



Fingerprint Access Control Terminal

User Manual



Legal Information

User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Please use this user manual under the guidance of professionals.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. 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.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

1 Regulatory Information	1
2 Safety Instruction	2
3 Available Models	4
4 Overview and Key Features	4
5 Appearance Description	5
6 Device Wiring	7
6.1 Terminal Description	7
6.2 External Device Wiring	8
7 Installation	8
7.1 Install without Gang Box	8
7.2 Install without Gang Box	9
8 Activation	10
8.1 Activate via Device	10
8.2 Activate via SADP	10
8.3 Activate Device via Client Software	11
9 Local Settings	12
9.1 Select Language	12
9.2 Add Administrator	12
9.3 Local Login	14
9.4 Communication Settings	14
9.4.1 Set Network	14
9.4.2 Change Verification Code	15
9.4.3 Set EHome Parameters	15
9.5 Personnel Management	16
9.5.1 Add Person	16
9.5.2 Manage Person (Search/Edit/Delete)	18
9.6 Attendance Status	18
9.6.1 Set Auto Attendance	19

9.6.2 Set Manual Attendance	19
9.6.3 Set Manual and Auto Attendance	20
9.6.4 Disable Attendance Mode	21
9.7 Time and Attendance Management	21
9.7.1 Manage Department (Edit/Search/Reset)	21
9.7.2 Shift Management	22
9.7.3 Manage Holiday (Add/Search/Edit/Delete)	24
9.7.4 Shift Schedule	25
9.7.5 Export Attendance Report	27
9.7.6 Data Transfer	28
9.8 System Settings	28
9.8.1 Set Time	28
9.8.2 Manage System Data	29
9.8.3 Set System Parameters	30
9.8.4 System Upgrade	31
9.8.5 Restore Settings	32
9.8.6 View System Information	32
10 Client Software Configuration	33
10.1 Device Management	33
10.1.1 Add Device	33
10.1.2 Edit Device's Network Information	40
10.1.3 Reset Device Password	41
10.2 Person Management	41
10.2.1 Add Organization	42
10.2.2 Configure Basic Information	42
10.2.3 Issue a Card to One Person	43
10.2.4 Upload a Face Photo from Local PC	44
10.2.5 Take a Photo via Client	44

10.2.6 Collect Face via Access Control Device	45
10.2.7 Collect Fingerprint via Client	45
10.2.8 Collect Fingerprint via Access Control Device	46
10.2.9 Configure Access Control Information	47
10.2.10 Customize Person Information	48
10.2.11 Configure Resident Information	48
10.2.12 Configure Additional Information	49
10.2.13 Import and Export Person Identify Information	49
10.2.14 Import Person Information	49
10.2.15 Import Person Pictures	50
10.2.16 Export Person Information	51
10.2.17 Export Person Pictures	51
10.2.18 Get Person Information from Access Control Device	51
10.2.19 Move Persons to Another Organization	52
10.2.20 Issue Cards to Persons in Batch	52
10.2.21 Report Card Loss	53
10.2.22 Set Card Issuing Parameters	53
10.3 Configure Schedule and Template	54
10.3.1 Add Holiday	54
10.3.2 Add Template	55
10.4 Set Access Group to Assign Access Authorization to Persons	56
10.5 Configure Advanced Functions	58
10.5.1 Configure Device Parameters	58
10.5.2 Configure Remaining Open/Closed	64
10.5.3 Configure Multi-Factor Authentication	66
10.5.4 Configure Custom Wiegand Rule	68

10.5.5 Configure Card Reader Authentication Mode and Schedule	69
10.5.6 Configure First Person In	70
10.5.7 Configure Anti-Passback	71
10.5.8 Configure Multi-door Interlocking	71
10.5.9 Configure Other Parameters	72
10.6 Configure Linkage Actions for Access Control ...	78
10.6.1 Configure Client Actions for Access Event	78
10.6.2 Configure Device Actions for Access Event	79
10.6.3 Configure Device Actions for Card Swiping	80
10.6.4 Configure Device Linkage for Mobile Terminal's MAC Address	81
10.6.5 Configure Device Actions for Person ID ...	82
10.7 Door/Elevator Control	83
10.7.1 Control Door Status	84
10.7.2 Control Elevator Status	84
10.7.3 Check Real-Time Access Records	85
10.8 Time and Attendance	86
10.8.1 Configure Attendance Parameters	86
10.8.2 Add Timetable	91
10.8.3 Add Shift	92
10.8.4 Manage Shift Schedule	92
10.8.5 Manually Correct Check-in/out Record ...	95
10.8.6 Add Leave and Business Trip	96
10.8.7 Calculate Attendance Data	97
10.8.8 Attendance Statistics	98
11 Mobile Client Configuration	100
11.1 Control Door Status	100
11.2 Set Door Open Duration	101

11.3 Change Super Password	102
11.4 View Access Control Logs	103
A. Tips for Scanning Fingerprint	104
B. Access Control Capacity	105
C. Attendance Record Deleting Rule	107
D. Attendance Report Table	108

1 Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at

designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

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

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

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

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.



2 Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

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

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

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

Dangers

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- 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

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic

sweat of the fingers may erode the surface coating of the device cover.

- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- You can view the device License via the website: <http://opensource.hikvision.com/Home/List?id=46>.

3 Available Models

The fingerprint access control terminal contains the following models:

Product Name	Model
Fingerprint Access Control Terminal	DS-K1T8003F
	DS-K1T8003MF
	DS-K1T8003EF

Use only power supplies listed in the user instructions:

Model	Manufacturer	Standard
DSA-12PFT-12FUK 120100	Dee Van Enterprise Co., Ltd.	BS
DSA-12PFT-12FAU 120100	Dee Van Enterprise Co., Ltd.	AS
DSA-12PFT-12FIN 120100	Dee Van Enterprise Co., Ltd.	IS
DSA-12PFT-12FUS 120100	Dee Van Enterprise Co., Ltd.	IEC
DSA-12PFT-12 FBZ 120100	Dee Van Enterprise Co., Ltd.	NBR

4 Overview and Key Features

Overview

DS-K1T8003 series fingerprint access control terminal is designed with a 2.4-inch LCD display screen. Offline operation and wired network (TCP/IP) transmission modes are supported as well.

Key Features

- Integrated management of access control and the attendance
- 2.4-inch LCD screen to display the time, the date and swiping/fingerprint authentication results
- Remotely adds fingerprints to the system
- Accurate and fast fingerprint recognition. The recognition time duration is less than 1s
- Max. 1000 users, Max. 1000 fingerprints, Max. 100,000 event records, and Max. 50,000 attendance records.
- Different authentication types can be configured according to different situations
- Stand-alone operation: locally adds person, card and fingerprint information
- Exports the swiping card data and the attendance report to the USB flash drive
- Up to 32 normal shifts, up to 32 man-hour shifts, and up to 32 attendance holiday schedules can be configured
- Generates the attendance report automatically
- The third party doorbell access
- Tamper alarm
- Supports multiple languages: English, Vietnamese, Brazilian Portuguese, Spanish, French, Italian
- Operates via Hik-Connect mobile client

5 Appearance Description

View the device appearance and the keypad's description.

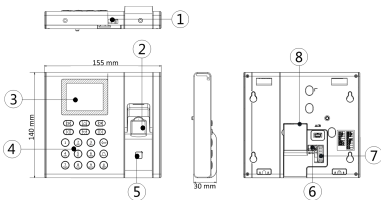


Figure 5-1 Device Appearance

Note

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

Table 5-1 Appearance Description

No.	Description
1	USB Interface
2	Fingerprint Recognition Area
3	Display Screen

No.	Description
4	Keypad
5	Card Swiping Area
6	Power Interface
7	Wiring Terminal
8	Network Interface

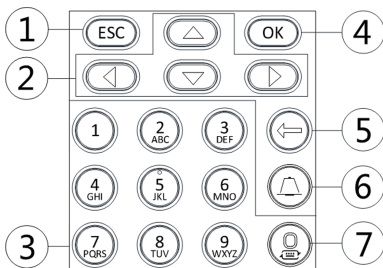


Figure 5-2 Keypad Description

Table 5-2 Keypad Description

No.	Description
1	<p>Exiting Key: Press the button to exit the menu.</p> <p>If you enable the attendance status function, the exiting key can be the shortcut key of the attendance status.</p>
2	<p>Direction Keys: Use direction keys to move the cursor in the menu.</p> <p>If you enable the attendance status function, the direction keys can be the shortcut key of the attendance status.</p>
3	<p>Numeric Keys/Letter Keys: Press to input numbers or letters.</p> <p>Key 0 can also represent a space key except you are using the number input method.</p>
4	<p>OK Key: Press OK key to confirm operations. Hold the key for 2 s to enter the login interface.</p> <p>If you enable the attendance status function, the OK key can be the shortcut key of the attendance status.</p>

No.	Description
5	Deleting Key: Press the key to delete the letters or numbers one by one in the textbox.
6	Doorbell Button: Press the doorbell button and the doorbell rings.
7	Editing Key: Press the key to enter the number 0. Hold the key to shift among numbers/lowercases, numbers/uppercases and symbols.

6 Device Wiring

6.1 Terminal Description

The terminal diagram are as follows.

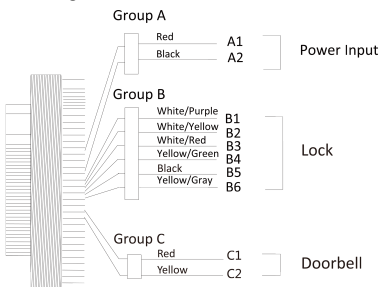


Figure 6-1 Terminal Diagram

Table 6-1 Wiring with Secure Door Control Unit Description

Cable Group	No.	Function	Color	Terminal Name	Description
Group A	A1	Power Input	Red	+12 V	12 VDC Power Supply
	A2		Black	GND	GND
Group B	B1	Lock	White/Purple	NC	Lock Wiring
	B2		White/Yellow	COM	
	B3		White/Red	NO	

Cable Group	No.	Function	Color	Terminal Name	Description
	B4		Yellow/Green	SENSOR	Door Contact Signal Input
	B5		Black	GND	GND
	B6		Yellow/Grey	BUTTON	Exit Door Wiring
Group C	C1	Doorbell	Red	BELL+	Doorbell Wiring
	C2		Yellow	BELL-	

6.2 External Device Wiring

Wire the external device.

The wiring diagram is as follows.

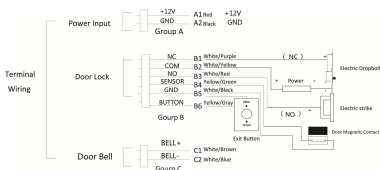


Figure 6-2 External Device Wiring

7 Installation

7.1 Install without Gang Box

Install the device on the wall directly without gang box.

Steps

1. Stick a mounting template on the wall at a required height, and drill 4 holes according to the mounting template on the wall.
2. Insert 4 supplied expansion sleeves of the setscrews in the drilled holes respectively.
3. Fix and fasten the expansion bolts in the expansion sleeves respectively.



Note

Reserve 5.2 mm to 5.5 mm of expansion bolts outside the wall for hanging the device.

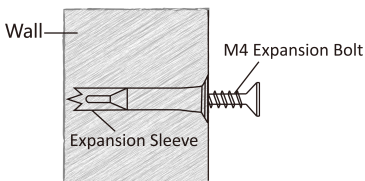


Figure 7-1 Install Expansion Screws

4. Align four holes of the device rear panel with the fixed screws and hang the device on the wall.

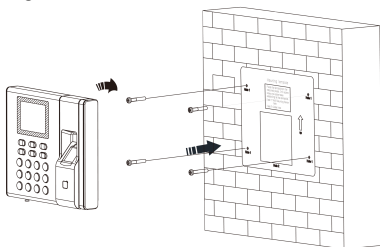


Figure 7-2 Install Device

7.2 Install without Gang Box

Install the device on the wall directly without gang box.

Steps

1. Stick a mounting template on the wall at a required height, and drill 4 holes according to the mounting template on the wall.
2. Insert 4 supplied expansion sleeves of the setscrews in the drilled holes respectively.
3. Fix and fasten the expansion bolts in the expansion sleeves respectively.



Note

Reserve 5.2 mm to 5.5 mm of expansion bolts outside the wall for hanging the device.

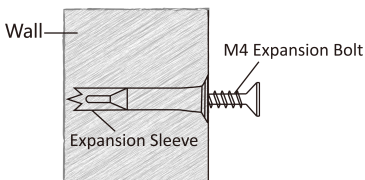


Figure 7-3 Install Expansion Screws

4. Align four holes of the device rear panel with the fixed screws and hang the device on the wall.

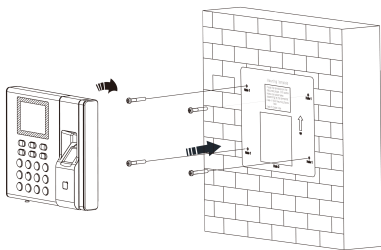


Figure 7-4 Install Device

8 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

8.1 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 reset your password regularly, especially in the high security system, resetting 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.

8.2 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

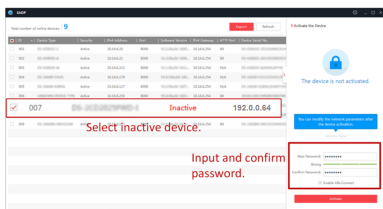
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



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.

8.3 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 reset your password regularly, especially in the high security system, resetting 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.

9 Local Settings

9.1 Select Language

You can select a language for the device system.

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

By default, the system language is English.



Note

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

9.2 Add Administrator

After the device activation and system language selection, you are required to add an administrator. You can set the administrator's user name, the card No. You can also add the user fingerprint, set the password, the department, and the authentication mode.

Steps

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

Figure 9-1 Add Administrator

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 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 32 characters are allowed in the user name.

Card

Set: Swipe card on the card swiping 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.
- If device does not support swiping card, you should enter the card No. manually. If you need to enter the card No. manually, you should enable Press Key to Input Card No.. For details, see *Configure Access Control Parameters*.

FP (Fingerprint)

On the Fingerprint page, select a target finger and record the 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*.
-

PWD (Password)

Create a password for the user and confirm the password.

 **Note**

Up to 8 characters are allowed.

Dept. (Department)

Select a department in the list and edit the department.

 **Note**

For detailed information about editing the department, see *Manage Department*.

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

9.3 Local Login

Log in the device as an administrator to manage the device parameters, including the user, the department, the shift, the holiday, the shift schedule, the report, the communication, the system, the time, etc.

Hold OK for 3 s to enter the login page. Select FP, Device PWD, or Card, and authenticate to enter the home page.

 **Note**

- Press the up or down key 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.
-

9.4 Communication Settings

Set device network, EHome, and Hik-Connect service.

9.4.1 Set 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. Network .
 2. Press OK to enter the Network page.
 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 ESC and select Yes to save the parameters and return to the previous menu.

9.4.2 Change Verification Code

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

Before You Start

Make sure your device has connect to a network.

Steps

1. Move the cursor and select Comm. Hik-Connect .
2. Input a new device verification code in the **Verification Code**.

Result

The device verification code is changed. You should input the new verification code when you add the device to the Hik-Connect mobile client.

9.4.3 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 .

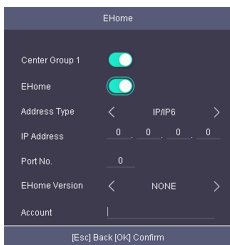


Figure 9-2 EHome Settings

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.

IP Address

Set the EHome server's IP address.

Port No.

Set the EHome server's port No.

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 and 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.

9.5 Personnel Management

9.5.1 Add Person

You can add users by setting the ID No., the user name, 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.



Figure 9-3 Add Person 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 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 32 characters are allowed in the user name.
-

Card

Set: Swipe card on the card swiping 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.
 - If device does not support swiping card, you should enter the card No. manually. If you need to enter the card No. manually, you should enable Press Key to Input Card No.. For details, see *Configure Access Control Parameters*.
-

FP (Fingerprint)

On the Fingerprint page, select a target finger and record the 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*.
-

PWD (Password)

Create a password for the user and confirm the password.

 **Note**

Up to 8 characters are allowed.

Dept. (Department)

Select a department in the list and edit the department.

 **Note**

For detailed information about editing the department, see *Manage Department*.

Auth

Select an authentication mode when verifying user's permission.

You can select Card/Fingerprint, Card, Fingerprint, Card & Password, Card and Fingerprint, Fingerprint & Password, Card & Fingerprint & Password, ID & Password, and Controller.

 **Note**

- If you select the authentication mode as **Controller**, you should set the authentication mode in *Set System Parameters*. The user will authenticate his 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 user will authenticate his 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 ESC, and select Yes to save the settings and exit the page.

9.5.2 Manage Person (Search/Edit/Delete)

Search, edit, delete the added users. You can also delete password, 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 OK 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 OK.

Select Edit User, Refer to *Add Person* to edit the user's information.

Press ESC, and select Yes to save the settings.

Delete

- Delete User: Delete the selected user.
- Delete PWD: Delete the selected user's password.
- Clear FP: Clear the all added fingerprints of the selected user.
- Clear Card: Delete all added cards of the selected user.

9.6 Attendance Status

Set attendance mode and choose attendance status. You can set the attendance status as check in, check out, break out, break in, overtime in, and over according to your actual situation.

9.6.1 Set Auto Attendance

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

Before You Start

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

Steps

1. Move the cursor and select System Att. Status to enter the Attendance Status page.
2. Move the cursor and select Attendance Mode and set the attendance mode as Auto.

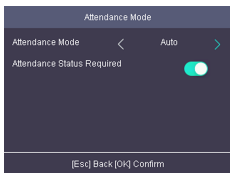


Figure 9-4 Auto Mode



Note

Make sure the attendance status is enabled. By default, it is enabled.

3. Press ESC and save the attendance mode.
4. Move the cursor and select Shortcut Key and define the shortcut key's attendance status and schedule.



Note

The attendance status will be valid within the configured schedule. For example, if set the Up key as check in and the Down key as check out, and set the check in's schedule as Monday 08:00, and check out's schedule as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

5. Press ESC and save the settings.

Result

Enter the initial page, the current attendance mode will be displayed on the page. When you authenticate on the initial page, the authentication will be marked as the configured attendance status according to the configured schedule.

9.6.2 Set Manual Attendance

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

Before You Start

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

Steps

1. Move the cursor and select System Att. Status to enter the Attendance Status page.

2. Move the cursor and select Attendance Mode and set the attendance mode as Manual.

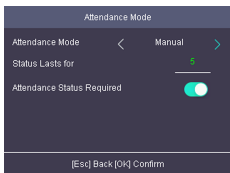


Figure 9-5 Manual Mode



Note

Make sure the attendance status is enabled. By default, it is enabled.

3. Press ESC and save the attendance mode.
4. Move the cursor and select Shortcut Key and define the shortcut key's attendance status.
5. Press ESC and save the settings.

Result

Press a key on the keypad to select an attendance status and authenticate. The authentication will be marked as the configured attendance status according to the defined shortcut key.

Or when you authenticate on the initial page, you will enter the Select Status page. Select a status to take attendance.



Note

If you do not select a status for about 20 s, the authentication will be failed and it will not be marked as a valid attendance.

9.6.3 Set Manual and Auto Attendance

Set the attendance mode as manual and auto and the system will auto change the attendance status according to the configured parameters. At the same time you can manually change the attendance status before the authentication.

Before You Start

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

Steps

1. Move the cursor and select System Att. Status to enter the Attendance Status page.
2. Move the cursor and select Attendance Mode and set the attendance mode as Manual and Auto.

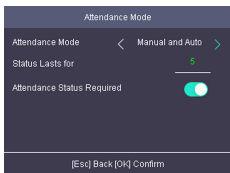


Figure 9-6 Manual and Auto Mode

 **Note**

Make sure the attendance status is enabled. By default, it is enabled.

3. Press ESC and save the attendance mode.
 4. Move the cursor and select Shortcut Key and define the shortcut key's attendance status and schedule.
-

 **Note**

The attendance status will be valid within the configured schedule. For example, if set the Up key as check in and the Down key as check out, and set the check in's schedule as Monday 08:00, and check out's schedule as Monday 17:00, the valid person's authentication before 17:00 on Monday will be marked as check in. And the valid person's authentication after 17:00 on Monday will be marked as check out.

5. Press ESC and save the settings.

Result

Enter the initial page, the current attendance mode will be displayed on the page. If you do not select a status, the authentication will be marked as the configured attendance status according to the schedule. If you press the key on the keypad, and select a status to take attendance, the authentication will be marked as the selected attendance status.

9.6.4 Disable Attendance Mode

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

Move the cursor and select System Att. Status to enter the Attendance Status page.

Move the cursor and select Attendance Mode and set the attendance mode as Disable.

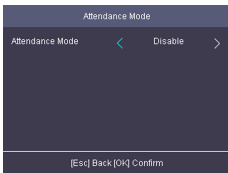


Figure 9-7 Disable Attendance Mode

The attendance status function is disabled, and you will not view or configure the attendance status on the initial page.

9.7 Time and Attendance Management

Manage department, shift, holiday, schedule, and report.

You can add, edit, delete department/shift/holiday/schedule. You can also export the attendance report.

Move the cursor and select Attendance to enter the Attendance page.

9.7.1 Manage Department (Edit/Search/Reset)

You can edit the department name, view the shift type and the shift name. You can also search the department by department name, or reset department parameters.

This is the start of your concept.

Edit Department

Move the cursor to the Dept., and press OK to enter the department list.

Select a department from the list and select Edit, and press OK to enter the Edit Dept. page. You can edit the department name, view the shift type and the shift name.

Edit Dept.	
No.	1
Name	test
Shift Type	Normal
Shift Name	2/Day
[ESC] Back [OK] Confirm	

Figure 9-8 Edit Department Page



Note

- The department name supports numbers, uppercase letters, lowercase letters, and symbols.
 - Up to 32 characters are supported in the department name.
 - You can configure the shift in the Shift Management. For detailed information, see *Shift Management*.
 - By default, the system contains 32 departments.
 - Press the up or down key on the keypad to change the input method.
-

Search Department

Search the target department by entering the department name. Move the cursor to the Dept., and press OK to enter the department list.

Enter the department name in the search box, and press OK to start search.

Reset Department

Reset all parameters of the target department to the default ones.

Move the cursor to the Dept., and press OK to enter the department list.

Select a department from the list and select Reset, and press OK. All parameters will be reset to default ones.

9.7.2 Shift Management

The normal shift and the man-hour shift are available to be configured. You can set the attendance rule and the attendance checking times in the normal shift. You can also set the working hours per day in the man-hour shift.

Normal Shift: It is applicable to the normal attendance situation.

Man-Hour Shift: It is applicable to the situation with flexible working hours.

Set Attendance Rule for Normal Shift

Move the cursor and select Shift Normal Rule , and press OK to enter the Rule page.

Setting	Value
On-Work Advanced Time	[Blue Bar]
Latest On-Work Check Time	0
Absence Time (Late)	0
Off-Work Early Time	0
Latest Off-Work Check Time	0
Absence Time (Early Leave)	[Blue Bar]

Figure 9-9 Attendance Rule Page

Set the attendance rule.

On-work Advanced Time

The allowable early duration to go to work.

Latest On-Work Check Time

The allowable late duration to go to work.

Absence Time (Late)

The late arrival threshold duration.

Off-Work Early Time

The allowable early duration to get off work.

Latest Off-Work Check Time

The allowable late duration to get off work.

Absence Time (Early Leave)

The early leave threshold duration.

Note

The available time is from 0 to 1440 min.

Set Normal Shift

Set the normal shift attendance information, including the shift name and the shift period. You can also reset the normal shift after editing.

Before You Start

Set the attendance rule. For details see *Set Attendance Rule for Normal Shift*.

Steps

1. Move the cursor and select Shift Normal to enter the Normal page.

Option
Rule
2/Day
4/Day
Custom1
Custom2

Figure 9-10 Normal Shift Page

2. Select a shift and press OK.

Note

By default, the normal shift type includes 2/Day (2 times per day), 4/Day (4 times per day), and 30 custom types.

3. Select Edit and press OK to enter the Edit Shift page.
4. Set the shift name and period in order.

Note

- The shift name supports numbers, uppercase letters, lowercase letters, Chinese characters and symbols.
 - Up to 32 characters are allowed in the shift name.
 - Up to 4 time periods can be edited.
-

5. Press ESC, and select Yes to save the settings.
6. **Optional:** Select a normal shift and select Reset and the shift will be reset to default value.

Set Man-Hour Shift

Set the man-hour shift parameters, including the shift name, the work duration, the latest on-work time, and the break time.

Steps

Up to 32 man-hour shifts can be configured.

1. Move the cursor and select Shift Man-Hour to enter the Man-Hour page.

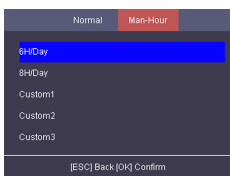


Figure 9-11 Man-Hour Shift Page

2. Select a shift from the list, and press OK .
3. Select Edit to enter the Edit Shift page.

Note

By default, the man-hour shift type includes 6H/Day (6 hours per day), 4H/Day (4 hours per day), and 30 custom types.

4. Edit shift name, shift duration (work duration), the latest on-work time, and the break time.

Note

- The break time will not be counted into the working hour.
 - If the Latest Time (On-Work) is set to 0, the Latest Time function will not be enabled.
-

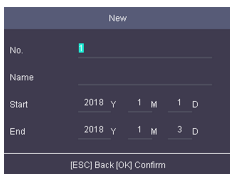
5. Press ESC and select Yes to save the settings.
6. **Optional:** Select a shift, press OK, and select Reset to reset the shift to default value.

9.7.3 Manage Holiday (Add/Search/Edit/Delete)

Set the attendance holiday. The attendance will not be recorded during the holiday.

Add Holiday

Move the cursor and select Holiday New to enter the New page. Enter No., name, start date, and end date. Press OK to save the settings.



New			
No.			
Name			
Start	2018 Y	1 M	1 D
End	2018 Y	1 M	3 D
[ESC] Back [OK] Confirm			

Figure 9-13 Add Holiday Page

Search Holiday

Move the cursor and select Holiday Holiday to enter the holiday list. Enter a holiday name and press OK to start search.

Edit Holiday

Move the cursor and select Holiday Holiday to enter the holiday list. Select a holiday and select Edit to edit the holiday.

Delete Holiday

Move the cursor and select Holiday Holiday to enter the holiday list. Select a holiday and select Delete to delete the holiday.

9.7.4 Shift Schedule

Combine shift and holiday according to your actual needs. Scheduling shift by department and scheduling shift by individual are supported.

Schedule Shift by Department: All persons in the department use the same shift schedule to check in/out.

Schedule Shift by Individual: Check in/out according to individual's conditions.

Schedule Shift by Department

All persons in the department use the same shift schedule to check in/out.

Before You Start

- Edit department. For details, see *Manage Department (Edit/Search/Reset)*.
- Set normal shift or man-hour shift. For details, see *Set Normal Shift* and *Set Man-Hour Shift*.

Steps

1. Move the cursor and select Schedule Dept. Shift to enter the Dept. Shift page.
2. Select a department from the list and press OK to enter the Edit Shift Schedule by Dept. page.

Edit Shift Schedule by Department				
Dept. Name	Company			
Set Shift	Set Shift			
Start	1970 Y	1 M	1 D	
End	2037 Y	12 M	31 D	
Add Holiday	Select Holiday			
[ESC] Back [OK] Confirm				

Figure 9-14 Edit Shift Schedule by Dept. Page

3. Edit parameters.

Dept. Name

The department name should be edited in Edit Dept. page. For details, see *Manage Department (Edit/Search/Reset)*.

Set Shift

Select a shift type and a shift times.

Start

Set the schedule's start date.

End

Set the schedule's end date.

Add Holiday

Select a holiday from the holiday list. For details about adding holiday, see *Manage Holiday (Add/Search/Edit/Delete)*.

4. Press ESC and select Yes to save the settings.

Schedule Shift by Individual

Check in/out according to individual's conditions.

Before You Start

- Add user before setting schedule shift by individual. For details, see *Add Person*.
- Set the normal shift or the man-hour shift. For details, see *Set Normal Shift* and *Set Man-Hour Shift*.

Steps



Note

The schedule shift by individual has higher priority than schedule shift by department. If a user has configured both schedule shift by department and by individual, the system will take attendance according to schedule shift by individual first.

1. Move the cursor and select Schedule Individual Shift to enter the Individual Shift page.
2. Select Add Individual Shift and press OK to enter the Add Shift Schedule page.

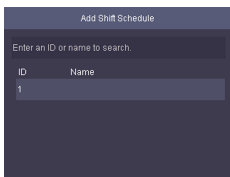


Figure 9-15 Add Shift Schedule Page

3. Select an individual in the list and press OK to enter the Edit Shift Schedule by Department page.

4. Edit the parameters.

Set Shift

Select a shift type and a shift times.

Start

Set the schedule's start date.

End

Set the schedule's end date.

Add Holiday

Select a holiday from the holiday list. For details about adding holiday, see *Manage Holiday (Add/Search/Edit/Delete)*.

5. Press ESC and select Yes to save the settings.

9.7.5 Export Attendance Report

Export the attendance record, the attendance report, the abnormal attendance record and the attendance management schedule.

Steps

1. Plug in a USB flash drive in the USB interface.

 **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 is more than 512 M.
-

2. Move the cursor and select Report. Press OK to enter the Report page.



Figure 9-16 Report Page

3. Select a report to export.

- When exporting attendance record, attendance report, and abnormal attendance record, you should enter the device No. attendance start date and end date.

Note

The device No. is for differentiating the reports of different devices.

- When selecting Attendance Management Schedule, shift settings table, normal shift schedule table and the man-hour shift schedule table will be exported.
-

Note

For details about the exported tables descriptions, see *Attendance Report Table*.

The exported table will be saved in the USB flash drive in Excel format.

9.7.6 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.

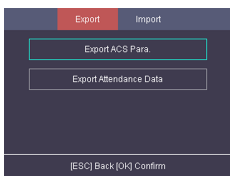


Figure 9-17 Export Data Page

Plug a USB flash drive in the device USB interface, and select **Export ACS Para.** or **Export Attendance Data**. Press OK to, 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.
-

Import Data

Move the cursor and select Transfer Import to enter the Import page. Select **Import ACS Para** and press OK. 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.
-

9.8 System Settings

9.8.1 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.

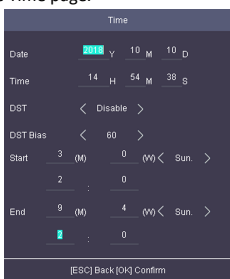


Figure 9-18 Time Page

2. Edit the parameters.

Date

The displayed date on the device.

Time

The displayed time on the device.



Note

The available range is from 1970.01.01 to 2037.12.31.

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.

9.8.2 Manage System Data

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

Steps

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

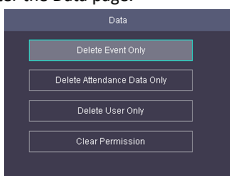


Figure 9-19 Data Page

3. Select an item and press OK to delete.

Delete Event Only

Delete all recorded events in the device.

Delete Attendance Data Only

Delete all attendance data 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.

9.8.3 Set System Parameters

Set the system parameters, including the device time format, the keypad sound, the voice prompt, the volume, the sleeping mode, the attendance record prompt the authentication mode, record delete function, and the language.

Steps

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

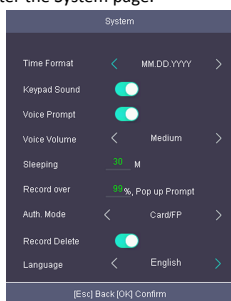


Figure 9-20 System Page

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.



Note

 refers to enabling the function and  refers to disabling the function.

Voice Prompt

Enable or disable the voice prompt according to your preference.

Note

 refers to enabling the function and  refers to disabling the function.

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.

Record over Threshold Prompt

If the attendance record memory reaches the configured value, the system will pop up a prompt to remind you. The available value is from 1 to 99.

Note

Up to 50,000 attendance records can be saved.

Auth Mode (Authentication Mode)

The authentication mode can be switched among "Card/FP (fingerprint)", "Card", "FP (fingerprint)", "Card & Password", "Card & FP (fingerprint)", "FP (fingerprint) & Password", "Card & FP (fingerprint)" & "Password", and "ID (employee ID) and password".

Record Delete

When the function is enabled, the system pops up a prompt on the initial page to remind records deleting. The system will delete the first 3000 attendance records when the memory reaches the configure threshold, in order to save the new attendance records. By default, the function is enabled. For details, see *Attendance Record Delete Rule*.

Language

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

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

9.8.4 System Upgrade

The system reads the upgrading file in the plugged USB flash drive to upgrade the device.

Steps

1. Plug the USB flash drive to the USB interface.

Note

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

2. Move the cursor and select System Upgrade .

3. Press OK.

Note

Do not power off during the device upgrading.

The system will read the digicap.dav file and upgrading automatically. After upgrading is completed, the device will reboot automatically.



After upgrading is completed, remove the USB flash drive.

9.8.5 Restore Settings

Restore system parameters to factory settings or default settings.

Steps

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

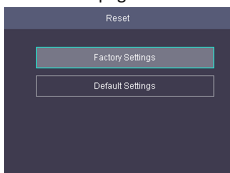


Figure 9-21 Reset Page

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. Confirm settings in the prompt page and the device starts restoring.

9.8.6 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 and fingerprint number.

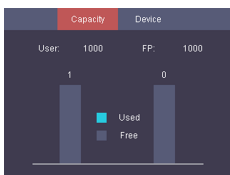


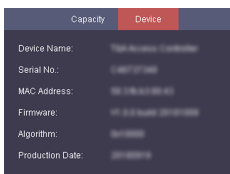
Figure 9-22 Capacity Page

Note

- The maximum user number is 1000.
 - The maximum fingerprint amount is 1000.
-

View Device Information

Move the cursor and select Info. Device to enter the Device page. You can view the device name, the serial No., the MAC address, the firmware, the algorithm version, and the production data.



Capacity	Device
Device Name:	TK-XXXXXX-XXXXXX
Serial No.:	123456789
MAC Address:	88:88:88:88:88:88
Firmware:	V1.0.0.0.0.0.0.0.0
Algorithm:	XXXXXX
Production Date:	20200101

Figure 9-23 Device Page

10 Client Software Configuration

10.1 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.

10.1.1 Add Device

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


Activate Devices

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. **Optional:** Click  on the right of **Device Management** and select Device.
The added devices are displayed in the list.
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 reset your password regularly, especially in the high security system, resetting 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.

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 Online Device

You can add single online device to the client software.

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 Online Device to show the online device area.
The searched online devices are displayed in the list.
 4. Select an online device from the Online Device area.
-



Note

For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to **Activate Devices**.

5. Click Add to open the device adding window.
6. Enter the required information.

Name

Enter a descriptive name for the device.

Address

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

Port

The port number is obtained automatically.

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 reset your password regularly, especially in the high security system, resetting 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.
-



Note


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

9. Click OK to add the device.

Add Multiple Online Devices

You can add multiple online devices to the client software.

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 Online Device to show the online device area.
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 detailed steps, refer to **Activate Devices**.

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 reset your password regularly, especially in the high security system, resetting 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 devices to the client.
- 8. 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.

9. Click OK 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 reset your password regularly, especially in the high security system, resetting 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 reset your password regularly, especially in the high security system, resetting 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. **Optional:** Click  on Operation column to view device status.


Add Device by EHome Account

You can add access control device connected via EHome protocol by specifying the EHome account.

Before You Start

Set the network center parameter first. For details, refer to **Set Network 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 EHome as the adding mode.
5. Enter the required information.

Device Account

Enter the account name registered on EHome protocol.


EHome Key

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.

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.
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.

Import Devices in a Batch

The devices can be added to the software in a batch by entering the device information in the pre-defined CSV file.

Steps

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

Adding Mode

You can enter 0 or 1 which indicated different adding modes. 0 indicates that the device is added by IP address or domain name; 1 indicates that the device is added via EHome.

Address

Edit the address of the device. If you set 0 as the adding mode, you should enter the IP address or domain name of the device; if you set 1 as the adding mode, this field is not required.

Port

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

Device Information

If you set 0 as the adding mode, this field is not required. If you set 1 as the adding mode, enter the EHome account.

User Name

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

Password

If you set 0 as the adding mode, enter the password. If you set 1 as the adding mode, enter the EHome key.




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 reset your password regularly, especially in the high security system, resetting 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

You can 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. 0 indicates disabling this function.

7. Click  and select the template file.

8. Click Add to import the devices.



10.1.2 Edit Device's Network Information

After activating device, you can edit the network information for the online device.

Before You Start

Activate the device if the device status is inactivated.

Steps

1. Enter Device Management page.
2. **Optional:** Click  on the right of **Device Management** and select Device.
3. Click Online Device to show the online device area.
All the online devices in the same subnet will display in the list.
4. Select an activated device in **Online Device** area.
5. Click  on the Operation column to open the Modify Network Parameter window.

 **Note**


This function is only available on the Online Device area. You can change the device IP address to the same subnet with your computer if you need to add the device to the software.


6. Change the device IP address to the same subnet with your computer.
 - Edit the IP address manually.
 - Check DHCP.
7. Enter the password created when you activate the device.
8. Click OK to complete the network settings.

10.1.3 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. **Optional:** Click  on the right of **Device Management** and select Device.
3. Click Online Device to show the online device area.

All the online devices in the same subnet will display in the list.
4. Select the device from the list and click  on the Operation column.
5. Reset the device password.
 - If the page with Export button, password, and confirm password field displays, 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.

- If GUID is supported, you can import the GUID files which is saved when activating the device.

 **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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

10.2 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and

attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

10.2.1 Add Organization

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

Steps


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




Note

Up to 10 levels of organizations can be added.

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

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

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



Note

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

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

10.2.2 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.

10.2.3 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.

10.2.4 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

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. Click Add Face in the Basic Information panel.

4. Select Upload.

5. Select a picture from the PC running the client.



Note

The picture should be in JPG or JPEG format and smaller than 200 KB.

6. **Optional:** Enable Verify by Device to check whether the facial recognition device managed in the client can recognize the face in the photo.

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 .

10.2.5 Take a Photo via Client

When adding person, you can take a photo of the person by the webcam of the PC running the client and set this photo as the person's profile.

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. Click Add Face in the Basic Information panel.

4. Select Take Photo.

5. Connect the face scanner to the PC running the client.

6. **Optional:** Enable Verify by Device to check whether the facial recognition device managed in the client can recognize the face in the photo.
7. Take a photo.
 - 1) Face to the webcam of the PC and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a face photo.
 - 3) **Optional:** Click  to capture again.
 - 4) Click OK to save the captured photo.
8. Confirm to add the person.
 - Click Add to add the person and close the Add Person window.
 - Click Add and New to add the person and continue to add other persons.

10.2.6 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.


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. Click Add Face in the Basic Information panel.
4. Select Remote Collection.
5. Select an access control device which supports face recognition function from the drop-down list.
6. Collect face.
 - 1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
 - 2) Click  to capture a photo.
 - 3) Click OK to save the captured photo.
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 .

10.2.7 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.

10.2.8 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 .

10.2.9 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.

Super User

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

Extended Door Open Time

When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

For details about setting the door's open duration, refer to ***Configure Parameters for Door/Elevator***.

Add to Blacklist

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

Mark as Visitor

If the person is a visitor, set the maximum times of authentications, including access by card and fingerprint to limit the visitor's access times.



Note

The maximum times of authentications should be between 1 and 100.

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.

10.2.10 Customize Person Information

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

Steps

1. Enter Person module.

2. Set the fields of custom information.

- 1) Click Custom Property.
- 2) Click Add to add a new property.
- 3) Enter the property name.
- 4) Click OK.

3. Set the custom information when adding a person.

- 1) Select an organization in the organization list to add the person and click Add.

Note

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

2) In the Custom Information panel, enter the person information.

- 3) Click Add to add the person and close the Add Person window, or click Add and New to add the person and continue to add other persons.

10.2.11 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 link 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.

10.2.12 Configure Additional Information

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

Steps

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



Note

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

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

10.2.13 Import and Export Person Identify Information

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

10.2.14 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.
-


10.2.15 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start

Be sure to have imported person information to the client beforehand.

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 and check Face.
4. **Optional:** Enable Verify by Device to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click  to select a face picture file.



Note

- The (folder of) face pictures should be in ZIP format.
 - Each picture file should be in JPG format and should be no larger than 200 KB.
 - Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.
-

6. Click Import to start importing.
The importing progress and result will be displayed.

10.2.16 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.

10.2.17 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start

Make sure you have added persons and their face pictures to an organization.

Steps

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



Note

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

3. Click Export to open the Export panel and check Face as the content to export.
4. Click Export to start exporting.



Note

- The exported file is in ZIP format.
 - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).
-

10.2.18 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.

10.2.19 Move Persons to Another Organization

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

Before You Start

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

Steps

1. Enter Person module.
2. Select an organization in the left panel.
The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click Change Organization.
5. Select the organization to move persons to.
6. Click OK.

10.2.20 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.

10.2.21 Report Card Loss

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

Steps

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

10.2.22 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.

10.3 Configure Schedule and Template

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



Note

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

10.3.1 Add Holiday

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

Perform this task when you need to add a holiday to pre-define the holidays.

Steps



Note

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

1. Click Access Control Template Holiday to enter the Holiday page.
2. Click Add on the left panel.

3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

 **Note**


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

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


 **Note**




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

- 3) **Optional:** Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

- 4) **Optional:** Select the time duration(s) that need to be deleted, and then click  in the Operation column to delete the selected time duration(s).
- 5) **Optional:** Click  in the Operation column to clear all the time duration(s) in the time bar.
- 6) **Optional:** Click  in the Operation column to delete this added holiday period from the holiday list.

6. Click Save.

10.3.2 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.

Perform this task if you want to add and configure template.

Steps

 **Note**

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

1. Click Access Control Template Template to enter the Template page.
-

 **Note**

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

All-Day Authorized

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

All-Day Denied


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

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


Note

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

- 3) **Optional:** Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .
 - 4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.
-


Note

Up to 4 holidays can be added to one template.

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

Note

For details about adding a holiday, refer to **Add Holiday**.

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

10.4 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.

Perform this task if you need to assign access group to persons.

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, face picture, 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 start applying all the selected access group(s) to the access control device or door station.




Caution

- Be careful to click Apply All, 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 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 Statusto 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.

10.5 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene, such as multi-factor authentication, anti-passback, etc.

Note

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

10.5.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device (access controller), access control points (door or floor), alarm inputs, alarm outputs, card readers and lane controller.


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.
-

RS-485 Comm. Redundancy

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

Display Detected Face

Display face picture when authenticating.

Display Card Number

Display the card information when authenticating.

Display Person Information

Display the person information when authenticating.

Overlay Person Info. on Picture

Display the person information on the captured picture.

Voice Prompt

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

Upload Pic. After Linked Capture

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

Save Pic. After Linked Capture

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

Press Key to Enter Card Number

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

Wi-Fi Probe

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

3G/4G


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

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/Elevator

After adding the access control device, you can configure its access point (door or floor) 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 or floors of the selected device.
3. Select a door or floor 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.

Extended Open Duration

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

Door Open Timeout Alarm

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

Lock Door when Door Closed

The door can be locked once it is closed even if the **Door Locked Time** is not reached.

Duress Code

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

Super Password

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

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/floor(s) to copy the parameters in the page to the selected doors/floor(s).


Note

The door or floor's status duration settings will be copied to the selected door/floor(s) as well.

Configure Parameters for Card Reader

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

Steps

1. Click Access Control Advanced Function Device Parameter .
2. In the device list on the left, click  to expand the door, select a card reader and you can edit the card reader's parameters on the right.

3. Edit the card reader basic parameters in the Basic Information page.



Note

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

Name

Edit the card reader name as desired.

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.

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.

Max. Interval When Entering PWD

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

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.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

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

Buzzing Time

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

Card Reader Type/Card Reader Description

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

Fingerprint Recognition Level

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

Default Card Reader Authentication Mode

View the default card reader authentication mode.

Fingerprint Capacity

View the maximum number of available fingerprints.

Existing Fingerprint Number

View the number of existed fingerprints in the device.

Score

The device will score the captured picture according to the yaw angle, pitch angle, and pupillary distance. If the score is less than the configured value, face recognition will be failed.

Face Recognition Timeout Value

If the recognition time is more than the configured time, the device will remind you.

Face Recognition Interval

The time interval between two continuous face recognitions when authenticating. By default, it is 2s.

Face 1:1 Matching Threshold

Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

1:N Security Level

Set the matching security level when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate when authentication.

Live Face Detection

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.

Live Face Detection Security Level

After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.

Max. Failed Attempts for Face Auth.

Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Lock Authentication Failed Face

After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection is failed for more than the configured attempts. The same user cannot authenticate via the fake face within 5 minutes. Within the 5 minutes, the user can authenticate via the real face twice continuously to unlock.

Application Mode

You can select indoor or others application modes according to actual environment.

4. Click OK.

5. **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 Input


After adding the access control device, you can configure the parameters for its alarm inputs.

Steps



Note

If the alarm input is armed, you cannot edit its parameters. Disarm it first.

1. Click Access Control Advanced Function Device Parameter .
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 input parameters.

Name

Edit the alarm input name as desired.

Detector Type

The detector type of the alarm input.

Zone Type

Set the zone type for the alarm input.

Sensitivity

Only when the duration of signal detected by the detector reaches the setting time, the alarm input is triggered. For example, you have set the sensitivity as 10ms, only when the duration of signal detected by the detector reach 10ms, this alarm input is triggered.

Trigger Alarm Output


Select the alarm output(s) to be triggered.

4. Click OK.
5. **Optional:** Click the switch on the upper-right corner to arm or disarm the alarm input.

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.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Steps

1. Click Access Control Advanced Function Device Parameter to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

Passing Mode

Select the controller which will control the barrier status of the device.

If you select **According to Lane Controller's DIP Settings**, the device will follow the lane controller's DIP settings to control the barrier. The settings on the software will be invalid.

If you select **According to Main Controller's Settings**, the device will follow the settings of the software to control the barrier. The DIP settings of the lane controller will be invalid.

Free Passing Authentication

If you enable this function, when both entrance and exit's barrier mode is Remain Open, the pedestrians should authenticate each time passing through the lane. Or an alarm will be triggered.

Opening/Closing Door Speed

Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.



The recommended value is 6.

Audible Prompt Duration

Set how long the audio will last, which is played when an alarm is triggered .



0 refers to the alarm audio will be played until the alarm is ended.

Temperature Unit

Select the temperature unit that displayed in the device status.

4. Click OK.

10.5.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed and set the elevator controller as free and controlled. 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 or elevator controller that need to be configured on the left panel.

3. To set the door or elevator controller status during the work day, click the Week Schedule and perform the following operations.
 - 1) For door, click Remain Open or Remain Closed.
 - 2) For elevator controller, click Free or Controlled.
 - 3) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.


**Note**

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

- 4) **Optional:** Perform the following operations to edit the time durations.

Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to .

Click the time duration and directly edit the start/end time in the appeared dialog.

Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to .

- 5) Click Save.

Related Operations


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

4. To set the door status during the holiday, click the Holiday and perform the following operations.
 - 1) Click Remain 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 copy the door status settings of this door to other door(s).

10.5.3 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.

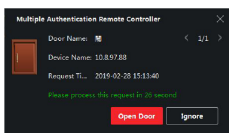


Figure 10-1 Remotely Open Door

 **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.

10.5.4 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.

Perform this task to configure the custom Wiegand rule for the third party card readers.

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 .
-

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



Note

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

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



Note

- Up to 80 bits are allowed in the total length.
 - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
 - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
-

6. Set output transformation rule.

- 1) Click Set Rule to open the Set Output Transformation Rules window.

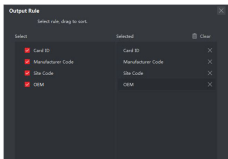


Figure 10-2 Set Output Transformation Rule

- 2) Select rules on the left list.
The selected rules will be added to the right list.
 - 3) **Optional:** Drag the rules to change the rule order.
 - 4) Click OK.
 - 5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.
7. Click Save.

10.5.5 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.

Perform this task if you need to configure the card reader's authentication mode and schedule.

Steps

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

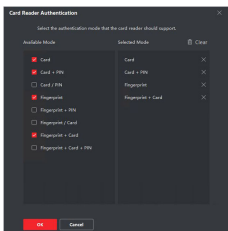


Figure 10-3 Select Card Reader Authentication Mode

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

10.5.6 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.

10.5.7 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 ***Configure Multi-door Interlocking***.

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.

10.5.8 Configure Multi-door Interlocking

You can set the multi-door interlocking between multiple doors of the same access control device. To open one of the doors, other doors must keep closed. That means in the interlocking combined door group, up to one door can be opened at the same time.

Perform this task when you want to realize interlocking between multiple doors.

Steps

Note

- Multi-door Interlocking function is only supported by the access control device which has more than one access control points (doors).
 - 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 anti-passing back function, refer to **Configure Anti-Passback**.
-

1. Click Access Control Advanced Function Multi-door Interlocking .
 2. Select an access control device on the left panel.
 3. Click Add on the Multi-door Interlocking List panel to open Add Access Control Point to open the Add window.
 4. Select at least two access control points(doors) from the list.
-

Note

Up to four doors can be added in one multi-door interlocking combination.

5. Click OK to add the selected access control point(s) for interlocking.
The configured multi-door interlocking combination will list on the Multi-door Interlocking List panel.
6. **Optional:** Select an added multi-door interlocking combination from the list and click Delete to delete the combination.
7. Click Apply to apply the settings to the access control device.

10.5.9 Configure Other Parameters

After adding the access control device, you can set its parameters such as network parameters, capture parameters, RS-485 parameters, Wiegand parameters, etc.

Set Multiple NIC Parameters

If the device supports multiple network interfaces, you can set the network parameters of these NICs via the client, such as IP address, MAC address, port number, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management module.
2. Select an access control device in the device list and click Modify.
3. Click Multiple NICs Settings to enter the Multiple NICs settings page.
4. Select an NIC you want to configure from the drop-down list.
5. Set its network parameters such as IP address, default gateway, subnet mask, etc.

MAC Address

A media access control address (MAC address) is a unique identifier assigned to the network interface for communications on the physical network segment.

MTU

The maximum transmission unit (MTU) of the network interface.

6. Click Save.

Set Network Parameters

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

Set Log Uploading Mode

You can set the mode for uploading logs via EHome protocol. Perform this task when you need to set the access control device's log uploading mode.

Steps

1. Click Access Control Device Management to enter the Device Management page.
2. Select the device in the device list and click Modify.
3. Click Network Settings Uploading Mode to enter the Uploading Mode page.
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.

7. Click Save.

Create EHome Account in Wire Communication Mode

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

Perform this task when you need to create EHome account in wire communication mode for access control device.

Steps



Note

This function should be supported by the device

1. Click Access Control Device Management to enter the Device Management page.
2. Select the device in the device list and click Modify.
3. Click Network Settings Network Center to enter the Network Center page.
4. Select the center group from the drop-down list.
5. Select the **Address Type** as IP Address or Domain Name.

6. Input IP address or domain name according to the address type.
7. Input 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.
9. Set an account name for the network center.
10. Click Save.

Create EHome Account in Wireless Communication Mode

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

Perform this task when you need to create EHome account in wireless communication mode for access control device.

Steps

 **Note**

This function should be supported by the device

1. Click Access Control Device Management to enter the Device Management page.
 2. Select the device in the device list and click Modify.
 3. Click Network Settings Wireless Communication Center to enter the Wireless Communication Center page.
 4. Select the center group from the drop-down list.
 5. Input the IP address and port number.
-

 **Note**

- By default, the port number for EHome is 7660.
 - The port number of the wireless network and wired network should be consistent with the port number of EHome.
-

6. Select the **Protocol Type** as EHome.
7. Set an account name for the network center.
8. Click Save.

Set Device Capture Parameters

You can configure the device capture parameters, including manual capture and linked capture.

 **Note**

- The Capture Settings should be supported by the device.
 - Before setting the capture setting, you should configure the Storage Server for picture storage. For details, refer to .
-

Set Triggered Capture Parameters

You can set the triggered capture parameters for the device with capture function.

Before You Start

Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to .

Perform this task when you need to set triggered capture parameters.

Steps

Note

This function should be supported by the device

1. Click Access Control Device Management to enter the Device Management page.
2. Select the device in the device list and click Modify.
3. Click Capture Settings Linked Capture to enter the Linked Capture page.
4. Set the picture size and quality.
5. Set the capture times once triggered.
6. Set the capture interval according to the capture times.
7. Click Save.

Set Manual Capture Parameters

You can set the manual capture parameters for the device with capture function.

Before You Start

Before setting the capture setting, you should configure the storage server for picture storage. For details, refer to .

Perform this task when you need to set manual capture parameters.

Steps

Note

This function should be supported by the device

1. Click Access Control Device Management to enter the Device Management page.
2. Select the device in the device list and click Modify.
3. Click Capture Settings Manual Capture to enter the Manual Capture page.
4. Select the resolution of the captured pictures from the drop-down list.
5. Select the picture quality as High, Medium, or Low.
6. Click Save.
7. **Optional:** Click Restore Default Value to restore the parameters to default settings.

Set Face Recognition Terminal Parameters

For face recognition terminal, you can set its parameters including face picture database, QR code authentication, etc.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management module.
2. Select an access control device in the device list and click Modify.

3. Click Face Recognition Terminal Settings to enter the Face Recognition Terminal Settings page.
4. Set the parameters.



Note

These parameters displayed vary according to different device models.

COM

Select a COM port for configuration. COM1 refers to the RS-485 interface and COM2 refers to the RS-232 interface.

Face Picture Database

select Deep Learning as the face picture database.

Authenticate by QR Code

If enabled, the device camera can scan the QR code to authenticate. By default, the function is disabled.

Blacklist Authentication

If enabled, the device will compare the person who want to access with the persons in the blacklist.

If matched (the person is in the blacklist), the access will be denied and the device will upload an alarm to the client.

If mismatched (the person is not in the blacklist), the access will be granted.

Save Authenticating Face Picture

If enabled, the captured face picture when authenticating will be saved on the device.

MCU Version

View the device MCU version.

5. Click Save.

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.

Perform this task when you need to set the access control device's RS-485 parameters.

Steps



Note

The RS-485 Settings should be supported by the device.

1. Click Access Control Device Management to enter the Device Management page.
2. Select the device in the device list and click Modify.
3. Click RS-485 Settings to enter the RS-485 settings page.
4. Select the serial port number from the dropdown 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 dropdown list.
6. Click Save.

- The configured parameters will be applied to the device automatically.
- After changing the working mode, the device will reboot automatically.

Set Wiegand Parameters

You can set the access control device's Wiegand channel and the communication mode.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management module.
 2. Select an access control device in the device list and click Modify.
 3. Click Wiegand Settings to enter the Wiegand Settings page.
 4. Check Enable 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.

Authenticate M1 Card Encryption

M1 card encryption can improve the authentication security level. After issuing the card, you can enable the M1 card encryption function in the client software.

Before You Start

Use the specified card enrollment station to issue card. See **Issue a Card to One Person** for details.

Perform this task when you need to enable M1 card encryption function.

Note

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

Steps

1. Click Access Control Device Management to enter the access control device management page.
2. Select the device in the device list, and click Modify to pop up Modify window.
3. Click M1 Card Encryption tab to enter the M1 Card Encryption page.
4. Check Enable checkbox to enable the M1 card encryption function.

5. Set the sector ID.

The sector ID ranges from 1 to 100.

6. Click Save to save the settings.

10.6 Configure Linkage Actions for Access Control

The events triggered by the access control devices, doors, card readers, and alarm inputs, as well as the card swiping of persons, mobile terminal's MAC address detected, and employee No. detected, can trigger a series of linkage actions to notify the security personnel and record the events.

Two types of linkage actions are supported: client actions and device actions.

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client playing alarm sound and sending an email to notify the security personnel.
- **Device Actions:** When the event is detected, it will trigger the actions of this device, such as buzzing, door open/closed, audio play, etc., to notify the security personnel and allow/forbid access.

10.6.1 Configure Client Actions for Access Event

You can assign client linkage actions to the event by setting up a rule. For example, when the event is detected, an audible warning appears to notify the security personnel.

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 .

Email Linkage

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

2) Click OK.

5. Enable the event so that when the event is detected, an 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/elevator, or card reader.

10.6.2 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.

Recording

The recording will be triggered.

Note

The device should support recording.

Buzzer on Reader

The audible warning of card reader will be triggered.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

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.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click Save.

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

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

Delete Linkage Settings Select the configured linkage settings in the device list and click Delete to delete it.

10.6.3 Configure Device Actions for Card Swiping

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

Steps

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

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.

 **Note**

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



Note

The device should support alarm input function.

Access Point

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

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click Save.

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

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

Delete Linkage Settings Select the configured linkage settings in the device list and click Delete to delete it.

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

10.6.4 Configure Device Linkage for Mobile Terminal's MAC Address

You can set the access control device's linkage actions for the specified MAC address of mobile terminal. When access control device detects the specified MAC address, 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 Mac Linkage.
 5. Enter the MAC address to be triggered.
-



Note

MAC Address Format: AA:BB:CC:DD:EE:FF.

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.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.



The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



The device should support alarm input function.

Access Point

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

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

7. Click Save to save the settings.

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

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

Delete Linkage Settings Select the configured linkage settings in the device list and click Delete to delete it.

10.6.5 Configure Device Actions for Person ID

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

Steps



It should be supported by the device.

1. Click Access Control Linkage Configuration .
2. Select the access control device from the list on the left.
3. Click Add button to add a new linkage.
4. Select the event source as Person Linkage.

5. Enter the employee number or select the person from the dropdown list.
6. Select the card reader where the card swipes to trigger the linked actions.
7. In the Linkage Target area, set the property target to enable this action.

Buzzer on Controller

The audible warning of access control device will be triggered.

Buzzer on Reader

The audible warning of card reader will be triggered.

Capture

The real-time capture will be triggered.

Recording

The recording will be triggered.



Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.



Note

The device should support zone function.

Access Point

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

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click Save.

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

Delete Linkage Settings

Select the configured linkage settings in the device list and click Delete to delete it.

Edit Linkage Settings

Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

10.7 Door/Elevator Control

In Monitoring module, you can view the real-time status of the doors or elevators managed by the added access control device. You can also control the doors and elevators 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/elevator control permission, the user can enter the Monitoring module and control the door/elevator. Or the icons used for control will not show. For setting the user permission, refer to .

10.7.1 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 .

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 .

Result

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

10.7.2 Control Elevator Status

You can control the elevator status of the added elevator controller, including opening elevator's door, controlled, free, calling elevator, etc.

Steps



Note

- You can control the elevator via the current client if it is not armed by other client. The elevator cannot be controlled by other client software if the elevator status changes.
 - Only one client software can control the elevator at one time.
 - The client which has controlled the elevator can receive the alarm information and view the elevator real-time status.
-

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 .

The elevators in the selected access point group will display.

3. Click a door icon to select an elevator.
4. Click the following buttons to control the elevator.

Open Door

When the elevator's door is closed, open it. After the open duration, the door will be closed again automatically.

Controlled

You should swipe the card before pressing the target floor button. And the elevator can go to the target floor.

Free

The selected floor's button in the elevator will be valid all the time.

Disabled

The selected floor's button in the elevator will be invalid and you cannot go to the target floor.

Result

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

10.7.3 Check Real-Time Access Records

The access records will display in real time, including card swiping records, face recognitions 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.

10.8 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.

10.8.1 Configure Attendance Parameters

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

Configure General Rule

You can configure the general rule for attendance calculation, such as the week beginning, month beginning, weekend, absence, etc.

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. Set the day as week beginning and the date as month beginning.
4. Select the day(s) as weekend.
5. Set absence parameters.
6. Click Save.

Configure Overtime Parameters

You can configure the overtime parameters for workday and non-workday, including overtime level, pay rate, attendance status for overtime, etc.

Steps

1. Enter Time & Attendance module.
2. Click Attendance Settings Overtime .
3. Set required information.

Overtime Level for Workday

When you work for 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 pay rate for three overtime levels, respectively.

Pay Rate

Set corresponding pay rates for three overtime levels, which can be generally used to calculate total work hours.

Overtime Rule for Non-Workday

You can enable overtime rule for non-workday and set calculation mode.

4. 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. Set the required parameters of the third-party database, including database type, server IP address, database name, user name and password.
5. Set table parameters of database according to the actual configurations.
 - 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.
6. Click Connection Test to test whether database can be connected.
7. Click Save to save the settings.

The attendance data will be written 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 Settings in the break time area to enter break time management page.
4. 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.

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

Date Format / Time Format

Set the date format and time format according to the actual needs.

Attendance Status Mark in Report

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 in Report

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

4. Click Save.

10.8.2 Add Timetable

You can add the timetable for the shift schedule.

Steps

1. Click Time & Attendance Timetable to enter timetable settings window.
2. Click Add to enter Add Timetable page.
3. Create a name for the timetable.
4. Select calculation method.

First Check-In & Last Check-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 Auth. 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.

5. **Optional:** Set **Get Device Status** switch to on to get attendance status from the device.
6. Set the related attendance time.

Work Time from

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

Late/Early Leave

Set the time period for late or early leave.

Valid Check-in/out Time

Set the time period during which the check-in or check-out is valid.

7. **Optional:** Select break time to exclude the duration from work hours.

Note

You can click Settings to manage break time. For more details about configuring break time, refer to **Configure Break Time**.

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

10.8.3 Add Shift

You can add the shift for the shift schedule.

Before You Start

Add a timetable first. See **Add 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.

The screenshot shows a web form for adding a shift. At the top, the 'Shift Name' is 'New Shift 1'. Below that, 'Shift Period' is set to '1' and 'Week(s)' is a dropdown. There are two radio buttons: 'Default Time...' (selected) and 'Normal Workd...'. Below the radio buttons are 'Delete' and 'Clear' buttons. A grid shows the shift period for 'Normal Workday: 09:00 - 18:00' from Monday to Friday, with blue bars indicating the shift time. The grid columns are labeled 'Time' with intervals from 00:00 to 24:00. At the bottom are 'Save' and 'Assign' buttons.

Figure 10-4 Add Shift

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 effective period for the shift schedule.

- 4) Set other parameters for the shift schedule, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.

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

10.8.4 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. Check the checkbox to enable **Multiple Shift Schedules**.



Note

After checking Multiple Shift Schedules, you can select the effective time period(s) from the added time periods for the persons in the department.

Multiple Shift Schedules

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

If the multiple shift schedules contains three time periods: 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 time periods. If the person checks in at 07:50, it will apply the nearest time period 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, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
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 Management 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. Check the checkbox to enable **Multiple Shift Schedules**.
-

Note

After checking the Multiple Shift Schedules, you can select the effective timetable(s) from the added timetables for the persons.

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, including Check-in Not Required, Check-out Not Required, Effective for Holiday, and Effective for Overtime.
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 can 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).

10.8.5 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.

10.8.6 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 field 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.

10.8.7 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 calculate the attendance data automatically at the time you configured every day.

Steps

 **Note**

It will calculate the attendance data till the previous day.

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 every day.
4. Click Save.

Manually Calculate Attendance Data

You can calculate the attendance data manually by setting the data range.

Steps

1. Enter the Time & Attendance module.

2. Click Attendance Statistics Calculate Attendance .
3. Set the start time and end time to define the attendance data range.
4. Set other conditions, including department, person name, employee No. and attendance status.
5. Click Calculate.

 **Note**

It can only calculate the attendance data within three months.

6. Perform one of the following operations.

Correct Check-in/out	Click Correct Check-in/out to add check-in/out correction.
Report	Click Report to generate the attendance report.
Export	Click Export to export attendance data to local PC.

 **Note**

The exported details are saved in CSV format.

10.8.8 Attendance Statistics

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

Get Original Attendance Record

You can search the employee's attendance time, attendance status, check point, etc. in a time period to get an original record of the employees.

Before You Start

- You should add organizations and persons in Person module and the persons has swiped card. 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 Original Records .
3. Set the attendance start time and end time that you want to search from.
4. Set other search conditions, such as department, person name, and employee No.

5. **Optional:** Click Get from Device to get the attendance data from the device.
6. **Optional:** Click Reset to reset all search conditions and edit the search conditions again.
7. Click Search.
The result displays on the page. You can view the employee's required attendance status and check point.
8. **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.

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 .

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. |

11 Mobile Client Configuration

After adding the access control device to the mobile client, you can control door status, set door open duration, change super password, and view access control logs.

11.1 Control Door Status

The Mobile Client allows you to control the status of the access control devices' related doors by the super password of the device.

Before You Start

- Add an access control device to the Mobile Client. See *Add Device for Management* in the user manual of Hik-Connect mobile client for details.
- Link doors to the access control device. See the user manual of the access control device for details.

Steps

Note

You can change the super password. See *Change Super Password* for details.

1. On the device list page, tap the door icon on the right of the access control device to enter the door control page.



Figure 11-1 The Icon Representing Door

2. Control the door status.

Remain Open

Keep the door open.

Open Door

Open the door for a configurable time period. When the time period expires, the door will close.

Note

For details about configuring the time period, see *Set Door Open Duration*.

Remain Closed

Keep the door closed. In this status, the door can only be opened by super card or super password.

Note

For details about super card, see the user manual of the access control device.

3. Enter the super password.
-

Note

By default, the super password is the device verification code. You can change the super password. See *Change Super Password* for details.

The door status will change.

11.2 Set Door Open Duration


You can set the door open duration for the access control device. When the duration expires, the door will close automatically.

Before You Start

You should have added an access control device to the Mobile Client.

See *Add Device for Management* in the user manual of the Hik-Connect mobile client for details.


Steps

1. Enter the Settings page of the access control device.
 - On the device list page, if the page is in the list mode, swipe the device name to the left and tap .
 - On the device list page, if the page is in thumbnail mode, tap the device name or tap **...**.
 - On the Live View page, tap **...** and then tap Settings.



Note

For details about how to enter the Live View page, see *Start and Stop Live View* on the user manual of Hik-Connect mobile client.

2. Tap Door Open Duration to open the Door Open Duration list.
3. Select a duration from the list.
4. Tap  to confirm the selection.

If you tap Open Door in the door control page, the door will open for the configured time duration.



Note

For details about controlling door status, see *Control Door Status*.

11.3 Change Super Password

The Mobile Client allows you to change the super password of the access control device, which can be used to open all the access control points (e.g., doors), even when the access control point is in remaining closed status.

Before You Start


Add an access control device to the Mobile Client. See *Add Device for Management* in the user manual of Hik-Connect mobile client for details.

Steps



Note

For details about super password of the access control device, see the user manual of the device.

1. Enter the Settings page of the access control device.
 - On the device list page, if the device list is in list mode, swipe the name of the access control device to the left and tap .
 - On the device list page, if the device list is in thumbnail mode, tap the name of the access control device or tap **...**.
 - On the Live View page, tap **...** and then tap Settings.



Note

For details about how to enter the Live View page, see *Start and Stop Live View* in the user manual of Hik-Connect mobile client.

2. Tap Change Password to enter the Change Password page.
3. Enter the old password and tap Next.

 **Note**

If it is the first time to set the super password, skip this step.

4. Create a new password and then tap Finish.
-

 **Note**

The password should contain 6 numbers.

11.4 View Access Control Logs

You can view the access control device's logs including the access control events and alarm information. You can also filter the logs.

Steps

1. On the device list page, tap the door icon on the right of the access control device to enter the door control page.



Figure 11-2 The Icon Representing Door

The log list will be displayed on the Log section of the page.

2. Perform the following operations.

- | | |
|-------------------------|---------------------------------------------------------------------------------------------------|
| Refresh Log List | Swipe the log list downward to refresh it. |
| View All Logs | Tap View All Logs to enter the Log page and view all access control device logs. |
| Filter Logs | On the Log page, tap Filter and then set the filtering condition (time and event type) to filter. |

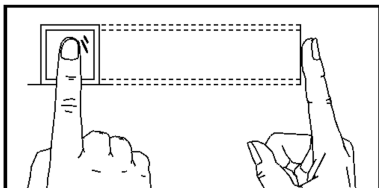
A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

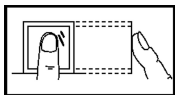
The figure displayed below is the correct way to scan your finger:



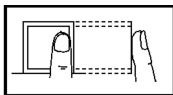
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

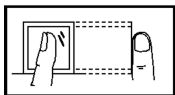
The figures of scanning fingerprint displayed below are incorrect:



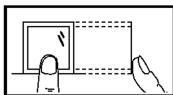
Vertical



Edge I



Side



Edge II

Environment

The scanner should avoid direct high 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 after drying the finger

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.

B. Access Control Capacity

View the access control data's capacity, including the card permission, door status, card reader authentication mode, and attendance data.

Table B-1 Card Permission

Content	Maximum Configurable Parameters
Week Schedule	32 Up to 8 time durations are supported for one week schedule
Holiday Schedule	128 Up to 8 time durations are supported for one holiday schedule. One holiday schedule can belong to multiple holiday groups.
Holiday Group	64 Up to 16 holiday schedules are supported for one holiday group.
Schedule Template	64 Up to 1 week schedule and 4 holiday groups are supported for one schedule template.

Table B-2 Door Status

Content	Maximum Configurable Parameters
Week Schedule	1
Holiday Schedule	32
Holiday Group	4
Schedule Template	1

Table B-3 Card Reader Authentication Mode

Content	Maximum Configurable Parameters
Week Schedule	2
Holiday Schedule	64
Holiday Group	8
Schedule Template	2

Table B-4 Attendance

Content	Maximum Configurable Parameters
Department	32
Normal Shift	32
Man-Hour Shift	32
Holiday	32
Holiday Group	64
Schedule by Department	32
Schedule by Individual	32

C. Attendance Record Deleting Rule

Enable Record Delete

Set the percentage of the attendance record over threshold prompt.

1. When the record reaches the threshold, an alarm of the attendance record over limit value will be displayed on device screen. The alarm information is: Log will be full, export the report. Card authentication is available. The interface will be back to the alarm interface after authenticating
2. When the record is full, an alarm of the attendance record over limit value will be displayed on the device screen. The alarm information is: Log is full, export the report. Card authentication is available. And the first 3000 attendance records will be deleted automatically. The interface will be back to the alarm interface after authentication.
3. Deleting by time and deleting all are available when deleting the attendance records.

Disable Record Delete

Set the percentage of the attendance record over threshold prompt.

1. When the record reaches the threshold, an alarm of the attendance record over limit value will be displayed on device screen. The alarm information is: Log will be full, export the report. Card authentication is available. The interface will be back to the alarm interface after authenticating.
2. When the record is full, an alarm of the attendance record over limit value will be displayed on the device screen. The alarm information is: Log is full, export the report. Card authentication is available. And there will be no new attendance records added. The interface will be back to the alarm interface after authenticating.
3. Deleting by time and deleting all are available when deleting the attendance records.

D. Attendance Report Table

Enter a short description of your concept here (optional).

This is the start of your concept.

Description of Attendance Report File Name

File Name Rule: Device No. + Report Type.xls

Device No.: A serial of numbers from 0 to 8.

Report Type:

- AbnormalAttendance1: The Attendance Abnormal table
- AbnormalAttendance2: When the row of the Abnormal Attendance table is more than 60000, the record will be export in two tables. Here AbnormalAttendance2 refers to the second abnormal attendance table.
- AttendanceSummary: The Attendance Summary table
- AttendanceRecord: The Attendance Record table
- AttendanceSchedule: The attendance schedule table
- NormalShift: The Normal Shift table
- ManHourShift: The Man-Hour Shift table

Attendance Schedule Table

Attendance Schedule											
Create Time: 2017-04-26 10:12:20											
Employee ID	Card No.	Name	Department	2017/01/01 (Sun.)		2017/01/02 (Mon.)		2017/01/03 (Tue.)		2017/01/04 (Wed.)	
				Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type	Shift No.	Shift Type

Attendance Schedule Table: All users shift schedule information for a period will be displayed in this table. You are able to set the shift information and the holiday (No attendance recorded during the holiday) in shift schedule configuration.

- Employee ID: The user's ID No.
- Card No.: The user's card No.
- Name: The user's name.
- Department: The department of the user.

Normal Shift Table

Normal Shift
Create Time: 2017-04-26 10:12:20

Shift No.	Shift Name	Period 1		Period 2		Period 3		Period 4	
		Start	Stop	Start	Stop	Start	Stop	Start	Stop

Normal Shift Table: Up to 4 periods can be configured in normal shift configuration. You are able to take attendance according to the configured period.

For example: If set Period 1 to 9:00 (Start) and 17:00 (End), it is effective for the user to take attendance between 9:00 and 17:00.

Combining with the attendance rule, you are able to set multiple attendance types.

Man-Hour Shift Table

Man-Hour Shift Table					
Create Time: 2017-04-26 10:12:20					
Shift No.	Shift Name	Work Duration (min)	Latest Start-Work Time	Period 1	
				Start	End

Man-Hour Shift Table: Set the Man-Hour Shift working duration. If set the Latest Start-Work Time to 0, all users are attendant. If set the Latest Start-Work Time to more than 0, the user will be absent by taking attendance after the configured time.

For example: If set the working duration to 6 hours, the start-work time to 09:00, the end-work time to 17:00 and the break period is from 12:00 to 13:00, the user actual working hour is 17:00 - 09:00 - (13:00 - 12:00).

Abnormal Attendance Table

Abnormal Attendance Table							
Create Time: 2017-04-26 10:12:20							
Employee ID	Card No.	Name	Department	SW-EW	Late Duration (min)	Early Leave Duration (min)	Total (min)

Abnormal Attendance Record Table: Calculate the abnormal attendance according to the attendance records and the shift schedule configuration.

- Employee ID: The user's ID No.
- Card No.: The user's card No.
- Name: The user's name.
- Department: The department of the user.
- Date: The date of the data generated.

- SW-EW: Up to 4 periods can be configured. It records the attendance time of each user every day.
- Late Duration (min): The start-work attendance time is later than the normal start-work time.
- Early Leave Duration (min): The end-work attendance time is earlier than the normal end-work time.
- Total: The absence time duration of the day.

Attendance Record Table

Attendance Record Table									
Create Time: 2017-04-26 10:12:20									
Employee ID	Card No.	Name	Department	2017/01/01	2017/01/02	2017/01/03	2017/01/04	2017/01/05	2017/01/06
				SW-EW	SW-EW	SW-EW	SW-EW	SW-EW	SW-EW

Attendance Record Table: Input the start work time and the end work time to export the effective attendance data during the configured duration.

- Employee ID: The user's ID No.
- Card No.: The user's card No.
- Name: The user's name.
- Department: The department of the user.

Attendance Summary Table

Attendance Summary Table									
Create Time: 2017-04-26 10:12:20									
Employee ID	Card No.	Name	Department	Late Times	Late Duration (min)	Early Leave Duration (min)	Absence Times	Absence Time Duration (min)	Attendance/Total Work Days

Attendance Summary Table: Enter the start time and the end time to calculate the user attendance information via the shift information and the holiday information according to the shift schedule configuration.

- Employee ID: The user's ID No.
- Card No.: The user's card No.
- The user's name.
- Department: The user's department.
- Late Times: The start-work attendance time is later than the normal start-work time. Late arriving for no more than once every day.
- Late Duration (min): Total time duration for late.

- Early Leave Times: The end-work attendance time is earlier than the normal end-work time. Early leave for no more than once every day.
- Early Leave Duration (min): Total time duration for early leave.
- Absence Times: Total absence times. 10. Absence Time Duration (min): Total absence duration. 11. Attendance/Total Work Days: Total attendance days.