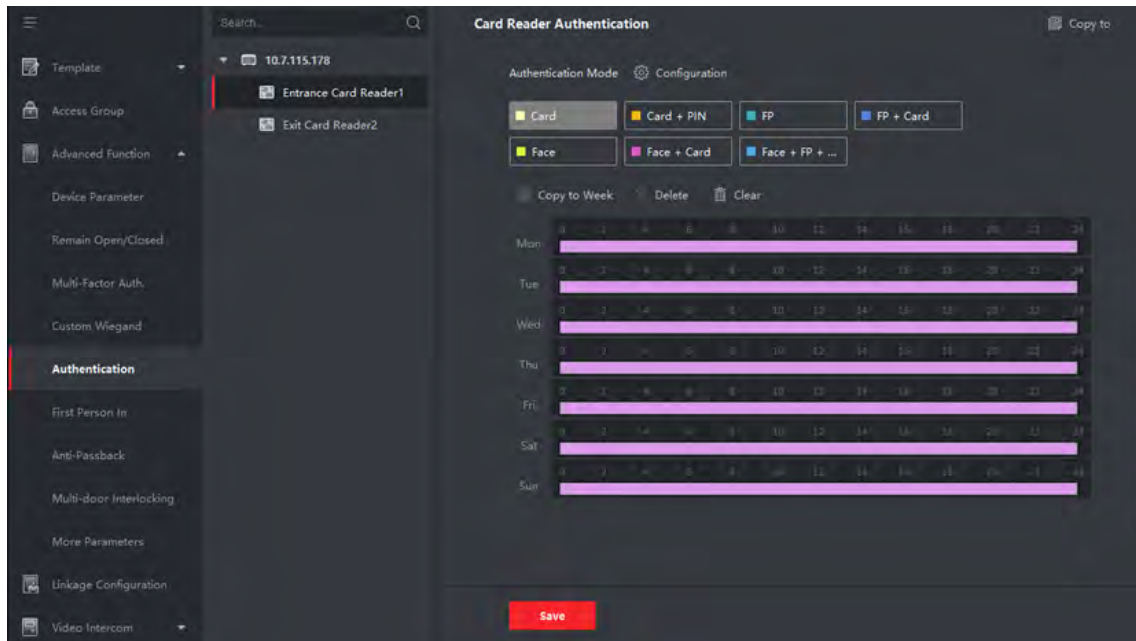


Figure 10-10 Set Authentication Modes for Card Readers

- 6. Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
- 7. Optional:** Click **Copy to** to copy the settings to other card readers.
- 8.** Click **Save**.

10.7.5 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

Set Network Parameters

After adding the access control device, you can set the device log uploading mode, and create EHome account via wired network.

Set Log Uploading Mode

You can set the mode for the device to upload logs via ISUP protocol.

Steps



Note

Make sure the device is not added by ISUP.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and enter **Network → Uploading Mode** .
4. Select the center group from the drop-down list.
5. Check **Enable** to enable to set the uploading mode.
6. Select the uploading mode from the drop-down list.
 - Enable **N1** or **G1** for the main channel and the backup channel.
 - Select **Close** to disable the main channel or the backup channel



- The main channel and the backup channel cannot enable N1 or G1 at the same time.
- N1 refers to wired network.

-
7. Click **Save**.

Create EHome Account in Wired Communication Mode

You can set the account for EHome protocol in wired communication mode. Then you can add devices via EHome protocol.

Steps



- This function should be supported by the device.
- Make sure the device is not added by EHome.

-
1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
 3. Select an access control device in the device list and enter **Network → Network Center** .
 4. Select the center group from the drop-down list.
 5. Select the **Address Type** as **IP Address** or **Domain Name**.
 6. Enter IP address or domain name according to the address type.
 7. Enter the port number for the protocol.



The port number of the wireless network and wired network should be consistent with the port number of EHome.

-
8. Select the **Protocol Type** as **EHome** and select EHome version.



If set the EHome version as **5.0**, you should create an EHome key for the EHome account.

-
9. Set an account name for the network center.
 10. Click **Save**.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps



The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption Verification** to enter the M1 Card Encryption Verification page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.



- The sector ID ranges from 1 to 100.
 - By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.
-

6. Click **Save** to save the settings.

Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Before You Start

Add access control device to the client, and make sure the device supports RS-485 interface.

Steps

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity type, communication mode, working mode, and connection mode in the drop-down list.



When the connection mode is **Connect Access Control Device**, you can select **Card No.** or **Person ID** as the output type.

6. Click **Save**.

- The configured parameters will be applied to the device automatically.
- When you change the working mode or connection mode, the device will reboot automatically.

Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode. After setting the Wiegand parameters, the device can connect to Wiegand card reader via Wiegand communication.

Steps



This function should be supported by the device.

1. Enter the Access Control module.
 2. On the navigation bar on the left, enter **Advanced Function → More Parameters**.
 3. Select an access control device in the device list and click **Wiegand** to enter the Wiegand Settings page.
 4. Set the switch to on to enable the Wiegand function for the device.
 5. Select the Wiegand channel No. and the communication mode from the drop-down list.
-



If you set **Communication Direction** as **Sending**, you are required to set the **Wiegand Mode** as **Wiegand 26, Wiegand 34, Wiegand 27, or Wiegand 35**.

6. Click **Save**.
 - The configured parameters will be applied to the device automatically.
 - After changing the communication direction, the device will reboot automatically.

10.8 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

10.8.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is via the client by configuring client actions for the access event. Client actions here refer to the actions automatically executed by the client itself, such as making an audible warning and sending an email. Once an event is triggered, the client will notify the security personnel, so that he/she can handle the event in time.

Before You Start

Add access control device to the client.

Steps

1. Click *Event Configuration* → *Access Control Event* .

The added access control devices will display in the device list.

2. Select a resource (including device, alarm input, door, and card reader) from the device list.

The event types which the selected resource supports appear.

3. Select the event(s) and click *Edit Priority* to define the priority for the event(s), which can be used to filter events in the Event Center.

4. Set the linkage actions of the event.

1) Select the event(s) and click **Edit Linkage** to set the client actions when the event(s) are triggered.

Audible Warning

The client software gives an audible warning when the event is triggered. You can select alarm sound for the audible warning.



For details about setting the alarm sound, refer to *Set Alarm Sound* in the user manual of the client software.

Send Email

Send an email notification about the event to one or more receivers.

For details about setting email parameters, refer to *Set Email Parameters* in the user manual of the client software.

2) Click **OK**.

5. Enable the event so that when the event is detected, event will be sent to the client and the linkage actions will be triggered.

6. Optional: Click *Copy to* to copy the event settings to other access control device, alarm input, door, or card reader.

10.8.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps



It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.

10.8.3 Configure Device Actions for Card Swiping

You can set the access control device's linkage actions for the specified card swiping. When you swipe the specified card, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps



It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Card Linkage**.
5. Enter the card number or select the card from the dropdown list.

6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

8. Click **Save**.

When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

10.8.4 Configure Device Actions for Person ID

You can set the access control device's linkage actions for the specified person ID. When access control device detects the specified person ID, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps



It should be supported by the device.

1. Click **Access Control** → **Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Person Linkage**.
5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

8. Click **Save**.

9. **Optional:** After adding the device linkage, you can do one or more of the following:

Delete Linkage Settings	Select the configured linkage settings in the device list and click Delete to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

10.9 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management***.

10.9.1 Control Door Status

You can control the status for a single door, including opening door, closing door, remaining the door open, and remaining the door closed.

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

Note

For managing the access point group, refer to *Group Management* in the user manual of the client software.

The doors in the selected access control group will display.

3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.
4. Click the following buttons to control the door.

Open Door

When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

Close Door

When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

Remain Open

The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

Remain Closed

The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.



The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

10.9.2 Check Real-Time Access Records

The access records will display in real time, including card swiping records, fingerprint comparison records, etc. You can view the person information and view the picture captured during access.

Steps

1. Click **Monitoring** and select a group from the drop-down list on the upper-right corner.
The access records triggered at the doors in the selected group will display in real time. You can view the details of the records, including card No., person name, organization, event time, etc.
2. **Optional:** Check the event type and event status so that these events will show in the list if the events are detected. The events of unchecked type or status will not be displayed in the list.
3. **Optional:** Check **Show Latest Event** and the latest access record will be selected and displayed at the top of the record list.
4. **Optional:** Click the event to view the accessed person details, including person pictures (captured picture and profile), person No., person name, organization, phone, contact address, etc.



You can double click the captured picture to enlarge it to view the details.

5. **Optional:** Right click on the column name of the access event table to show or hide the column according to actual needs.

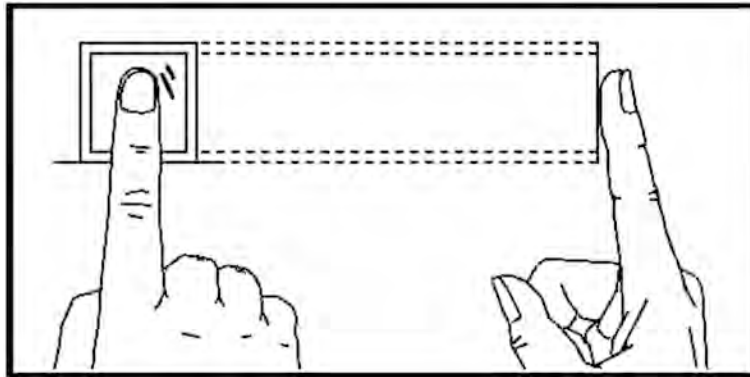
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

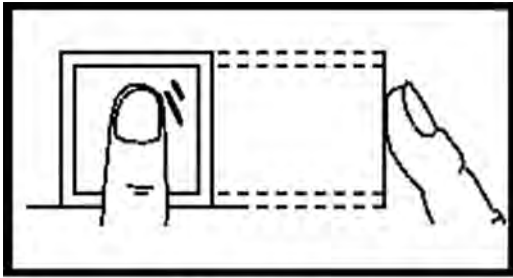
The figure displayed below is the correct way to scan your finger:



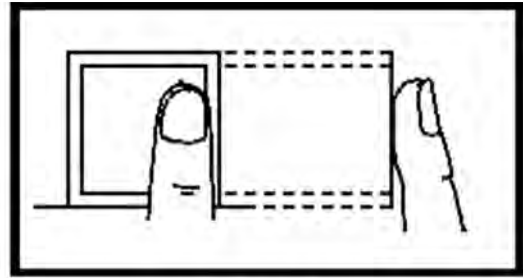
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

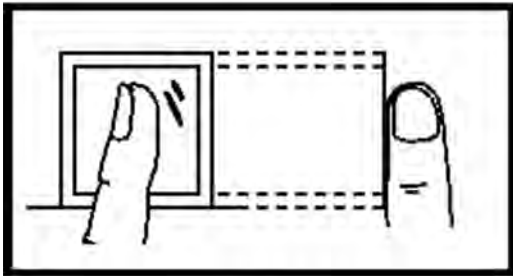
The figures of scanning fingerprint displayed below are incorrect:



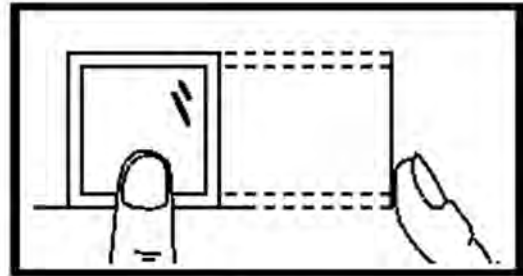
Vertical



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.

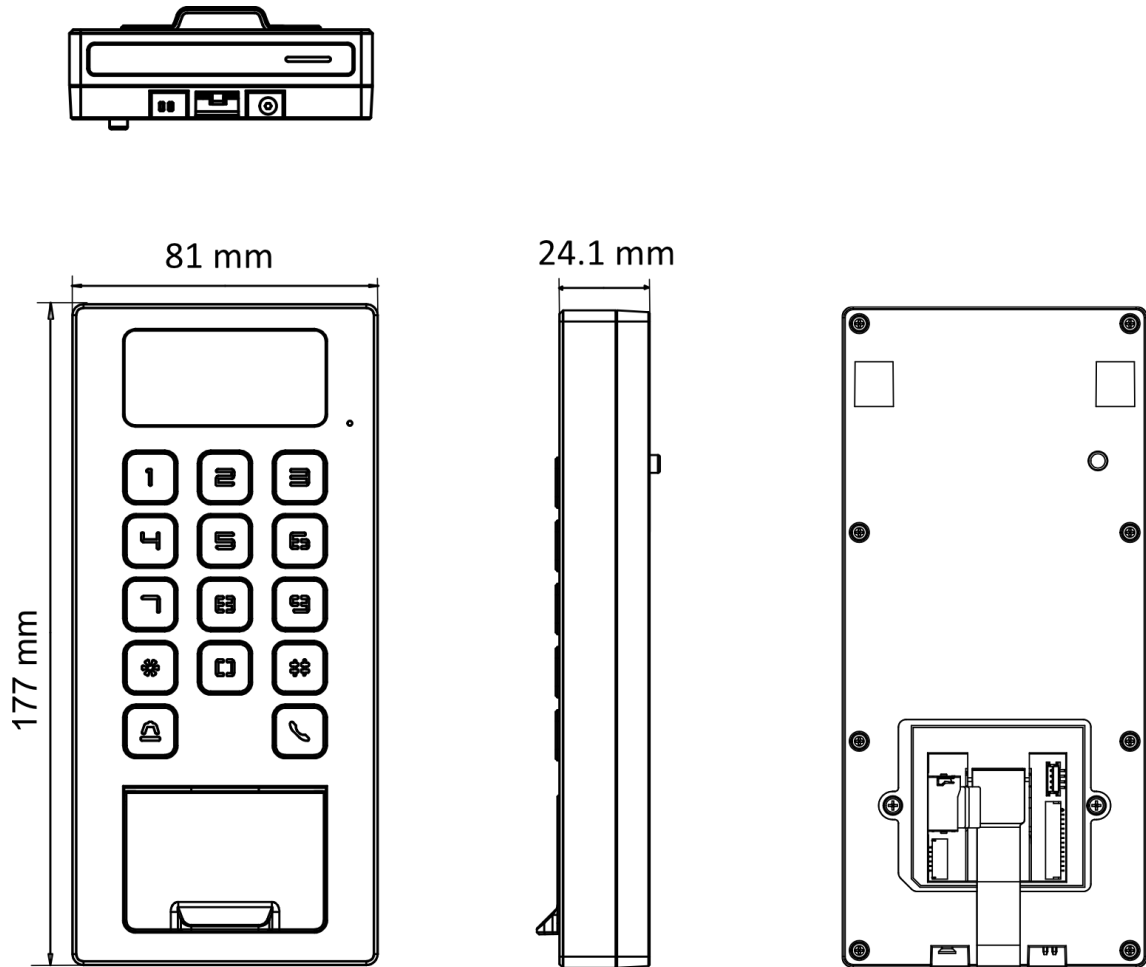
Others

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



Appendix C. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure C-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure C-2 Device Command



See Far, Go Further