HIKVISION

Access Control Terminal

User Manual

Legal Information

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 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 INSPECTION, 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 LATER 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.
ℹ **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, RE Directive 2014/53/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

- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- An all-pole mains switch shall be incorporated in the electrical installation of the building.
- 1. This equipment is not suitable for use in locations where children are likely to be present.
  2. CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
  3. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
  4. Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
  5. Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
  6. Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
  7. Dispose of used batteries according to the instructions.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- 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.
- 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

- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- The USB port of the equipment is used for connecting to a mouse, a keyboard, or a USB flash drive only.
- The serial port of the equipment is used for debugging only.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- 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.

Available Model

Product Name	Model
Access Control Terminal	DS-K1T105AM
	DS-K1T105AE
	DS-K1T201AMF
	DS-K1T201AEF

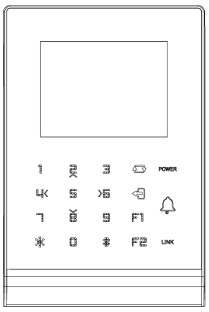
Use only power supplies listed in the user instructions:

Model	Manufacturer
KPL-050F-VI	Channel Well Technology Co Ltd.

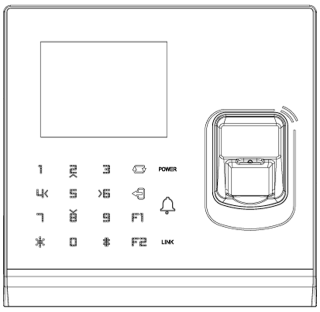
Contents

Chapter 1 Overview

1.1 Introduction



DS-K1T105A is a series of standalone access control terminal with a 2.8-inch LCD display screen. It supports smart card recognition TCP/IP communication method, Wi-Fi communication method, and also supports offline operation.



DS-K1T201A series is an optical fingerprint access control terminal with multiple advanced technologies including fingerprint recognition, Wi-Fi, card recognition, 2.8-inch LCD display screen. It is equipped with optical fingerprint recognition module, and supports offline operation.

1.2 Features

1.2.1 Features of Device without Fingerprint Module

- Doorbell ringtone settings function.
- Touch mode and blue light display technique for keypad.
- Stand-alone settings for the device.
- 2.8-inch LCD display screen.
- Transmission modes of wired network (TCP/TP) and Wi-Fi.
- Supports multiple door opening modes (card, card + password, exit button, etc.).
- Supports RS-485 communication for connecting to external card reader.
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller.
- Max. 100,000 valid card No., and Max. 300,000 access control events records storage.
- Supports EM card reading (supported by device that can read EM card).
- Supports M1 card reading, including card No. reading, & writing function (supported by device that can read M1 card).

- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, and duress card alarm.
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the terminal.
- Data can be permanently saved after power-off.

1.2.2 Features of Device with Fingerprint Module

- Doorbell ringtone settings function.
- Touch mode and blue light display technique for keypad.
- Stand-alone settings for the device.
- 2.8-inch LCD display screen.
- Transmission modes of wired network (TCP/TP) and Wi-Fi.
- Supports RS-485 communication for connecting external card reader.
- Supports working as a card reader, and supports Wiegand interface and RS-485 interface for accessing the controller.
- Max. 10,000 card No., Max. 300,000 access control events records, and Max. 5000 fingerprints storage.
- Adopts the optical fingerprint module, supporting 1:N mode (fingerprint, card + fingerprint) and 1:1 mode (card + fingerprint).
- Supports multiple authentication modes (card, fingerprint, card + fingerprint, card + password, fingerprint + password, card + fingerprint + password, and so on).
- Supports EM card reading (supported by device that can read EM card).
- Supports M1 card reading, including card No. reading, and sector reading & writing (supported by device that can read Mifare card).
- Tampering detection, unlocking overtime alarm, invalid card swiping over times alarm, duress card alarm, and so on.
- Accurate data and time display provided by built-in electronic clock and watchdog program to ensure the basic function of the device.
- Data can be permanently saved after power-off.

Chapter 2 Appearance

2.1 Appearance of Access Control Terminal without Fingerprint Module

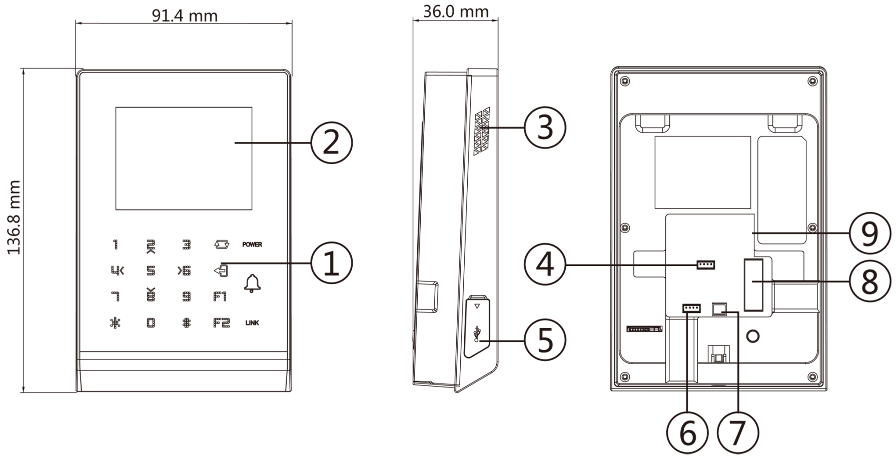


Figure 2-1 Diagram of Access Control Terminal Appearance (Without Fingerprint Module)

Table 2-1 Description of Access Control Terminal (Without Fingerprint Module)

No.	Description
1	Keypad
2	Display Screen
3	Loudspeaker
4	MDEBUG Debugging Port (for debugging use only)
5	USB Interface
6	SDEBUG Debugging Port (for debugging use only)
7	Power Interface
8	Wiring Terminal
9	Network Interface

2.2 Appearance of Access Control Terminal with Fingerprint Module

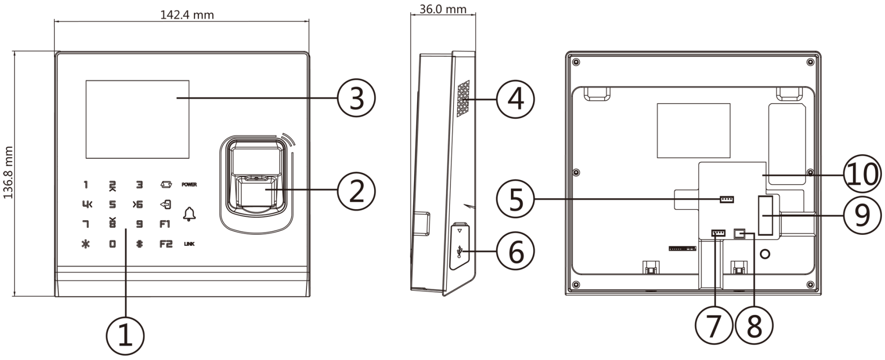


Figure 2-2 Diagram of Access Control Terminal Appearance (With Fingerprint Module)

Table 2-2 Description of Access Control Terminal (With Fingerprint Module)

No.	Description
1	Keypad
2	Fingerprint Module/Card Presenting Area
3	Display Screen
4	Loudspeaker
5	MDEBUG Debugging Port (for debugging only)
6	USB Interface
7	SDEBUG Debugging Port (for debugging use only)
8	Power Interface
9	Wiring Terminal
10	Network Interface

2.3 Appearance Description

View the device keypad's description.

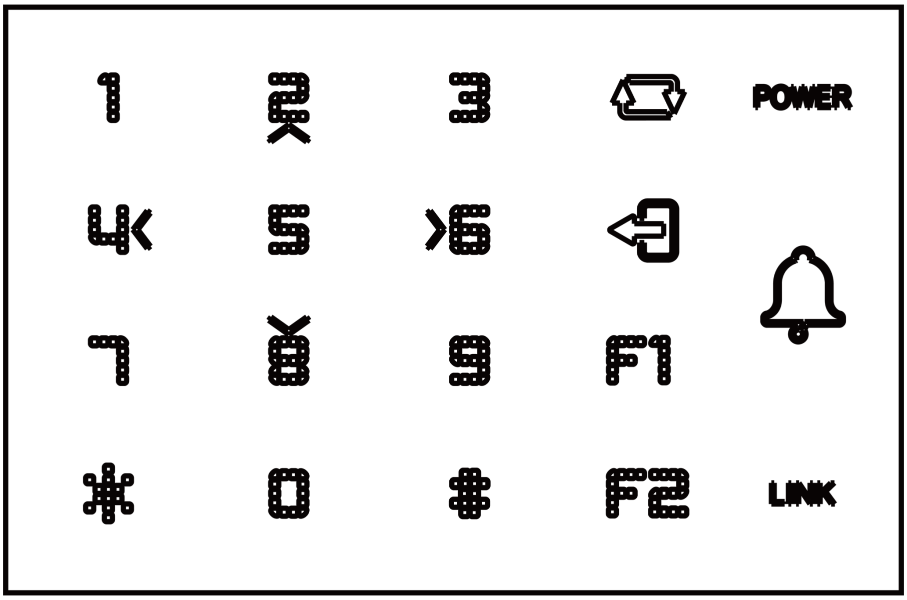


Figure 2-3 Keypad Diagram

Note

The pictures here are for reference only. Some models do not support card swiping function. For details, refer to the actual product.

Table 2-3 Keypad Description

Button	Description
⇄	Shift between numeric key and direction key on the non-initial page.
0~9	Numeric Key: Enter numbers/lowercases, numbers/uppercases and symbols in the textbox. When entering non-numeric characters, 0 can be a space key.
*	Exiting key.
#	Hold the key to enter the login page. Press the key to confirm. After login, the key can be a confirmation or selection key.
⌫	Deleting key. Press to delete contents in the textbox.
POWER	Power status indicator. Solid Blue: Normal Power; Off: Power Exception
LINK	Solid Blue: Present normal card/Network or Wi-Fi is connected/Client software is armed. Flashing Blue: Card reader mode.

Button	Description
	Solid Red: Present illegal card. Off: Network or Wi-Fi is disconnected/Client software is not armed.
F1	Editing key. Press to shift among numbers/lowercases, numbers/ uppercases and symbols.
F2	Reserved.

Chapter 3 Installation

3.1 Install Access Control Terminal (Without Fingerprint Module)

Before You Start

Make sure that the wall is strong enough to withstand three times the weight of the device.

Steps

1. Install the 86 gang box into the wall.

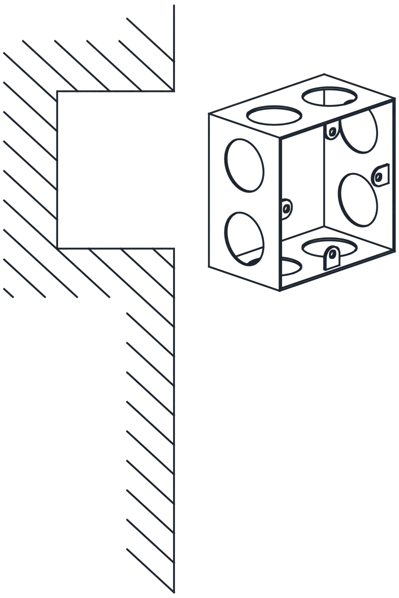


Figure 3-1 Install 86 Gang box

2. Secure the device mounting plate on the gang box with 2 screws (supplied).

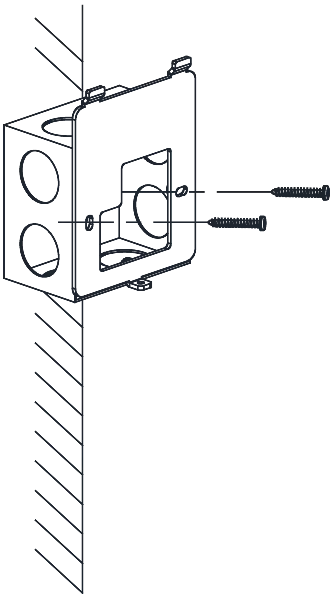


Figure 3-2 Install Mounting Plate

3. Route the cables through the cable hole of the mounting plate and connect the cables with the connecter on the rear panel of the device.
4. Align the terminal with mounting plate.
5. Buckle the terminal on the plate.

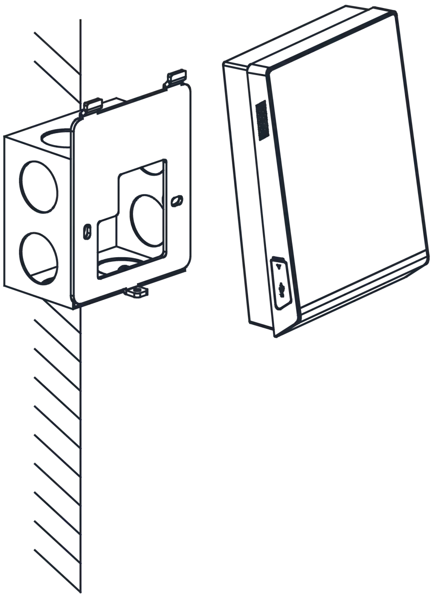


Figure 3-3 Buckle Terminal on Plate

6. Tighten the screw to fix the terminal on the mounting plate and complete the installation.

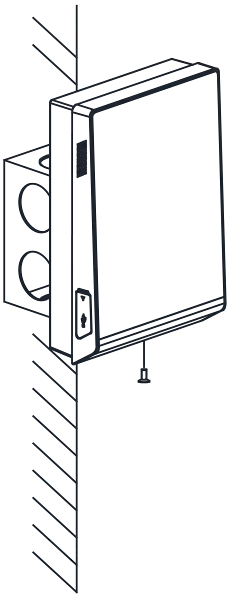


Figure 3-4 Tighten Screw

3.2 Install Access Control Terminal (With Fingerprint Module)

Before You Start

Make sure that the wall is strong enough to withstand three times the weight of the device.

Steps

1. Install the 86 gang box into the wall.

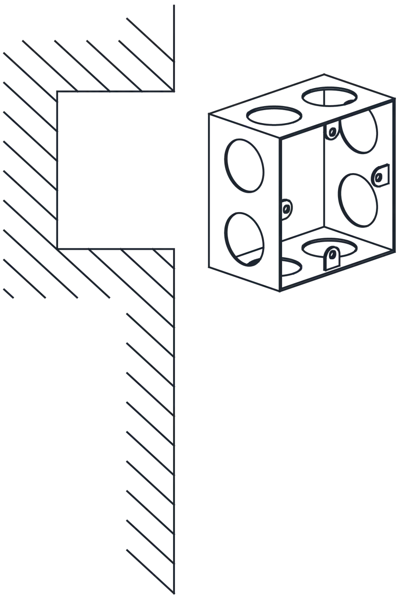


Figure 3-5 Install 86 Gang box

2. Secure the device mounting plate on the gang box with 2 screws (supplied).

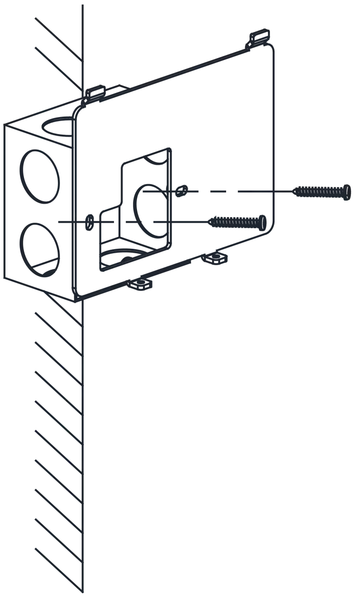


Figure 3-6 Install Mounting Plate

3. Route the cables through the cable hole of the mounting plate and connect the cables with the connecter on the rear panel of the device.

4. Align the terminal with mounting plate.

5. Buckle the terminal on the plate.

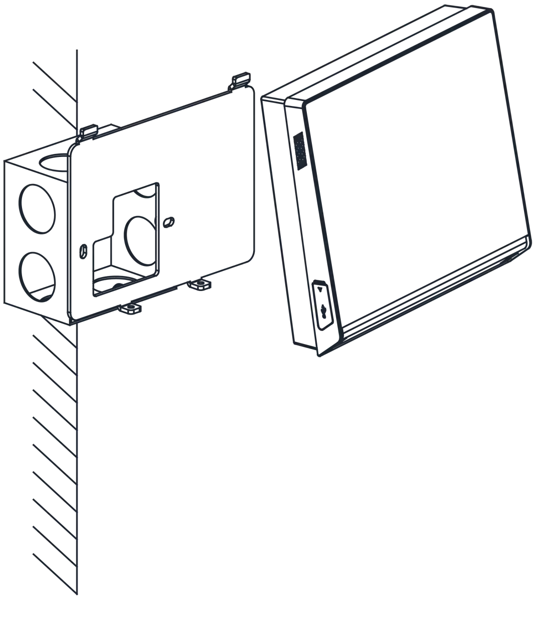


Figure 3-7 Buckle Terminal on Plate

6. Tighten the screws to fix the terminal on the mounting plate and complete the installation.

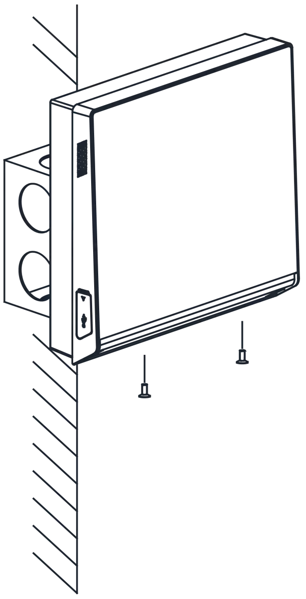


Figure 3-8 Tighten Screws

Chapter 4 Wiring

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

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

Note

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

4.1 Terminal Description

You can view the terminal names of the access control terminal and their detailed information, including the terminal function, cable color, terminal name, etc.

The terminals diagram is as follows:

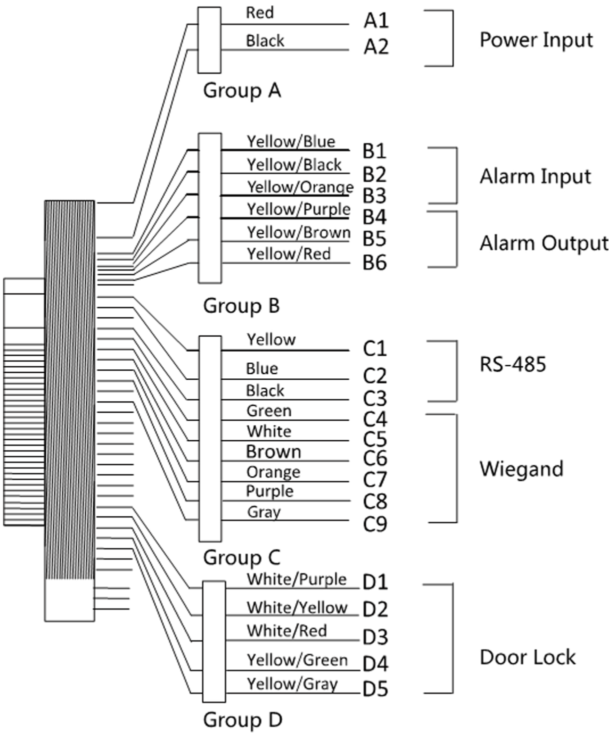


Figure 4-1 Terminal Diagram

The description of each terminal are as follows:

Table 4-1 Terminal Descriptions

Line Group	No.	Function	Color	Terminal Name	Description
Line Group A	A1	Power Input	Red	+12V	12 V DC Power Supply
	A2		Black	GND	GND
Line Group	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	GND
	B3		Yellow/Orange	IN2	Alarm Input2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Line Group C	C1	RS-485 Communication Port	Yellow	485 +	RS-485 Wiring
	C2		Blue	485 -	
	C3		Black	GND	

Line Group	No.	Function	Color	Terminal Name	Description
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Indicator of Card Reader Control Output (Valid Card Output)
	C7		Orange	WG_ERR	Indicator of Card Reader Control Output (Invalid Card Output)
	C8		Purple	BUZZER	Buzzer Wiring
	C9		Grey	TAMPER	Tampering Alarm Wiring
Line Group D	D1	Lock	White/Purple	NC	Lock Wiring
	D2		White/Yellow	COM	
	D3		White/Red	NO	
	D4		Yellow/Green	SENSOR	Door Contact Signal Input
	D5		Yellow/Grey	BUTTON	Exit Door Wiring

4.2 Access Control Terminal Wiring

You can wire the external devices, including power supply, the alarm input devices, the alarm output devices, the security control panel, the Wiegand card, the door lock, the door contact, and the exit button, with the access control terminal according to the following diagram.

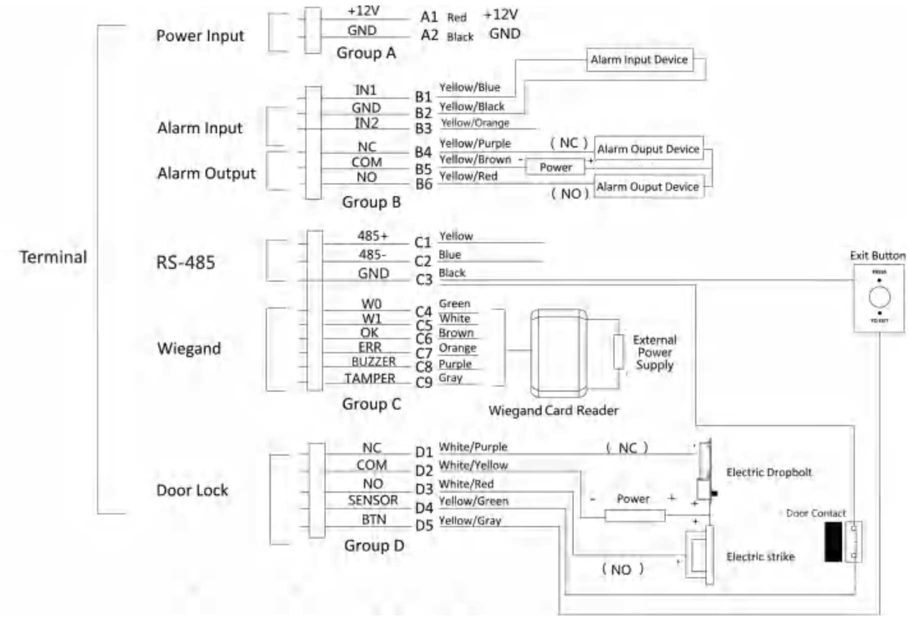


Figure 4-2 Wiring Overview

- When connecting door contact and exit button, the device and the RS-485 card reader should use the common ground connection.
- You should set the face recognition terminal's Wiegand direction as **Input** to connect to a Wiegand card reader. If connects to an access controller, you should set the Wiegand direction as **Output** to transmit authentication information to the access controller.
- For details about Wiegand direction settings, see ***Set Wiegand Parameters*** .
- The suggested external power supply for door lock is 12 V, 1 A. The suggested external power supply for the Wiegand card reader is 12 V, 1 A.
- Do not wire the device to the electric supply directly.

4.3 RS-485 Card Reader Wiring

You can connect the access control terminal with the external RS-485 card reader by wiring the RS-485 cables and the external power supply cables with the RS-485 card reader.

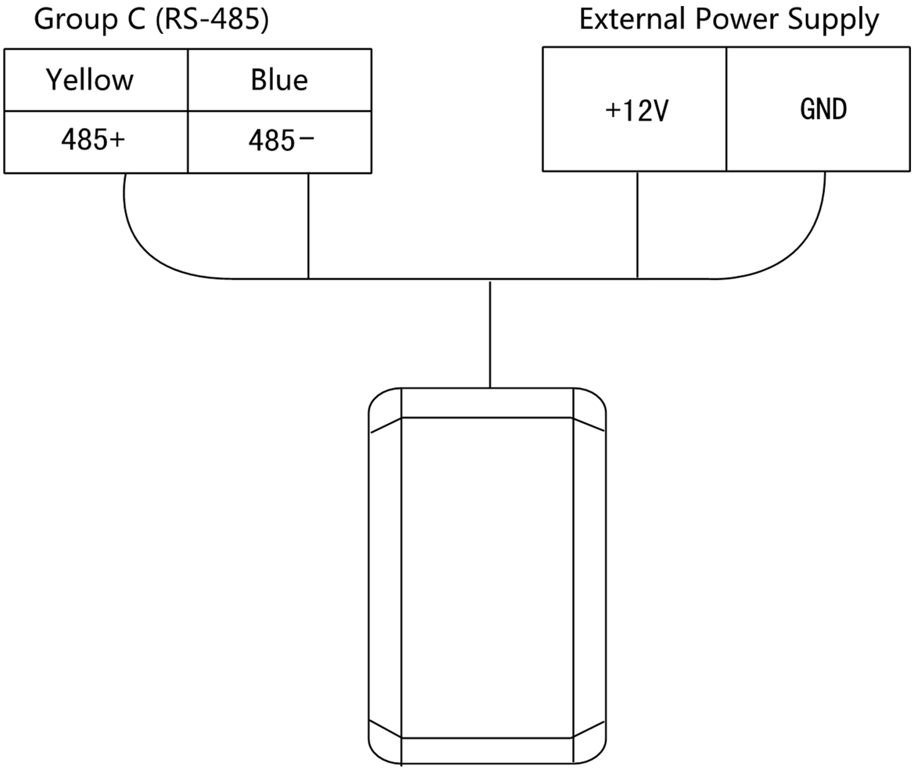


Figure 4-3 Wiring of External RS-485 Card Reader

4.4 Wiegand Card Reader Wiring

You can connect the access control terminal with the external Wiegand card reader by wiring the Wiegand cables and the external power supply cables with the Wiegand card reader.

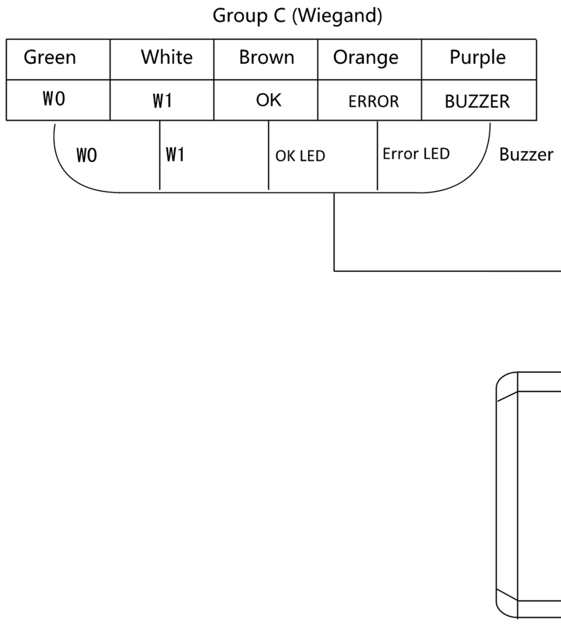


Figure 4-4 Wiring of Wiegand Card Reader

Note

- Set the dial-up of the external card reader as 2 when connected to the access control terminal.
- The external power supply and the access control terminal should use the same GND cable.

4.5 Device Wiring as RS-485 Card Reader

The access control terminal can be switched into the card reader mode. It can access to the access control as a RS-485 card reader.

Note

When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.

The wiring diagram is as follows:

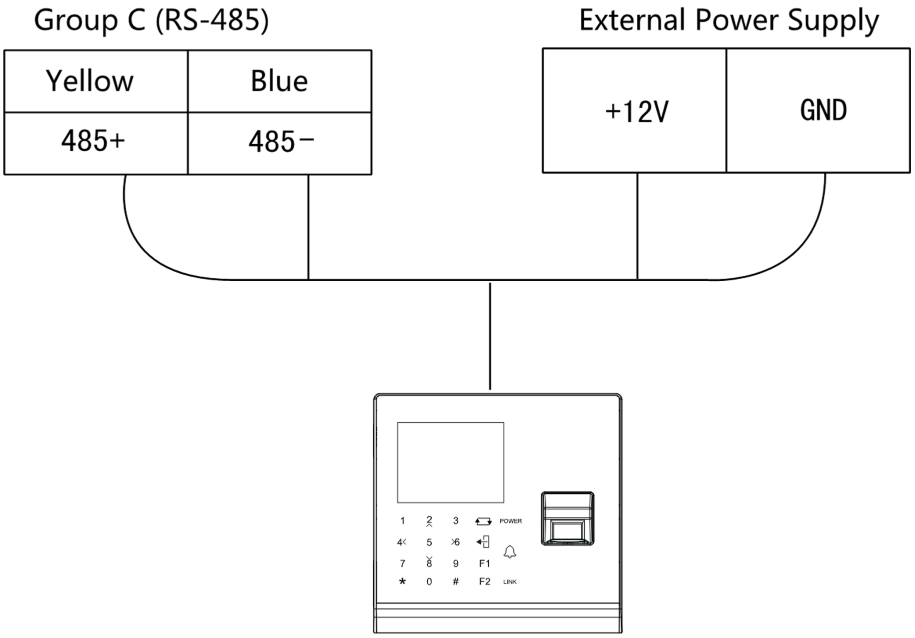


Figure 4-5 Wiring of RS-485 Output

Note

-
- When the access control terminal works as a RS-485 card reader, the default RS-485 address is 1.
- The external power supply and the access control terminal should use the same GND cable.

4.6 Device Wiring as Wiegand Card Reader

The access control terminal can access to the access control as a Wiegand card reader.

Note

When the access control terminal works as a card reader, it only supports being connected to the controller, but does not support alarm input or output, or the connection of external devices.

The wiring diagram is as follows:

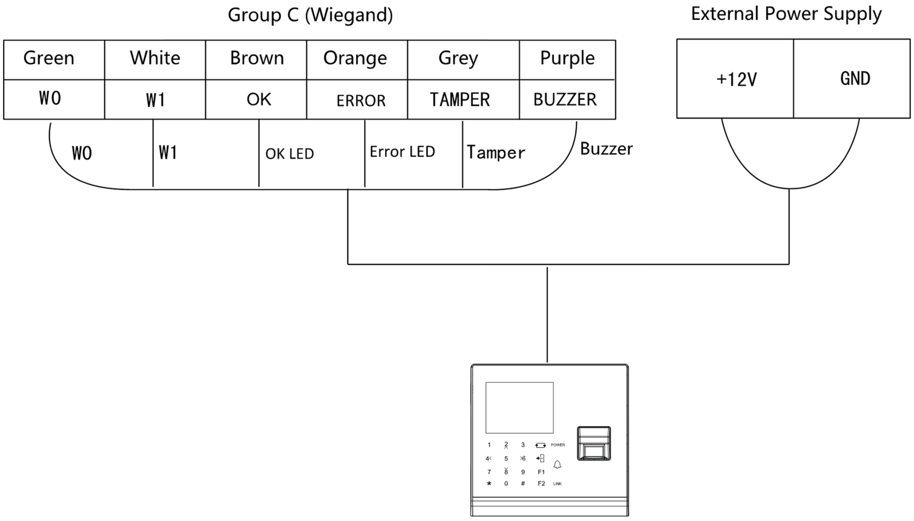


Figure 4-6 Wiring as Wiegand Card Reader

Note

- When the access control terminal works as a card reader, you must connect the WG_ERR, BUZZER and WG_OK terminals if you want to control the LED and buzzer of the Wiegand card reader.
- Set the working mode of the terminal as card reader. If the terminal is required to work as a card reader. The card reader mode support to communicate by Wiegand or RS-485.
- The distance of Wiegand communication should be no longer than 80 m.
- The external power supply and the access control terminal should use the same GND cable.

Chapter 5 Activation

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

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

The default values of the device are as follows:

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

5.1 Activate via Device

If the device is not activated before first login, the system will enter the Device Activation interface after powering on.

Steps

1. Create a device password for activation.
2. Confirm the password.

   Note

   Press the up or down key on the keypad to change the input method.

3. Press **OK** to activate the device.

   Note

   We highly recommend you to create a strong 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.

What to do next

After the device activation, you will enter the administrator adding page. Add an administrator before other operations.

5.2 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.

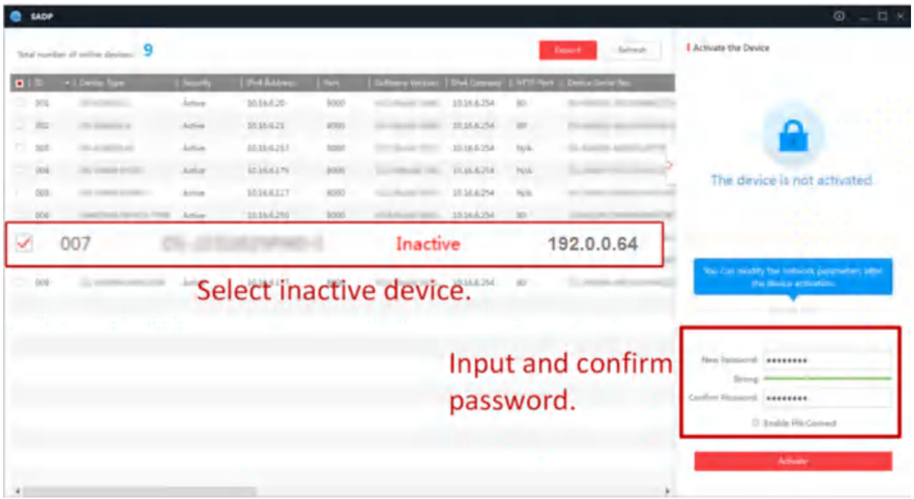
2. Find and select your device in online device list.

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.

5.3 Activate Device via Client Software

For some devices, you are required to create the password to activate them before they can be added to the 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.
7. Click **OK** to activate the device.

Chapter 6 Local Settings

6.1 Add Administrator

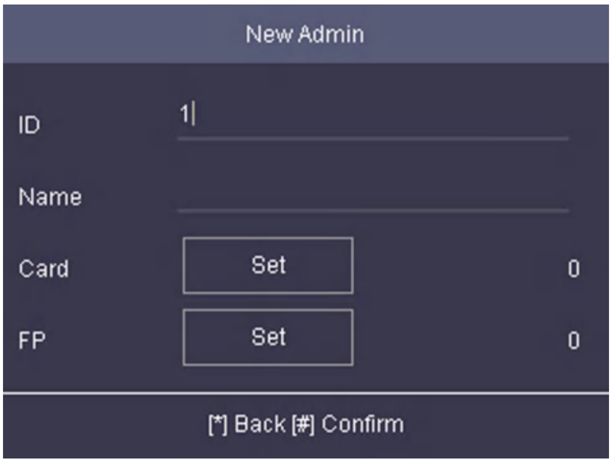
After the device activation, you are required to add an administrator. You can set the administrator's user name, the card No, and fingerprint.

Steps

Note

Parts of device models supports the fingerprint function.

1. Enter the New Admin page.



New Admin

ID 1

Name

Card Set 0

FP Set 0

[*] Back [#] Confirm

Figure 6-1 Add Administrator

2. Enter the administrator's parameters.

ID (Employee ID)

By default, the ID No. will be increased in sequence. You can edit the ID according to your preference.

Note

- The ID refers to the user attendance serial No.
- The ID should be between 1 and 99999999 and should not start with 0.
- The ID should be used for once.

Name

Enter the new user name.

Note

- Press the up or down key on the keypad to change the input method.
- Up to 64 characters are allowed in the user name.

Card

Set: Present card on the card presenting area or enter card No. manually, and select a card property.

View Info.: View the user's added card information.

Note

- The card No. is required.
- Up to 20 digits can be contained in the card No.
- The card No. can be 0.
- The card No. can start with 0 when it contains more than one numbers. E.g. 012345.
- The card No. should be used for once.

FP (Fingerprint)

On the Fingerprint page, select a target finger and record according to the voice prompt.

Note

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added to one user.
- You can also scan the fingerprints via the external fingerprint recorder and apply the fingerprints to the device by the client software.
- For detailed information about scanning the fingerprint, see ***Tips for Scanning Fingerprint*** .
- Parts of device models supports the fingerprint function.

3. Press **#** to save the settings and exit the page.

6.2 Login

Log in the device as an administrator to mange the device parameters, including the communication, the user, the access control parameters, the time, the report, the system, etc.

Hold ***** for 3 s to enter the login page. Select **FP**, **DEV PWD** (Device Password), or **Card**, and authenticate to enter the home page.

Note

- Press **F1** on the keypad to change the input method.
- The login page varies depending on different device model. When operation, refer to the actual device page.

6.3 Communication Settings

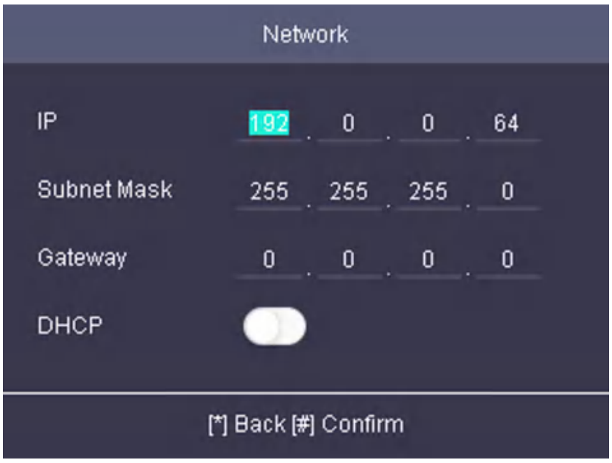
Set device wired network, RS-485, Wiegand, Wi-Fi, EHome parameters.

6.3.1 Set Wired Network

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

Steps

1. Move the cursor and select **Comm. → Wired** .
2. Press * to enter the Wired Network page.



Network

IP 192 . 0 . 0 . 64

Subnet Mask 255 . 255 . 255 . 0

Gateway 0 . 0 . 0 . 0

DHCP

Figure 6-2 Wired Network Settings

3. Edit the IP address, the subnet mask, and the gateway.

Note

The device's IP address and the PC's should be in the same network segment.

4. **Optional:** Enable **DHCP**.

   The system will automatically assign IP address for the device.
5. Press * to save the settings and exit the page.

6.3.2 Set Wi-Fi Parameters

You can enable the Wi-Fi function and you can transmit the data via Wi-Fi.

Steps

Note

The function is supported by parts of the device models.

1. Move the cursor and select **Comm. → Wi-Fi** .
2. Press * to enter the Wi-Fi page.

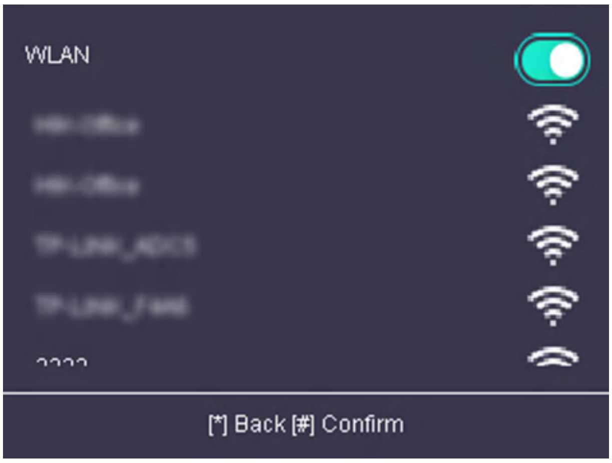


Figure 6-3 Wi-Fi Page

3. Enable the WLAN function.
4. Select a Wi-Fi from the list and set the Wi-Fi parameters, including the Wi-Fi password and DHCP.
   - Enable **DHCP**, and the system will automatically assign IP address for the Wi-Fi.
   - Disable **DHCP**, and you should set the IP address, subnet mask, and gateway.
5. Press * to save the settings and exit the page.

6.3.3 Set EHome Parameters

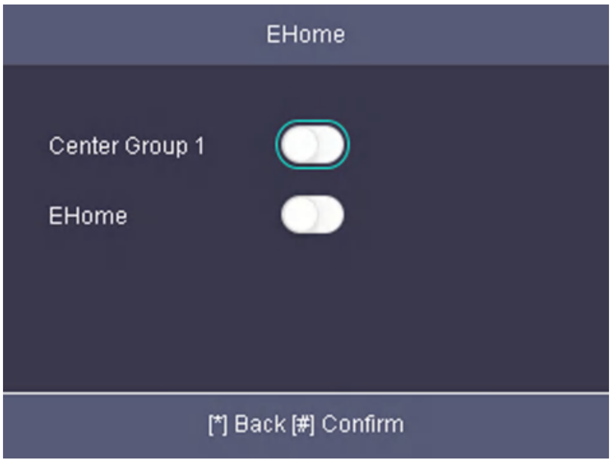
Set EHome parameters and the device can upload data via EHome protocol.

Before You Start

Make sure your device has connect to a network.

Steps

1. Move the cursor and select **Comm. → EHome** .



EHome

Center Group 1

EHome

[*] Back [#] Confirm

Figure 6-4 EHome Settings

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

   Center Group 1

   Enable center group 1 and the data will be uploaded to the center group.

   EHome

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

   Address Type

   Select an address type according to your actual needs. If you select domain name, you should configure the domain name.

   IP Address

   Set the EHome server's IP address.

   Port No.

   Set the EHome server's port No.

   Domain Name

   Set the domain name of EHome server.

   EHome Version

   Set the EHome version according to your actual needs. If you choose V5.0, you should create an account and EHome key. If you choose other version, you should create an EHome account only.

   Note

   - Remember the EHome account and EHome key. You should enter the account name or the key when the device should communicate with other platforms via EHome protocol.
   - EHome key range: 8 to 32 characters.

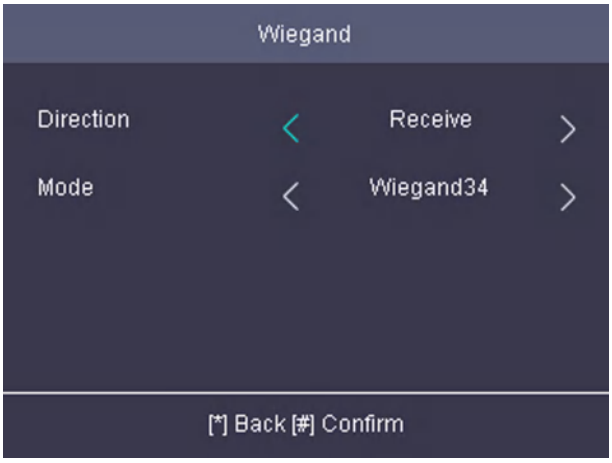
3. Press ***** and select **Yes** to save the settings and exit the page.

6.3.4 Set Wiegand Parameters

You are able to set the Wiegand direction (send/receive) and the Wiegand mode (Wiegand 26/ Wiegand 34).

Steps

1. Move the cursor and select **Comm. → Wiegand** .



Wiegand

Direction < Receive >

Mode < Wiegand34 >

[*] Back [#] Confirm

Figure 6-5 Wiegand Settings

2. Set the Wiegand parameters.

   Direction

   Send

   The device can connect to the access controller to upload the card No. bia the Wiegand 26 or the Wiegand 34 mode.

   Receive

   The terminal can connect to the Wiegand card readers. No need to configure the Wiegand mode.

   Mode

   Wiegand 26 and Wiegand 34 can be selected. The default Wiegand mode is Wiegand 34.

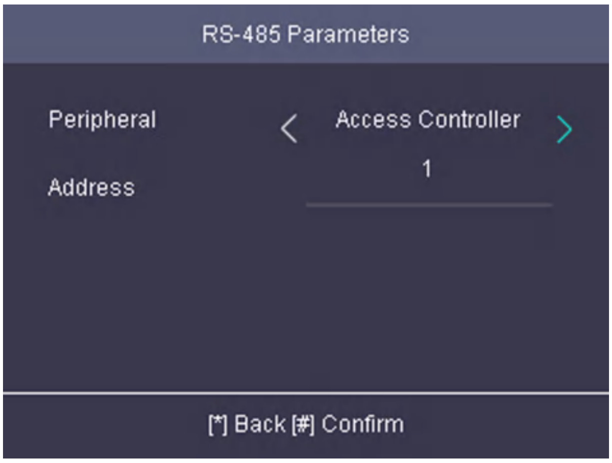
3. Press ***** and select **Yes** to save the settings and exit the page.

6.3.5 Set RS-485 Parameters

The face recognition terminal can connect card reader via the RS-485 terminal.

Steps

1. Move the cursor and select **Comm. → RS-485** on the Home page to enter the RS-485 page.



RS-485 Parameters

Peripheral: Access Controller

Address: 1

Figure 6-6 Set RS-485 Parameters

2. Select an peripheral type according to your actual needs.
3. Press * and select **Yes** to save the settings and exit the page.

Note

The device will reboot automatically after change the peripheral type.

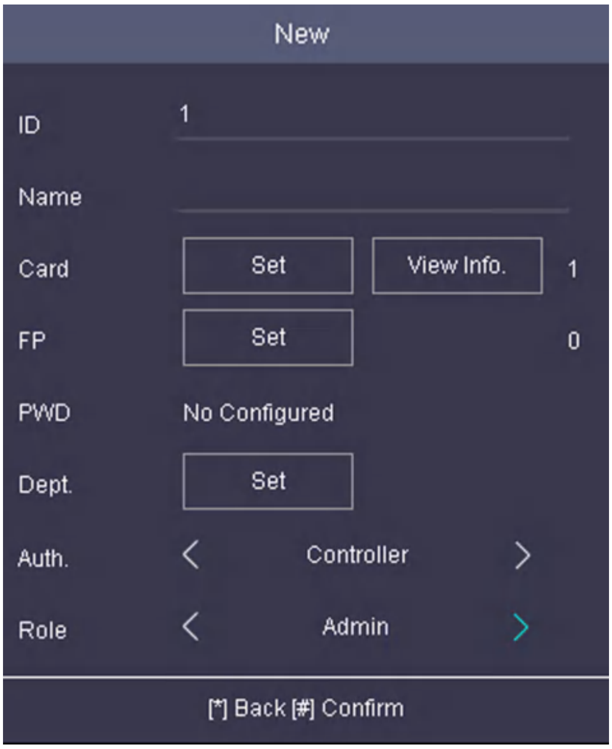
6.4 Person Management

6.4.1 Add Person

You can add users by setting the ID No., the user name, and the card No. You can also record the user fingerprint, set the password, the department, the role and the authentication mode.

Steps

1. Move the cursor and select **User → New** to enter the New page.



New

ID 1

Name

Card 1

FP 0

PWD No Configured

Auth. Controller

Role Admin

Figure 6-7 New Page

2. Enter the new user's parameters.

ID (Employee ID)

By default, the ID No. will be increased in sequence. You can edit the ID according to your preference.

Note

- The ID refers to the user attendance serial No.
- The ID should be between 1 and 99999999 and should not start with 0.
- The ID should be unique.

Name

Enter the new user name.

Note

- Press the up or down key on the keypad to change the input method.
- Up to 64 characters are allowed in the user name.

Card

Set: Present card on the card presenting area or enter card No. manually, and select a card property.

View Info.: View the user's added card information.

Note

- The card No. is required.
- Up to 20 digits can be contained in the card No.
- The card No. can be 0.
- The card No. can start with 0 when it contains more than one numbers. E.g. 012345.
- The card No. should be unique.

FP (Fingerprint)

On the Fingerprint page, select a target finger and record according to the voice prompt.

Note

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added to one user.
- You can also scan the fingerprints via the external fingerprint recorder and apply the fingerprints to the device by the client software.
- For detailed information about scanning the fingerprint, see ***Tips for Scanning Fingerprint*** .
- Parts of device models supports the fingerprint function.

Dept. (Department)

Select a department in the list and edit the department.

Note

For detailed information about editing the department, see .

Auth.

Select an authentication mode when verifying user's permission.

Note

- If you select the authentication mode as **Controller**, you should set the authentication mode in ***Set System Parameters*** . The system will authenticate user's identity according to the configured authentication mode. By default, the authentication mode is **Controller**. This mode is applicable to edit users' authentication modes in batch.
- If an user needs to use a special authentication mode, which is different from the authentication mode configured in ***Set System Parameters*** , he can use card/fingerprint, card, etc. The system will authenticate the user's identity according to the configured authentication mode first. This mode is applicable to edit single user's authentication mode, which has special permissions.

Role

Select the user's role as administrator or normal user.

- Admin: The admin has all permissions to operate the device.
- User: The normal user can check attendance on the initial page.

Note

- All persons can enter the main page by entering the device password to operate if there is no admin user configured.
- After configuring the admin, you should authenticate the admin to enter the main page.
- You can use the USB interface to import the user information. For details, see ***Data Transfer*** .

3. Press ***** to save the settings and exit the page.

6.4.2 Manage Person (Search/Edit/Delete)

Search, edit, delete the added users. You can also manage added fingerprints, manage user's cards.

Search User

Move the cursor and select **User → User** to enter the user list.
Enter the user's name or employee ID in the search box, and press ***** to start search.

Edit User

Move the cursor and select **User → User** to enter the user list. Select an user in the list and press *****.
Select **Edit User** and refer to ***Add Person*** to edit the user's information.

Delete

You can delete user, delete password, clear all fingerprints, and clear all added cards' information .

6.5 Identity Authentication

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

Authentication via Multiple Credentials

If the configured authentication mode is Card & Password, Card & Fingerprint, Card & Fingerprint & Password, you should authenticate the card first, and then authenticate other credentials according to the prompt.
If the configured authentication mode is Fingerprint & Password, you should authenticate the fingerprint first, and then authenticate other credentials according to the prompt.

Note

- Parts of device models supports the fingerprint function.
- For details about fingerprint authentication, see ***Tips for Scanning Fingerprint*** .

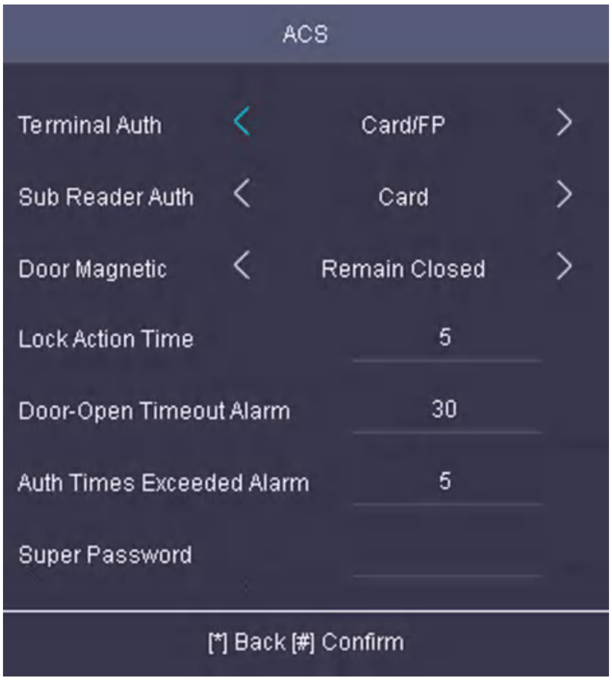
Authentication via Multiple Credentials

If the configured authentication mode is Card/Password, Card/Fingerprint, Card/Fingerprint/ Password, fingerprint, card, you should authenticate the credential.

6.6 Set Access Control Parameters

Set the device's access control parameters, including the device authentication, the sub reader authentication, the door contact status, the open duration, the door-open timeout alarm, and the authentication times exceeded, and the super password.

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



ACS

Terminal Auth < Card/FP >

Sub Reader Auth < Card >

Door Magnetic < Remain Closed >

Lock Action Time 5

Door-Open Timeout Alarm 30

Auth Times Exceeded Alarm 5

Super Password

[*] Back [#] Confirm

Figure 6-8 Access Control Parameters

The available parameters descriptions are as follows:

Table 6-1 Access Control Parameters Descriptions

Parameter	Description
Terminal Auth	Select the face recognition terminal's authentication mode. You can also customize the authentication mode.

Parameter	Description
	Note • Only the device with the fingerprint module supports the fingerprint related function. • Biometric recognition products are not 100% applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes. • If you adopt multiple authentication modes, you should authenticate other methods before authenticating face.
Sub Reader Auth	Select the card reader's authentication mode.
Door Contact	You can select "Remain Open" or "Remain Closed" according to your actual needs. By default, it is **Remain Closed**.
Open Duration	Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. Available door locked time range: 1 to 255s.
Door-Open Timeout Alarm	Configure the maximum time duration for door opening. If the door-open time has exceeded the configured value, it will trigger an alarm.
Auth Times Exceeded Alarm	Configure the maximum times for authentication.
Super Password	Set the device super password. After saving the settings, you can input the super password in the initial interface to access the door.

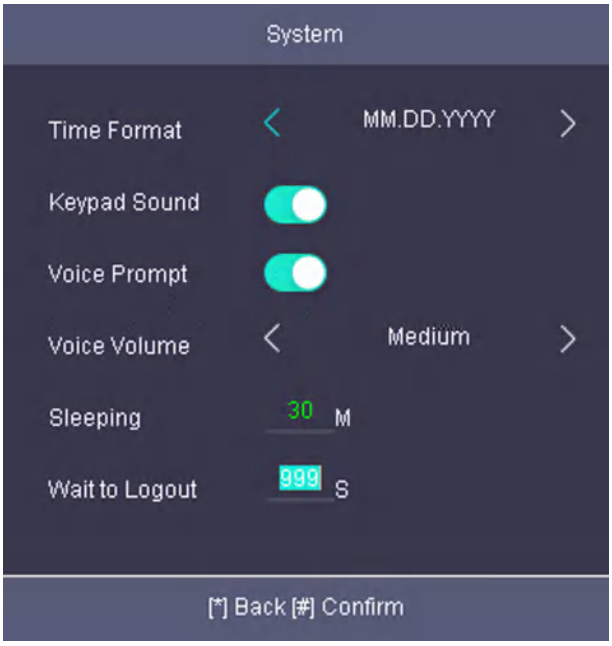
6.7 Basic Settings

6.7.1 Set System Parameters

Set the system parameters, including the device time format, the keypad sound, the voice prompt, the volume, and the sleeping mode.

Steps

1. Move the cursor and select **System → System** .
2. Press * to enter the System page.



System

Time Format < MM.DD.YYYY >

Keypad Sound

Voice Prompt

Voice Volume < Medium >

Sleeping 30 M

Wait to Logout 999 S

[*] Back [#] Confirm

Figure 6-9 System Page

3. Edit the parameters.

Time Format

Select an appropriate time format according to your preference.

Keypad Sound

Enable or disable the keypad sound according to your preference.

Voice Prompt

Enable or disable the voice prompt according to your preference.

Voice Volume

Set the device voice prompt volume.

Sleeping

Set the device sleeping waiting time (minute). When you are on the initial page and if you set the sleeping time to 30 min, the device will sleep after 30 min without any operation.

Note

If you set the sleeping time to 0, the device will not enter sleeping mode.

Wait to Logout

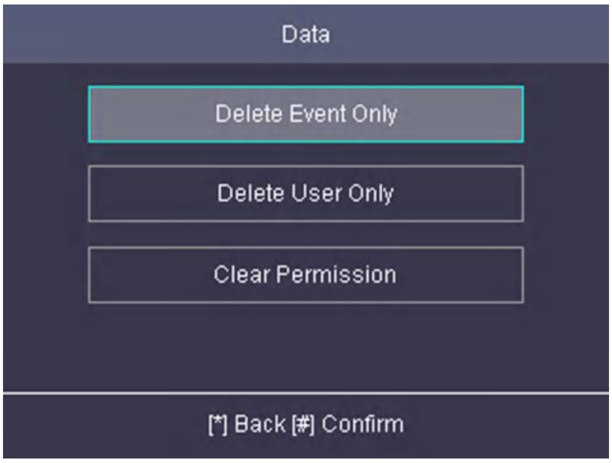
If there is no operation within the configured time, the system will logout.

6.7.2 Manage System Data

Delete the saved event, attendance data, user data, or permission.

Steps

1. Move the cursor and select **System → Data** .
2. Press * to enter the Data page.



Data

Delete Event Only

Delete User Only

Clear Permission

[*] Back [#] Confirm

Figure 6-10 Data Page

3. Select an item and press **OK** to delete.

   Delete Event Only

   Delete all recorded events in the device.

   Delete User Only

   Delete all user data in the device, including the attendance records.

   Clear Permission

   Clear the admin management permission. The admin will turn to the normal user. The user will not be deleted.

6.7.3 System Upgrade

You can upgrade the system online or locally. The system reads the upgrading file in the plugged USB flash drive or gain the upgrading package from the platform to upgrade the device.

Steps

1. Move the cursor and select **System → Upgrade** .
2. Upgrade the system.
   - Local Upgrade: Plug the USB flash drive to the USB interface. Press **OK**. The system will read the digicap.dav file and upgrading automatically. After the upgrading is completed, the device will reboot automatically.

   Note

   - The upgrading file should be in the root directory.
   - The upgrading file name in the USB flash drive should be digicap.dav.

- Do not power off during the device upgrading.
- After the upgrading is completed, remove the USB flash drive.

- Online upgrade: The system will gain the upgrade package from the platform to upgrade.

6.7.4 Restore Settings

Restore system parameters to factory settings or default settings.

Steps

1. Move the cursor and select **System → Reset** .
2. Press * to enter the Reset page.

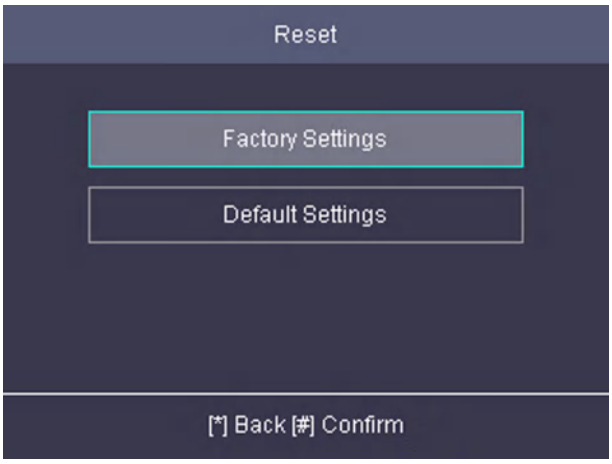


Figure 6-11 Reset Page

3. Select **Factory Settings** or **Default Settings**.

   Factory Settings

   All parameters of the device will restore to the factory parameters.

   Default Settings

   All parameters, excluding the communication parameters, the remote user management, and events, will restore to the factory parameters.

4. Press * to confirm the settings in the prompt page and the device starts restoring.

6.7.5 Data Transfer

You can export the access control parameters (fingerprint and user information) and the attendance data (data after attendance, card swiping data for instance). You can also import the access control parameters from the USB flash drive.

Export Data

Move the cursor and select **Transfer → Export** to enter the Export page.

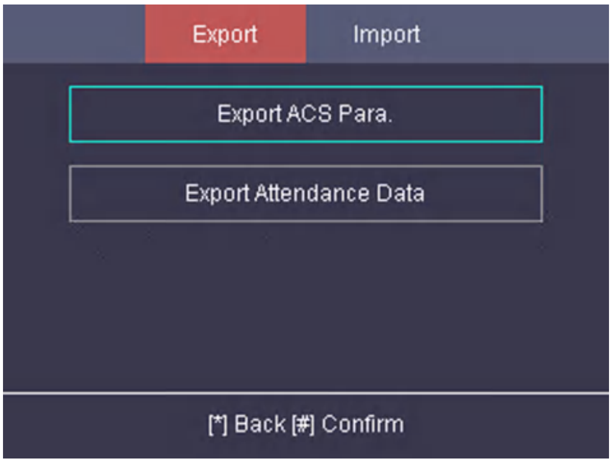


Figure 6-12 Export Data Page

Plug a USB flash drive in the device USB interface, and select **Export ACS Para.** or **Export Attendance Data**, enter the key, and press *. The data will be exported to the USB flash drive.

Note

- The supported USB flash drive format is FAT32.
- The USB flash drive memory should be from 1G to 32G. Make sure the free space of the USB flash drive should be more than 512 M.
- Remember the key property, and you should use the key to import the data to another device.

Import Data

Move the cursor and select **Transfer → Import** to enter the Import page. Select **Import ACS Para**, enter the key, and press *. The system will gain access control parameters from the USB flash drive.

Note

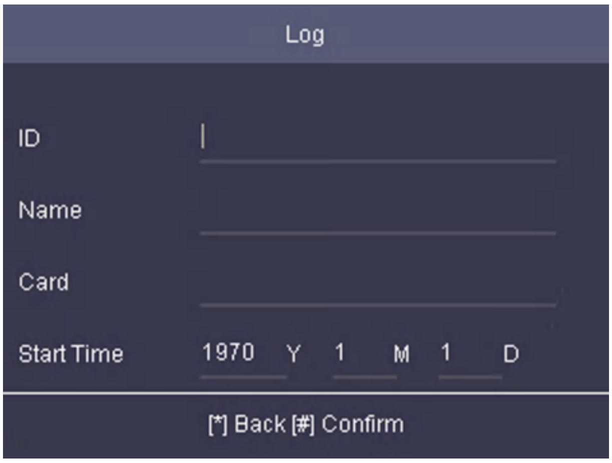
- The supported USB flash drive format is FAT32.
- The file for importing should be in the root directory.

6.7.6 Log Query

You can search the authentication logs via the user's employee ID, name, or card.

Steps

1. On the Home page, move the cursor and select **Log**.



Log

ID |

Name

Card

Start Time 1970 Y 1 M 1 D

[*] Back [#] Confirm

Figure 6-13 Log Query Page

2. Enter the employee ID, the user name, the card No., the start time, and the end time.
3. Press ***to** start searching.

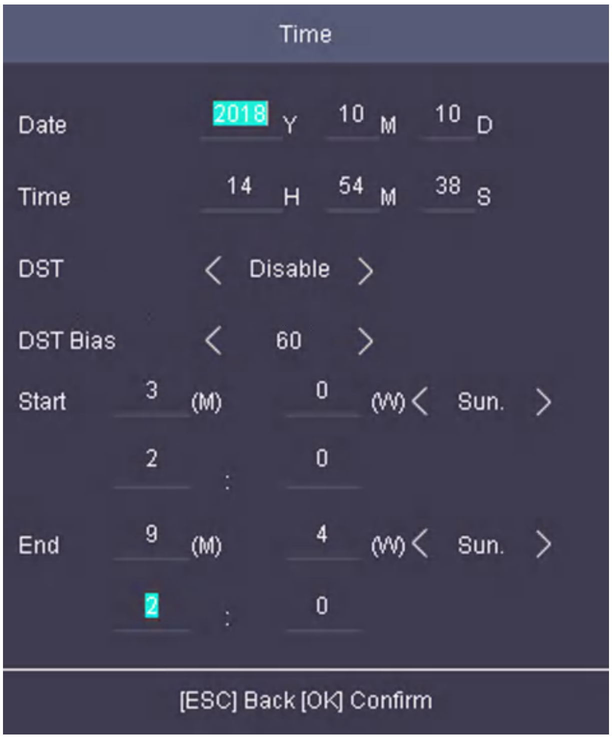
   The result will be displayed on the page.

6.7.7 Set Time

Set the device time and DST.

Steps

1. Move the cursor and select **Time** in the main page and press **OK** to enter the Time page.



Time

Date 2018 Y 10 M 10 D

Time 14 H 54 M 38 S

DST < Disable >

DST Bias < 60 >

Start 3 (M) 0 (W) < Sun. >

2 : 0

End 9 (M) 4 (W) < Sun. >

2 : 0

[ESC] Back [OK] Confirm

Figure 6-14 Time Page

2. Edit the parameters.

Date

The displayed date on the device.

Note

The available range is from 1970.01.01 to 2037.12.31.

Time

The displayed time on the device.

DST

Select to enable or disable the DST. When the DST is enabled, you can set the DST bias time, the start time and the end time.

- DST Bias: You can select 30min, 60min, 90min and 120min.
- Start: Set the start time of the DST.
- End: Set the end time of the DST.

3. Press **ESC** and select **Yes** to save the settings and exit the page.

6.7.8 View System Information

View system information, including system capacity and device information.

View System Capacity

Move the cursor and select **Info. → Capacity** to enter the Capacity page.
You can view the added device user number, card number, and fingerprint number.

Note

Parts of device models supports display the fingerprint capacity.

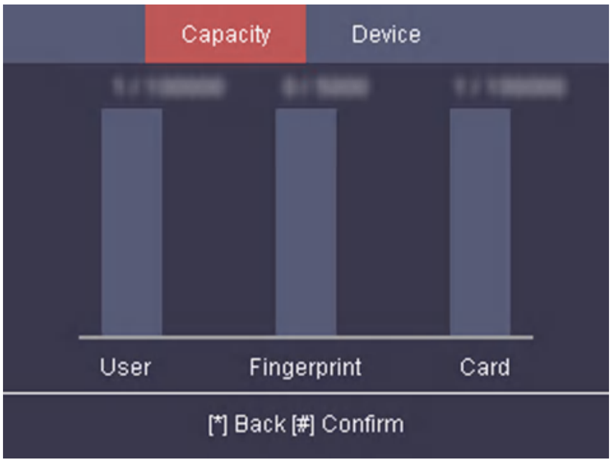


Figure 6-15 Capacity Page

View Device Information

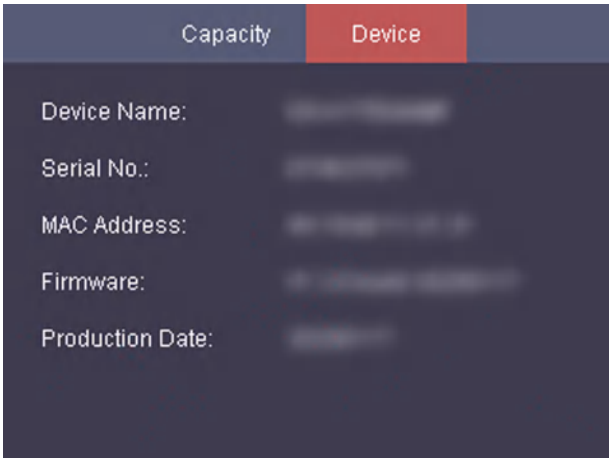
Move the cursor and select **Info. → Device** to enter the Device page.
Select **Device Information** or **User Manual**.

Device Information

You can view the device name, the serial No., the MAC address, the firmware, and the production date.

User Manual

Scan the QR code to view the device user manual.



Device Name:

Serial No.:

MAC Address:

Firmware:

Production Date:

Figure 6-16 Device Page

Chapter 7 Client Software Configuration

7.1 Configuration Flow of Client Software

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

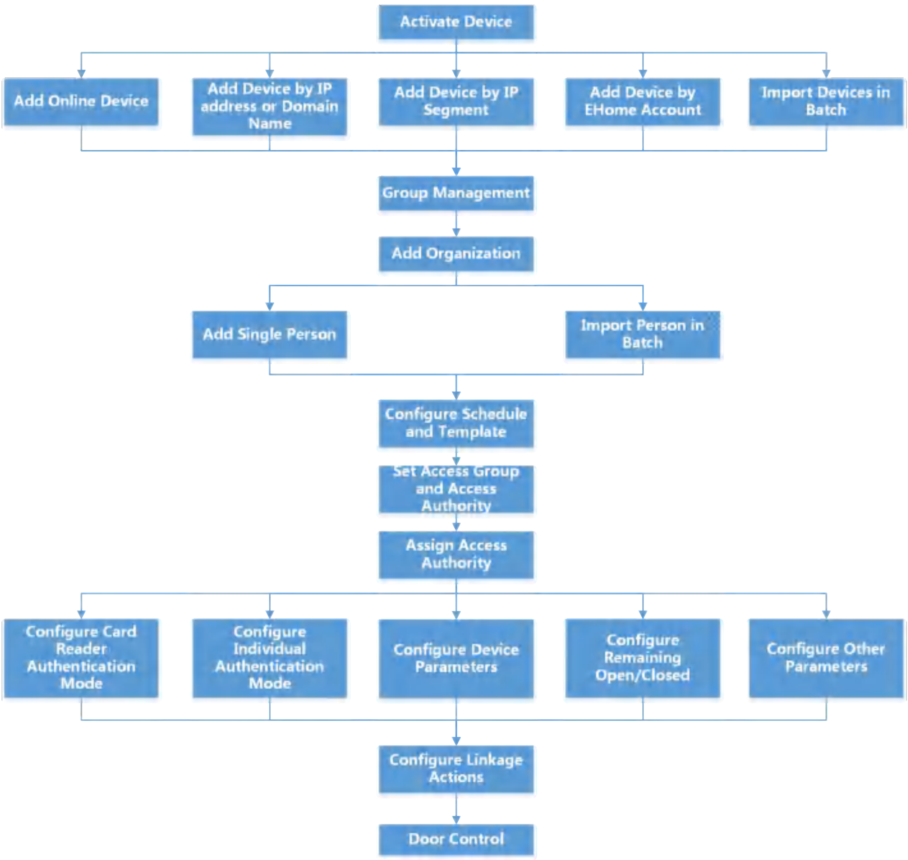

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign Access Authority
Configure Card Reader Authentication Mode
Configure Individual Authentication Mode
Configure Device Parameters
Configure Remaining Open/Closed
Configure Other Parameters
Configure Linkage Actions
Door Control

Figure 7-1 Flow Diagram of Configuration on Client Software

7.2 Device Management

You can manage devices on the client, including adding, editing, and deleting the devices. You can also perform operations such as checking device status.

7.2.1 Add Device

After running the client, devices including access control devices, video intercom devices, etc., should be added to the client for the remote configuration and management, such as controlling door status, attendance management, event settings, etc.

Add Online Device

The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area.

Note

- You can click **Refresh per 60s** to refresh the information of the online devices.
- SADP log function can be enabled or disabled by right-clicking **Online Device**.

Add Single or Multiple Online Devices

The client can detect online devices which are in the same network as the PC running the client. You can select a detected online device displayed in the online device list and add it to the client. For detected online devices sharing the same user name and password, you can add them to the client in a batch.

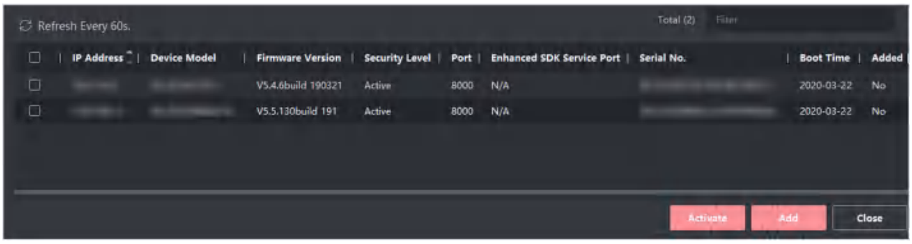
Before You Start

- The device(s) to be added are in the same network as the PC running the client.
- The device(s) to be added have been activated.

Steps

1. Click **Device Management → Device** 。
2. Click **Online Device** to show the online device area.

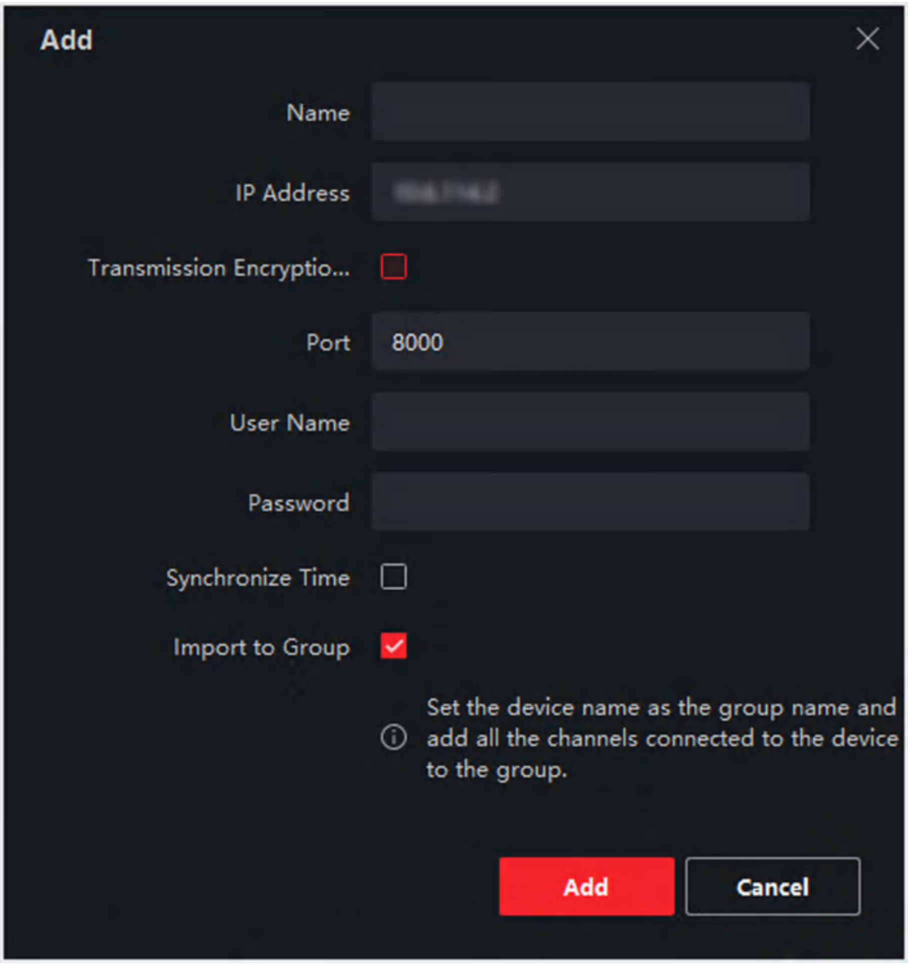
   The searched online devices are displayed in the list.



□	IP Address	Device Model	Firmware Version	Security Level	Port	Enhanced SDK Service Port	Serial No.	Boot Time	Added
□	[redacted]	[redacted]	V5.4.6build 190321	Active	8000	N/A	[redacted]	2020-03-22	No
□	[redacted]	[redacted]	V5.5.130build 191	Active	8000	N/A	[redacted]	2020-03-22	No

Figure 7-2 Online Device

3. In the **Online Device** area, check one or more online device(s), and click **Add** to open the device adding window.



Add

Name

IP Address [redacted]

Transmission Encryptio... □

Port 8000

User Name

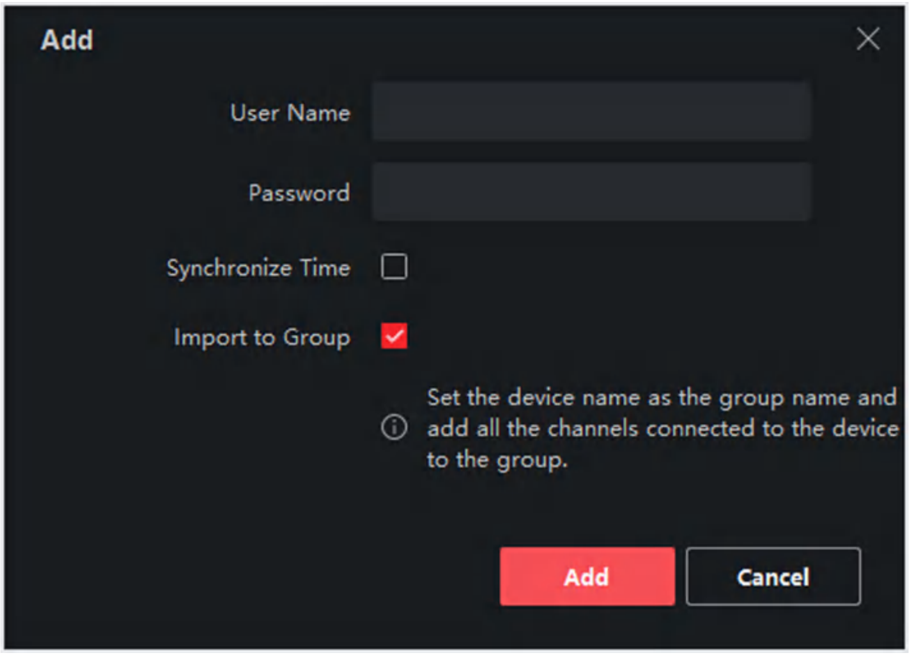
Password

Synchronize Time □

Import to Group ☑

ⓘ Set the device name as the group name and add all the channels connected to the device to the group.

Figure 7-3 Add Single Online Device



Add

User Name

Password

Synchronize Time □

Import to Group ☑

ⓘ Set the device name as the group name and add all the channels connected to the device to the group.

Figure 7-4 Add Multiple Online Devices

4. Enter the required information.

Name

Enter a descriptive name for the device.

IP Address

Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

Port

You can customize the port number. The port number of the device is obtained automatically in this adding mode.

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. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
6. **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.
7. Click **Add**.

Add Multiple Detected Online Devices

For detected online devices sharing the same user name and password, you can add them to the client in a batch.

Before You Start

Make sure the to-be-added devices are online.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

   The searched online devices are displayed in the list.
4. Select multiple devices.

   Note

   For the inactive device, you need to create the password for it before you can add the device properly. For details, refer to .
5. Click **Add** to open the device adding window.
6. Enter the required information.

   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.

7. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
8. **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.
9. Click **Add** to add the devices.

Add Device by IP Address or Domain Name

When 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, and other related parameters.

Steps

1. Enter Device Management module.
2. **Optional:** Click ▴ on the right of **Device Management** and select **Device**.

   The added devices are displayed in the list.
3. Click **Add** to open the Add window.
4. Select **IP/Domain** as the adding mode.
5. Enter the required information, including name, address, port number, user name, and password.

   Name

   Create a descriptive name for the device. For example, you can use a name 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 have the same port No. The default value is 8000.

   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.

6. **Optional:** 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.

Note

You can import all the channels of the device to the corresponding group by default.

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.
9. Perform the following operations after adding the devices.

Remote Configuration

Click ⚙ on Operation column to set remote configuration of the corresponding device.

Note

- For some models of devices, you can open its web window. To open the original remote configuration window, press **Ctrl** and click ⚙ .
- For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click ▤ on Operation column to view device status.

Add Devices by IP Segment

If you want to add devices of which the IP addresses are within an IP segment, you can specify the start IP address and end IP address, user name, password, and other parameters to add them.

Steps

1. Enter the Device Management module.
2. **Optional:** Click ▴ on the right of **Device Management** and select **Device**.

   The added devices are displayed in the list.

3. Click **Add** to open the Add window.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Start IP

   Enter a start IP address.

   End IP

   Enter an end IP address in the same network segment with the start IP.

   Port

   Enter the device port No. The default value is 8000.

   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.

6. **Optional:** 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.

   ℹ **Note**

   You can import all the channels of the device to the corresponding group by default.

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.
9. **Optional:** Click ▤ on Operation column to view device status.

Add Device by EHome Account

For access control devices supports EHome 5.0 protocol, you can add them to the client by EHome protocol after entering device ID and key, if you have configured their server addresses, port No., and device IDs.

Before You Start

Make sure the devices have connected to the network properly.

Steps

1. Enter Device Management module.

   The added devices are displayed on the right panel.
2. Click **Add** to open the Add window.
3. Select **EHome** as the adding mode.
4. Enter the required information.

   Device Account

   Enter the account name registered on EHome protocol.

   EHome Key

   For EHome 5.0 devices, enter the EHome key if you have set it when configuring network center parameter for the device.

   Note

   This function should be supported by the device.
5. **Optional:** Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
6. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to the group.
7. Finish adding the device.
   - Click **Add** to add the device and go back to the device list.
   - Click **Add and New** to save the settings and continue to add other device.

   Note

   Face pictures cannot be applied to devices added by EHome account.
8. **Optional:** Perform the following operation(s).

   Device Status

   Click on Operation column to view device status.

   Edit Device Information

   Click on Operation column to edit the device information, such as device name, device account, and EHome key.

   Check Online User

   Click on Operation column to check the online users who access the device, such as user name, user type, user's IP address, and login time.

   Refresh

   Click on Operation column to get the latest device information.

   Delete Device

   Select one or multiple devices and click **Delete** to delete the selected device(s) from the client.

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 ***8000***.

   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.
8. Perform the following operations after adding the devices.

Remote Configuration

Click ⚙ on Operation column to set remote configuration of the corresponding device.

Note

- For some models of devices, you can open its web window. To open the original remote configuration window, press **Ctrl** and click ⚙ .
- For detail operation steps for the remote configuration, see the user manual of the device.

Device Status

Click ▤ on Operation column to view device status.

7.2.2 Reset Device Password

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

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices in the same subnet will display in the list.
3. Select the device from the list and click 🔧 on the Operation column.
4. Click **Export** to save the device file on your PC and then send the file 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.

7.3 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.

7.3.1 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.

7.3.2 Import Resources to Group

You can import the device resources 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 such as **Access Control Point**.
4. Click **Import**.
5. Select the channel names from the To Be Imported area.
6. Click **Import** to import the selected resources to the group.

7.3.3 Edit Resource Parameters

After importing the resources to the group, you can edit the resource parameters. For access points, you can edit the resource name.

Before You Start

Import the resources to group. Refer to ***Import Resources to Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.

   All the added groups are displayed on the left.
3. Select a group on the group list and click a resource type.

   The resource channels imported to the group will display.
4. Click ✎ in the Operation column to open the Edit Camera window.
5. Edit the required information.
6. Click **OK** to save the new settings.

7.3.4 Remove Resources from Group

You can remove the added resources from the group.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.

   All the added groups are displayed on the left.
3. Click a group to show the resources added to this group.
4. Select the resource(s) and click **Delete** to remove the resource(s) from the group.

7.4 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.

7.4.1 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 surbodinate 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.

7.4.2 Configure Basic Information

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

Steps

1. Enter **Person** module.
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, gender, tel, email address, etc.
5. **Optional:** Set the effective period of the person. Once 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.

   Example

   For example, if the person is a visitor, his/her effective period may be short and temporary.
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.

7.4.3 Issue a Card to One Person

When adding person, you can issue a card with a unique card number to the person as a credential. After issued, the person can access the doors which he/she is authorized to access by swiping the card on the card reader.

Steps

Note

Up to five cards can be issued to one person.

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 → Card** panel, click **+**.
4. Enter the card number.
   - Enter the card number manually.
   - Place the card on the card enrollment station or card reader and click **Read** to get the card number. The card number will display in the Card No. field automatically.

     Note

     You need to click **Settings** to set the card issuing mode and related parameters first. For details, refer to ***Set Card Issuing Parameters*** .
5. Select the card type according to actual needs.

   Normal Card

   The card is used for opening doors for normal usage.

   Duress Card

   When the person is under duress, he/she can swipe the duress card to open the door. The door will be unlocked and the client will receive a duress event to notify the security personnel.

   Patrol Card

   This card is used for the inspection staff to check the their attendance of inspection. By swiping the card on the specified card reader, the person is marked as on duty of inspection at that time.

   Dismiss Card

   By swiping the card on the card reader, it can stop the buzzing of the card reader.
6. Click **Add**.

The card will be issued to the person.

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.

7.4.4 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.

7.4.5 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.

7.4.6 Configure Access Control Information

When adding a person, you can set her/his access control properties, such as setting the person as visitor or as blacklist person, or as super user who has super authorization.

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 **Access Control** panel, set the person's access control properties.

   PIN Code

   The PIN code must be used after card or fingerprint when accessing. It cannot be used independently. It should contain 4 to 8 digits.

   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 Blacklist, 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 blacklist, or set her/him as visitor.

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.

7.4.7 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.

7.4.8 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

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 **Resident Information** panel, select the indoor station to bind it to the person.

Note

If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
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.

7.4.9 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 .

7.4.10 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.

7.4.11 Import Person Information

You can enter the information of multiple persons in a predefined template (a CSV 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 file with person information.
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 10,000 persons.

7.4.12 Export Person Information

You can export the added persons' information to local PC as a CSV 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 and check **Person Information** as the content to export.
4. Check desired items to export.
5. Click **Export** to save the exported CSV file in your PC.

7.4.13 Get Person Information from Access Control Device

If the added 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 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.
- The gender of the 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 the access control device from the drop-down list.
5. Click **Get** to start importing the person information to the client.

   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.

7.4.14 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**.

7.4.15 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 display.
3. Set the card issuing parameters. For details, refer to ***Set Card Issuing Parameters*** .
4. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
5. Click the card number column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Enter the card number manually and press **Enter** key on your keyboard.

   The card number will be read automatically and the card will be issued to the person in the list.
6. Repeat the above step to issue the cards to the persons in the list in sequence.

7.4.16 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.

7.4.17 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 models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

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 IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

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, 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.

7.5 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*** .

7.5.1 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**.

7.5.2 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.

7.6 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.

Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
- You can add up to 128 access groups in total.
- 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, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → 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) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click **OK**.
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.

   To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.
2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.

   ⚠ **Caution**

   - Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may brings risk to the devices.
   - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).
3) View the apply status in the Status column or click **Applying Status**to view all the applied access group(s).

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.

7.7 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.

7.7.1 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.

Steps

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

Note

If you can 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.

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.

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.

Enable NFC Card

If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

Enable M1 Card

If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

Enable EM Card

If enable the function, the device can recognize the EM card. You can present EM card on the device.

Enable CPU Card

Reserved. If enable the function, the device can recognize the CPU card. You can present CPU card on the device.

Enable ID Card

Reserved. If enable the function, the device can recognize the ID card. You can present ID card on the device.

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 Left 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.

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.

Basic

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.

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Card Reader Type/Card Reader Description

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

Fingerprint

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

4. Click **Advanced** to configure more parameters.

Basic Information

Enable Card Reader

Enable the function and e device can be used as an 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.

Buzzing Time

Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Fingerprint

Fingerprint Recognition Level

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

Fingerprint Recognition Interval

Select the fingerprint recognition level in 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.

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.

7.7.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed. For example, you can set the door remaining closed in the holiday, and set the door remaining open 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 Open/Closed** to enter the Remain Open/ Closed page.
2. Select the door that need to be configured on the left panel.
3. To set the door status during the work day, click the **Week Schedule** and perform the following operations.
   1) Click **Remain Open** or **Remain Closed**.
   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 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) 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 Open** or **Remain Closed**.
   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).

7.7.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multi-Factor Auth** .

2. Select an access control device in device list on the left panel.

3. Add a person/card group for the access control device.

1) Click **Add** on the right panel.
2) Create a name for the group as desired.
3) Specify the start time and end time of the effective period for the person/card group.
4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

Note

Make sure you have issue card to the person.

Make sure you have set access group and apply the access group to the access control device successfully.

5) Click **Save**.
6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.

4. Select an access control point (door) of selected device on the left panel.
5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Authentication Groups panel.
   2) Select a configured template as the authentication template from the drop-down list.

Note

For setting the template, refer to ***Configure Schedule and Template*** .

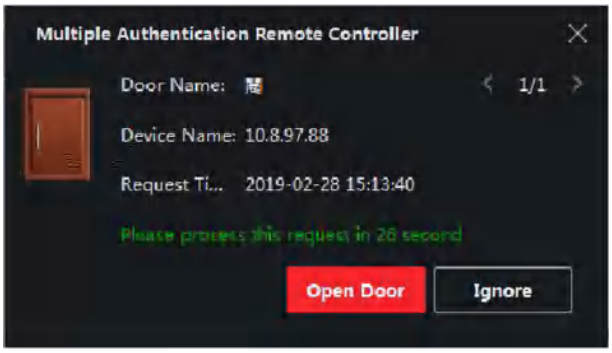
   3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

Local Authentication

Authentication by the access control device.

Local Authentication and Remotely Open Door

Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.



Multiple Authentication Remote Controller

Door Name: [illegible]

Device Name: 10.8.97.88

Request Ti... 2019-02-28 15:13:40

Please process this request in 28 second

Figure 7-5 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

   4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.

5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

6) Click **Save**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

7. Click **Save**.

7.7.4 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.

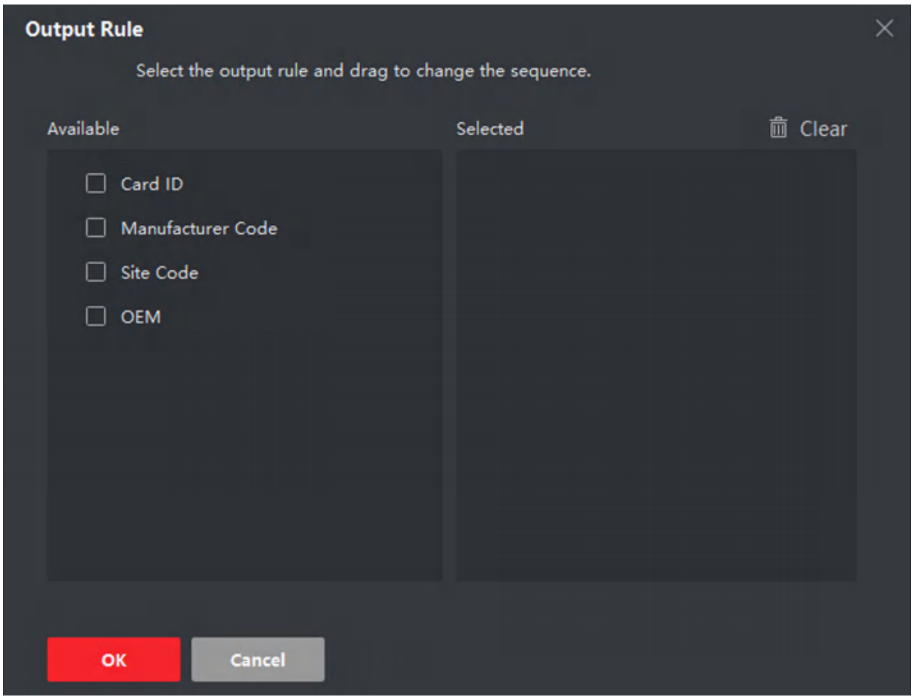
4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

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.



Select the output rule and drag to change the sequence.

Figure 7-6 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.

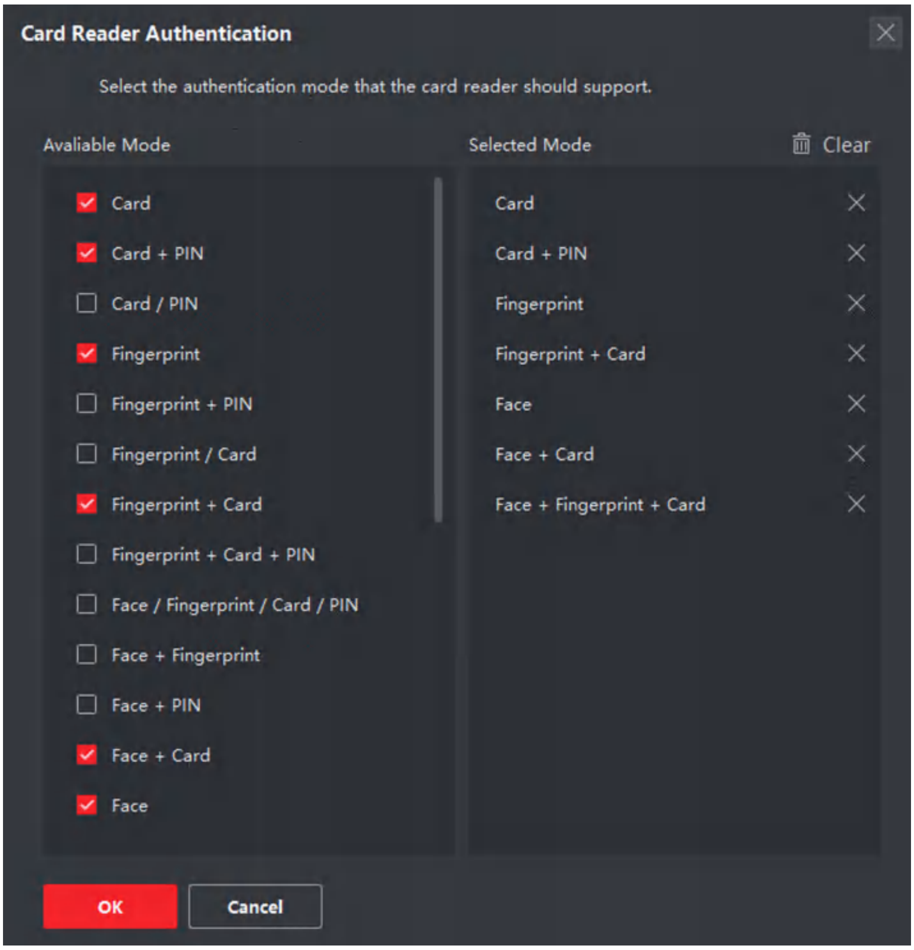
7. Click **Save**.

7.7.5 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**.



Card Reader Authentication

Select the authentication mode that the card reader should support.

Avaliable Mode

- ☑ Card
- ☑ Card + PIN
- ☐ Card / PIN
- ☑ Fingerprint
- ☐ Fingerprint + PIN
- ☐ Fingerprint / Card
- ☑ Fingerprint + Card
- ☐ Fingerprint + Card + PIN
- ☐ Face / Fingerprint / Card / PIN
- ☐ Face + Fingerprint
- ☐ Face + PIN
- ☑ Face + Card
- ☑ Face

Selected Mode

- Card
- Card + PIN
- Fingerprint
- Fingerprint + Card
- Face
- Face + Card
- Face + Fingerprint + Card

Figure 7-7 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.

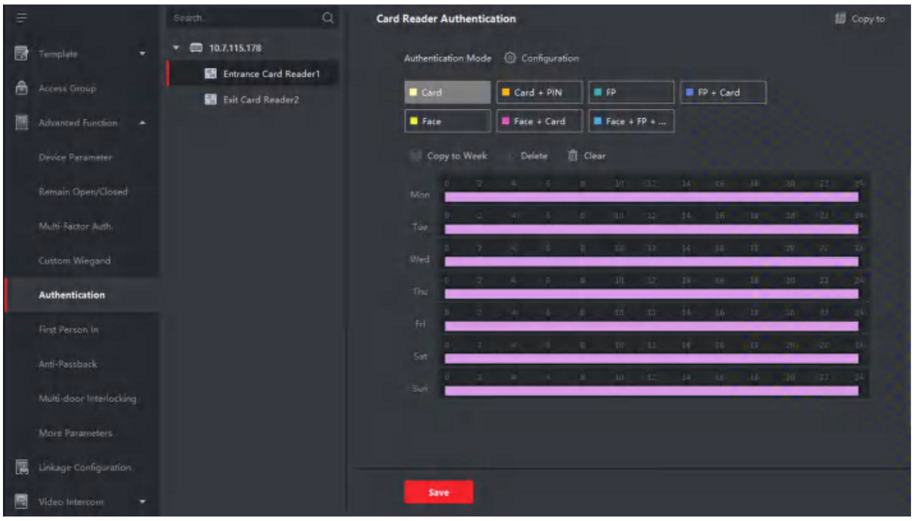


Figure 7-8 Set Authentication Modes for Card Readers

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**.

7.7.6 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

Set the access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

Perform this task when you want to configure opening door with first person.

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

   Enable Remaining Open after First Person

   The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.

Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

7.7.7 Configure Anti-Passback

You can set to only pass the access control point according to the specified path and only one person could pass the access control point after swiping the card.

Before You Start

Enable the anti-passing back function of the access control device.

Perform this task when you want to configure the anti-passing back for the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the Anti-Passpack Settings page.
2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click ✎ of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path
If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

7.7.8 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 ISUP account via wired network.

Set Log Uploading Mode

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

Steps

Note

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 → 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

   Note

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

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

Note

- 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.

   Note

   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.

   Note

   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

Note

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** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

Note

- 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.

Steps

Note

The RS-485 Settings 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 **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.

Note

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

Note

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.

   Note

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

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

7.8 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, ..

7.8.1 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 by configuring linked actions of access event on the client. You will be notified on the client once an event is triggered, so that you can response to the event instantly. You can also configure client actions of access points in a batch at a time.

Steps

Note

The linkage actions here refer to the linkage of the client software's own actions such as audible warning, email linkage, etc.

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

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

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

   The event types which the selected resource supports will display.

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 events triggered.

      Audible Warning

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

      Note

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

      Send Email

      Send an email notification of the alarm information to one or more receivers.

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

   2) Click **OK**.
5. Enable the event so that when the event is detected, en 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.

7.8.2 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

Note

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.

   Capture

   The real-time capture will be triggered.

   Access Point

   The door status of open, close, remain open, and remain close will be triggered.

   Note

   The target door and the source door cannot be the same one.

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.

7.8.3 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 host buzzer, and other actions on the same device.

Steps

Note

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 drop-down 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.

   Capture

   The real-time capture will be triggered.

   Access Point

   The door status of open, close, remain open, or remain closed 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.

7.8.4 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 buzzer on card reader, and other actions.

Steps

Note

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** to add a new linkage.
4. Select **Person Linkage** as the event source.
5. Enter the employee number or select the person from the drop-down list.
6. Select the card reader where the card swipes.
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.

Capture

An event-related picture will be captured when the selected event happens.

Recording

An event-related picture will be captured when the selected event happens.

Note

The device should support recording.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

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

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.

7.9 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*** .

7.9.1 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.

Note

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.

7.9.2 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.

Note

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.

7.10 Event Center

In the Event Center, you can view the real-time events, search the historical events and view the pop-up alarm information.

Before the client can receive the event information from the device, you need to arm the device first. For details, refer to ***Enable Receiving Events from Devices*** .

Before the you can view the pop-up alarm information, you need to enable alarm triggered pop-up image in the event center. For details, refer to .

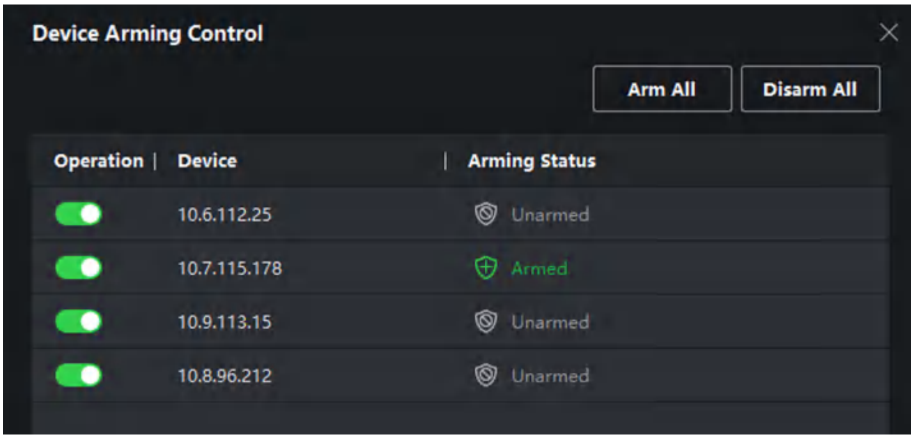
7.10.1 Enable Receiving Events from Devices

Before the client can receive the event information from the device, you need to arm the device first.

Steps

1. Click ☰ → **Tool** → **Device Arming Control** open Device Arming Control page.

   All the added devices display on this page.
2. In the Operation column, turn on the switch to enable auto-arming, or click **Arm All** to arm all the devices.



Operation	Device	Arming Status
	10.6.112.25	Unarmed
	10.7.115.178	Armed
	10.9.113.15	Unarmed
	10.8.96.212	Unarmed

Figure 7-9 Device Arming Control

3. View the arming status of each device in the Arming Status column.

Result

The events of armed device(s) are automatically uploaded to the client when the event is triggered.

7.10.2 View Real-Time Events

In the Real-time Event module of the event center page, you can view the real-time event information, including event source, event time, priority, event key words, etc.

Before You Start

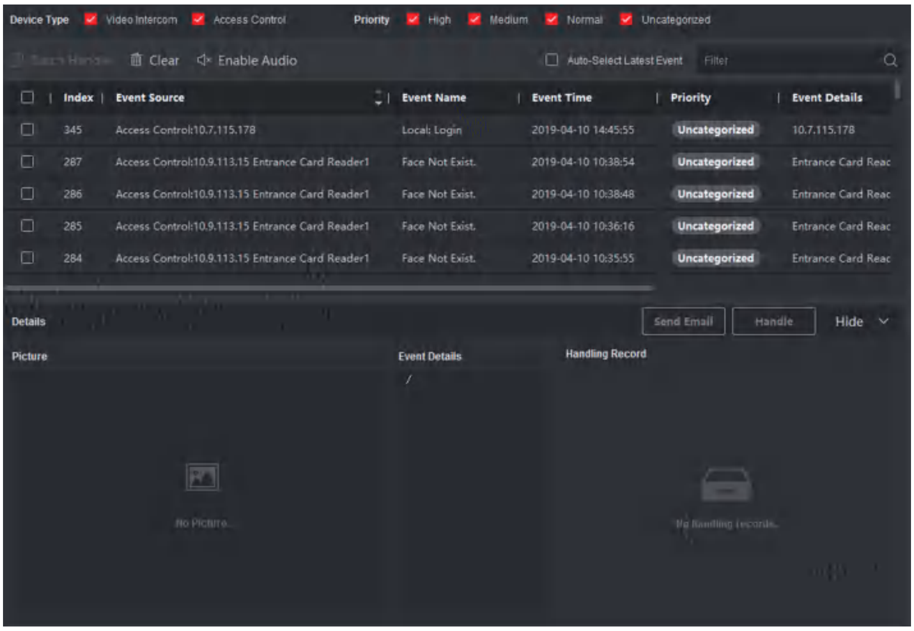
Enable receiving events from devices before the client can receive event information from the device, see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center → Real-time Event** to enter the real-time event page and you can view the real-time events received by the client.

Event Time

For video device, event time is the client time when it receives the event. For none-video device, event time is the time when the event is triggered.



Device Type ☑ Video Intercom ☑ Access Control Priority ☑ High ☑ Medium ☑ Normal ☑ Uncategorized

Clear · Enable Audio · □ Auto-Select Latest Event · Filter

□	Index	Event Source	Event Name	Event Time	Priority	Event Details
□	345	Access Control:10.7.115.178	Local: Login	2019-04-10 14:45:55	Uncategorized	10.7.115.178
□	287	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:38:54	Uncategorized	Entrance Card Reac
□	286	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:38:48	Uncategorized	Entrance Card Reac
□	285	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:36:16	Uncategorized	Entrance Card Reac
□	284	Access Control:10.9.113.15 Entrance Card Reader1	Face Not Exist.	2019-04-10 10:35:55	Uncategorized	Entrance Card Reac

Figure 7-10 View Real-Time Events

2. Set the filter conditions or enter the event key word in the Filter text field to display the required events only.

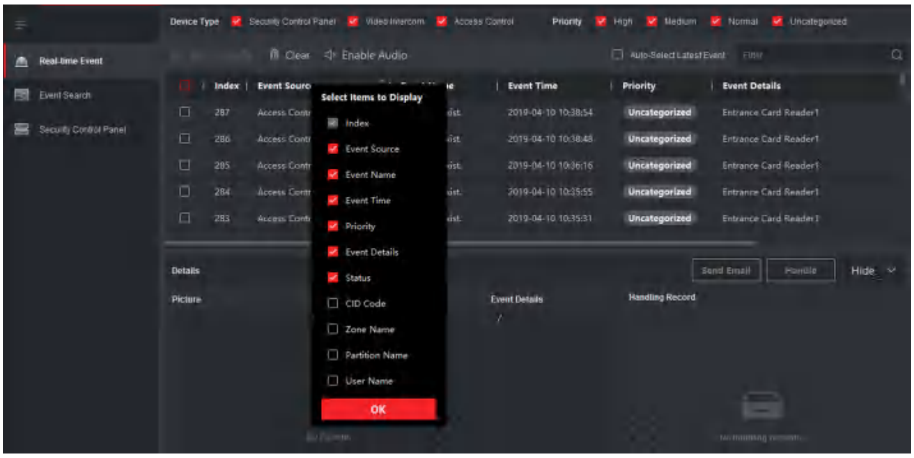
   Device Type

   The type of device that occurred the event.

   Priority

   The priority of the event that indicates the urgent degree of the event.

3. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.



Device Type ☑ Security Control Panel ☑ Video Intercom ☑ Access Control Priority ☑ High ☑ Medium ☑ Normal ☑ Uncategorized

Select Items to Display

☑ Index
☑ Event Source
☑ Event Name
☑ Event Time
☑ Priority
☑ Event Details
☑ Status
□ CID Code
□ Zone Name
□ Partition Name
□ User Name

OK

Figure 7-11 Customize Event Related Items to be Displayed

4. View the event information details.
   1) Select an event in the event list.
   2) Click **Expand** in the right-lower corner of the page.

3) View the related picture, detail description and handing records of the event.
4) **Optional:** Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

5. Optional: Perform the following operations if necessary.

Handle Single Event
Click **Handle** to enter the processing suggestion, and then click **Commit**.

> **Note**
>
> After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

Handle Events in a Batch
Select events that need to be processed, and then click **Handle in Batch**. Enter the processing suggestion, and then click **Commit**.

Enable/Disable Alarm Audio
Click **Enable Audio**/**Disable Audio** to enable/disable the audio of the event.

Select the Latest Event Automatically
Check **Auto-Select Latest Event** to select the latest event automatically and the event information details is displayed.

Clear Events
Click **Clear** to clear the all the events in the event list.

Send Email
Select an event and then click **Send Email**, and the information details of this event will be sent by email.

> **Note**
>
> You should configure the email parameters first, see *Set Email Parameters* in the user manual of client software for details.

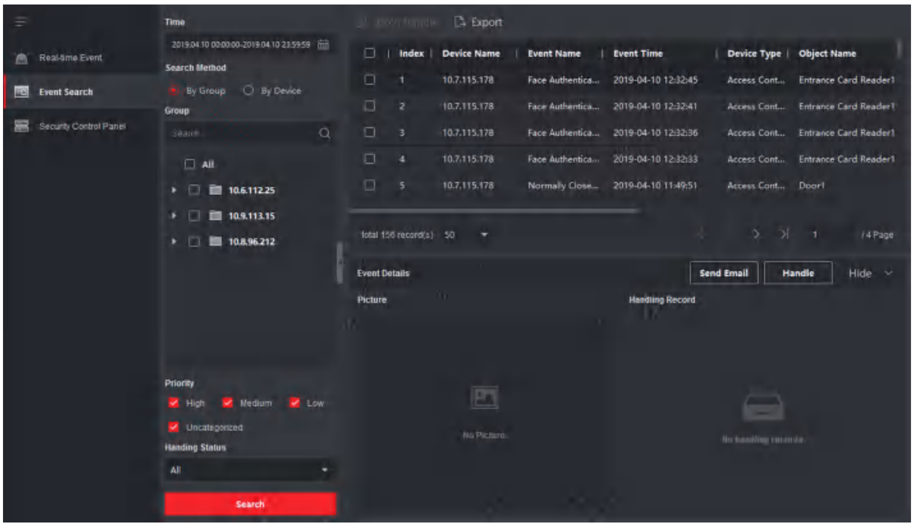
7.10.3 Search Historical Events

In the Event Search module of the event center page, you can search the historical events via time, device type, and other conditions according to the specified device type, and then process the events.

Before You Start
Enable receiving events from devices before the client can receive event information from the device,see ***Enable Receiving Events from Devices*** for details.

Steps

1. Click **Event Center → Event Search** to enter the event search page.



Time: 2019.04.10 00:00:00-2019.04.10 23:59:59

Search Method: ● By Group ○ By Device

Group

□ All
□ 10.6.112.25
□ 10.9.113.15
□ 10.8.96.212

Priority: ☑ High ☑ Medium ☑ Low ☑ Uncategorized

Handing Status: All

□	Index	Device Name	Event Name	Event Time	Device Type	Object Name
□	1	10.7.115.178	Face Authentica...	2019-04-10 12:32:45	Access Cont...	Entrance Card Reader1
□	2	10.7.115.178	Face Authentica...	2019-04-10 12:32:41	Access Cont...	Entrance Card Reader1
□	3	10.7.115.178	Face Authentica...	2019-04-10 12:32:36	Access Cont...	Entrance Card Reader1
□	4	10.7.115.178	Face Authentica...	2019-04-10 12:32:33	Access Cont...	Entrance Card Reader1
□	5	10.7.115.178	Normally Close...	2019-04-10 11:49:51	Access Cont...	Door1

Total 156 record(s) 50 1 /4 Page

Event Details

Figure 7-12 Search History Event

2. Set the filter conditions to display the required events only.

Time

The client time when the event starts.

Search by

Group: Search the events occurred on the resources in the selected group.

Device: Search the events occurred on the selected device.

Device Type

The type of device that occurred the event.

All

All the device types, and you can set the following filter conditions: group, priority, and status.

Video Intercom

For the events of video intercom, you need to select searching scope: All Record and Only Unlocking.

- **All Records**: You can filter the events from all the video intercom events, and you need to set the following filter conditions: device, priority, status.
- **Only Unlocking**: You can filter the events from all the video intercom unlocking events, and you need to set the following filter conditions: device, unlocking type.

Access Control

For the events of access control, you can set the following filter conditions: device, priority, status, event type, card reader type, person name, card no., organization.

Note

Click **Show More** to set the event type, card reader type, person name, card no., organization.

Group

The group of the device that occurred the event. You should set the group as condition only when you select the Device Type as **All**.

Device

The device that occurred the event.

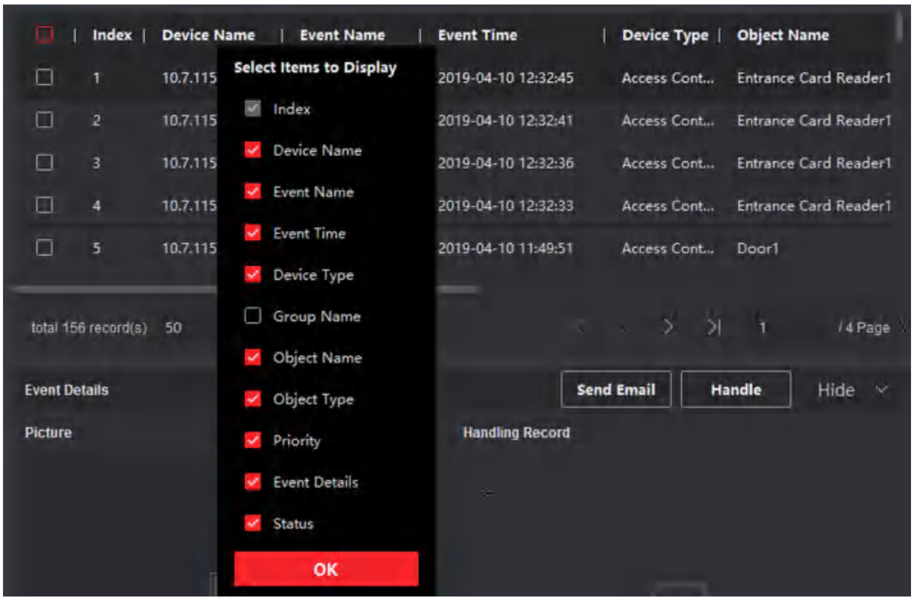
Priority

The priority including low, medium, high and uncategorized which indicates the urgent degree of the event.

Status

The handling status of the event.

3. Click **Search** to search the events according the conditions you set.
4. **Optional:** Right click the table header of the event list to customize the event related items to be displayed in the event list.



☐	Index	Device Name	Event Name	Event Time	Device Type	Object Name
☐	1	10.7.115		2019-04-10 12:32:45	Access Cont...	Entrance Card Reader1
☐	2	10.7.115		2019-04-10 12:32:41	Access Cont...	Entrance Card Reader1
☐	3	10.7.115		2019-04-10 12:32:36	Access Cont...	Entrance Card Reader1
☐	4	10.7.115		2019-04-10 12:32:33	Access Cont...	Entrance Card Reader1
☐	5	10.7.115		2019-04-10 11:49:51	Access Cont...	Door1

total 156 record(s) 50

Select Items to Display

☑ Index
☑ Device Name
☑ Event Name
☑ Event Time
☑ Device Type
☐ Group Name
☑ Object Name
☑ Object Type
☑ Priority
☑ Event Details
☑ Status

Figure 7-13 Customize Event Related Items to be Displayed

5. **Optional:** Handle the event(s).
   - Handle single event: Select one event that need to be processed, and then click **Handle** in the event information details page, and enter the processing suggestion.
   - Handle events in a batch: Select the events which need to be processed, and then click **Handle in Batch**, and enter the processing suggestion.

Note

After an event is handled, the **Handle** button will become **Add Remark**, click **Add Remark** to add more remarks for this handled event.

6. **Optional:** Select an event and then click **Send Email**, and the information details of this event will be sent by email.

   Note

   You should configure the email parameters first, see *Set Email Parameters* in the user manual of client software for details.

7. **Optional:** Click **Export** to export the event log or event pictures to the local PC in CSV format. You can set the saving path manually.
8. Hover the cursor on the related picture, and then click the download icon on the upper-right corner of the picture to download it to the local PC. You can set the saving path manually.

7.11 Time and Attendance

The Time and Attendance module provides multiple functionalities to track and monitor when employees start and stop work, and full control of employees working hours such as late arrivals, early departures, time taken on breaks and absenteeism.

Note

In this section, we introduce the configurations before you can getting the attendance reports. The access records recorded after these configurations will be calculated in the statistics.

7.11.1 Configure Attendance Parameters

You can configure the attendance parameters, including the general rule, overtime parameters, attendance check point, holiday, leave type, etc.

Set Weekend

The days of weekends may vary in different countries and regions. The client provides weekends definition function. You can select one or more days as the weekends according to actual requirements, and set different attendance rules for weekends from workdays.

Steps

Note

The parameters configured here will be set as default for the newly added time period. It will not affect the existed one(s).

1. Enter Time & Attendance module.
2. Click **Attendance Settings → General Rule** .
3. Select the day(s) as weekend, such as Saturday and Sunday.
4. Click **Save**.

Configure Overtime Parameters

You can configure the overtime parameters for workday and weekend, including overtime level, work hour rate, attendance status for overtime, etc.

Steps

1. Click **Time & Attendance → Attendance Settings → Overtime** .
2. Set required information.

   Overtime Level for Workday

   When you work for a certain period after end-work time on workday, you will reach different overtime level: overtime level 1, overtime level 2 and overtime level 3. You can set different work hour rate for three overtime levels, respectively.

   Work Hour Rate

   Work Hour Rate is used to calculate work hours by multiplying it by overtime. When you work for a certain period after end-work time on workday, you will reach different overtime level. You can set different work hour rates (1-10, can be a decimal) for three overtime levels. For example, your valid overtime is one hour (in overtime level 1), and the work hour rate of overtime level 1 is set as 2, then the work hours in the period will be calculated as 2 hours.

   Overtime Rule for Weekend

   You can enable overtime rule for weekend and set calculation mode.
3. Click **Save**.

Configure Attendance Check Point

You can set the card reader(s) of the access point as the attendance check point, so that the authentication on the card readers will be recorded for attendance .

Before You Start

You should add access control device before configuring attendance check point. For details, refer to ***Add Device*** .

Steps

Note

By default, all card readers of the added access control devices are set as attendance checkpoint.

1. Enter the Time & Attendance module.

2. Click **Attendance Settings → Attendance Check Point** to enter the Attendance Check Point Settings page.
3. **Optional:** Set **Set All Card Readers as Check Points** switch to off.

   Only the card readers in the list will be set as the attendance check points.
4. Check the desired card reader(s) in the device list as attendance check point(s).
5. Set check point function as **Start/End-Work**, **Start-Work** or **End-Work**.
6. Click **Set as Check Point**.

   The configured attendance check point displays on the right list.

Configure Holiday

You can add the holiday during which the check-in or check-out will not be recorded.

Add Regular Holiday

You can configure a holiday which will take effect annually on regular days during the effective period, such as New Year's Day, Independence Day, Christmas Day, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Check **Regular Holiday** as holiday type.
4. Custom a name for the holiday.
5. Set the first day of the holiday.
6. Enter the number of the holiday days.
7. Set the attendance status if the employee works on holiday.
8. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year.
9. Click **OK**.

   The added holiday will display in the holiday list and calendar.

   If the date is selected as different holidays, it will be recorded as the first-added holiday.
10. **Optional:** After adding the holiday, perform one of the following operations.

Edit Holiday	Click ✎ to edit the holiday information.
Delete Holiday	Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Add Irregular Holiday

You can configure a holiday which will take effect annually on irregular days during the effective period, such as Bank Holiday.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Holiday** to enter the Holiday Settings page.
3. Click **Add** to open the Add Holiday page.
4. Check **Irregular Holiday** as holiday type.
5. Custom a name for the holiday.
6. Set the start date of the holiday.

   Example

   If you want to set the forth Thursday in November, 2019 as the Thanksgiving Day holiday, you should select 2019, November, 4th, and Thursday from the four drop-down lists.
7. Enter the number of the holiday days.
8. Set the attendance status if the employee works on holiday.
9. **Optional:** Check **Repeat Annually** to make this holiday setting effective every year
10. Click **OK**.

    The added holiday will display in the holiday list and calendar.

    If the date is selected as different holidays, it will be recorded as the first-added holiday.
11. **Optional:** After adding the holiday, perform one of the following operations.

    Edit Holiday Click ✎ to edit the holiday information.

    Delete Holiday Select one or more added holidays, and click **Delete** to delete the holiday(s) from the holiday list.

Configure Leave Type

You can customize the leave type (major leave type and minor leave type) according to actual needs. You can also edit or delete the leave type.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → Leave Type** to enter the Leave Type Settings page.
3. Click **Add** on the left to add a major leave type.
4. **Optional:** Perform one of the following operations for major leave type.

   Edit Move the cursor over the major leave type and click ✎ to edit the major leave type.

   Delete Select one major leave type and click **Delete** on the left to delete the major leave type.
5. Click **Add** on the right to add a minor leave type.
6. **Optional:** Perform one of the following operations for minor leave type.

   Edit Move the cursor over the minor leave type and click ✎ to edit the minor leave type.

Delete Select one or multiple major leave types and click **Delete** on the right to delete the selected minor leave type(s).

Synchronize Authentication Record to Third-Party Database

The attendance data recorded in client software can be used by other system for calculation or some other operations. You can enable synchronization function to apply the authentication record from client software to the third-party database automatically.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Settings → Third-Party Database** .
3. Set **Apply to Database** switch to on to enable synchronization function.
4. Select database Type as **SQLServer** or **MySql**.

   Note

   If you select **MySql**, you should import the configuration file (libmysql.dll) from local PC.

5. Set the other required parameters of the third-party database, including server IP address, database name, user name and password.
6. Set table parameters of database according to the actual configuration.
   1) Enter the table name of the third-party database.
   2) Set the mapped table fields between the client software and the third-party database.
7. Click **Save** to test whether database can be connected and save the settings for the successful connection.
   - The attendance data will be written to the third-party database.
   - During synchronization, if the client disconnects with the third-party database, the client will start reconnection every 30 mins. After being reconnected, the client will synchronize the data recorded during the disconnected time period to the third-party database.

Configure Break Time

You can add break time and set start time, end time, duration, calculation mode and other parameters for the break. The added break time can also be edited or deleted.

Steps

1. Click **Time & Attendance → Timetable** .

   The added timetables are displayed in the list.
2. Select an added timetable or click **Add** to enter setting timetable page.
3. Click **Break Time** to enter Break Time page.
4. Click **Break Time Settings**.
5. Add break time.
   1) Click **Add**.

2) Enter a name for the break time.
3) Set related parameters for the break time.

Start Time / End Time

Set the time when the break starts and ends.

No Earlier Than / No Later Than

Set the earliest swiping time for starting break and the latest swiping time for ending break.

Break Duration

The duration from start time to end time of the break.

Calculation

Auto Deduct

The fixed break duration will be excluded from work hours.

Must Check

The break duration will be calculated and excluded from work hours according to actual check-in and check-out time.

Note

If you select **Must Check** as calculation method, you need to set attendance status for late or early returning from break.

6. Click **Save** to save the settings.
7. **Optional:** Click **Add** to continue adding break time.

Configure Report Display

You can configure display contents displayed in the attendance report, such as the company name, logo, date format, time format, and mark.

Steps

1. Enter Time & Attendance module.
2. Click **Attendance Statistics → Report Display** .
3. Set the display settings for attendance report.

Company Name

Enter a company name to display the name in the report.

Attendance Status Mark

Enter the mark and select the color. The related fields of attendance status in the report will display with the mark and color.

Weekend Mark

Enter the mark and select the color. The weekend fields in the report will display with the mark and color.

4. Click **Save**.

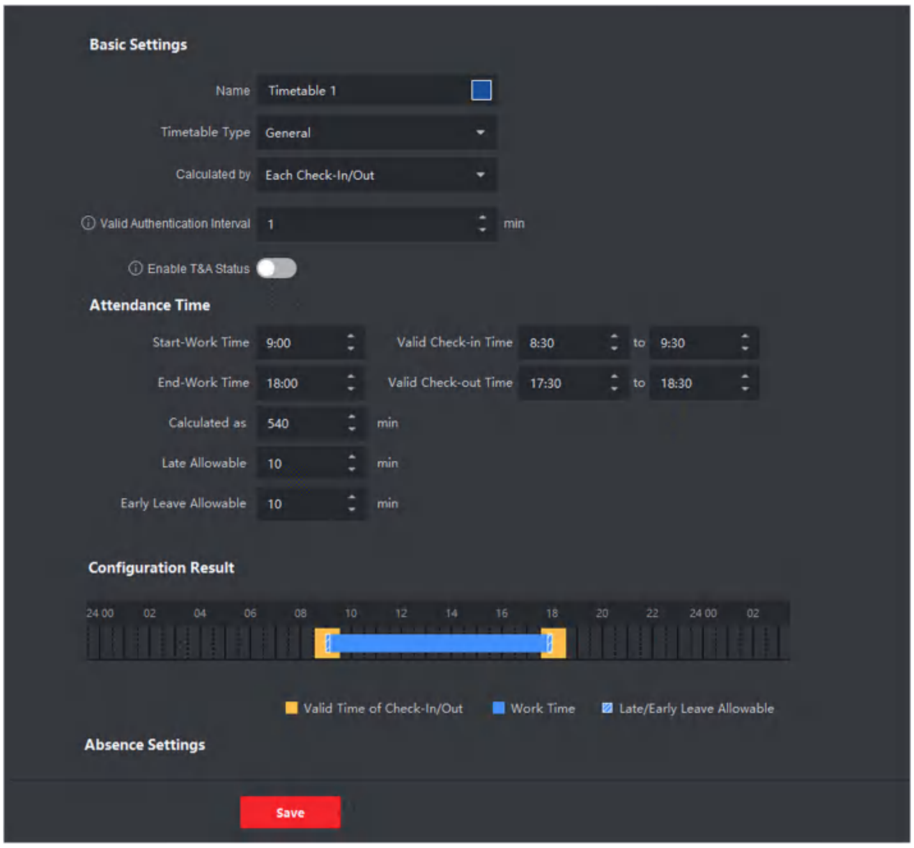
7.11.2 Add General Timetable

On the timetable page, you can add general timetable for employees, which requires the fixed start-work time and end-work time. Also, you can set valid check-in/out time, allowable timetable for being late and leaving early.

Steps

1. Click **Time and Attendance → Timetable** to enter the timetable settings page.

2. Click **Add** to enter add timetable page.



Basic Settings

Name: Timetable 1

Timetable Type: General

Calculated by: Each Check-In/Out

Valid Authentication Interval: 1 min

Enable T&A Status

Attendance Time

Start-Work Time: 9:00 Valid Check-in Time: 8:30 to 9:30

End-Work Time: 18:00 Valid Check-out Time: 17:30 to 18:30

Calculated as: 540 min

Late Allowable: 10 min

Early Leave Allowable: 10 min

Configuration Result

Absence Settings

Save

Figure 7-14 Add Timetable

3. Create a name for the timetable.

Note

You can click the color icon beside the name to customize the color for the valid timetable on the time bar in the Configuration Result area.

4. Select the timetable type as general.

5. Select calculation method.

First In & Last Out

The first check-in time is recorded as start work time and the last check-out time is recorded as the end-work time.

Each Check-In/Out

Each check-in time and check-out time is valid and the sum of all periods between adjacent check-in and check-out time will be recorded as the valid working duration.

You need to set **Valid Authentication Interval** for this calculation method. For example, if the interval between card swiping of the same card is less than the set value, the card swiping is invalid.

6. **Optional:** Set **Enable T&A Status** switch to on to calculate according to attendance status of the device.

Note

This function should be supported by the device.

7. Set the related attendance time parameters as the following:

Start/End-Work Time

Set the start-work time and end-work-time.

Valid Check-in/out Time

On the time bar, adjust the yellow bar to set the timetable during which the check-in or check-out is valid.

Calculated as

Set the duration calculated as the actual work duration.

Late/Early Leave Allowable

Set the timetable for late or early leave.

8. Set absence related parameters.

Check-In, Late for

You can set the late time duration for the employee who has checked in but is late for work. If the employee exceeds the required time period, his/her attendance data will be marked as absent.

Check-Out, Early Leave for

You can set the early leave time duration for the employee who checks out earlier than the normal leave time, and his/her attendance data will be marked as absent.

No Check-in

If the employee does not check in, his/her attendance data may be marked as absent or late.

No Check-Out

If the employee does not check out, his/her attendance data may be marked as absent or early leave.

9. Click **Save** to add the timetable.

10. Optional: Perform one or more following operations after adding timetable.

Edit Timetable	Select a timetable from the list to edit related information.
Delete Timetable	Select a timetable from the list and click **Delete** to delete it.

7.11.3 Add Shift

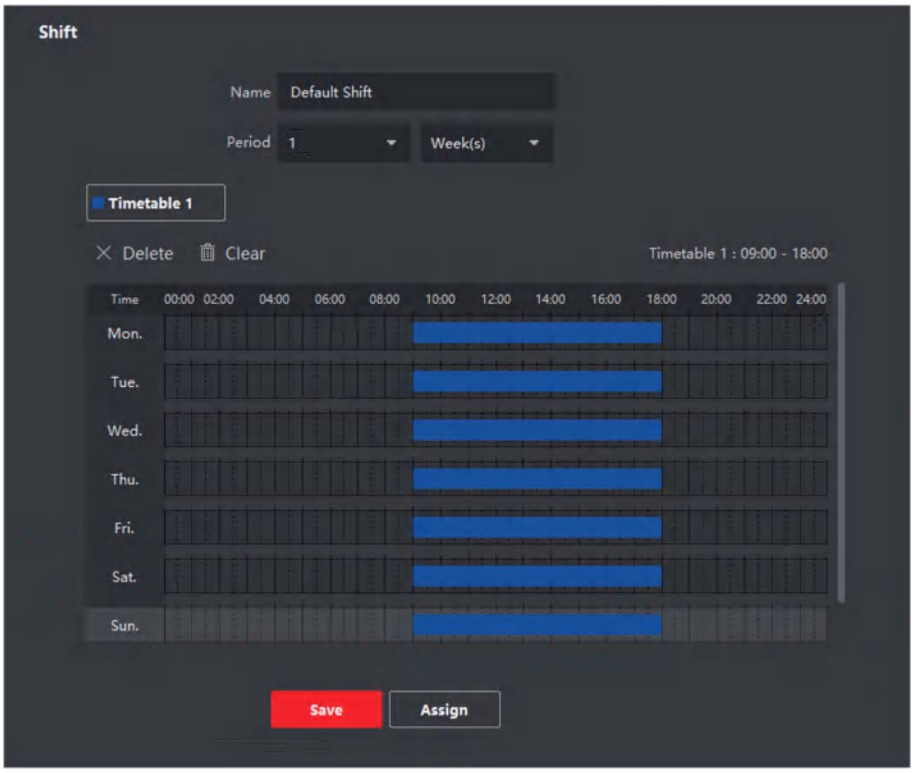
You can add shift for employees including setting shift period (day, week, month) and the effective attendance time. According to the actual requirements, you can adding multiple timetables in one shift for employees, which requires them to check in and check out for each timetable.

Before You Start

Add a timetable first. See ***Add General Timetable*** for details.

Steps

1. Click **Time & Attendance → Shift** to enter shift settings page.
2. Click **Add** to enter Add Shift page.
3. Enter the name for shift.
4. Select the shift period from the drop-down list.
5. Select the added timetable and click on the time bar to apply the timetable.



Shift

Name: Default Shift

Period: 1 Week(s)

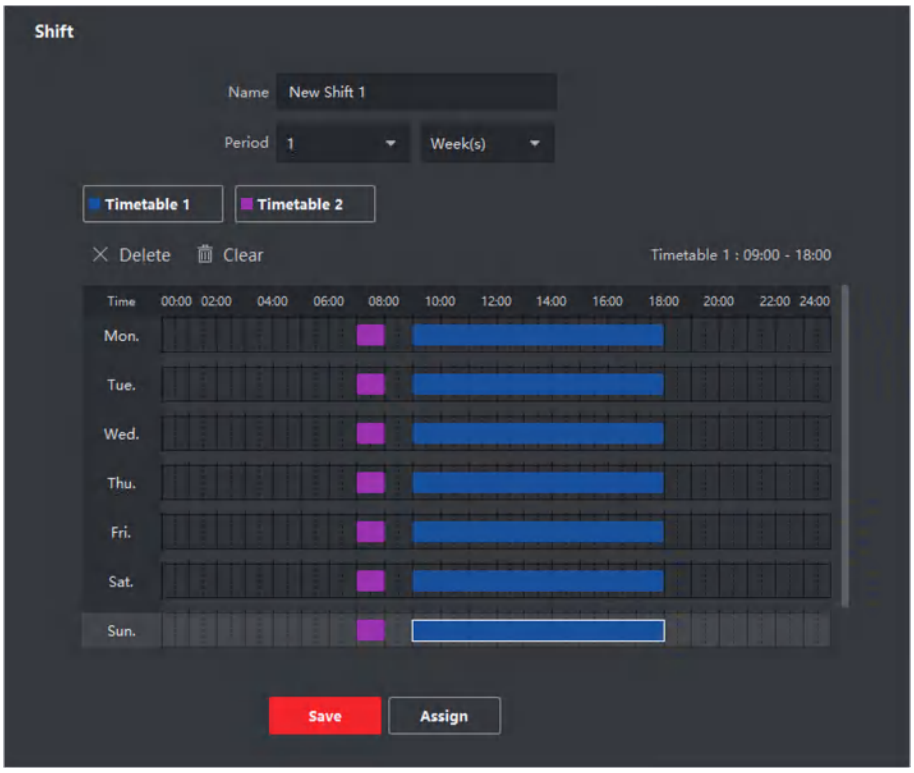
Timetable 1

Timetable 1 : 09:00 - 18:00

Figure 7-15 Add Shift

Note

You can select more than one timetables. The start and end work time and the valid check-in and out time in different time tables can not be overlapped.



Shift
Name New Shift 1
Period 1 Week(s)
Timetable 1
Timetable 2
Delete
Clear
Timetable 1 : 09:00 - 18:00
Time 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Sun.
Save
Assign

Figure 7-16 Add Multiple Timetables

6. Click **Save**.

   The added shift lists on the left panel of the page. At most 64 shifts can be added.

7. **Optional:** Assign the shift to organization or person for a quick shift schedule.
   1) Click **Assign**.
   2) Select **Organization** or **Person** tab and check the desired organization(s) or person(s) box.

      The selected organizations or persons will list on the right page.
   3) Set the Expire Date for the shift schedule.
   4) Set other parameters for the schedule.

      Check-in Not Required

      Persons in this schedule do not need to check-in when they come to work.

      Check-out Not Required

      Persons in this schedule do not need to check-out when they end work.

      Scheduled on Holidays

      On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

Effective for Overtime

The persons' overtime will be recorded for this schedule.

5) Click **Save** to save the quick shift schedule.

7.11.4 Manage Shift Schedule

Shift work is an employment practice designed to make use of all 24 hours of the clock each day of the week. The practice typically sees the day divided into shifts, set periods of time during which different shifts perform their duties.

You can set department schedule, person schedule, and temporary schedule.

Set Department Schedule

You can set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Before You Start

In Time & Attendance module, the department list is the same with the organization. You should add organization and persons in Person module first. See ***Person Management*** for details.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Department Schedule** to enter Department Schedule page.
3. Select the department from the organization list on the left.

Note

If **Include Sub Organization** is checked, when selecting the organization, its sub organizations are selected at the same time.

4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

Note

This is only available for shift with only one timetable.

Multiple Shift Schedules

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

   Check-in Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Scheduled on Holidays

   On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.
8. Click **Save**.

Set Person Schedule

You can assign the shift schedule to one or more persons. You can also view and edit the person schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The person schedule has the higher priority than department schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule page.
2. Click **Person Schedule** to enter Person Schedule page.
3. Select the organization and select the person(s).
4. Select the shift from the drop-down list.
5. **Optional:** Enable **Multiple Shift Schedules** and select the effective time period(s) from the added timetables for the persons.

   Note

   This is only available for shift with only one timetable.

   Multiple Shift Schedules

   It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.
   If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be

effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

6. Set the start date and end date.
7. Set other parameters for the schedule.

   Check-in Not Required

   Persons in this schedule do not need to check-in when they come to work.

   Check-out Not Required

   Persons in this schedule do not need to check-out when they end work.

   Scheduled on Holidays

   On the holidays, this schedule is still effective and the persons needs to go to work according to the schedule.

   Effective for Overtime

   The persons' overtime will be recorded for this schedule.
8. Click **Save**.

Set Temporary Schedule

You can add a temporary schedule for the person and the person will be assigned with the shift schedule temporarily. You can also view and edit the temporary schedule details.

Before You Start

Add department and person in Person module. See ***Person Management*** for details.

Steps

Note

The temporary schedule has higher priority than department schedule and person schedule.

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Click **Temporary Schedule** to enter Temporary Schedule page.
3. Select the organization and select the person(s).
4. Click one date or click and drag to select multiple dates for the temporary schedule.
5. Select **Workday** or **Non-Workday** from drop-down list.

   If **Non-Workday** is selected, you need to set the following parameters.

   Calculated as

   Select normal or overtime level to mark the attendance status for temporary schedule.

   Timetable

   Select a timetable from drop-down list.

   Multiple Shift Schedule

It contains more than one timetables. The person can check in/out in any of the timetables and the attendance will be effective.

If the multiple shift schedules contains three timetables: 00:00 to 07:00, 08:00 to 15:00 and 16:00 to 23:00. The attendance of the person adopting this multiple shift schedules will be effective in any of the three timetables. If the person checks in at 07:50, it will apply the nearest timetable 08:00 to 15:00 to the person's attendance.

Rule

Set other rule for the schedule, such as **Check-in Not Required**, and**Check-out Not Required**.

6. Click **Save**.

Check Shift Schedule

You can check the shift schedule in calendar or list mode. You ca also edit or delete the shift schedule.

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the Shift Schedule Management page.
2. Select the organization and corresponding person(s).
3. Click ▦ or ☰ to view the shift schedule in calendar or list mode.

Calendar

In calendar mode, you can view the shift schedule for each day in one month. You can click the temporary schedule for one day to edit or delete it.

List

In list mode, you can view the shift schedule details about one person or organization, such as shift name, type, effective period and so on. Check the shift schedule(s), and click **Delete** to delete the selected shift schedule(s).

7.11.5 Manually Correct Check-in/out Record

If the attendance status is not correct, you can manually correct the check-in or check out record. You can also edit, delete, search, or export the check-in or check-out record.

Before You Start

- You should add organizations and persons in Person module. For details, refer to ***Person Management*** .
- The person's attendance status is incorrect.

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Correct Check-In/Out** to enter adding the check-in/out correction page.
3. Select person from left list for correction.
4. Select the correction date.

5. Set the check-in/out correction parameters.
   - Select **Check-in** and set the actual start-work time.
   - Select **Check-out** and set the actual end-work time.

Note

You can click ⊕ to add multiple check in/out items. At most 8 check-in/out items can be supported.

6. **Optional:** Enter the remark information as desired.
7. Click **Save**.
8. **Optional:** After adding the check-in/out correction, perform one of the following operations.

View Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.

Note

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

Edit
- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the related filed in Date, Handling Type, Time, or Remark column to edit the information.

Delete Delete the selected items.

Export Export the attendance handling details to local PC.

Note

The exported details are saved in CSV format.

7.11.6 Add Leave and Business Trip

You can add leave and business trip when the employee want to ask for leave or go on a business trip.

Before You Start

You should add organizations and persons in the Person module. For details, refer to ***Person Management*** .

Steps

1. Click **Time & Attendance → Attendance Handling** to enter attendance handling page.
2. Click **Apply for Leave/Business Trip** to enter adding the leave/business trip page.
3. Select person from left list.
4. Set the date(s) for your leave or business trip.
5. Select the major leave type and minor leave type from the drop-down list.

Note

You can set the leave type in Attendance Settings. For details, refer to ***Configure Leave Type*** .

6. Set the time for leave.
7. **Optional:** Enter the remark information as desired.
8. Click **Save**.
9. **Optional:** After adding the leave and business trip, perform one of the following operations.

View
Click ▦ or ☰ to view the added attendance handling information in calendar or list mode.

Note

In calendar mode, you need to click **Calculate** to get the attendance status of the person in one month.

Edit
- In calendar mode, click the related label on date to edit the details.
- In list mode, double-click the filed in Date, Handling Type, Time, or Remark column to edit the related information.

Delete
Delete the selected items.

Export
Export the attendance handling details to local PC.

Note

The exported details are saved in CSV format.

7.11.7 Calculate Attendance Data

You need to calculate the attendance data before searching and viewing the overview of the attendance data, employees' detailed attendance data, employees' abnormal attendance data, the employees' overtime working data, and card swiping log.

Automatically Calculate Attendance Data

You can set a schedule so that the client can automatically calculate attendance data of the previous day at the time you configured every day.

Steps

Note

1. Enter the Time & Attendance module.
2. Click **Attendance Settings → General Rule** .

3. In the Auto-Calculate Attendance area, set the time that you want the client to calculate the data.
4. Click **Save**.

   The client will calculate the attendance data of the previous day from the time you have configured.

Manually Calculate Attendance Data

You can manually calculate attendance data by setting conditions including attendance time, department, attendance status, etc.

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Calculation** .
3. Set the start time and end time to define the attendance data range.
4. Select the department from the drop-down list.
5. **Optional:** Set other conditions, including name and person ID.
6. Check attendance status (supports multi-selection).
7. Click **Calculate**.

   Note

   Only the attendance data within three months can be calculated.

8. **Optional:** Perform one of the following operations.

   Correct Check-in/out
   Select one person, click **Correct Check-in/out** to add check-in/out correction.

   Select Items to Display
   Click ⚙ on the upper right corner, or right click the table header of the attendance data list to customize the items to be displayed in the list.

   Adjust Items Sequence
   Click one item (except Person ID) and move the mouse to customize the sequence of different items.

   Generate Report
   Click **Report** to generate the attendance report.

   Note

   The report items will be displayed in the sequence you have set.

   Export Report
   Click **Export** to export attendance data (CSV file) to local PC.

   Note

   The report items will be displayed in the sequence you have set.

7.11.8 Attendance Statistics

You can check the original attendance record, generate and export the attendance report based on the calculated attendance data.

Get an Overview of Employees' Attendance Data

You can search and view the employee's attendance records on the client, including attendance time, attendance status, check point, etc.

Before You Start

- You should add organizations and persons in Person module and the persons have swiped cards. For details, refer to ***Person Management*** .
- Calculate the attendance data.

Note

- The client will automatically calculate the previous day's attendance data at 1:00 am on the next day.
- Keep the client running at 1:00 am or it cannot calculate the previous day's attendance data automatically. If not calculated automatically, you can calculate the attendance data manually. For details, refer to ***Manually Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Attendance Record** .
3. Set the attendance start time and end time that you want to search.
4. Set other search conditions, including department, name, and person ID.
5. Select data source as **Original Records on Device** or **Manual Handling Records**.
6. **Optional:** Click **Get Events from Device** to get the attendance data from the device.
7. **Optional:** Click **Reset** to reset all the search conditions and edit the search conditions again.
8. Click **Search**.

   The result displays on the page. You can view the employee's required attendance status and check point.
9. **Optional:** After searching the result, perform one of the following operations.

Generate Report	Click **Report** to generate the attendance report.
Export Report	Click **Export** to export the results to the local PC.
Custom Export	For details, refer to .

Generate Instant Report

It supports to generate the a series of attendance reports manually to view the employees' attendance results.

Before You Start
Calculate the attendance data.

Note

You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

Steps

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Report** .
3. Select a report type.
4. Select the department or person to view the attendance report.
5. Set the start time and end time during which the attendance data will be displayed in the report.
6. Click **Report** to generate the statistics report and open it.

Custom Attendance Report

The client supports multiple report types and you can pre-define the report content and it can send the report automatically to the email address you configured.

Steps

Note

Set the email parameters before you want to enable auto-sending email functions. For details, refer to *Set Email Parameters* in the user manual of the client software.

1. Enter the Time & Attendance module.
2. Click **Attendance Statistics → Custom Report** .
3. Click **Add** to pre-define a report.
4. Set the report content.

   Report Name

      Enter a name for the report.

   Report Type

      Select one report type and this report will be generated.

   Report Time

      The time to be selected may vary for different report type.

Person

Select the added person(s) whose attendance records will be generated for the report.

5. **Optional:** Set the schedule to send the report to the email address(es) automatically.
   1) Check the **Auto-Sending Email** to enable this function.
   2) Set the effective period during which the client will send the report on the selected sending date(s).
   3) Select the date(s) on which the client will send the report.
   4) Set the time at which the client will send the report.

   Example

   If you set the effective period as ***2018/3/10 to 2018/4/10***, select ***Friday*** as the sending date, and set the sending time as ***20:00:00***, the client will send the report at 8 p.m. on Fridays during 2018/3/10 to 2018/4/10.

   Note

   Make sure the attendance records are calculated before the sending time. You can calculate the attendance data manually, or set the schedule so that the client can calculate the data automatically every day. For details, refer to ***Calculate Attendance Data*** .

   5) Enter the receiver email address(es).

   Note

   You can click **+** to add a new email address. Up to 5 email addresses are allowed.

   6) **Optional:** Click **Preview** to view the email details.
6. Click **OK**.
7. **Optional:** After adding the custom report, you can do one or more of the followings:

Edit Report	Select one added report and click **Edit** to edit its settings.
Delete Report	Select one added report and click **Delete** to delete it.
Generate Report	Select one added report and click **Report** to generate the report instantly and you can view the report details.

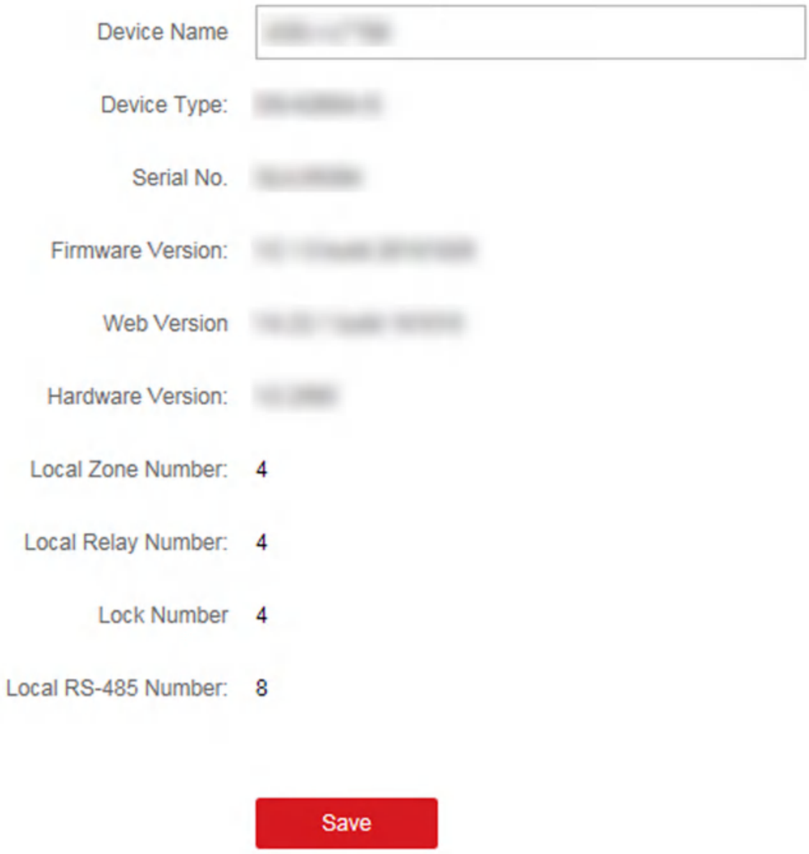
7.12 Remote Configuration (Web)

Configure device parameters remotely.

7.12.1 View Device Information

View and set device name, view device type, serial No., version, relay number, and lock number.

Select a device from the Device for Management tab and click ⚙ → **System** → **Device Information** to enter the Device Information page.



Device Name [redacted]

Device Type: [redacted]

Serial No. [redacted]

Firmware Version: [redacted]

Web Version [redacted]

Hardware Version: [redacted]

Local Zone Number: 4

Local Relay Number: 4

Lock Number 4

Local RS-485 Number: 8

Figure 7-18 View Device Information

You can set the device name, view the device type, serial No., version, relay number, and lock number. Click **Save** to save the settings.

7.12.2 Change Device Password

You can change the device password.

Before You Start

Make sure the device is activated. For details, see *Activation*.

Steps

1. On the Device for Management page, click ⚙ → **System** → **User** to enter the User tab.
2. Select a user and click **Edit** to enter the Edit page.
3. Input the old password, create a new password, and confirm the new 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.

4. Click **OK**.

Result

The device password is changed. You should enter the new password on the Device for Management page to reconnect the device.

7.12.3 Time Management

Manage device's time zone, time synchronization, and DST parameters.

Time Zone and Time Synchronization

On the Device for Management page, select a device and click ⚙ → **System** → **Time** to enter the Time tab.
You can select a time zone, set NTP parameters, or manually synchronize time.

Time Zone

Select a time zone from the drop-down list.

NTP

The device will synchronize time with NTP automatically. After you enable **NTP**, you should set the NTP server address, NTP port, and synchronization interval.

Manual Time Synchronization

After you enable **Manual Time Synchronization**, you can manually set the device time.

If you check **Synchronize with Computer Time**, the **Set Time** will display the current computer's time. At this time, uncheck **Synchronize with Computer Time**, and click 📅 , you can edit the device time manually.

Click **Save** to save the settings.

DST

On the Device for Management page, click **Remote Configuration** → **System** → **Time** → **DST** to enter the DST tab.
Enable DST and you can edit the DST bias time, the DST start time, and end time.
Click **Save**.

7.12.4 System Maintenance

You can reboot the device, restore the device to the default settings, and upgrade the device.

Reboot

On the Device for Management page, click ⚙ → **System → System Maintenance** to enter the System Maintenance tab.
Click **Reboot** and the device starts rebooting.

Restore Default Settings

On the Device for Management page, click **Remote Configuration → System → System Maintenance** to enter the System Maintenance tab.

Restore Default

The parameters will be restored the default ones, excluding the IP address.

Restore All

All device parameters will be restored to the default ones. The device should be activated after restoring.

Upgrade

On the Device for Management page, click **Remote Configuration → System → System Maintenance** to enter the System Maintenance tab.
Select a device type from the drop-down list, click **Browse** and select an upgrade file from the local computer, and click **Upgrade**.

Note

- If you select Card reader as the device type, you should also select a card reader No. from the drop-down list.
- The upgrade will lasts for about 2 min. Do not power off during the upgrading. After upgrading, the device will reboot automatically.

7.12.5 Configure RS-485 Parameters

You can set the RS-485 parameters including the baud rate, data bit, stop bit, parity type, communication mode, work mode, and connection mode.

Steps

1. Click **Maintenance and Management → Device** to enter the device list.
2. Click ⚙ to enter the remote configuration page.
3. Click **System → RS-485 Settings** to enter the Configuring the RS-485 Parameters tab.
4. Select the serial No. of the port from the drop-down list to set the RS-485 parameters.
5. Set the baud rate, data bit, the stop bit, parity, flow control, communication mode, working mode, and the connection mode from the drop-down list.

6. Click **Save** and the configured parameters will be applied to the device automatically.

   Note

   After changing the working mode, the device will be rebooted. A prompt will be popped up after changing the working mode.

7.12.6 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click ⚙ → **System** → **Security** to enter the Security Mode tab.

Select a security mode from the drop-down list, and click **Save**.

You can also enable **SSH** or **HTTP** to get a more secure network.

Security Mode

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

Compatible Mode

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

7.12.7 Network Parameters Settings

Set device network parameters, including the NIC type, DHCP, and HTTP.

On the Device for Management page, click ⚙ → **Network** → **Network Parameters** to enter the Network Parameters Settings tab.

NIC Type

Select a NIC type from the drop-down list. You can select either Self-adaptive, 10M, or 100M.

DHCP

If you disable the function, you should manually set the device's IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU, and port.

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

HTTP

Set the HTTP port, DNS1 server address, and DNS2 server address.

7.12.8 Report Strategy Settings

You can set the center group for uploading the log via the EHome protocol.

On the Device for Management page, click ⚙ → **Network** → **Report Strategy** to enter the Report Strategy Settings tab.

You can set the center group and the system will transfer logs via EHome protocol. Click **Save** to save the settings.

Center Group

Select a center group from the drop-down list.

Main Channel

The device will communicate with the center via the main channel.

Note

N1 refers to wired network.

7.12.9 Network Center Parameters Settings

You can set the notify surveillance center, center's IP address, the port No., the protocol (EHome), the EHome account user name,etc. to transmit data via EHome protocol.

On the Device for Management page, click **Remote Configuration** → **Network** → **Network Center Parameters** to enter the Network Center Parameters Settings tab.

Select a center from the drop-down list.

After enabling the function, you can set the center's address type, IP address/domain name, and port No., create EHome user name, etc.

Note

If set the EHome type as EHome5.0, you should create an EHome key as well.

Click **Save**.

After creating the EHome information, you can add the device via EHome protocol.

7.12.10 Configure Wi-Fi

Steps

1. On the Device for Management page, click ⚙ → **Network** → **Wi-Fi** to enter the **Wi-Fi Settings** tab.
2. Check **Enable** to enable the Wi-Fi function.
3. Enter the SSID name and password or you can select a network from the Wi-Fi list.
4. Set the Wi-Fi **Security Mode** from the drop-down list.
5. **Optional:** Click **Refresh** to refresh the network status.
6. **Optional:** Set WLAN parameters.
   1) On the **Wi-Fi Settings** page, click **WLAN** to enter the **WLAN** page.
   2) Uncheck **DHCP** and set the IP address, the subnet mask, the default gateway, the MAC address, the DNS1 IP Address, and the DNS2 IP address.

7. Click **Save**.

7.12.11 Set Relay Parameters

Click **Maintenance and Management → Device** to enter the device list.

Click ⚙ to enter the remote configuration page.

Click **Alarm → Relay** . Select a relay and click ⚙ and set the relay name and output delay time. Click **OK** to save the settings.

7.12.12 Set Access Control Parameters

Steps

1. On the Device for Management page, click ⚙ **→ Others → Access Control Parameters** to enter the **Access Control Parameters** tab.
2. Check the checkbox to enable the function.

   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.
3. Click **Save**.

7.12.13 Set CPU Card Reading Mode

Steps

1. On the Device for Management page, click ⚙ **→ Others → CPU Card Reading Settings** to enter the **CPU Card Reading Settings** tab.
2. Select a reading mode from the dropdown list.
3. Click **Save**.

7.12.14 Configure Volume Input or Output

Steps

1. On the Device for Management page, click ⚙ **→ Image → Audio Input or Output** to enter **Audio Input or Output** tab.
2. Move the block to adjust the device output volume.
3. Click **Save**.

7.12.15 Operate Relay

Steps

1. Click **Maintenance and Management → Device** to enter the device list.

2. Click ⚙ to enter the remote configuration page.
3. Click **Operation → Relay** .
4. Enable or disable the relay.

7.13 View Relay Status

Click **Maintenance and Management → Device** to enter the device list.

Click ⚙ to enter the remote configuration page.

Click **Status → Relay** and you can view the relay status.

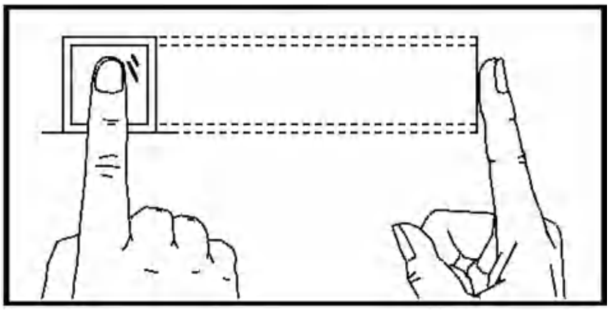
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

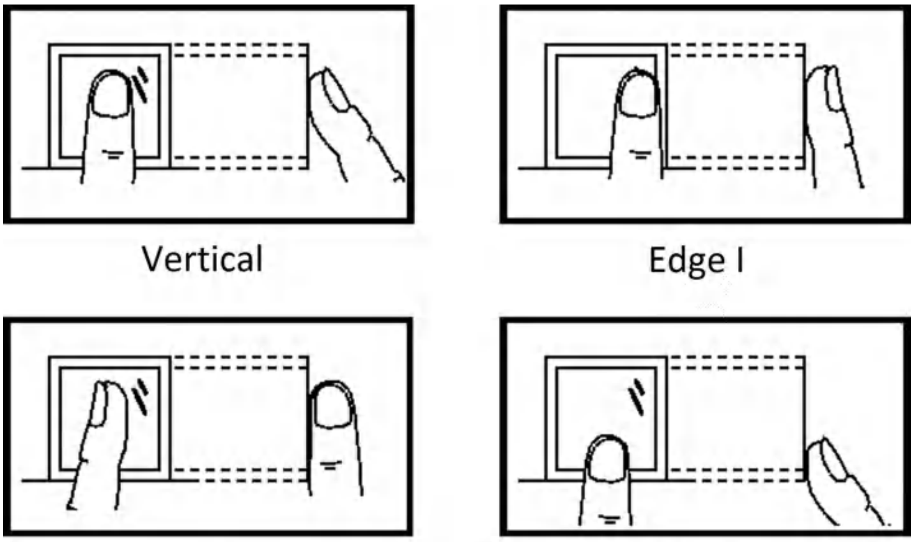
The figure displayed below is the correct way to scan your finger:



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

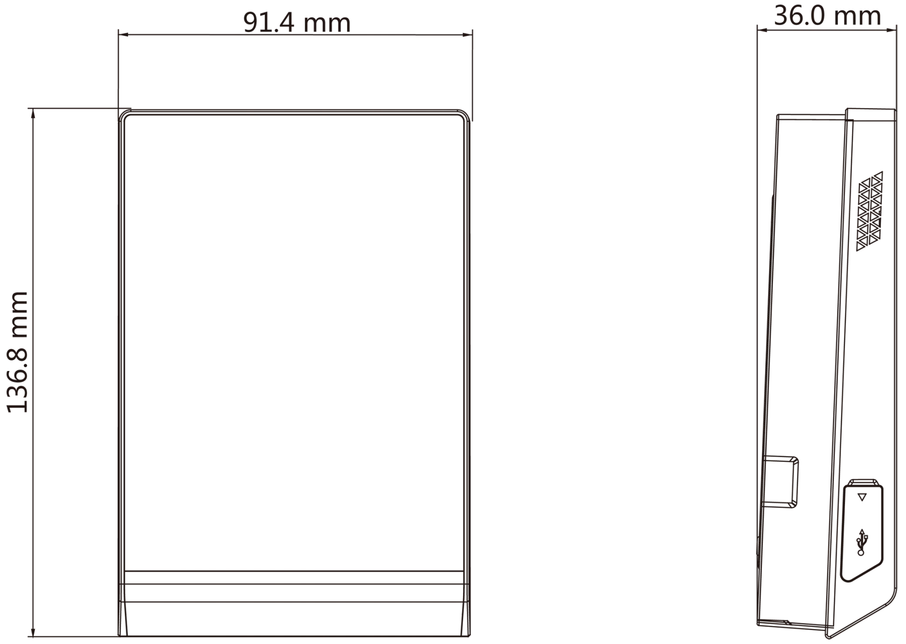
The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

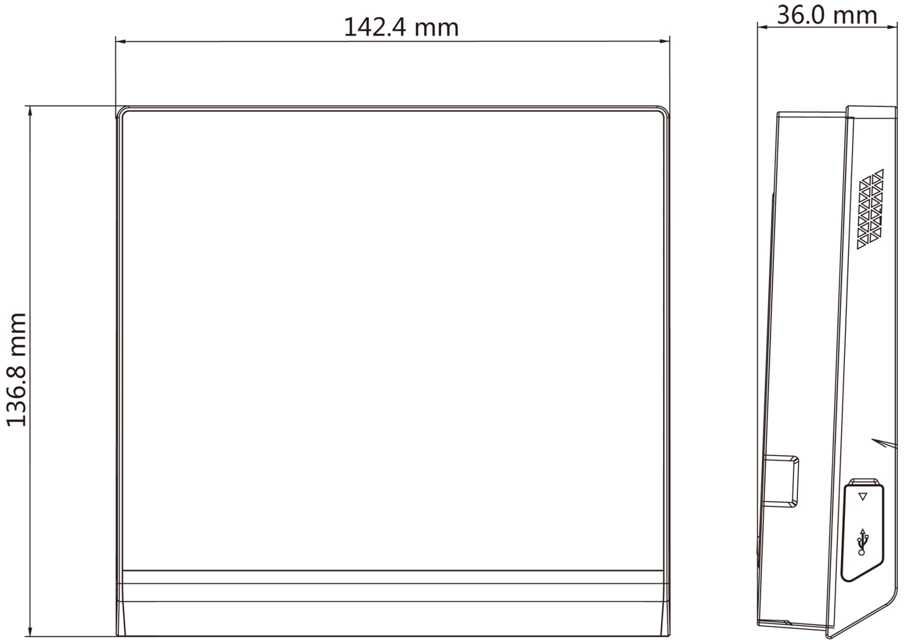
If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. Dimension

Dimension of Device without Fingerprint Module



Dimension of Device with Fingerprint Module



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