HIKVISION®

Face Recognition Terminal

User Manual

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA
Hikvision Canada, 4848 rue Levy, Saint Laurent, Quebec, Canada, H4R 2P1
Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690
E-Mail: sales.usa@hikvision.com • www.hikvision.com

About this Manual

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company Website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Manual Illustrations and Features

Graphics (screen shots, product pictures, etc.) in this document are for illustrative purposes only. Your actual product may differ in appearance. Your product might not support all features discussed in this document.

Trademarks Acknowledgement

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

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS," WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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 TO THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED FOR ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

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

EU Conformity Statement

CE 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 LVD Directive 2014/35/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 (A)/NMB-3(A) standards requirements.

Hikvision North America Privacy Policy

Last Updated: December 2018
Hikvision USA Inc. and Hikvision Canada Inc. and its affiliates (collectively "HIKVISION") provide the following services for use in conjunction with various HIKVISION Internet-connected products ("Products"): a HIKVISION user Website and user accounts that may be accessed at

us.hikvision.com,

ca.hikvision.com,

https://distributors-us.hikvision.com/,

https://distributors-us.hikvision.com/guestLogin.htm,

https://ezviz-rma.hikvision.com/,

https://order-na.hikvision.com,

and all associated sites connected with us.hikvision.com (the "Website"); and any services available on the Website, Web Apps, and Mobile Apps ("Available Services"). The term "HIKVISION Services" means the Website and Available Services.

This Privacy Policy explains how HIKVISION handles the collection, storage, and disclosure of information, including personal information, regarding our HIKVISION Services. It also applies to any information we collect from the operation and use of Products we sell while connected to the HIKVISION Services (the "Products), and any other HIKVISION Service that links to this Privacy Policy.

We may modify this Privacy Policy at any time, provided certain provisions of this Privacy Policy prove to be incomplete or outdated and further provided that these changes are reasonable for you, taking into account your interests. If we make material changes to this Privacy Policy, we will notify you by the e-mail address specified in your account or by means of notice on our Websites.

You can determine when this Privacy Policy was last revised by referring to the date it was "Last Updated" above.

What Information We Collect
In order to provide HIKVISION services to you, we will ask you to provide personal information that is necessary to provide those services to you. If you do not provide your personal information, we may not be able to provide you with our products or services.

"Personal information" shall have the same meaning as "personal data" and shall include any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. Examples of personal information include your name, telephone number, e-mail address, and physical address.

Personal information also includes information that alone cannot directly identify you, but with other information we have access to can identify you such as product serial numbers, log data that automatically records information about your visit such as your browser type, domains, page views, the URL of the page that referred you, the URL of the page you next visit, your IP address, and page navigation, unique device ID collected from Products and your mobile devices, data from cookies, pixel tags, and Web beacons, video content files that do not contain personal visual identity information, the country and time zone of the connected Product, geo-location, mobile phone carrier identification,

and device software platform and firmware information.

How We Collect and Use Your Information
Here are some examples of the personal information we may collect and how we may use it:

- When you create your account to use HIKVISION Services ("Account"), we will collect information including your name, phone number, and e-mail and physical address. In addition, when you install and activate Products, we will collect certain basic information via our HIKVISION Services such as your product name, the product's verification code, and serial number, which are unique to the Product connected to the HIKVISION Services and associated with your Account.

- When you respond to our e-mails, contact our customer service, or use other customer support tools, we collect your information to provide you with support, verify your identity with your Account profile information, and confirm your Product.

We may also use the information we collect for the following Purpose

- send you reminders, technical notices, updates, alerts, support and administrative messages, service bulletins, and requested information; and

- pursuant to our legitimate business interests:

  - operate, maintain, improve, and develop our HIKVISION Services and Products;

  - personalize your experience with our HIKVISION Services and Products;

  - increase the safety of our HIKVISION Services and Products – for example, for user authentication, security protection, fraud detection, filing, and backups;

  - perform analytics and conduct customer research;

  - communicate and provide to existing customers additional information that may be of interest to you about our products and services;

  - manage our everyday business needs such as auditing, administration of our HIKVISION Services, forum management, fulfillment, analytics, fraud prevention, and enforcement of our corporate reporting obligations and Terms of Service;

  - enhance other information we have about you to help us better understand you and determine your interests; and

  - in the context of a corporate transaction (e.g., corporate restructuring, sale or assignment of assets, merger) and to protect our rights or property, to enforce our Terms of Service and legal notices and for the establishment, exercise, and defense of legal claims;

with your express consent to

  - send you electronic communications in order to inform you about new products and services, unless you choose to unsubscribe;

  - use certain non-essential cookies to better understand user behavior, in order to optimize user experience, perfect function design, and offers for products and services from us or to provide better services;

- meet a legal obligation, a court order or other binding decision(s); and accomplish a purpose unrelated

to those described in this Privacy Policy by first notifying you and, where required, offering you a choice as to whether or not we may use your Personal Information in this different manner.

Cookies and Other Technologies
We also use cookies, Web beacons, pixel tags, and other technologies to keep records, store your preferences, improve our advertising, and collect information such as log data and device data. This allows us to better understand how you use our HIKVISION Services and Products, diagnose and troubleshoot any problems you have, and otherwise administer and improve our HIKVISION Services and Products. For more information about cookies, please refer to our **Use of Cookies** (https://order-na.hikvision.com/helpCenter/useOfCookies).

How We Share Your Information
HIKVISION may disclose personal information to cloud service provider, network service provider, and other service providers on the basis of non-disclosure agreements.

The following are the limited situations where we may share personal information:

- We share your personal information with HIKVISION affiliates, who are required to use that information in accordance with the purposes described in this Privacy Policy.

- We use service providers, vendors, technicians, and other third-parties to help us process, store, and protect some of your data and otherwise help us administer our Products and HIKVISION Services effectively, provide a better user experience, process your purchases, and increase the quality of our Products and HIKVISION Services. These third-parties are forbidden from using your personal information for non-HIKVISION purposes and are required to protect your information in accordance with this Privacy Policy and applicable laws.

- We may provide information to third-parties if we believe in good faith that we are required by mandatory law to do so. For example, to comply with legal orders and government requests; response to a subpoena, or similar legal process, including to law enforcement agencies, regulators, and courts; to protect the interests of our customers and users of the HIKVISION Service; to respond to claims that any content posted or displayed using the HIKVISION Service violates the rights of third parties; in an emergency protect the health and safety of users of the HIKVISION Service or the general public; or to enforce compliance with our Terms of Service.

- If HIKVISION and/or all or part of our assets are ever sold or transferred, your personal information may be among the items sold or transferred. Under such circumstance, we will notify you by the e-mail address specified in your account or by means of notice on us.hikvision.com and associated Websites of (i) the identity and contact information of the purchaser or transferee, (ii) your right to revoke your consent to the provision of personal information, and (iii) the means by which you may revoke such consent.

- We share information to protect our own legitimate business interests when we believe in good faith that we are required or permitted by law to do so. For example, we may share your personal information as needed to support auditing, compliance, and corporate governance functions; to combat fraud or criminal activity; to protect our rights or those of our affiliates and users; or as part of legal proceedings affecting HIKVISION.

We may also disclose non-personal information (for example, aggregated or anonymized data) publicly or with third-parties, provided those data have been rendered anonymous in such a way that the data subject is no longer identifiable. For example, we may share non-personal information:

- for the same reasons we might share Personal information;

- to better understand how our customers interact with our HIKVISION Services and Products, in order to optimize your experience, improve our products, or provide better services;

- for our own research and data analytics; or

- to our vendors for their own analysis and research.

Securing Your Personal Information
HIKVISION has implemented commercially reasonable administrative, technical, and physical security controls that are designed to safeguard personal information. We also conduct periodic reviews and assessments of the effectiveness of our security controls.

Notwithstanding the above, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, HIKVISION cannot guarantee that your personal information is under absolute security with the existing security technology. If you have any questions about the security of our HIKVISION Services, you can contact us at the contact information below in **Contact Us**.

Accessing, Correcting, and Retention of Your Personal Information
HIKVISION generally stores your personal information on HIKVISION's servers, which is established upon Amazon Servers, until you delete or edit it, or for as long as you remain a HIKVISION customer in order to provide you with the most relevant offers.

Keeping your personal information current helps ensure that we provide you with the most relevant offers. You can access, update, or delete your personal information via your Account profile. We are ready to assist you in managing your subscriptions, deactivating your account, and removing your active profile and data. Your personal information might not be immediately deleted, as we are required to retain records relating to previous purchases through our HIKVISION Services for financial reporting and compliance reasons pursuant to applicable laws. In addition, because of the way we maintain certain services, after you delete certain information, we may temporarily retain backup copies of such information before it is permanently deleted.

We will retain your personal information for the period necessary to fulfill the purpose outlined in this Privacy Policy unless a longer retention period is required or permitted by applicable law.

If you are located in the European Union, subject to limitations in applicable law, you have certain rights in respect to your personal information such as a right of access, rectification, restriction, opposition, and portability. In order to exercise your rights please contact us at the contact information below in **Contact Us**. You also have the right to withdraw your consent at all times, free of charge. You can do this by opting out from direct marketing and by rejecting the use of cookies through your browser settings. If you have concerns about how we handle your personal information, you have the right to lodge a complaint with the data protection authority in your country of residence.

Social Community Features and Social Networks

Social Community Features
Our HIKVISION Services may allow you to publicly post or share information, communicate with others, or otherwise make information accessible to others. Prior to doing so, please read our Terms of Service carefully. All the information you post, share, or communicate may be accessible to anyone with Internet access, and any personal information you include may be read, collected, and used by others.

Social Networks
You have the option to link social networks such as Facebook to your Account. You will be able to post HIKVISION activity to your social network. By proceeding through any of the above steps, you grant HIKVISION permission to access elements of your social network profile information that you have made

available to be shared and to use it in accordance with the social network's terms of use and this Privacy Policy.

Links to Other Websites
We may permit others to link to the HIKVISION services or to post a link to their Website. We do not endorse these Websites and are not responsible for other Websites or their privacy practices. Please read their privacy policies before submitting information.

Your Choices

We think that you benefit from a more personalized experience when we know more about you and your preferences. However, you can limit the information you provide to HIKVISION as well as the communications you receive from HIKVISION through your Account preferences.

Commercial E-mails
You will receive commercial e-mails from us only if you have granted prior express consent or if sending those e-mails is otherwise permitted, in accordance with applicable laws.

You may choose not to receive commercial e-mails from us by following the instructions contained in any of the commercial e-mails we send or by logging into your Account and adjusting your e-mail preferences. Please note that even if you unsubscribe from commercial e-mail messages, we may still e-mail you non-commercial e-mails related to your Account on the HIKVISION Services.

Device Data
You may manage how your mobile device and mobile browser share certain device data with HIKVISION by adjusting the privacy and security settings on your mobile device. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

Children's Privacy
HIKVISION does not intend that any portion of its HIKVISION Services will be accessed or used by children under the age of 18, or equivalent minimum age in the relevant jurisdiction and such use is prohibited. Our HIKVISION Services are designed and intended for adults. By using the HIKVISION Services, you represent that you are at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction and understand that you must be at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction in order to create an account and purchase the goods or services advertised through our HIKVISION Services. If we obtain actual knowledge that an account is associated with a registered user who is under the age of 18 years old, or equivalent minimum age in the relevant jurisdiction, we will promptly delete information associated with that account. If you are a parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction and believe he or she has disclosed personal information to us please contact us at the contact information below in **Contact Us**. A parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction may review and request deletion of such child's personal information as well as prohibit the use thereof.

Global Operations
We transfer and process your information globally both in our own facilities and with service providers, or partners, regardless of where you use our Services. The laws, regulations, and standards of the country in which your information is stored or processed may be different from those of your own country.

California Privacy Rights: Pursuant to Section 1798.83 of the California Civil Code, residents of California can obtain certain information about the types of personal information that companies with whom they have an established business relationship have shared with third parties for direct marketing

purposes during the proceeding calendar year. In particular, the law provides that companies must inform consumers about the categories of personal information that have been shared with third parties, the names and addresses of those third parties, and examples of the types of services or products marketed by those third parties. To request a copy of the information disclosure provided by HIKVISION pursuant to Section 1798.83 of the California Civil Code, please contact us at the contact information below in **Contact Us**. Please allow 30 days for a response.

Contact Us
Please contact us if you have any questions or comments about our privacy practices or this Privacy Policy. You can always reach us through the below contact information:

- A&E Program: aepartners.usa@hikvision.com
- Cybersecurity: security.usa@hikvision.com
- Dealer Partner Program: partners.usa@hikvision.com
- Marketing: marketing.usa@hikvision.com
- OEM/ODM: oem.usa@hikvision.com
- Sales: inside.usa@hikvision.com
- Technical Support: techsupport.usa@hikvision.com
- Canadian Technical Support: techsupport.ca@hikvision.com
- Need Help with This Product/Product Detail feature: inside.usa@hikvision.com
- A&E partner inquiries (user registration, new project support, etc.): aepartners.usa@hikvision.com
- HDP partner inquiries (user registration, new partner registration, etc.): partners.usa@hikvision.com
- US Hikcentral Trial Version Request: sales.usa@hikvision.com
- Canada Hikcentral Trial Version Request: sales.canada@hikvision.com
- Hikvision Robotics Division: robotics.USA@hikvision.com
- Hikvision OEM/ODM Division: OEMODM.usa@hikvision.com
- A&E partner registrations: sarkis.timourian@hikvision.com
- RMA: rma.usa@hikvision.com
- Customer Service: csr.usa@hikvision.com
- Careers: hr.usa@hikvision.com
- Hikvision B2B Portal: b2b.usa@hikvision.com

Please provide: (i) your name (or nickname), your country or region of residence and your preferred method of contact; and (ii) the details of your request or comment along with any corresponding Website links.

Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding**
  Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.

- **Electrical Wiring**
  Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.

- **Surge Suppressor (Required)**
  Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:

  - Specifications
    - > Listed by Underwriter's Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
    - > Minimum protection of 1,000 joules or higher
    - > Clamping voltage of 400 V or less
    - > Response time of 1 nanosecond or less
  - Usage
    - > Surge suppressors must not be daisy chained with power strips or other surge suppressors
  - Maintenance
    - > Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
    - > Replace yearly in storm-prone areas
    - > Replace every two years as routine maintenance

Symbol Conventions

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

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100-240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected into the power socket.
- If smoke, odor, or noise rise from the device, turn off the power at once, unplug the power cable, and then contact the service center.

Preventive and Cautionary Tips
Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with a UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- 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.

Table of Contents

Chapter 1 Overview

1.1 Introduction

The DS-K1T606 series face recognition terminal is an access control device that is equipped with face recognition functionality. It is mainly deployed as part of secure access control systems, such as logistic centers, airports, university campuses, alarm centrals, dwellings and so on.

1.2 Main Features

- 5-inch LCD touch screen that displays the operation interface
- 2,000,000 pixel wide-angle lens
- Face recognition distance: 1 ft to 3.3 ft (0.3 m to 1 m)
- Live face detection: only a live face can be detected and authenticated
- Deep learning algorithm
- Maximum storage space of 3000 face pictures and 5000 fingerprints

Note: Only products with the fingerprint module support the fingerprint scanning function.

- Multiple authentication modes: face picture, fingerprint, card, or password, fingerprint and password, fingerprint and card, face picture and fingerprint, etc.

Note: Only products with the fingerprint module support fingerprint scanning function.

- Face recognition duration ≤ 1s/user; face recognition accuracy rate >99%
- Device parameter management, search, and settings
- Imports card and user data to the device via TCP/IP communication or a USB flash drive
- Transmits data (authentication results and face pictures) to the client software via the TCP/IP communication protocl
- Imports data (face pictures) to the device and exports data (added face pictures, captured face pictures, and events) from the device via USB flash drive
- Stand-alone operation
- Connects to one external card reader via the RS-485 protocol
- Connects to the secure door control unit via the RS-485 protocol to avoid door opening when the terminal is damaged
- Connects to the external access controller or Wiegand card reader via Wiegand protocol
- Voice prompt and prompt sound output
- Watchdog design for protecting the device and ensuring that the device is running properly
- EHome protocol and public network communication

Chapter 2 Appearance

Refer to the following contents for detailed information on the face recognition terminal:

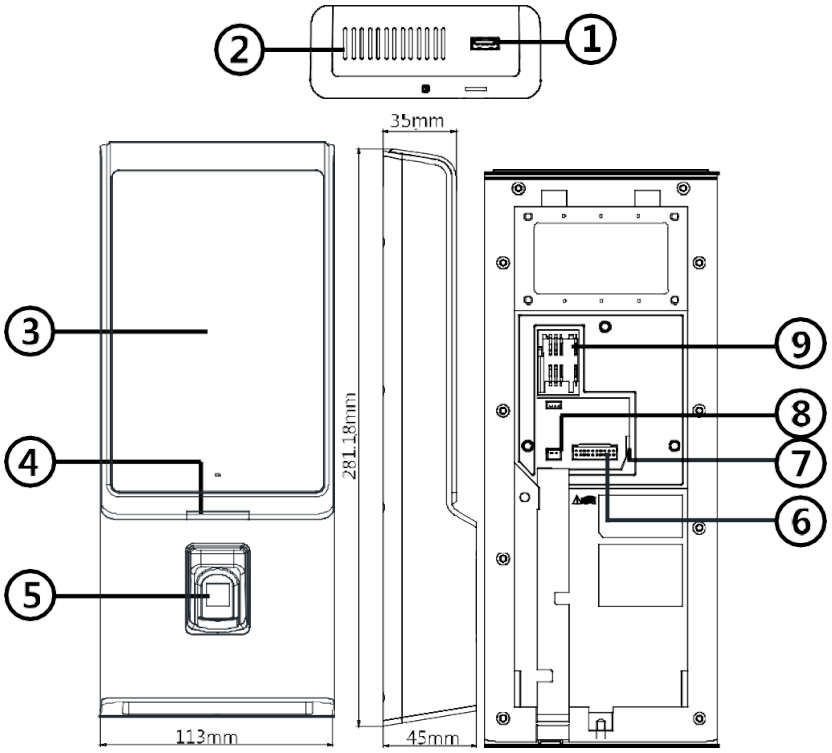


Figure 2-1: Face Recognition Terminal Diagram

Table 2-1 Description of Face Recognition Terminal

No.	Name	Description
1	USB Interface	Plug in the USB flash drive to import or export data
2	Loudspeaker	Sound emitter
3	Display Screen	5-inch LCD touch screen with a resolution of 800 × 480 pixels
4	Indicator	Solid Red: Standby
		Flashing Red: Authentication failed
		Solid Green: Authentication completed
		Flashing Green: Authenticating (combined)
5	Fingerprint Module + Card Swiping Area	Area where fingerprint can be inputted or card can be swiped ***Note:*** *Only devices with the fingerprint scanning function contain this element.*
	Card Swiping Area	Area where card can be swiped ***Note:*** *Only devices without the fingerprint scanning function contain this element.*
3	Sensor	Detects illumination intensity. When the environment is too dark, the device will automatically enable the supplementary light.
4	Display Screen	5" LCD touch screen with a resolution of 800 x 480
5	Wiring Terminals	Connect to other external devices, including the RS-485 card reader, Wiegand card reader, door lock, alarm input, alarm output, etc.
6	Network Interface	Ethernet connection
7	Power Interface	Power supply connection
8	Micro SIM Card Slot	Insert SIM card

Chapter 3 Terminal Descriptions

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

Refer to the following terminal diagram and connection description table for more information:

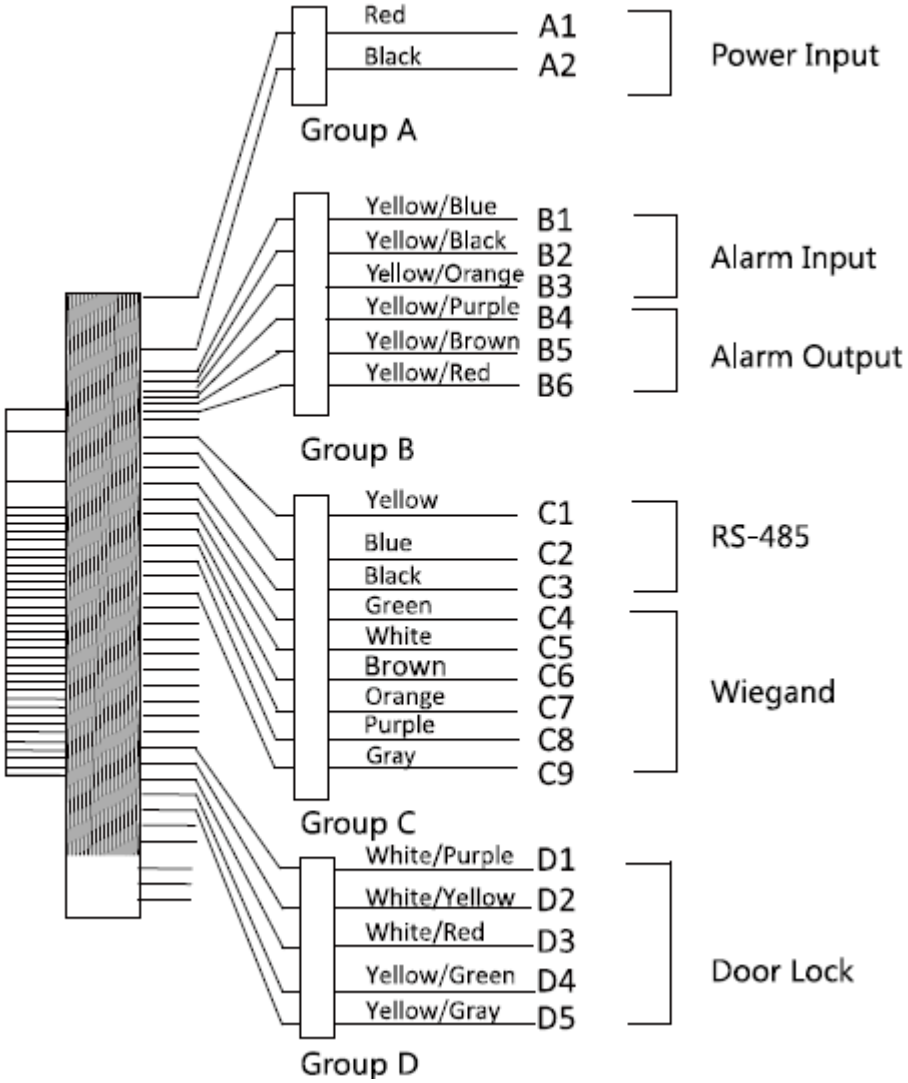


Figure 3-1: Terminal Inputs and Outputs

Table 3-1: Terminal Connection Descriptions

Group	No.	Function	Color	Name	Description
Group A	A1	Power Input	Red	+12V	12V DC Power Supply
	A2		Black	GND	Ground
Group B	B1	Alarm Input	Yellow/Blue	IN1	Alarm Input 1
	B2		Yellow/Black	GND	Ground
	B3		Yellow/Orange	IN2	Alarm Input 2
	B4	Alarm Output	Yellow/Purple	NC	Alarm Output Wiring
	B5		Yellow/Brown	COM	
	B6		Yellow/Red	NO	
Group C	C1	RS-485	Yellow	485+	RS-485 Wiring
	C2		Blue	485-	
	C3		Black	GND	Ground
	C4	Wiegand	Green	W0	Wiegand Wiring 0
	C5		White	W1	Wiegand Wiring 1
	C6		Brown	WG_OK	Wiegand Authenticated
	C7		Orange	WG_ERR	Wiegand Authentication Failed
	C8		Purple	BUZZER	Buzzer Wiring
	C9		Gray	TAMPER	Tampering Alarm Wiring
Group D	D1	Door Lock	White/Purple	NC	Lock Wiring (NC)
	D2		White/Yellow	COM	Ground
	D3		White/Red	NO	Lock Wiring (NO)
	D4		Yellow/Green	SENSOR	Door Magnetic Sensor Signal Input
	D5		Yellow/Gray	BUTTON	Exit Door Wiring

Chapter 4 Terminal Connection

You can connect the RS-485 terminal to the RS-485 card reader, the NC and COM terminals to the door lock, the SENSOR/BUTTON terminal to the exit button, the alarm output and input terminal to the alarm output/input devices, and the Wiegand terminal to the Wiegand card reader or the access controller.

If the WIEGAND terminal is connected to the access controller, the face recognition terminal can transmit authentication information to the access controller, and the access controller can determine whether to open the door or not.

The wiring diagram is as follows:

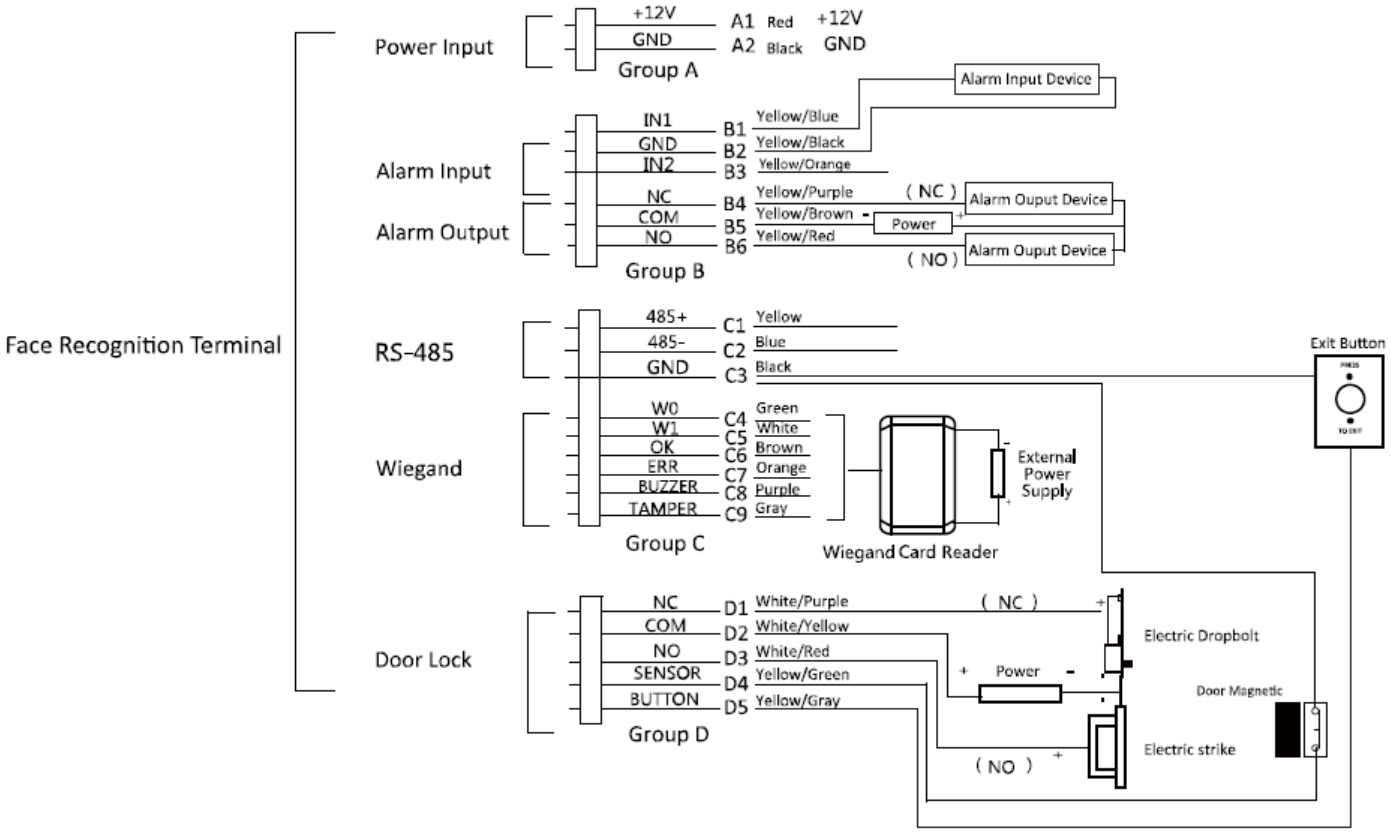


Figure 4-1: Face Recognition Wiring Diagram

Note: The Wiegand terminal displayed above is a Wiegand input terminal. You should set the face recognition terminal's Wiegand direction to "Input" to connect to a Wiegand card reader. To connect an access controller, set the Wiegand direction to "Output" to transmit authentication information to the access controller. For details about Wiegand direction settings, see *Setting Wiegand Parameters* in Section *6.3.1 Communication Settings*.

You can also connect the terminal to the secure door control unit. The wiring diagram is as follows:

Note: The secure door control unit should connect to an external power supply separately.

Chapter 5 Installation

Installation Environment:
If the device is installed indoors, the device should be at least 6.6 ft (2 m) away from the light, and at least 9.8 ft (3 m) away from the window or the door.

Ensure that the environment illumination is greater than 100 lux.

Note: For details about the installation environment, see *Appendix C Tips for Installation Environment*.

Installation Types:
Wall mounting with gang box and wall mounting without gang box.

5.1 Installation with Gang Box

Before you start:
Connect the supplied cable to the device terminals on the device rear panel.

1. According to the datum line on the mounting template, stick the mounting template on the wall or other surface, 4.6 ft (1.4 m) above the ground.

2. Drill holes in the wall or other surface according to the mounting template, and install the gang box (the dimensions of the gang box are 3.15" x 3.15", or 80 mm x 80 mm).

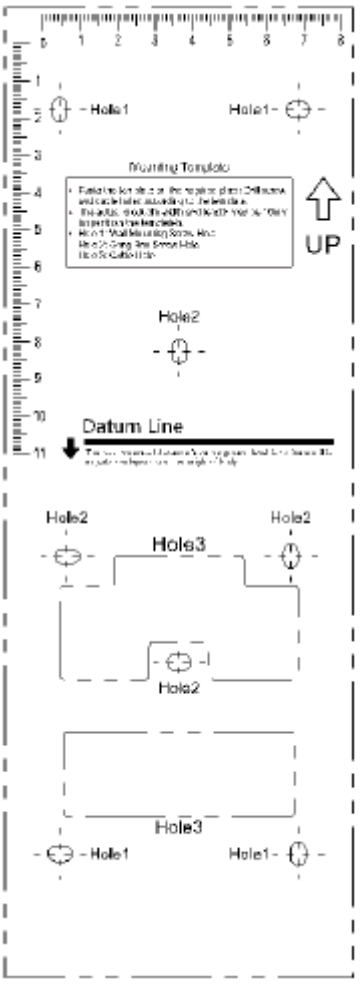


Figure 5-1: Wall Mounting Template

3. Use two supplied screws to secure the mounting plate to the gang box.
4. Use another four supplied screws to secure the mounting plate to the wall.
5. Route the cables through the cable hole of the mounting plate, and connect to the corresponding external device cables.
6. Remove the screw at the bottom of the device.
7. Align the device with the mounting plate and buckle them together.
8. Use a hex wrench to fasten the screw to the bottom.

Notes:

- The installation height shown here is the recommended height. You can change it according to your actual needs.
- You can also install the device to the wall or other places without the gang box. For details, see *Installing without Gang Box*.
- For easy installation, drill holes on mounting surface according to the supplied mounting template.

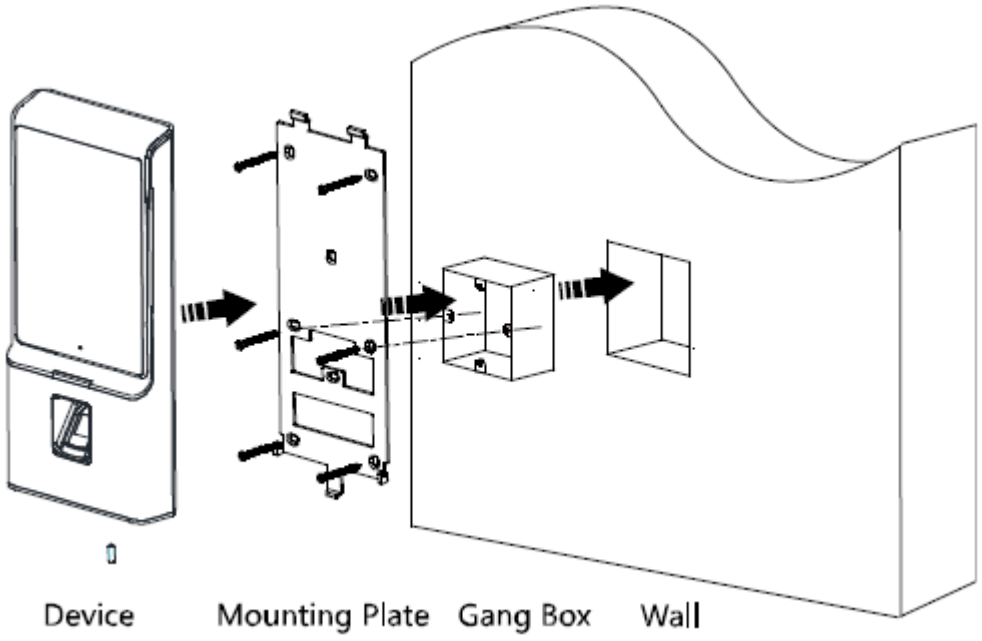


Figure 5-2: Device and Gang Box Installation

5.2 Installing without Gang Box

Before you start:
Connect the supplied cable to the device terminals on the device rear panel.

1. According to the baseline on the mounting template, fix the mounting template to the wall or other surface. This should be at a height of 4.6 ft (1.4 m).

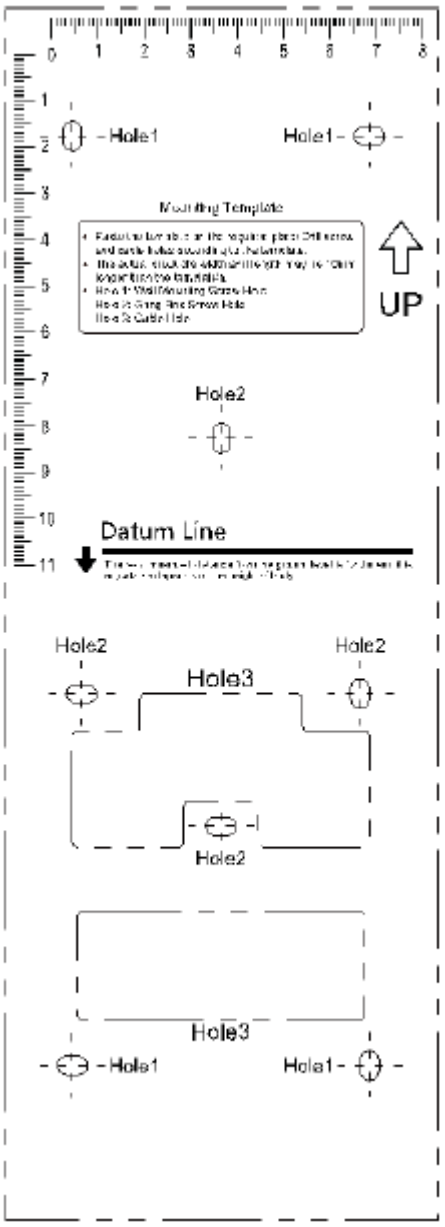


Figure 5-3: Mounting Template

2. Drill 4 holes on the wall or other surface by following the locations of Hole 1 in the mounting template.

3. Insert the screw sockets of the set screws into the drilled holes.

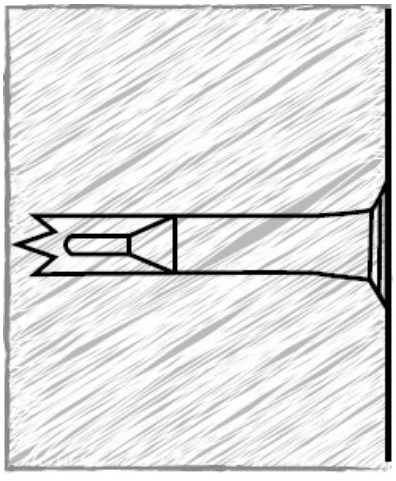


Figure 5-4: Set Screw Diagram

4. Align the drilled holes with the 4 holes of the mounting plate.
5. Route the cables through the cable hole of the mounting plate, and connect it to the corresponding external device cables.
6. Fix and fasten the screws into the sockets on the wall or other surface.
7. Remove the screw at the bottom of the device.
8. Align the device with the mounting plate and buckle them together.
9. Use a hex wrench to tighten the screw at the bottom.

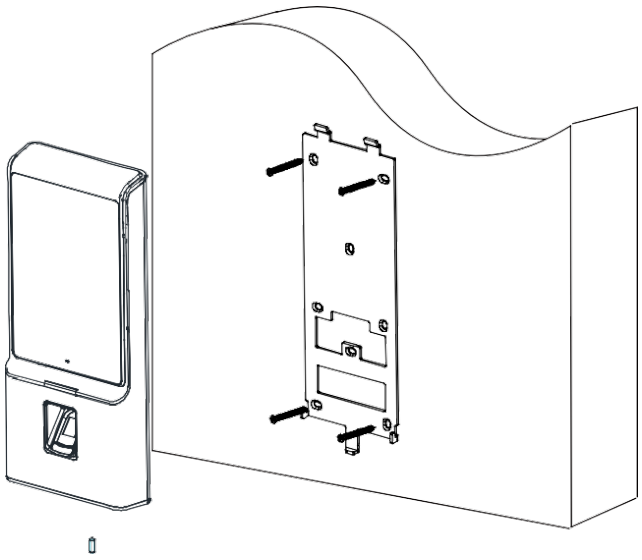


Figure 5-5: Mounting Plate and Device Installation

Chapter 6 Basic Operation

6.1 Activate Device

Purpose:
Activate the terminal before first use.

Activation via device, activation via SADP, and activation via client software are supported. The default values of the control terminal are the following:

- Default IP address: 192.0.0.64.
- Default port number: 8000.
- Default user name: admin.

6.1.1 Activating via Device

Figure 6-1: Device Activation and Password Input

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

1. Create a password in the Password field.

2. Confirm the password by typing it again in the Confirm field.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

3. Tap **Activate** and the device will be activated.

6.1.2 Activating via SADP Software

Purpose:
SADP software is used for detecting an online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install SADP according to the prompts. Follow the steps to activate the device**.**

1. Run the SADP software to search for online devices.

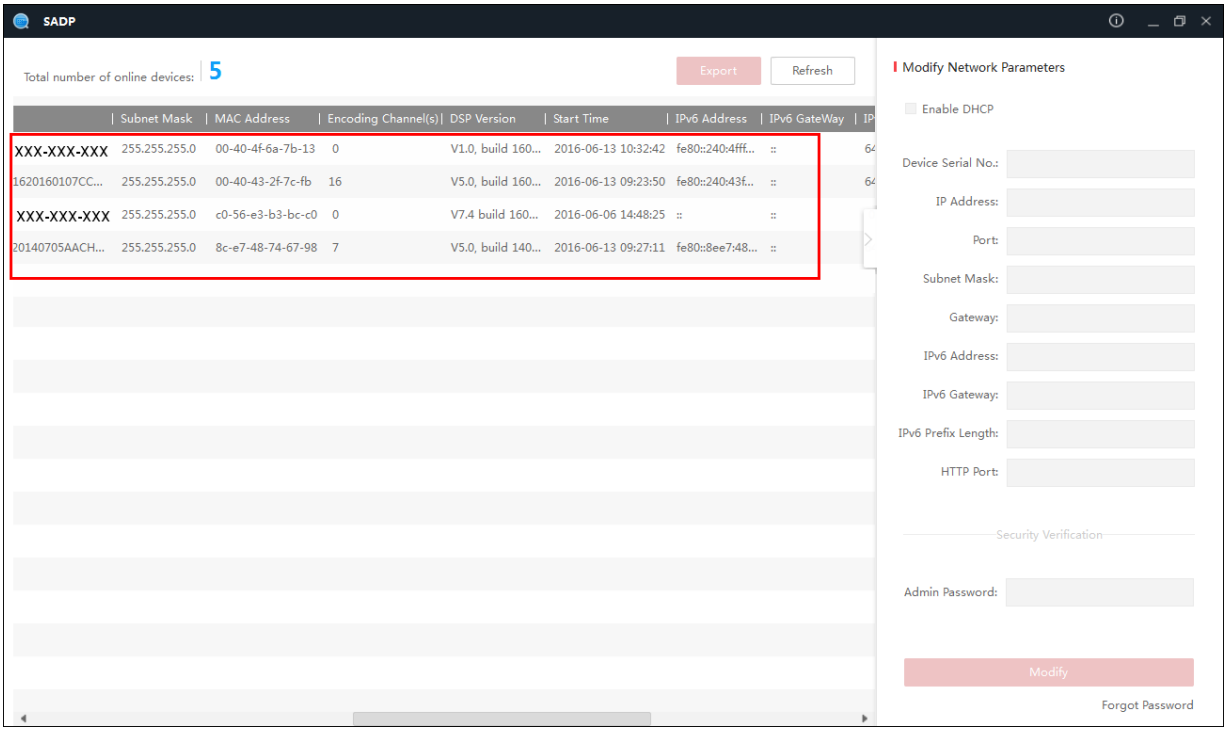


Figure 6-2: SADP Interface

2. Check the device status from the device list, and select an inactive device.

3. Create a password in the password field, and confirm the password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

4. Click **Activate** to activate the device.

5. Check the activated device. You can change the device IP address to the same network segment with your computer by either editing the IP address manually or checking the Enable DHCP checkbox.

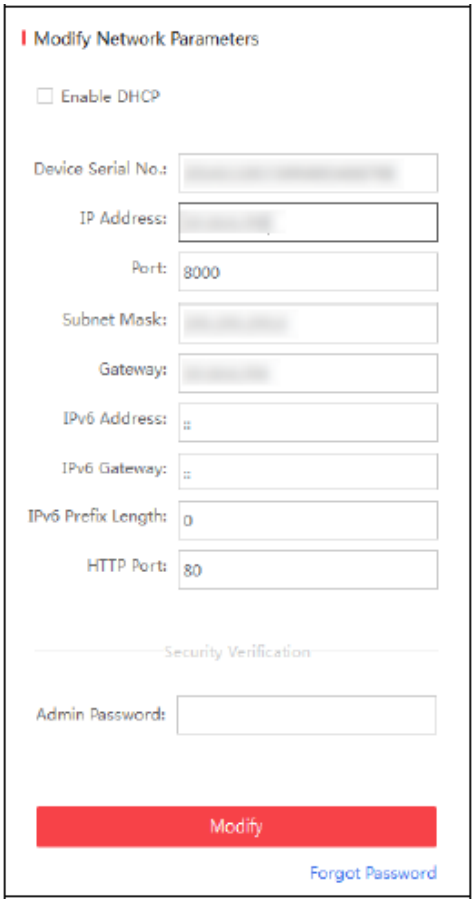


Figure 6-3: Network Parameter Modification

6. Input the password and click **Modify** to save the IP address.

6.1.3 Activating via Client Software

Purpose:
The client software is a versatile video management software for multiple kinds of devices.

Obtain the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

1. Run the client software and the control panel of the software pops up, as shown in the figure below.

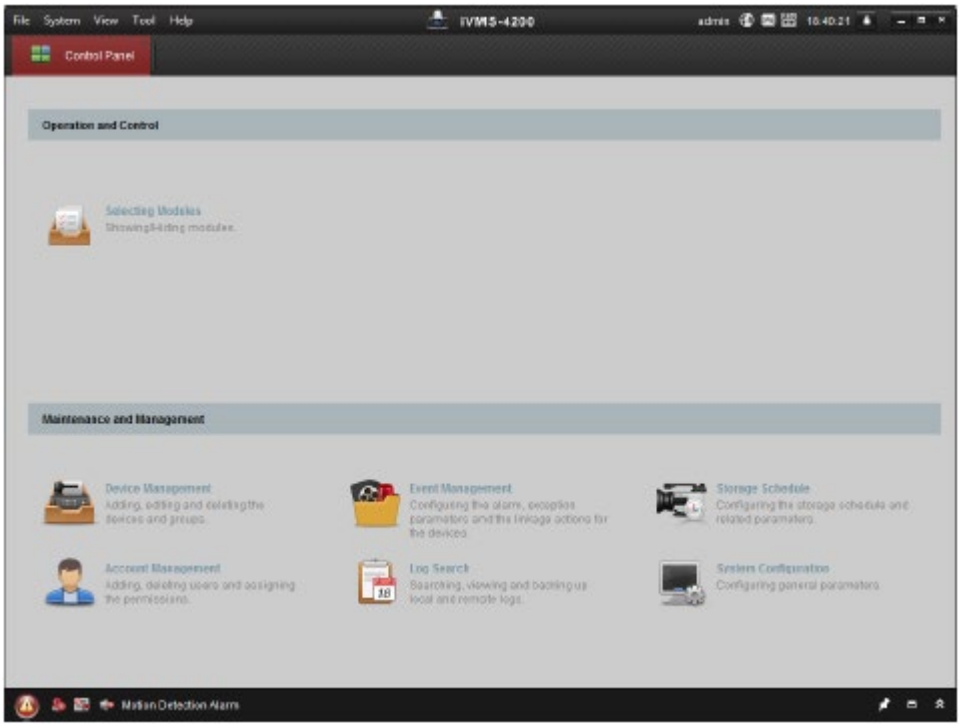


Figure 6-4: Device Management Interface

2. Click **Device Management** to enter the Device Management interface.

3. Check the device status from the device list, and select an inactive device.

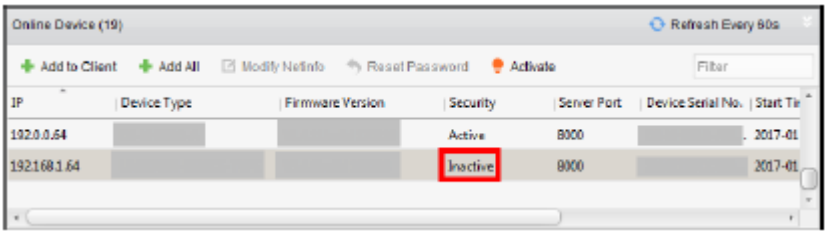


Figure 6-5: Device List Page

4. Check the device status from the device list, and select an inactive device.

5. Click Activate to display the Activation interface.

6. In the pop-up window, create a password in the password field, and confirm the password.

WARNING

We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Figure 6-6: Device Activation Password Page

7. Click **OK** button to start activation.
8. Click the **Modify Netinfor** button to display the Network Parameter Modification interface.
9. Change the device IP address to the same network segment as your computer by modifying the IP address manually.
10. Input the password and click **OK** to save the settings.

After activation, you will enter the initial page:

Figure 6-7: Initial Device Page

6.2 Login

Option 1
If this is your first login, proceed as follows:

1. Tap the settings icon at the lower right corner of the initial page to enter the Input Password page.

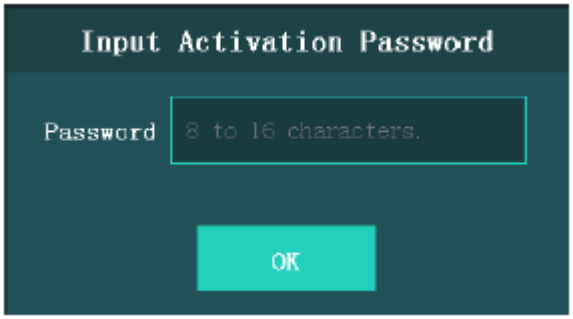


Figure 6-8: Activation Password Input Page

2. Tap the Password field and input the device activation password.
3. Tap OK to enter the home page.

Option 2
If you have already set the administrator in the User Management page, proceed as follows:

1. Tap the settings icon at the lower right corner of the initial page to enter the Login page.

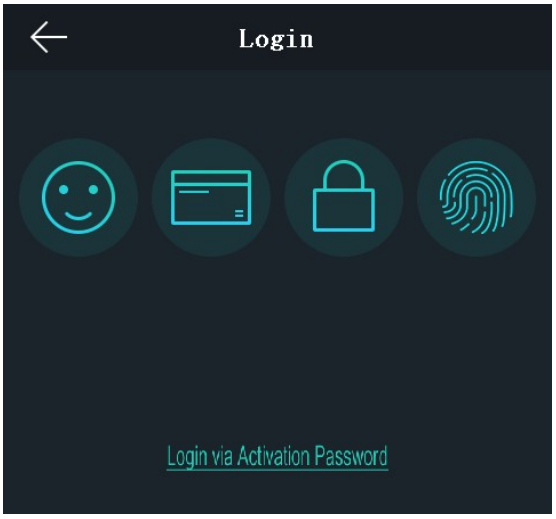


Figure 6-9: Authentication Mode Selection Interface

2. Select the login type.
3. Authenticate permissions to enter the home page.
   - Tap one of the four authentication modes on the upper side of the page and authenticate permissions.
   - Otherwise, tap **Login via Activation Password** and input the device activation password to enter the home page.

The home page is shown as below:

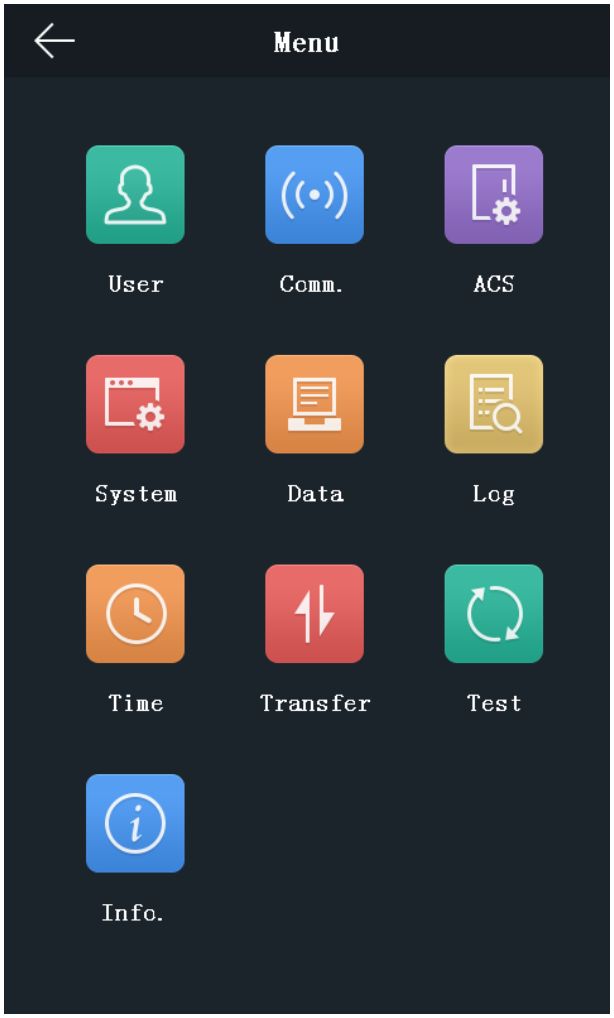


Figure 6-10: Home Page

Notes:

- The device will be locked for 30 minutes after 5 failed password attempts.
- The supported authentication modes are as follows:

  Face picture or fingerprint, card or password, fingerprint and password, fingerprint and card, face picture and password, face picture and card, card and password, fingerprint, face picture, employee ID and password, card, fingerprint or card, fingerprint or password, card or password, employee ID and fingerprint, fingerprint and card and password, employee ID and fingerprint and password, face picture and fingerprint and card, face picture and password and fingerprint, employee ID and face picture.

- Only devices equipped with the fingerprint scanning function support fingerprint authentication mode.
- For details about setting the administrator authentication mode, see *6.4.1 Adding User*.

6.3 General Parameters Settings

6.3.1 Communication Settings

Purpose:
Set the network parameters, the Wi-Fi parameter, the RS-485 parameters, and the Wiegand parameters on the communication settings page.

Tap **Comm.** (Communication Settings) on the Home page to enter the Communication Settings page.

Setting Network Parameters

Purpose:
Set the device network parameters, including the IP address, the subnet mask, and the gateway.

1. On the Communication Settings page, tap **Network** to enter the Network tab.
2. Tap **IP Address**, **Subnet Mask**, or **Gateway** and input the parameters.
3. Tap **OK** to save the settings.

Note: The device's IP address and the computer IP address should be in the same LAN.

4. Tap  to save the network parameters and go back to the Home page.

Setting Wi-Fi Parameters

Purpose:
Enable Wi-Fi function and set the Wi-Fi related parameters.

1. On the Communication Settings page, tap **Wi-Fi** to enter the Wi-Fi tab.
2. Tap  to enable the Wi-Fi function.

The icon will turns to  and all searched Wi-Fi will be listed in the Wi-Fi list.

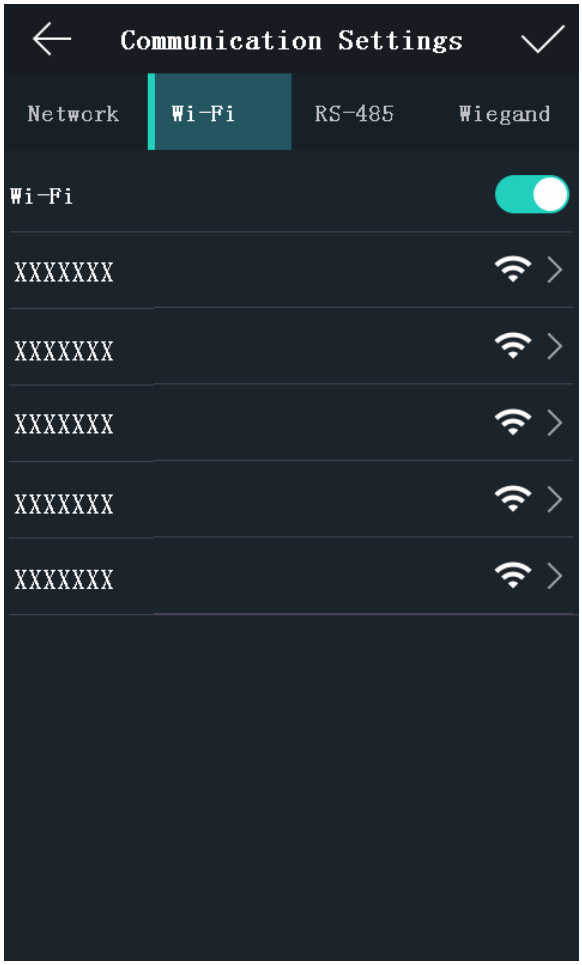


Figure 6-11: Wireless Network Selector

3. Select a Wi-Fi in the list to enter the Wi-Fi parameters settings page.

4. Select an IP mode.

If selecting **Static**, you should input the Wi-Fi password, IP address, subnet mask and gateway. If selecting **Dynamic**, you should input the Wi-Fi password.

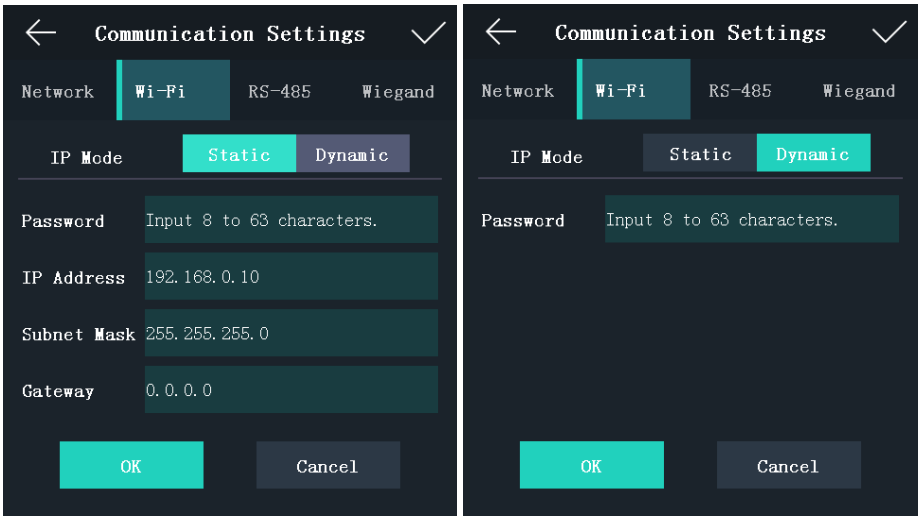


Figure 6-12: Static and Dynamic IP Mode Wireless Settings

Note: Numbers, upper case letters, lower case letters, and special characters are allowed in the Wi-Fi password.

5. Tap **OK** to save the settings and go back to the Wi-Fi tab.

6. Tap ✓ to save the Wi-Fi parameters and go back to the Home page.

Setting RS-485 Parameters

Purpose:
The face recognition terminal can connect external secure door control unit or card reader via the RS-485 terminal.

1. In the Communication Settings page, tap **RS-485** to enter the RS-485 tab.

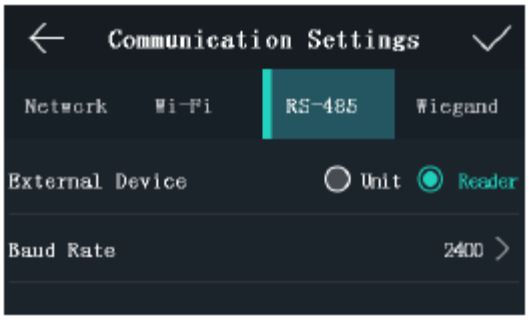


Figure 6-13: RS-485 Settings

2. Select your preferred external device.

Note: Unit represents the secure door control unit and Reader represents the card reader.

3. Tap Baud Rate to enter the Baud Rate page.
4. Select a baud rate for connecting external device via the RS-485 protocol.
5. Tap ✓ to save the selected baud rate and go back to the RS-485 tab.
6. Tap ✓ to save the RS-485 parameters and go back to the Home page.

Note: If you change the external device, and after you save the device parameters, the device will reboot automatically.

Setting Wiegand Parameters

Purpose:
Set the Wiegand transmission direction and the Wiegand mode.

1. On the Communication Settings page, tap **Wiegand** to enter the Wiegand tab.

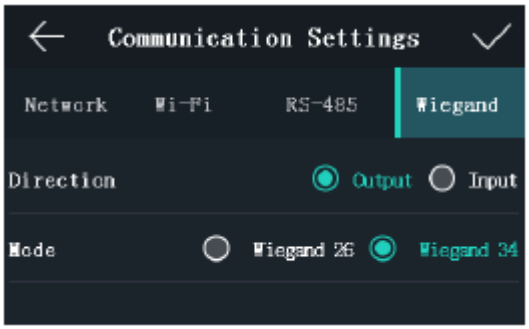


Figure 6-14: Wiegand Mode

2. Select the transmission direction and its mode.

Transmission Direction:

- Output: A face recognition terminal can connect to an external access controller. The two devices will transmit the card number via Wiegand 26 or Wiegand 34 modes.
- Input: A face recognition terminal can connect to a Wiegand card reader. There is no need to set the Wiegand mode.

Mode:
Select Wiegand 26 or Wiegand 34. The system selects Wiegand 34 by default.

3. Tap ✓ to save the Wiegand parameters and go back to the Home page.

Note: When the Wiegand mode is changed and the parameters are saved, the device will reboot automatically.

6.3.2 System Settings

Purpose:
In the System Settings page, you can set the system basic parameters, set the face picture parameters, and upgrade the firmware.

On the Home page, tap **System** (System Settings) to enter the System Settings page.

Setting Basic Parameters

Purpose:
Set the device ID, time format, keyboard sound, voice prompt, voice volume, power saving mode, auto enable supplement light, and brightness.

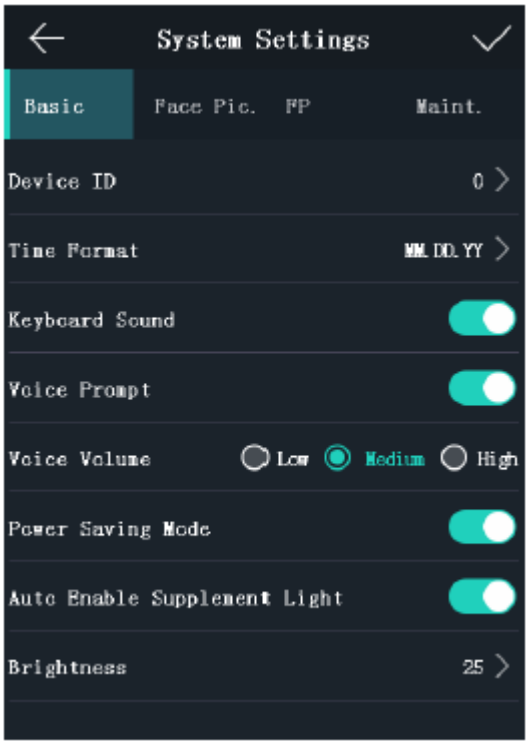


Figure 6-15: System Settings

Table 6-1: Description of System Settings

Parameter	Description
Device ID	Set the face recognition terminal's device ID number. The device ID is the DIP address for that is used for communication between the device and the access controller, if the device connects to an access controller via the RS-485 protocol.
Time Format	You can select one of the following formats: MM/DD/YYYY, MM.DD.YYYY, DD-MM-YYYY, DD/MM/YYYY, DD.MM.YYYY, YYYYMMDD, YY-MM-DD, YY/MM/DD, and MM-DD-YYYY.
Keyboard Sound	Tap  or  to disable or enable the keyboard sound.
Voice Prompt	Tap  or  to disable or enable the voice prompt.
Voice Volume:	You can adjust the voice volume to Low, Medium or High.
Power Saving Mode	You can enable power saving mode to lower power consumptions.
Auto Enable Supplement Light:	If enabling the function, when the device detects obstructions via the active infrared intrusion detector, the supplement light will be automatically turned on. If not, the supplement light will be turned off automatically.
Brightness	Set the brightness of the supplement light. The brightness ranges from 0 to 100. 0 indicates that the supplement light is turned off. 1 is equivalent to the darkest light, and 100 is equivalent to the brightest light.

Note: The device ID should consist of numbers and range from 0 to 255.

Setting Face Picture Parameters

Purpose:
Set the following face picture security parameters: 1:N Level, 1:1 Level, Liveness Level, Recognition Interval, Duplicated Person, Live Face Detection, Lock Face, and Max. Failed Attempts.

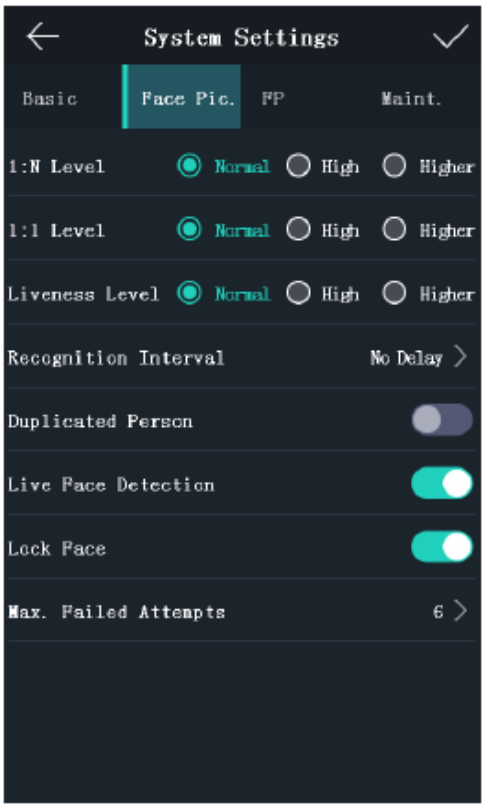


Figure 6-16: Face Picture Parameters

Table 6-2: Description of Face Picture Parameters

Parameter	Description
1:N Level	Set the matching security level when authenticating via 1:N matching mode.
1:1 Level	Set the matching security level when authenticating via 1:1 matching mode.
Liveness Level	After enabling Live Face Detection function, you can set the matching security level when performing live face authentication.
Recognition Interval	The time interval between two continuous face recognitions when authenticating. It is 2s by default. ***Note:*** You can input the number from 1 to 10 or 255. 255 represents infinity.
Duplicated Person	If enabling the function, when authentication face picture, the system will remind you when the authenticated face picture is the same with the one in the database.
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.
Lock Face	After enabling the Live Face Detection function, the system will lock the user's face for 5 minutes if the live face detection has failed for more than the configured number of attempts. The same user cannot authenticate with an incorrect face within those 5 minutes. Within the same 5 minutes, the user can authenticate using a real face twice continuously to unlock.
Max. Failed Attempts	Set the maximum live face detection failed attempts. The system will lock the user's face for 5 minutes if live face detection has failed for more times than the number of configured attempts. The same user cannot authenticate using an incorrect face within those 5 minutes. Within these 5 minutes, the user can successfully authenticate twice using a real face.

Setting Fingerprint Parameters

Purpose:
Set the fingerprint security level in this section.

Note: Only the device with the fingerprint scanning function supports the fingerprint related function.

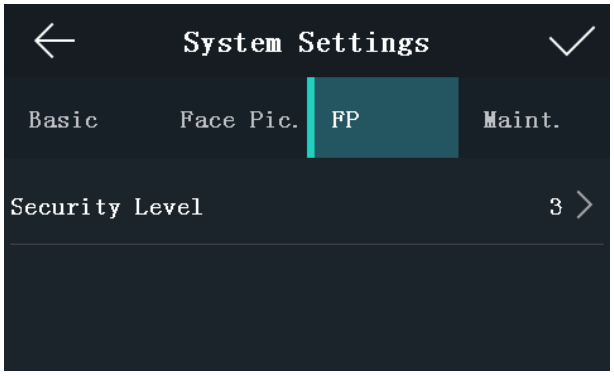


Figure 6-17: Security Level Settings

Table 6-3: Security Level Description

Parameter	Description
Security Level	Set the fingerprint security level. The higher the security level, the lower the false acceptance rate (FAR) is. The higher the security level, the higher the false rejection rate (FRR) is.

Rebooting Device

1. In the System Settings page, tap **Maint.** (Maintenance) to enter the Maintenance page.
2. Tap **Reboot.**

The device will start to reboot.

Upgrading Firmware

1. Tap **Maint.** (Maintenance) in the System Settings page.
2. Plug in the USB flash drive.
3. Tap Upgrade.

The device will automatically read the upgrading file in the USB flash drive and upgrade the firmware.

Note:

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

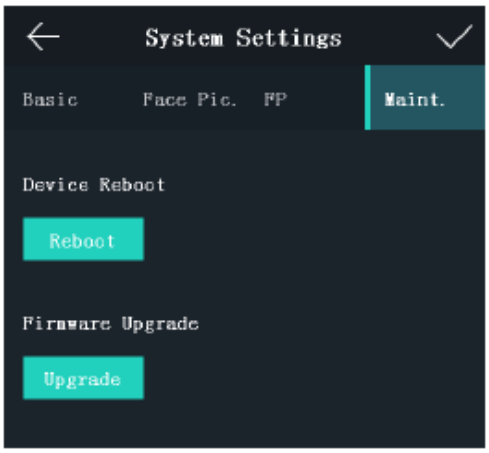


Figure 6-18: Device Reboot and Firmware Upgrade Page

6.3.3 Setting Time

Purpose:
Set the device time and the DST in this section.

1. Tap **Time** (Time Settings) on the Home page to enter the Time Settings page.

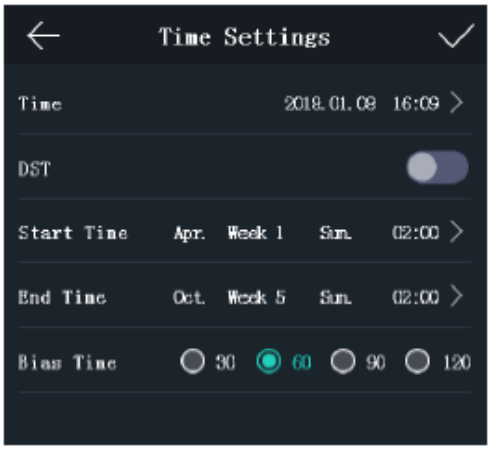


Figure 6-19: Time Settings Page

2. Edit the time parameters.

Table 6-4: Time Parameter Descriptions

Parameter	Description
Time	Set the time that will be displayed on the device screen.
DST	Enable or disable DST function. When enabling the DST function, you can set the DST start time, end time, and the bias time. **Start Time:** Set the DST start time. **End Time:** Set the DST end time. **Bias Time:** Set the DST bias time when the DST starts.

3. Tap ✓ to save the settings and go back to the Home page.

6.4 User Management

Purpose:
On the user management interface, you can add, edit, delete and search the user. Tap **User** on the Home page to enter the User Management page.

Figure 6-20: User Management Interface

6.4.1 Adding User

Purpose:
On the Add User page, you can add users, including the employee number, name, and card number. You can also link the fingerprint, the face picture to the user, or set password, authentication mode, schedule template, administrator permission for the user.

Notes:

- Up to 5000 users can be added.
- The device with the DS-K1T606M model does not support fingerprint function.

1. On the User Management page, tap **+** to enter the Add User page.
2. Tap the **Employee ID.** field and edit the employee ID.

Notes:
The employee ID should be between 1 and 99999999. The employee ID should not start with 0 and should not be duplicated.

3. Tap the **Name** field and input the user name on the soft keyboard.

Notes:

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

4. Tap the **Card** field and input the card No.

Option 1: Input the card No. manually.

Option2: Swipe the card over the card swiping area to get the card No.

Notes:

- The card No. cannot be empty.
- Up to 20 characters are allowed in the card number.
- By default, the card number contains 10 characters. The system will use 0 to supplement the 10-character-card number. For example, 5 and 0000000005 are two different card numbers.
- The card No. cannot be duplicated.

5. Tap the **Password** field and create a password and confirm the password.

Note:

- Only numbers are allowed in the password.
- Up to 8 characters are allowed in the password.

6. Tap the **Fingerprint** field to enter the Add Fingerprint page.

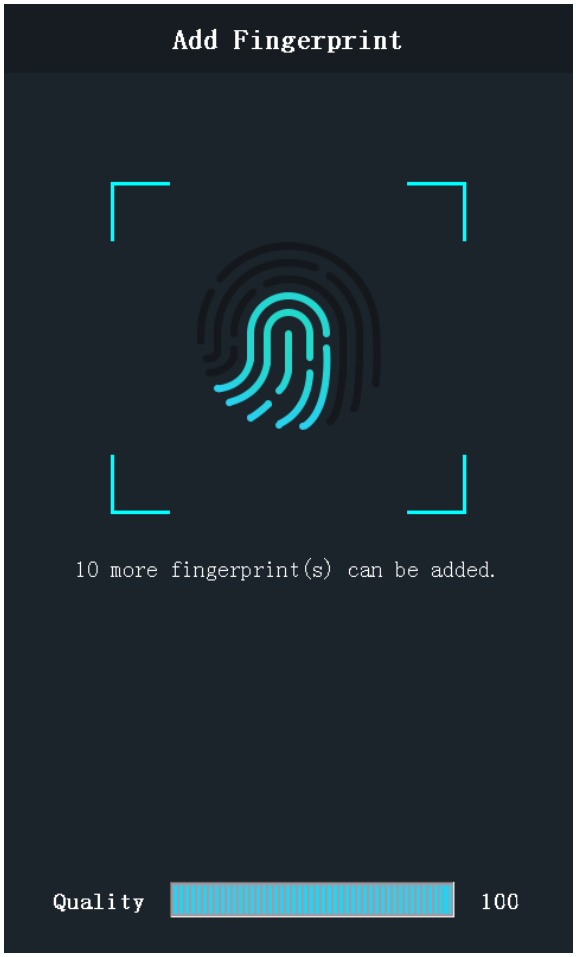


Figure 6-21: Add Fingerprint Page

Follow the steps below to add fingerprint.

1) Place your finger on the fingerprint module.
2) Follow the instructions on the screen to record the fingerprint.
3) After adding the fingerprint completely, tap **Yes** in the pop-up dialog to save the fingerprint and continue to add another fingerprint.

Alternatively, tap **No** to save the fingerprint and go back to the Add User page.

Notes:

- The same fingerprint cannot be repeatedly added.
- Up to 10 fingerprints can be added for one user.
- Use the client software or the fingerprint recorder to record fingerprints.
- For details about the instructions of scanning fingerprints, see Appendix A Tips for Scanning Fingerprint.

7. Tap the **Face Picture** field to enter the face picture adding page.

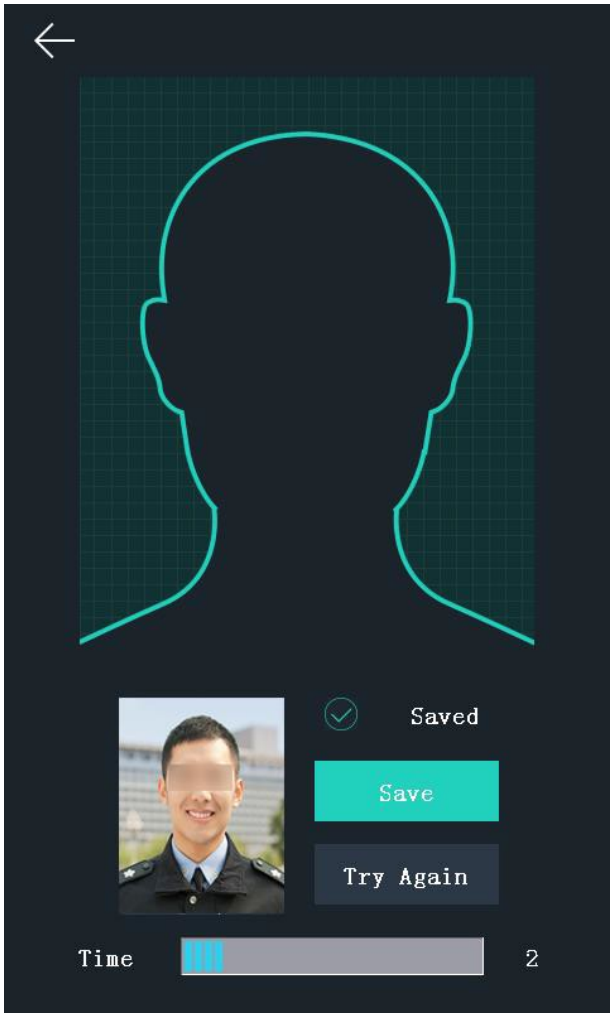


Figure 6-22: User Face Picture Addition

Follow the steps below to add the user's face picture.

1) Position your face looking at the camera.

Note: Make sure your face picture is in the face picture outline when adding the face picture.

After completely adding the face picture, a captured face picture will be displayed on the page.

Notes:

- Make sure the captured face picture is good quality and accurate.
- For details about the instructions of adding face pictures, see Appendix B Tips When Collecting/Comparing Face Picture.

2) Tap **Save** to save the face picture.

Otherwise, tap **Try Again** and adjust your face position to add the face picture again.

Note: The maximum duration for adding a face picture is 15s. Check the remaining time for adding a face picture on the left side of the page.

8. Tap the **Profile Photo** field and view the captured picture when adding the face picture.

9. Tap the **Schedule Template** field to enter the Schedule Template page. Select a schedule template

and tap ✓ to save the settings.

Note: For details about setting the schedule template, see *7.6 Schedule and Template*. After applying the schedule tem plate from the client software to the device, select the corresponding schedule template

10. Tap **Authentication Mode** to enter the Authentication Mode page. Select **Device** or **Custom** as the authentication mode.

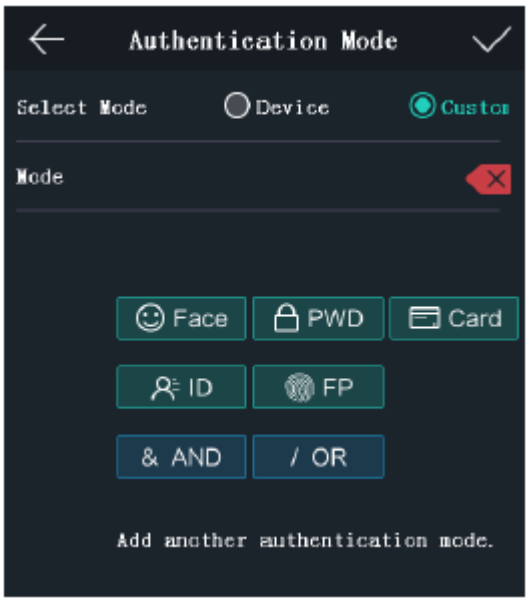


Figure 6-23: Authentical Mode Page

- **Device:** If you want to select the device mode, you should first set the terminal authentication mode in Access Control Settings. For details see *6.5 Setting Access Control Parameters*.
- **Custom:** Combine different authentication modes together, as required.

Tap ✓ to save the settings.

Note: The DS-K1T606M product model does not support the fingerprint function.

11. Enable or disable the **Administrator Permission** function.

Enable Administrator Permission	The user is an administrator. Other than the normal attendance function, the user can also enter the Home page after completing authentication.
Disable Administrator Permission	The user is a normal user, and can only use the attendance function on the initial page.

12. Enable or disable the **Duress Card** function.

    When the function is enabled, the user's card will be the duress card. When the user authenticates by swiping this duress card, the device will upload a duress card event to the client software.

13. Tap ✓ to save the user parameters and go back to the Home page.

6.4.2 Managing User

Searching User

Purpose:
You can search the user in the list according to the employee ID, the card number, or the user name.

1. On the User Management page, Tap 🔍 to enter the Search User page.

Figure 6-24: Search User Page

2. Tap Card on the left of the page and select a search type from the drop-down list.
3. Tap the input box and input the employee ID, the card number, or the user name that you wish to search for.
4. Tap 🔍 to start the search.

The search results will be displayed in the list below.

Editing User

Purpose:
You can edit the added user information by following the steps in this section.

1. In the User Management page, tap the user that needs to be edited, to enter the Edit User page.
2. Refer to the parameter instructions in *Section 6.4.1 Adding User* to edit the user information.
3. Tap ✓ to save the settings and go back to the User Management page.

Note: The employee ID cannot be edited.

6.5 Setting Access Control Parameters

Purpose:
Set the following access control permissions: Reader/Terminal Authentication Mode, Door Magnetic Sensor, Anti-Passback, Lock Locked Time, Door Open Timeout Alarm, and Max. Failed Authentications.

1. On the Home page, tap **ACS** (Access Control Settings) to enter the Access Control Settings page.

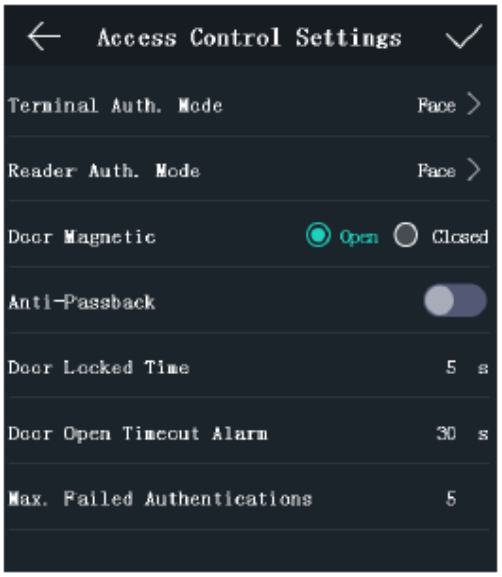


Figure 6-25: Access Control Settings

2. Edit the access control parameters.

The available parameters descriptions are as follows:

Table 6-5: Access Control Parameter Setting Descriptions

Parameter	Description
Terminal Auth. Mode (Terminal Authentication Mode)	Select and customize the face recognition terminal authentication mode. ***Notes:*** • Only the device with the fingerprint scanning function supports related fingerprint functionality. • For better security, do not use single authentication mode.
Reader Auth. Mode (Card Reader Authentication Mode)	Select the card reader authentication mode.
Door Magnetic	Select **Remain Open** or **Remain Closed**, as required. Remain Closed is enabled by default.
Anti-Passback	When enabling the anti-passback function, you should set the anti-password path in the iVMS-4200 Client Software. The person should authenticate according to the configured path. Otherwise, authentication will fail.
Door Locked Time	Set the door unlocking duration. If the door is not opened in the set time, the door will be locked. The available door locked time range is 1 to 255 s.

Door Open Timeout Alarm	The alarm can be triggered if the door has not been closed. The available door locked time range is 1 to 255 s.
Max. Failed Authentications	Set the maximum authentication times. If authentication fails a set number of times, the alarm will be triggered. The available door locked time range is 1 to 255 s.

3. Tap ✓ to save the settings.

6.6 Other Managements

6.6.1 Managing Data

Purpose:
In the Data Management page, you can Delete All Events, Delete User Data, Delete All Data, Clear Permission, Delete Captured Pictures, Restore to Factory Settings, or Restore to Default Settings.

1. Tap **Data** (Data Management) to enter the Data Management page.

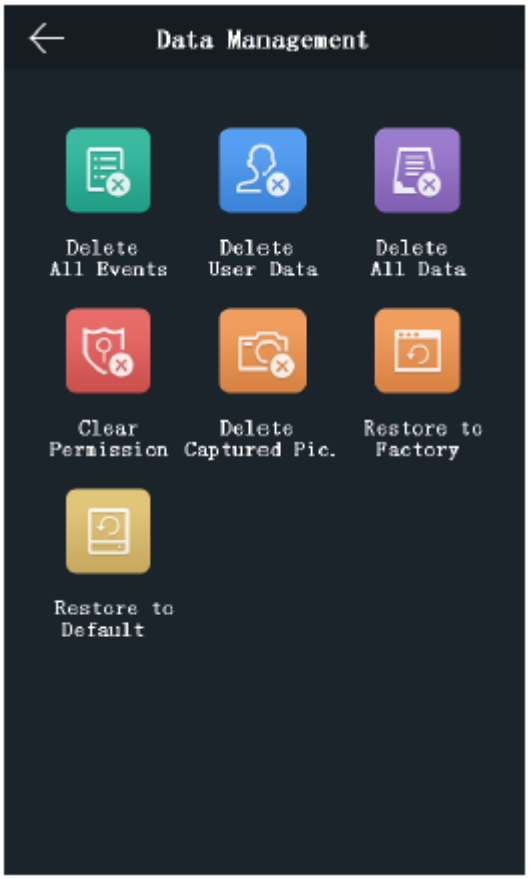


Figure 6-26: Data Management Page

2. Tap the button on the page to manage data.

The available button descriptions are as follows:

Table 6-6: Data Management Function Descriptions

Parameter	Description
Delete All Events	Delete all events stored in the device.
Delete User Data	Delete all user data in the device.
Delete All Data:	Delete all user data and events stored in the device.
Clear Permission	Clear the administrator permission. The administrator and related logs will not be deleted.
Delete Captured Pic.	Delete the device captured pictured.
Restore to Factory	Restore the system to the factory settings. The device will reboot afterwards.
Restore to Default	Restore the system to the default settings. The system will save the communication settings and the remote user settings. Other parameters will be restored to default.

3. Tap **Yes** on the pop-up window to complete the settings.

6.6.2 Managing Log Query

Purpose:
You can search the authentication logs within a period of time by inputting the employee ID, card number, or user name.

1. On the Home page, tap **Log** (Log Query) to enter the Log Query page.
2. Tap Card on the left of the page and select a search type from the drop-down list.
3. Tap the input box and input the employee ID, the card number, or the user name for search.
4. Select time.

   You can select from Custom, Yesterday, This Week, Last Week, This Month, Last Month, or All.

   If you select **Custom**, you can customize the start time and the end time for search.
5. Tap  to start search.

The result will be displayed in the page.

6.6.3 Importing/Exporting Data

Purpose:
In the Transfer page, you can export the attendance data, the user data, the user picture, the access control parameter, and the captured picture to the USB flash drive. You can also import the user data, the user picture, and the access control parameter from the USB flash drive.

Tap **Transfer** on the Home page to enter the Transfer page.

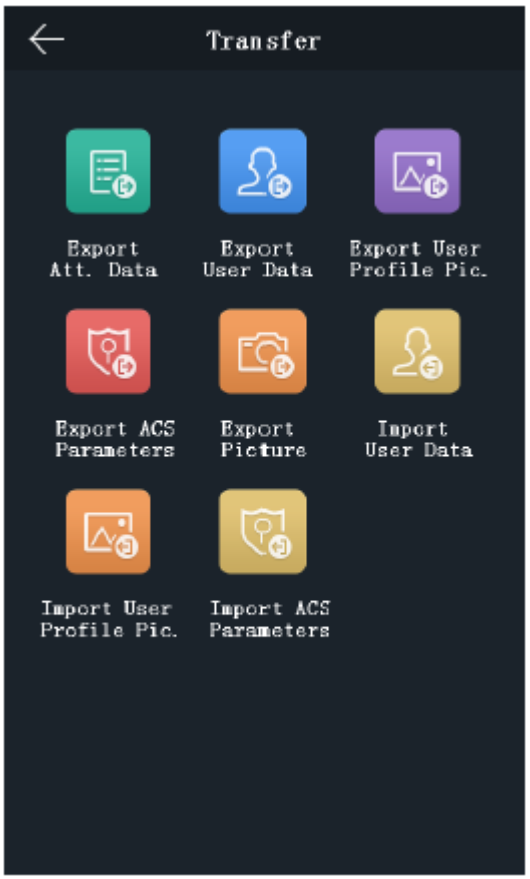


Figure 6-27: Transfer Settings Page

Exporting Data

1. Plug a USB flash drive in the device.
2. On the Transfer page, tap one of the following: **Export Att. Data**, **Export User Data**, **Export User Profile Pic.**, **Export ACS Parameters**, **or Export Picture** (Export Captured Picture).
3. Tap **Yes** on the pop-up page and the data will be exported from the device to the USB flash drive.

Notes:

- The supported USB flash drive format is FAT32.
- The system supports the USB flash drive with the storage of 1 GB to 32 GB. Make sure that there are more than 512 MB on the USB flash drive.
- The exported user data is a BIN file, which cannot be edited.

Importing Data

1. Plug a USB flash drive into the device.
2. On the Transfer page, tap one of the following: **Import User Data**, **Import User Profile Pic.**, **or Import ACS Parameters**.
3. Tap **Yes** on the pop-up window and the data will be imported from the USB flash drive to the device.

Notes:

- If you want to transfer all user information from one device (Device A) to another (Device B), you should export the information from Device A to the USB flash drive and then import from the USB

flash drive to Device B. In this case, you should import the user data before importing the profile photo.

- The supported USB flash drive format is FAT32.
- The imported picture should be saved in the root directory (enroll_pic) and the picture file name should be named according to the following rule:
- Card No._Name_Department_Employee ID_Gender.jpg
- The employee ID should between 1 and 99999999, should not be duplicated, and should not start with 0.
- Face picture requirements: the picture should be taken in full-face view, directly facing the camera. Do not wear a hat or head covering when taking the face picture. The format should be JPEG or JPG. The resolution should be more than 640 × 480 pixel and less than 2160 × 3840 pixel. The picture size should be between 50 KB and 200 KB. The pupillary distance should be 60 pixels.

6.6.4 Testing

Purpose:
Test the capability of the device's face detection function, voice prompt function, fingerprint authentication function, time, and buttons.

Note: The device with the model of DS-K1T606E does not display the fingerprint test page. Tap **Test** on the Home page to enter the Automatic Test page.

Figure 6-28: Face Functionality Test Page

Table 6-7: Face Functionality Test Descriptions

Parameters	Description
Face Test	Position your face looking at the camera and the device will test the face detection function.
Voice Test	If the voice prompt function is working properly, you will hear the voice prompt "Authenticated" from the device. A prompt will also be displayed on the page.
RTC Test	If the device RTC is working properly, the page will display the current device time.
Fingerprint Test	Tap **Start** on the page, and put your finger on the fingerprint module. If the function is working properly, the page will display the fingerprint quality.

6.6.5 Viewing System Information

Viewing Capacity

Purpose:
You can view the added user's number, the face picture's number, the card's number, the password's number, and the fingerprint's number.

Note: The device with the model of DS-K1T606E does not support displaying the fingerprint capacity.

Tap **Info.** (System Information) **-> Capacity** on the Home page to enter the Capacity page.

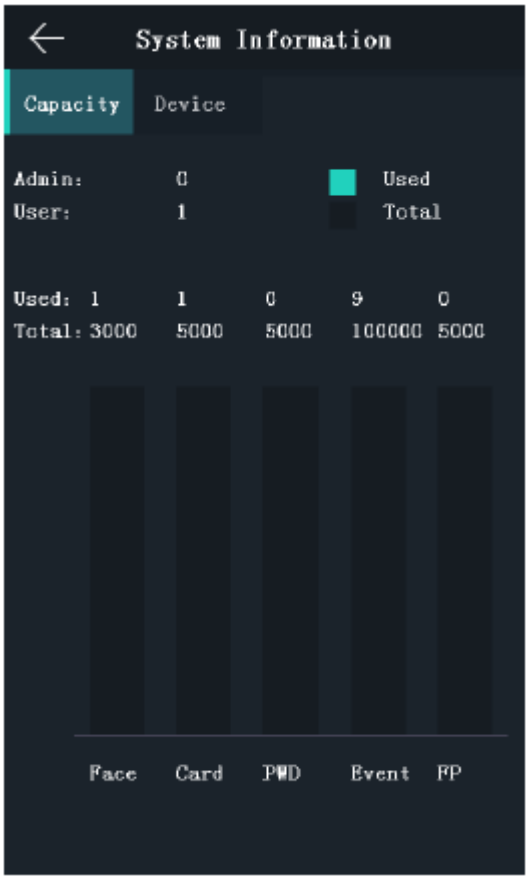


Figure 6-29: System Information Page

Viewing Device Information

Purpose:
You can view the device model, the serial number, the MAC address, the firmware version, the face algorithm version, the production date, and the fingerprint algorithm version.

Tap **Device** to enter the Device page.

Note: The device information page may vary according to different device models.

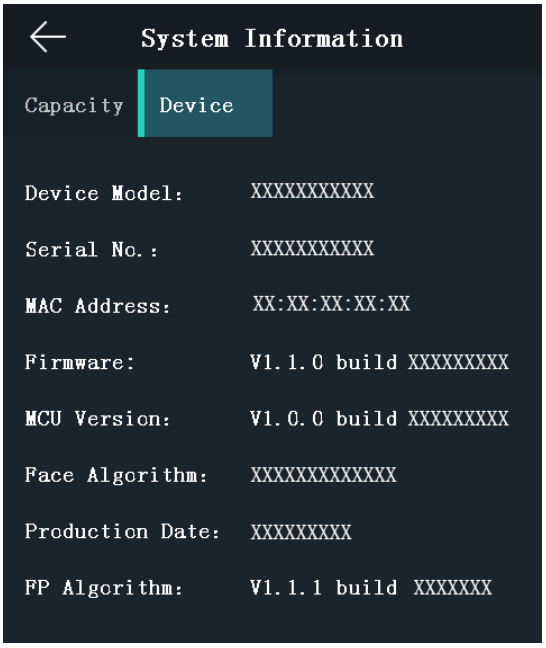


Figure 6-30: System Information Page

6.7 Authenticating Identity

Purpose:
You can authenticate identity via 1:1 or 1:N matching. If it is difficult to recognize the face, use the 1:1 face matching mode. If the light quality or other environmental factors make it difficult to complete face recognition, you can use fingerprint authentication or other authentication modes.

Note: If you require a higher security level, do not use single authentication mode.

1:N Matching	Compare the captured face picture or the collected fingerprint picture with all face pictures or all fingerprint pictures stored in the device
1:1 Matching	Compare the captured face picture or the collected fingerprint picture with the face picture, fingerprint picture, or password stored alongside the employee ID.

6.7.1 Authenticating via 1:1 Matching

1. On the Initial page, tap **1:1** at the lower right corner of the page to enter the 1:1 matching page.
2. Input the employee ID.
3. Tap , , or to authenticate via face picture, fingerprint, or password.

Note: Tap to switch to the password inputting page. Input the super password or duress code for authentication.

6.7.2 Authenticating via Other Types

1. According to the configured authentication mode, authenticate by comparing face pictures, fingerprints or by swiping card.

Face Picture Authentication	Stand in front of the device. Position your face looking at the camera and the device will enter the face picture authentication mode. ***Note:*** For detailed information about authenticating face picture, see *Appendix B Tips When Collecting/Comparing Face Picture*.
Fingerprint Picture Authentication	Scan your fingerprint on the fingerprint module of the device. For detailed information about scanning a fingerprint, see *Appendix A Tips for Scanning Fingerprint*.
Authentication by Swiping Card	Swipe card above the card swiping area.

2. If the user has no other authentication modes, the authentication is complete. If the user has other authentication modes after the first authentication, follow the instructions to continue authenticating until the authentication is completed.

Chapter 7 Client Operation

Set and operate the access control devices via the client software. This chapter will introduce the access control device related operations in the client software. For integrated operations, refer to the *iVMS-4200 Client Software User Manual*.

7.1 User Registration and Login

Register the super user name and password when using the iVMS-4200 client software for the first time.

1. Input the super user name and password. The software will judge password strength automatically, and we highly recommend that you use a strong password to ensure your data security.
2. Confirm the password.
3. Optionally, check the checkbox Enable Auto-login to log into the software automatically.
4. Click Register. Then, you can log into the software as the super user.

WARNING

- A user name cannot contain any of the following characters: / \ : * ? " < > |. And the length of the password cannot be less than 6 characters.
- For your privacy, we strongly recommend changing the password to something 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.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

When opening iVMS-4200 after registration, you can log into the client software with the registered user name and password.

1. Input the user name and password you registered.
2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
3. Click **Login**.

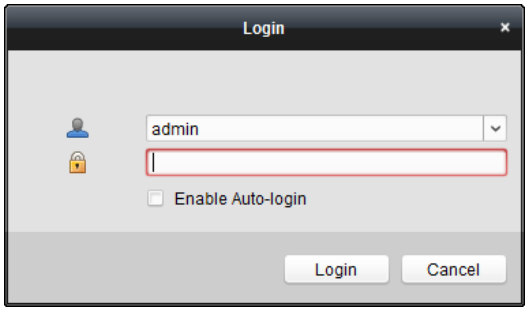


Figure 7-1: iVMS-4200 Login Page

After running the client software, you can open the wizards (video wizard, video wall wizard, security control panel wizard, access control and video intercom wizard, and attendance wizard) that will help

you add the device and perform other operations. For detailed wizard configuration, refer to the *iVMS-4200 Quick Start Guide*.

7.2 System Configuration

Purpose:
You can synchronize the missed access control events with the client.

1. Click **Tool** – **System Configuration**.
2. In the System Configuration window, check the Auto-synchronize Access Control Event checkbox.
3. Set the synchronization time.

The client will auto-synchronize the missed access control event to the client at the set time.

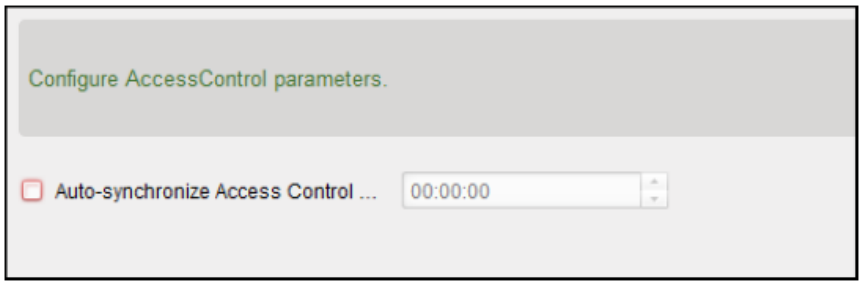


Figure 7-2: Synchronization Time Window

7.3 Access Control Management

Purpose:
The Access Control module is applicable to access control devices and video intercom. It provides multiple functionalities, including person and card management, permission configuration, access control status management, video intercom, and other advanced functions.

You can also set the event configuration for access control and display access control points and zones on E-map.

Note: Users with access control module permissions, the user can enter the Access Control module and configure the access control settings.

Click  in the control panel, and check **Access Control** to add the Access Control module to the control panel.

Click  to enter the Access Control module.

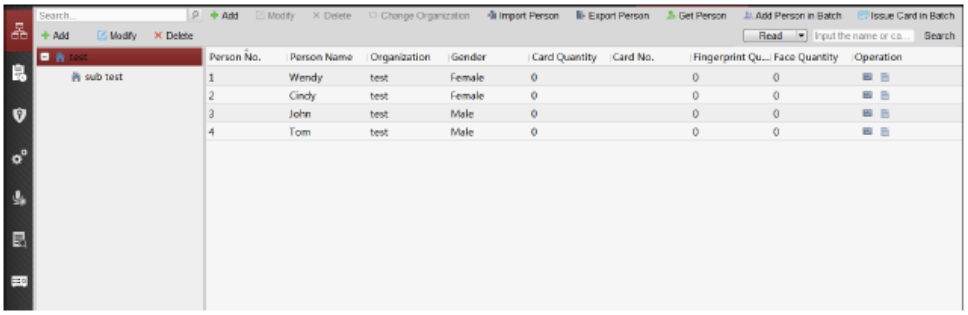


Figure 7-3: Access Control Module

Before you start:
When opening the Access Control module for the first time, the following dialog will display and you are required to select the scene according to the actual needs.

Non-residence: Set the attendance rule when adding a person, while set the access control parameters.

Residence: You cannot set the attendance rule when addinga person.

Figure 7-4: Scene Selector

Note: Once the scene is configured, you cannot change it later.

7.3.1 Adding Access Control Device

Click  in the Access Control module to enter the following interface.

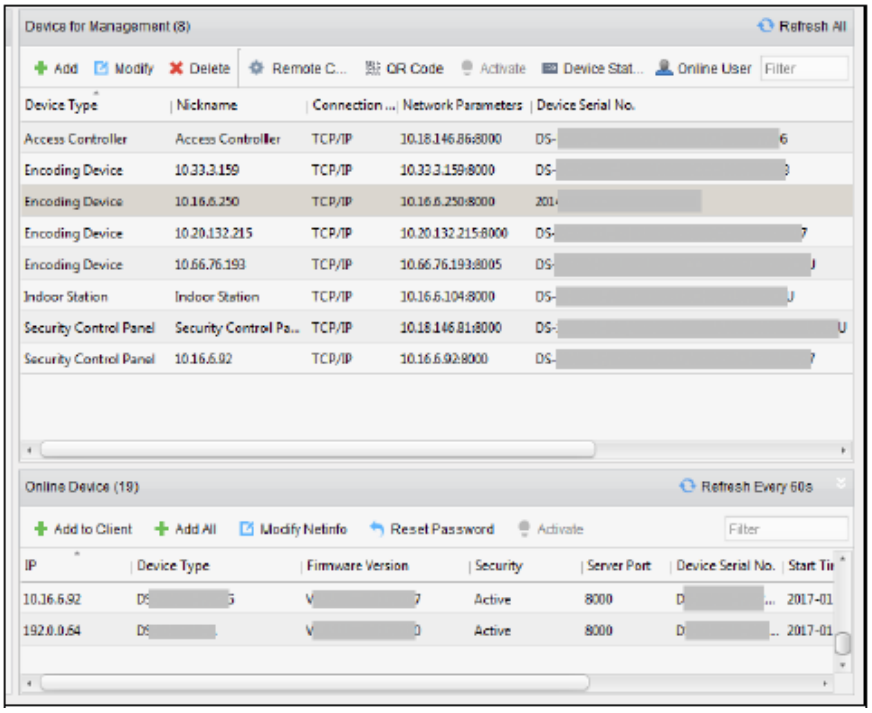


Figure 7-5: Device Management Interface

Note: After adding the device, you should check the device arming status in **Tool** – **Device Arming Control**. If the device is not armed, you should arm it, or you will not receive the real-time events via the client software. For details about device arming control, refer to *7.12 Arming Control*.

Creating Password

Purpose:
For some devices, you are required to create a password in order to activate them, before they can be added to the software and work properly.

Note: This function should be supported by the device.

1. Enter the Device Management page.
2. In the **Device for Management** or **Online Device** area, check the device status (shown on **Security** column) and select an inactive device.
3. Click the **Activate** button to display the Activation interface.
4. Create a password in the password field and confirm the password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

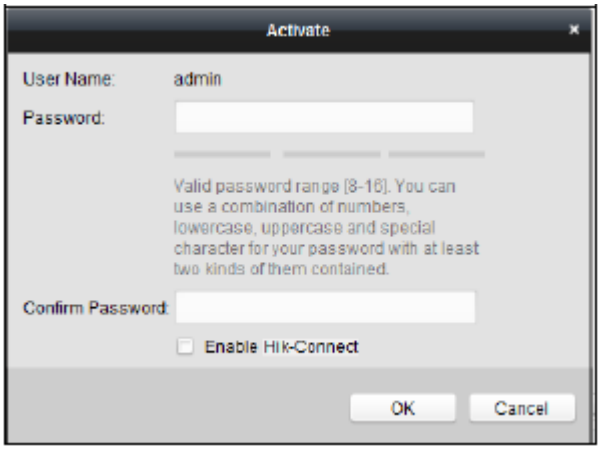


Figure 7-6: Password Selection Page

5. (Optional) Enable Hik-Connect service when activating the device if the device supports.

    1) Check **Enable Hik-Connect** checkbox to display the Note dialog box.

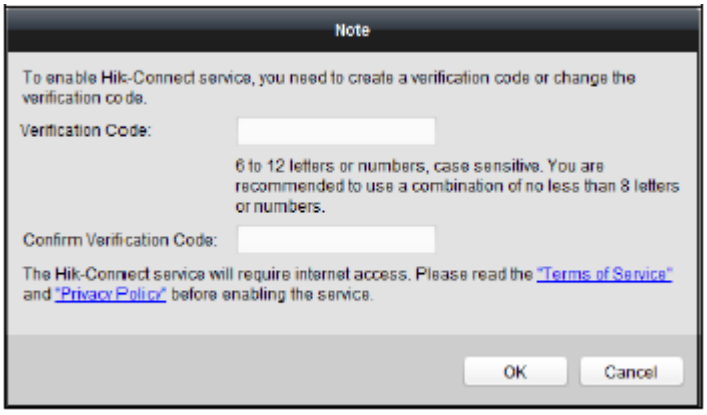


Figure 7-7: Verification Code Page

2) Create a verification code.

3) Confirm the verification code.

4) Click **Terms of Service** and **Privacy Policy** to read the requirements.

5) Click **OK** to enable the Hik-Connect service.

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

   A "The device is activated" window displays when the password is set successfully.

7. Click **Modify Netinfo** to display the **Modify Network Parameter** interface.

Note: This function is only available in the **Online Device** area. You can change the device IP address to the same subnet as your computer if you need to add the device to the software.

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of DHCP.

9. Input the password set in Step 4 and click **OK** to complete the network settings.

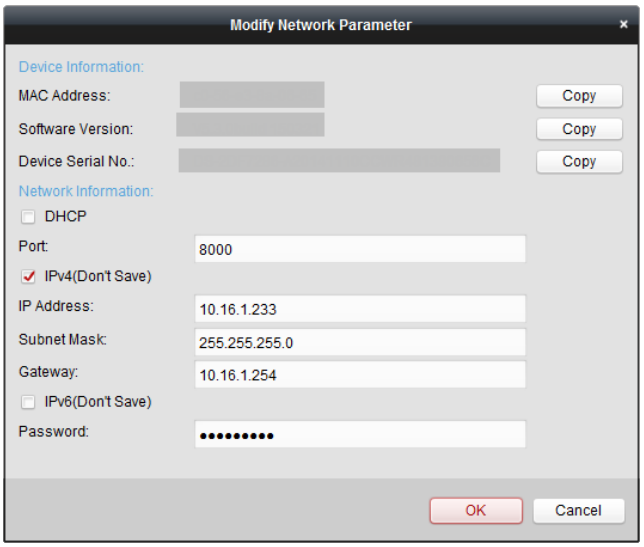


Figure 7-8: Network Parameter Modification Page

Adding Online Device

Purpose:
The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click the **Refresh Every 60s** button to refresh the information of the online devices.

Note: You can click to hide the **Online Device** area.

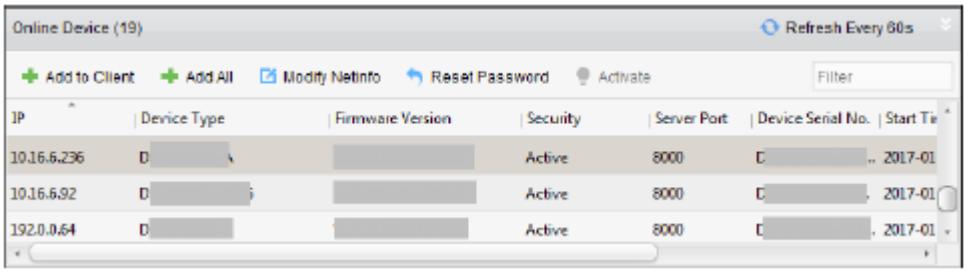


Figure 7-9: Online Devices Page

1. Select the devices to be added from the list.

Note: For inactive devices, create a strong password before adding the device.

2. Click **Add to Client** to open the device adding dialog box.

3. Input the required information.

Nickname: Edit a name for the device.

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

Port: Input the device port number. The default value is *8000*.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all of the device channels of the corresponding group by default.

Note: iVMS-4200 also provides a method to add the offline devices.

   1) Check the **Add Offline Device** checkbox.

   2) Input the required information, including the device channel number and alarm input number.

   3) Click **Add**.

When offline devices come online, the software connects to them automatically.

5. Click **Add** to add the device.

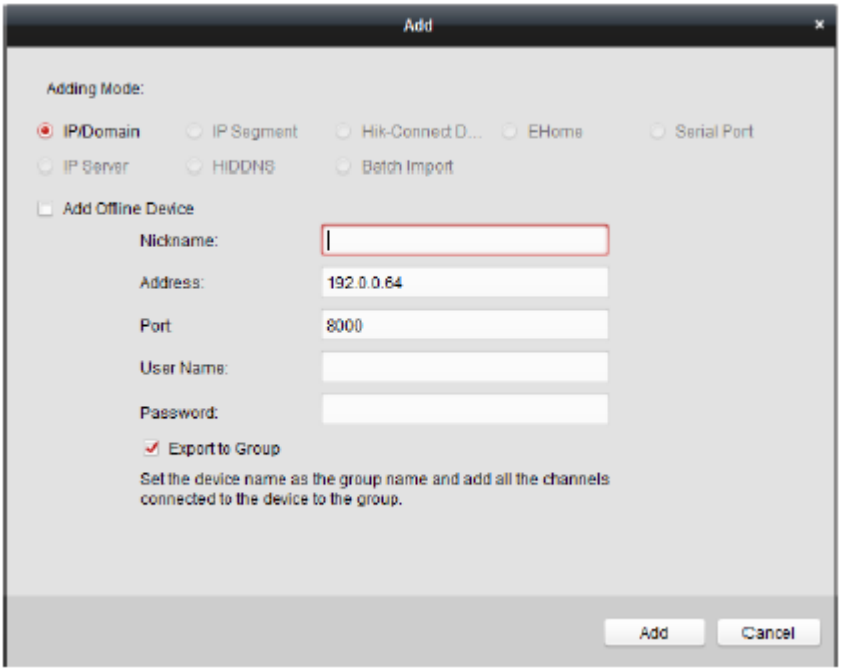


Figure 7-10: Device Addition Page

Adding Multiple Online Device

If you want to add multiple online devices to the client software, click and hold the *Ctrl* key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.

Adding All Online Devices

If you want to add all the online devices to the client software, click **Add All** and click **OK** in the pop-up message box. Then, enter the user name and password for the devices to be added.

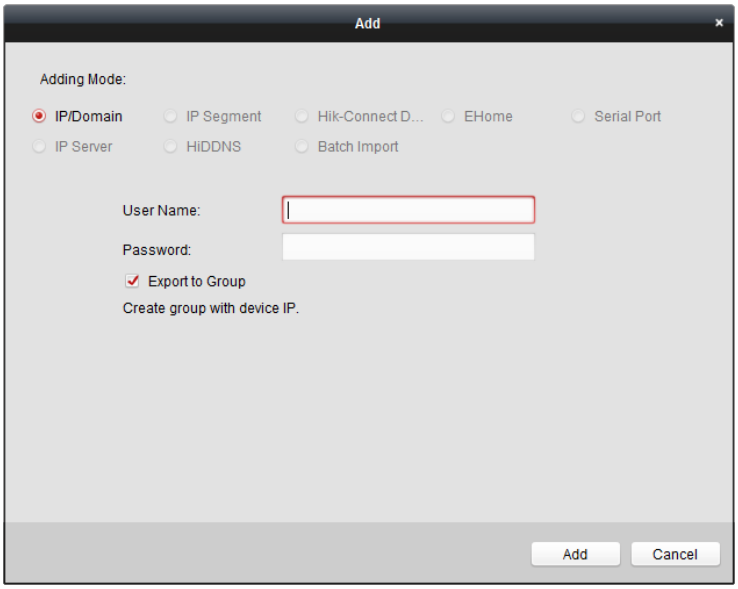


Figure 7-11: Device Addition Page

Adding Devices by IP or Domain Name

1. Click **Add** to open the device adding dialog box.
2. Select IP/Domain as the adding mode.
3. Input the required information.

Nickname: Edit a name for the device.

Address: Input the device's IP address or domain name.

Port: Input the device port number. The default value is *8000*.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all of the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

    2) Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add** to add the device.

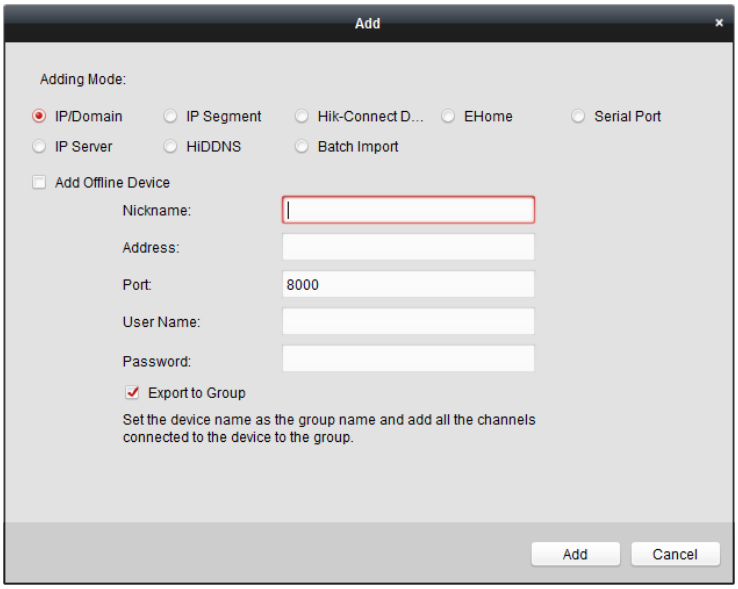


Figure 7-12: Device Addition Page

Adding Devices by IP Segment

1. Click **Add** to open the device adding dialog box.
2. Select IP Segment as the adding mode.
3. Input the required information.

Start IP: Input a start IP address.

End IP: Input an end IP address in the same network segment with the start IP.

Port: Input the device port number. The default value is *8000*.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

2) Input the required information, including the device channel number and alarm input number.

3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add**.

You can add the device which the IP address is between the start IP and end IP to the device list.

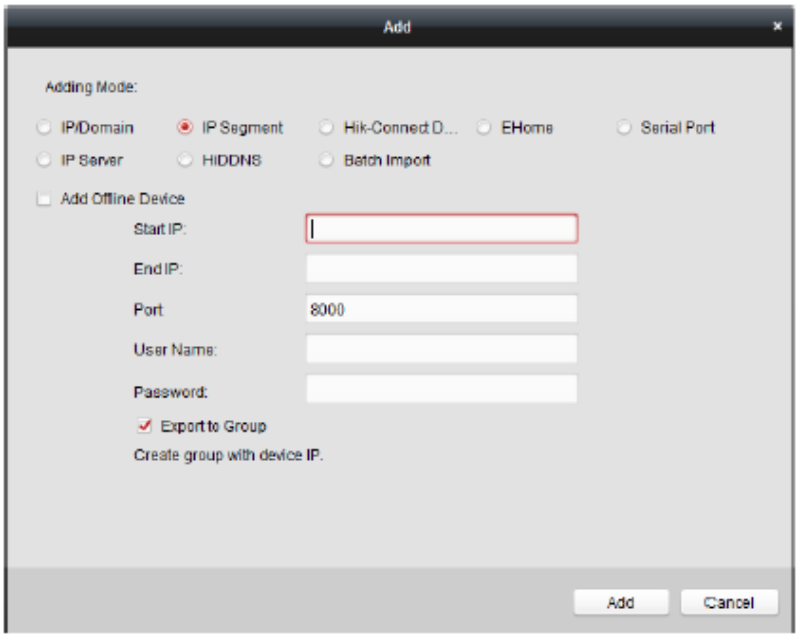


Figure 7-13: Device Addition Page

Adding Devices by Hik-Connect Domain

Purpose:
You can add the devices connected via Hik-Connect by inputting the Hik-Connect account and password.

Before you start: Add the devices to Hik-Connect account via iVMS-4200, iVMS-4500 Mobile Client, or Hik-Connect. For details about adding the devices to Hik-Connect via iVMS-4200, refer to *the iVMS-4200 Client Software User Manual.*

Add Single Device

1. Click **Add** to open the device adding dialog box.
2. Select **Hik-Connect Domain** as the adding mode.
3. Select **Single Adding**.
4. Input the required information.

Nickname: Edit a name for the device that you wish to add.

Device Serial No.: Input the device serial number.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Hik-Connect Account: Input the Hik-Connect account.

Hik-Connect Password: Input the Hik-Connect password.

5. Optionally, check the **Export to Group** checkbox to create a group by device name. You can import all the channels of the device to the corresponding group by default.

6. Click **Add** to add the device.

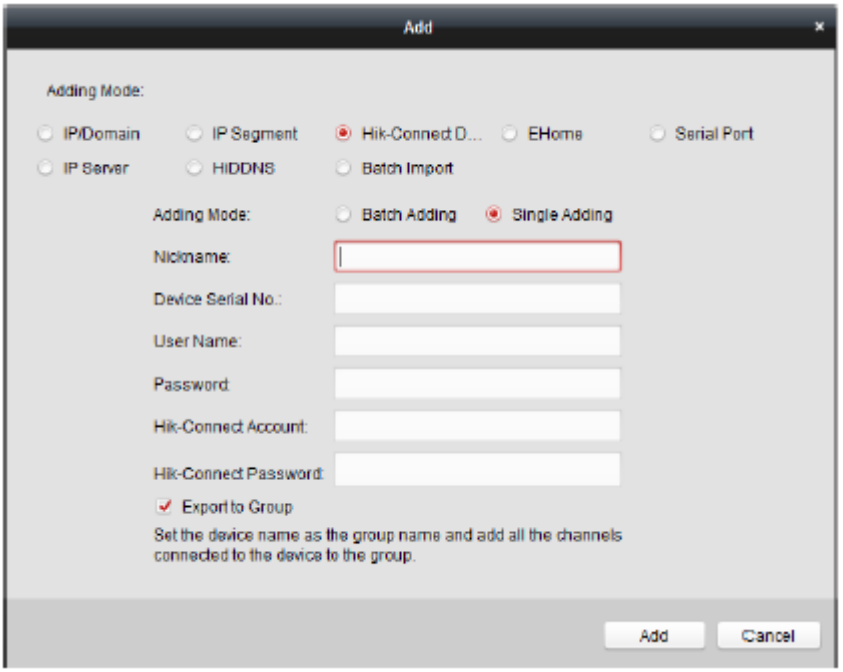


Figure 7-14: Device Addition Page

Add Devices in Batch

1. Click **Add** to open the device adding dialog box.

2. Select **Hik-Connect Domain** as the adding mode.

3. Select **Batch Adding**.

4. Input the required information.

Hik-Connect Account: Input the Hik-Connect account.

Hik-Connect Password: Input the Hik-Connect password.

5. Click **Get Device List** to show the devices added to Hik-Connect account.

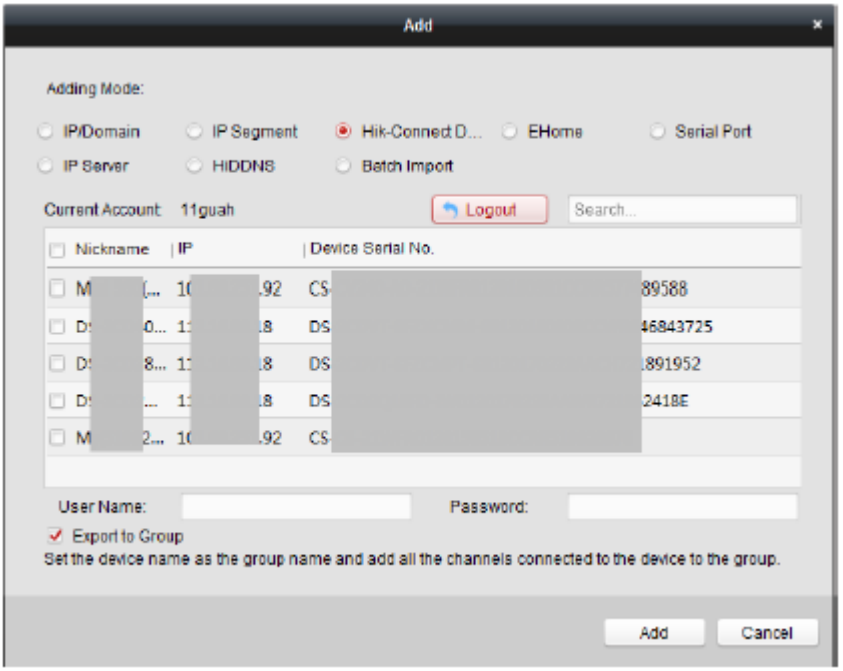


Figure 7-15: Device Addition Page

6. Check the appropriate checkbox to select the desired device.
7. Input the user name and password for the devices to be added.
8. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default.
9. Click **Add** to add the devices.

Adding Devices by EHome Account

Purpose:
You can add access control device connected via EHome protocol by inputting the EHome account.
Before you start: Set the network center parameter first. For details, refer to *Chapter 7.3.4 Network Settings.*

1. Click **Add** to open the device adding dialog box.
2. Select **EHome** as the adding mode.

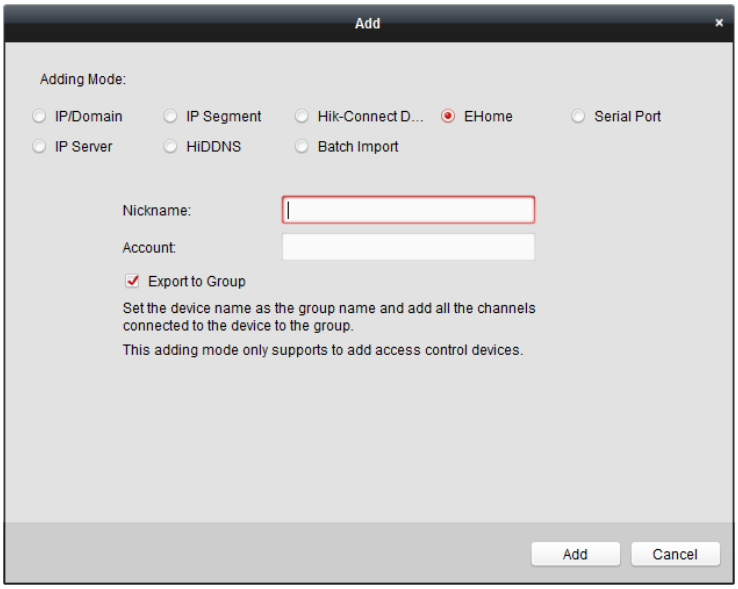


Figure 7-16: Device Addition Page

3. Input the required information.

Nickname: Edit a name for the device that you wish to add.

Account: Input the account name registered on the EHome protocol.

4. Optionally, check the **Export to Group** checkbox to create a group according to device name. You can import all the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

    2) Input the required information, including the device channel number and alarm input number.

    3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add** to add the device.

Adding Devices by Serial Port

Purpose:
You can add access control devices that are connected via a serial port.

1. Click **Add** to open the device adding dialog box.

2. Select **Serial Port** as the adding mode.

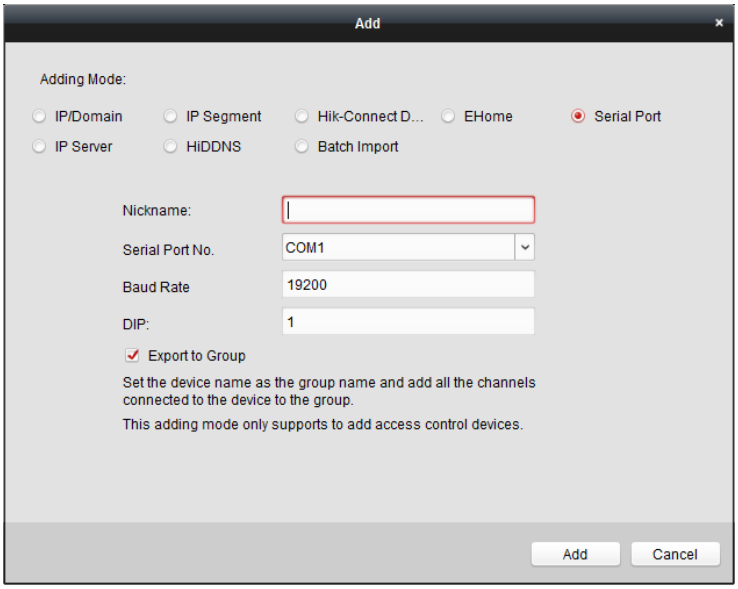


Figure 7-17: Device Addition Page

3. Input the required information.

Nickname: Edit a name for the device that you wish to add.

Serial Port No.: Select the device's connected serial port number.

Baud Rate: Input the baud rate of the access control device.

DIP: Input the DIP address of the device.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

    2) Input the required information, including the device channel number and alarm input number.

    3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add** to add the device.

Adding Devices by IP Server

1. Click **Add** to open the device adding dialog box.

2. Select **IP Server** as the adding mode.

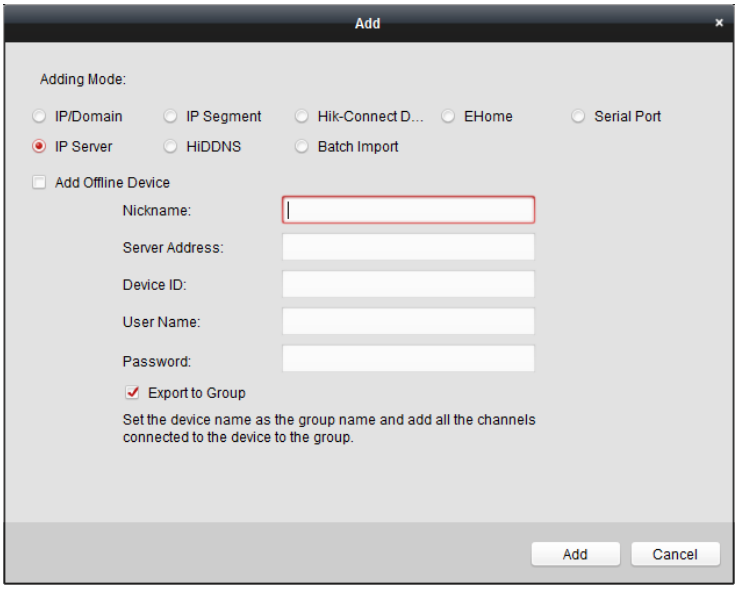


Figure 7-18: Device Addition Page

3. Input the required information.

Nickname: Edit a name for the device that you wish to add.

Server Address: Input the IP address of the PC that installs the IP Server.

Device ID: Input the device ID registered on the IP Server.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

    2) Input the required information, including the device channel number and alarm input number.

    3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add** to add the device.

Adding Devices by HiDDNS

1. Click **Add** to open the device adding dialog box.

2. Select **HiDDNS** as the adding mode.

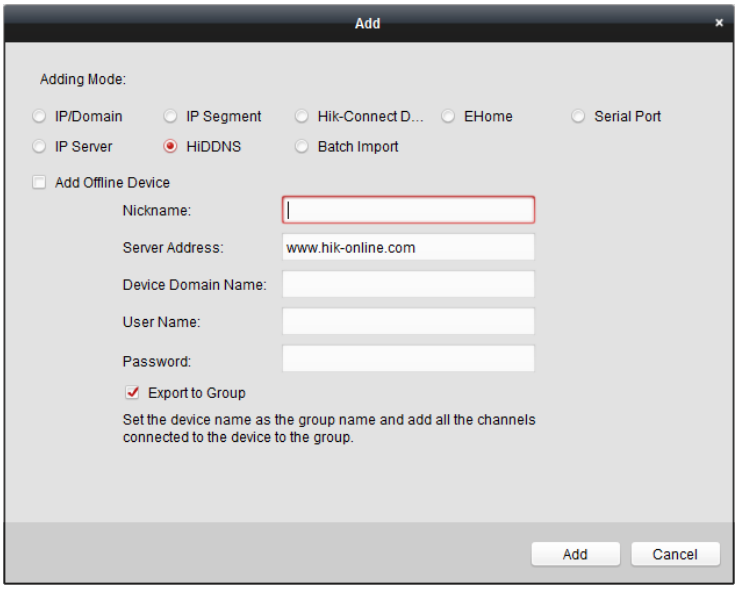


Figure 7-19: Device Addition Page

3. Input the required information.

Nickname: Edit a name for the device that you wish to add.

Server Address: *www.hik-online.com*.

Device Domain Name: Input the device domain name registered on HiDDNS server.

User Name: Input the device user name. The default user name is *admin*.

Password: Input the device password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

4. Optionally, check the **Export to Group** checkbox to create a group by the device name. You can import all the channels of the device to the corresponding group by default. ***Note:*** iVMS-4200 also provides a method to add the offline devices.

    1) Check the **Add Offline Device** checkbox.

    2) Input the required information, including the device channel number and alarm input number.

    3) Click **Add**.

When the offline device comes online, the software will connect to it automatically.

5. Click **Add** to add the device.

Importing Devices in Batch

Purpose:
The devices can be added to the software in batch by inputting the device information in the pre-defined CSV file.

1. Click **Add** to open the device adding dialog box.
2. Select **Batch Import** as the adding mode.

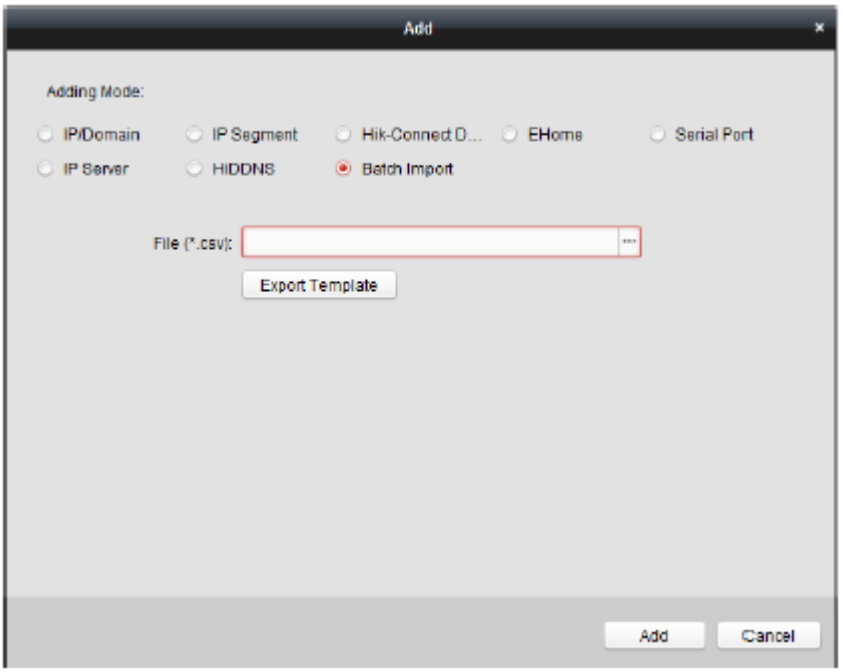


Figure 7-20: Device Addition Page

3. Click **Export Template** and save the pre-defined template (CSV file) on your PC.
4. Open the exported template file and input the required information of the devices to be added on the corresponding column.
   - **Nickname**: Edit a name for the device that you wish to add.
   - **Adding Mode**: You can input 0, 2, 3, 4, 5, or 6. Each number indicates a different adding mode. 0 indicates that the device is added by IP address or domain name; 2 indicates that the device is added via IP server; 3 indicates that the device is added via HiDDNS; 4 indicates that the device is added via EHome protocol; 5 indicates that the device is added by serial port; 6 indicates that the device is added via Hik-Connect Domain.
   - **Address**: Edit the address of the device. If you set 0 as the adding mode, you should input the IP address or domain name of the device; if you set 2 as the adding mode, you should input the IP address of the PC that installs the IP Server; if you set 3 as the adding mode, you should input www.hik-online.com.
   - **Port**: Input the device port number. The default value is 8000.
   - **Device Information**: If you set 0 as the adding mode, this field is not required; if you set 2 as the adding mode, input the device ID registered on the IP Server; if you set 3 as the adding mode, input the device domain name registered on HiDDNS server; if you set 4 as the adding mode, input the EHome account; if you set 6 as the adding mode, input the device serial number.

- **User Name**: Input the device user name. The default user name is *admin*.
- **Password**: Input the device password.

WARNING
We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

- **Add Offline Device**: You can input 1 to enable adding the offline device, and then the software will automatically connect it when the offline device comes online. 0 indicates that this function is disabled.
- **Export to Group**: You can input 1 to create a group according to device name (nickname). All the channels of the device will be imported to the corresponding group by default. 0 indicates that this function is disabled.
- **Channel Number**: If you set 1 for Add Offline Device, input the channel number of the device. If you set 0 for Add Offline Device, this field is not required.
- **Alarm Input Number**: If you set 1 for Add Offline Device, input the alarm input number of the device. If you set 0 for Add Offline Device, this field is not required.
- **Serial Port No.**: If you set 5 as the adding mode, input the serial port number for the access control device.
- **Baud Rate**: If you set 5 as the adding mode, input the baud rate of the access control device.
- **DIP**: If you set 5 as the adding mode, input the DIP address of the access control device.
- **Hik-Connect Account**: If you set 6 as the adding mode, input the Hik-Connect account.
- **Hik-Connect Password**: If you set 6 as the adding mode, input the Hik-Connect password.

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

The devices will be displayed on the device list for management after being added successfully. Check the resource usage, HDD status, recording status, and other information of the added devices on the list.

Click **Refresh All** to refresh the information of all added devices. You can also input the device name in the filter field for search.

7.3.2 Viewing Device Status

In the device list, select the device and then click **Device Status** button to view its status.

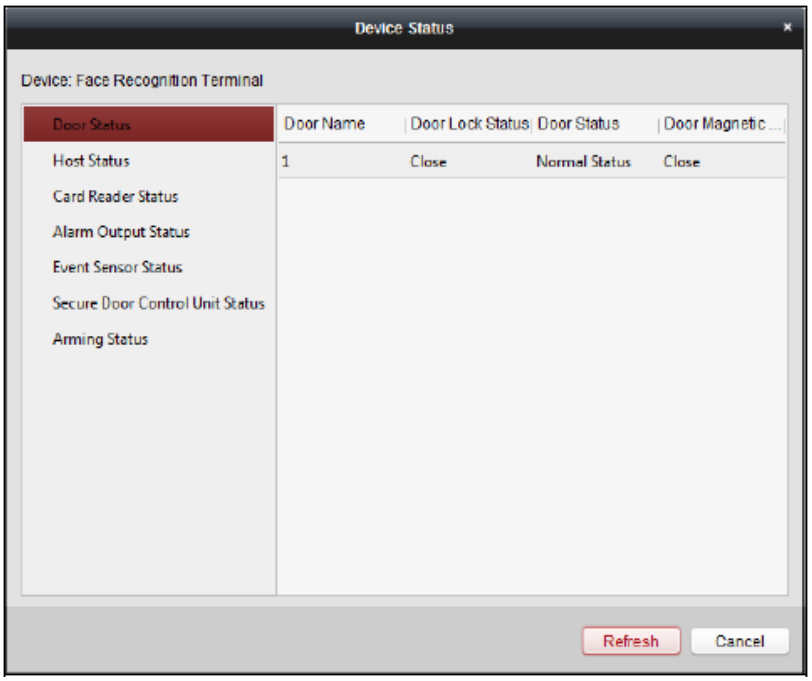


Figure 7-21: Device Status Page

Note: The interface may differ from the picture displayed above. Refer to the actual interface when adopting this function.

Door Status: Connected door status

Host Status: The status of the host, including Storage Battery Power Voltage, Device Power Supply Status, Multi-door Interlocking Status, Anti-passing Back Status, and Host Anti-Tamper Status.

Card Reader Status: Card reader status

Note: For card readers that are connected using RS-485, online or offline status can be viewed. For Wiegand connections, only offline status can be viewed.

Alarm Output Status: The alarm output status of each port

Event Sensor Status: The event sensor status of each port

Secure Door Control Unit Status: The online status and tamper status of the Secure Door Control Unit

Arming Status: Device status

7.3.3 Editing Basic Information

Purpose:
After adding the access control device, you can edit the device basic information.

1. Select the device from the device list.
2. Click **Modify** to display the modifying device information window.
3. Click **Basic Information** tab to enter the Basic Information interface.

4. Edit the device information, including the adding mode, the device name, the device IP address, port number, user name, and the password.

7.3.4 Network Settings

Purpose:
After adding the access control device, set the uploading mode, as well as the network center and wireless communication center.

Select the device in the device list, and click **Modify** to display the modifying device information window.

Click **Network Settings** tab to enter the network settings interface.

Uploading Mode Settings

Purpose:
Set the center group for uploading the log via the EHome protocol.

1. Click the **Uploading Mode** tab.

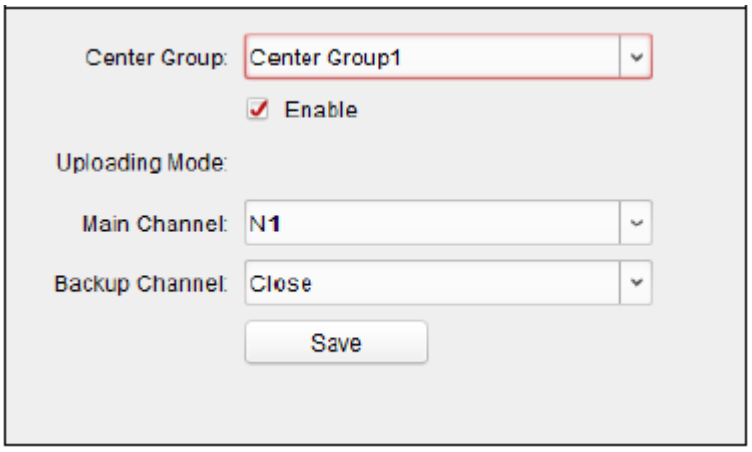


Figure 7-22: Uploading Mode Page

2. Select the center group in the dropdown list.
3. Check the **Enable** checkbox to enable the selected center group.
4. Select the uploading mode in the dropdown list. Enable **N1/G1** for the main channel and the backup channel, or 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.
5. Click **Save** button to save parameters.

Network Center Settings

Set the account for EHome protocol in Network Settings page, and add devices via the EHome protocol.

1. Click the **Network Center** tab.

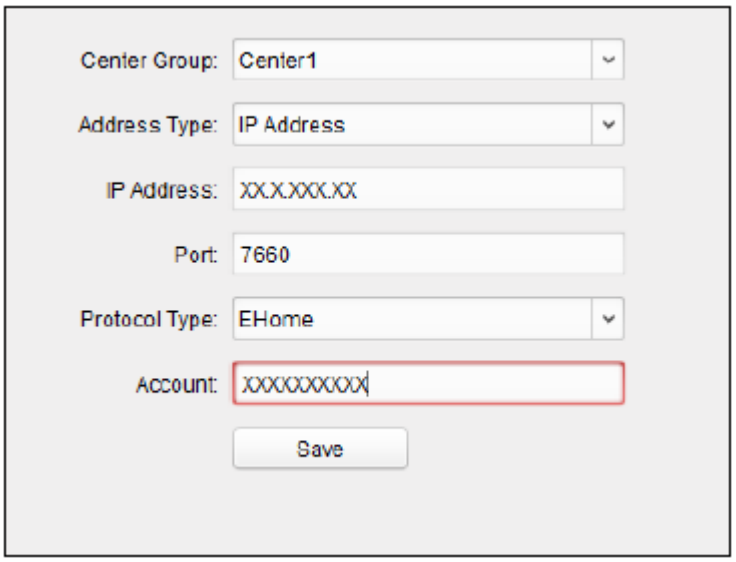


Figure 7-23: Network Settings Page

2. Select the center group in the dropdown list.
3. Select the Address Type as **IP Address** or **Domain Name.**
4. Input IP address or domain name according to the address type.
5. Input the port number for the protocol. The default port number is 7660.
6. Select the protocol type as EHome.
7. Set an account name for the network center.

Note: The account should contain 1 to 32 characters and only letters and numbers are allowed.

8. Click **Save** button to save parameters.

Notes:

- The port No. of the wireless network and wired network should be consistent with the port No. of EHome.
- Set the domain name in Enable NTP area *Editing Time* section in Remote Configuration. For details, refer to *Time* in *7.3.8 Remote Configuration*.

Wireless Communication Center Settings

1. Click the **Wireless Communication Center** tab.

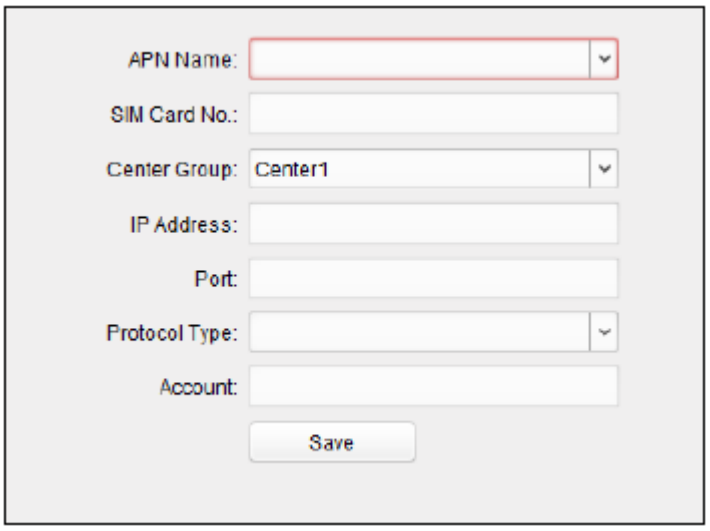


Figure 7-24: Network Settings Page

2. Select the APN name as CMNET or UNINET.
3. Input the SIM Card number.
4. Select the center group in the dropdown list.
5. Input the IP address and port number.
6. Select the protocol type as EHome. By default, the port number for EHome is 7660.
7. Set an account name for the network center. A consistent account should be used in one platform.
8. Click **Save** button to save parameters.

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

7.3.5 Capture Settings

Set the capture linkage and manual capture parameters.

Select the device in the device list, and click **Modify** to display the modifying device information window.

Click **Capture Settings** tab to enter the capture settings interface.

Notes:

- The **Capture Settings** should be supported by the device.
- Before setting the capture setting, configure the storage server for picture storage.

Linked Capture

1. Select the **Linked Capture** tab.
2. Set the picture size and quality.
3. Set the linked capture times once triggered.

4. Set the capture interval according to the capture times.
5. Click **Save** to save the settings.

Manual Capture

1. Select the **Manual Capture** tab.

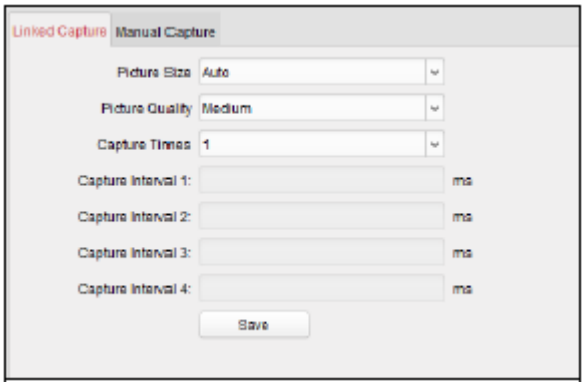


Figure 7-25: Linked Capture Page

2. Select the resolution of the captured pictures from the dropdown list.
3. Select the picture quality as **High**, **Medium**, or **Low**.
4. Click **Save** to save the settings.
5. You can click **Restore Default Value** to restore the parameters to default settings.

7.3.6 RS-485 Settings

Purpose:
Set the RS-485 parameters including the serial port, the baud rate, the data bit, the stop bit, the parity type, the communication mode, the working mode, and the connection mode.

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

1. Select the device in the device list, and click **Modify** to display the modifying device information window.
2. Click **RS-485 Settings** tab to enter the RS-485 settings interface.

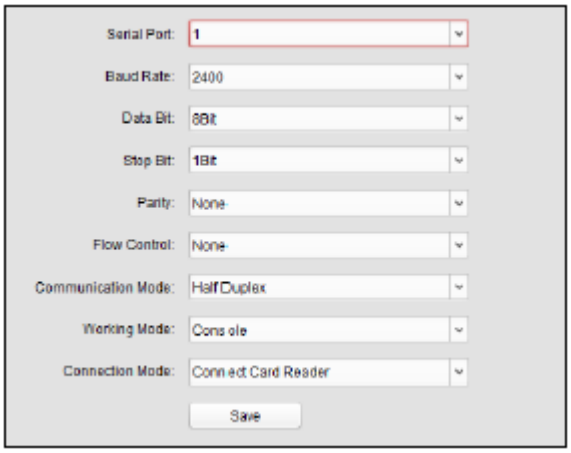


Figure 7-26: RS-485 Settings Page

3. Select the serial number of the port from the dropdown list to set the RS-485 parameters.

4. Set the baud rate, data bit, the stop bit, parity, flow control, communication mode, working mode, and the connection mode in the dropdown list.

5. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the working mode, the device will be rebooted. A prompt will be displayed after changing the working mode.

7.3.7 Wiegand Settings

Purpose:
Set the Wiegand channel and the communication mode. ***Note:*** The Wiegand Settings should be supported by the device.

1. Select the device in the device list, and click **Modify** to display the modifying device information window.

2. Click the **Wiegand Settings** tab to enter the Wiegand Settings interface.

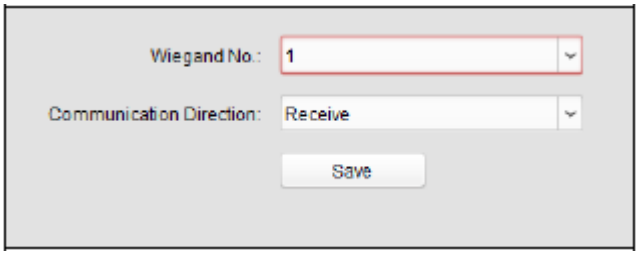


Figure 7-27: Wiegand Settings Page

3. Select the Wiegand channel number and the communication mode in the dropdown list.

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

4. Click **Save** to save the settings and the configured parameters will be applied to the device automatically.

Note: After changing the communication direction, the device will be rebooted. A prompt will be displayed after changing the communication direction.

7.3.8 Remote Configuration

Purpose:
In the device list, select the device and click **Remote Configuration** button to enter the remote configuration interface. Set the detailed parameters of the selected device.

Checking Device Information

1. In the device list, you can click **Remote Configuration** to enter the remote configuration interface.

2. Click **System** -> **Device Information** to check the device basic information and the device version information.

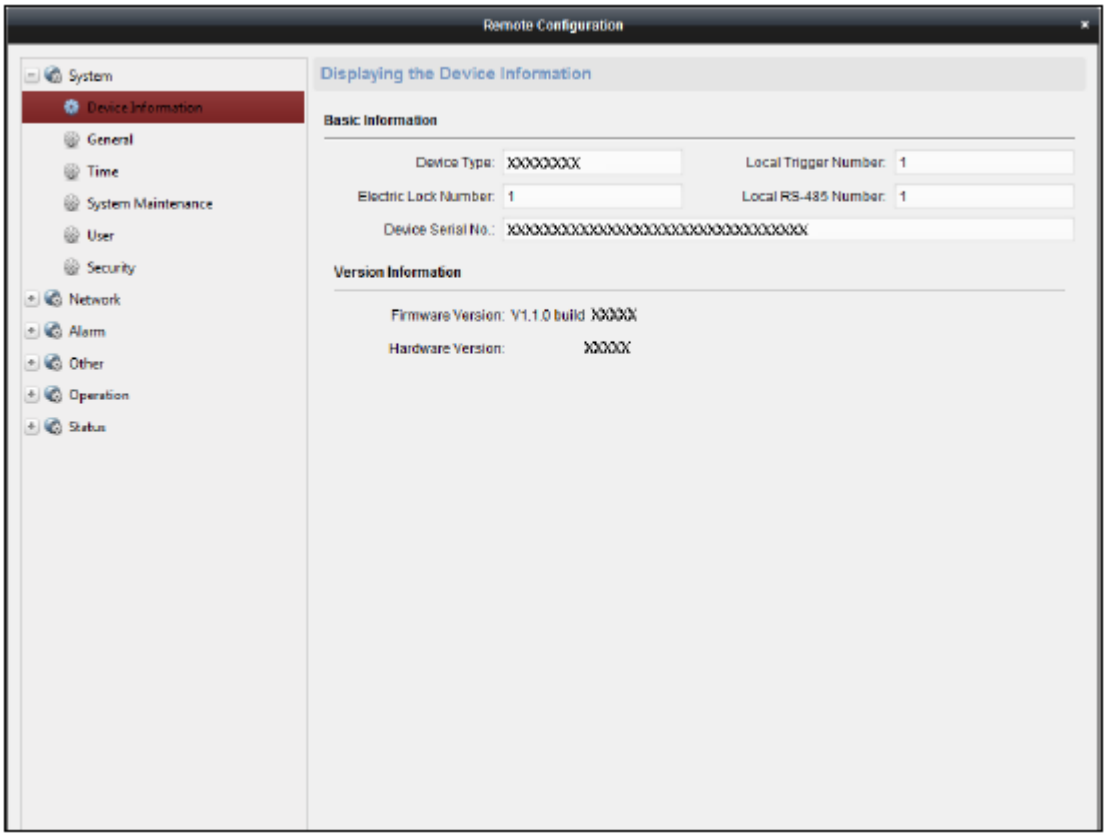


Figure 7-28: Remote Configuration Page

Editing Device Name

In the Remote Configuration interface, click **System** -> **General** to configure the device name and overwrite record files parameter. Click **Save** to save the settings.

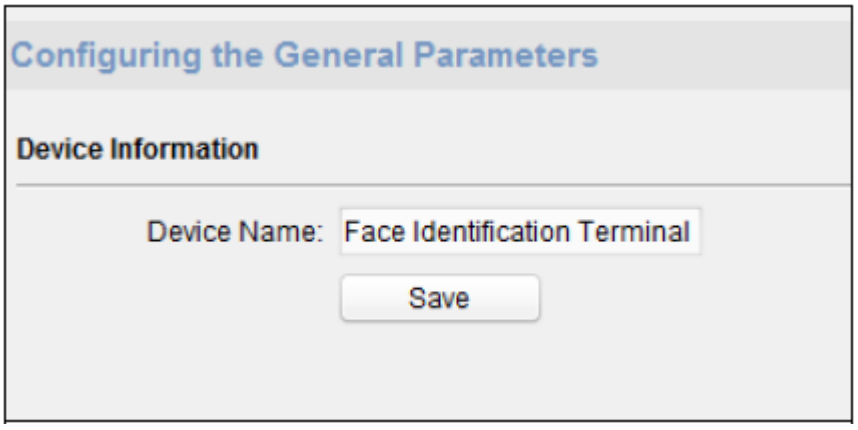


Figure 7-29: Remote Configuration Page

Editing Time

1. In the Remote Configuration interface, click **System** -> **Time** to configure the time zone.
2. (Optional) Check **Enable NTP** and configure the NTP server address, the NTP port, and the synchronization interval.
3. (Optional) Check **Enable DST** and configure the DST star time, end time and the bias.
4. Click **Save** to save the settings.

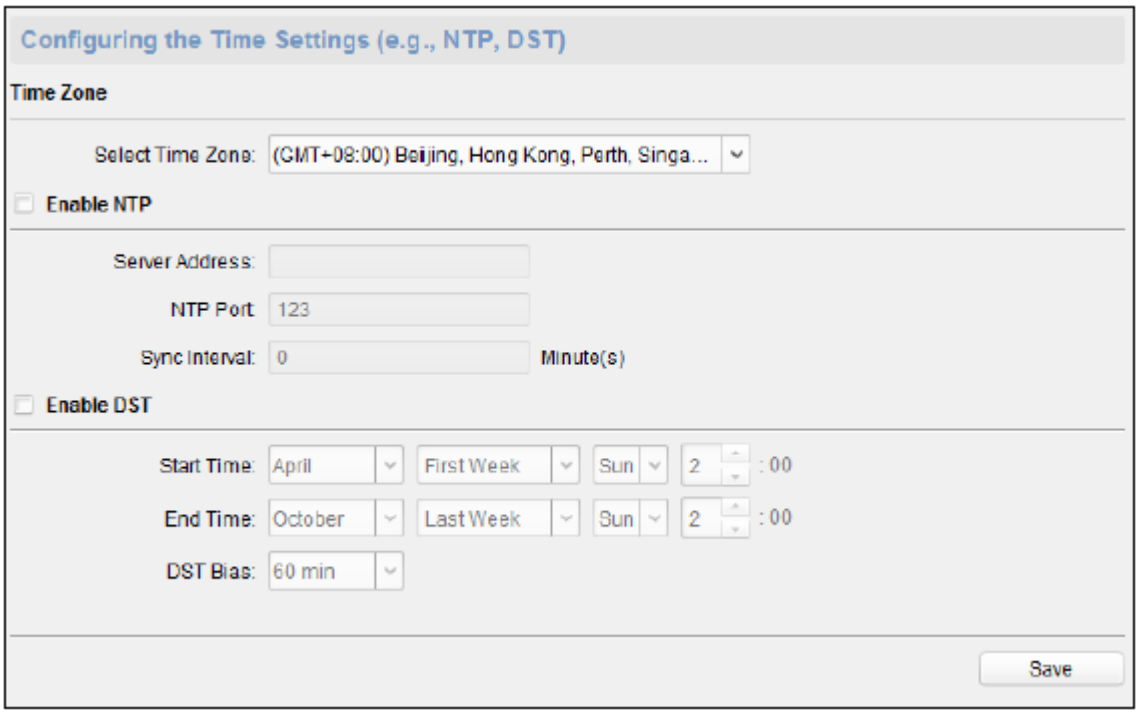


Figure 7-30: Time Settings Configuration Page

Setting System Maintenance

Purpose:
Reboot the device remotely, restore the device to default settings, import configuration file, upgrade the device, etc.

1. In the Remote Configuration interface, click **System** -> **System Maintenance**.
2. Click **Reboot** to reboot the device.

   Or, click **Restore Default Settings** to restore the device settings to the default ones, excluding the IP address.

   Or, click **Restore All** to restore the device parameters to the default ones. The device should be activated after restoring.

   Note: The configuration file contains the device parameters.

   Or, click **Import Configuration File** to import the configuration file from the local PC to the device.

   Or, click **Export Configuration File** to export the configuration file from the device to the local PC

   Note: The configuration file contains the device parameters.
3. You can also remote upgrade the device.
   1) In the Remote Upgrade part, click ··· to select the upgrade file.
   2) Click **Upgrade** to start upgrading.

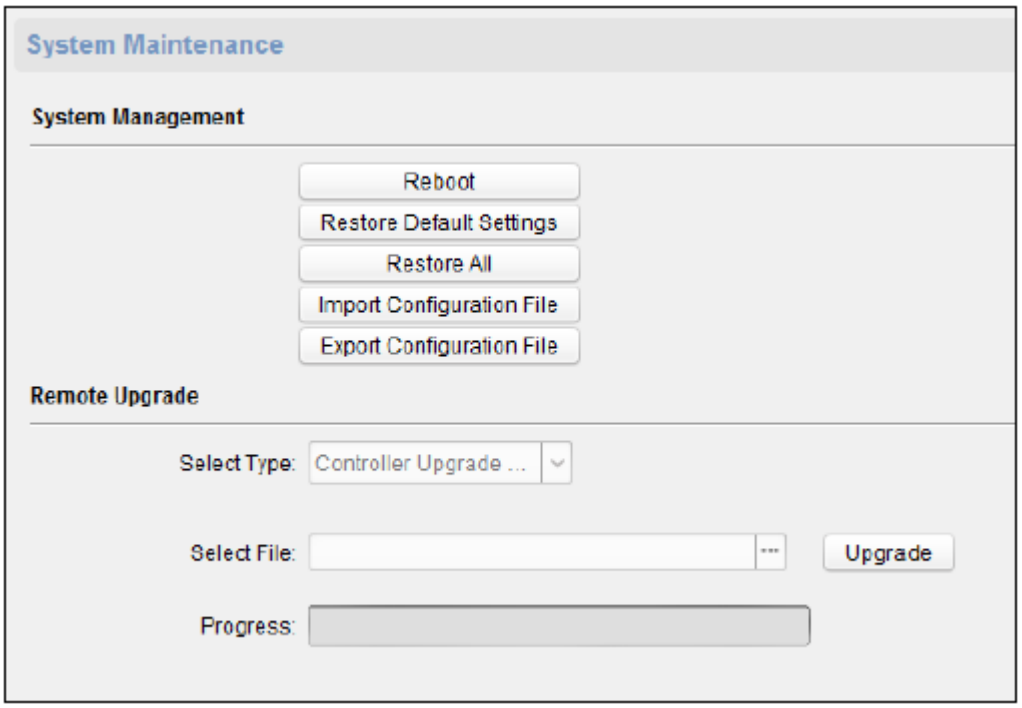


Figure 7-31: Time Settings Configuration Page

Managing User

1. In the Remote Configuration interface, click **System** -> **User**.
2. Click **Add** to add the user (not supported by the elevator controller).

Otherwise, select a user in the user list and click **Edit** to edit the user. Edit the user password, the IP address, the MAC address and the user permission. Click **OK** to confirm editing.

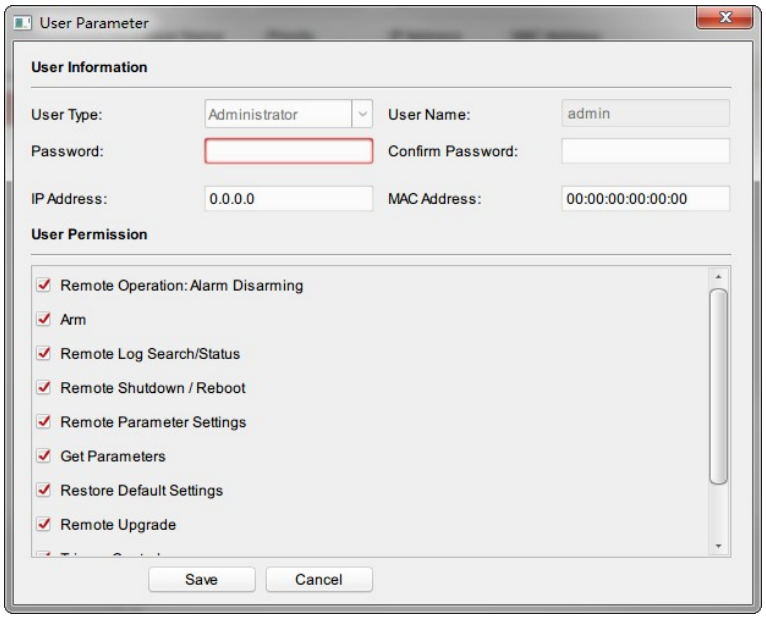


Figure 7-32: User Management Page

Setting Security

3. Click **System** -> **Security**.

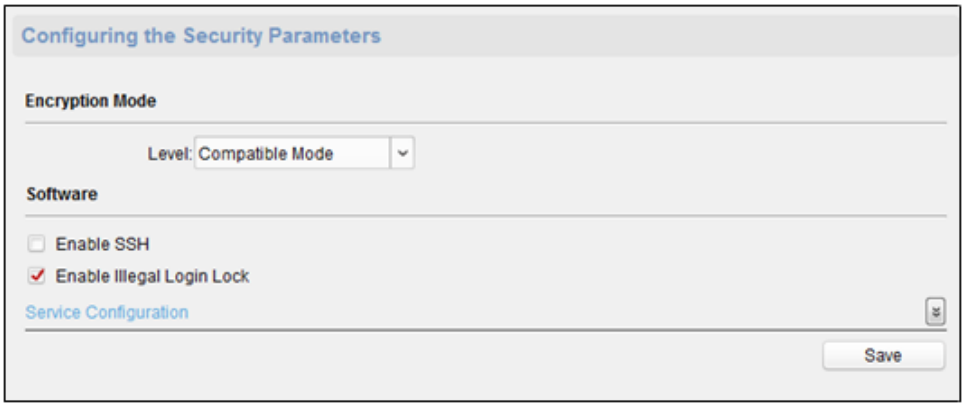


Figure 7-33: Security Parameter Configuration Page

4. Select the encryption mode in the dropdown list.

You can select **Compatible Mode** or **Encryption Mode**.

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

Configuring Network Parameters

Click **Network** -> **General**. Configure the NIC type, the IPv4 address, the subnet mask (IPv4), the default gateway (IPv4), MTU address, MTU, and the device port. Click **Save** to save the settings.

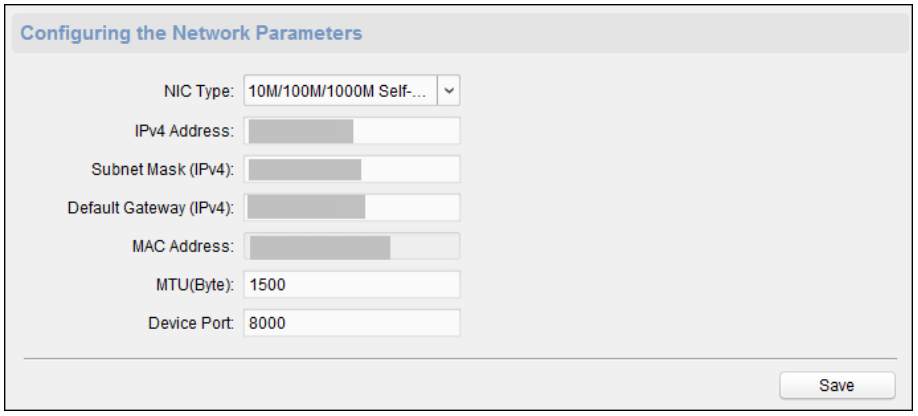


Figure 7-34: Network Parameter Configuration Page

Configuring Upload Method

Purpose:
Set the center group for uploading the log via the EHome protocol.

1. Click **Network** -> **Report Strategy**.

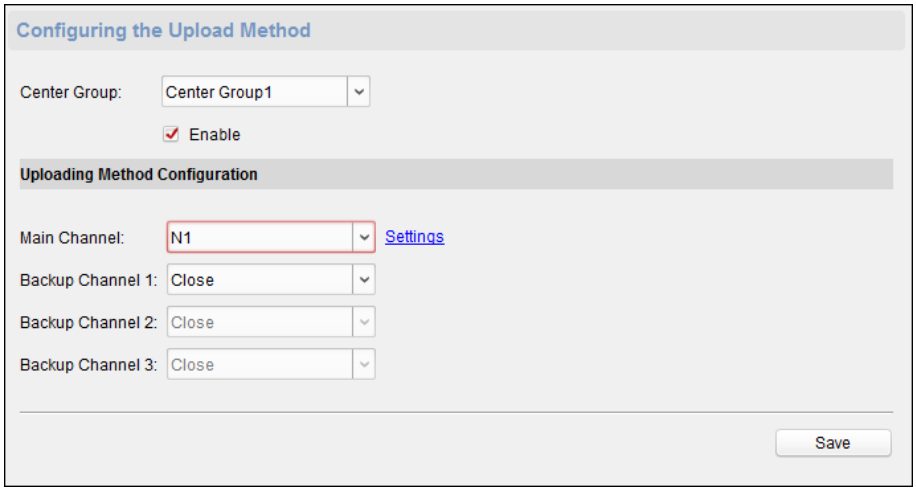


Figure 7-35: Upload Method Configuration Page

2. Select a Center Group from the drop-down list.
3. Check the **Enable** check box.
4. Set the uploading method.

Set the main channel and the backup channel.

5. Click **Settings** on the right of the channel field to set the detailed information.
6. Click **Save** to save the settings.

Configuring Network Center

Set the notify surveillance center, center IP address, the port number, the Protocol (EHome), and the EHome account user name to transmit data via EHome protocol. For details about EHome protocol's transmission, refer to *Network Center Settings* in *Chapter 7.3.4 Network Settings.* Click **Save** to save the settings.

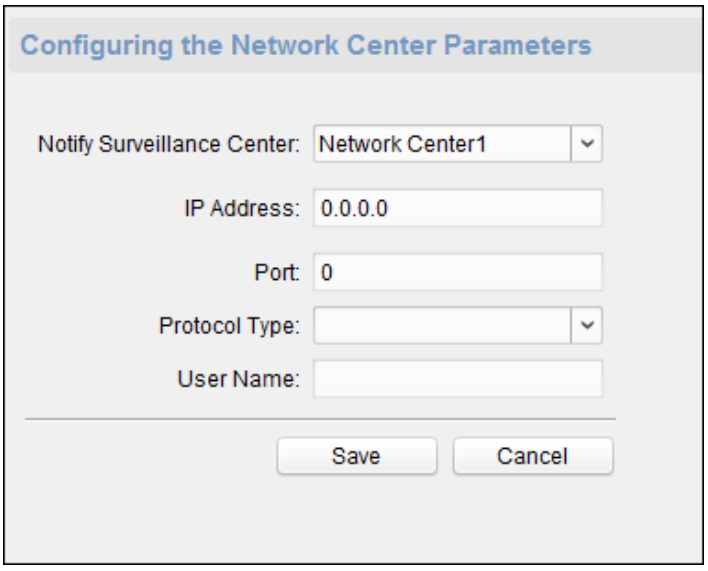


Figure 7-36: Network Center Configuration Page

Configuring Advanced Network

Click **Network** -> **Advanced Settings**. You can configure the DNS IP address 1, the DNS IP address 2, the

security control platform IP, and the security control platform port. Click **Save** to save the settings.

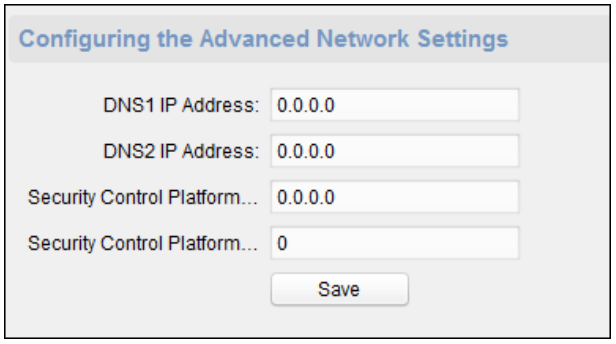


Figure 7-37: Advanced Network Configuration Page

Configuring Wi-Fi

1. Click **Network** –> **Wi-Fi**.

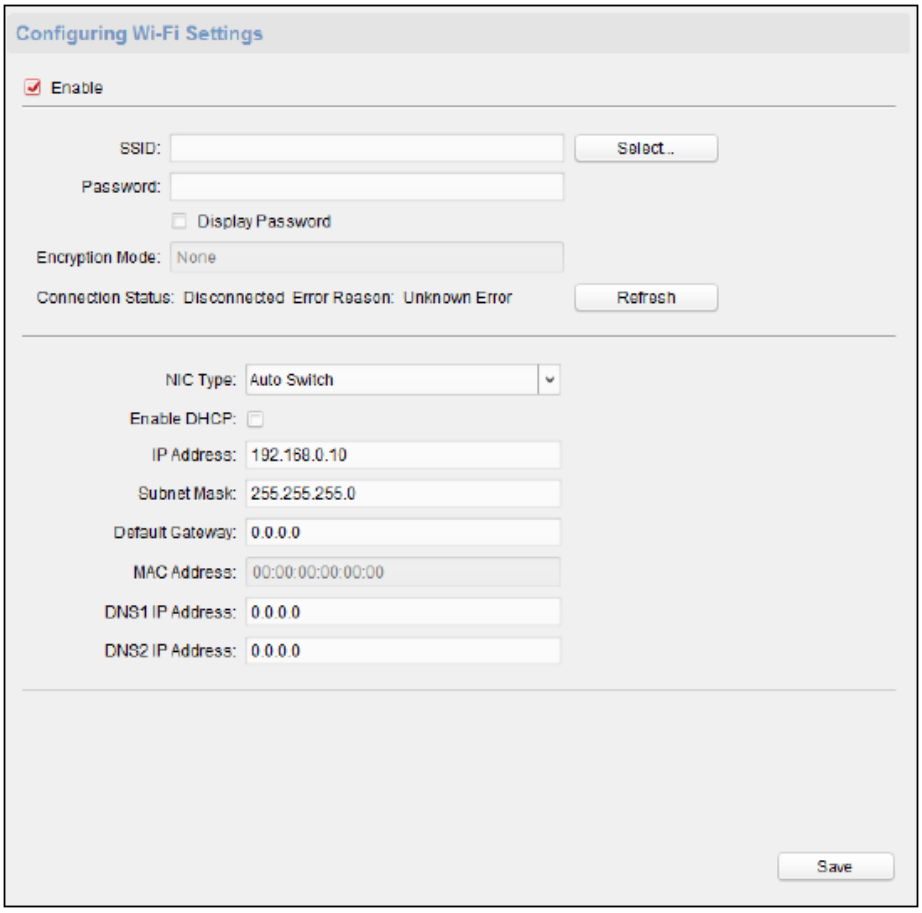


Figure 7-38: Wi-Fi Settings Configuration Page

2. Check **Enable** to enable the Wi-Fi function.
3. Input the hot spot name.

Or you can click **Select...** to select a network.

4. Input the Wi-Fi password.
5. (Optional) Click **Refresh** to refresh the network status.
6. (Optional) Select the NIC Type.

7. (Optional) Select to uncheck **Enable DHCP** and set the IP address, the subnet mask, the default gateway, the MAC address, the DNS1 IP Address, and the DNS2 IP address.

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

Configuring Relay Parameters

1. Click **Alarm** -> **Relay**.

View the relay parameters.

Figure 7-39: Relay Parameters Configuration Page

2. Click the  to display the Relay Parameters Settings window.

3. Set the relay name and the output delay.

4. Click **Save** to save the parameters.

Otherwise, click **Copy to...** to copy the relay information to other relays.

Configuring Access Control Parameters

1. In the Remote Configuration interface, click **Other** -> **Access Control Parameters**.

2. Select and check the desired item.

   - **Overlay User Information on Picture:** Display the user information on the captured picture.
   - **Enable Voice Prompt:** If the checkbox has been selected, the voice prompt is enabled on the device. A voice prompt will be made when operating the device.
   - **Upload Pictures after Capturing:** If the checkbox has been selected, the pictures captured by the linked camera will be uploaded to the system automatically.
   - **Save Captured Pictures:** If the checkbox has been selected, the picture captured by linked camera can be saved to the device. You can view the picture in *7.9 Searching Access Control Event*.

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

Uploading Background Picture

Click **Other** -> **Picture Upload**. Click  to select a local picture. You can also click **Preview** to preview the picture. Click **Upload** to upload the picture.

Note: The function must be supported by the device.

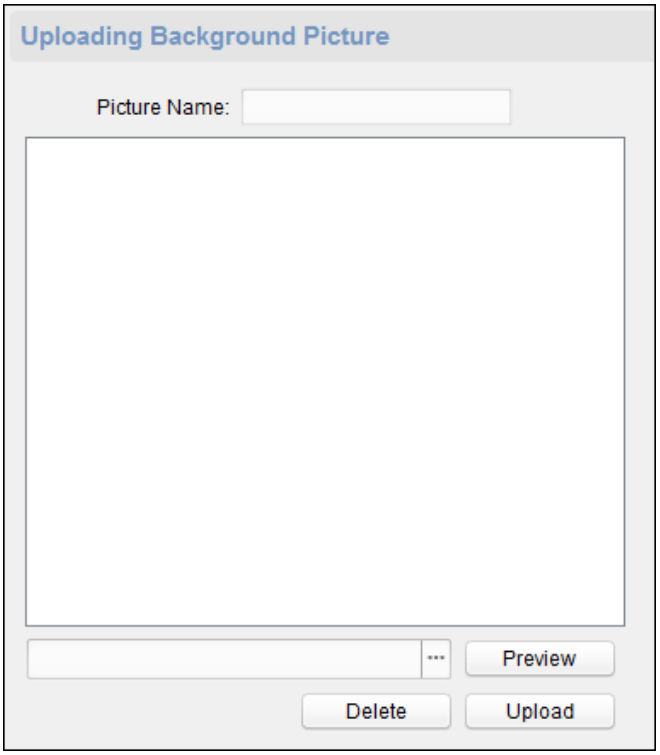


Figure 7-40: Background Picture Upload Interface

Configuring Face Detection Parameters

Click **Other** -> **Face Detection**. You can check the **Enable** checkbox to enable the device face detection function.

After enabling the function, the device should detect the face while authenticating. Otherwise, authentication will fail.

Note: Only devices with video function support this function.

Figure 7-41: Enable Face Detection Parameter Page

Operating Relay

1. Click **Operation** -> **Relay**.

View the relay status.

2. Check the relay checkbox
3. Click **Open** or **Close** to open/close the relay.
4. (Optional) Click **Refresh** to refresh the relay status.

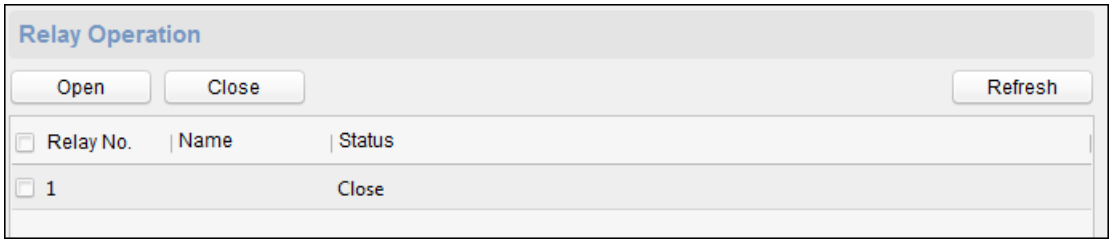


Figure 7-42: Relay Operation Page

Viewing Relay Status

Click **Status** -> **Relay** to view the relay status.

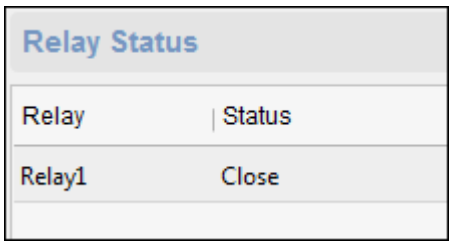


Figure 7-43: Relay Status Page

7.4 Organization Management

Add, edit, or delete the organization, as desired.

Click  tab to enter the Person and Card Management interface.

7.4.1 Adding Organization

1. In the organization list on the left, add a top organization as the parent organization of all organizations.

Click **Add** button to display the adding organization interface.

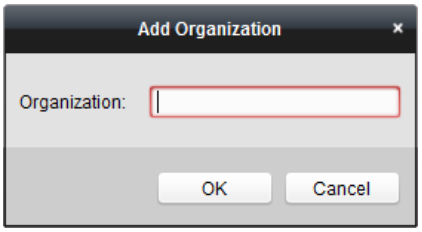


Figure 7-44: Add Organization Page

2. Input the Organization Name as desired.
3. Click **OK** to save the adding.
4. Add multiple levels of organizations according to the actual needs. To add sub organizations, select the parent organization and click **Add**. Repeat *Step 2* and *3* to add the sub organization.

Then the added organization will be the sub-organization of the upper-level organization.

Note: Up to 10 levels of organizations can be created.

7.4.2 Modifying and Deleting Organization

Select the added organization and click **Modify** to modify its name. Select an organization, and click **Delete** button to delete it.

Notes:
Lower-level organizations will also be deleted if you delete an organization.

Make sure there is no person added under the organization, otherwise the organization cannot be deleted.

7.5 Person Management

After adding the organization, add the person to the organization and manage the added person options, such as issuing cards in batch, importing and exporting person information in batch, etc.

Note: Up to 10,000 persons or cards can be added.

7.5.1 Adding Person

Adding Person (Basic Information)

1. Select an organization in the organization list and click **Add** button on the Person panel to display the adding person dialog box.

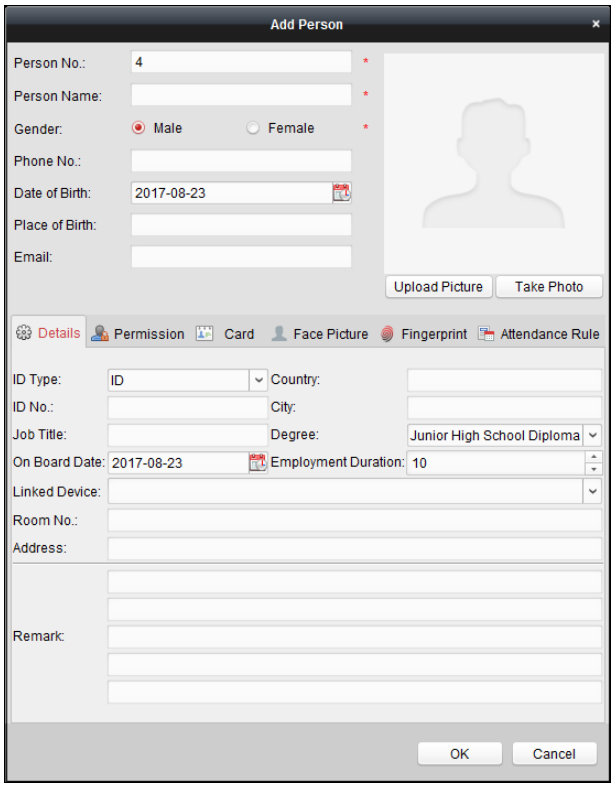


Figure 7-45: Add Person Box

2. The **Person No.** will be generated automatically and is not editable.

3. Input the basic information, including person name, gender, phone No., birthday details, and email address.

4. Click **Upload Picture** to select the person picture from the local PC to upload it to the client.

Note: The picture should be in *.jpg format.

5. (Optional) Click **Take Phone** to capture the person's photo with the PC camera.
6. Click **OK** to finish adding.

Adding Person (Detailed Information)

1. In the Add Person interface, click **Details** tab.

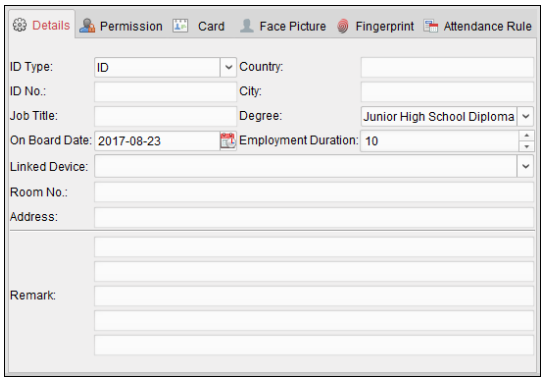


Figure 7-46: Person Details Page

2. Input the detailed information of the person, including person's ID type, ID No., country, etc., according to actual needs.

   - **Linked Device:** Bind the indoor station to the person.

Note: If **Analog Indoor Station** is selected as a Linked Device, the **Door Station** field will display, and the door station will have to be selected to communicate with the analog indoor station.

   - **Room No.:** Input the room No. of the person.

3. Click **OK** to save the settings.

Adding Person (Permission)

Assign the (including operation permissions of access control device and access control permissions) to the person when adding the person.

Note: For setting the access control permission, refer to *Chapter 7.7 Permission Configuration.*

1. In the Add Person interface, click the **Permission** tab.

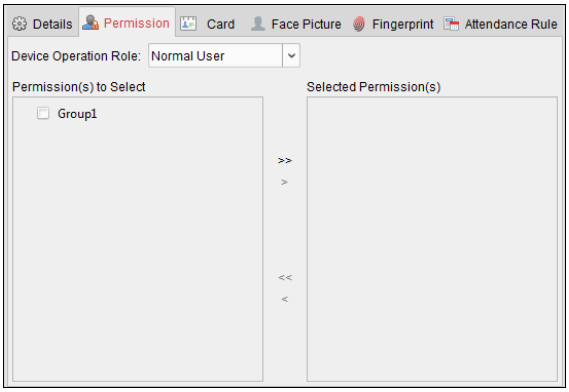


Figure 7-47: Permissions Details Page

2. In the Device Operation Role field, select the role of operating the access control device. **Normal User:** The person has the permission to check-in/out on the device, pass the access control point, etc.

   Administrator: The person has the normal user permission, as well as permission to configure the device, including adding normal user, etc.

3. In the Permission(s) to Select list, all the configured permissions display.

   Check the permission checkbox and click **>** to add to the Selected Permission list. (Optional) Click **>>** to add all the displayed permissions to the Selected Permission list.

   (Optional) In the Selected Permission list, select the selected permission and click **<** to remove it. You can also click **<<** to remove all the selected permissions.

4. Click **OK** to save the settings.

Adding Person (Card)

Add a card and issue the card to the person.

Adding General Card

1. In the Add Person interface, click **Card** tab.

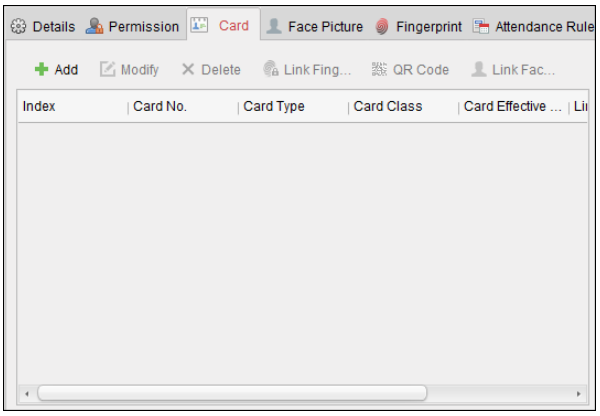


Figure 7-48: Add Card Page

2. Click **Add** to display the Add Card dialog box.

3. Click **Card** to enter the Card tab.

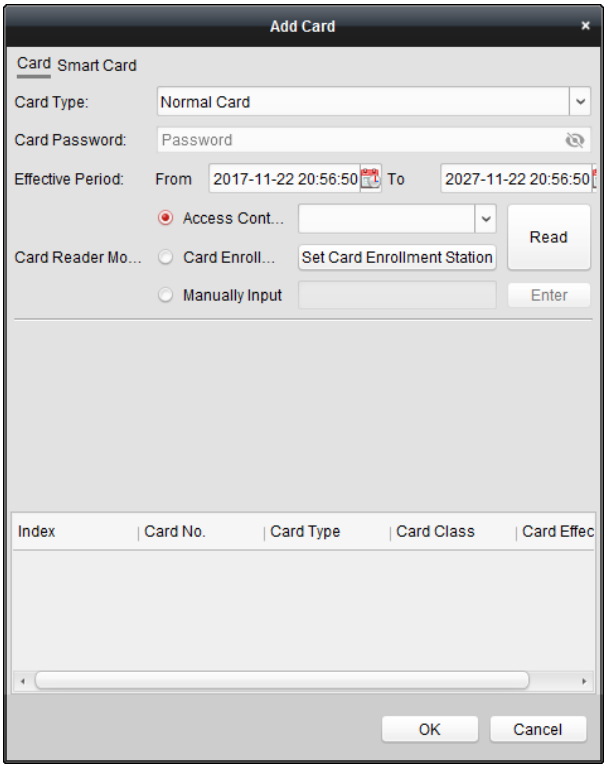


Figure 7-48: Card Details Box

4. Select the card type according to actual needs.

   - **Normal Card**
   - **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
   - **Card in Blacklist**: The card swiping action will be uploaded and the door cannot be opened.
   - **Patrol Card**: The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
   - **Duress Card**: The door can open by swiping the duress card when there is a duress situation. At the same time, the client can report a duress event.
   - **Super Card**: The card is valid for all the doors of the controller during the configured schedule.
   - **Visitor Card**: The card is assigned for visitors. For the Visitor Card, set the **Max. Swipe Times**.

Note: The Max. Swipe Times should be between 0 and 255. When setting 0, card swiping is unlimited.

5. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

Note: The password will be required when the card holder swiping the card to get enter to or exit from the door if you enable the card reader authentication mode as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For details, *Chapter 7.8.2 Card Reader Authentication.*

6. Click to set the effective time and expiry time of the card.

7. Select the Card Reader Mode for reading the card number.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card number.
- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card number.

Note: The Card Enrollment Station should connect with the PC running the client. Click **Set Card Enrollment Station** to enter the following dialog box.

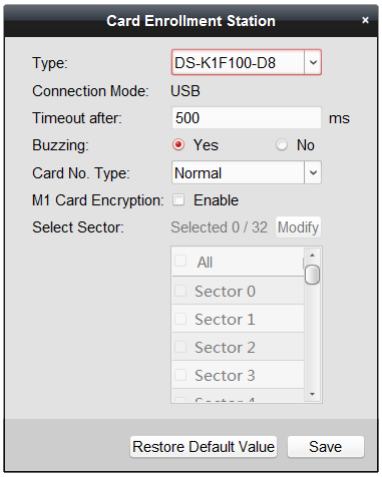


Figure 7-49: Card Enrollment Box

1) Select the Card Enrollment Station type.

Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

2) Set the serial port No., the baud rate, the timeout value, the buzzing, or the card No. type.

   If the card is M1 card, and the M1 Card Encryption function must be enabled, check **Enable** checkbox of M1 Card Encryption and click **Modify** to select the sector.

3) Click **Save** button to save the settings.

   Click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card number and click **Enter** to input the card number.

8. Click **OK** and the card will be issued to the person.
9. (Optional) Select the added card and click **Modify** or **Delete** to edit or delete the card.
10. (Optional) Generate and save the card QR code for QR code authentication.

    1) Select an added card and click **QR Code** to generate the card QR code.

    2) In the QR code pop-up window, click **Download** to save the QR code to the local PC. Print the QR code for authentication on the specified device.

Note: The device should support the QR code authentication function. For details about setting the QR code authentication function, see the user manual for the specific device.

11. (Optional) Click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping card when passing the door.

12. (Optional) Click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping card when passing the door.

13. Click **OK** to save the settings.

Adding Smart Card

Purpose:
Store fingerprints and ID card information in the smart card. When authenticating, after swiping the smart card on the device, scan your fingerprint or swipe your ID card on the device. The device will compare the fingerprint or ID card information in the smart card with the ones that have been collected. If a smart card is used for authentication, there is no need to store the fingerprints or ID card information in the device in advance.

1. In the Add Person page, set the person basic information.
2. Click **Card** to enter the card tab.
3. Click **Add** to display the Add Card dialog box.
4. Click **Smart Card** to enter the Smart Card tab.

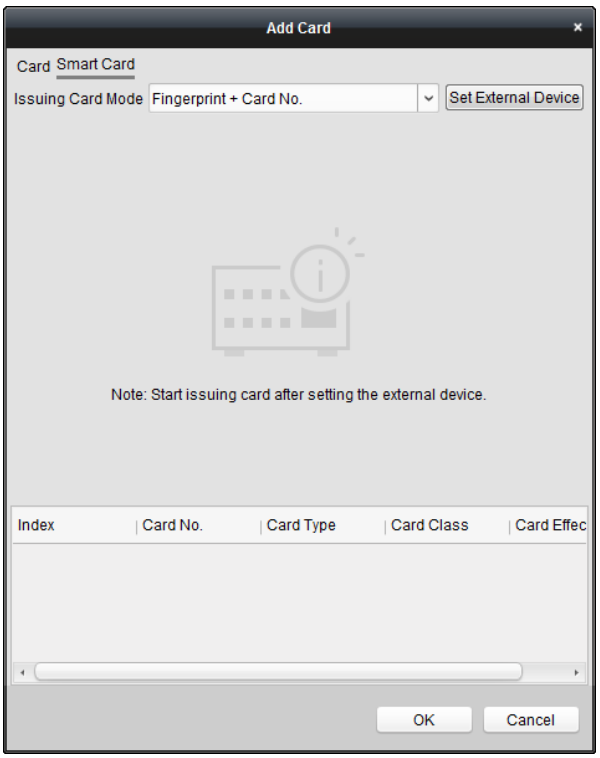


Figure 7-50: Add Smart Box

5. Select an issuing card mode from the dropdown list.
6. Set the external device.
    1) Click **Set External Device** to enter the Set External Device page.
    2) (Optional) Select the issuing card mode again.
    3) Set a card enrollment station.
    4) If "Fingerprint + Card No." is selected as the issuing mode, set the fingerprint recorder model.

If "ID Card No. + Card No." is selected as the issuing mode, set the ID card reader model.

If "Fingerprint + ID Card No. + Card No." is selected as the issuing mode, set the fingerprint recorder model and the ID card reader model.

5) Click **OK** save the settings.

7. Select a card type for the smart card.

- **Normal Card**
- **Card for Disabled Person**: The door will remain open for the configured time period for the card holder.
- **Card in Blacklist:** The card swiping action will be uploaded and the door cannot be opened.
- **Patrol Card:** The card swiping action can be used for checking the working status of the inspection staff. The access permission of the inspection staff is configurable.
- **Duress Card:** The door can open by swiping the duress card when there is duress. At the same time, the client can report the duress event.
- **Super Card:** The card is valid for all the doors of the controller during the configured schedule.
- **Visitor Card:** The card is assigned for visitors. For the Visitor Card, set the Max. Swipe Times.

Note: The Max. Swipe Times should be between 0 and 255. When this value is set to 0, card swiping is unlimited.

- **Dismiss Card:** Swipe the card to dismiss the alarm.

8. Set other parameters of the card.

1) Set the card password.

2) Set the card effective date.

3) Scan your fingerprint and swipe your ID card according to the prompt.

4) Swipe the smart card.

The added card information will display in the list below.

9. Click **OK** and the card(s) will be issued to the person.

10. (Optional) Select the added card and click **Modify** or **Delete** to edit or delete the card.

11. (Optional) Generate and save the card QR code for QR code authentication.

1) Select an added card and click **QR Code** to generate the card QR code.

2) In the QR code pop-up window, click **Download** to save the QR code to the local PC. You can print the QR code for authentication on the specified device.

Note: The device should support QR code authentication functionality. For details about setting the QR code authentication function, see the specified device user manual.

12. (Optional) Click **Link Fingerprint** to link the card with the person's fingerprint, so that the person can place the finger on the scanner instead of swiping the card when passing the door.

13. (Optional) Click **Link Face Picture** to link the card with the face picture, so that the person can pass the door by scanning the face via the device instead of swiping the card when passing the door.

14. Click **OK** to save the settings.

Adding Person (Fingerprint)

1. In the Add Person interface, click **Fingerprint** tab.

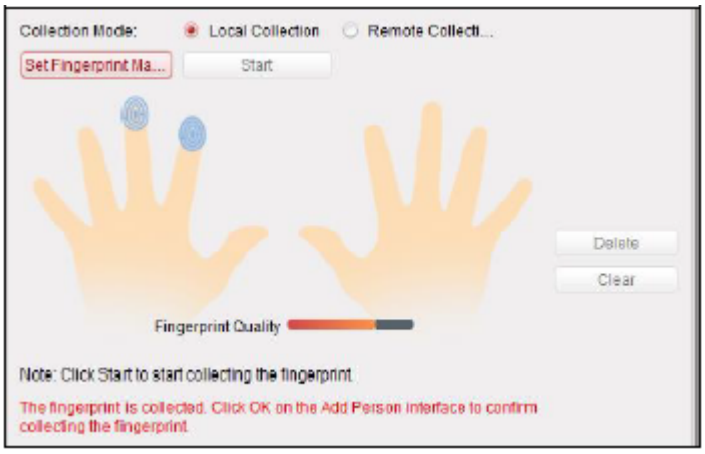


Figure 7-51: Add Fingerprint Page

2. Select **Local Collection** as desired.

3. Before inputting the fingerprint, connect the fingerprint machine to the PC and set its parameters first.

   Click **Set Fingerprint Machine** to enter the following dialog box.

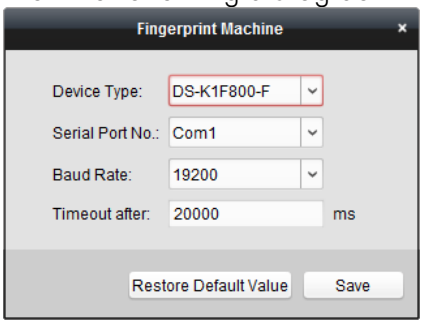


Figure 7-52: Set Fingerprint Machine Box

   1) Select the device type.

      Currently, the supported fingerprint device types include the DS-K1F800-F, DS-K1F810-F, DS-K1F820-F, and DS-K1F181-F models.

   2) The DS-K1F800-F model supports the setting of the serial port number, baud rate, and overtime parameters of the fingerprint machine.

   3) Click **Save** button to save the settings.

      You can click **Restore Default Value** button to restore the default settings.

Notes:

- The serial port number should correspond to the serial port number of the PC. Check the serial port number in the Device Manager.
- The baud rate should be set according to the external fingerprint card reader. The default value is 19200.
- **Timeout after** field refers to the valid fingerprint collecting time. If the user does not input a fingerprint or inputs a fingerprint unsuccessfully, the device will indicate that fingerprint collecting has ended.

4. Click **Start** button, click to select the fingerprint to start collecting.
5. Lift and rest the corresponding fingerprint on the fingerprint scanner twice to collect the fingerprint to the client.
6. (Optional) Click **Remote Collection** to collect a fingerprint from the device.

Note: The function should be supported by the device.

7. (Optional) Select the registered fingerprint and click Delete to delete it. Click Clear to clear all fingerprints.
8. Click OK to save the fingerprints.

Adding Person (Attendance Rule)

Set the attendance rule for the person.

Note: This tab page will display when you select **Non-Residence** mode in the application scene, when running the software for the first time.

1. In the Add Person interface, click the **Attendance Rule** tab.

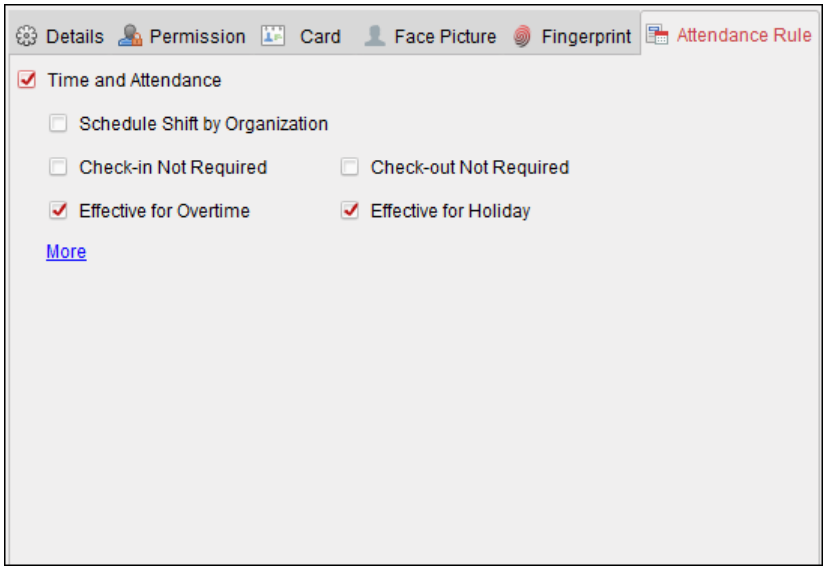


Figure 7-53: Set Attendance Rule Page

2. If time and attendance functionality is added for a person, check the Time and Attendance checkbox to enable this function for that person. The person's card swiping records will be recorded and analyzed for time and attendance.

   For details about Time and Attendance, click **More** to enter the Time and Attendance module.

3. Click **OK** to save the settings.

Importing and Exporting Person Information

Person information can be imported and exported in batch.

1. **Exporting Person:** Export the added person information in Excel to the local PC.

    1) After adding the person, click **Export Person** button in the Person and Card tab to display the following dialog box.

    2) Click ... to select the path that the exported Excel file should be saved to.

    3) Check the checkboxes to select the person information to be exported.

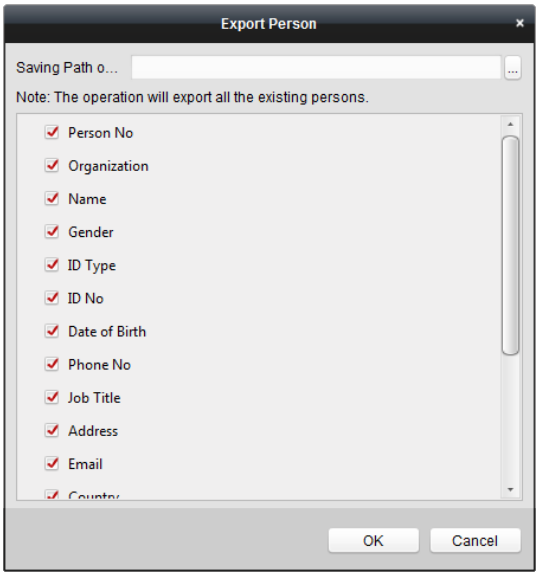


Figure 7-54: Export Person Settings Box

    4) Click **OK** to start exporting.

2. **Importing Person:** Import the Excel file with the person information in batch from the local PC.

    1) Click **Import Person** button in the Person and Card tab.

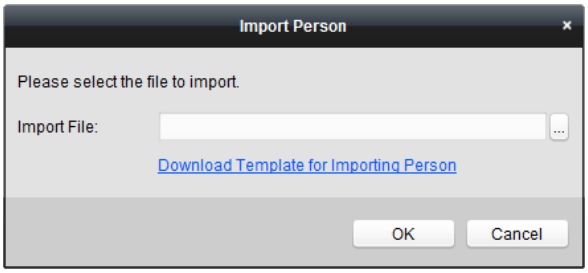


Figure 7-55: Import Person Box

    2) Click **Download Template for Importing Person** to download the template first.

    3) Enter the person information to the downloaded template.

    4) Click ... to select the Excel file with person information.

    5) Click **OK** to start importing.

Getting Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, issued card information), obtain the person information from the device and import it to the client for further use.

Note: This function is only supported by devices that have had TCP/IP communication enabled when the device was added.

1. In the organization list on the left, select the organization that the persons should be imported to.
2. Click **Get Person** button to display the following dialog box.

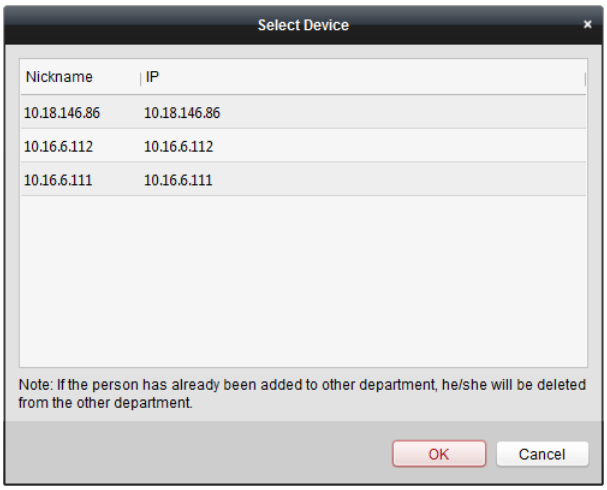


Figure 7-56: Select Device Dialogue Box

3. The added access control device will be displayed.
4. Click to select the device and then click **OK** to start getting the person information from the device.

   Otherwise, double click the device name to start obtaining the person information.

Notes:

- The person information, including person details, fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
- 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.
- Up to 10000 persons can be imported.

7.5.2 Managing Person

Modifying and Deleting Person

To modify the person information and attendance rule, click or in the Operation column, or select the person and click **Modify** to open the editing person dialog box.

Click to view the person's card swiping records.

To delete the person, select a person and click **Delete** to delete it.

Note: If a card is issued to the current person, the linkage will be invalid after the person is deleted.

Changing Person to Other Organization

Move the person to another organization, if needed.

1. Select the person in the list and click the **Change Organization** button.

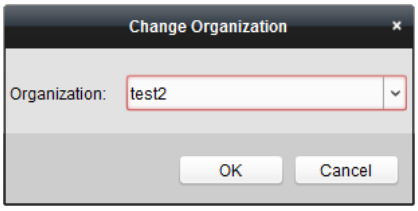


Figure 7-57: Change Organization Box

2. Select the organization to move the person to.
3. Click **OK** to save the settings.

Searching Person

Input the keyword of card No. or person name in the search field, and click **Search** to search the person.

Input the card No. by clicking **Read** to get the card number via the connected card enrollment station.

Click **Set Card Enrollment Station** in the dropdown list to set the parameters.

7.5.3 Issuing Card in Batch

Issue multiple cards in batch for persons with no card issued.

1. Click **Issue Card in Batch** button to enter the following dialog box.

All of the added persons without an issued card will be displayed in the Person(s) with No Card Issued list.

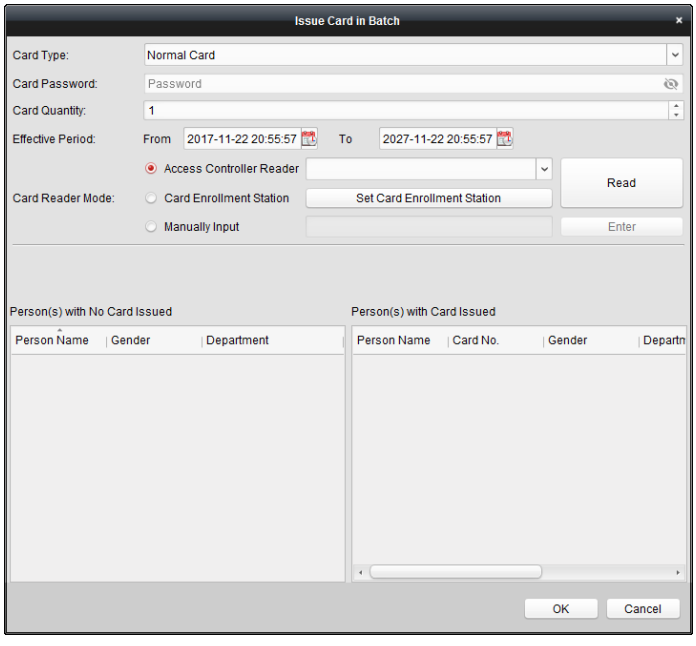


Figure 7-58: Issue Card in Batch Box

2. Select the card type, as needed.

Note: For details about the card type, refer to the *Adding Person* section.

3. Input the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.

Note: The password will be required when the card holder swiping the card to get enter to or exit from the door, if the card reader authentication mode has been enabled as **Card and Password**, **Password and Fingerprint**, and **Card, Password, and Fingerprint**. For further details, refer to *Chapter 7.8.2 Card Reader Authentication.*

4. Input the card quantity issued for each person.

For example, if the Card Quantity is 3, read or enter three card numbers for each person.

5. Click to set the effective time and expiry time of the card.

6. In the Person(s) with No Card Issued list on the left, select the person to issue card.

Note: Click on the Person Name, Gender, and Department column to sort the persons according to actual needs.

7. Select the Card Reader Mode for reading the card number.

- **Access Controller Reader:** Place the card on the reader of the Access Controller and click **Read** to get the card number.
- **Card Enrollment Station:** Place the card on the Card Enrollment Station and click **Read** to get the card number.

Note: The Card Enrollment Station should connect with the PC running the client. Click **Set Card Enrollment Station** to enter the following dialog:

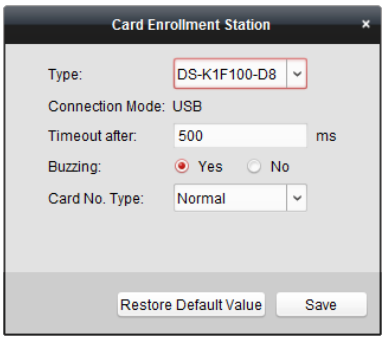


Figure 7-59: Card Enrollment Selection Box

1) Select the Card Enrollment Station type.

Note: Currently, the supported card reader types include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E models.

2) Set the connected card enrollment station parameters.

If the card is an M1 card, and if you need to enable the M1 Card Encryption function, check **Enable** checkbox under M1 Card Encryption and click **Modify** to select the sector.

3) Click **Save** button to save the settings.

Click **Restore Default Value** button to restore the defaults.

- **Manually Input:** Input the card number and click **Enter**.

8. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.

9. Click **OK** to save the settings.

7.6 Schedule and Template

Purpose:
You can configure the template including week schedule and holiday schedule. After setting the templates, you can adopt the configured templates to access control permissions when setting the permission, so that the access control permission will take effect in the time durations of the template.

Click  to enter the schedule and template interface.

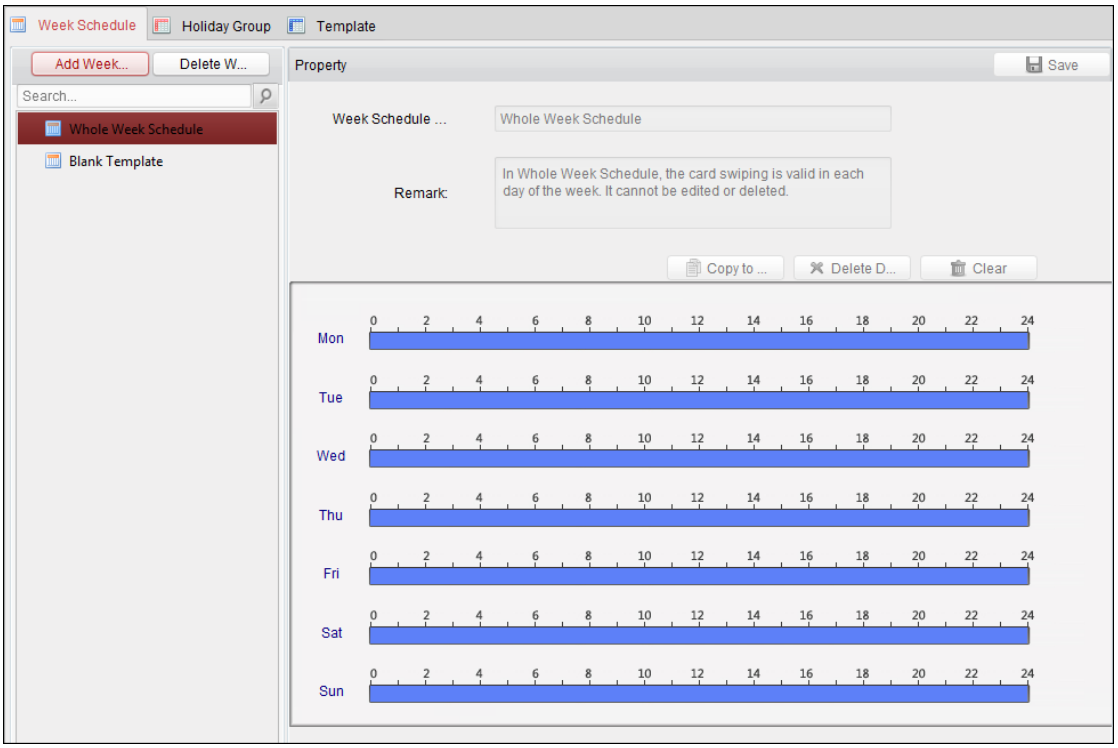


Figure 7-60: Week Schedule Configuration Page

Manage the access control permission schedule, including Week Schedule, Holiday Schedule, and Template. For permission settings, refer to *Chapter 7.7 Permission Configuration.*

7.6.1 Week Schedule

Click **Week Schedule** tab to enter the Week Schedule Management interface.

The client defines two kinds of week plans by default: **Whole Week Schedule** and **Blank Schedule**, which cannot be deleted and edited.

- **Whole Week Schedule:** Card swiping is valid on each day of the week.

- **Blank Schedule:** Card swiping is invalid on each day of the week.

Perform the following steps to define custom schedules.

1. Click **Add Week Schedule** button to display the adding schedule interface.

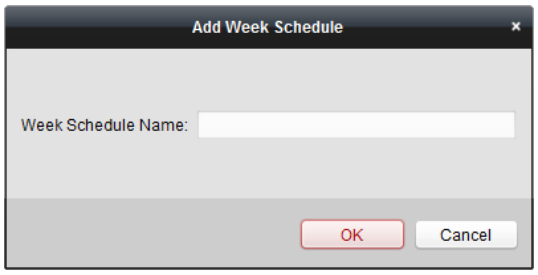


Figure 7-61: Add Week Schedule Box

2. Input the name of week schedule and click **OK** button to add the week schedule.
3. Select the added week schedule in the schedule list and you can view its properties on the right. Edit the week schedule name and input any relevant information.
4. In the week schedule, click and drag a day to draw on the schedule. This means that a configured permission has been activated for a given time period.

Note: Up to 8 time periods can be set for each day in the schedule.

5. When the cursor turns to , move the selected time bar that was just edited. Also, edit the displayed time point to set the accurate time period.

When the cursor turns to , lengthen or shorten the selected time bar.

6. Optionally, select the schedule time bar, and then click **Delete Duration** to delete the selected time bar, click **Clear** to delete all time bars, or click **Copy to Week** to copy the time bar settings to the whole week.
7. Click **Save** to save the settings.

7.6.2 Holiday Group

Click **Holiday Group** tab to enter the Holiday Group Management interface.

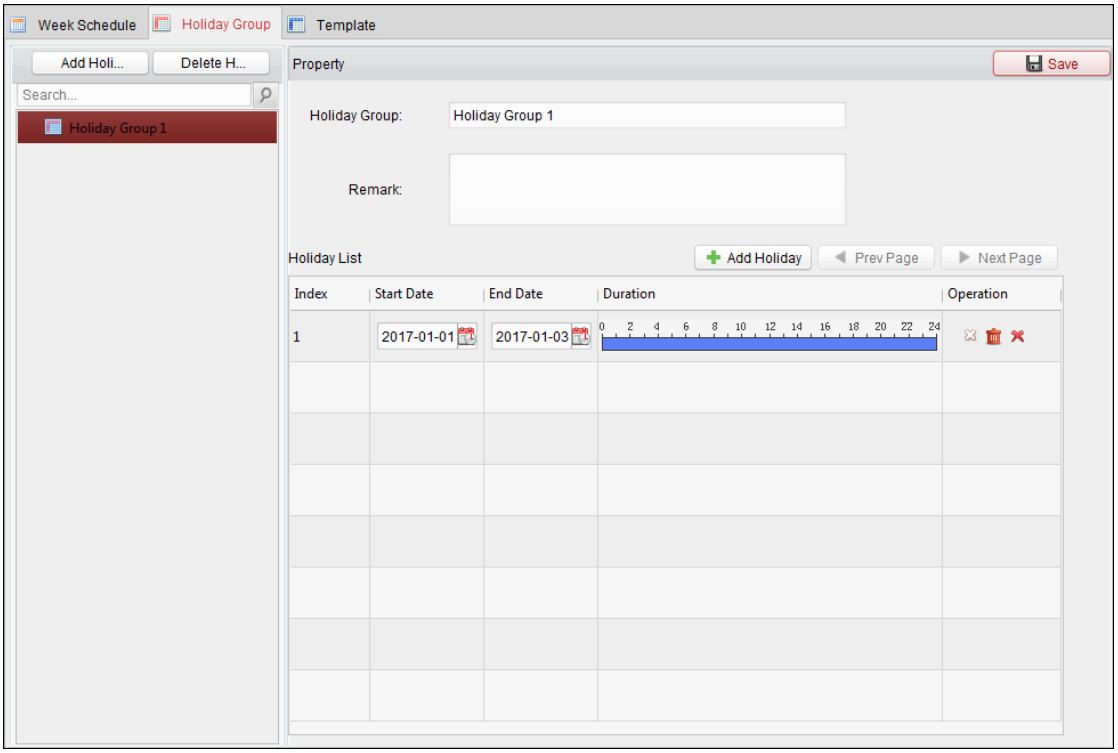


Figure 7-62: Holiday Group Configuration Page

1. Click **Add Holiday Group** button on the left to display the adding holiday group interface.

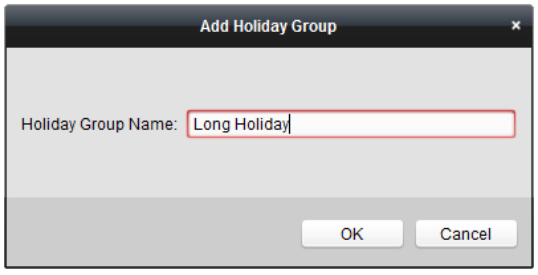


Figure 7-63: Holiday Group Addition Box

2. Input the name of holiday group in the text filed and click **OK** to add the holiday group.
3. Select the added holiday group and edit the holiday group name and input any relevant information.
4. Click **Add Holiday** icon on the right to add a holiday period to the holiday list and configure the duration of the holiday.

Note: Up to 16 holidays can be added to one holiday group.

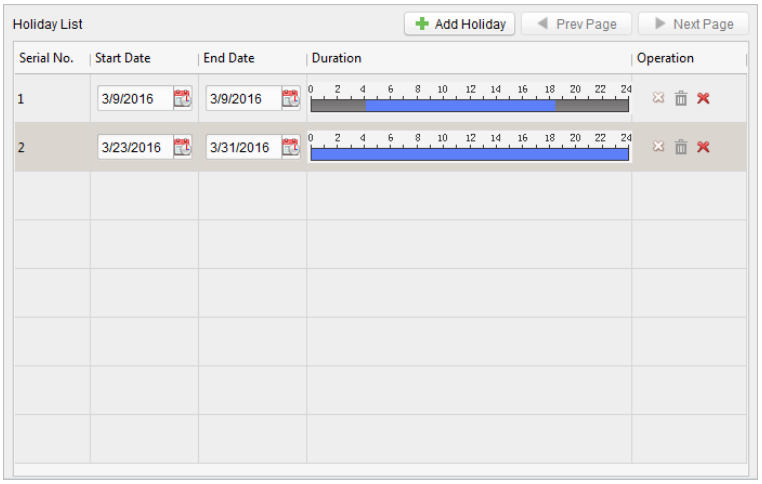


Figure 7-64: Holiday Setting List Page

1) In the period schedule, click and drag to draw the period, which means that the configured permission has been activated for that period of time.

Note: Up to 8 time durations can be set for each period in the schedule.

2) When the cursor turns to , move the selected time bar that was just edited. Edit the displayed time point to set the accurate time period.

3) When the cursor turns to , you can lengthen or shorten the selected time bar.

4) Optionally, you can select the schedule time bar, and then click to delete the selected time bar, or click to delete all the time bars of the holiday, or click to delete the holiday directly.

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

Note: The holidays cannot be overlapped with each other.

7.6.3 Template

After setting the week schedule and holiday group, you can configure the template which contains week schedule and holiday group schedule.

Note: The priority of holiday group schedule is higher than the week schedule. Click **Template** tab to enter the Template Management interface.

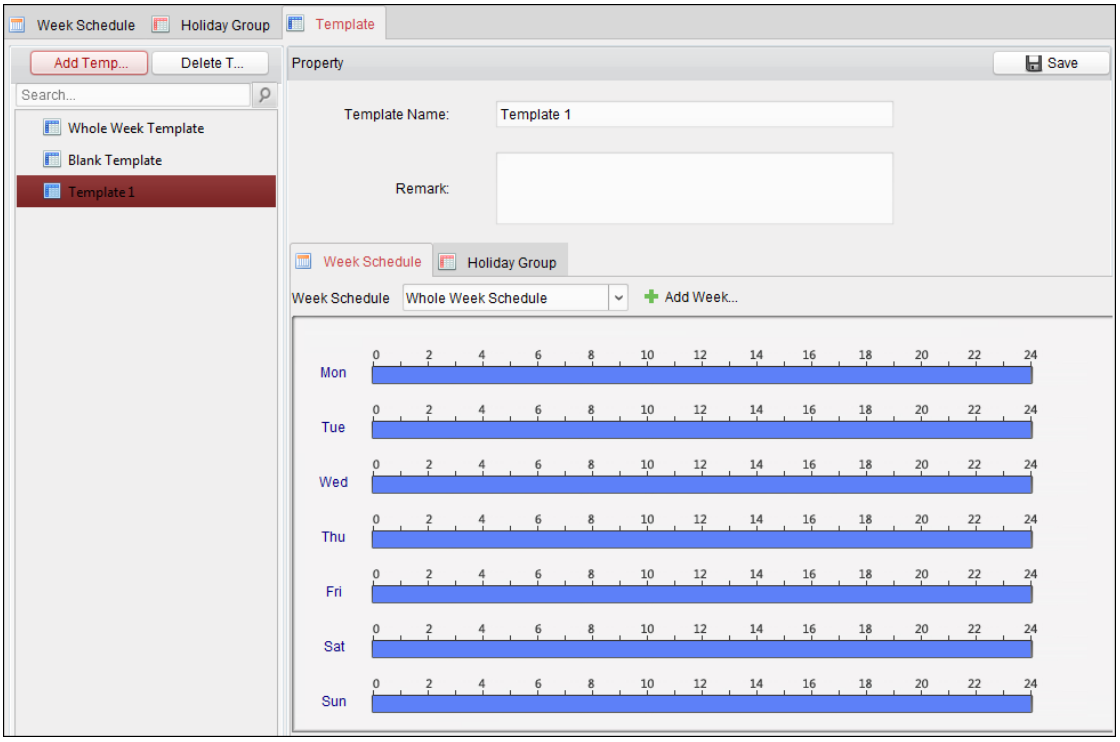


Figure 7-65: Holiday Template Page

There are two pre-defined templates by default: **Whole Week Template** and **Blank Template**, which cannot be deleted and edited.

- **Whole Week Template:** The card swiping is valid on each day of the week and has no holiday group schedule.
- **Blank Template:** The card swiping is invalid on each day of the week and has no holiday group schedule.

Define custom templates, as required.

1. Click **Add Template** to display the adding template interface.

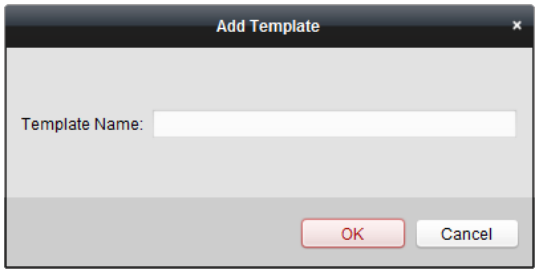


Figure 7-66: Add Holiday Template Box

2. Input the template name in the text field and click **OK** button to add the template.
3. Select the added template and edit its properties on the right. Edit the template name and input any relevant information.
4. Select a week schedule to apply to the schedule.

Click **Week Schedule** tab and select a schedule in the dropdown list.

You can also click **Add Week Schedule** to add a new week schedule. For details, refer to *Chapter 7.6.1 Week Schedule.*

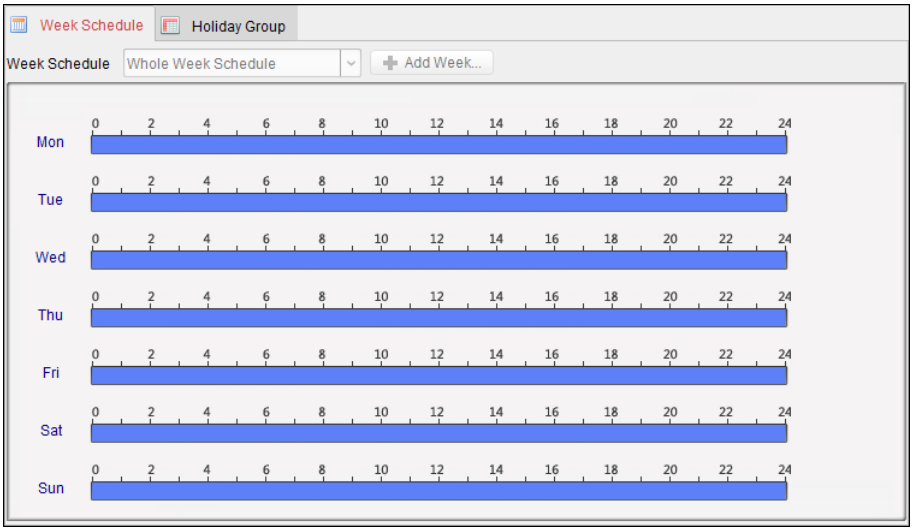


Figure 7-67: Week Schedule Page

5. Select holiday groups to apply to the schedule.

Note: Up to 4 holiday groups can be added.

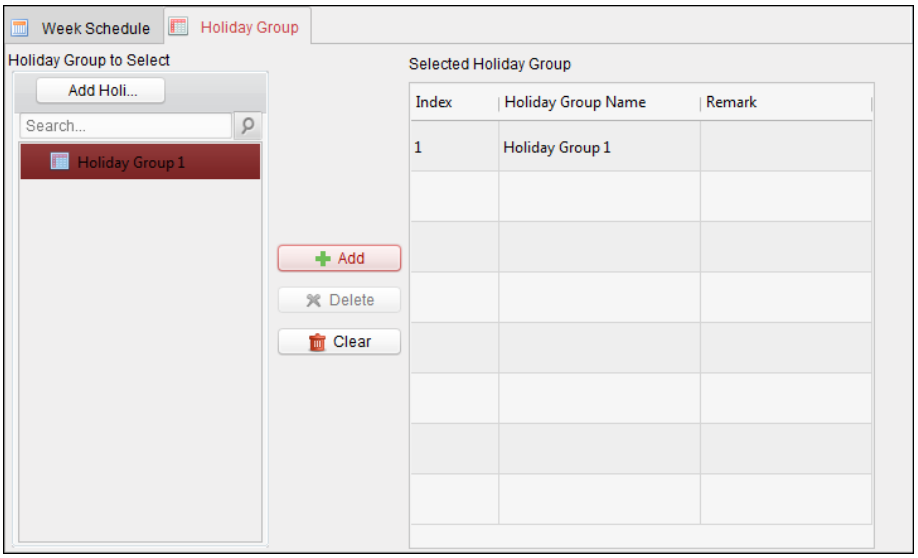


Figure 7-67: Holiday Group Configuration Page

Click to select a holiday group in the list and click **Add** to add it to the template. Click **Add Holiday Group** to add a new one. For details, refer to *Chapter 7.6.2 Holiday Group.*

Select an added holiday group in the right-side list and click **Delete** to delete it. Click **Clear** to delete all added holiday groups.

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

7.7 Permission Configuration

In the Permission Configuration module, add, edit, and delete the access control permission, and then apply the permission settings to the device for it to take effect.

Click  icon to enter the Access Control Permission interface.

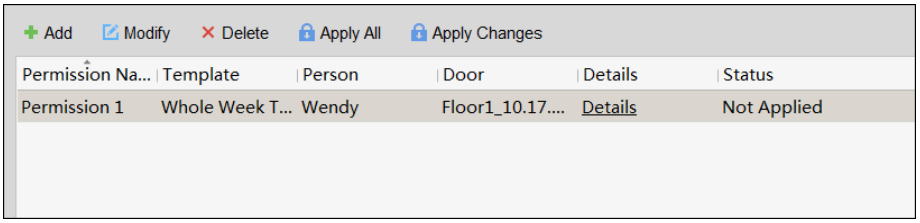


Figure 7-68: Permission Addition List

7.7.1 Adding Permission

Purpose:
Assign access control entrance/exit (door) permissions in this section.

Notes:

- Add up to 4 permissions to one access control point of one device.
- Add up to 128 permissions in total.

1. Click the **Add** icon to enter the following interface.

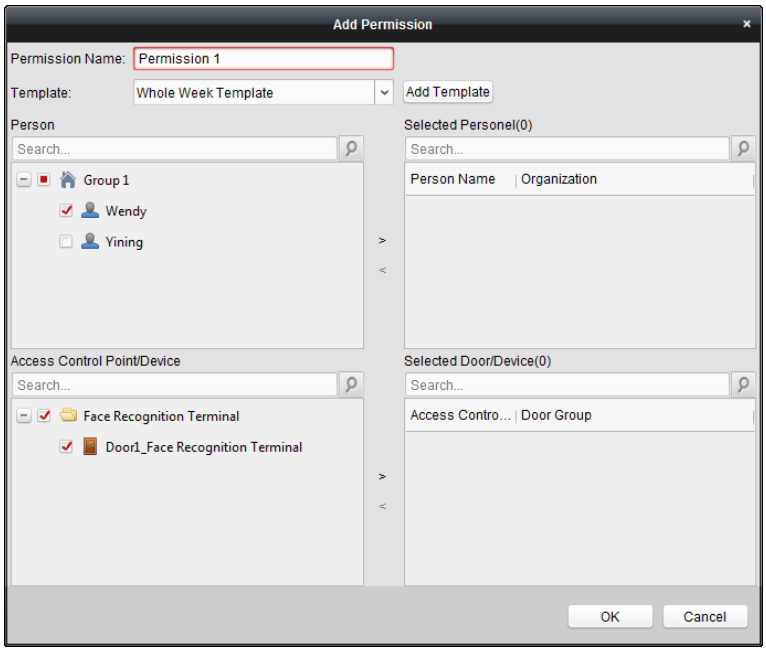


Figure 7-69: Permission Addition Box

2. In the Permission Name field, input the name for the permission.

3. Click on the dropdown menu to select a template for the permission.

Note: Configure the template before defining permission settings. Click **Add Template** button to add the template. Refer to *Chapter 7.6 Schedule and Template* for details.

4. All of the added persons are displayed in the Persons list.

Check the checkbox(es) to select person(s) and click **>** to add to the Selected Person list. (Optional) Select the person in the Selected Person list and click **<** to cancel the selection.

5. In the Access Control Point/Device list, all the added access control points (doors) and door stations will be displayed.

Check the checkbox(es) to select door(s) or door station(s), and click **>** to add to the selected list.

(Optional) Select the door or door station in the selected list and click **<** to cancel the selection.

6. Click **OK** button to complete the permission adding. The selected person will have the permission to enter/exit the selected door/door station with their linked card(s) or fingerprints.

7. (Optional) after adding the permission, you can click **Details** to modify it. Select the permission and click **Modify** to modify.

Select the added permission in the list and click **Delete** to delete it.

7.7.2 Applying Permission

Purpose:
After configuring the permissions, apply the added permission to the access control device to take effect.

1. Select the permission(s) to apply to the access control device.

To select multiple permissions, hold the *Ctrl* or *Shift* key and select permissions.

2. Click **Apply All** to start applying all the selected permission(s) to the access control device or door station.

Click **Apply Changes** to apply the changed part of the selected permission(s) to the device(s).

3. The following window will display, indicating the applying permission result.

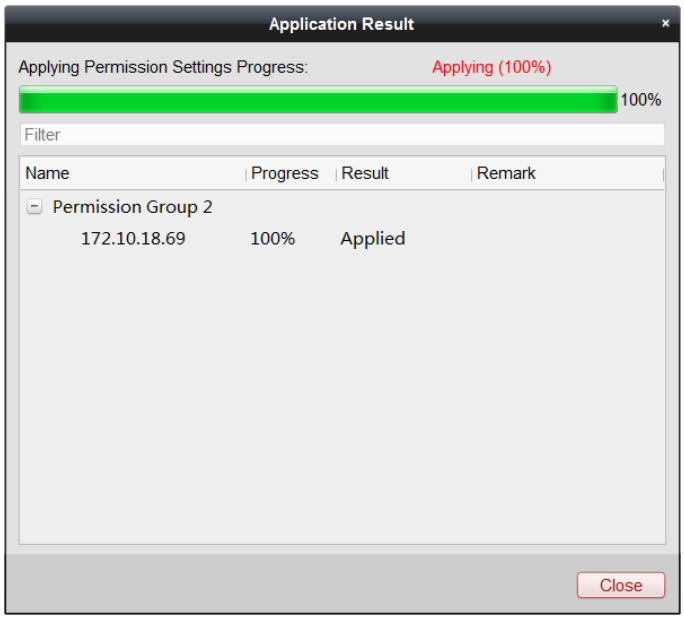


Figure 7-70: Permission Application Results Box

Notes:

- When the permission settings are changed, the following hint box will display.

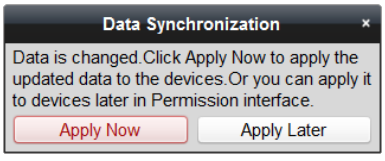


Figure 7-71: Data Synchronization Dialogue Box

Click **Apply Now** to apply the changed permissions to the device.

Otherwise, click **Apply Later** to apply the changes later in the Permission interface.

- The permission changes include changes of schedule and template, permission settings, person's permission settings, and related person settings (including card No., fingerprint, face picture, linkage between card No. and fingerprint, linkage between card No. and fingerprint, card password, card effective period, etc.)

7.8 Advanced Functions

Purpose:
After configuring the person, template, and access control permission, configure the advanced functions of the access control applications, such as access control parameters, authentication password, and opening door with first card, anti-passing back, etc.

Note: The advanced functions should be supported by the device. Click  to enter the following interface.

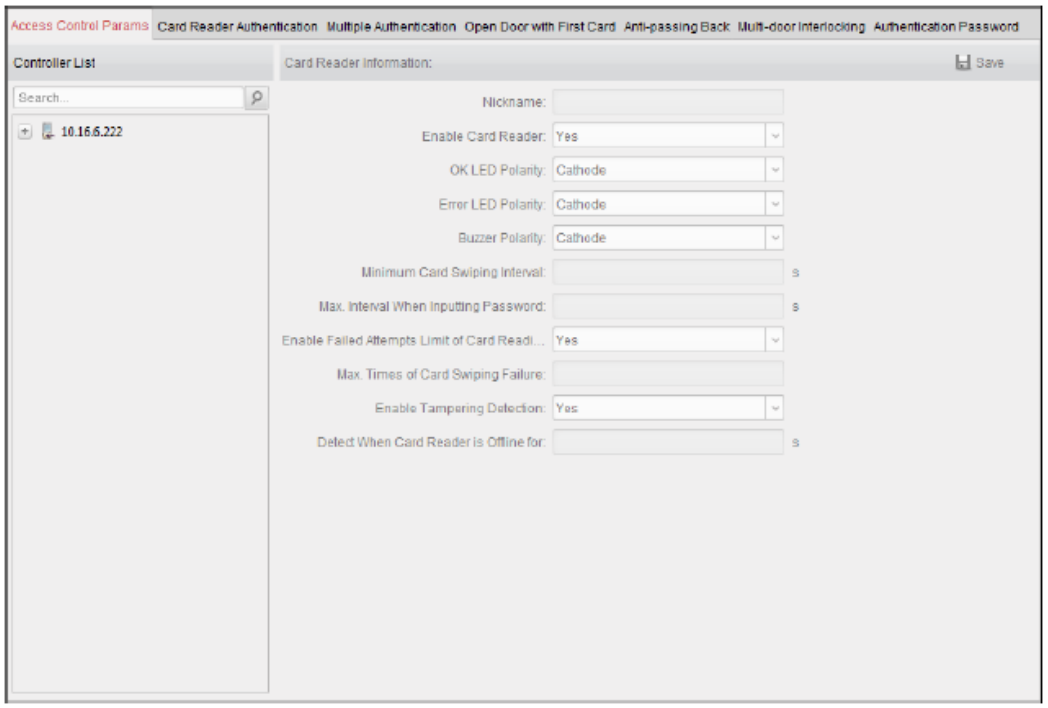


Figure 7-72: Access Control Parameters Page

7.8.1 Access Control Parameters

Purpose:
After adding the access control device, configure its access control point (door) parameters, and its card reader parameters.

Click **Access Control Parameters** tab to enter the parameters settings interface.

Door Parameters

1. In the controller list on the left, click  to expand the access control device, select the door (access control point) and you can edit the information of the selected door on the right.

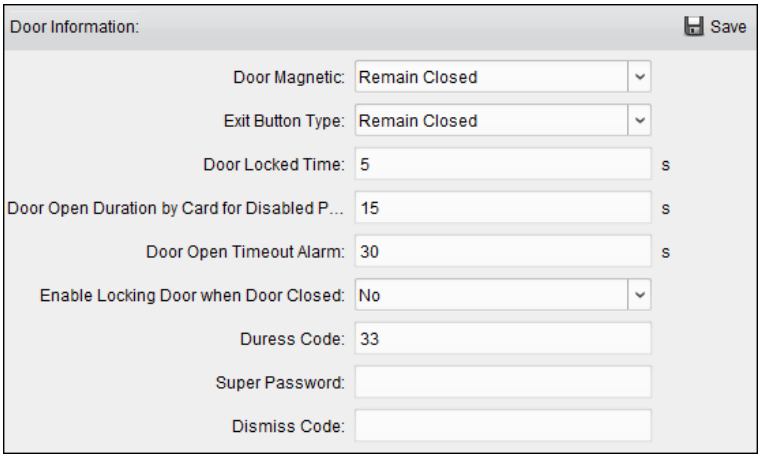


Figure 7-73: Door Parameters Page

2. You can edit the following parameters:

- **Door Magnetic**: The Door Magnetic is in **Remain Closed** status (excluding special conditions).
- **Exit Button Type**: The Exit Button Type is **Remain Open** status (excluding special conditions).
- **Door Locked Time**: After swiping the normal card and relay action, the timer for locking the door will begin working.
- **Door Open Duration by Card for Disabled Person:** The magnetic door can be enabled with appropriate delay after a disabled person swipes the card.
- **Door Open Timeout Alarm**: The alarm can be triggered if the door has not been closed.
- **Enable Locking Door when Door Closed**: The door can be locked once it is closed, even if the Door Locked Time has not been reached.
- **Duress Code**: The door can open by inputting the duress code when there is a duress event. 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:** Set the dismiss code and use the dismiss code to stop the card reader buzzer.

Notes:

- The duress code, super password, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The duress code, super password, and the dismiss code should contain 4 to 8 numbers.

3. Click **Save** button to save parameters.

Card Reader Parameters

4. In the device list on the left, click ⊞ to expand the door, select the card reader name. and edit the card reader parameters on the right.

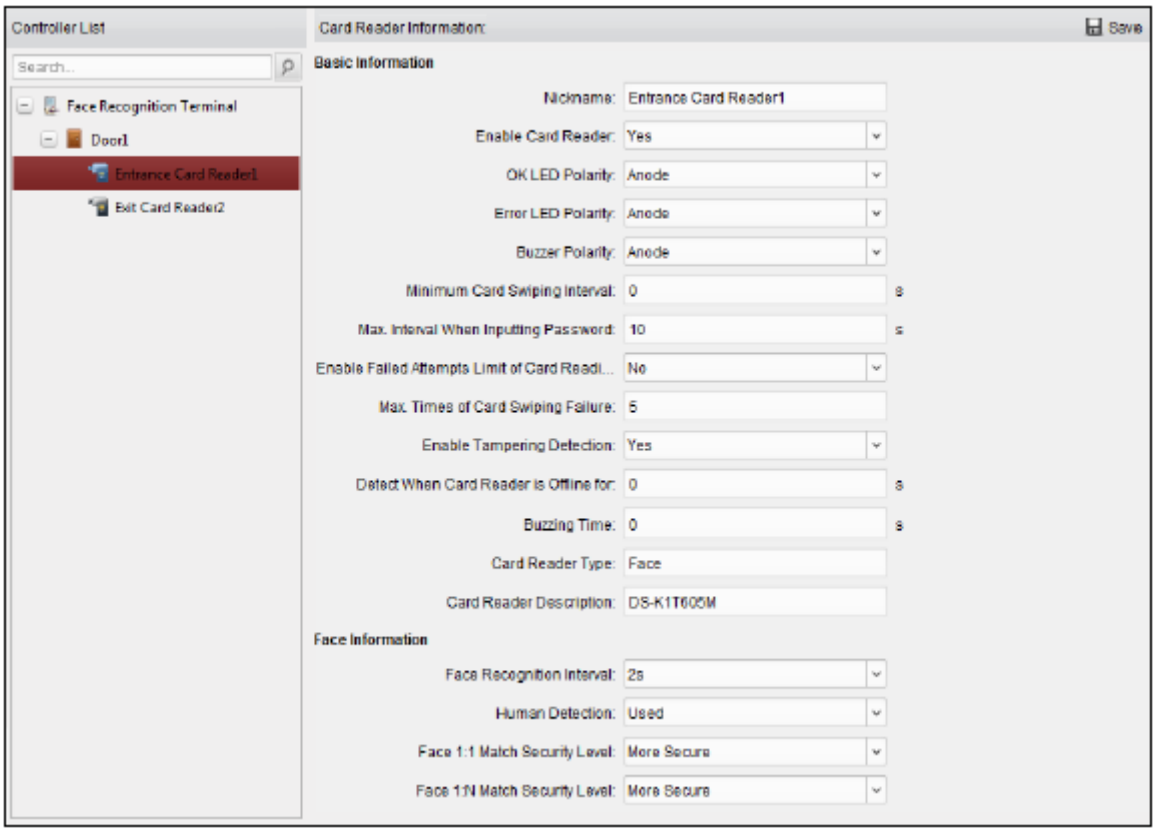


Figure 7-74: Card Reader Information Page

5. You can edit the following parameters:

- **Nickname:** Edit the card reader name.
- **Enable Card Reader:** Select **Yes** to enable the card reader.
- **OK LED Polarity:** Select the OK LED Polarity of the card reader mainboard.
- **Error LED Polarity:** Select the Error LED Polarity of the card reader mainboard.
- **Buzzer Polarity:** Select the Buzzer LED Polarity of the card reader mainboard.
- **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. Set it as 0 to 255.
- **Max. Interval When Inputting Password:** 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.
- **Enable Failed Attempts Limit of Card Reading:** Enable to report alarm when the card reading attempts reach the set value.
- **Max. Times of Card Swiping Failure:** Set the max. failure attempts of the reading card.
- **Enable Tampering Detection:** Enable the anti-tamper detection for the card reader.
- **Detect When Card Reader is Offline for:** 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 5999s. 0

represents continuous buzzing.

- **Card Reader Type:** Get the card reader's type.
- **Card Reader Description:** Get the card reader description.
- **Face Recognition Interval:** The time interval between two continuous face recognitions when authenticating. By default, it is 2s.
- **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.
- **1:1 Security Level:** Set the matching security level when authenticating via 1:1 matching mode.
- **1:N Security Level:** Set the matching security level when authenticating via 1:N matching mode.

7.8.2 Card Reader Authentication

Purpose:
Set the passing rules for the card reader of the access control device.

1. Click **Card Reader Authentication** tab and select a card reader on the left.
2. Click **Configuration** button to select the card reader authentication modes for setting the schedule.

Notes:

- The available authentication modes depend on the device type.
- Password refers to the card password set when issuing the card to the person in *Chapter 7.5 Person Management.*

  1) Select the modes and click » to add to the selected modes list. Click ↑ or ↓ to adjust the display order.
  2) Click **OK** to confirm the selection.

3. After selecting the modes, the selected modes will display as icons. Click the icon to select a card reader authentication mode.
4. Click and drag your mouse on a day to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.

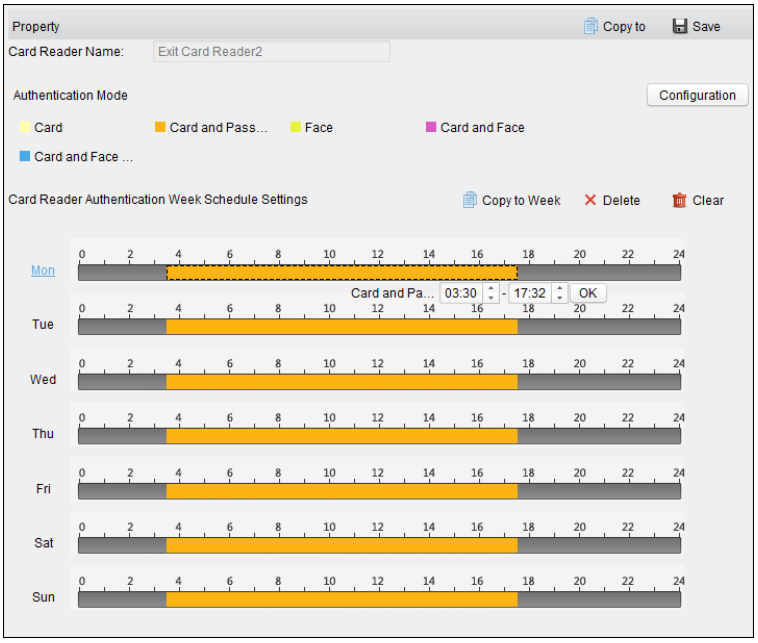


Figure 7-75: Card Reader Authentication Page

5. Repeat the above step to set other time periods.

Otherwise, select a configured day and click **Copy to Week** button to copy the same settings to the whole week.

(Optional) Click **Delete** to delete the selected time period, or click **Clear** button to delete all the configured time periods.

6. (Optional) Click **Copy to** button to copy the settings to other card readers.

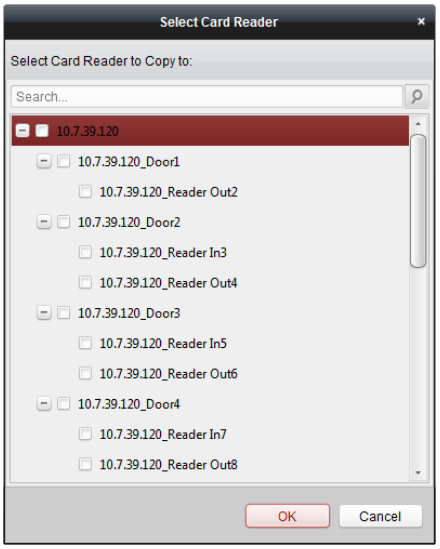


Figure 7-76: Card Reader Selection Page

7. Click **Save** button to save parameters.

7.8.3 Multiple Authentication

Purpose:
Manage the cards by group and set the authentication for multiple cards for one access control point (door).

Note: Please set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration.*

1. Click **Multiple Authentication** tab to enter the following interface.

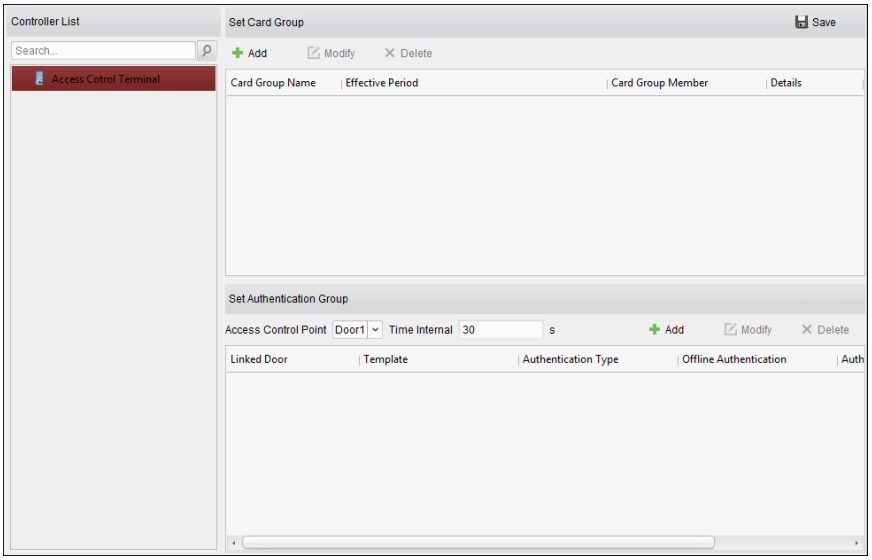


Figure 7-77: Multiple Authentication Page

2. Select access control device from the list on the left.

3. In the Set Card Group panel on the right, click **Add** button to display the following dialog:

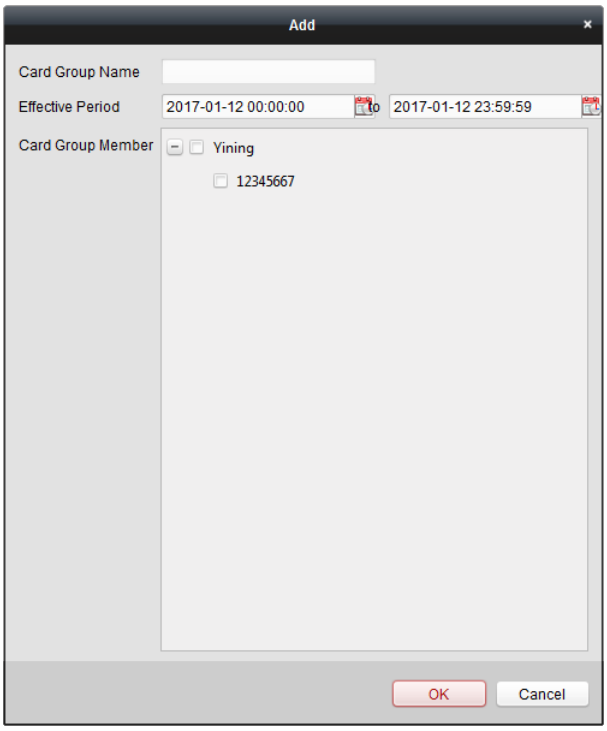


Figure 7-78: Add Group Name Box

1) In the Card Group Name field, input the name for the group as desired.

2) Click to set the effective time and expiry time of the card group.

3) Check the checkbox(es) to select the card(s) to add the card group.

4) Click **OK** to save the card group.

4. In the Set Authentication Group panel, select the access control point (door) of the device for multiple authentications.

5. Input the time interval for card swiping.

6. Click **Add** to display the following dialog box.

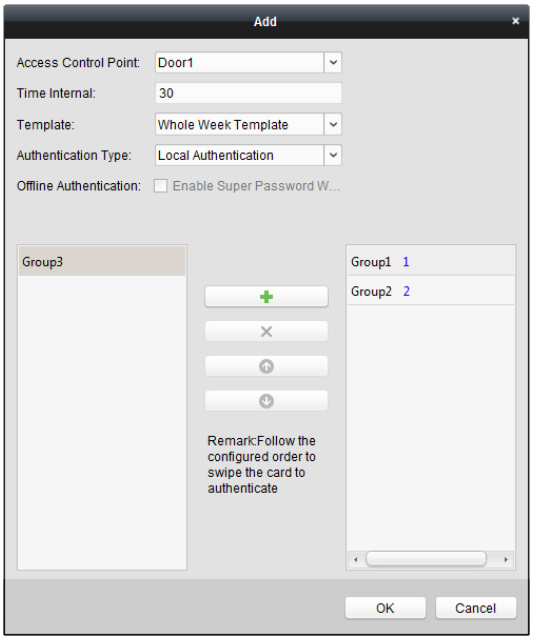


Figure 7-79: Add Group Name Box

1) Select the template of the authentication group from the dropdown list. For details about setting the template, refer to *Chapter 7.6 Schedule and Template*.

2) Select the authentication type of the authentication group from the dropdown list.

- **Local Authentication:** Authentication via access control device.
- **Local Authentication and Remotely Open Door:** Authentication via the access control device and the client.

  For Local Authentication and Remotely Open Door type, check the checkbox to enable super password authentication when the access control device is disconnected from the client.
- **Local Authentication and Super Password:** Authentication via the access control device and super password.

3) In the list on the left, the added card group will display. Click the card group and click ✚ to add the group to the authentication group.

   Click the added card group and click ✕ to remove it from the authentication group.

   Click ↑ or ↓ to set the card swiping order.

4) Input the **Card Swiping Times** for the selected card group.

Notes:

- The Card Swiping Times should be larger than 0 and smaller than the added card quantity in the card group.

- The upper limit of Card Swiping Times is 16.

5) Click **OK** to save the settings.

7. Click **Save** to save and take effect of the new settings.

Notes:

- For each access control point (door), up to 20 authentication groups can be added.
- For the authentication group which certificate type is **Local Authentication**, up to 8 card groups can be added to the authentication group.
- For the authentication group which certificate type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 card groups can be added to the authentication group.

7.8.4 Open Door with First Card

Purpose:
Set multiple first cards for one access control point. After the first card is swiped, multiple persons can access the door or other authentication actions. The first card mode contains Remain Open with First Card, Disable Remain Open with First Card, and First Card Authorization.

- **Remain Open with First Card:** The door remains open for the configured time period following the first card swipe until the remain open duration period ends.
- **Disable Remain Open with First Card:** Disable this function.
- **First Card Authorization:** All authentications (except for super card, super password, duress card, and duress code authorizations) are allowed only after the first card is authorized.

Notes:

- The first card authorization is effective only on the current day. The authorization will expire after 12:00 AM on the current day.
- Swipe the first card again to disable the first card mode.

1. Click **Open Door with First Card** tab to enter the following interface.

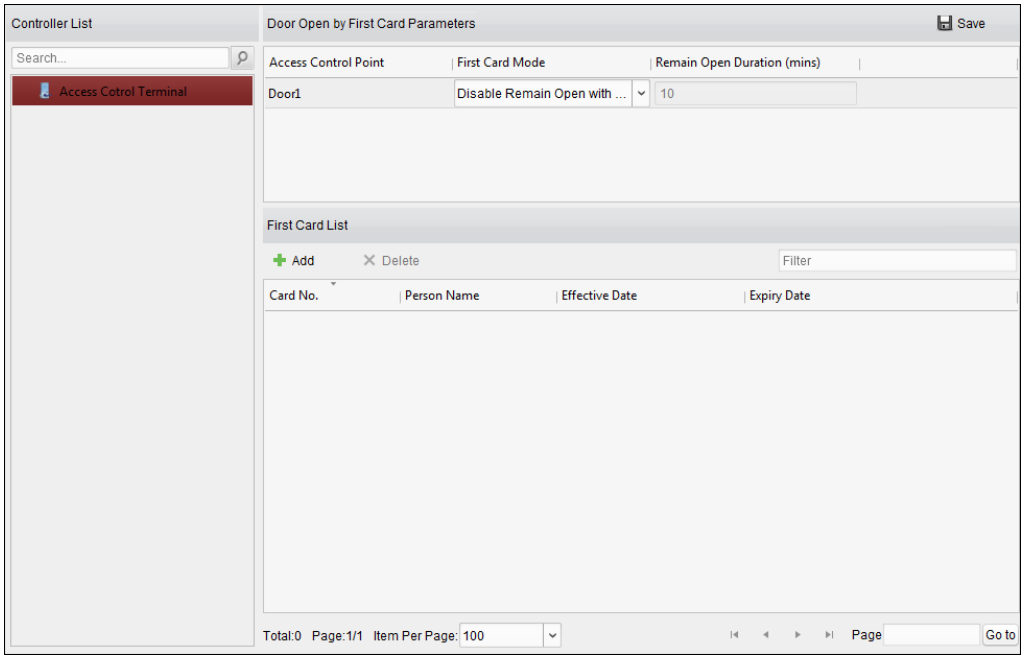


Figure 7-80: Door Open by First Card Parameters Page

2. Select an access control device from the list on the left.
3. Select the first card mode in the drop-down list for the access control point.
4. (Optional) Select Remain Open with First Card and set a remain open duration.

Notes:

- The Remain Open Duration should be between 0 and 1440 minutes. By default, it is 10 minutes.
- Swipe the first card again to disable the first card mode.

5. In the First Card list, click the **Add** button to display the following dialog box.

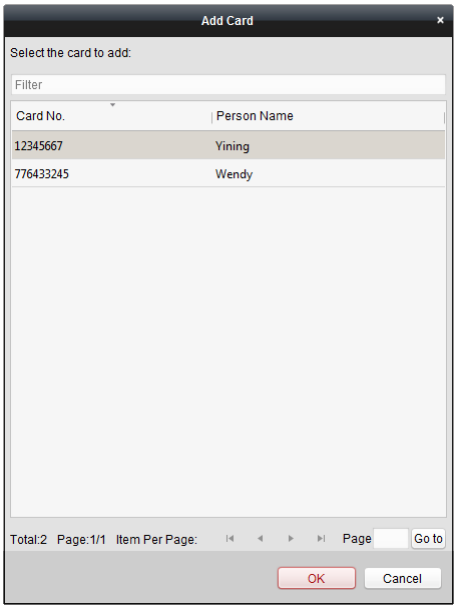


Figure 7-81: Add Card Page

1) Select the cards to add as first card for the door.

Note: Set the card permission and apply the permission setting to the access control device first. For details, refer to *Chapter 7.7 Permission Configuration.*

2) Click **OK** button to save adding the card.

6. Click the **Delete** button to remove the card from the first card list.

7. Click **Save** to save the new settings and have them take effect.

7.8.5 Anti-Passing Back

Purpose:
Set the passing of an access control point only by means of a specified path, and only allow one person to pass the access control point after swiping the card.

Notes:

- Either the anti-passing back or multi-door interlocking function can be configured for one access control device at the same time.
- Enable the anti-passing back function on the access control device first.

1. Click **Anti-Passing Back** tab to enter the following interface.

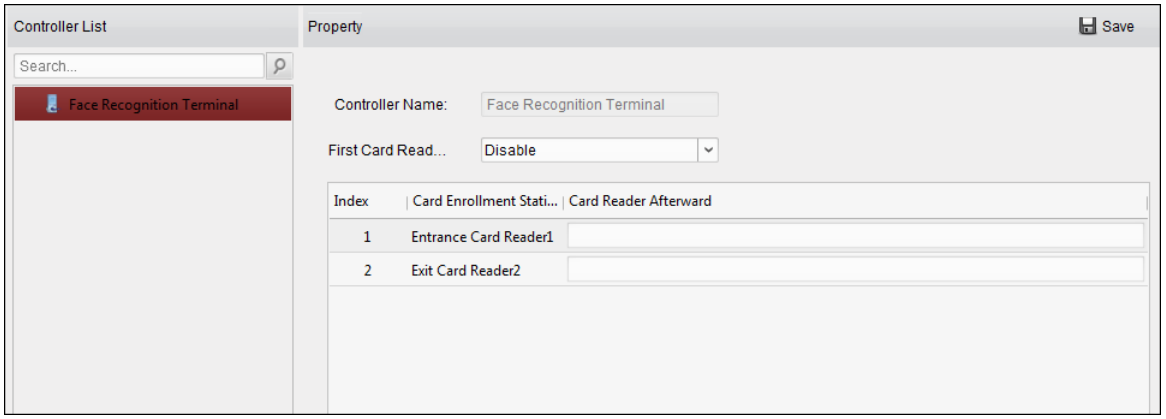


Figure 7-82: Add Card Page

2. Select an access control device from the device list on the left.

3. In the First Card Reader field, select the card reader as the beginning of the path.

4. Click the **Card Reader Afterward** text field and select the linked card readers. **Example:** If Reader In_01 is selected at the beginning, and Reader In_02 and Reader Out_04 are selected as linked card readers, the only way to get through the access control points is by swiping the card in the following order: Reader In_01, Reader In_02, and Reader Out_04.

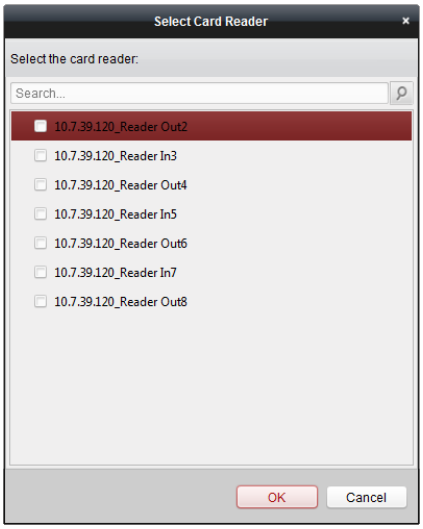


Figure 7-83: Card Reader Selection Box

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

5. (Optional) Enter the Select Card Reader dialog box again to edit the other card readers.
6. Click **Save** to save the new settings and have them take effect.

7.9 Searching Access Control Event

Purpose:
Search the access control history events including remote event and local event via the client.

Local Event: Search the access control event from the database of the control client.

Remote Event: Search the access control event in the device. Click , followed by the Access Control Event in order to enter the following interface.

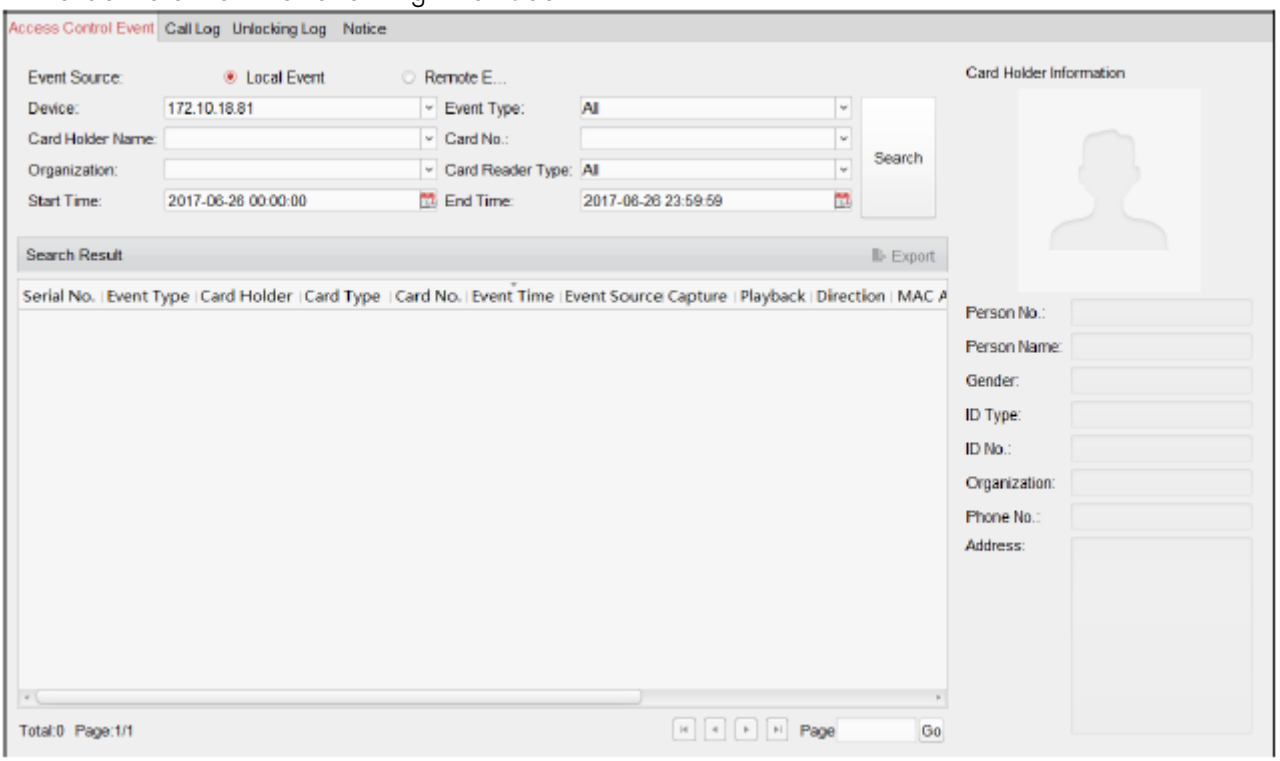


Figure 7-84: Access Control Event Page

7.9.1 Searching Local Access Control Event

1. Select the Event Source as **Local Event**.
2. Input the search condition according to actual needs.
3. Click **Search**. The results will be listed below.
4. For access control events triggered by the card holder, click the event to view the card holder details, including person No., person name, organization, phone number, contact address, and picture.
5. (Optional) If the event contains linked pictures, click the **Capture** column to view picture captured by the camera when the alarm is triggered.
6. (Optional) If the event contains a linked video, click the **Playback** column to view the recorded video file of the triggered camera when the alarm is triggered.

Note: In order to set the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage.*

7. Click **Export** to export the search result to the local PC in *.csv file.

7.9.2 Searching Remote Access Control Event

1. Select the Event Source as **Remote Event**.
2. Input the search conditions, as required.
3. (Optional) Check **With Alarm Picture** checkbox to search events that contain alarm pictures.
4. Click **Search**. The results will be listed below.
5. Click **Export** to export the search results to the local PC in a *.csv file.

7.10 Access Control Event Configuration

Purpose:
For the added access control device, configure its access control linkage, including access control event linkage, access control alarm input linkage, event card linkage, and cross-device linkage.

Click the  icon on the control panel, or click **Tool**->**Event Management** to open the Event Management page.

7.10.1 Access Control Event Linkage

Purpose:
Assign linkage actions to the access control event by setting up a rule. For example, when the access control event is detected, an audible warning appears or other linkage actions happen.

Note: The linkage here refers to the linkage of the client software's own actions.

1. Click the **Access Control Event** tab.
2. The added access control devices will display in the Access Control Device panel on the left. Select the access control device, alarm input, access control point (door), or card reader to configure the event linkage.
3. Select the event type to set the linkage.
4. Select the triggered camera. The image or video from the triggered camera will display when the selected event occurs.

To capture the picture of the triggered camera when the selected event occurs, set the capture schedule and the storage in Storage Schedule.

5. Check the checkboxes to activate the linkage actions. For details, refer to *Table 14.1 Linkage Actions for Access Control Event*.
6. Click **Save** to save the settings.
7. Click Copy to button to copy the access control event to other access control device, alarm input, access control point, or card reader.

Select the parameters for copy, select the target to copy to, and click **OK** to confirm.

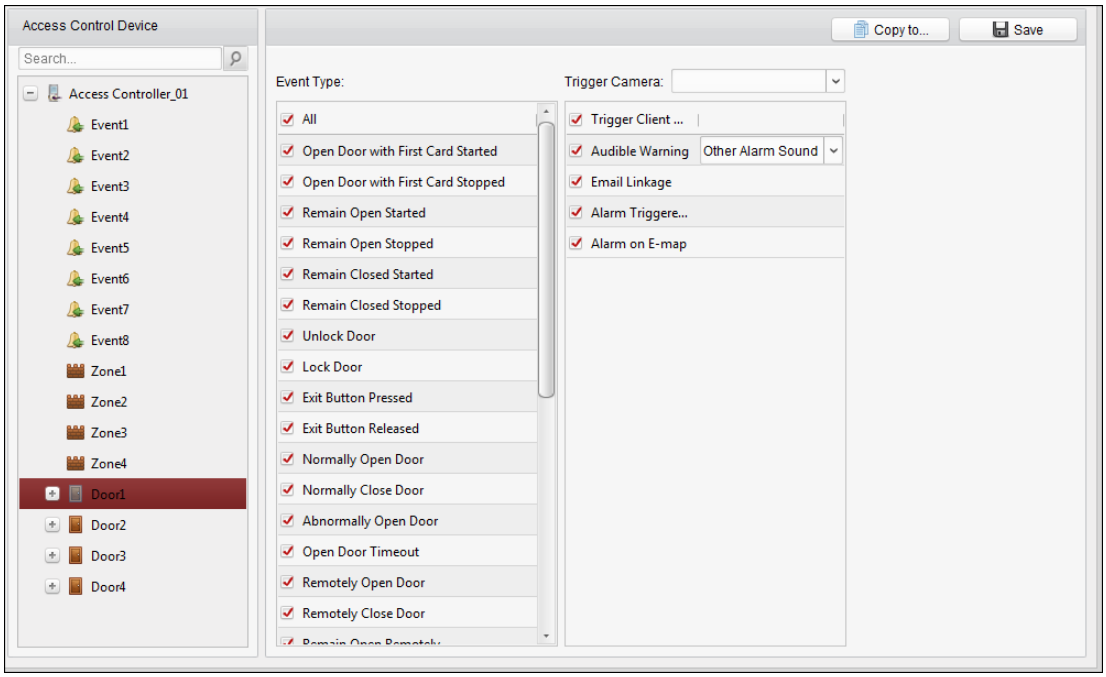


Figure 7-85: Access Control Event Configuration Page

Table 7-1: Linkage Actions for Access Control Events

Linkage Actions	Descriptions
Audible Warning	The client software emits an audible warning when alarm is triggered. Select the alarm sound to receive an audible warning.
Email Linkage	Send an email notification of the alarm information to one or more recipients.
Alarm on E-map	Display the alarm information on the E-map. ***Note:*** This linkage is only available to access control point and alarm input.
Alarm Triggered Pop-up Image	The image with alarm information pops up when alarm is triggered.

7.10.2 Event Card Linkage

Click **Event Card Linkage** tab to enter the following interface.

Note: The Event Card Linkage should be supported by the device.

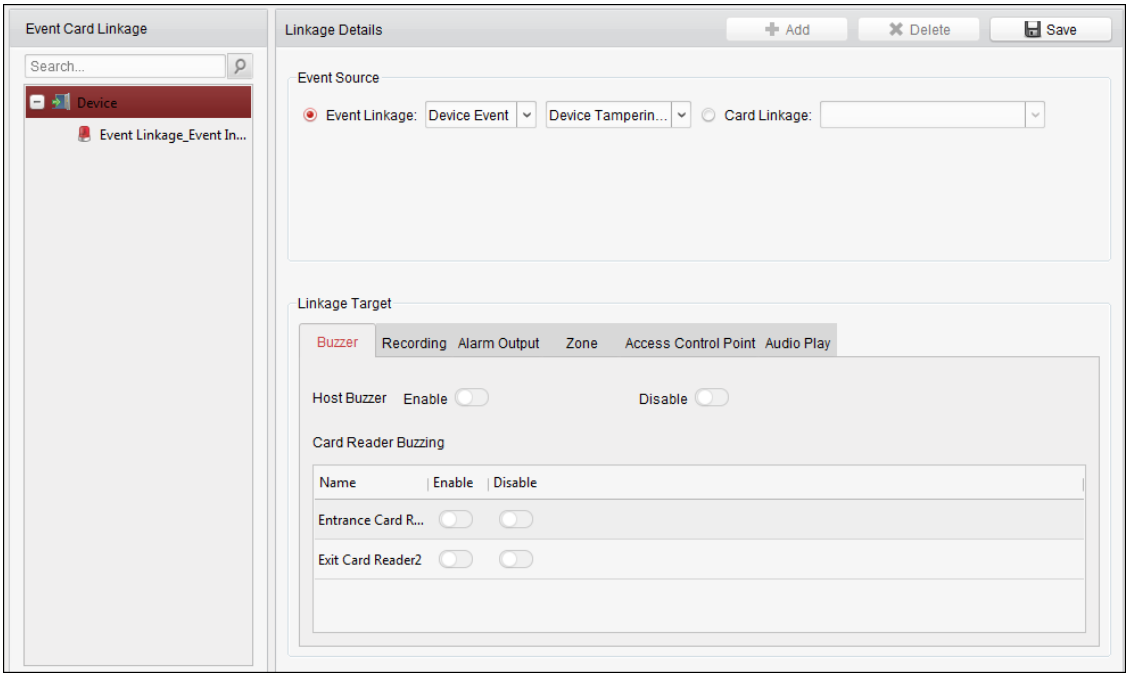


Figure 7-86: Event Card Linkage Details Page

Select the access control device from the list on the left.

Click **Add** button to add a new linkage. Select the event source as **Event Linkage** or **Card Linkage**.

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, or card reader event.

1. Select a device on the left and click **Add.**
2. Click to select the linkage type as **Event Linkage**, and select the event type from the dropdown list.
   - For Device Event, select the detailed event type from the dropdown list.
   - For Alarm Input, select the type as alarm or alarm recovery and select the alarm input name from the panel.

- For Door Event, select the detailed event type and select the source door from the panel.
- For Card Reader Event, select the detailed event type and select the card reader from the panel.

3. Click different tabs to set different parameters. Switch the property from to  to enable this function.

Set the buzzer, recording, alarm output, zone, access control point, and audio play parameters.

Table 7-2: Event Linkage Type Descriptions

Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The controller's audible warning will be triggered.
	Card Reader Buzzing	The card reader's audible warning will be triggered.
Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.
Zone	Zone	The zone will be armed or disarmed according to your settings.
Access Control Point	Access Control Point	The door status (open, close, remain open, and remain closed) will be triggered. ***Notes:*** • The door status (open, close, remain open, and remain closed) cannot be triggered at the same time. • The target door and the source door cannot be the same one.
Audio Play	Audio Play Status	The audio prompt will be triggered. The audio index related to the audio content will be played according to the configured play mode.

4. Click **Save** to save and the parameters and have them take effect.

Card Linkage

1. Click to select the linkage type as **Card Linkage**.
2. Input the card number or select the card from the dropdown list.
3. Select the card reader from the panel for triggering.
4. Click different tabs to set different parameters. Switch the property from to  to enable this function.

Set the parameters of buzzer, recording, alarm output, zone, access control point, and audio play.

Table 7-3: Card Linkage Type Descriptions

Linkage Type	Linkage Target	Descriptions
Buzzer	Host Buzzer	The controller's audible warning will be triggered.
	Card Reader Buzzing	The card reader's audible warning will be triggered.
Recording	Capture Status	The real-time capture will be triggered.
Alarm Output	Alarm Output	The alarm output will be triggered for notification.

Zone	Zone	The zone will be armed or disarmed according to your settings.
Access Control Point	Access Control Point	The door status (open, close, remain open, and remain closed) will be triggered. ***Notes:*** • The door status (open, close, remain open, and remain closed) cannot be triggered at the same time. • The target door and the source door cannot be the same one.
Audio Play	Audio Play Status	The audio prompt will be triggered. The audio index related to the audio content will be played according to the configured play mode.

5. Click **Save** to save and take effect of the parameters.

7.10.3 Cross-Device Linkage

Purpose:
The actions of other access control device can be triggered by setting up a rule when the access control event is triggered.

Click **Cross-Device Linkage** tab to enter the following interface.

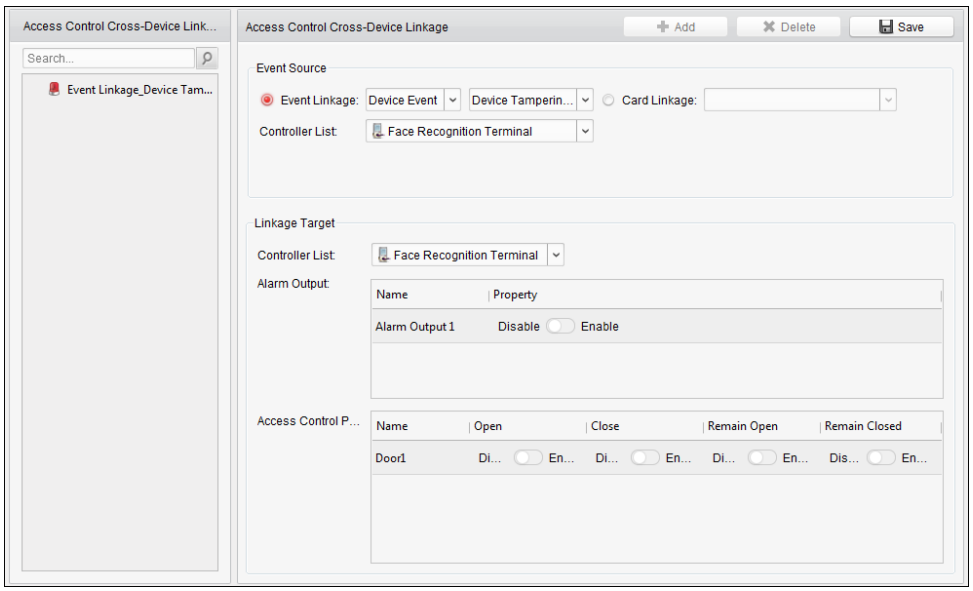


Figure 7-87: Cross-Device Linkage Configuration Page

Click **Add** button to add a new client linkage. Select the event source as **Event Linkage** or **Card Linkage.**

Event Linkage

For the event linkage, the alarm event can be divided into four types: device event, alarm input, door event, and card reader event.

1. Select the linkage type as **Event Linkage**, select the access control device as event source, and select the event type from the dropdown list.

   - For Device Event, select the detailed event type from the dropdown list.

- For Alarm Input, select the type as alarm or alarm recovery, and select the alarm input name from the table.
- For Door Event, select the detailed event type and select the door from the table.
- For Card Reader Event, select the detailed event type and select the card reader from the table.

2. Set the linkage target. Select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.
   - **Alarm Output:** The alarm output will be triggered for notification.
   - **Access Control Point:** The open, close, remain open, or remain closed door status will be triggered.

Note: The open, close, remain open, or remain closed door status cannot be triggered at the same time.

3. Click **Save** button to save parameters.

Card Linkage

1. Click to select the linkage type as **Card Linkage**.
2. Select the card from the dropdown list and select the access control device as event source.
3. Select the card reader from the table for triggering.
4. Set the linkage target, select the access control device from the dropdown list as the linkage target, and switch the property from to to enable this function.

   Alarm Output: The alarm output will be triggered for notification.
5. Click **Save** button to save parameters.

7.11 Door Status Management

Purpose:
The door status of the added access control device will be displayed in real time. Check the door status and the linked event(s) of the selected door. Control door status and set status duration.

7.11.1 Access Control Group Management

Purpose:
Before controlling the door status and setting the status duration, the door must be organized into a group for convenient management.

Perform the following steps to create the group for the access control device:

1. Click on the control panel to open the Device Management page.
2. Click **Group** tab to enter the Group Management interface.

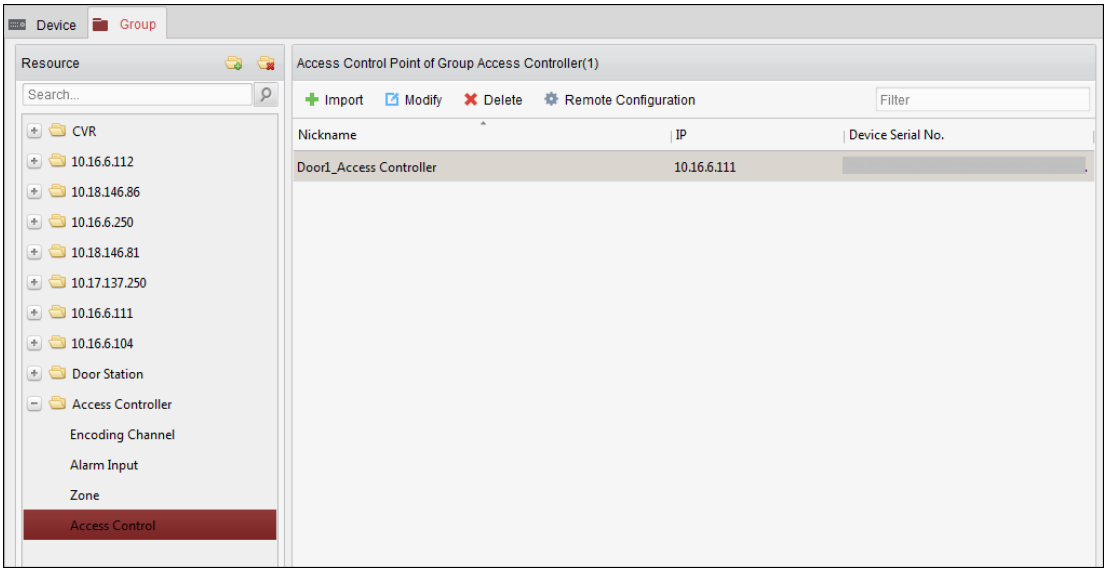


Figure 7-88: Group Management Interface

3. Perform the following steps to add the group.

   1) Click to open the Add Group dialog box.

   2) Input a group name.

   3) Click **OK** to add the new group to the group list.

      Check the **Create Group by Device Name** checkbox to create a new group according to the name of the selected device.

Figure 7-89: Group Addition Dialogue Box

4. Perform the following steps to import the access control points to the group:

   1) Click **Import** on Group Management interface, and then click the **Access Control** tab to open the Import Access Control page.

Notes:

- Select the **Alarm Input** tab and import the alarm inputs into group.
- For the Video Access Control Terminal, add the cameras as an encoding channel to the group.

   2) Select the names of the access control points in the list.

   3) Select a group from the group list.

   4) Click **Import** to import the selected access control points to the group.

Click **Import All** to import all the access control points to a selected group.

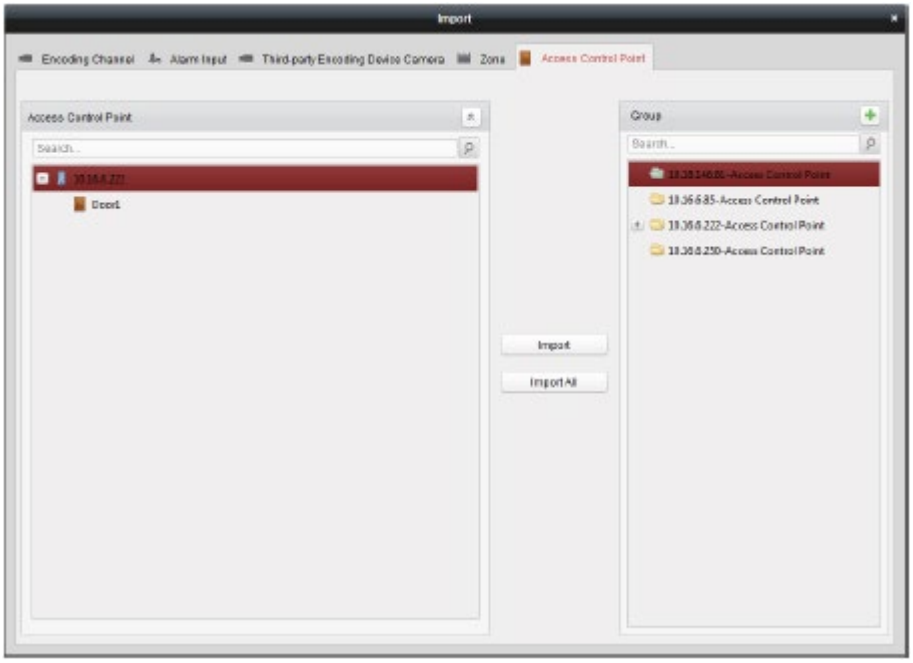


Figure 7-90: Alarm Import Page

5. After importing the access control points to the group, click or double-click the group/access control point name to modify it.

7.11.2 Anti-Control the Access Control Point (Door)

Purpose:
You can control the status for a single access control point (a door), including opening door, closing door, remaining open, and remaining closed.

Click the  icon on the control panel to enter the Status Monitor interface.

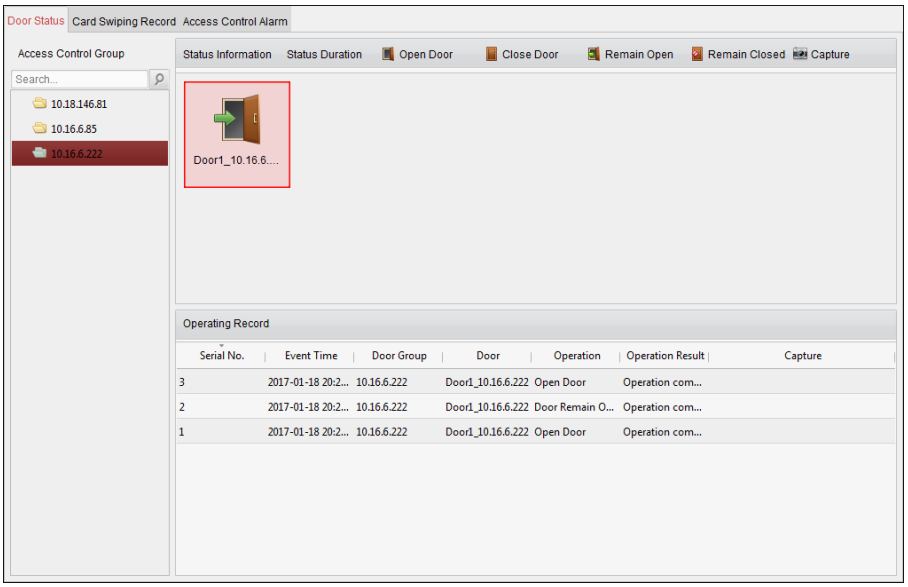


Figure 7-91: Status Monitoring Page

1. Select an access control group on the left. For managing the access control group, refer to *Chapter 7.11.1 Access Control Group Management.*

2. The access control points of the selected access control group will be displayed on the right. Click

the icon on the Status Information panel to select a door.

3. Click the following button listed on the **Status Information** panel to control the door.

Open Door: Click to open the door once.

Close Door: Click to close the door once.

Remain Open: Click to keep the door open.

Remain Closed: Click to keep the door closed.

Capture: Click to capture the picture manually.

4. You can view the anti-control operation result in the Operation Log panel.

Notes:

- Select the status as **Remain Open/Remain Closed**, the door will keep open/closed until a new anti-control command is made.
- The **Capture** button is available when the device supports capture function. The latter cannot be performed until the storage server is configured.
- If the door is in remain closed status, only a super card can open the door, or the door can be opened via the client software.

7.11.3 Status Duration Configuration

Purpose:
Schedule weekly time periods for an access control point (door) to remain open or remain closed.

In the Door Status module, click **Status Duration** button to enter the Status Duration interface.

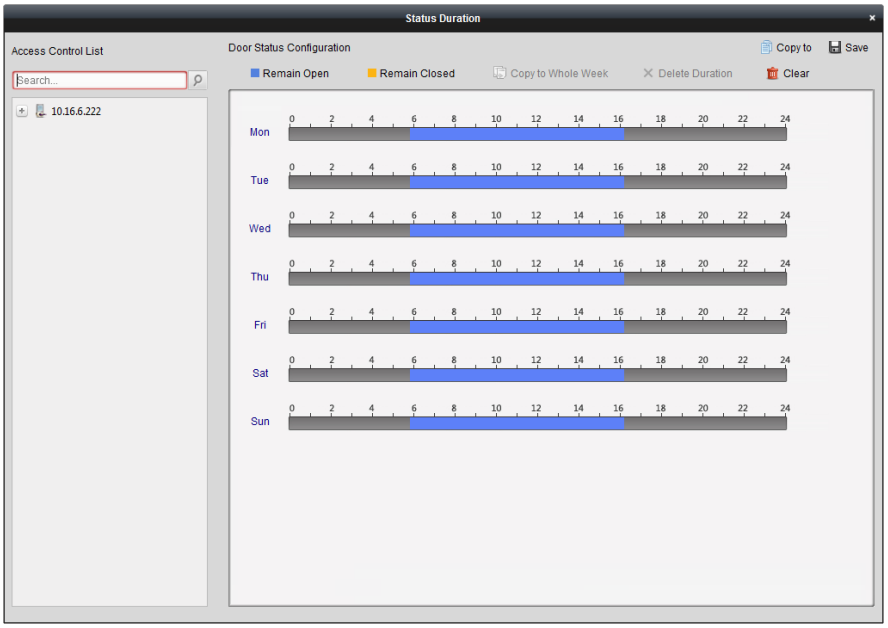


Figure 7-92: Door Status Configuration Page

1. Click to select a door from the access control device list on the left.
2. On the Door Status Configuration panel on the right, draw a schedule for the selected door.

1) Select a door status brush as Remain Open or Remain Closed.

Remain Open: The door will keep open during the configured time period. The brush is marked as .

Remain Closed: The door will keep closed during the configured duration. The brush is marked as .

2) Click and drag on the timeline to draw a color bar on the schedule to set the duration.

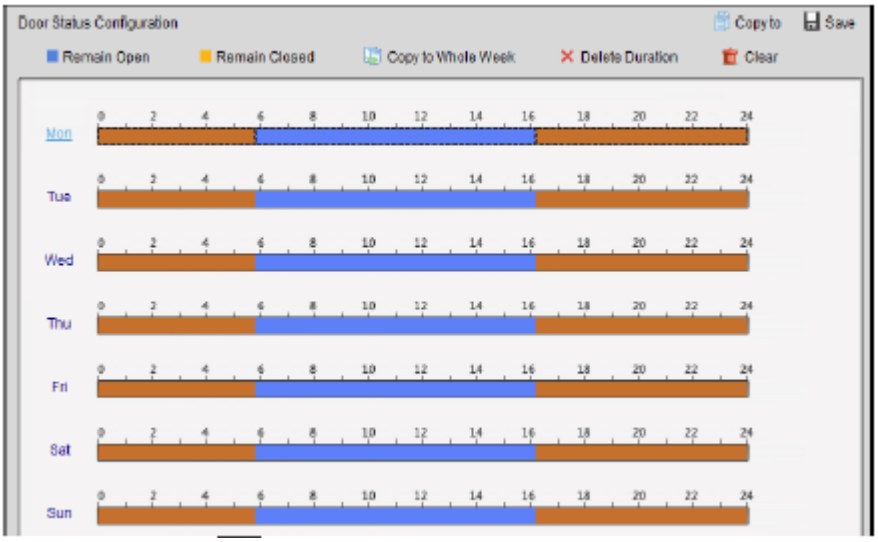


Figure 7-93: Door Status Configuration Page

3) When the cursor turns to , move the selected time bar that was just edited. Also, edit the displayed time point to set the accurate time period.

When the cursor turns to , lengthen or shorten the selected time bar.

3. Optionally, select the schedule time bar and click **Copy to Whole Week** to copy the time bar settings to the other days in the week.

4. Select the time bar and click **Delete Duration** to delete the time period. Alternatively, click **Clear** to clear all configured durations on the schedule.

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

6. Click **Copy to** button to copy the schedule to other doors.

7.11.4 Real-time Card Swiping Record

Click **Card Swiping Record** tab to enter the following interface.

The logs of card swiping records of all access control devices will be displayed in real time. View the details of the card swiping event, including card No., person name, organization, event time, etc.

Click the event to view the card holder details, including person No., person name, organization, phone, contact address, etc.

7.11.5 Real-time Access Control Alarm

Purpose:
The access control event logs will be displayed in real time, including device exception, door event, card reader event, and alarm input.

Click **Access Control Alarm** tab to enter the following interface.

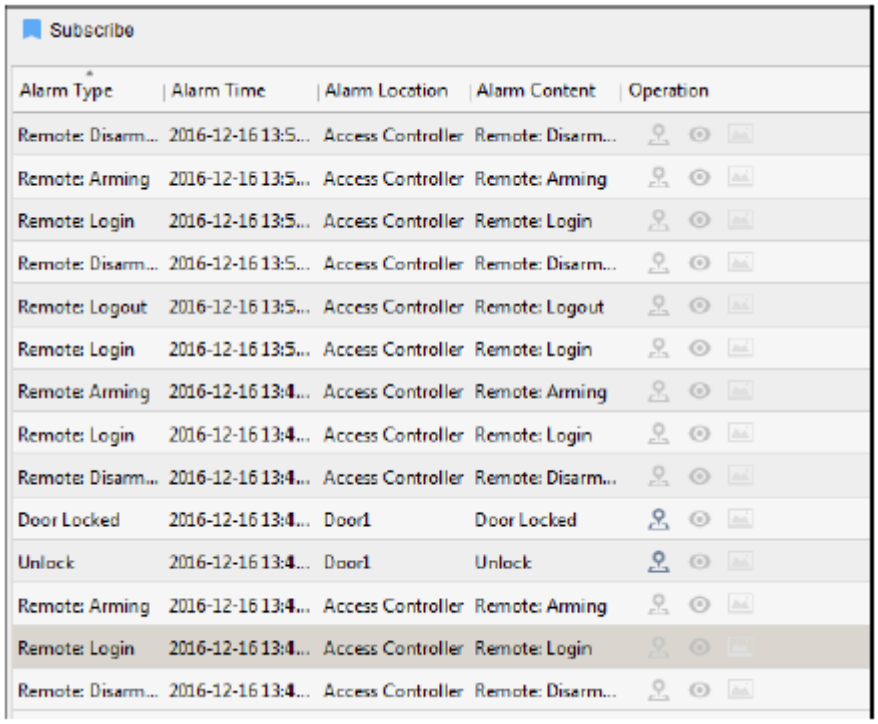


Figure 7-94: Real-Time Access Control Status Page

1. All access control alarms will be displayed in the list in real time. View the alarm type, alarm time, location, etc.
2. Click to view the alarm on E-map.
3. Click or to view the live view or the captured picture of the triggered camera when the alarm is triggered.

Note: To set the triggered camera, refer to *Chapter 7.10.1 Access Control Event Linkage.*

4. Click **Subscribe** to select the alarm that the client can receive when the alarm is triggered.

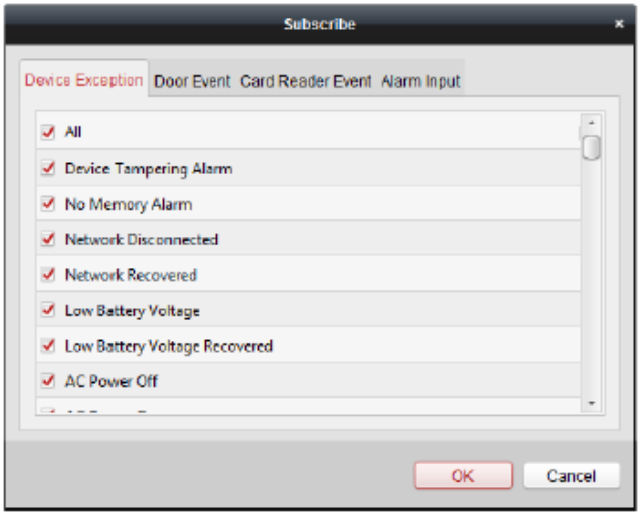


Figure 7-95: Client Alarm Subscription Box

1) Check the checkbox(es) to select the alarm(s), including device exception alarm, door event alarm, card reader alarm, and alarm input.

2) Click **OK** to save the settings.

7.12 Arming Control

Purpose:
Arm or disarm the device. After arming the device, the client can receive the alarm information from the device.

1. Click **Tool->Device Arming Control** to display the Device Arming Control window.

2. Arm the device by checking the corresponding checkbox.

Then the alarm information will be auto uploaded to the client software when the alarm occurs.

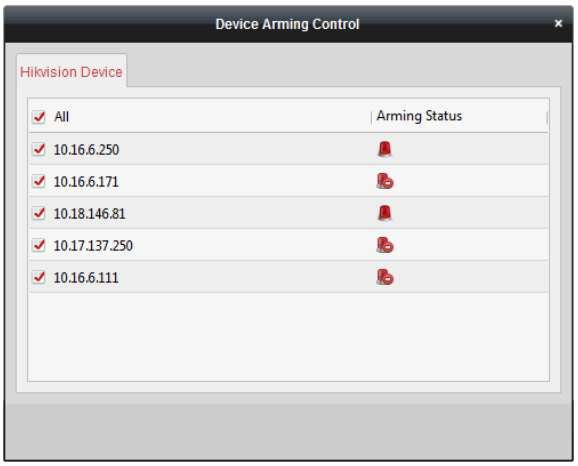


Figure 7-96: Device Arming Control Page

7.13 Time and Attendance

Purpose:
The Time and Attendance module provides multiple functionalities, including shift schedule management, attendance handling, attendance statistics and other advanced functions.

Before you start:
Add the organization and person in the Access Control module. For details, refer to *Chapter 7.4.1 Adding Organization* and *Chapter 7.5.1 Adding Person.*

Perform the following steps to access the Time and Attendance module. Click to enter the Time and Attendance module, as follows:

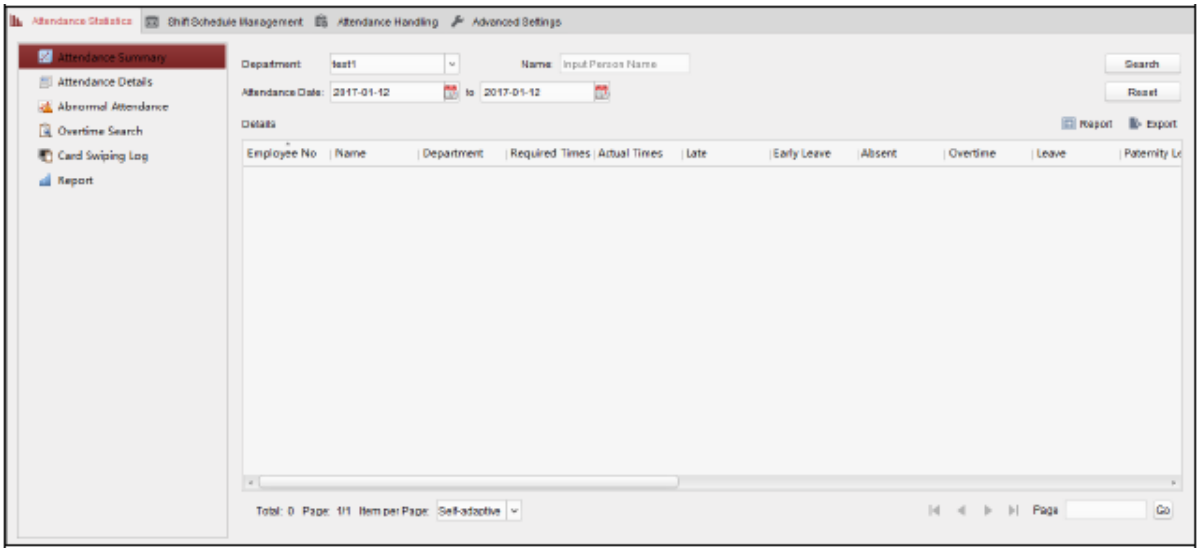


Figure 7-97: Attendance Statistics Page

7.13.1 Shift Schedule Management

Open the Time and Attendance module and click **Shift Schedule Management** to enter the Shift Schedule Management interface.

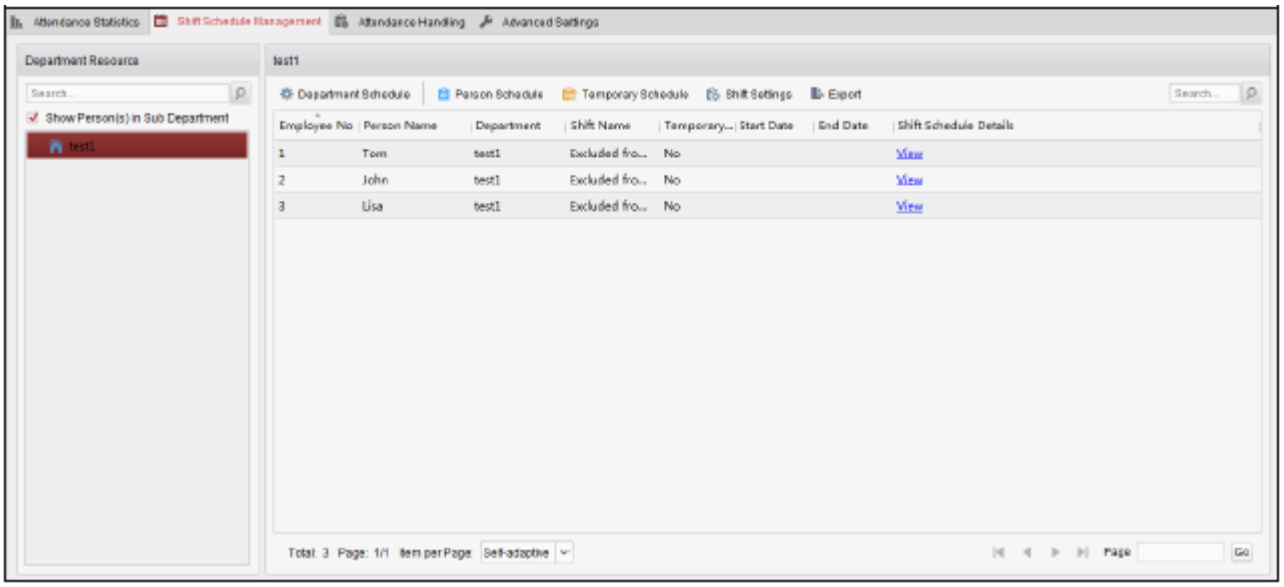


Figure 7-98: Shift Schedule Management Page

Shift Settings

Purpose:
Add a time period and shift for the scheduled shift. Click **Shift Settings** to display the Shift Settings dialog box.

Adding Time Period

1. Click **Time Period** tab.
2. Click **Add**.

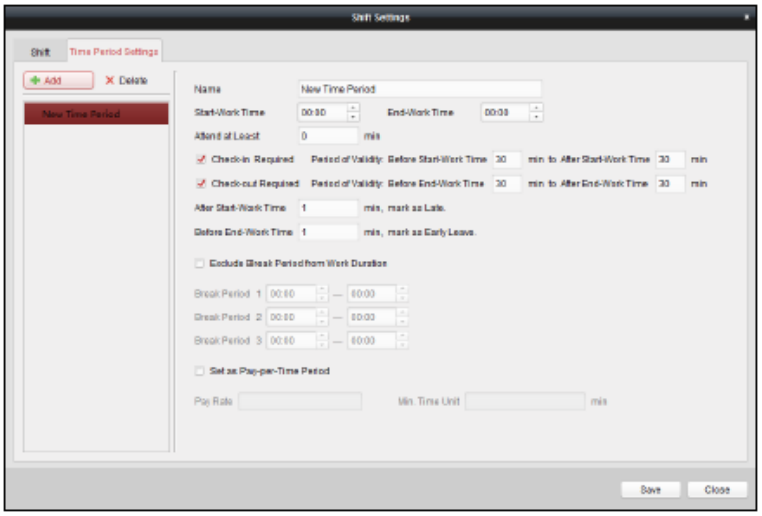


Figure 7-99: Time Period Addition Page

3. Set the related parameters.

Name: Set the name for time period.

Start-Work/End-Work Time: Set the start-work time and end-work time.

Attend at Least: Set the minimum attendance time.

Check-in / Check-out Required: Check the checkboxes and set the valid period for check-in or check-out.

Mark as Late/Mark as Early Leave: Set the time period for late or early leave.

Exclude Break Period from Work Duration: Check the checkbox and set the break period that is to be excluded.

Note: Up to 3 break periods can be set.

Set as Pay-per-Time Period: Check the checkbox and set the pay rate and minimum time unit.

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

The added time period will display on the left panel of the dialog box.Click **Delete** to delete the time period.

Adding Shift

1. Click **Shift** Tab.
2. Click **Add**.

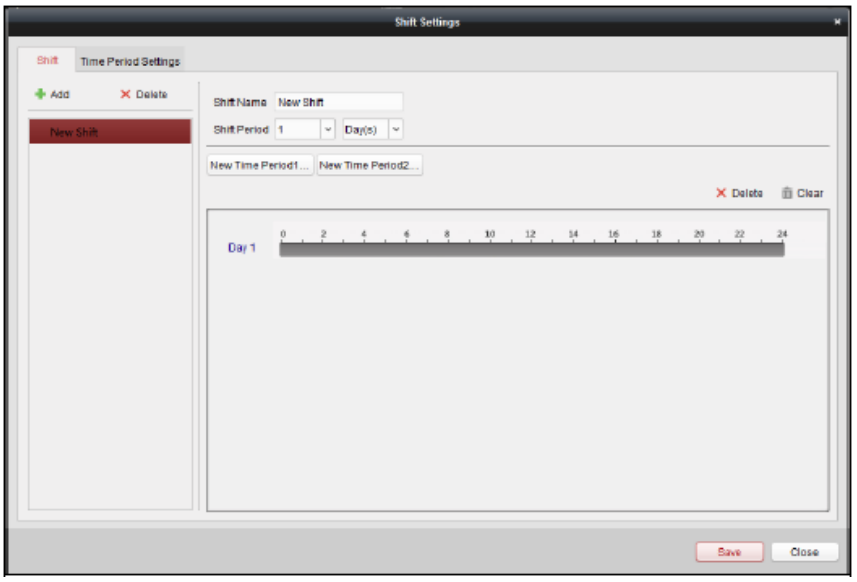


Figure 7-100: Shift Addition Page

3. Set the name for the shift.
4. Select the shift period from the drop-down list.
5. Configure the shift period with the added time period.
    1) Select the time period.
    2) Click the time bar to apply the time period for the selected day.

Click the time period on the bar and click ✕ or **Delete** to delete the period. Click **Clear** to delete all time periods for a given day.

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

The added shift will be displayed on the left panel of the dialog box. Click **Delete** on the left panel to delete the shift.

Shift Schedule Settings

Purpose:
After setting the shift, set the department schedule, person schedule, and temporary schedule.

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

Department Schedule
Set the shift schedule for one department, and all the persons in the department will be assigned with the shift schedule.

Note: In the Time and Attendance module, the department list is the same with the **organization** in Access Control. For setting the organization in Access Control, refer to *Chapter 7.4 Organization Management.*

1. Open the Shift Schedule Management interface and select the department on the left panel.
2. Click **Department Schedule** to display the Department Schedule dialog box.

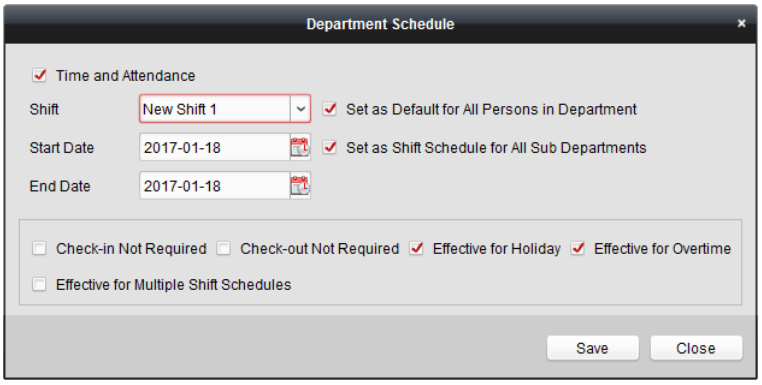


Figure 7-101: Department Schedule Configuration Page

3. Check the **Time and Attendance** checkbox.

All persons in the department, except those excluded from attendance, will have the attendance schedule applied to them.

4. Select the shift from the drop-down list.

5. Set the start date and end date.

6. (Optional) Set other parameters for the schedule.

Select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.

Notes:

- Multiple Shift Schedules contain more than one time periods. The person can check in/out in any of the time periods and the attendance will be effective.

Example: 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.

- After checking the **Effective for Multiple Shift Schedules** checkbox, select the effective time period(s) from the added time periods for the persons in the department.

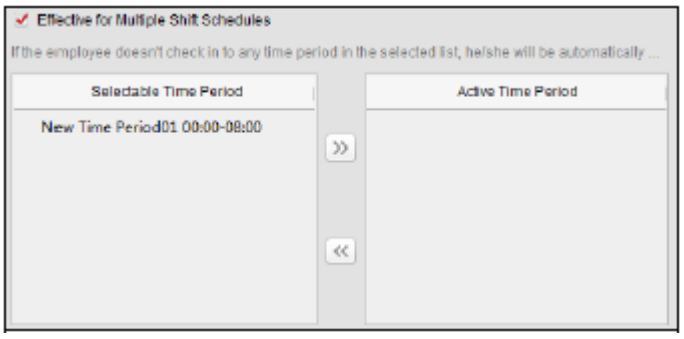


Figure 7-102: Effective for Multiple Shift Schedules Page

1) In the Selectable Time Period list on the left, click the added time period and click » to add it to the right.

2) (Optional) To remove the selected time period, select it and click «.

7. (Optional) Check **Set as Default for All Persons in Department** checkbox. All persons in the department will use this shift schedule by default.

8. (Optional) If the selected department contains sub department(s), the Set as **Shift Schedule for All Sub Departments** checkbox will display. Check it to apply the department schedule to its sub departments.

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

Person Schedule

1. Open the Shift Schedule Management interface and select the department on the left panel.

2. Select the person(s) on the right panel.

3. Click **Person Schedule** to display the Person Schedule dialog box.

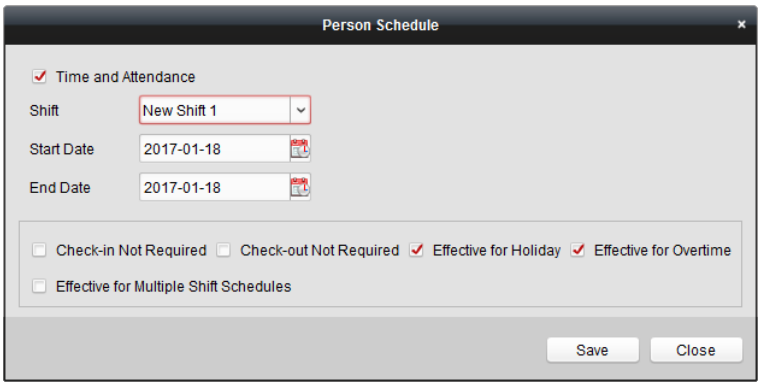


Figure 7-103: Person Schedule Page

4. Check **Time and Attendance** checkbox.

The configured person will apply the attendance schedule.

5. Select the shift from the drop-down list.

6. Set the start date and end date.

7. (Optional) Set other parameters for the schedule.

Select Check-in Not Required, Check-out Not Required, Effective for Holiday, Effective for Overtime, Effective for Multiple Shift Schedules.

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

Temporary Schedule

1. Open the Shift Schedule Management interface and select the department on the left panel.

2. Select the person(s) on the right panel.

3. Click **Temporary Schedule** to display the Temporary Schedule dialog box.

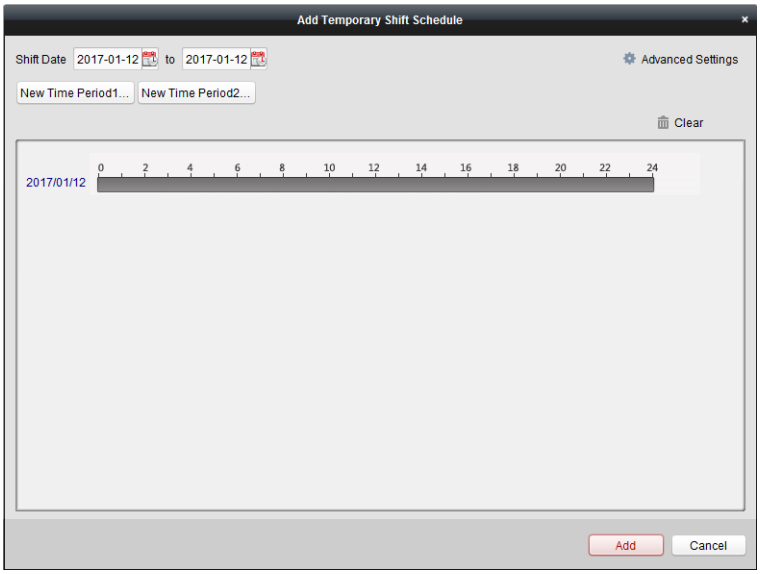


Figure 7-104: Add Temporary Shift Schedule Page

4. Click to set the shift date.

5. Configure the shift date with the added time period.

    1) Select the time period.

    2) Click the time bar to apply the time period for the select date.

Click the time period on the bar and click to delete the period. Also, click **Clear** to delete all days in a time period.

6. Click **Advanced Settings** to advanced attendance rules for the temporary schedule.

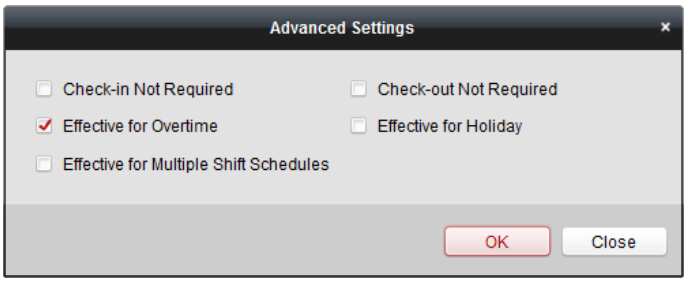


Figure 7-105: Advanced Shift Schedule Settings Page

7. Click **Add** to save the settings.

Checking Shift Schedule Details

1. On the Shift Schedule Management interface, select the department on the left panel.

2. Select the person(s) on the right panel.

3. Click **View** to display Shift Schedule Details dialog box. Check the shift schedule details.

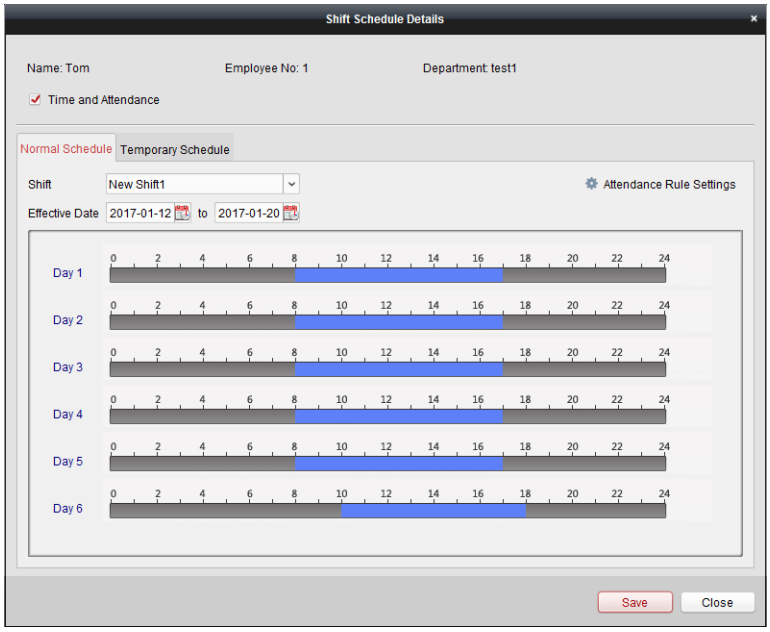


Figure 7-106: Shift Schedule Details Box

4. Click **Normal Schedule** tab.

Check and edit the normal schedule details.

1) Select the shift from the drop-down list.

2) Click **Attendance Rule Settings** to display the Attendance Rule Settings dialog box.

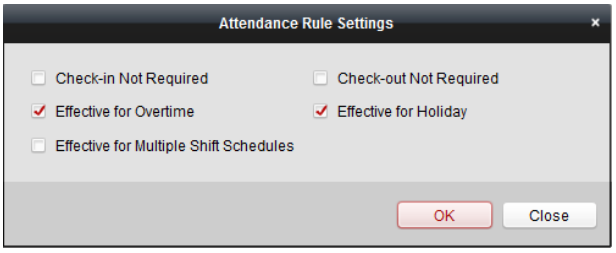


Figure 7-107: Attendance Rule Settings Box

You can check the attendance rules as desired and click **OK** to save the settings.

1) Click to set the effective date.

2) Click **Save** to save the settings.

5. (Optional) Click **Temporary Schedule** tab.

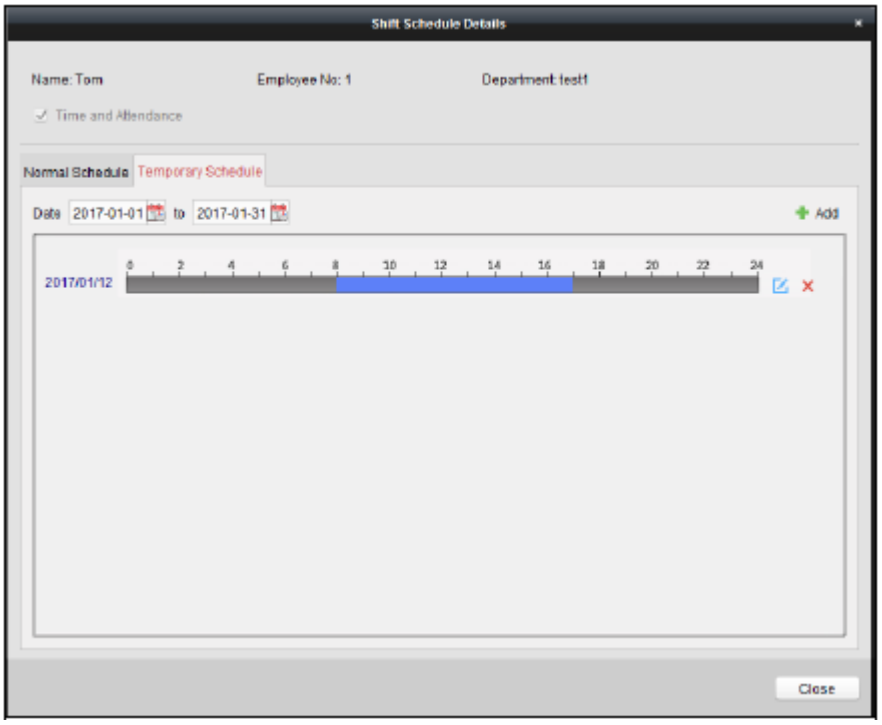


Figure 7-108: Shift Schedule Details Page

Check and edit the temporary schedule details.

(Optional) Click **Add** to add temporary schedule for the selected person.

(Optional) Click to edit the time period.

(Optional) Click to delete the temporary schedule.

Exporting Shift Schedule Details
In the Shift Schedule Management interface, select the department on the left panel and click **Export** to export all persons' shift schedule details to local PC.

Note: The exported details are saved in *.csv format.

7.13.2 Attendance Handling

Purpose:
Handle attendance functionalities, including check-in correction, check-out correction, leave and business trip, and manual attendance calculation.

Open the Time and Attendance module and click **Attendance Handling** to enter the Attendance Handling interface.

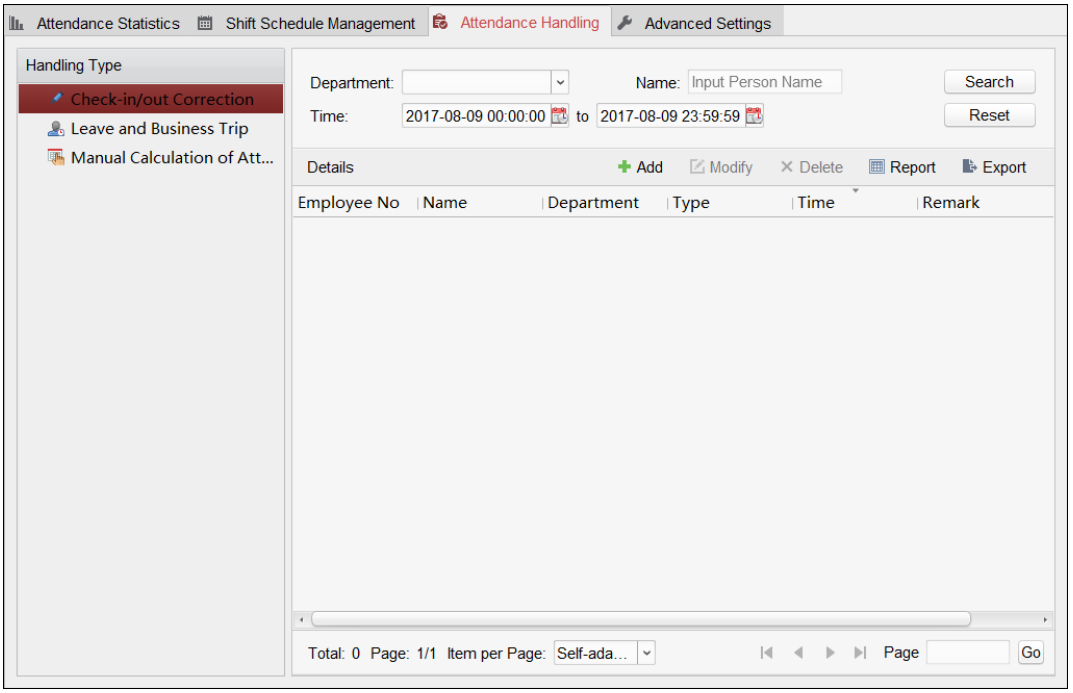


Figure 7-109: Attendance Handling Configuration Page

Check-in/out Correction

Purpose:
Add, edit, delete, search in the check-in/out correction and generate reports. Export the check-in/out correction details to a local PC.

Add Check-in/out Correction

1. Click the **Check-in/out Correction** tab.
2. Click **Add** to display Add Check-in/out Correction dialog box.

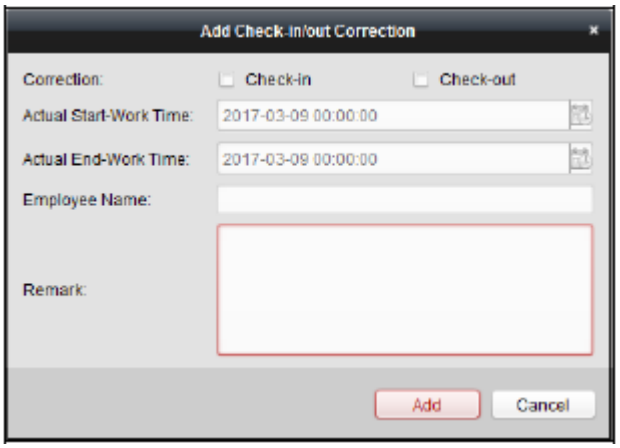


Figure 7-110: Check-in/out Correction Box

3. Set the check-in/out correction parameters.

For Check-in Correction: Check the **Check-in** checkbox and set the actual start-work time.

For Check-out Correction: Check the **Check-out** checkbox and set the actual end-work time.

4. Click **Employee Name** field and select the person.

Input the keyword and click to search for a person.

5. (Optional) Enter related information.
6. Click **Add** to add the check-in/out correction.

The added check-in/out correction will display on the Attendance Handling interface.

(Optional) Select the check-in/out correction and click **Modify** to edit the correction.

(Optional) Select the check-in/out correction and click **Delete** to delete the correction.

(Optional) Click **Report** to generate the check-in/out correction report.

(Optional) Click **Export** to export the check-in/out correction details to local PC.

Note: The exported details are saved in *.csv format.

Search Check-in/out Correction

1. Click **Check-in/out Correction** tab.
2. Set the searching conditions.

Department: Select the department from the drop-down list.

Name: Input the person name.

Time: Click to set the specified time as time range.

3. Click **Search** to search the check-in/out corrections.

The check-in/out correction details will display on the list. You can also click **Reset** to reset the searching conditions.

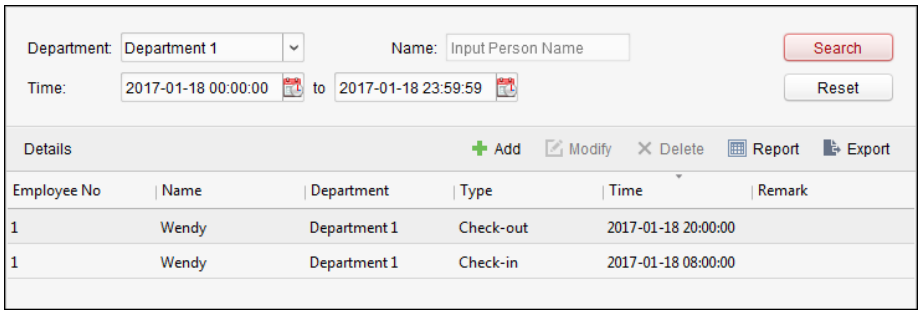


Figure 7-111: Check-in/out Search Page

Leave and Business Trip

Purpose:
Add, edit, delete, search for leave and business trip information, and generate reports. Export the leave and business trip details to local PC.

Add Leave and Business Trip

1. Click **Leave and Business Trip** tab.

2. Click **Add** to display Add Leave and Business Trip Application dialog box.

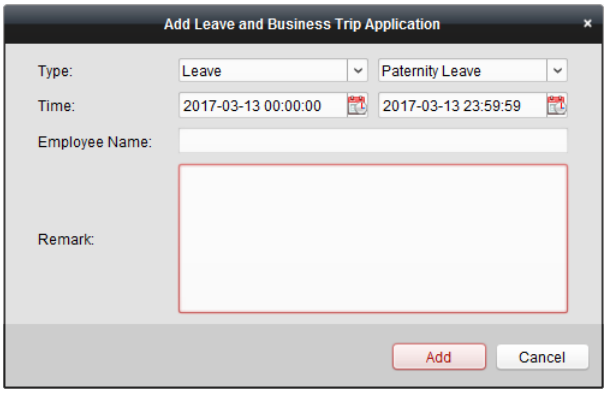


Figure 7-112: Leave and Business Trip Application Box

3. Select the leave and business trip type from the Type drop-down list.

Configure the leave type in Advanced Settings. For details, refer to *Chapter 0 Leave Type Settings*.

4. Click to set the specified time as a timerange.

5. Click the **Employee Name** field and select the person for this application.

Input the keyword and click to search for a person.

6. (Optional) Enter relevant information.

7. Click **Add** to add the leave and business trip.

The added leave and business trip will display on the Attendance Handling interface. (Optional) Select the leave and business trip and click **Modify** to edit the leave or business trip.

(Optional) Select the leave and business trip and click **Delete** to delete the leave or business trip.

(Optional) Click **Report** to generate the leave or business trip report. (Optional) Click **Export** to export the leave or business trip details to local PC.

Note: The exported details are saved in *.csv format.

Search Leave and Business Trip

1. Click **Leave and Business Trip** tab.

2. Set the searching conditions.

Department: Select the department from the drop-down list.

Name: Input the person name.

Time: Click to set the specified time as time range.

3. Click **Search** to search the leave and business trips.

The leave and business trip details will display on the list. You can also click **Reset** to reset the searching conditions.

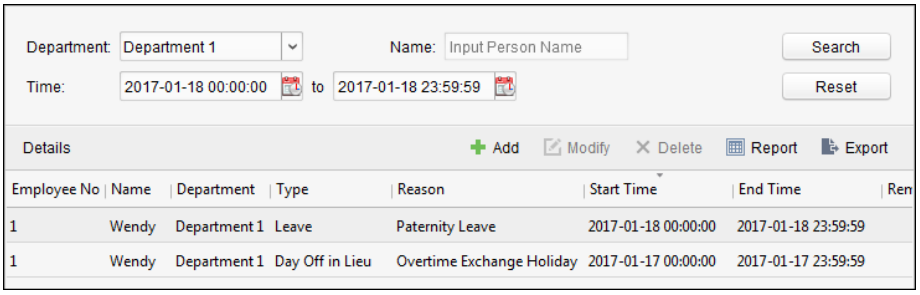


Figure 7-113: Leave and Business Trip Search Page

Manual Calculation of Attendance

Purpose:
Calculate the attendance result manually by specifying the start time and end time.

1. Click **Manual Calculation of Attendance** tab.
2. Set the start time and end time for calculation.
3. Click **Calculate** to start.

Note: Only attendance data for the past three months can be calculated.

7.13.3 Advanced Settings

Purpose:
Configure basic settings, attendance rules, attendance check points, holiday settings, and leave types for attendance.

Open the Time and Attendance module and click **Advanced Settings** to enter the Advanced Settings interface.

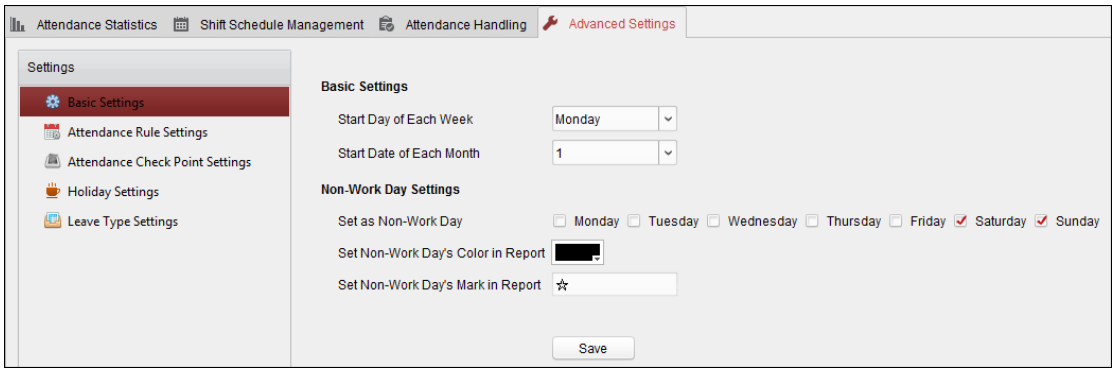


Figure 7-114: Advanced Settings Page

Basic Settings

1. Click **Basic Settings** tab to enter the Basic Settings interface.

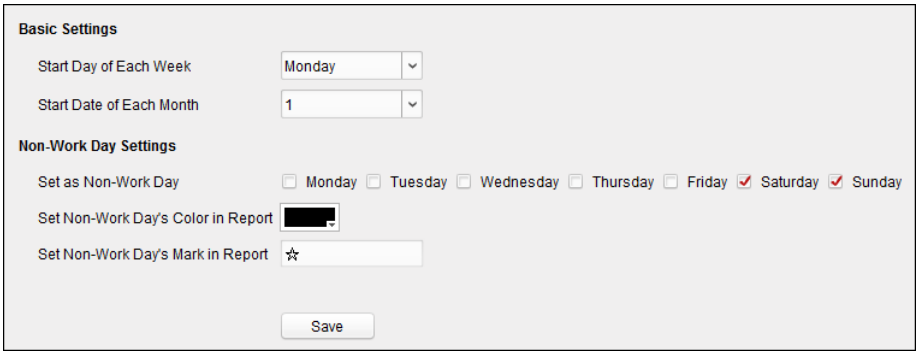


Figure 7-115: Basic Settings Page

2. Set the basic settings.

   Start Day of Each Week: Select a day as the start day of each week.

   Start Date of Each Month: Select a day as the start date of each month.

3. Set the non-work day settings.

   Set as Non-Work Day: Check the checkbox(es) to set the selected day(s) as a non-work day.

   Set Non-Work Day's Color in Report: Click the color field and select the color to mark a non-work day in the report.

   Set Non-Work Day's Mark in Report: Input the mark as non-work day in the report.

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

Attendance Rule Settings

1. Click **Attendance Rule Settings** tab to enter the Attendance Rule Settings interface.

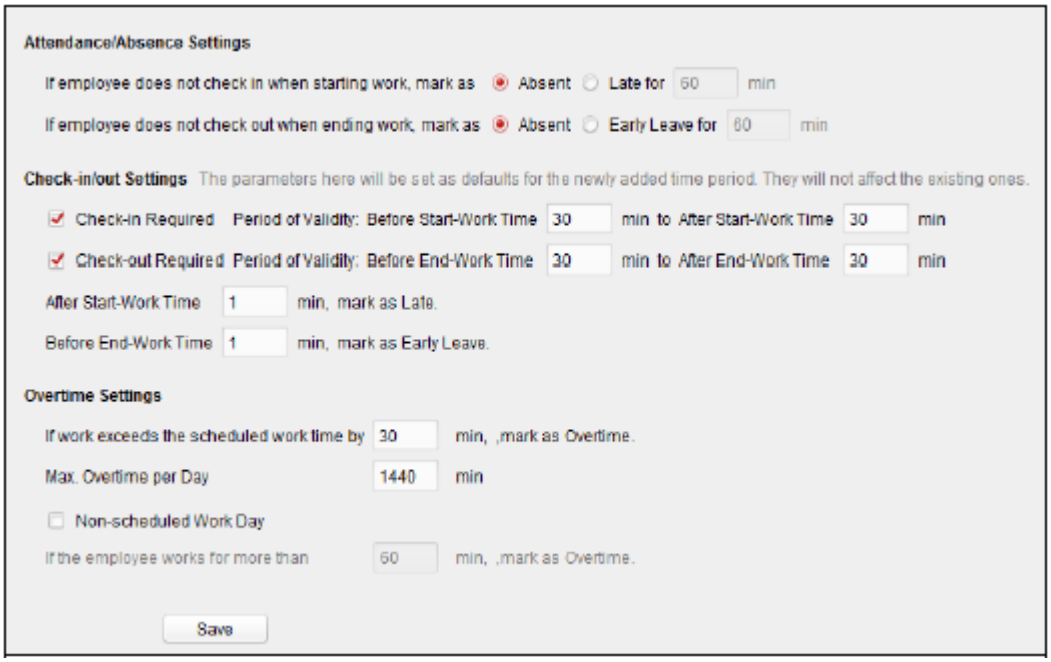


Figure 7-116: Attendance Rule Settings Page

2. Set attendance or absence settings.

If the employee does not check in when starting work, they can be marked as **Absent** or **Late**, and the

late time can be set.

If the employee does not check out when ending work, **Absent** or **Early Leave** can be selected, and early leave duration can be selected.

3. Set Check-in/out Settings.

Check **Check-in Required** or **Check-out Required** and set a valid period.

Set the late rule or early leave rule.

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

4. Set the overtime settings.

Set the overtime rule and set the maximum overtime for each day.

(Optional) Check the **Non-scheduled Work Day** checkbox and set the overtime rule for a non-work day.

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

Attendance Check Point Settings

Set the card reader(s) of the access control point as the attendance check point, so that the card will be valid on other card reader(s) for attendance purposes.

1. Click **Attendance Check Point Settings** tab to enter the Attendance Check Point Settings interface.

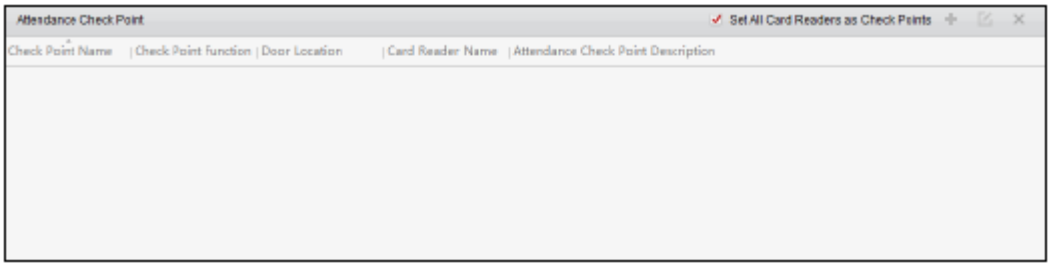


Figure 7-117: Attendance Checkpoint Settings Page

2. Click + to display Add Attendance Check Point dialog box.

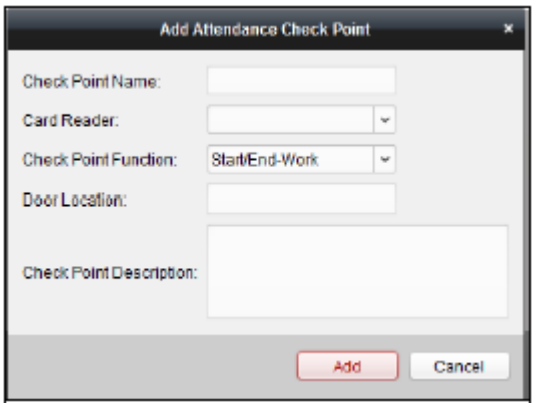


Figure 7-118: Attendance Checkpoint Settings Box

3. Set the related information.

Check Point Name: Input a name for the check point.

Card Reader: Select the card reader from the drop-down list.

Check Point Function: Select the function for the check point.

Door Location: Input the door location.

Check Point Description: Set the description information for the check point.

4. Click **Add** to add the attendance check point.

The added attendance check point will be displayed on the list.

5. (Optional) Check the **Set All Card Readers as Check Points** checkbox. It is possible to use all card readers as check points.

Note: If this checkbox is unchecked, only the card readers in the list will be added as attendance check points.

Edit or delete the card readers.

Click to edit the card reader.

Click to delete the card reader.

Holiday Settings

1. Click **Holiday Settings** tab to enter the Holiday Settings interface.

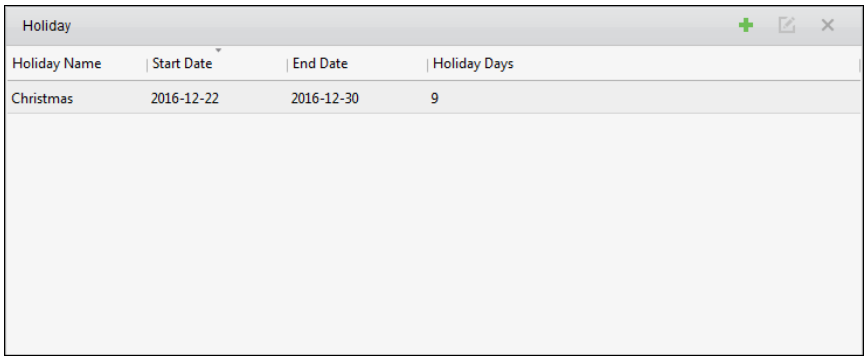


Figure 7-119: Holiday Settings Page

2. Click to display Add Holiday dialog box.

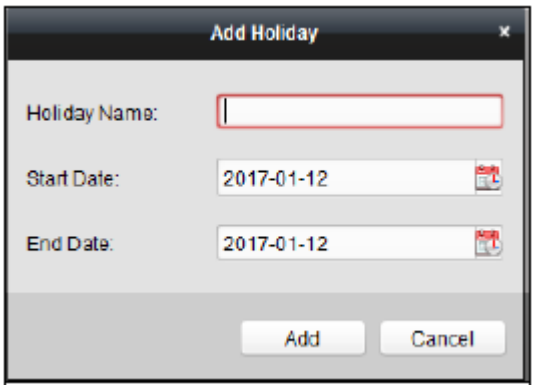


Figure 7-120: Holiday Addition Box

3. Set the related parameters.

Holiday Name: Input the name for the holiday.

Start Date/End Date: Click to specify the holiday date.

4. Click **Add** to add the holiday.

The added holiday will display on the list.

Edit or delete the holiday.

Click to edit the holiday.

Click to delete the holiday.

Leave Type Settings

Purpose

1. Click **Leave Type Settings** tab to enter the Leave Type Settings interface.

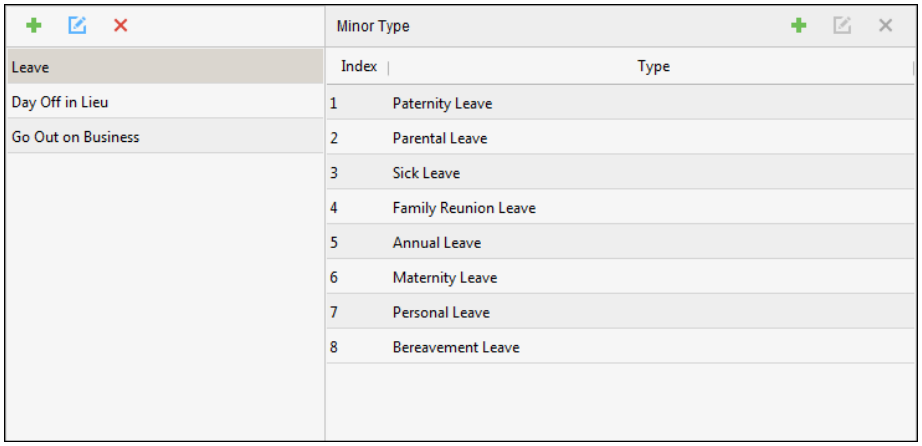


Figure 7-121: Leave Type Settings Page

2. Add the major leave type.

    1) Click on the left panel to display the Add Major Leave Type dialog box.

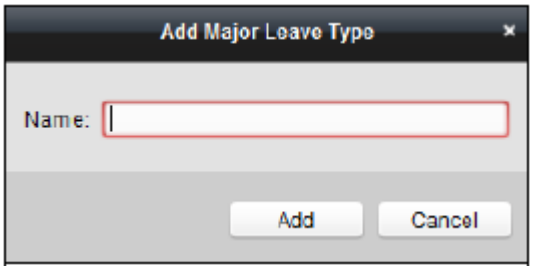


Figure 7-122: Major Leave Type Addition Box

    2) Input the name for major leave type.

    3) Click **Add** to add the major leave type.

Edit or delete the major leave type.

Click to edit the major leave type.

Click to delete the major leave type.

3. Add the minor leave type.

    1) Select the major leave type.

The minor leave type belonging to this major leave type will display on the right panel.

    2) Click on the right panel to display the Add Minor Leave Type dialog box.

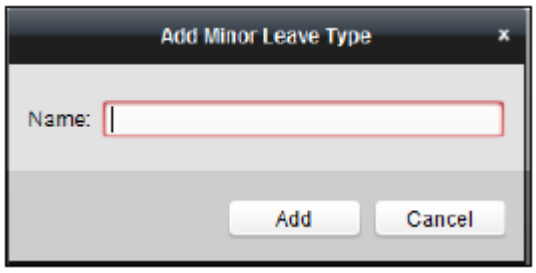


Figure 7-123: Minor Leave Type Addition Box

    3) Input the name for the minor leave type.

    4) Click **Add** to add the minor leave type.

Edit or delete the major leave type.

Click to edit the minor leave type.

Click to delete the minor leave type.

7.13.4 Attendance Statistics

Purpose:
After calculating attendance data, check the attendance summary, attendance details, abnormal attendance, overtime, card swiping logs, and reports based on the calculated attendance data.

Notes:

- The client automatically calculates the previous attendance data for the previous day at 1:00 am the next day.
- The client must be 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 *Manual Calculation of Attendance* in *Chapter 7.13.2 Attendance Handling*.

Attendance Summary

Purpose:
Obtain all attendance information statistics of the employees in the specified time period.

1. In the Time and Attendance module, click the **Attendance Statistics** tab to enter the Attendance Statistics page.
2. Click the **Attendance Summary** item on the left panel to enter the Attendance Summary interface.

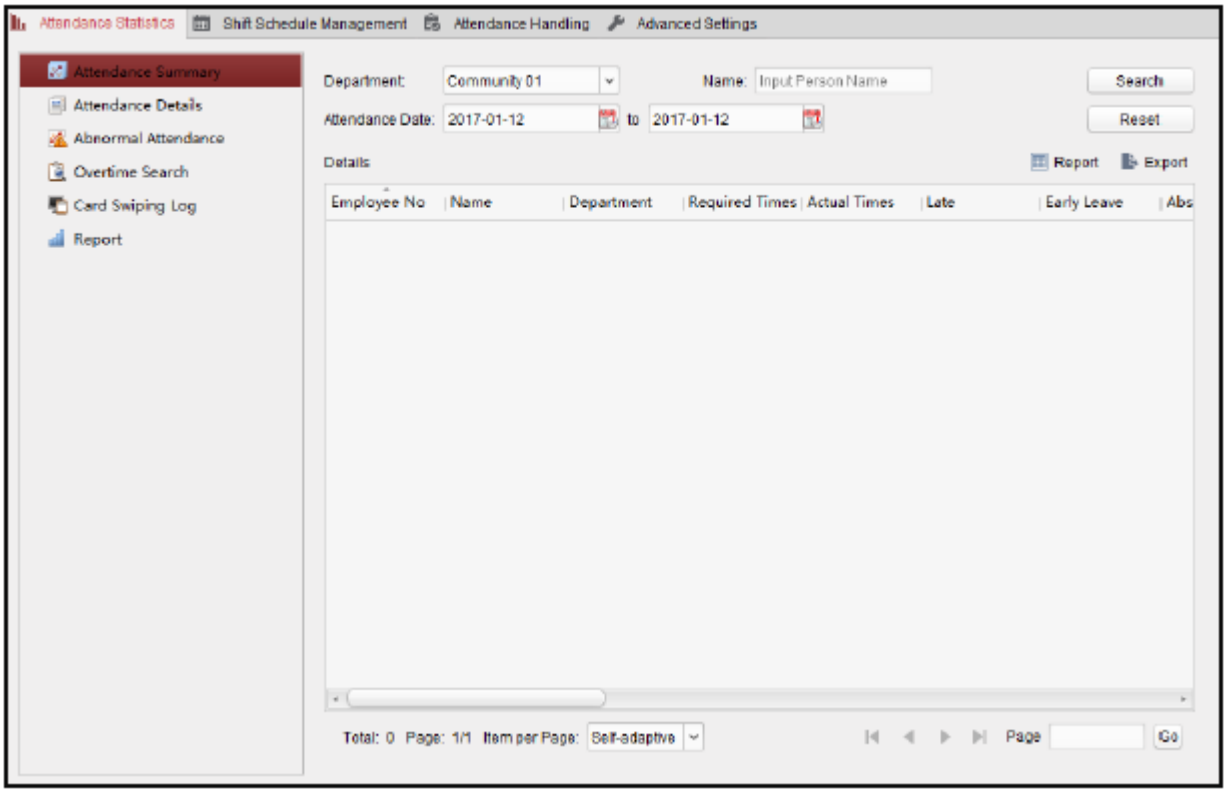


Figure 7-123: Attendance Summary Page

3. Set the search conditions, including department, employee name and attendance date.

(Optional) Click **Reset** to reset all the configured search conditions.

4. Click **Search** to start searching and the matched results will list on this page. (Optional) Click **Report** to generate the attendance report.

(Optional) Click **Export** to export the results to the local PC.

Attendance Details

1. In the Attendance Statistics page, click the **Attendance Details** item on the left panel to enter the Attendance Details interface.

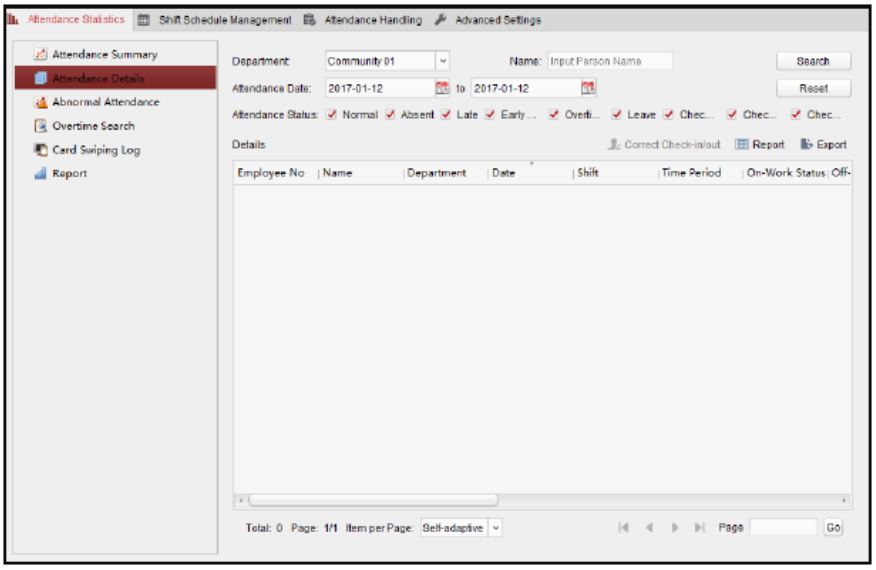


Figure 7-124: Attendance Details Page

2. Set the search conditions, including department, employee name, attendance date and status. (Optional) You can click **Reset** to reset all the configured search conditions.

3. Click **Search** to start searching and the matched results will list on this page.

(Optional) Select a result item in the list and click **Correct Check-in/out** to correct the check-in or check-out status.

(Optional) Click **Report** to generate the attendance report. (Optional) Click **Export** to export the results to the local PC.

Abnormal Attendance

Search and get the statistics regarding abnormal attendance data, including No., name and department of the employees, abnormal type, start/end time and date of attendance.

Overtime Search

Search and obtain the overtime status statistics of the selected employee in the specified time period. Check the detailed overtime information, including No., name and department of the employees, attendance date, overtime duration and overtime type.

Card Swiping Log

Search the card swiping logs used for the attendance statistics. After searching the logs, check the card swiping details, including name and department of the employees, card swiping time, card reader authentication mode and card No.

Report

In the Attendance Statistics page, click **Report** item on the left panel to enter the Report interface.

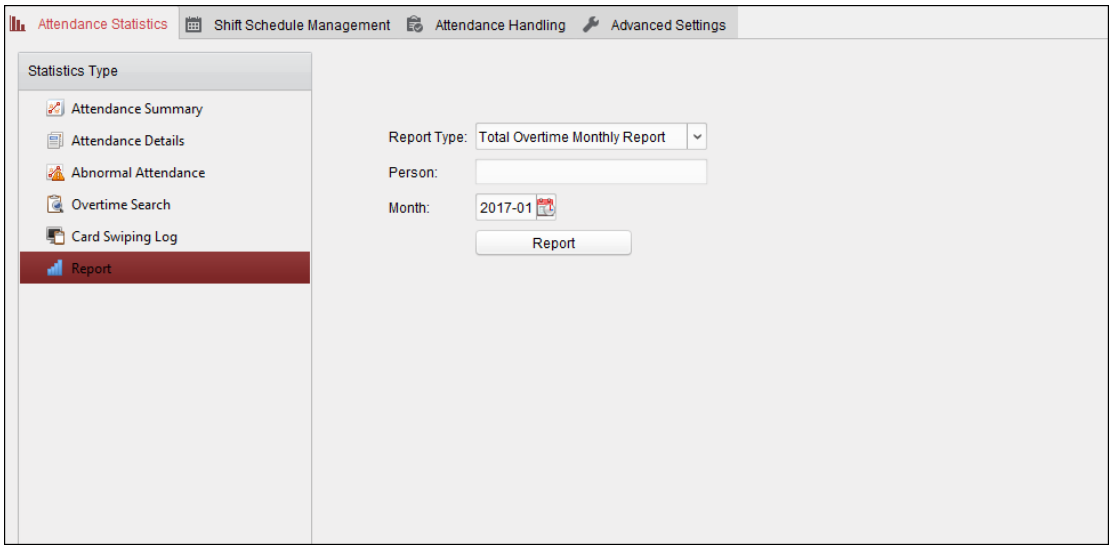


Figure 7-124: Attendance Statistics Page

Generating Total Overtime Monthly Report

1. Click in the Report Type field to unfold the drop-down list and select **Total Overtime Monthly Report** as the report type.

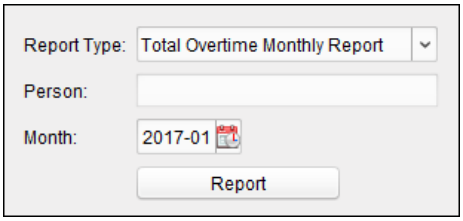


Figure 7-125: Total Overtime Monthly Report Generation Box

2. Click the **Person** field to select the person.
3. Click to specify amonth.
4. Click **Report** to start generating the matched total overtime monthly report.

Generating Overtime Details Monthly Report

Select **Overtime Details Monthly Report** as the report type. Generate a monthly overtime report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

Generating Attendance Monthly Report

Select **Attendance Monthly Report** as the report type. Generate a monthly attendance report. For detailed operations, refer to *Generating Total Overtime Monthly Report.*

Generating Start/End-Work Time Report

1. Click in the report type field to unfold the drop-down list and select **Start/End-Work Time Report** as the report type.
2. Click **Department** field to select the department.
3. Click to specify the start date and end date of a date period.
4. Click **Report** to start generating the matched total overtime monthly report.

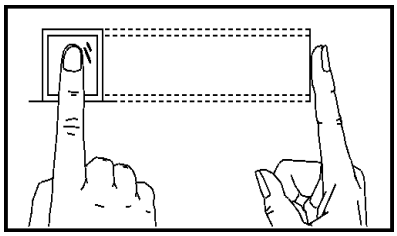
Generating Department Attendance Report

Set the report type as **Department Attendance Report** and generate the department attendance report. For detailed operations, refer to *Generating Start/End-Work Time Report* above.

Appendix A Tips for Scanning Fingerprint

Recommended Finger
Forefinger, middle finger or the third finger.

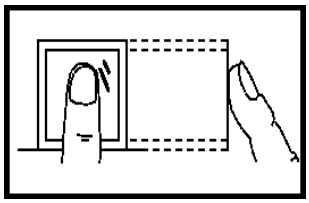
Correct Scanning
The figure displayed below is the correct way to scan your finger:



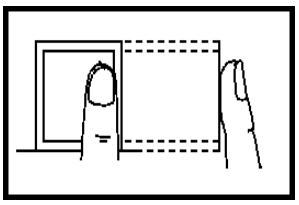
Press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning
The following images show incorrect ways of scanning your finger:

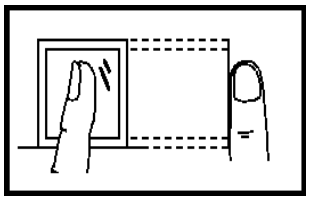
Vertical



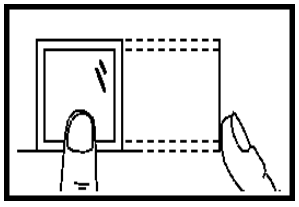
Edge I



Side



Edge II



Environment
The scanner should avoid direct high light, high temperature, humid conditions, and rain.

When environmental conditions are dry, the scanner may not recognize your fingerprint successfully. Clean your finger of any dust and scan it again after drying it.

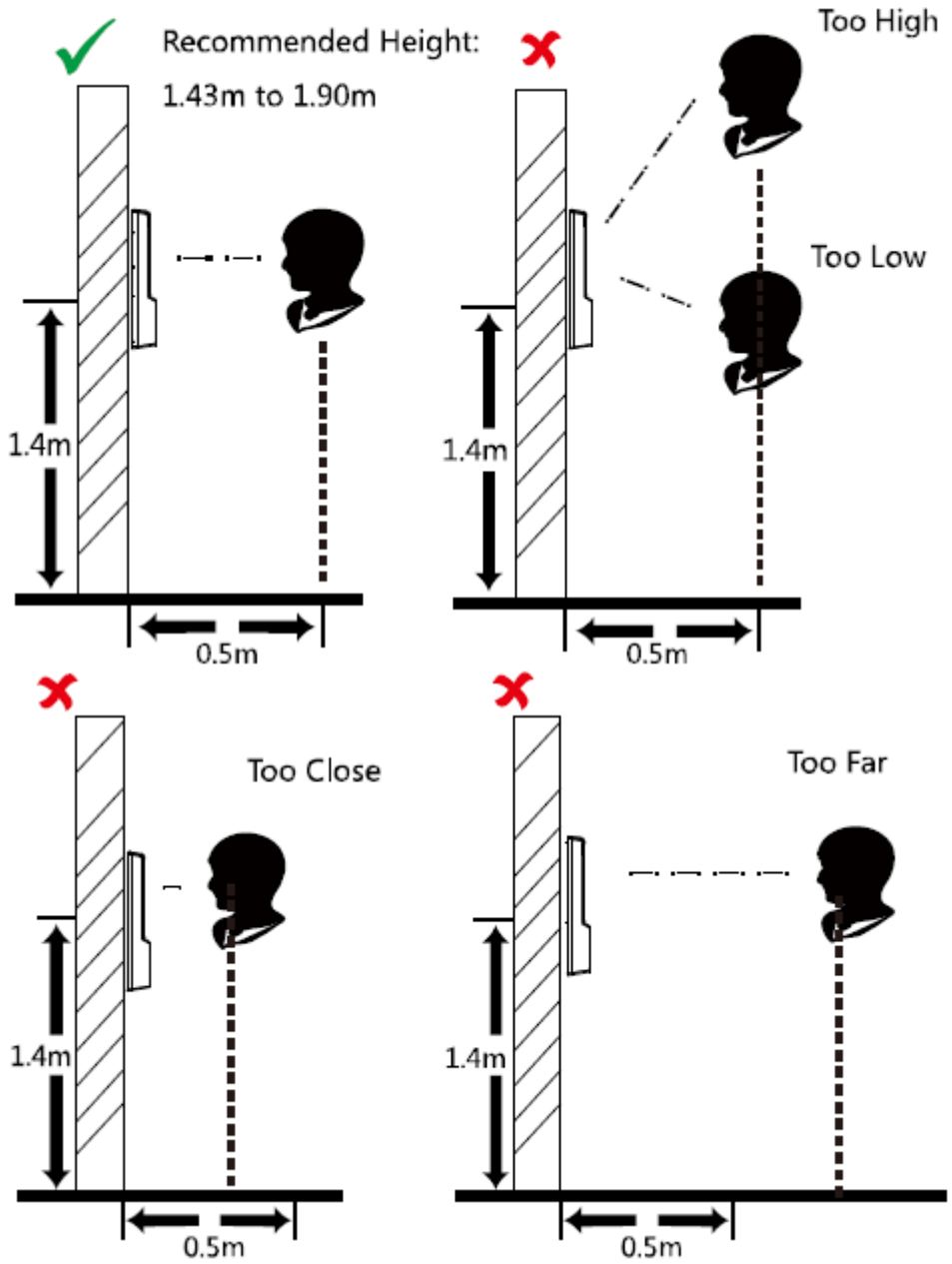
Others
If your fingerprint is shallow, or it is hard to scan your fingerprint, use other authentication methods.

If you have injuries on the scanned finger, the scanner may not recognize your fingerprint. Change to another finger and try again.

Appendix B Tips When Collecting/Comparing Face Picture

1. Positions (recommended distance: 0.5 m or 1.64 ft)

Pictures should be taken or compared from the following positions:



Note: For details on the relationship between a person's height, device height, and the distance between the person and the device, see Appendix C.

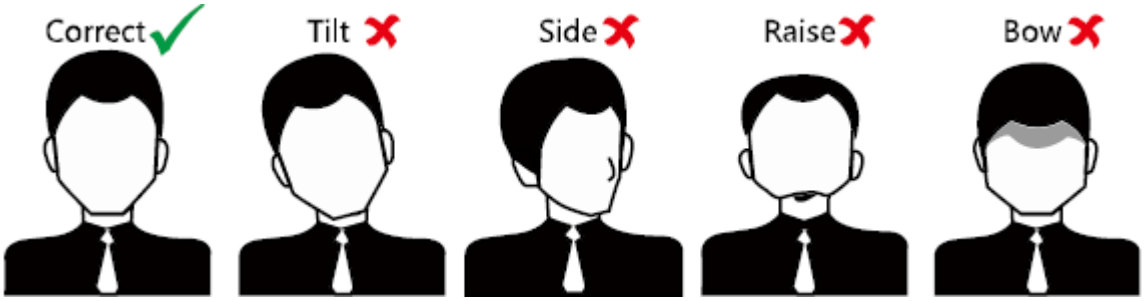
2. Expression

Keep your expression natural when collecting or comparing face pictures, just like the expression in the picture below.

- Do not wear a hat, sunglasses, or other accessories that can affect the facial recognition function.
- Ensure that your hair does not cover your eyes, ears, etc., and do not use heavy makeup.

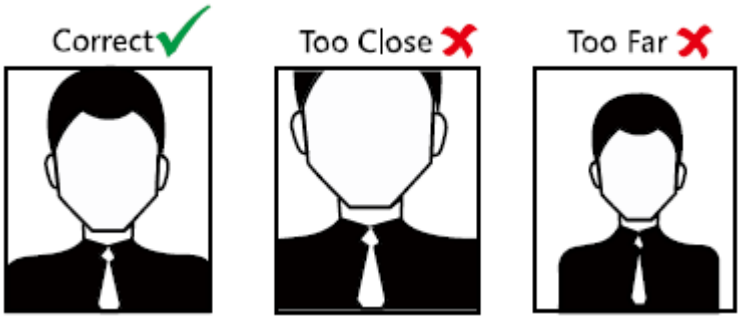
3. Posture

In order to obtain a good quality and accurate face picture, position your face while looking at the camera when collecting or comparing face pictures.



4. Size

Make sure that your face is in the middle of the collecting window.



Appendix C Tips for Installation Environment

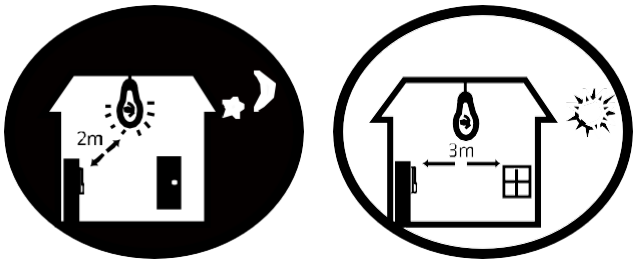
1. Light Source Illumination Reference Value

Candle: 10 lux

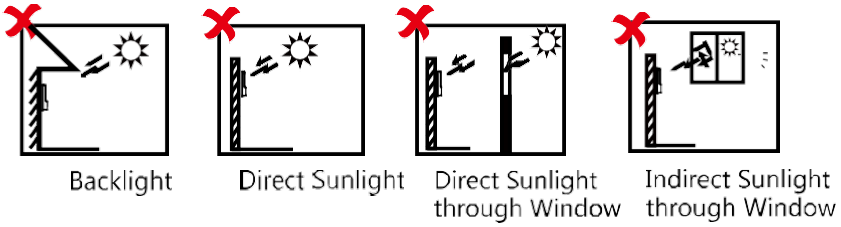
Bulb: 100 to 850 lux

Sunlight: more than 1200 lux

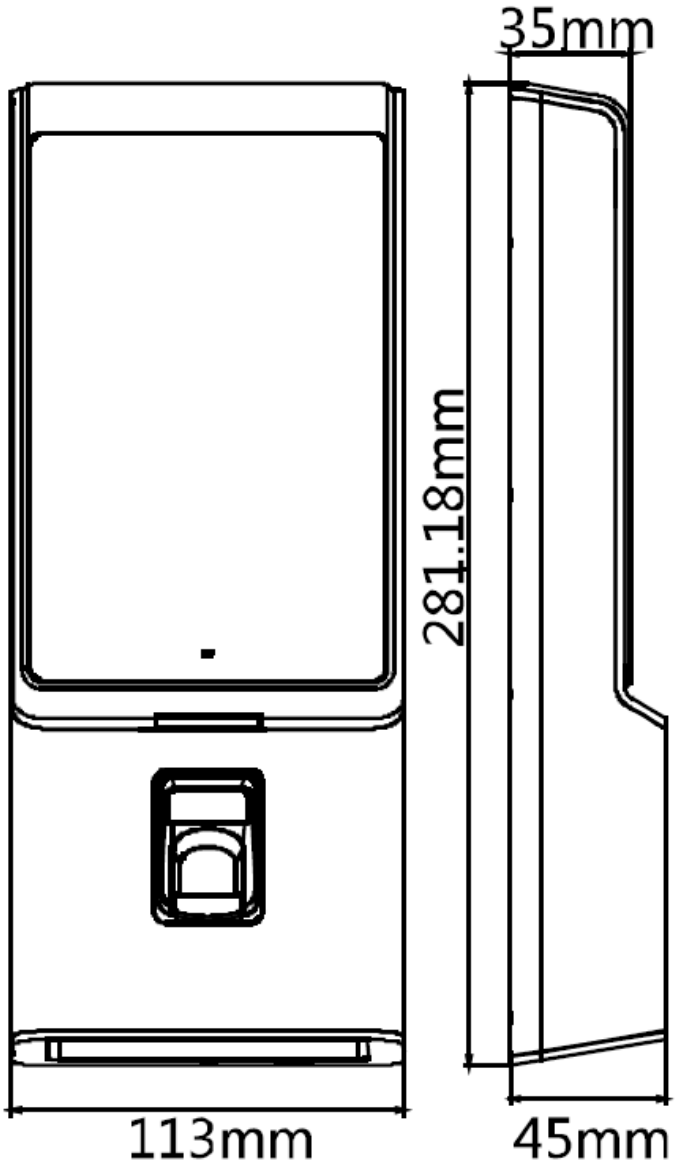
2. Install the device indoors, at least 6.6 ft (2 m) away from the light, and at least 9.8 ft (3 m) away from the window or door.



3. Avoid backlight, as well as direct and indirect sunlight.



Appendix D Dimensions



See Far, Go Further