User Manual

ZKBioSecurity

Date: March 2020

Software Version: ZKBioSecurity V5000 2.0.0

Doc Version: 2.9

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zktecousa.com.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com

If there is any issue related to the product, please contact us.

ZKTeco US Headquarters

Address 1600 Union Hill Road

Alpharetta, GA 30005

Phone 862-505-2101

For business related queries, please write to us at: sales@zktecousa.com.

To know more about our global branches, visit www.zktecousa.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of ZKBioSecurity V5000 2.0.0 software.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual
	The general information which helps in performing the operations faster
	The information which is significant
	Care taken to avoid danger or mistakes
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 Requirement and Introduction

Today, modern companies' concern for security has rapidly increased. Every company wants to work in a secured environment. To reach this level, ZKTECO brings to you a management system that helps customers to integrate operations of safety procedures on one platform. The system is divided into ten modules, namely: Personnel, Access, Attendance, Elevator, Hotel Systems, Visitor Systems, Parking Lot Systems, Patrol Systems, Video Systems and Systems Management.

❖ **Features**

- It can manage around 30,000 personnel data with its powerful data processing capacity.
- Users' data are more secured with multi-level management role-based level management.
- It can track events and operations in Real-time to ensures prompt feedbacks of data to the supervisor.

❖ **Configuration Requirements**

- Dual core processor with speeds of 2.4GHz or above.
- System Memory of 4GB or above.
- Available space of 30GB or above. We recommend using NTFS hard disk partition as the software installation directory.
- Monitor Resolution of 1024*768px or above.

❖ **Operating System**

- Supported Operating Systems: Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows Server 2008/2013(32/64).
- Supported Databases: Postgre SQL (Default), SQL Server & Oracle (Optional).
- Recommended browser version: IE 11+/Firefox 27+/Chrome 33+.

✍**Note:** You must use IE 8.0 or newer version for fingerprint registration and verification.

1.1 Personnel Module

This module is used to set Person details and their department. It primarily consists of two parts: Department Management settings, which is used to set the Company's organizational chart; Personnel Management settings, which is used to input person information, assign departments, maintain and manage personnel.

1.2 Access Control Module

This module is a web-based management system which enables normal access control functions, management of networked access control panel via computer, and unified personnel access management. The access control system sets door opening time and levels for registered users.

1.3 Attendance Module

It can achieve cross-regional attendance centralized control through the shift and shift management. You can apply for Appended Receipt, Leave, Overtime, etc. in Exception Management. In this module, you can also attendance point for access/parking and other functions.

1.4 Elevator Module

This module is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's access rights to different floors and elevator control time, and supervise elevator control events. You may set registered users' rights to floors. Only authorized users can reach certain floors within a period of time after being authenticated.

1.5 Video Module (Video Linkage & VMS)

Video provides video linkage function to manage the Video Server, view the Real-Rime Video, and query the Video Record, popup the Real-Time Video when linkage events occur.

VMS supports features such as real-time preview, video playback, linkage alarm, and decoding video, etc. It also provides flexible and diverse solutions to meet the need of small and medium projects.

1.6 FaceKiosk Module

The FaceKiosk device based on visible light face is used to verify face by uploading and downloading personnel access level. In addition, advertisement pictures and videos can be sent to the FaceKiosk device to make full use of the functions of the device in different time periods.

1.7 Face Intellect Module

Software support Face Intellect devices, intelligent recognition and face matching. It can cooperate with the access control module when it is used as a reader, the door will be opened by access control panel after verification.

1.8 Temperature Module

System Management is primarily used to assign system users and configure the roles of corresponding modules, manage databases such as backup, initialization, and recovery, and set system parameters and manage system operation logs.

1.9 System Management Module

System Management is primarily used to assign system users and configure the roles of corresponding modules, manage databases such as backup, initialization, and recovery, and set system parameters and manage system operation logs.

2 System Operations

2.1 Login to the System

After installing the software, double-click the ZKBioSecurity icon to enter the system. You may also open the recommended browser and input the IP address and server port in the address bar. The IP address is set as: http://127.0.0.1:8098 by default.

If the software is not installed in your server, you may input the IP address and server port in the address bar.

The user name of the Superuser is [admin], and the password is [admin], then click [**login**]. After the first login to the system, please reset the password in [Personnel Information].

If the user needs to use the software in different languages, please choose the language from the drop-down menu above the login field. The supported languages are Chinese (Simplified), English, Spanish, Thai, Indonesian, Vietnamese, Chinese (Traditional), Russian, and Korean.

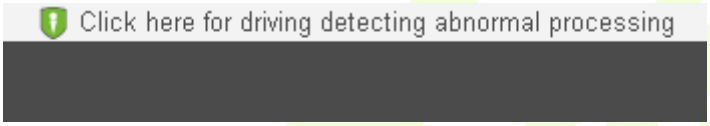
In the login interface, if the user has already installed the fingerprint driver, enrolled the fingerprint, and started the service, click the **Fingerprint** button next to the Login button. Now, the user can verify the fingerprint through the fingerprint scanner to login to the software.

✍**Note:**

- The user name of the super user is [admin], and the password is [admin]. After the first login to the system, please reset the password in [Personnel Information].
- If you have selected the HTTPS port during software installation, input the server IP address and port number (for example, https://127.0.0.1:8448) in the address bar and press Enter. The following prompt may be displayed:

Here, you need to add a site exception following the exception adding prompts after you press Advanced. Different browsers may have different setting.

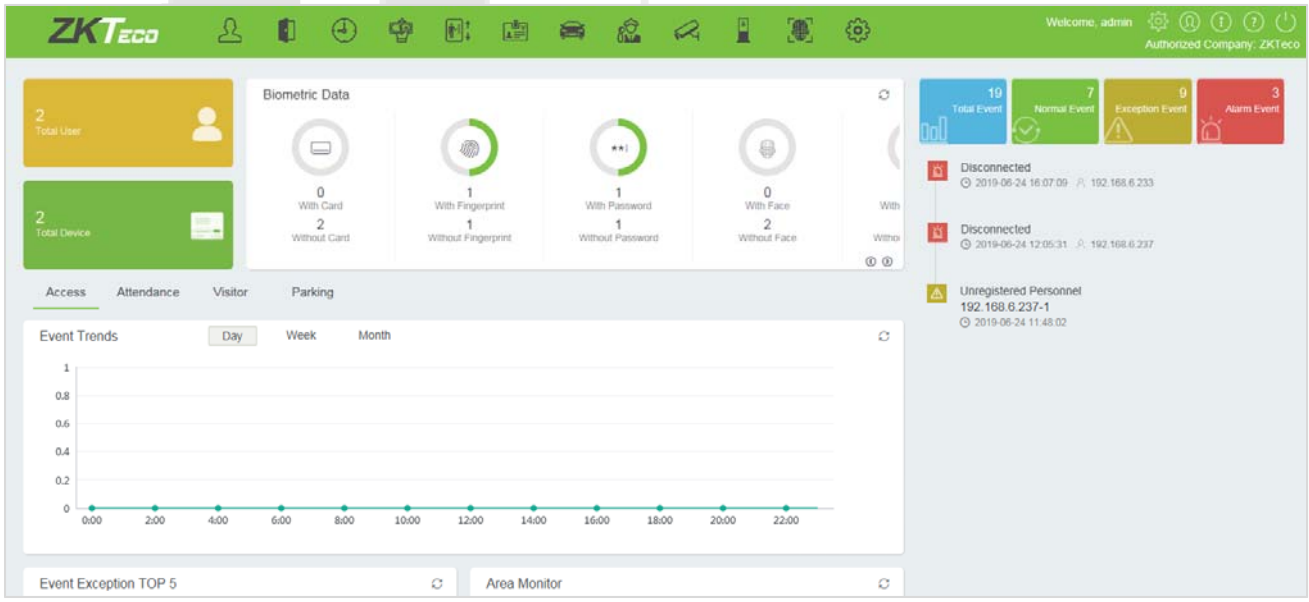
- If you have selected the HTTPS port during software installation, the following message may be displayed on the login page:



Click **Connect.** On the page that is displayed, download issonline.exe and corresponding certificates before using functions such as fingerprint and external devices.

2.2 Dashboard

After logging in, the home page is displayed as shown below. If you want to go to home page from any interface, then you can click ZKTeco on the upper left corner of the interface to return to the home page.

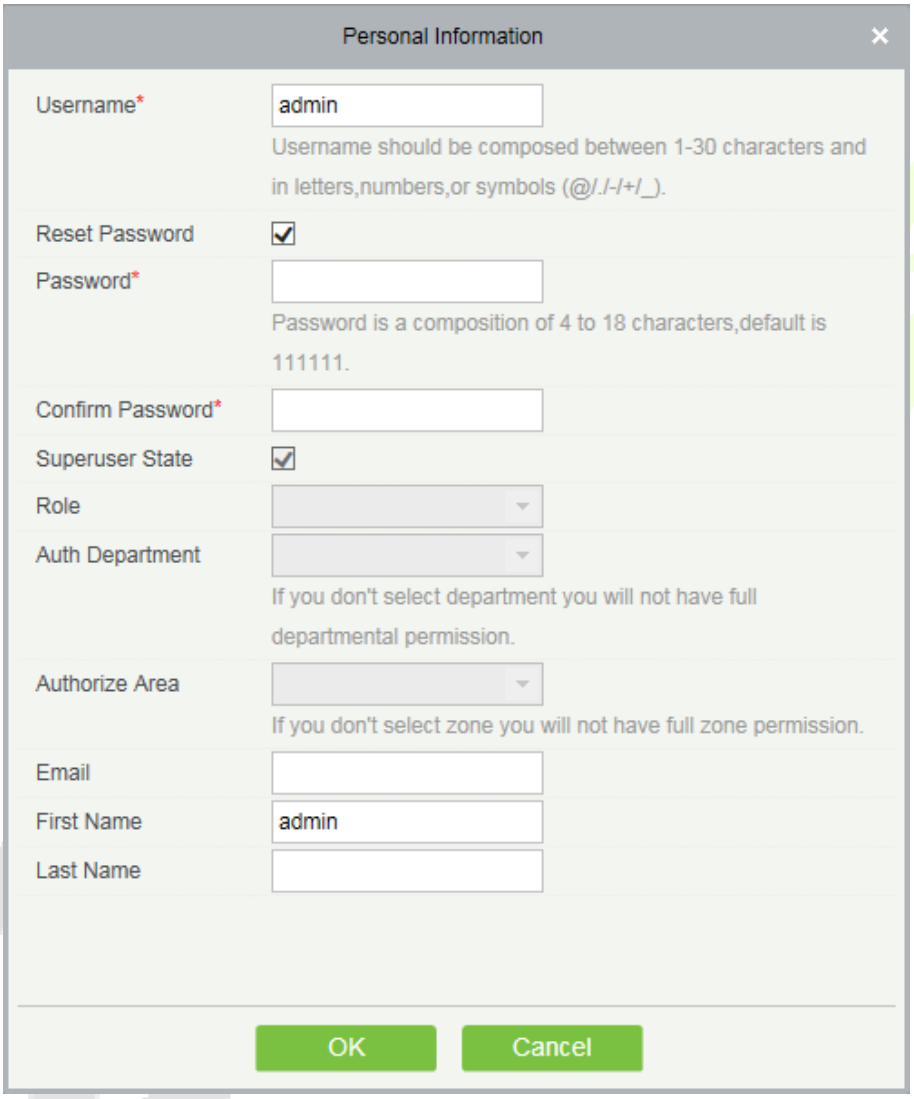


2.3 Activating the System

Please refer to the corresponding license document.

2.4 Modifying Password

You can modify the login password in [**Personal Information**] :

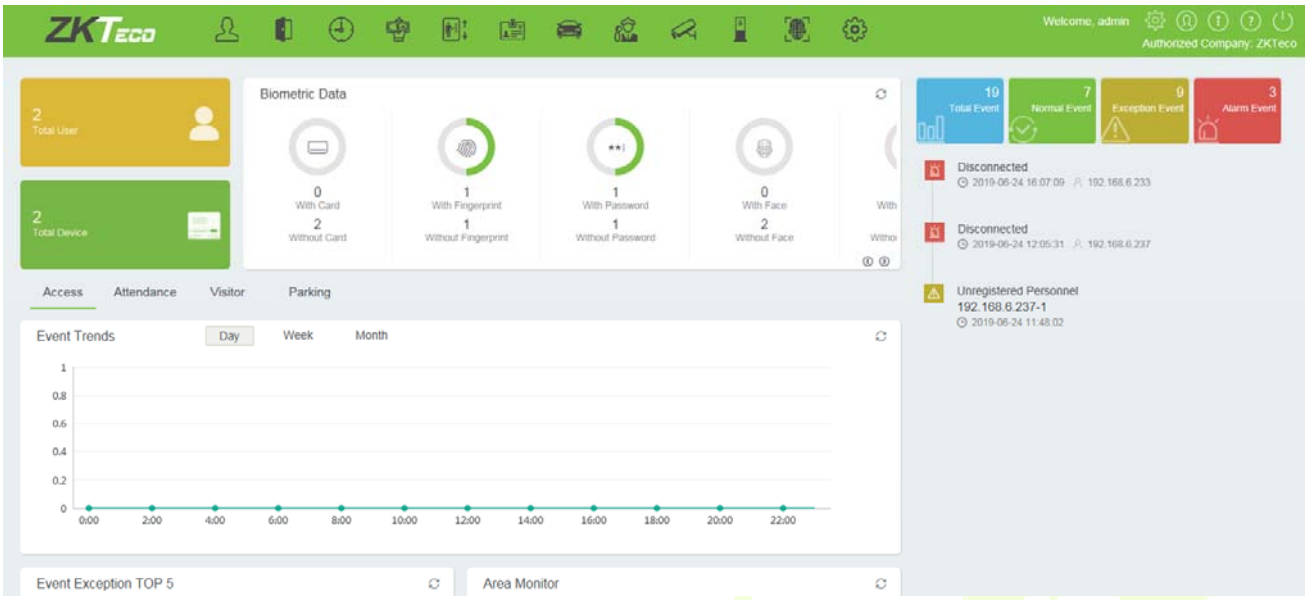


Check [**Reset Password**] box to modify the password.

✍**Note:** Both, super user and the new user are created by the superuser (the default password for the new users is 111111). The user name is not case-insensitive, but the password is case-sensitive.

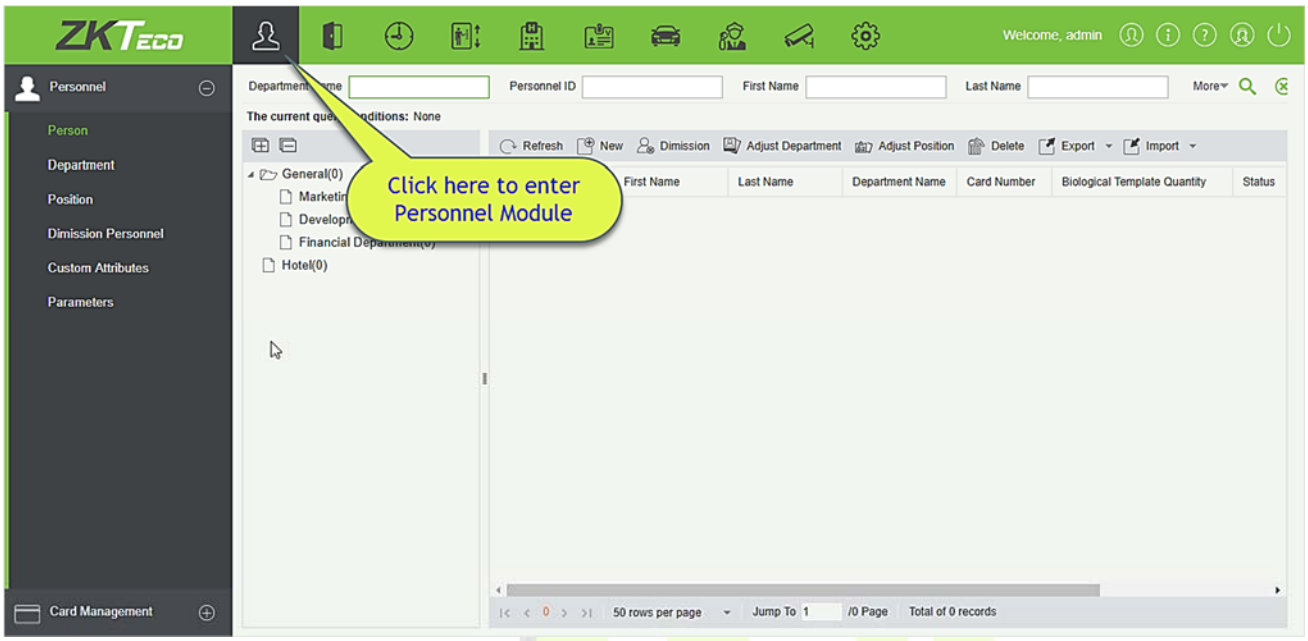
2.5 Exit the system

Click the [**Logout**] button on the upper right corner of the interface to exit the system.



3 Personnel Management

Before using the other functions, please configure the personnel system: Personnel and Card Management.



3.1 Personnel

Personnel system includes these modules: Person, Department, **Position**, **Dismission Personnel**, **Custom Attributes**, and **Parameters**.

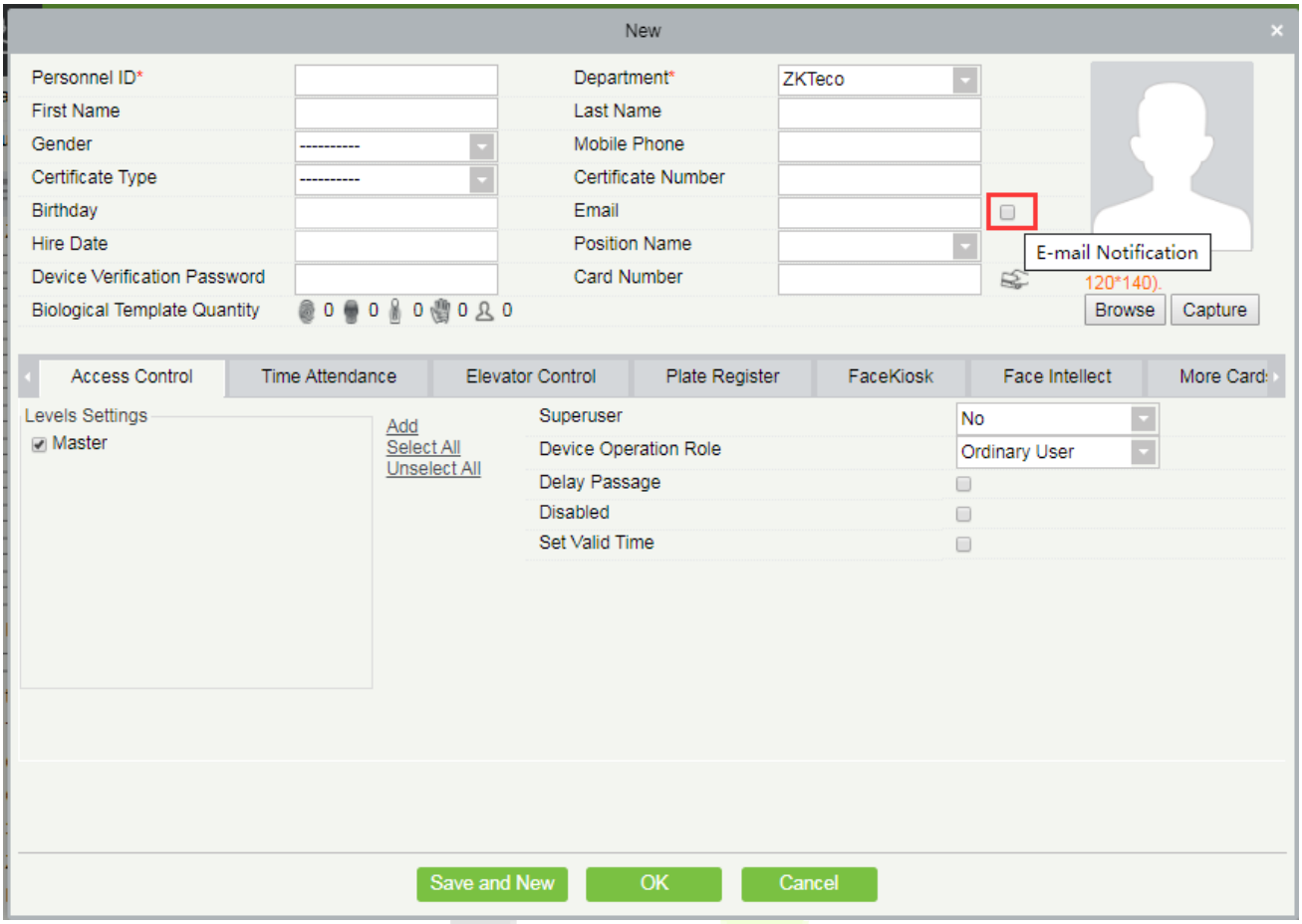
3.1.1 Person

When using this management program, the user shall register personnel in the system, or import personnel information from other software or documents into this system. For details, see Common Operations.

Main functions of Personnel Management include Add, Edit, Delete, Export and Import personnel, and Adjust Department.

- **Add Personnel**

1. Click **[Personnel]** > [**Person**] > [**New**]:



Fields are as follows:

Personnel ID: An ID may consist of up to 9 characters, within the range of 1 to 79999999. It can be configured based on actual conditions. The Personnel No. contains only numbers by default but may also include letters.

✍Notes:

- When configuring a personnel number, check whether the current device supports the maximum length and whether letters can be used in personnel ID.
- To edit the settings of the maximum number of characters of each personnel number and whether letters can also be used, please click Personnel > Parameters.

Department: Select from the pull-down menu and click [**OK**]. If the department was not set previously, only one department named [**Company Name**] will appear.

First Name/Last Name: The maximum number of character is 50.

Gender: Set the gender of personnel.

Password: Set password for personnel accounts. It can only contain up to 6-digits. If a password exceeds the specified length, the system will truncate it automatically. It cannot be the same with others password and the duress password.

Certificate Type: There are four types of certificates: ID, Passport, Driver License and Others. Click icon to recognize the Certificate automatically. Please refer 3.1.7 Parameters and 15.2.5 Client Register to see how to register one.

Certificate Number: Click icon and the Certificate information will pop up automatically.

Social Security Number: Set personnel social security number. The max length is 20.

Mobile Phone: The max length is 20, and this is an optional field.

Reservation Code: The max length is 6; the initial password is 123456.

Position: It is the designation of the personnel. It can be referred as the level of personnel in workmanship.

Birthday: Input employee's actual birthday.

Email: Set the available email address of the personnel. The max length is 30. Punctuations, namely, the " - ", " _ " and " . " are supported. If the Event Notification is checked, the Email is required.

E-mail Notification: After checking this menu, the system will send an email to the relevant person once an access or an elevator event occurs. If there is no setting to email sending server, the Email Parameter Settings window will pop up if this menu is checked. Please refer to E-mail Management for the setting information.

Card number: The max length is 10, and it should not be repeated.

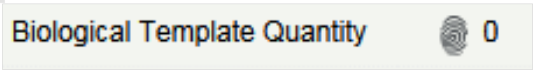
Hire Date: It is the date on which the personnel are appointed. Click to select the date.

Personal Photo: The picture preview function is provided, supporting common picture formats, such as **jpg**, **jpeg**, **bmp**, **png**, **gif** etc. The best size is 120×140 pixels.

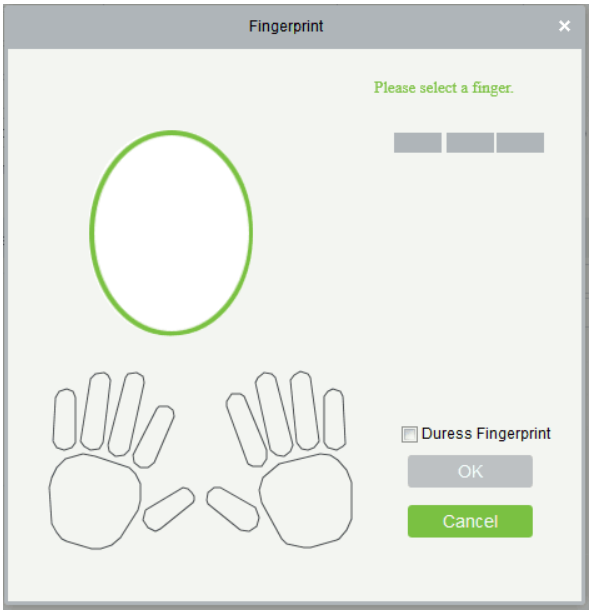
- **Browse:** Click [**Browse**] to select a local photo to upload.
- **Capture:** Taking photo by camera is allowed when the server is connected with a camera.

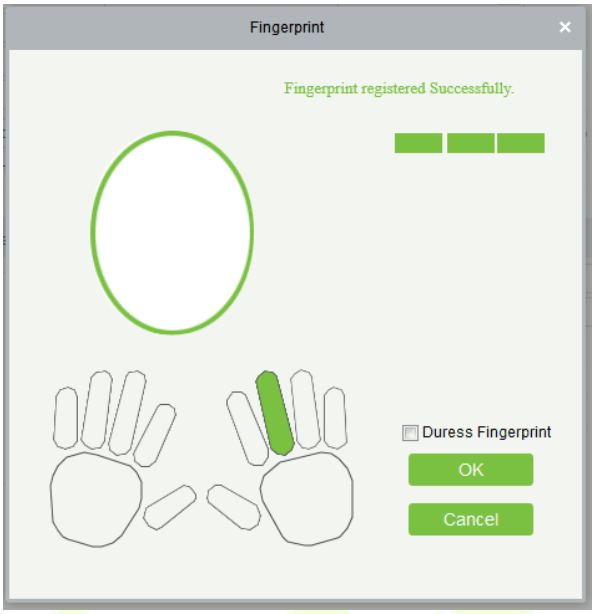
Register Fingerprint/Finger Vein: Enroll the Personnel Fingerprint, Finger Vein or Duress Fingerprint. To trigger the alarm and send the signal to the system, scan the Duress Fingerprint.

How to register fingerprint:



1) Move the cursor to the fingerprint icon position, a registration pop-up or drive download box will appear, click [**Register**].
2) Select a fingerprint, press on the sensor by three times, then "**Fingerprint registered Successfully**" will be prompted.
3) Click [**OK**] to complete registration.



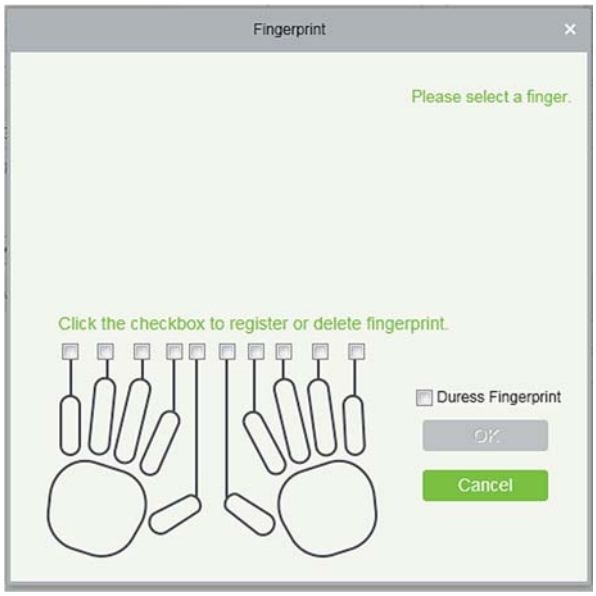


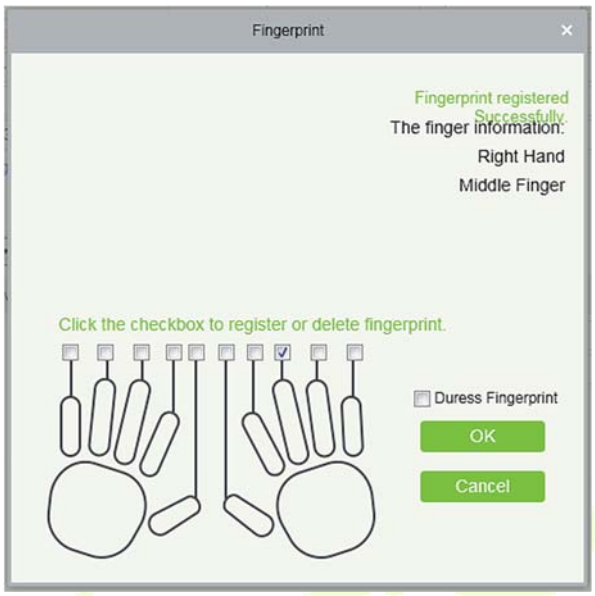
Click a fingerprint to delete. If you need to register a duress fingerprint, check the Duress Fingerprint box.

✍Notes:

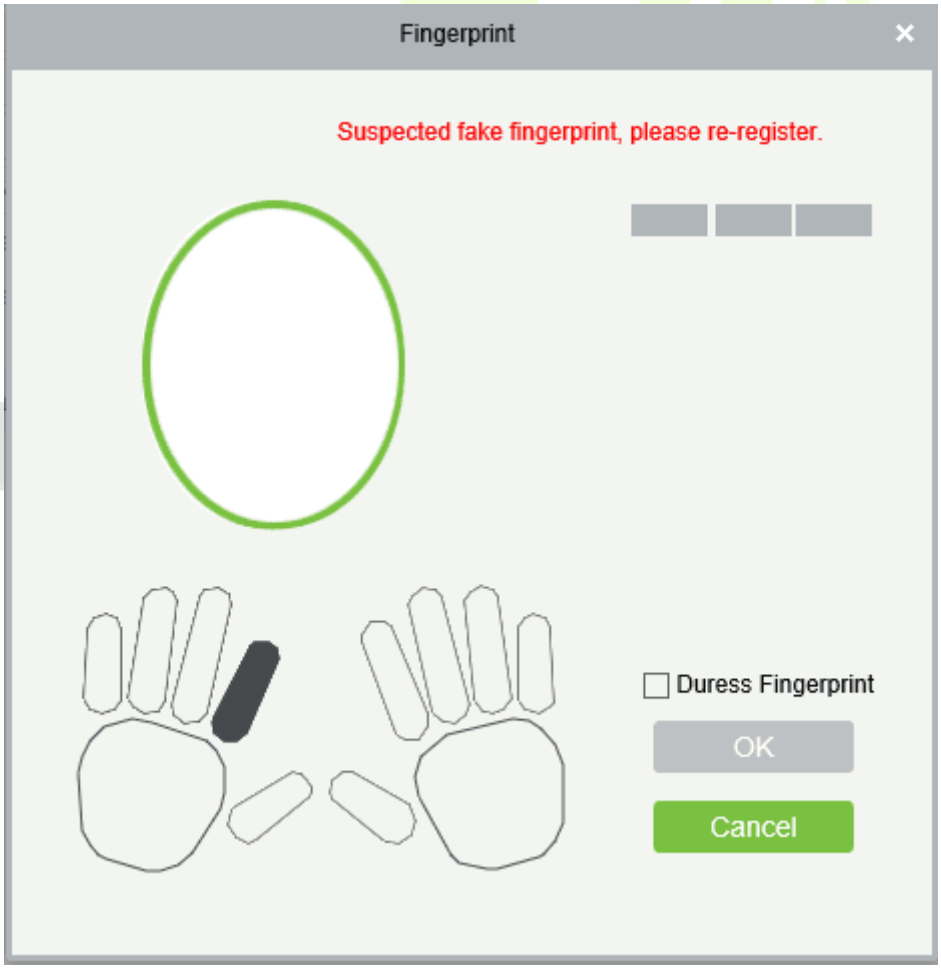
- If fingerprints are duplicated, "Don't repeat the fingerprint entry" will be prompted.
- If the fingerprint sensor driver is not installed, click "Install driver" and the system will prompt to download and install driver.
- After installing the fingerprint sensor driver, if the fingerprint register button is grey in IE browser while it is normal in other browsers (such as Firefox, Google), you can change the settings of IE browser, as per the following:

1) In IE browser, click **[Tools]** > [**Internet Options**] > [**Security**] > [**Credible Sites**], add http://localhost to the credible sites, then restart the IE browser.
2) In IE browser, click [**Tools**] > [**Internet Options**] > [**Advanced**] > [**Reset**] to pop up a dialog of Reset Internet Explorer Settings, click [**Reset**] to confirm; then restart the IE browser (you may try when Point 1 does not help).
3) If all the above settings do not work, please execute following operations (take IE11 browser as an example): click [**Tools**] > [**Internet Options**] > [**Advanced**] > [**Security**], check the option of **[Allow software to run or install even if the signature is ...**], and remove the tick before [**Check for server certificate revocation**], then restart IE.
4) If the browser is below IE8, the fingerprint registration page will be different:





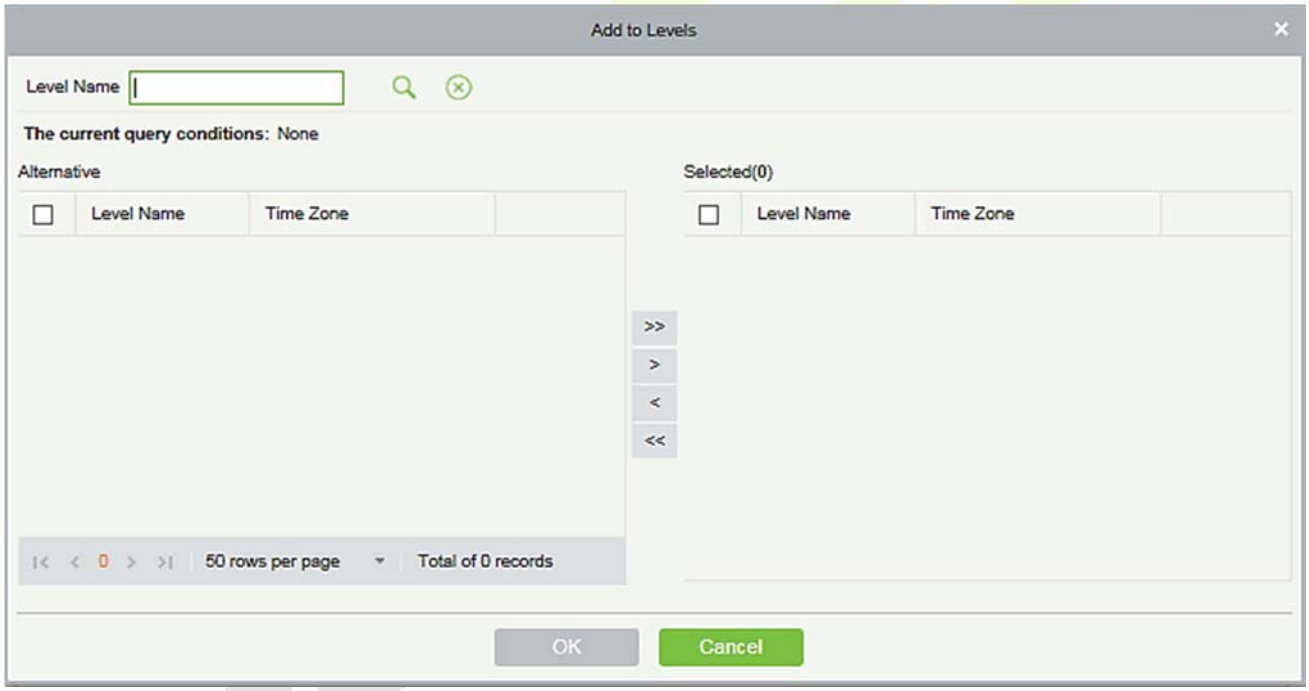
5) The system supports the access from the Live20R fingerprint device and the fake fingerprint prevention function.



2. Set the Access Control parameters for the personnel. Click [**Access Control**] :

Fields are as follows:

Level Settings: Click [**Add**], then set passage rules of special positions in different time zones.



Superuser: In access controller operation, a super user is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door-opening priority.

Device Operation Authority: Select administrator to get its levels.

Delay Passage: Extend the waiting time for the personnel through the access points. Suitable for physically-challenged or people with other disabilities.

Disabled: Temporarily disable the personnel's access level.

Set Valid Time: Set Temporary access level. Doors can be set to open only within certain time periods. If it

is not checked, the time to open the door is always active.

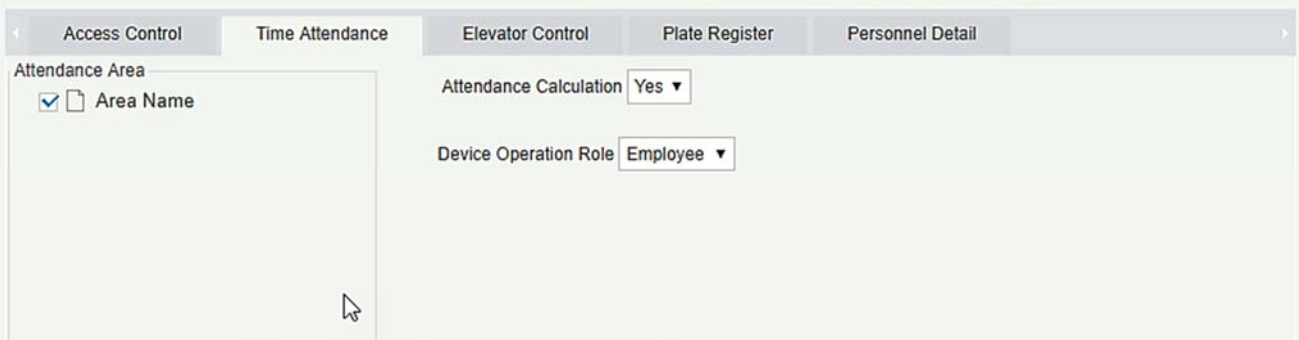
✍**Note:** The system will automatically search for the relevant numbers in the departure library during verification.

The Personnel Information List, by default, is displayed as a table. If Graphic Display is selected, photos and numbers will be shown. Put the cursor on a photo to view details about the personnel.

✍**Notes:**

- Not all devices support the "Disabled" function. When a user adds a device, the system will notify the user whether the current device supports this function. If the user needs to use this function, please upgrade the device.
- Not all the devices support the "Set Valid Time" function of setting the hour, minute, and second. Some devices only allow users to set the year, month, and day of the local time. When a user adds a device, the system will notify the user whether the current device support this function. If the user needs to use this function, please upgrade the device.

3. Set the Time Attendance parameters for the personnel. Click [**Time Attendance**]:



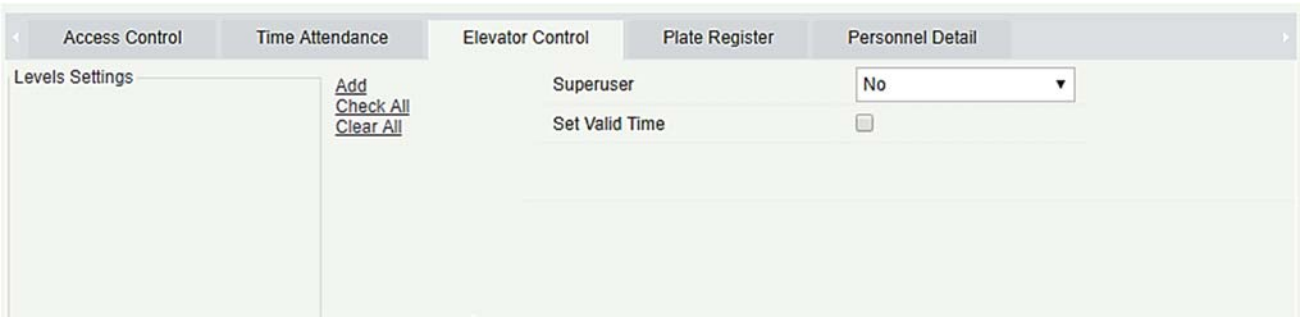
Fields are as follows:

Attendance Area: You can set the staff attendance area.

Attendance Calculation: Set if the attendance needs to be calculated or not. Select [Yes] for calculating attendance. Select [No] for not calculating the attendance.

Device Operation Role: It will set the authority for operating the device and send it to the corresponding device.

4. Set the Elevator Control parameters for the personnel. Click [**Elevator Control**]:



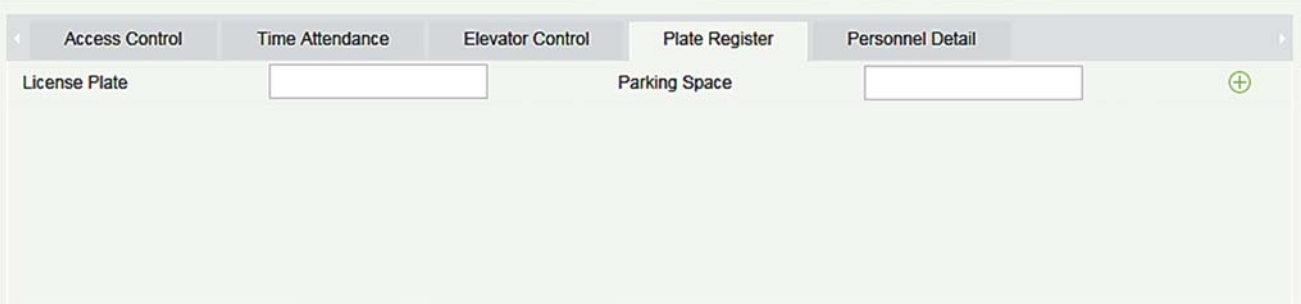
Fields are as follows:

Superuser: In elevator controller operation, a super user is not restricted by the regulations on time zones, holidays and has extremely high door-opening priority.

Set Valid Time: Set Temporary elevator level. Floor buttons can be set to be pressed only within the time periods. If it is not checked, the time to press the floor button is always active.

✍**Note:** The Elevator level must be set in advance.

5. Set the Elevator Control parameters for the personnel. Click [**Elevator Control**]:



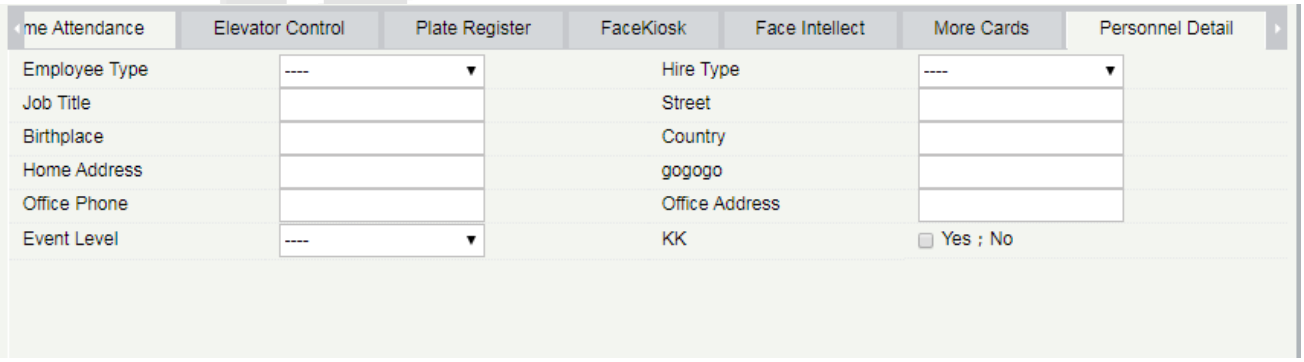
Fields are as follows:

License Plate: The user needs to register the license plate.

Parking Space: Parking space corresponding to the vehicle.

✍**Note:** Each personnel may register a maximum of 6 license plates.

6. Click [**Personnel Detail**] to access the details and editing interface, and enter more information.



7. After entering the information, click [**OK**] to save and exit, the person details will be displayed in the added list.

- **Edit Personnel**

Click [**Personnel**] > [**Person**], then select a person, and click [**Edit**].

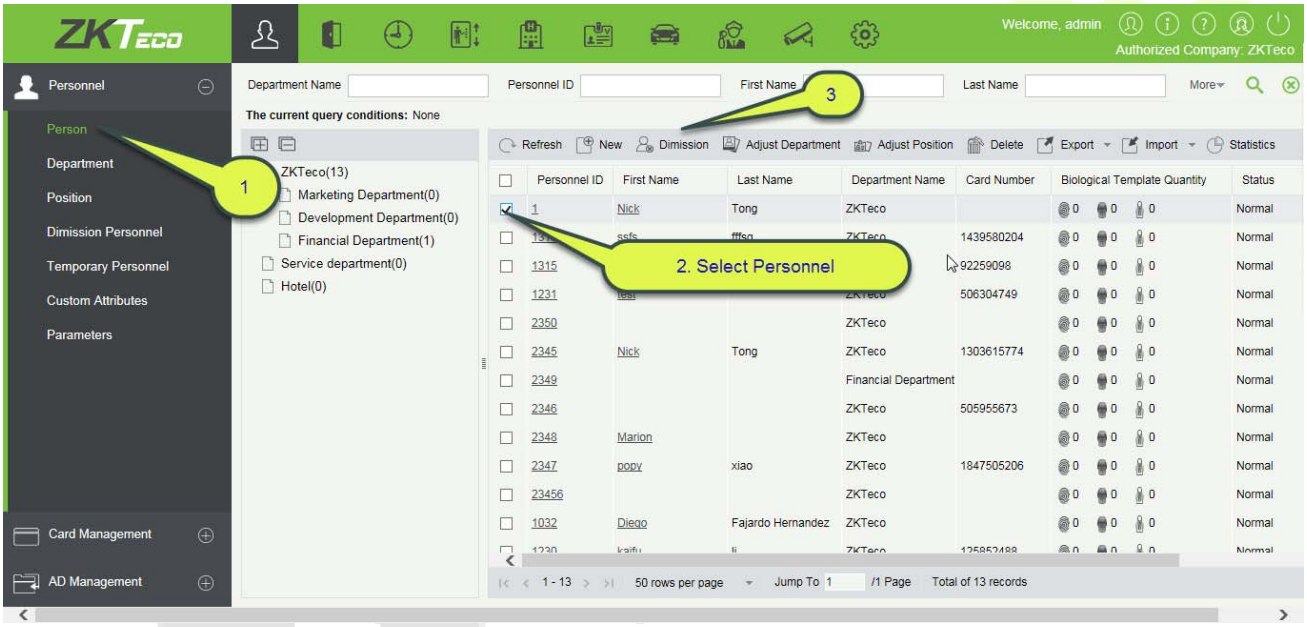
- **Delete Personnel**

Click [**Personnel**] > [**Person**], then select a person, and click [**Delete**] > [**OK**] to delete.

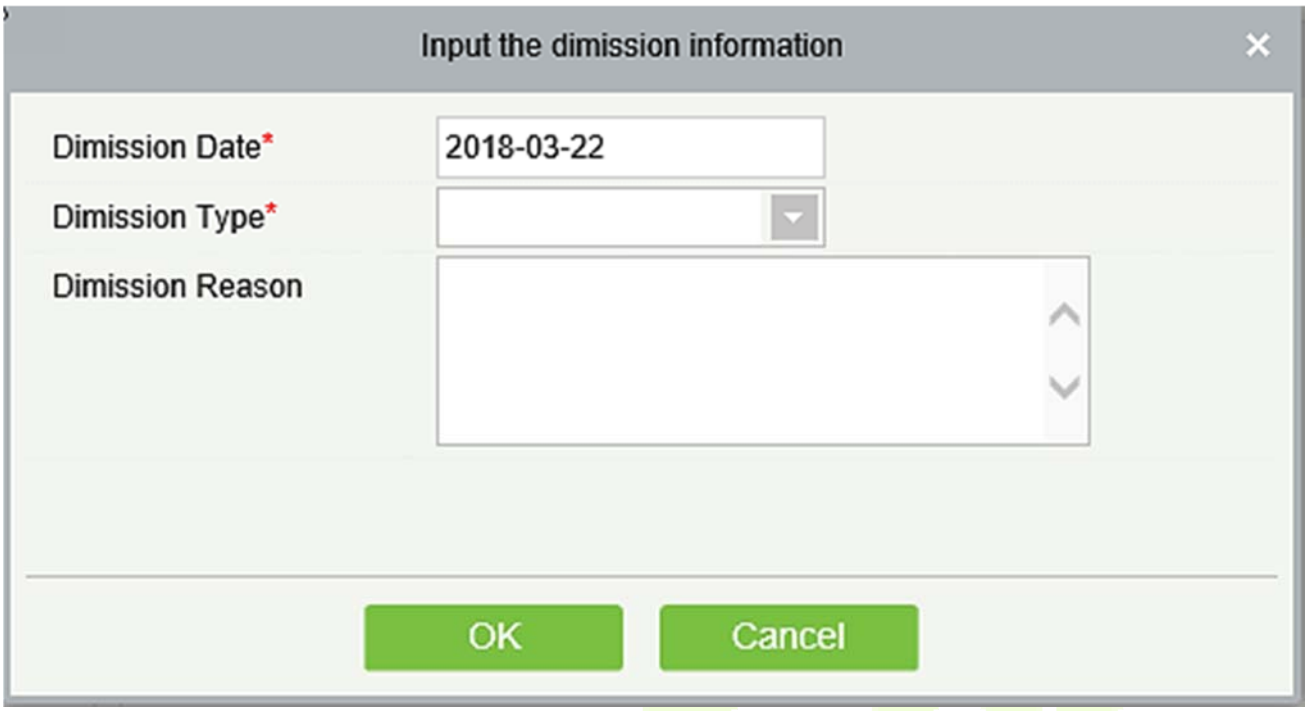
✍**Note:** All relevant information about the person will be deleted.

- **Dimission**

1. Click [**Personnel**] > [**Person**], then select a person, and click [**Dimission**].

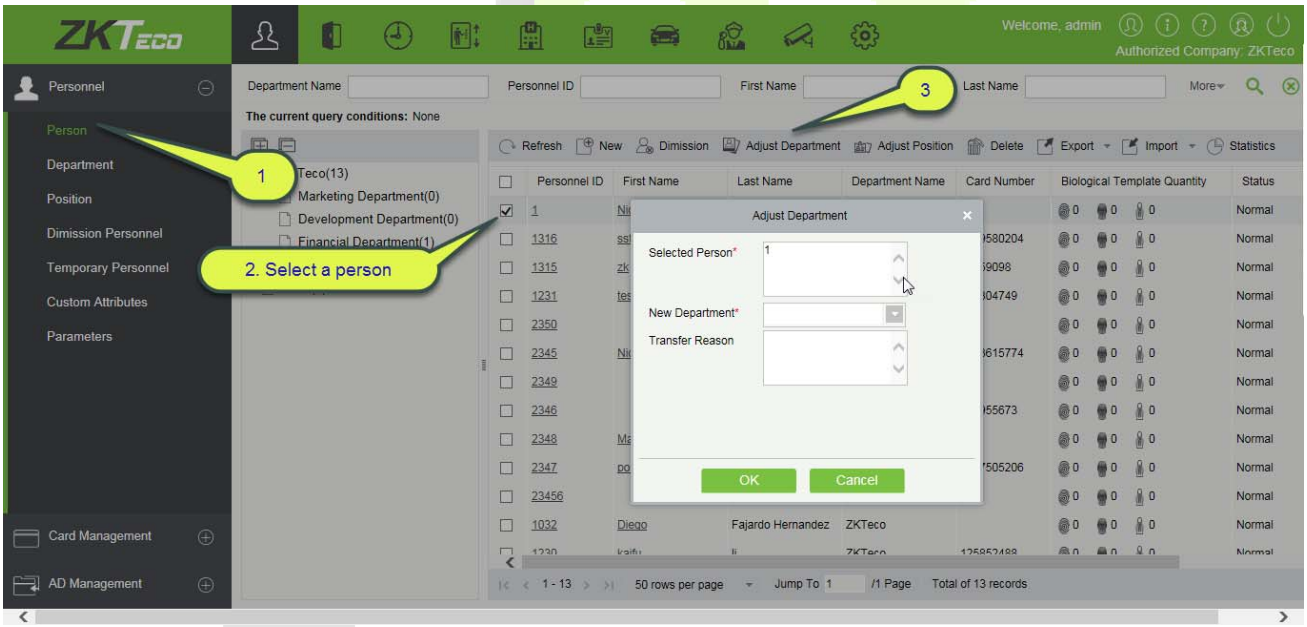


2. Select the date, then select type and write reason and click [**OK**].



Adjust Department

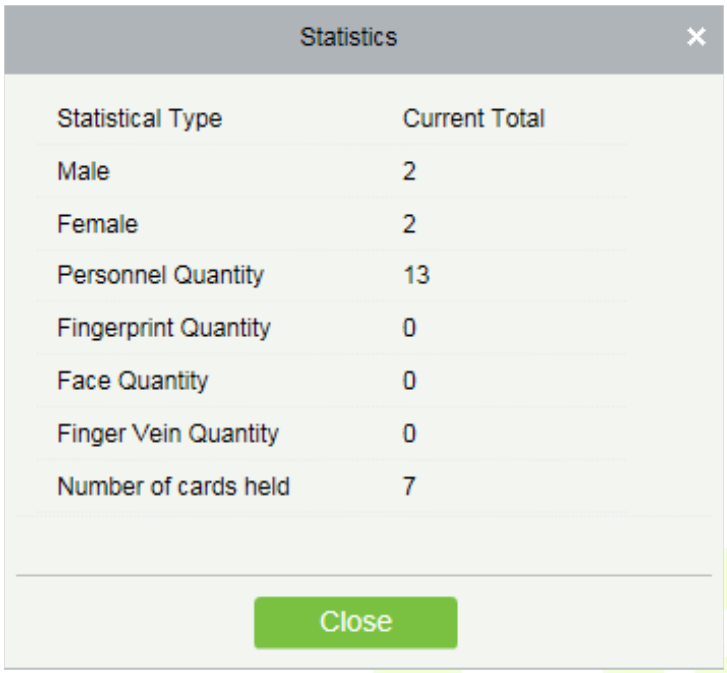
1. Click [**Personnel**] > [**Person**], then select a person, and click [**Adjust Department**]:



2. Select [**New Department**].
3. Click [**OK**] to save and exit.

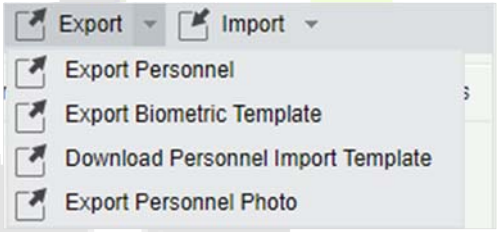
Statistics

Click [**Personnel**] > [**Person**] > [**Statistics**]. View the number of personnel, the number of fingerprints, face templates, finger vein enrolled, card numbers, gender and other statistical information.

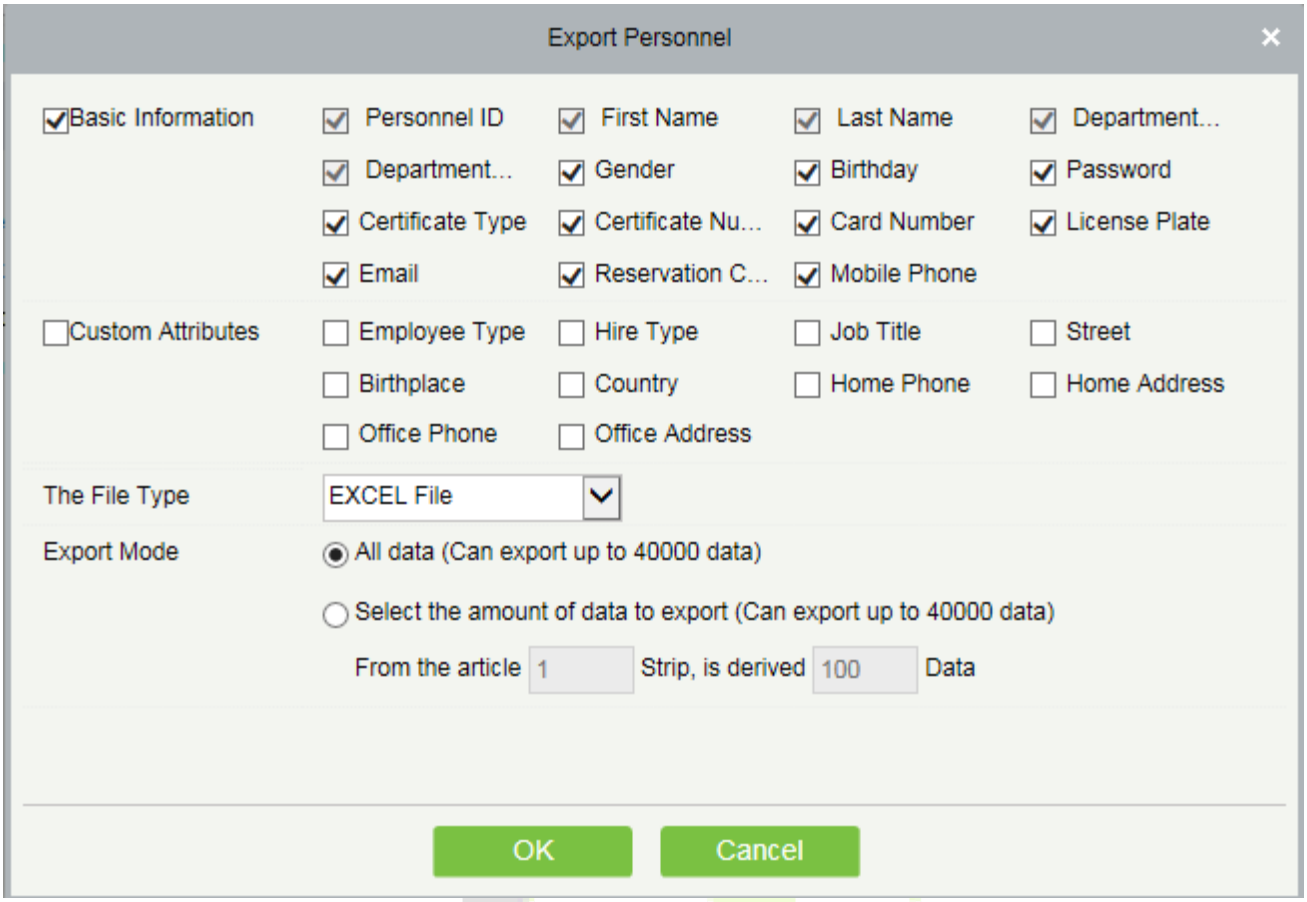


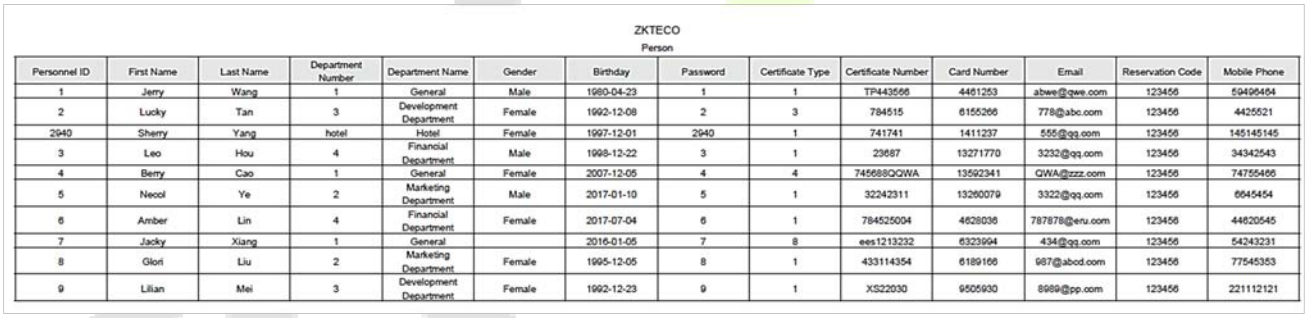
- **Export**

Click [**Personnel**]> [**Person**]> [**Export**] to export personnel information, personnel biometric templates, personnel import templates and personnel photo.



1. Export Personnel: Personnel's basic information is all checked (selected); check custom attributes as required.



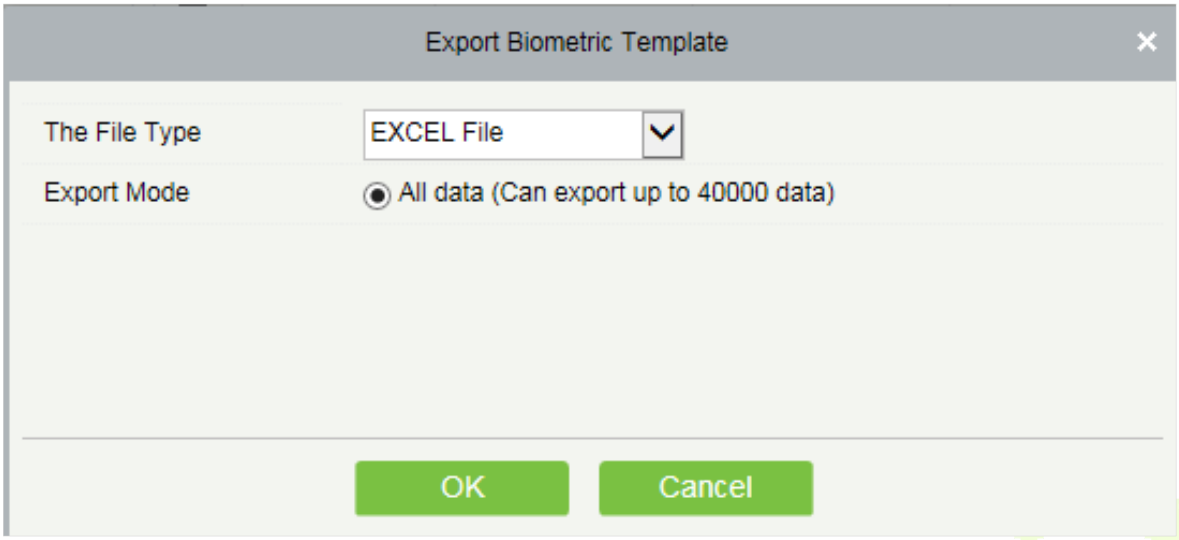


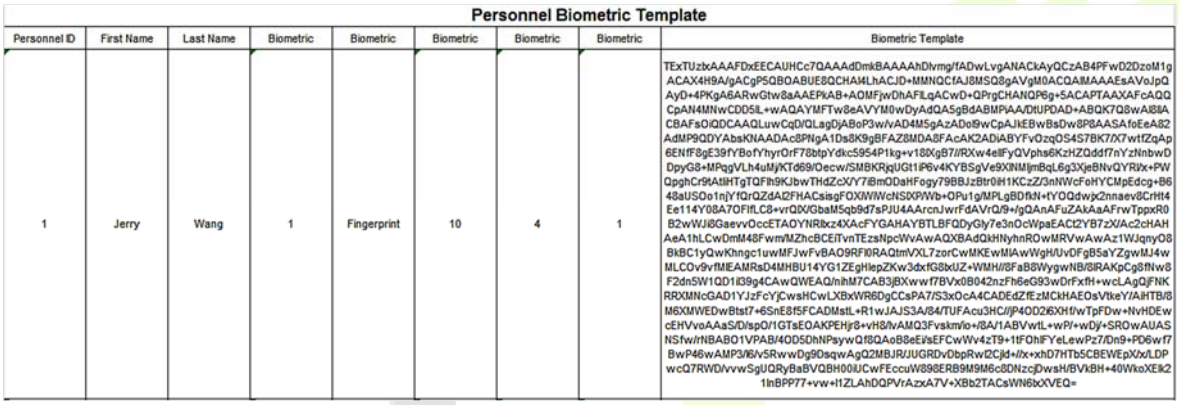
ZKTECO

Person

Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Password	Certificate Type	Certificate Number	Card Number	Email	Reservation Code	Mobile Phone
1	Jerry	Wang	1	General	Male	1980-04-23	1	1	TP443566	4461253	abwe@qwe.com	123456	59496464
2	Lucky	Tan	3	Development Department	Female	1992-12-08	2	3	784515	6155266	778@abc.com	123456	4425521
2940	Sherry	Yang	hotel	Hotel	Female	1997-12-01	2940	1	741741	1411237	555@qq.com	123456	145145145
3	Leo	Hou	4	Financial Department	Male	1998-12-22	3	1	23687	13271770	3232@qq.com	123456	34342543
4	Berry	Cao	1	General	Female	2007-12-05	4	4	745688QQWA	13592341	QWA@zzz.com	123456	74755466
5	Necol	Ye	2	Marketing Department	Male	2017-01-10	5	1	32242311	13260079	3322@qq.com	123456	6645454
6	Amber	Lin	4	Financial Department	Female	2017-07-04	6	1	784525004	4628036	787878@eru.com	123456	44620545
7	Jacky	Xiang	1	General		2016-01-05	7	8	ees1213232	6323994	434@qq.com	123456	54243231
8	Glori	Liu	2	Marketing Department	Female	1995-12-05	8	1	433114354	6189166	987@abcd.com	123456	77545353
9	Lilian	Mei	3	Development Department	Female	1992-12-23	9	1	XS22030	9505930	8989@pp.com	123456	221112121

2. Export the Biometric Template.

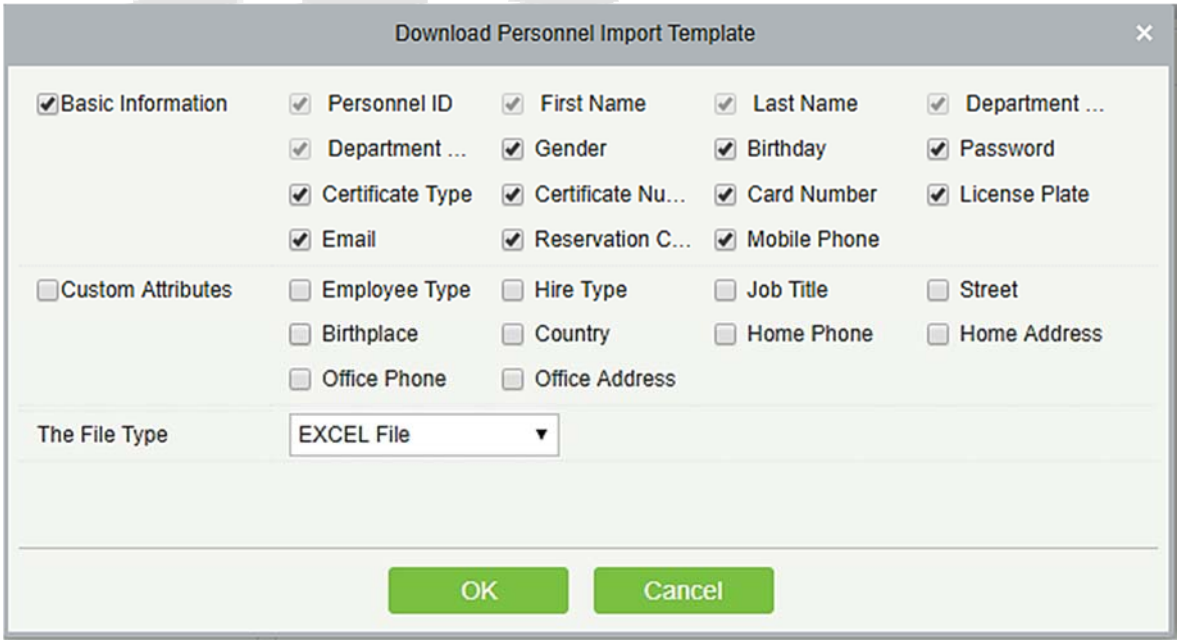




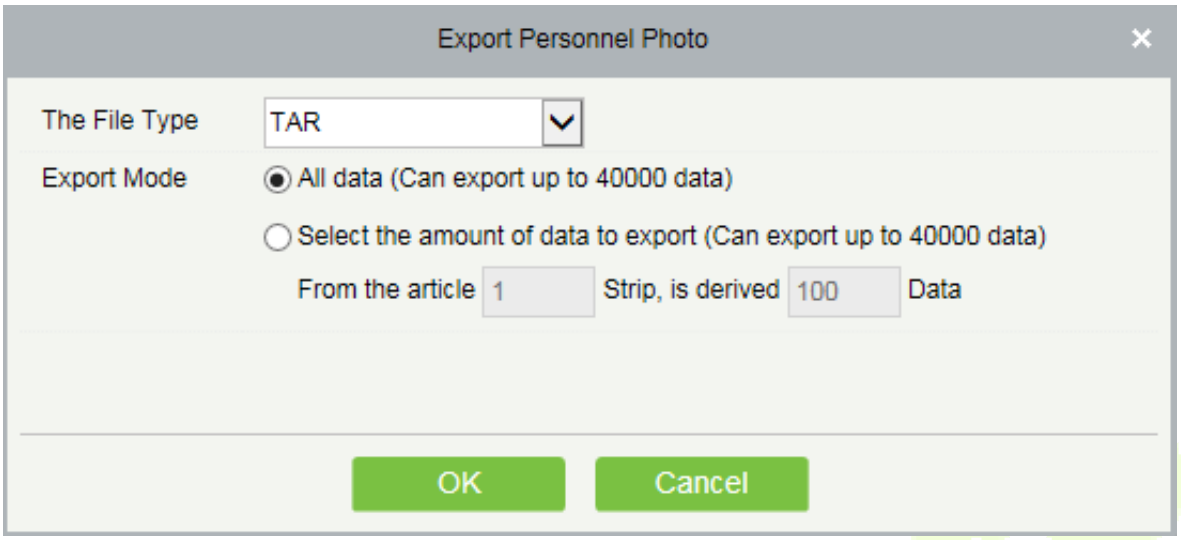
Personnel Biometric Template

Personnel ID	First Name	Last Name	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric Template
1	Jerry	Wang	1	Fingerprint	10	4	1	TExTUzkxAAAFDxEECAUHCc7QAAAdDmkBAAAAhDlvmg/fADwLvgANACkAyQCzAB4PFwD2DzoM1g ACAX4H9A/gACgP5QBOABUE8QCHAl4LhACJD+MMNQCfAJ8MSQ8gAVgM0ACQAIMAAAEsAVoJpQ AyD+4PKgA6ARwGtw8aAAEPkAB+AOMFjwDhAFlLgACwD+QPrgCHANQP6g+5ACAPTAAXAFcAQQ CpAN4MNwCDD5iL+wAQAYMFTw8eAVYM0wDyAdQA5gBdABMPiAA/DtUPDAD+ABQK7Q8wAI8lA CBAFsOiQDCAAQLuwCqD/QLagDjABoP3wvAD4M5gAzADol9wCpAJkEBwBsDw8P8AASAfoEeA82 AdMP9QDYAbsKNAADAc8PNgA1Ds8K9gBFAZ8MDA8FAcAK2ADiABYFv0zqOS4S7BK7/X7wtfZqAp 6ENfF8gE39fYBofYhyrOrF78btpYdkc5954P1kg+v18lXgB7//RXw4elFyQVphs6KzHZQddf7nYzNnbwD DpyG8+MPqgVLh4uMjKTd69/Oecw/SMBKRjqUGt1iP6v4KYBSgVe9XNMjmBqL6g3XjeBNvQYRix+PW QpghCr9tAtlHTgTQFlh9KJbwTHdZcX/Y7/BmODaHFogy79BBJzBtr0lH1KCzZ/JnNWcFoHYCMpEdcg+B6 48aUSOo1njYfQrQZdAI2FHACsisgFOXiWcNSXPWb+OPu1g/MPLgBDfkN+tYOQdwjx2nnaev8CrHt4 Ee114Y08A7OFlfLC8+vrQDXGbaM5qb9d7sPJU4AArcnJwrFdAVrQ/9+/gQAnAFuZAkAaAFrwTppxR0 B2wWJi8GaevvOccETAOYNRlbz4XAcFYGAHAYBTLBFQDyGly7e3nOcWpaEACt2YB7zX/Ac2cHAH AeA1hLCwDmM48FwmMZhcBCEiTvnTEzsNpcWvAwAQXBAdQkHNyhnROwMRVwAwAz1WJqnyO8 BkBC1yQwKhngc1uwMFJwFvBAQ9RFI0RAQtmVXL7zorCwMKEwMIAwWgH/UvDFgB5aYZgwMJ4w MLCOv9vfMEAdRsD4MHBU14YG1ZEgHiepZKw3dxfG8xUZ+WMHl/8FaB8WygwNB/8RAKpCg8fNw8 F2dn5W1QD1i39g4CAwQWEAQ/nhM7CAB3jBXwwf7BVx0B042nzFh6eG93wDrFxfH+wcLAgQjFNK RRXMNcGAD1YJzFcYjCwsHCwLXBxWR6DgCCsPA7/S3xOcA4CADEdZfEzMCkHAEOsVtkeY/AiHTB/8 M6XMWEDwBtst7+6SnE8f5FCADMstL+R1wJAJS3A/84/TUFAcu3HC//jP4OD2i6XHf/wTpFDw+NvHDEw cEHVvoAAaS/D/spO/1GTsEOAKPEHjr8+vH8/lvAMQ3Fvskmvlo+/8A/1ABVwtL+wP/+wDj/+SROwAUAS NSfw/rNBABO1VPAB/4OD5DhNPsywQf8QAoB8eEi/sEFCwWv4zT9+1tFOhlFYeLewPz7/Dn9+PD6wf7 BwP46wAMP3/l6Vv5RwwDg9OsqwAgQ2MBJR/JUGRDvDbpRw/2Cjd+/lx+xhD7HTb5CBEWEpX/xfLDP wcQ7RWDlvvwSgUQRyBaBVQBH00IUCwFEccuW898ERB9M9M6c8DNzcjDwsH/BVkBH+40WkoXEIk2 1InBPP77+vw+I1ZLAhDQPVrAzxA7V+XBb2TACsWN6bXVEQ=

3. Download Personnel Import Template: Before exporting personnel template, you can configure the corresponding fields (including custom attributes fields) to be exported, the required fields (Personnel ID, Name, Department ID, Department Name) do not support configuration.



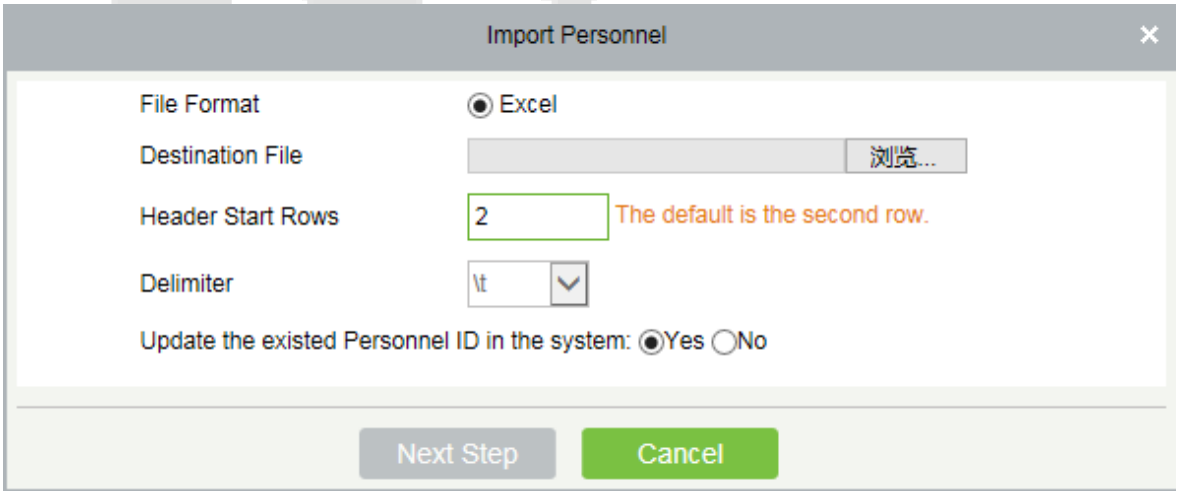
4. Export Personnel Photo.



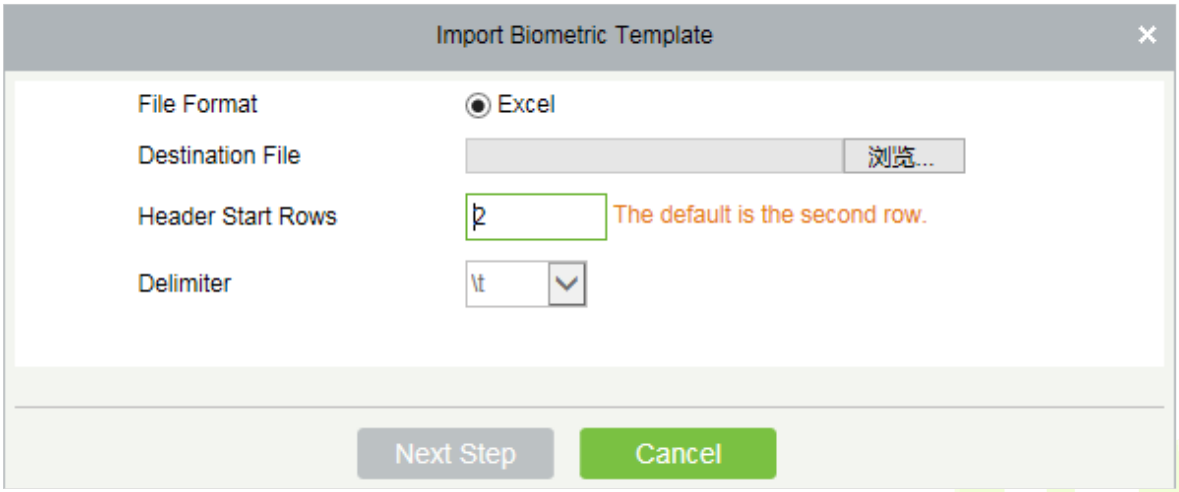
- **Import**

Click [**Personnel**] > [**Person**] > [**Import**] to import personnel information and personnel biometric templates. It only supports personnel information templates for importing.

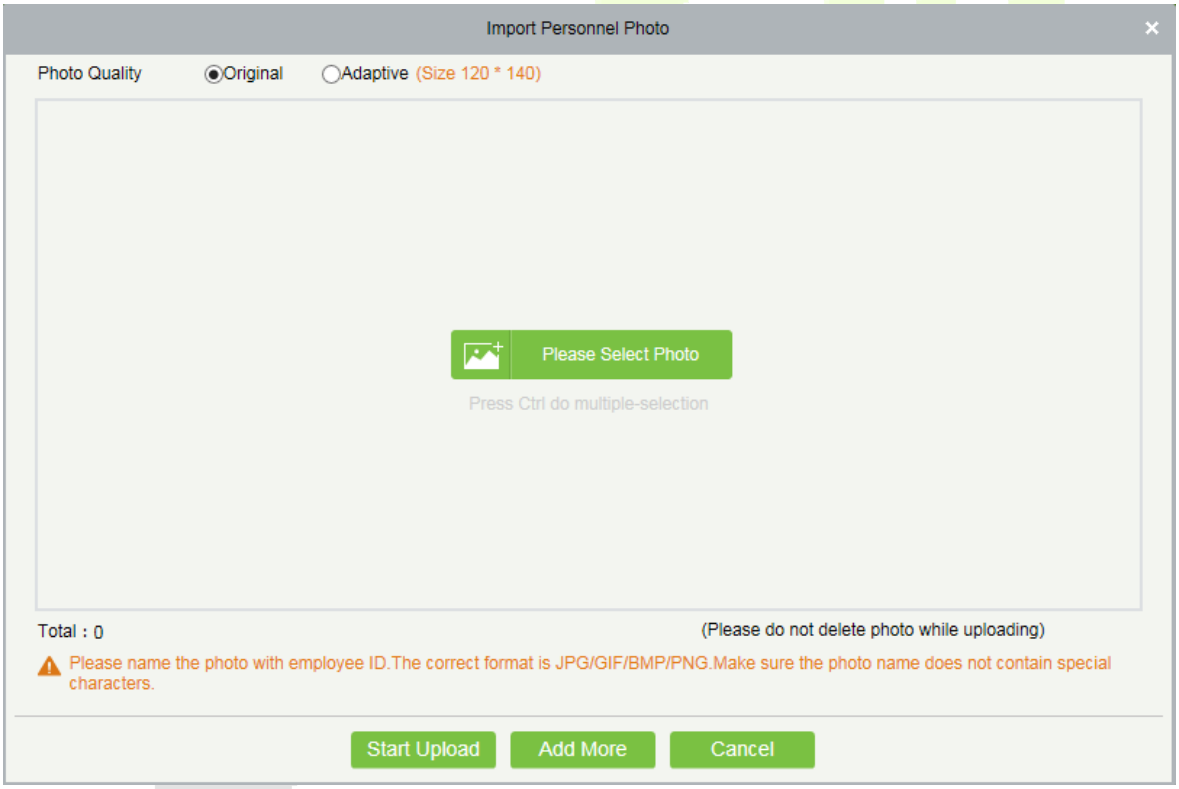
1. Import Personnel: Select "Yes" for [**Update the existed Personnel ID in the system**], the original data will be overwritten when the personnel ID is repeated; select "No", the opposite.



2. Import Biometric Template.



3. Import Personnel Photo: The personnel photo need to be named by personnel ID, supporting common picture formats, such as JPG, JPEG, PNG, GIF, etc., jpeg, png, gif, etc.



Note: You can import the personnel photos in 2 ways: Importing distinctive photos and Compressed package. While importing distinctive photos, the user can import a maximum of 3000 photos at a time. While importing the compresses package, it must be in ZIP format and must not exceed 500MB.

- **Print Card**

Click [**Personnel**] > [**Person**] > [**Import**] to open the card printing interface.

✍Notes:

1) The card template can be defined in [**System**]> [**Basic Management**] > [**Print Template**].

2) Before selecting the printer, the user must first download and install the driver through [**Personnel**] > [**Person**] > [**Parameters**] > [**Registration Client**]. The registration code can be added through [**System**]> [**Authority Management**] > [**Client Register**]. Only after the registration code is registered successfully, the client can do the card printing operation.

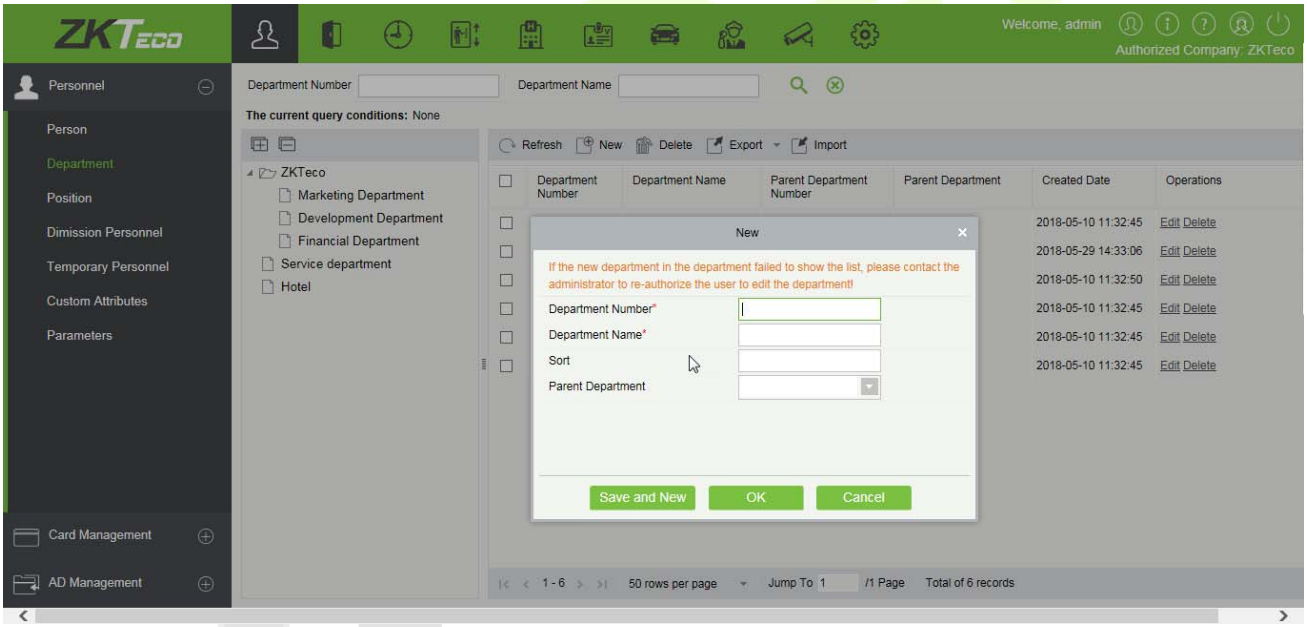
3.1.2 Department

Before managing company personnel, it is required to set a departmental organization chart of the company. Upon the first use of the system, by default it has a primary department named [General] and numbered [1]. This department can be modified but can't be deleted.

Main functions of Department Management include **Add**, **Edit**, **Delete**, **Export** and **Import Department**.

- **Add a Department**

1. Click [**Personnel**] > [**Personnel**] > [**Department**] > [**New**]:



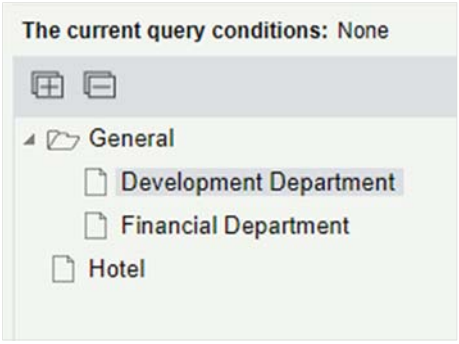
Fields are as followed:

Department Number: Letters and numbers are available. It cannot be identical to the number of another department. The number shall not exceed 30 digits.

Department Name: Any combination of a maximum of 100 characters. In case of different levels, the department names can be repeated.

Sort: Number only. The valid range is 1-999999999. The smaller the number of department sort in a same level, the higher ranks such department have. If this field is empty, it will be arranged in accordance with the increasing order.

Parent department: Select a parent department from the pull-down list. Parent Department is an important parameter to determine the company's organizational chart. On the left of the interface, the company's organizational chart will be shown in the form of a department tree.



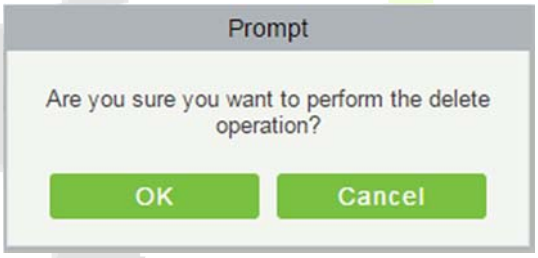
2. After filling the details, you can click [**OK**] to complete adding; click [**Cancel**] to cancel it, or click [**Save and new**] to save and continue adding new department.
3. To add a department, you can also choose **[Import]** to import department information from other software or other documents into this system. For details, see Common Operations.

- **Edit a Department**

Click [**Personnel**] > [**Personnel**] > [**Department**] > [**Edit**].

- **Delete a Department**

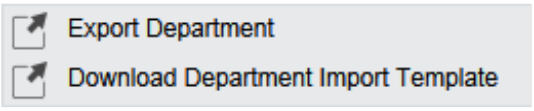
1. Click **[Personnel]** > **[Personnel]** > **[Department]** > **[Delete]**:



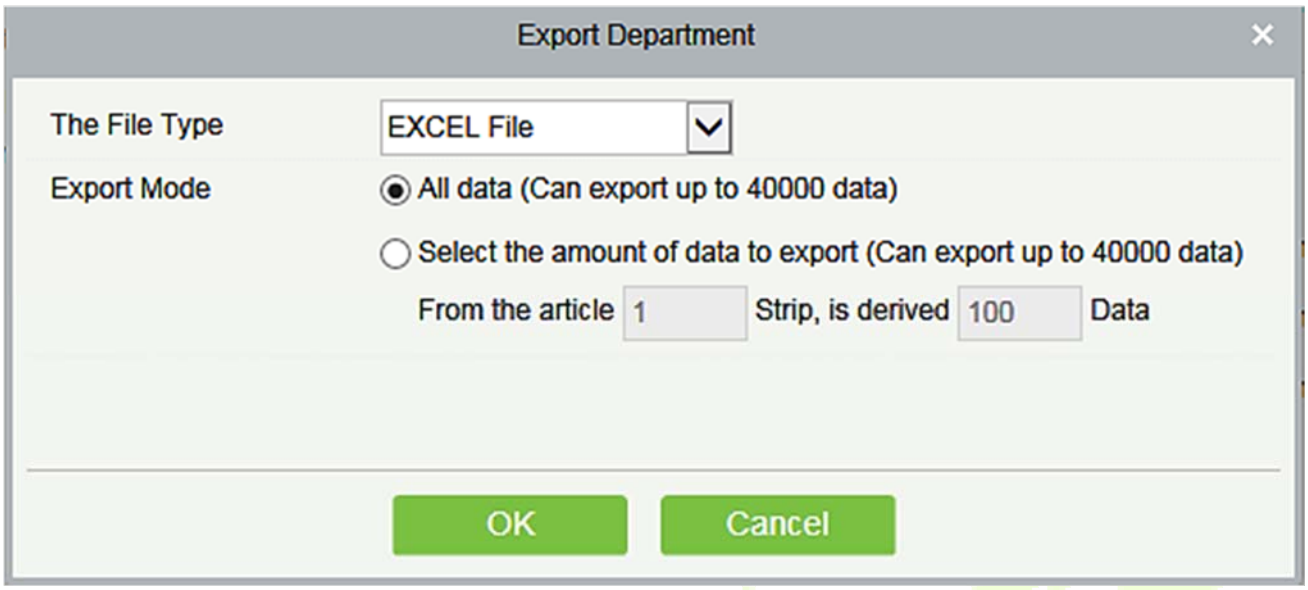
2. Click [**OK**] to delete.

✍**Note:** If the department has sub-departments or personnel, the department cannot be deleted.

- **Export**



1. Export Department includes Exporting Department and Downloading Department Import Template.
2. Department: can be exported in EXCEL, PDF, CSV file format.

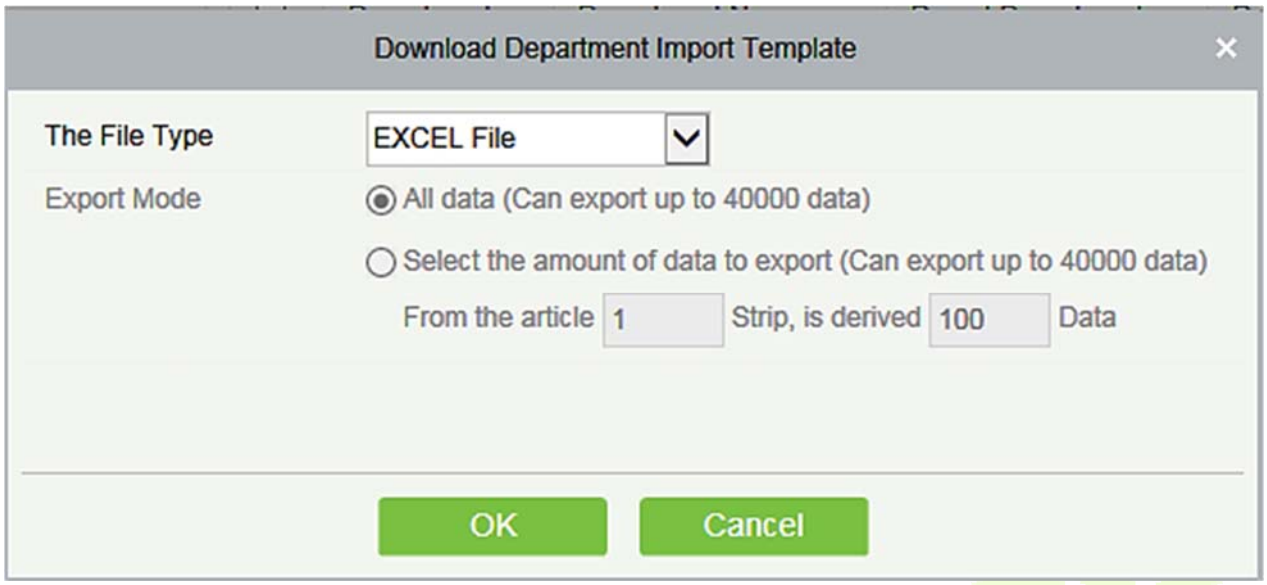


ZKTECO

Department

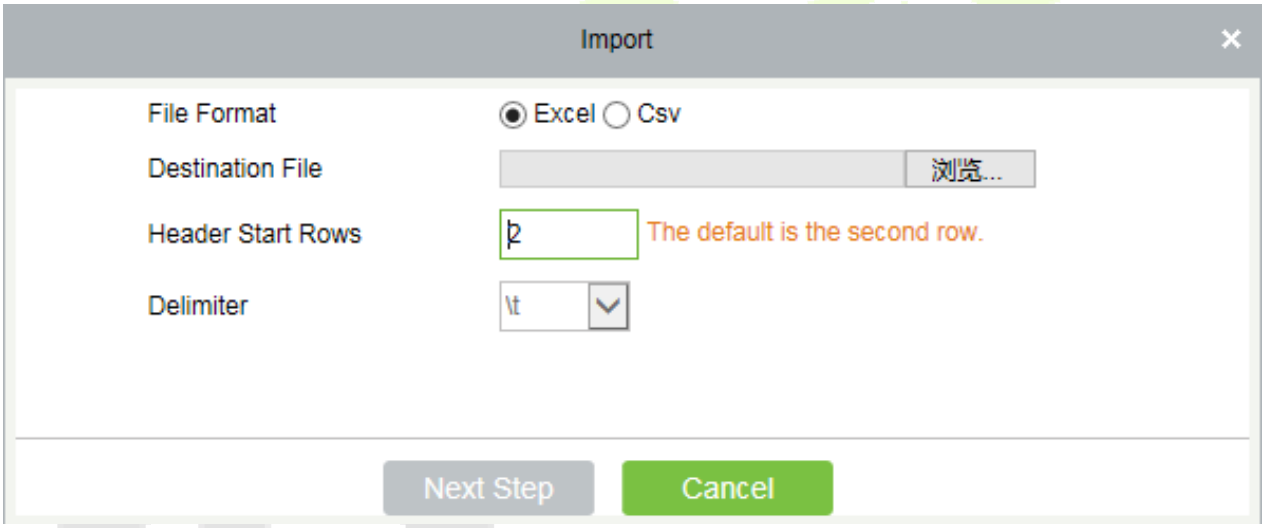
Department Number	Department Name	Parent Department Number	Parent Department	Created Date
hotel	Hotel			2017-12-15 09:06:51
4	Financial Department	1	General	2017-12-15 09:06:48
3	Development Department	1	General	2017-12-15 09:06:48
2	Marketing Department	1	General	2017-12-15 09:06:48
1	General			2017-12-15 09:06:48

3. Download Department Import Template: Excel template file can be exported, and you have to use this template format to import department.

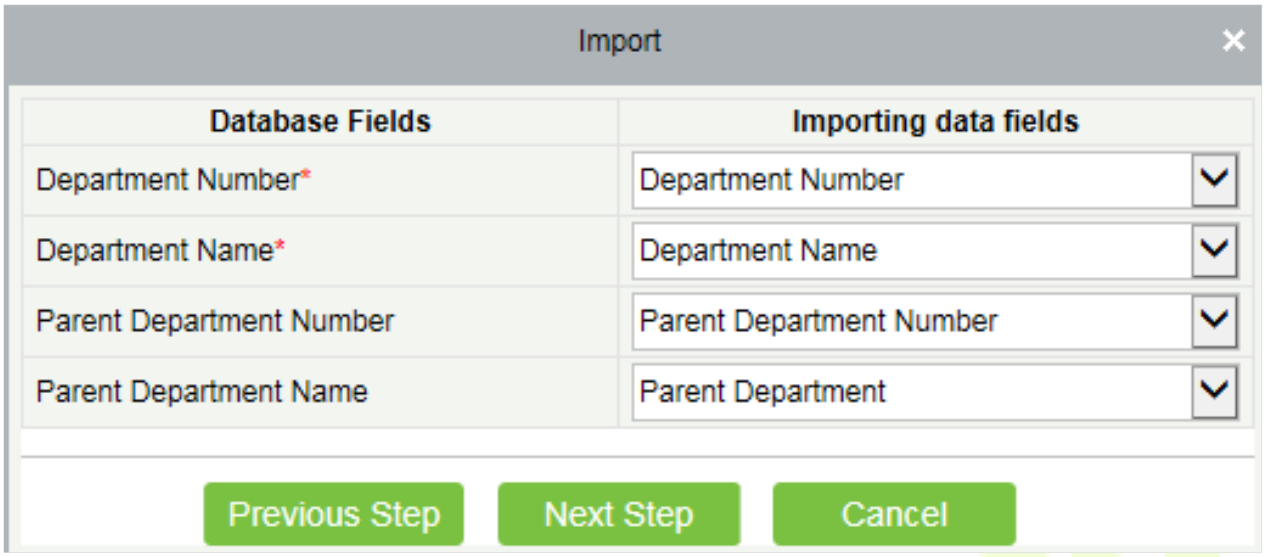


- **Import**

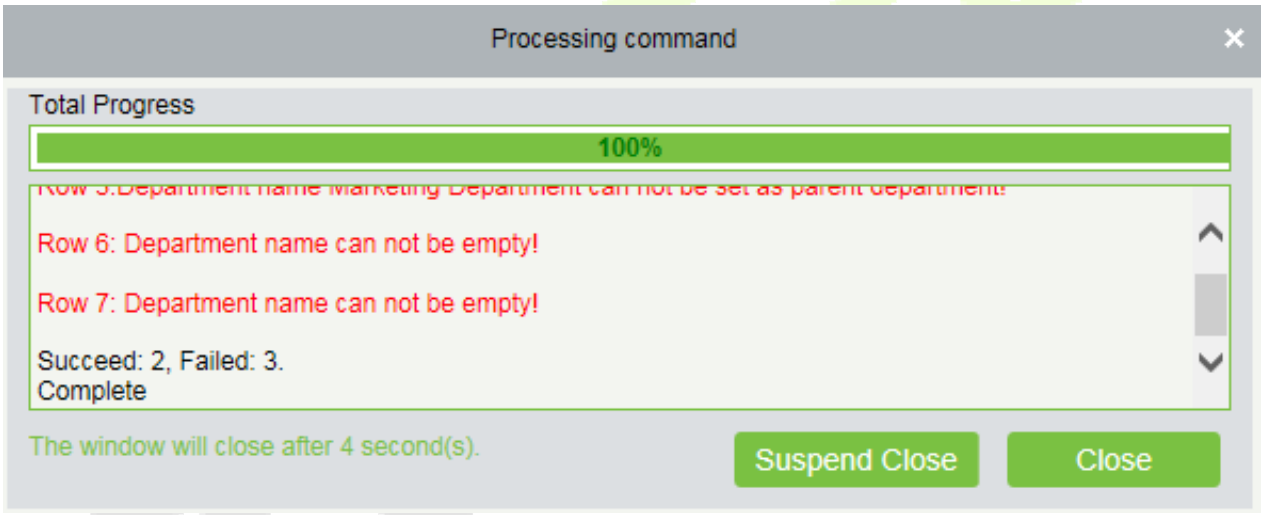
1. Click [**Personnel**] > [**Department**] > [**Import**], the import interface is as follows:



2. Import department information: can import EXCEL, CSV format files.
3. Select the destination file, fill in the header start rows, click [**Next Step**], the interface are as follow:



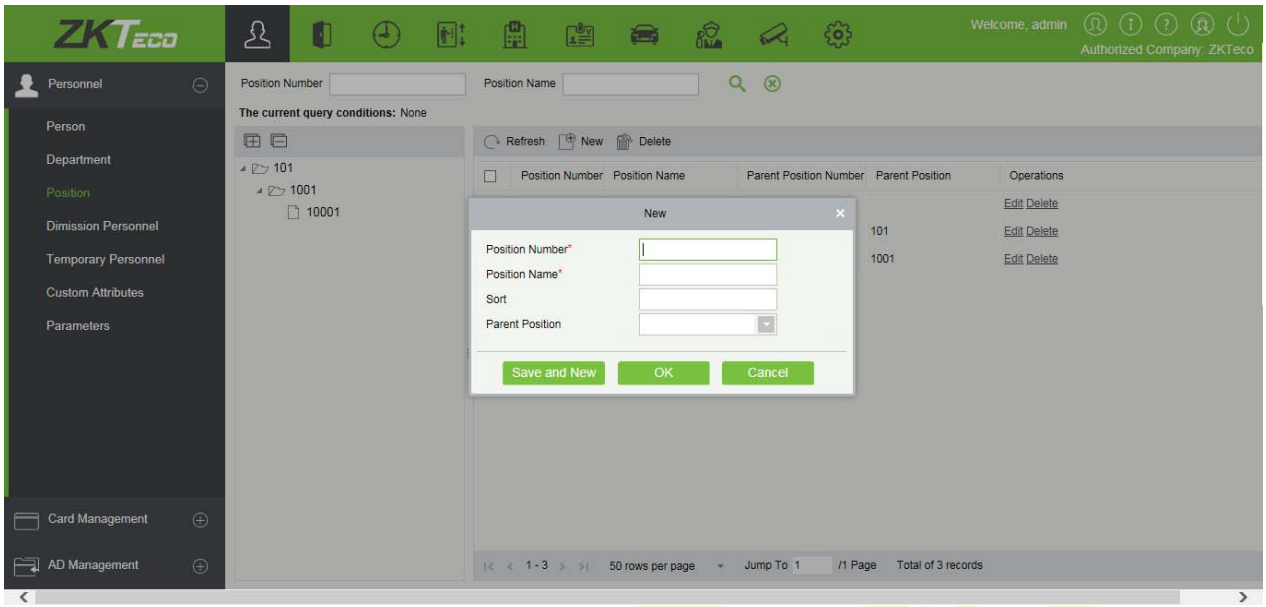
4. After importing the file, the system will match the imported report field and the data segment field automatically. If the matching is incorrect, you can modify it. Click [**Next**].



3.1.3 Position

To organize the personnel as per their competency and skills, you can set position as required. If you set position, you can easily filter report only for a particular post.

1. Click [**Personnel**] > [**Personnel**] > [**Position**] > [**New**]:



Fields are as follows:

Position Number: Set the value of position number. It can be letters or numbers, or combination of both. Special characters are not allowed. Length shall not exceed 30 digits.

Position Name: Set a suitable name for the position. Any character, maximum combination of 100 characters. Position names should not be repeated.

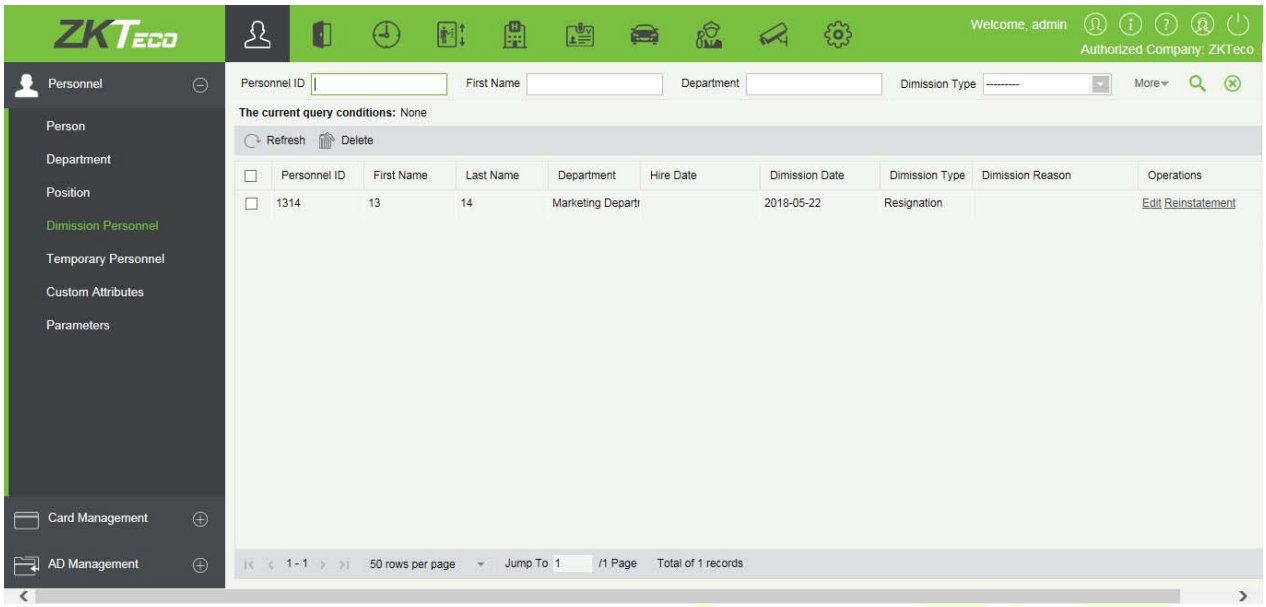
Sort: Supports only numbers. The valid range is 1-999999999. The smaller the number of department sort in a same level, the higher ranking a department has. If not filled in, it will be arranged in accordance with the added order.

Parent Position: By default, there are no position. It is an important parameter to organize the personnel as per their skills and competency.

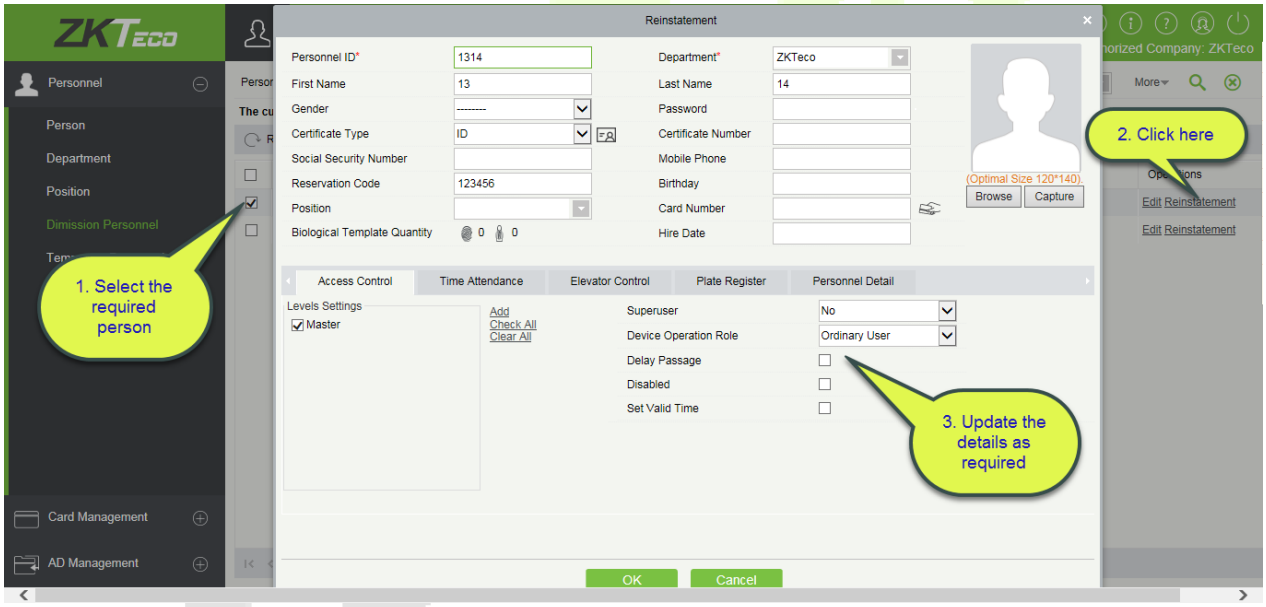
2. Fill the details as required and save.

3.1.4 Dimission Personnel

This parameter will display the personnel who are not working in company anymore. Once the person is dimissoned, it will be listed here.



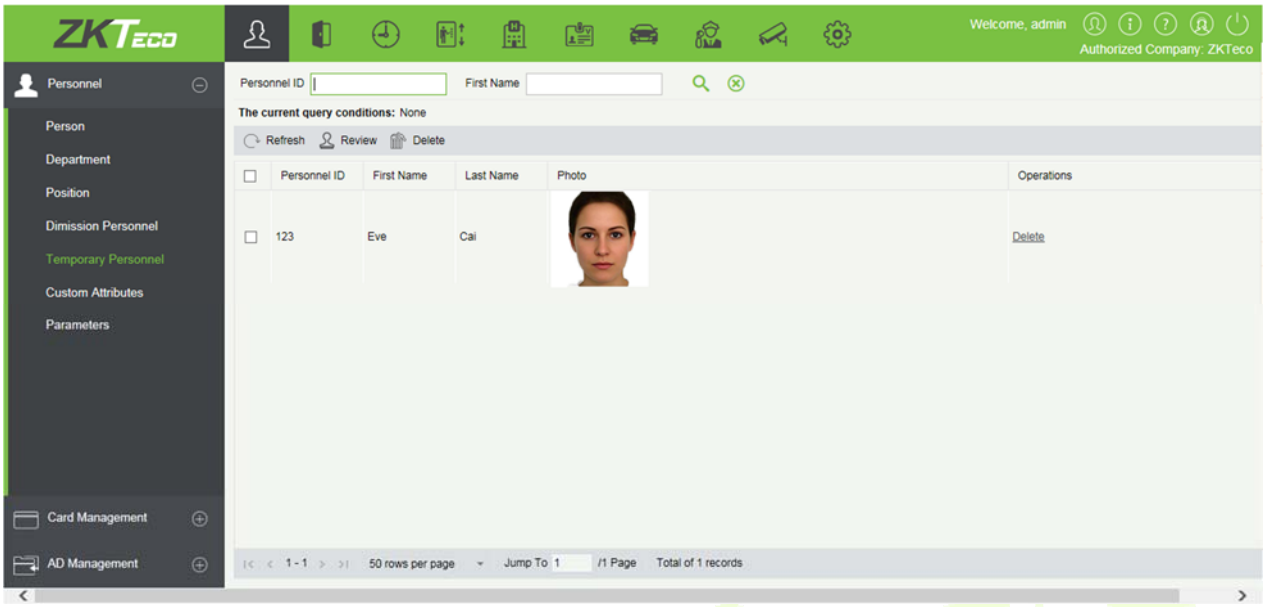
1. You can re-employ personnel by selecting the required employee and click [**Reinstatement**] below operations tab.



2. Once the details are updated, click [**OK**] to save.

3.1.5 Temporary Personnel

This parameter will display the personnel who are uploaded by scanning the QR code of the big-screen facial recognition time and attendance device (uFace WG100).

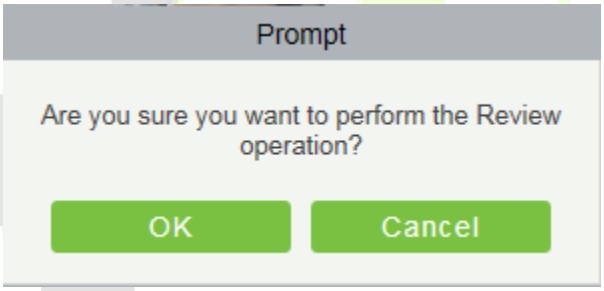


- **Refresh**

Click [**Refresh**] at the upper part of the list to load new temporary personnel.

- **Review**

Select a temporary personnel and click [**Review**]:



The person reviewed will be automatically added to the list of person.

- **Delete**

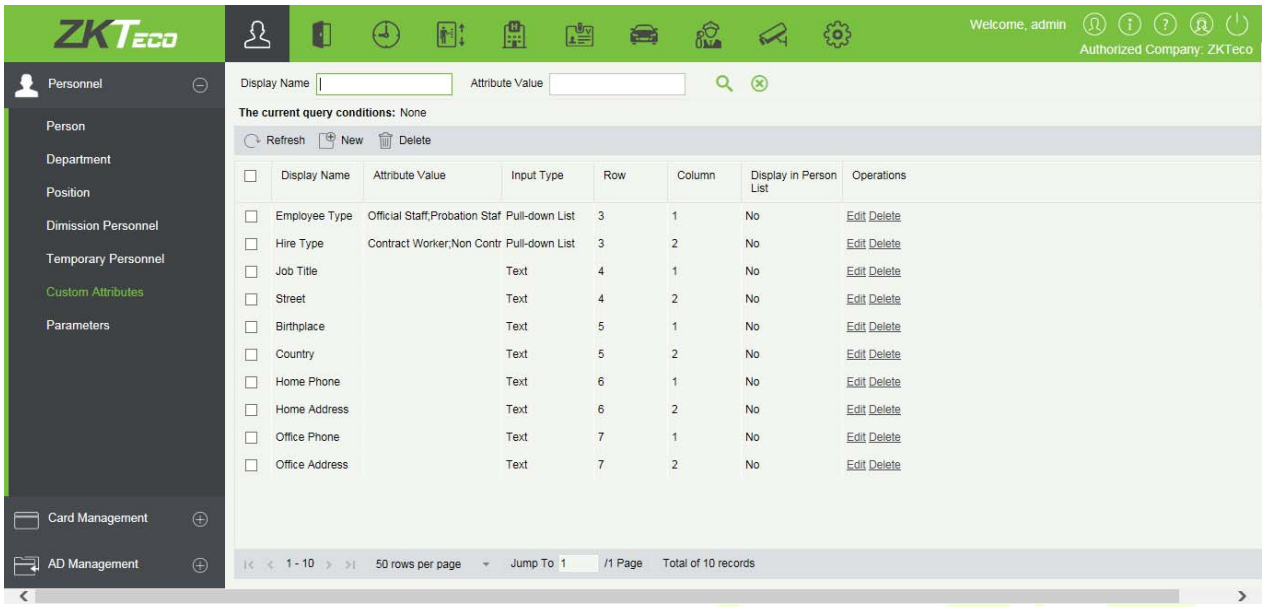
Delete the selected temporary personnel.

3.1.6 Custom Attributes

Some personal attributes can be customized or deleted to meet different customers' requirements. When the system is used for the first time, the system will initialize some personal attributes by default. Customized personal attributes can be set for different projects according to requirements.

- **New a Custom Attribute**

Click [**Personnel**] > [**Personnel**] > [**Custom Attributes**] > [**New**], then edit the parameters and click [**OK**] to save and exit.



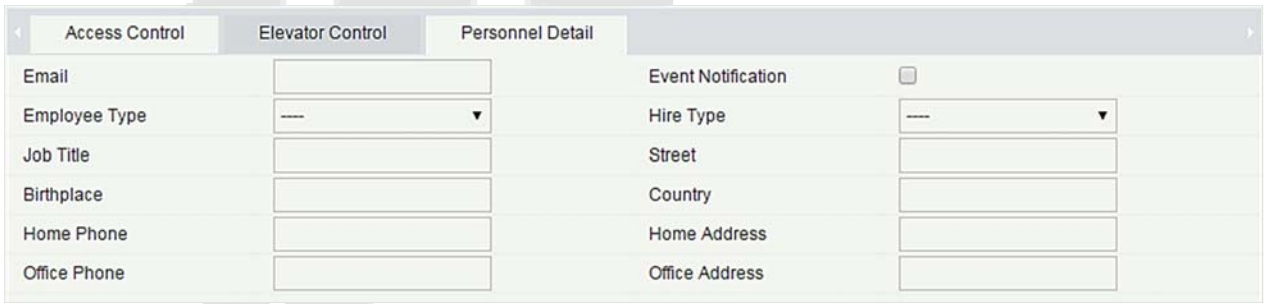
Fields are as follows:

Display Name: Must be filled and should not be repeated. Max length is 30.

Input Type: Select the display type from "Pull-down List", "Multiple Choice", "Single Choice" and "Text".

Attribute Value: Suitable for lists displaying as ''Pull-down List'', ''Multiple Choice'' and ''Single Choice'' lists. Use a ";" to distinguish the multiple values. If the input type is "Text", the attribute value is not suitable.

Row/Colum: The column and row of a field are used together to control the display position of the field. Numerals are supported. The column number cannot exceed 99, and the row number can only be 1 or 2. The combination of the column and row must not be duplicated. As shown in the following figure, Employee Type, is in the first column and first row, and Hire Type is in the first column and second row.



- **Editing a Custom Attribute**

Click [**Edit**] to modify the corresponding attributes.

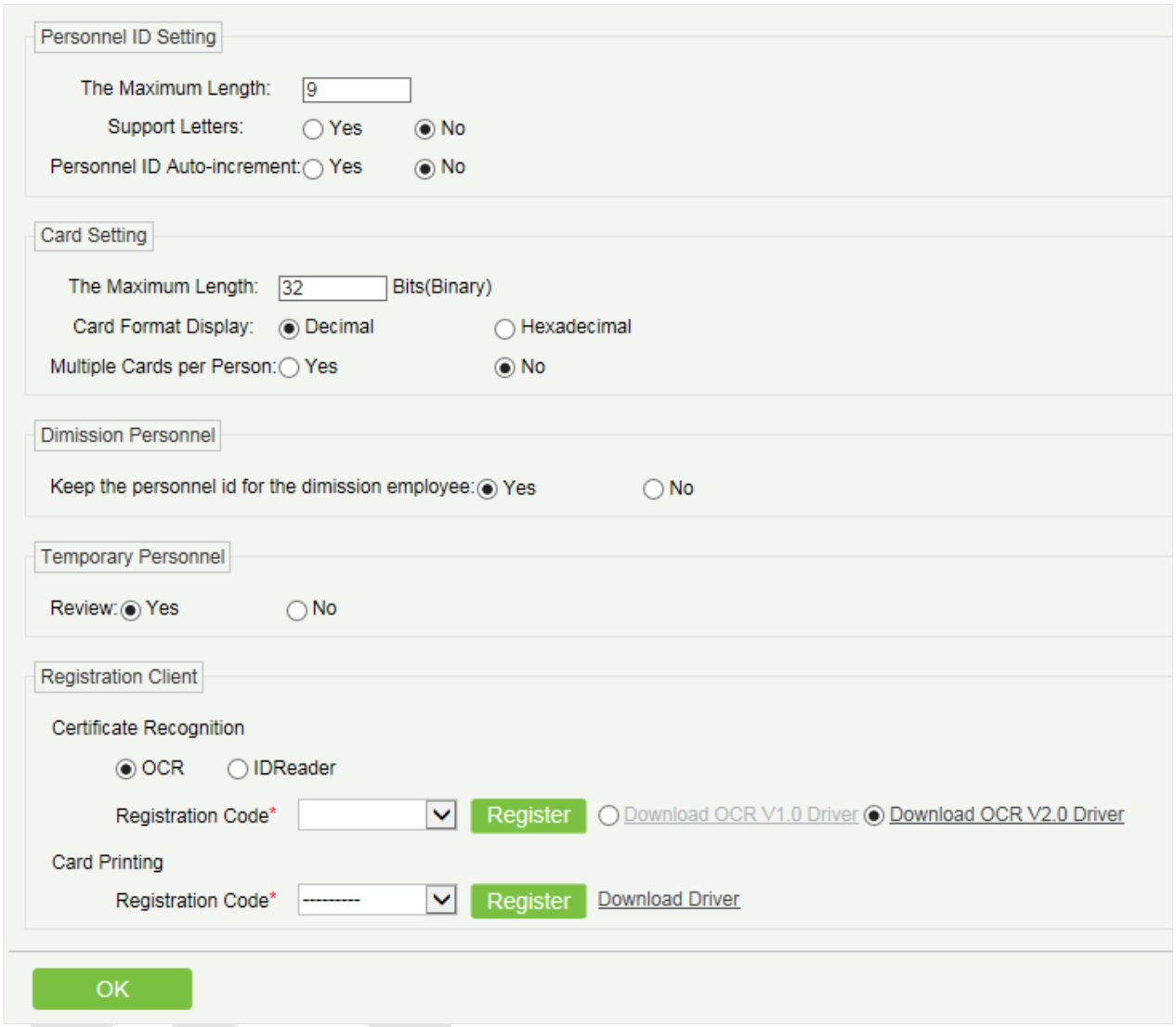
- **Deleting a Custom Attribute**

Click [**Delete**] to delete an unused attribute. If the attribute is in use, the system will pop up confirmation before confirming to delete.

✍**Note:** The custom attribute will not be recovered once deleted.

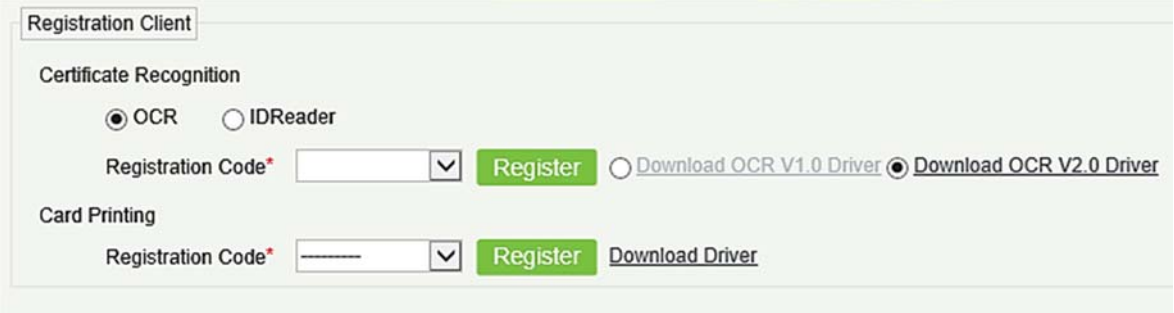
3.1.7 Parameters

1. Click [**Personnel**] > [**Personnel**] > [**Parameters**]:



2. Set the maximum length for a Personnel ID. And whether it will support letters or not. If Personnel ID Auto increment is selected as Yes, then while adding personnel one by one, the ID in field automatically updates to the next new number.
3. Set the maximum length (binary number) of the card number that the current system will support.
4. Set whether the personnel ID for the demission employee can be kept.
5. Set whether the temporary personnel uploaded and registered by scanning the QR code of the big-screen facial recognition time and attendance device need to review.
6. Set the card format currently used in the system. The card format cannot be switched once it is set up.
7. Set whether "Multiple Cards per Person" will be allowed or not.
8. Used the QR code to Self-Registration.
9. Registration Client.

➢ If no driver has been installed, the [Download Driver] link is displayed. Click the link to download and install the driver.



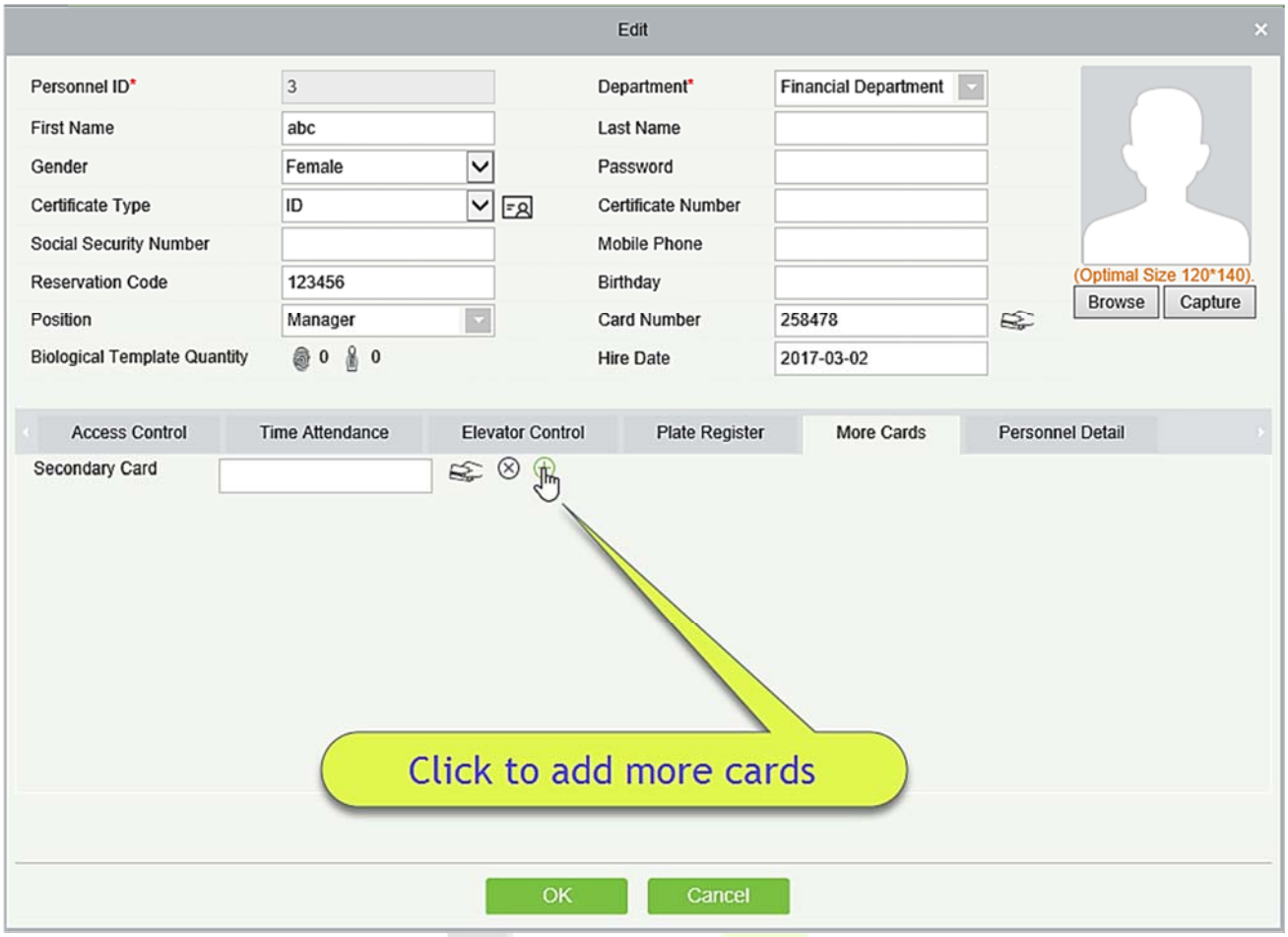
➢ Select the corresponding registration code and click [**Register**].

✍**Note:** Click [**System**] > [**Authority Management**] > [**Client Register**] to view the registration code.

10. Click [**OK**] to save the settings and exit.

- **More Cards**

After the "Multiple cards per person" function is enabled, you can set multiple cards on the Personnel page.



✍**Note:** Not all devices support this function. For details, please consult the technical personnel.

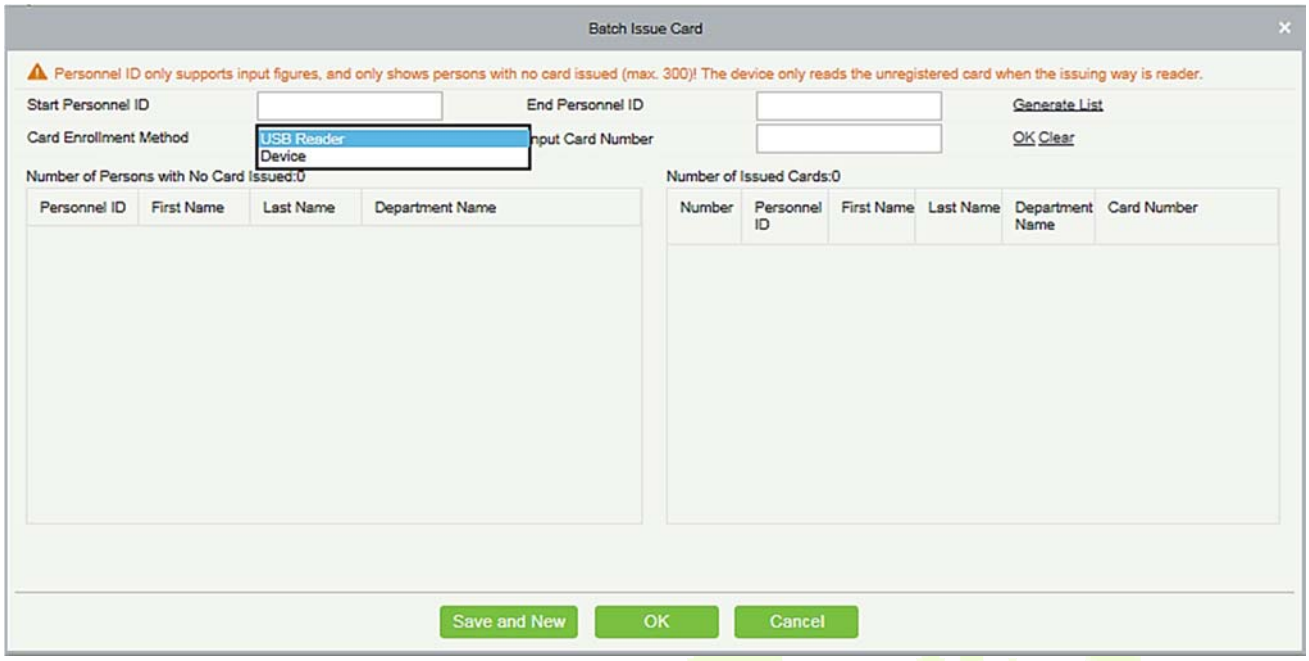
3.2 Card Management

There are three modules in card management: Card, Wiegand Format and Issue Card Record.

3.2.1 Card

- **Batch Issue Card**

1. Click [**Personnel**] > [**Card Manage**] > [**Batch Issue Card**]:



2. Enter Start and End Personnel No. and click [**Generate List**] to generate personnel list and show all personnel without cards within this number series.

✍**Note:** The Start and End Personnel No. only support numbers.

3. Select Card Enrollment Method: Register with a USB Reader or device.

If you want to enroll a card with a USB Reader, you may place the card over the "issue machine" directly. The System will get the card number and issue it to the user in the list on the left.

For the use of device, you need to select the position of punching, click [**Start to read**], the system will read the card number automatically, and issue it to the user in the list on the left one by one. After that, click [**Stop to read**].

✍**Note:** During the "Batch Issue Card", system will check whether the card issuer issues card or not, if card has been issued before, the system will prompt "The Card Number has already been issued".

4. Click [**OK**] to complete card issue and exit.

3.2.2 Wiegand Format

Wiegand Format is the card format that can be identified by the Wiegand reader. The software is embedded with 9 Wiegand formats. You may set the Wiegand card format as needed.

Name	Mode	Site Code	Auto	Operations
Wiegand 형식26	Mode One	0	Yes	Edit
Wiegand 형식26a	Mode One	0	No	Edit
Wiegand 형식34	Mode One	0	Yes	Edit
Wiegand 형식34a	Mode One	0	No	Edit
Wiegand 형식36	Mode One	0	Yes	Edit
Wiegand 형식37	Mode One	0	Yes	Edit
Wiegand 형식37a	Mode One	0	No	Edit
Wiegand 형식50	Mode One	0	Yes	Edit
Wiegand 형식66	Mode One	0	Yes	Edit
5656	Mode One	0	No	Edit Delete

Card Formats Testing

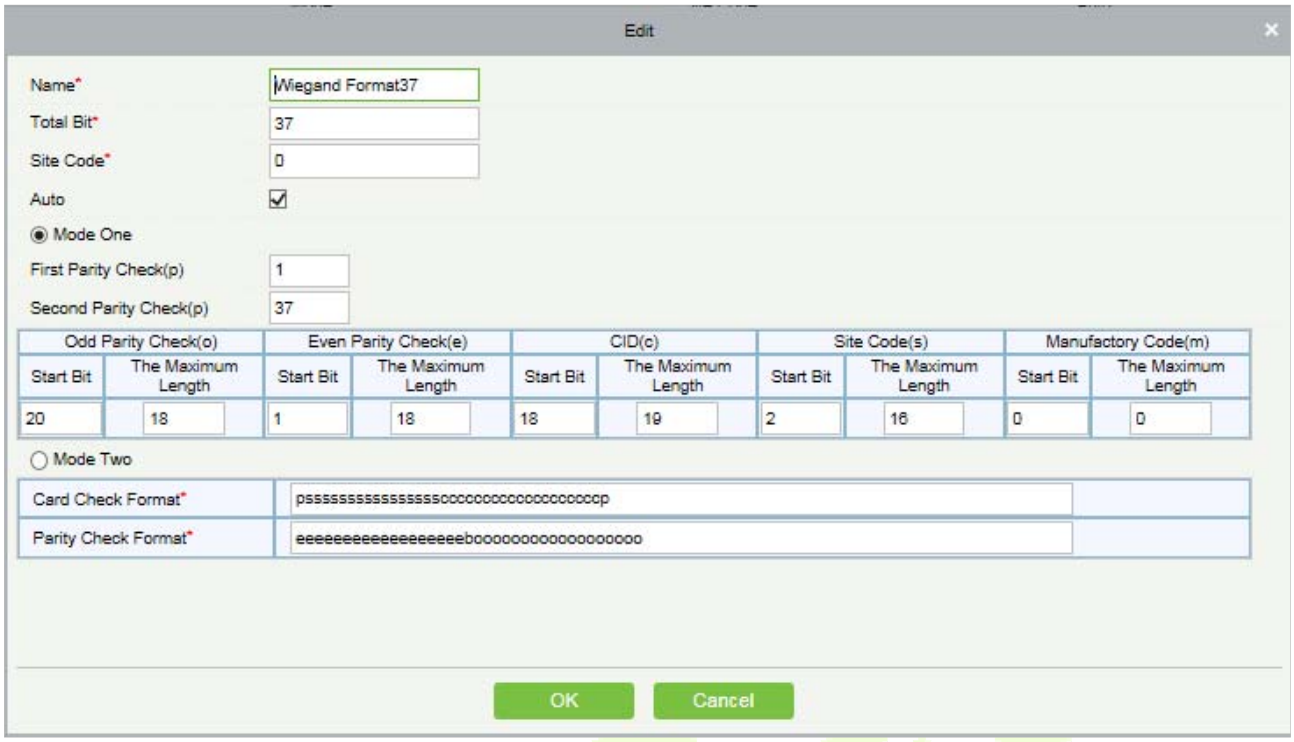
When the card number does not match with the one which is displayed on the system, the user can use the **Card Formats Testing function** to calibrate the Wiegand format. The page is explained as follows:

Select the device that supports the card format test function, and fill the card number and the site code (optional):

1) Click [**Read Card**], and swipe the card on the reader.The original card number will be displayed on the **Original Card Number** text box.
2) Click [**Recommended Card Format**] and the recommended Wiegand card format will be displayed below.
3) Click [**Auto calculate site code while the site code is left bank**] and the software will calculate the site code according to the card format and card number.
4) Click [**OK**] and the page will jump to the Wiegand format page to save the new Wiegand format.

✍**Note:** The card format testing function is only supported by few devices.

This software supports two modes for adding the Wiegand Format:If mode 1 does not meet your setting requirements, you may switch it to mode 2. Take Wiegand Format 37 as an example:



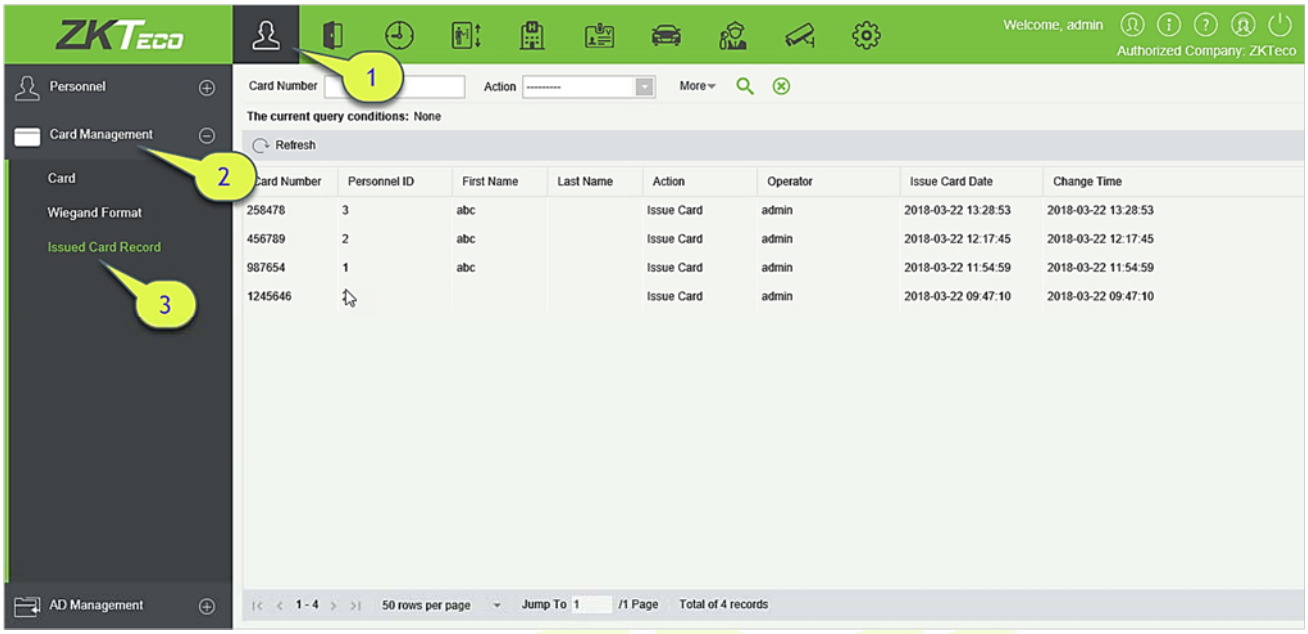
Format Specifying:

"P" indicates Parity Position; "s" indicates Site Code; "c" indicates Cardholder ID; "m" indicates Manufactory Code; "e" indicates Even Parity; "O" indicates Odd Parity; "b" indicates both odd check and even check; "x" indicates parity bits no check.

The previous Wiegand Format 37: the first parity bits (p) check "eeeeeeeeeeeeeeeee"; the second parity bits check "ooooooooooooooooo". Card Check Format can only be set "p, x, m, c, s"; Parity Check Format can only be set "x, b, o, e".

3.2.3 Issue Card Record

It records the life cycle of a card and display the operations performed on the card.



✍**Note:** The cards and card issuing records of an employee will be deleted altogether when the employee's account is deleted completely.

4 Access

The system needs to be connected to an access controller to provide access control functions. To use these functions, the users must install devices and connect them to the network first, then set corresponding parameters, so that they can manage devices, upload access control data, download configuration information, output reports and achieve digital management of the enterprise.

4.1 Device

Add an access device, then set the communication parameters of the connected devices, including system settings and device settings. When communication is successful, you can view here the information of the connected devices, and perform remote monitoring, uploading and downloading etc.

4.1.1 Device

- **Add Device**

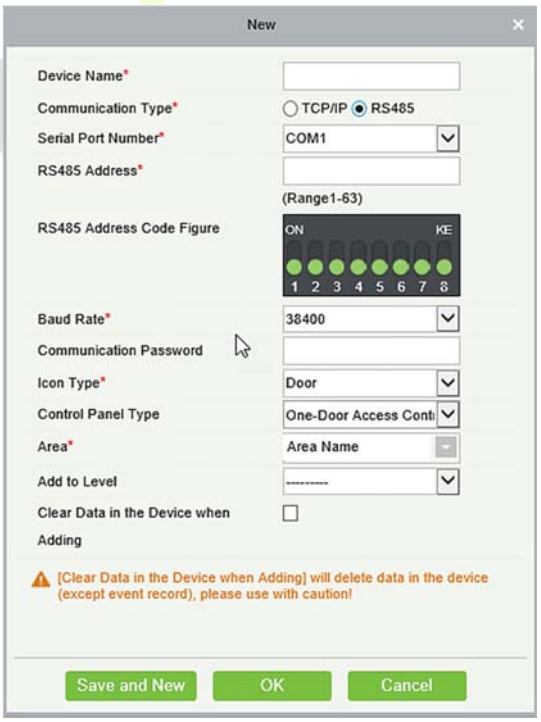
There are two ways to add Access Devices.

1. Add Device by manually

A. Click [**Access Device**] > [**Device**] > [**New**] on the Action Menu, the following interface will be shown:

TCP/ IP communication mode

RS485 communication mode



Fields are as follows:

IP Address: Enter the IP Address of the access controller.

Communication port: The default value is 4370.

Serial Port No.: COM1~COM254.

RS485 Address: The machine number, ranging from 1 to 63. If Port No. is the same, it is not allowed to set repeated RS485 addresses.

Baud Rate: Same as the baud rate of the device. The default is 38400.

RS485 Address Code Figure: Display the code figure of RS485 address.

Common options:

Device Name: Any character, up to a combination of 20 characters.

Communication Password: A maximum of 6 digits; both number and letters are available.

✍Notes:

- You do not need to input this field if it is a new factory device or just completed initialization.
- When communication password for the standalone device's is set as "0", it means no password. However, in case for access control panel, it means the password is 0.
- You need to restart the device after setting the door sensor of the standalone device.

Icon Type: It will set the representation of the device. You can choose as per the kind of device; Door, Parking barrier, Flap Barrier.

Control Panel Type: One-door access control panel, two-door access control panel, four-door access control panel, Standalone Device.

Area: Select specific areas of devices. After setting areas, devices (doors) can be filtered by areas upon Real-Time Monitoring.

Switch to Two-door Two-way: When the control panel type is set to the four-door access control panel, the four-door access control panel can be switched to the two-door two-way access control panel in the system.

Add to Level: Automatically add the device to the selected level. The device cannot be automatically added to the selected level if the number of personnel exceeds 5000. You can add personnel after the device is successfully added.

Clear Data in the Device when Adding: If this option is checked, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

B. After editing, click [**OK**], and the system will try to connect the current device.

If it is successfully connected, it will read the corresponding extended parameters of the device.

Extended Device Parameters: It includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity.

✍**Note:** When deleting a new device, the software will clear all user information, time zones, holidays, and access control levels settings (including access levels, anti-pass back, interlock settings, linkage settings etc.) from the device, except the events records (unless the information in the device is unusable, or it is recommended not to delete the device in used to avoid loss of information).

Access Controller Settings:

- TCP/ IP Communication Requirements

Supports enabling TCP/ IP communication, directly connect device to the PC or connect to the local network, input the IP address and other information of the device.

- RS485 Communication Requirements

Supports enabling RS485 communication, connect device to PC by RS485, input the serial port number, RS485 machine number, band rate and other information of the device.

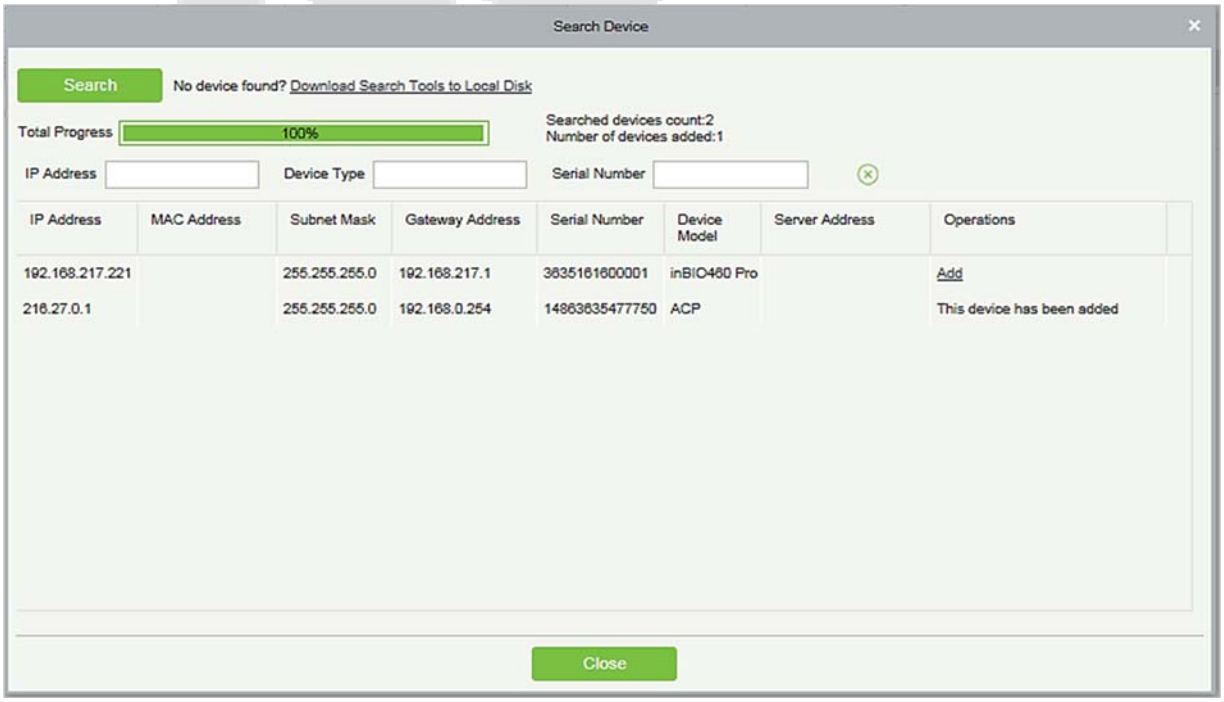
2. Add Device by Searching Access Controllers

Search the access controllers in the Ethernet.

1) Click [**Access Device**] > [**Device**] > [**Search Device**], to open the Search interface.

2) Click [**Search**], and it will prompt [Searching……].

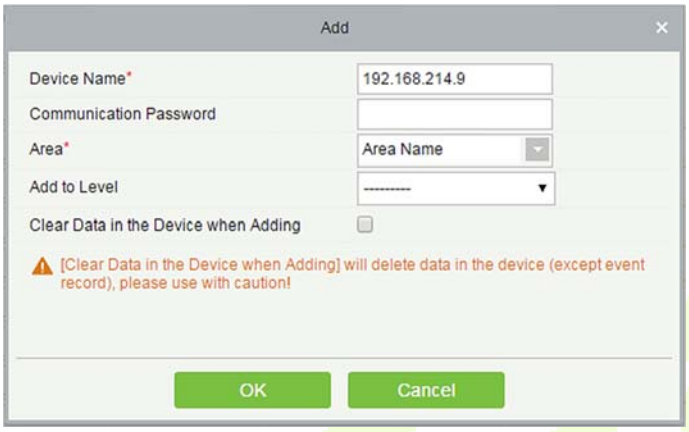
3) After searching, the list and total number of access controllers will be displayed.



✍**Note:** UDP broadcast mode will be used to search access device. This mode cannot perform cross-Router function. IP address can provide cross-net segment, but it must be in the same subnet, and needs to be configured the gateway and IP address in the same net segment.

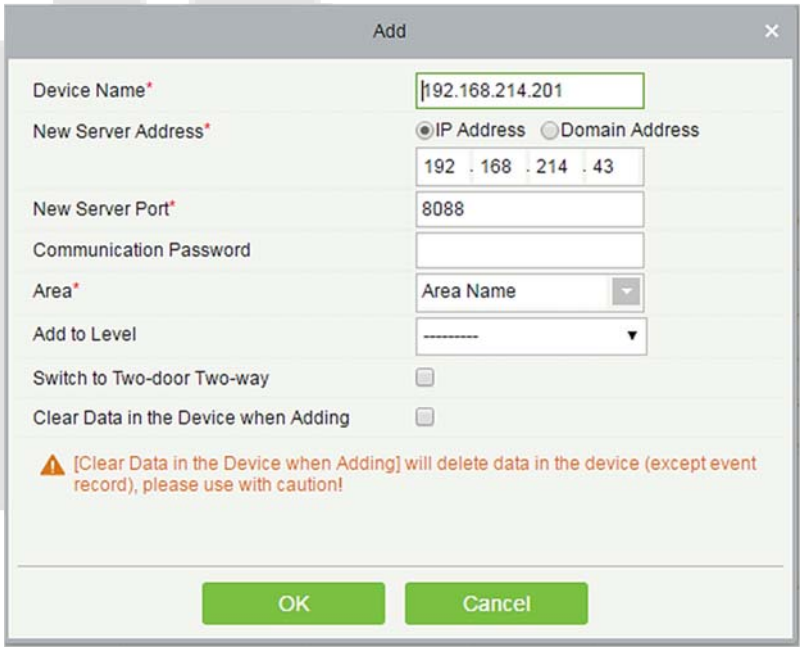
4) Click on [**Add**] in the search list.

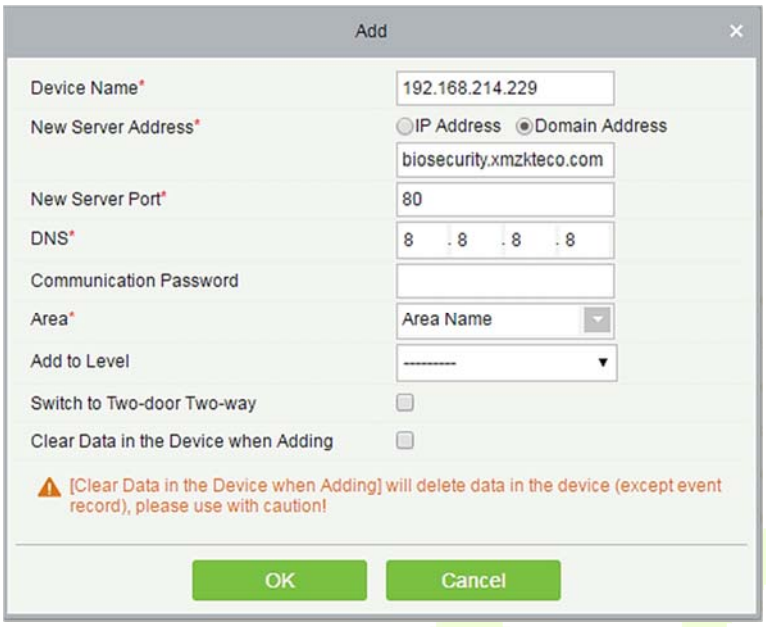
If the device is a pull device, you may input a device name, and click [**OK**] to complete device adding.



Clear Data in the device when Adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs).

If the device is a push firmware device, the following windows will pop-up after clicking [**Add**]. If IP Address in [**New Server Address**] is selected, then configure IP address and port number. If Domain Address in [**New Server Address**] option is selected, then configure domain address, port number and DNS. Device will be added to the software automatically.





New Server Address: To add a device by IP Address or Domain Address, devices can be added to the software by entering the domain address.

New Server Port: Set the access point of system.

DNS: Set a DNS address of the server.

Clear Data in the Device when Adding: If this option is selected, then after adding device, the system will clear all data in the device (except the event logs). If you add the device merely for demonstration or testing, there is no need to tick it.

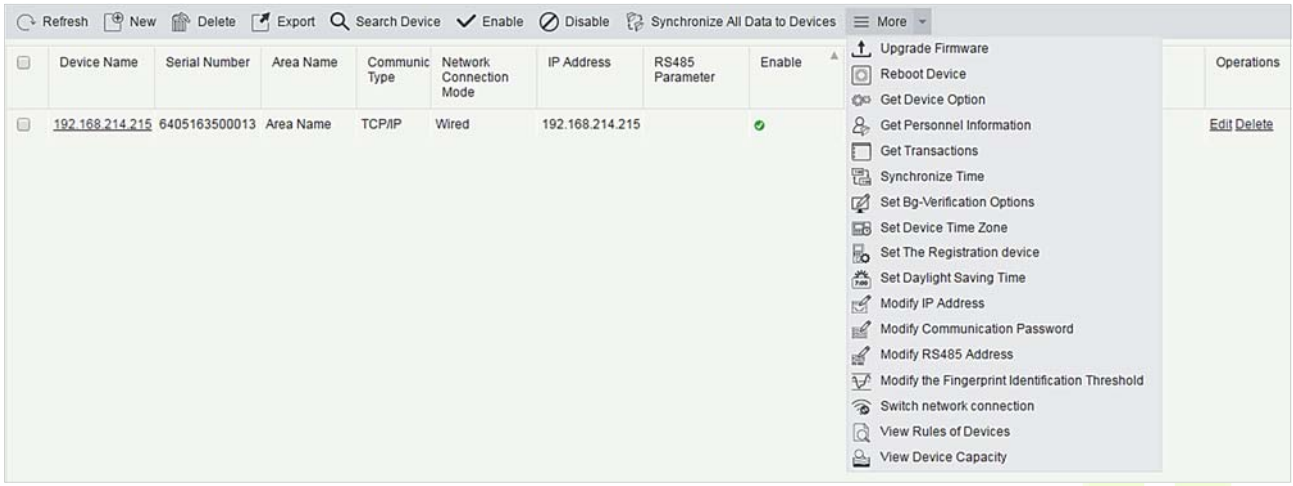
✍**Note:** When using either of the above three device adding methods, if there exist residual data in the original device, please sync original data to it after adding a new device to the software by clicking [**Device**] > [**Synchronize All Data to Devices**], otherwise these original data may conflict with normal usage.

5) The default IP address of the access device may conflict with the IP of a device on the Local network. You can modify its IP address: click [**Modify IP Address**] beside the [**Add**] and a dialog box will pop up in the interface. Enter the new IP address and other parameters (Note: Configure the gateway and IP address in the same net segment).

✍**Note:** Some PUSH devices support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

4.1.2 Device Operation

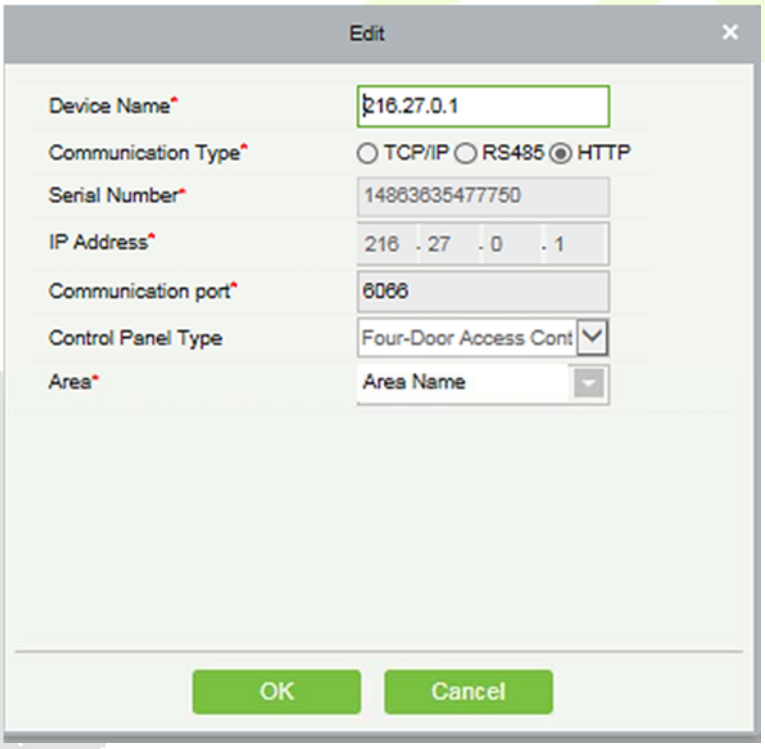
For communication between the system and device; data uploading, configuration downloading, device and system parameters shall be set. Users can edit access controllers within relevant levels in the current system; users can only add or delete devices in Device Management if needed.



- **Edit or Delete a Device**

Edit: Click Device Name or click [**Edit**] to access the edit interface.

Delete: Select device, click [**Delete**], and click [**OK**] to delete the device.

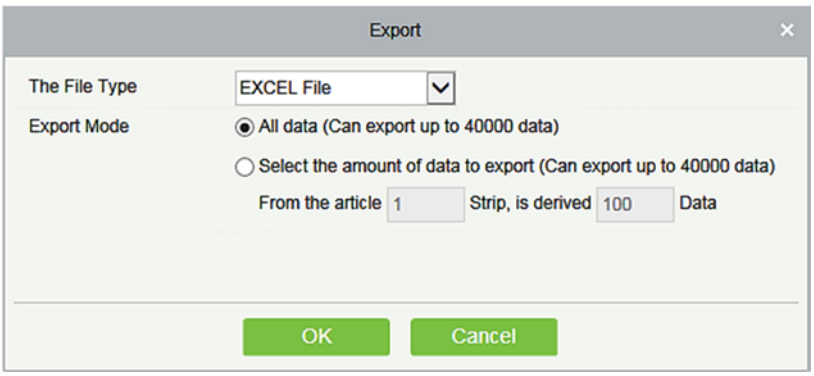


For the details and settings of the above parameters, see Device. Items in grey are not editable. The device Name should be unique and must not be identical to another device.

Access Control Panel Type cannot be modified. If the type is wrong, users need to manually delete the device and add it again.

Export

Device information can be exported in EXCEL, PDF, CSV file format.



ZKTECO

Device

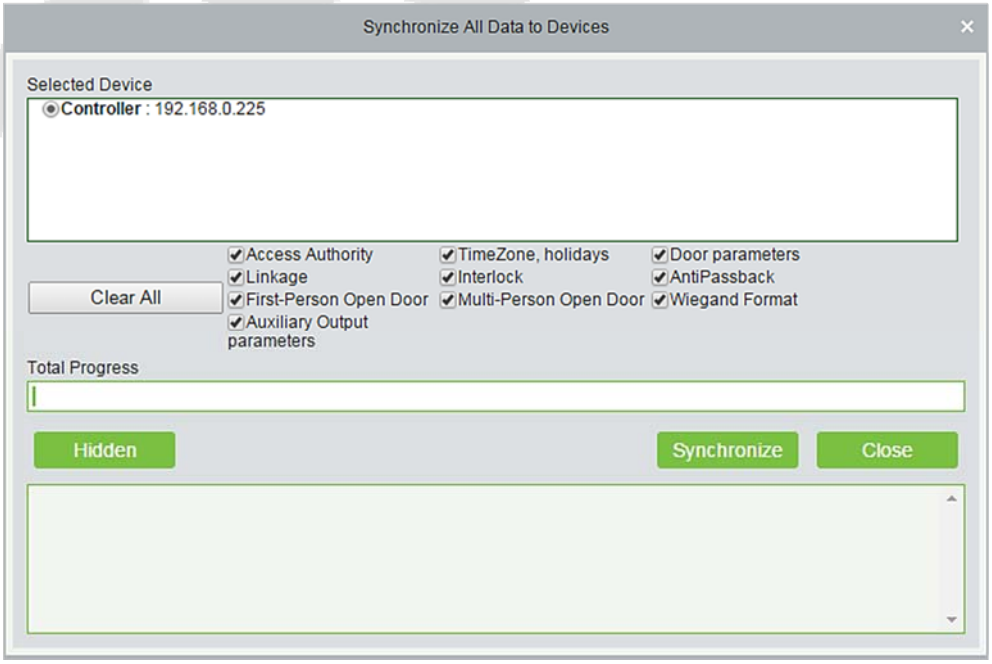
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Disable/Enable

Select device, click [**Disable/Enable**] to stop/start using the device. When communication between the device and the system is interrupted or device fails, the device may automatically appear in disabled status. After adjusting local network or device, click [**Enable**] to reconnect the device and restore device communication.

Synchronize All Data to Devices

Synchronize data of the system to the device. Select device, click [**Synchronize All Data to Devices**] and click [**OK**] to complete synchronization.



✍**Note:** [**Synchronize All Data to Devices**] will delete all data in the device first (except transactions), and thus download all settings again. Please keep the internet connection stable and avoid power down situations. If the device is working normally, please use this function with caution. Execute it in rare user situations to avoid impact on normal use of the device.

- **Upgrade Firmware**

Tick the device that needs to be upgraded, click [**Upgrade firmware**] to enter edit interface, then click [**Browse**] to select firmware upgrade file (named emfw.cfg) provided by Access software, and click [**OK**] to start upgrading.

✍**Note:** The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware or upgrade it following the instructions of the distributor. Unauthorized upgrade may affect normal operations.

- **Reboot Device**

It will reboot the selected device.

- **Get Device Option**

It gets the common parameters of the device. For example, get the firmware version after the device is updated.

- **Get Personnel Information**

Renew the current number of personnel, fingerprints, finger vein and face templates in the device. The final value will be displayed in the device list.

- **Get Transactions**

Get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.

Get New Transactions: The system only gets new transactions since the last collected and recorded transaction. Repeated transactions will not be rewritten.

Get All Transactions: The system will get transactions again. Repeated entries will not be shown twice.

When the network status is healthy and the communication between the system and device is normal, the system will acquire transactions of the device in real-time and save them into the system database. However, when the network is interrupted or communication is interrupted for any reasons, and the transactions of the device have not been uploaded into the system in real-time, [Get Transactions] can be used to manually acquire transactions of the device. In addition, the system, by default, will automatically acquire transactions of the device at 00:00 on each day.

✍**Note:** Access controller can store up to 100 thousand of transactions. When transactions exceed this number, the device will automatically delete the oldest stored transactions (deletes 10 thousand transactions by default).

- **Synchronize Time**

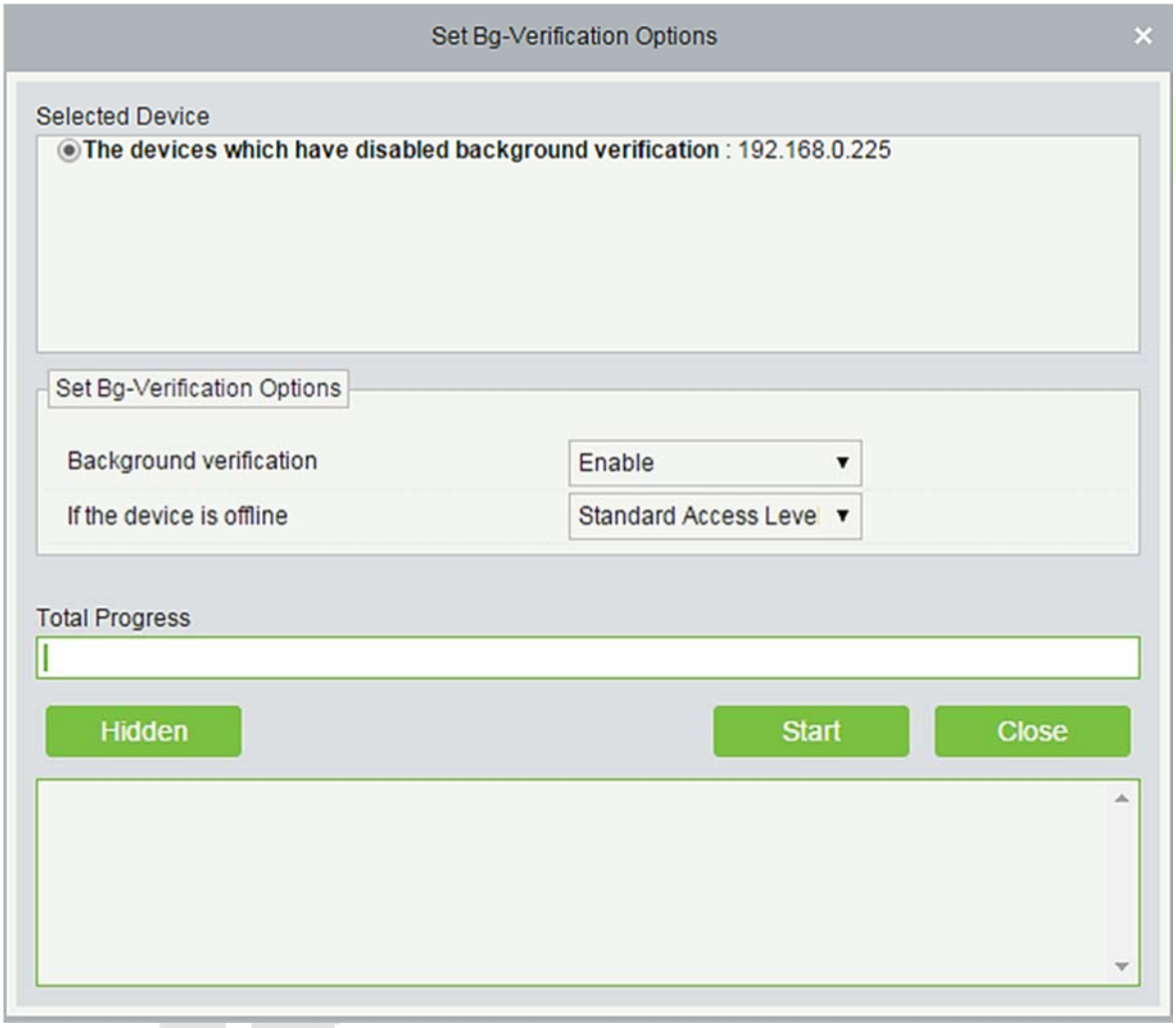
It will synchronize device time with server's current time.

- **Set Server**

It will set parameters of the device connected to the server.

- **Set Background Verification Parameters**

1. Select the required online device; click [**More**] > [**Set Bg verification parameters**]:



Background verification: Enable or Disable Background verification function.

If the device is offline: If the controller is offline, the device has levels of Standard Access Level or Access Denied.

2. After setting parameters, click [Start] button to issue command to the device setting.

✍**Note:** If you need advanced access control functions, please enable [Background verification], and issue the background verification parameters to the device.

- **Set Device Time Zone**

If the device supports the time zone settings and is not in the same time zone with the server, you need to set the time zone of the device. After setting the time zone, the device will automatically synchronize the time according to the time zone and server time.

- **Set Daylight Saving Time**

According to the requirements of different regions, set Daylight Saving Time rules.

- **Modify IP Address**

Select a device and click [**Modify IP address**] to open the modification interface. It will obtain a real-time network gateway and subnet mask from the device. (Failed to do so, you cannot modify the IP address). Then enter a new IP address, gateway, and subnet mask. Click [**OK**] to save and quit. This function is the similar as [Modify IP Address Function] in Device.

- **Modify Communication Password**

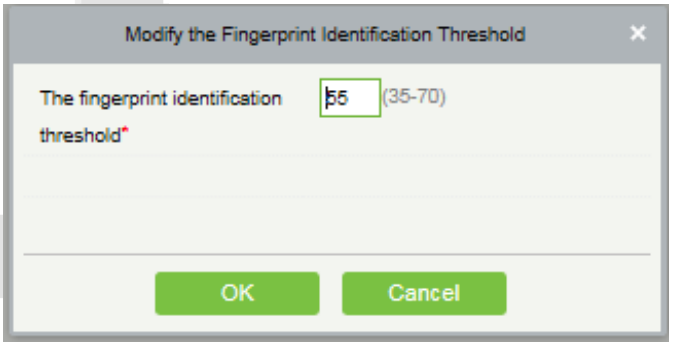
The system will ask for the old communication password before modifying it. After verification, input the new password twice, and click [**OK**] to modify the communication password.

✍**Note:** Communication password shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password setting can improve the device's security. It is recommended to set communication password for each device.

- **Modify RS485 Address**

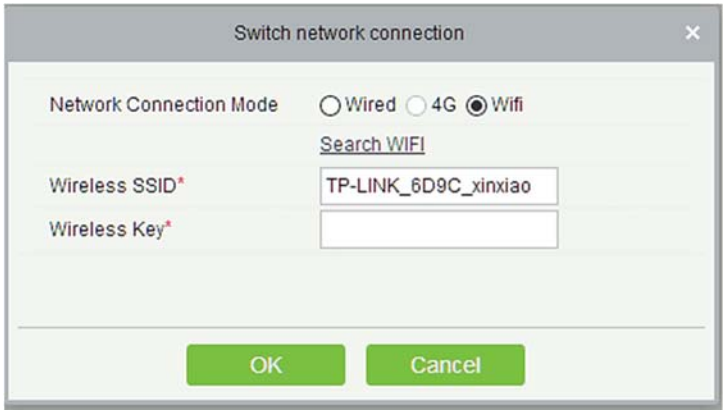
Only the devices that use RS485 communication and with no DIP Switch can modify RS485 address.

- **Modify the fingerprint identification threshold (Ensure that the access controller supports fingerprint function)**



Users can modify the fingerprint identification thresholds in the devices; it ranges from 35 to 70 and it is 55 by default. The system will read the thresholds from the device. Users can view the thresholds devices list. More than one device can be changed by using Batch operation function.

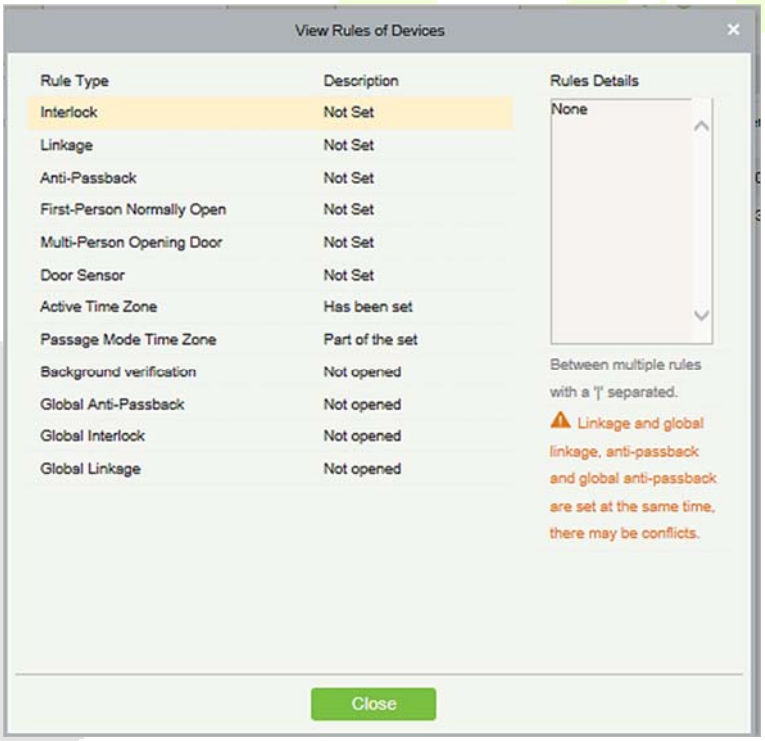
- **Switch network connection**



This function is applicable to InBio5 series access control panels, which is used to switch among different network connection modes of the control panel.

- **View Rules of Devices**

Shows the Access rules in the device.

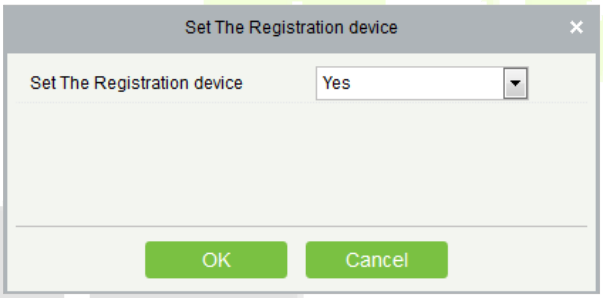


- **View Device Capacity**

It checks the capacity of personnel's biometric details in the device.

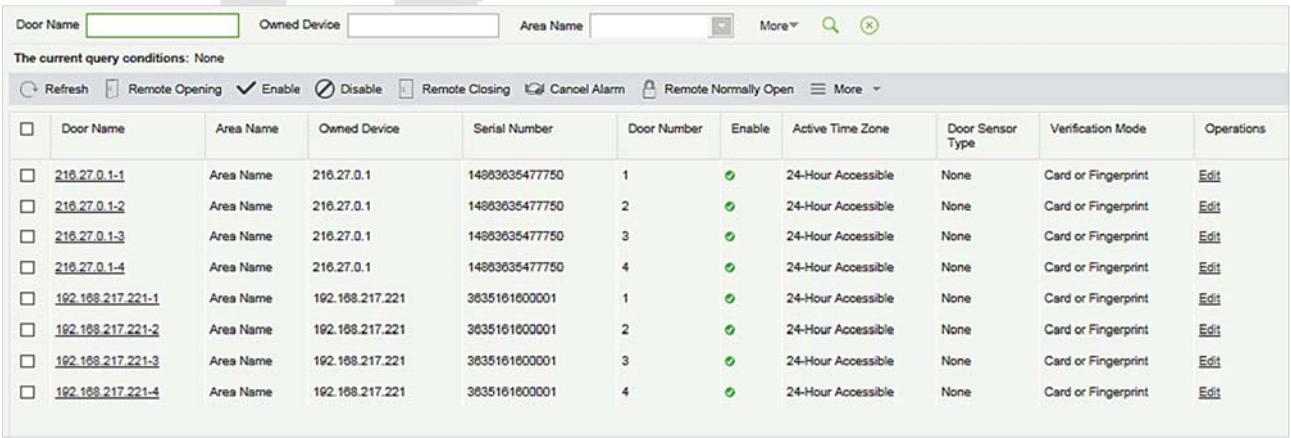
- **Set the Registration device**

Set the registration device only when the standalone device's data such as personnel can automatically upload.



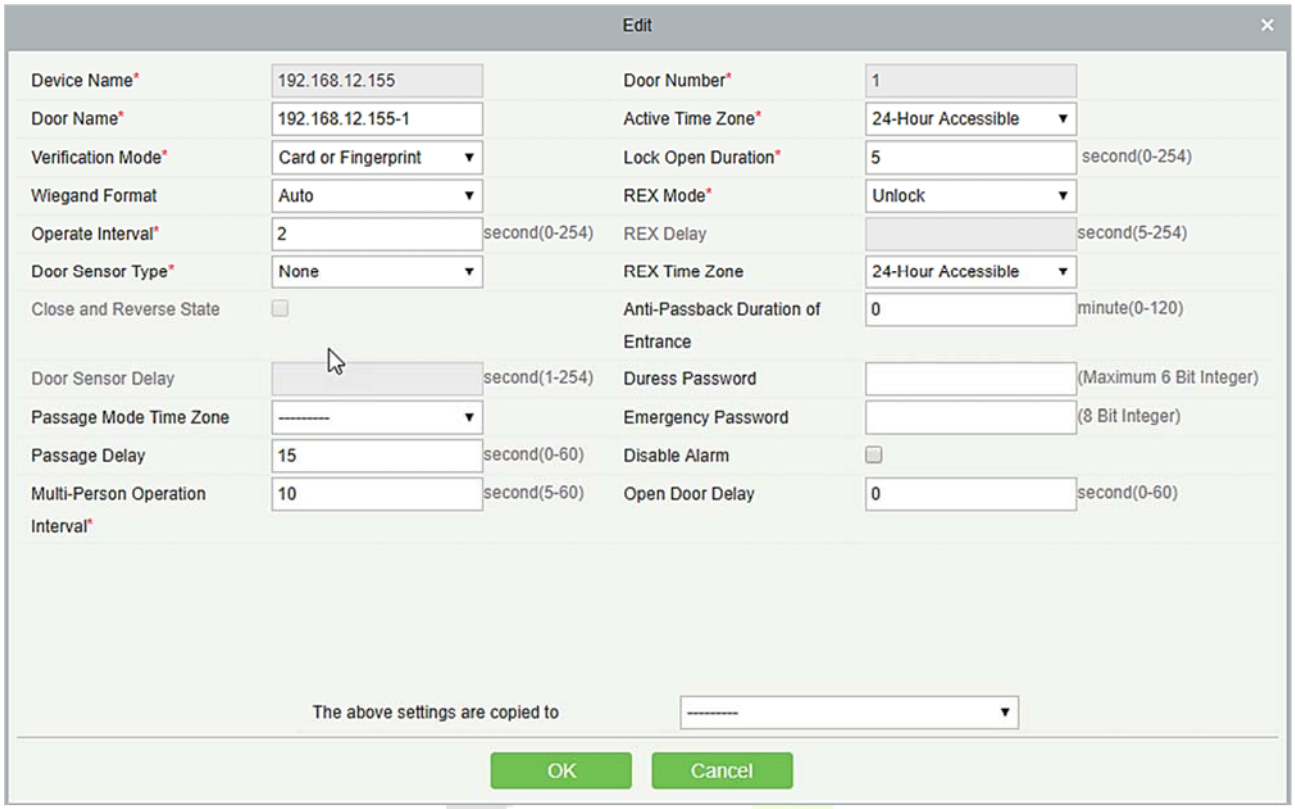
4.1.3 Doors

1. Click [**Access Device**] > [**Device**] > [**Door**] to enter Door Management interface (click "Area Name" in the left, system will automatically filter and display all access devices in this area).



- **Door parameter modification:**

Select the door to be modified, and click Door Name or [**Edit**] button below operations to open the Edit interface:



Fields are as follows:

Device Name: It can't be edited.

Door Number: System will automatically name it according to doors quantity of the device. This number will be consistent with the door number on the device.

✍**Note:** By default, the suffix number in the Door Name is consistent with the Door Number, but 1/2/3/4 in Anti-Passback and interlock refer to the Door Number, rather than the number following the Door Name, and they are not necessarily related.

Door Name: The default is "device name _door number". The field can be modified as needed. Up to 30 characters can be entered.

Active Time Zone: Active Time Zone must be input, so that the door can be opened and closed normally. A Passage Mode Time Zone must be set within the Active Time Zone. By default, both are null.

✍**Note:** For a door, in Normal Open state, a person who is allowed to be verified 5 times consecutively (verification interval should be within 5 seconds) can release the current Normal Open status and close the door. The next verification will be a normal verification. This function is only effective at the Active Time Zone of specified doors. And within the same day, other Normal Open intervals set for the door and First-Person Normally Open settings will not take effect anymore.

Lock Open Duration: It is the time period for which the door remains unlocked after punching. The unit is second (range: 0~254 seconds), and the default value is 5 seconds.

Operate Interval: It is the Interval between two punches. The unit is second (range: 0~254 seconds), and the default value is 2 seconds.

Anti-Passback Duration of Entrance: Only one entry is allowed with a reader in this duration. The unit is minute (range: 0~120 minutes), and the default value is 0 minute.

Door Sensor Type: None (will not detect door sensor), Normal Open, Normal Close. The default value is NO. If you have selected as Normal Open or Normal Close, you need to set Door Sensor Delay and decide whether or not Close and Reverse-lock is required. When the door sensor type is set as Normal Open or Normal Close, the default door sensor delay is 15 seconds, and the close and reverse state is enabled.

Door Sensor Delay: The duration for delayed detection of the door sensor after the door is opened. When the door is not in the Normally Open period, and the door is opened, the device will start the counting. It will trigger an alarm when the delay duration is expired and stops the alarm when you close the door. The default door sensor delay is 15s (range: 1~254 seconds). Door Sensor Delay should be greater than the Lock Open Duration.

Close and Reverse State: It will set to either lock or not lock the door after door closing. Check it for locking after door closing.

Verification Mode: Identification modes include Only Card, Card plus Password, Only Password, Card plus Fingerprint, Card or Fingerprint. The default value is Card or Fingerprint. When both Card and Password mode is selected, make sure the door is equipped with a reader that has keyboard.

Wiegand Format: Select the Wiegand card format that can be identified by the Wiegand reader of the door. If the format of punched card is different with the setting format, the door cannot be opened. The software is embedded with 9 formats, and the default is Wiegand card format, except for the card format name containing a, b or c.

Request to Exit (REX Mode): Locking indicates that the door will be locked after the exit button is pressed. Unlocking indicates that the door will be unlocked after the exit button is pressed. The default value is unlocking.

Request to Exit Delay (REX Delay): It indicates the alarm delay time for door detection after the exit button is locked. When the door is unlocked forcibly, the system will detect the door status after a period of time. The default is 10s (range: 1~254 seconds). The exit button has to be locked before setting this option.

REX Time Zone: The button is available only in the specified time segment.

Anti-Passback Duration of Entrance: Based on the lock opening duration, the door sensor delays exit delay. The duration of the entry will be extended. To function this feature, you need to check [Delay passage] option to extend relevant duration when adding or editing staff information. For example, you may extend the duration of entrance for people with disabilities.

Open Door Delay: The time period to keep the door open after the verification completes (range: 1~60 seconds).

Multi-Person Operation Interval: The time interval between two verifications with cards or fingerprints (range: 1~60 seconds).

Duress Password, Emergency Password: Duress means any threats, violence, constraints, or other action used to coerce someone into doing something against their will. In these situations, input Duress Password (with an authorize card) to open the door. When the door is opened with Duress Password, the alarm is triggered. Upon emergency, user can use Emergency Password (named Super Password) to open door. Emergency Password allows normal opening, and it is effective in any time zone and any type of verification mode, usually used for the administrator.

- **Duress Password Opening** (**used with an authorized card**): Password should be a number not exceeding 6 digits. When Only Card verification mode is used, you need to press [**ESC**] first, and then press the password plus [**OK**] button, then finally punch legal card. The door opens and triggers the alarm. When Card + Password verify mode is used, please punch legal card first, then press the password plus [**OK**] button (same as normal opening in card plus password verification mode), the door opens and triggers the alarm.
- **Emergency Password Opening**: Password must be 8 digits. The door can be opened only by entering the password. Please press [**ESC**] every time before entering password, and then press [**OK**] to execute.

When using Duress Password or Emergency Password, the interval for entering each number shall not exceed 10 seconds, and both the passwords should not be the same.

Disable Alarm: Check the box to disable the alarm voice in real-time monitoring page.

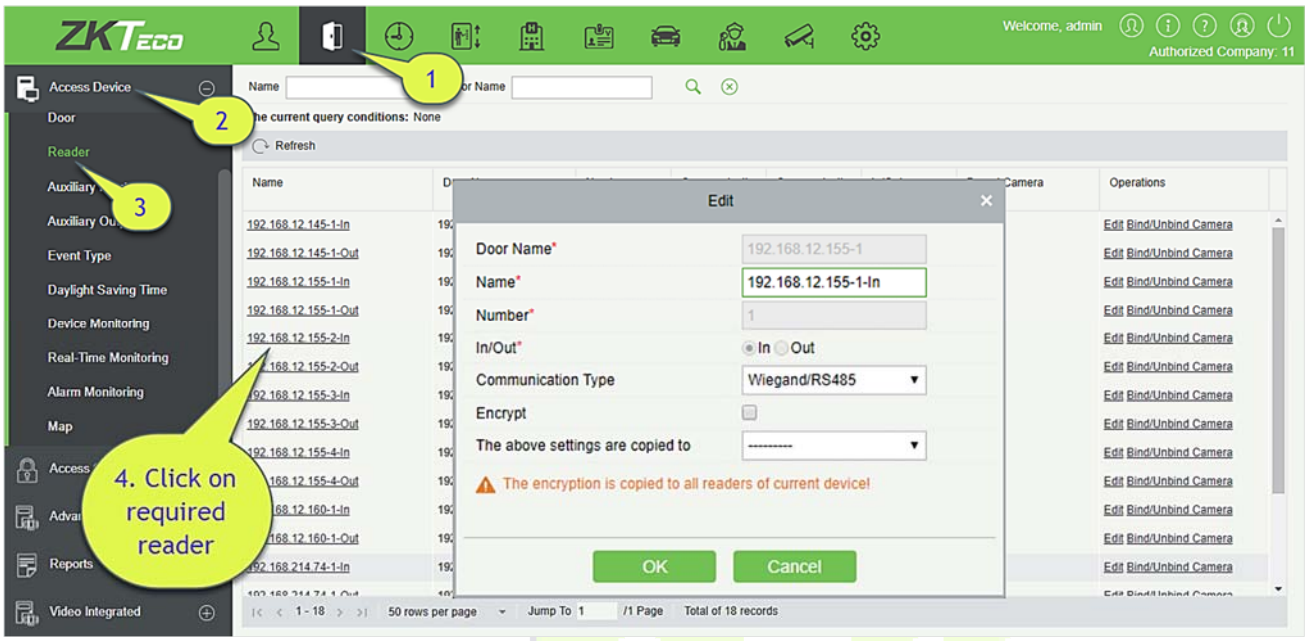
The above Settings are Copied to: It has below two options.

- All doors of current device: Click to apply the above settings to all doors of the current access device.
- All doors of all devices: Click to apply the above settings to all doors of all access devices within the current user's level.

2. After setting parameter(s), click [**OK**] to save and exit.

4.1.4 Reader

1. Click [**Access Device**] > [**Reader**] on the Action Menu, click on reader name or [**Edit**]:



Name: Name of the reader displayed on the list page.

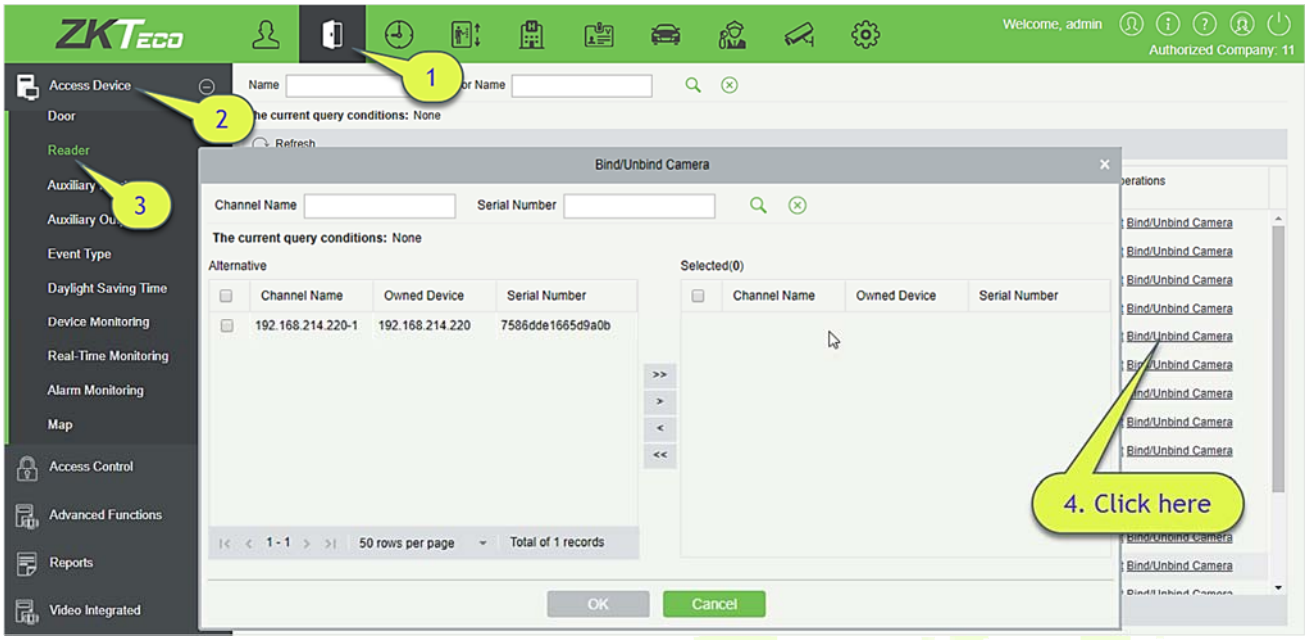
Communication Type: Wiegand/RS485, Wiegand, RS485, and Disabled are available. When a communication type is selected, the reader interface on the device will receive data (including card and fingerprint data) for the specified type only.

Encrypt: If this option is selected, the device may only be used with encrypted readers, such as SF10 and FR1300.

Bind/Unbind Camera

Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos or screenshots) once there is a corresponding event occurs.

2. Click [**Bind/Unbind Camera**] to select channel(s):



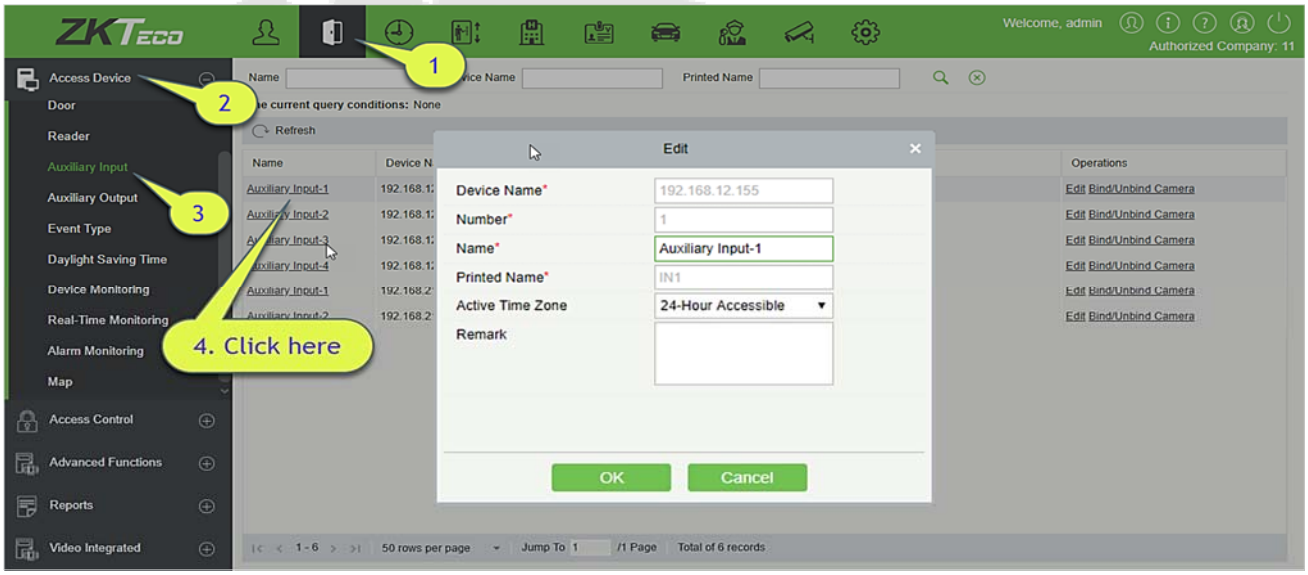
3. Select and move the required reader towards right list and Click [**OK**] to finish.

✍**Note:** A reader can be used to bind more than one channel.

4.1.5 Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

1. Click [**Access Device**] > [**Auxiliary Input**] on the Action Menu, to access below shown interface:
2. Click on Name or [**Edit**] to modify the parameters as shown below:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: It will be the printed name on the hardware, such IN5.

Active Time Zone: Auxiliary input is available only in the specified time segment.

✍**Note:** Only Name, Active Time Zone and Remarks can be modified.

3. Click [**OK**] to save the name and remark and exit.

Bind/Unbind Camera

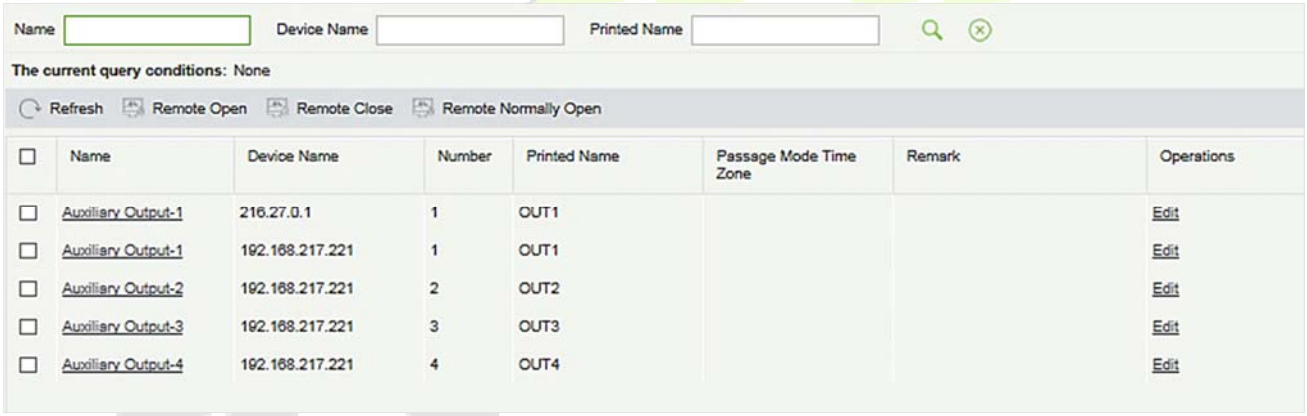
Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos or screenshots) once there is a corresponding event occurs. For this, the interaction setting in Linkage or in Global Linkage should be done before. For details, please refer to Reader: Bind/Unbind Camera.

✍**Note:** An auxiliary input point can bind more than one channel.

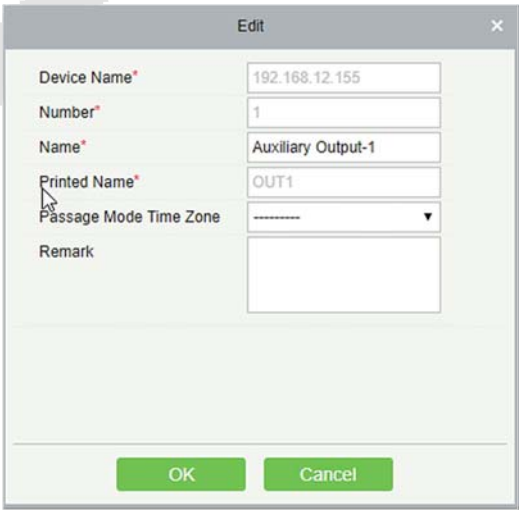
4.1.6 Auxiliary Output

It is mainly related to alarm and is used when linkage is working.

1. Click [**Access Device**] > [**Auxiliary Output**] on the Action Menu to access the following interface:



2. Click [**Edit**] to modify the parameters:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example OUT2.

Passage Mode Time Zone: The auxiliary output will be in normal open or normal close in the selected time zone.

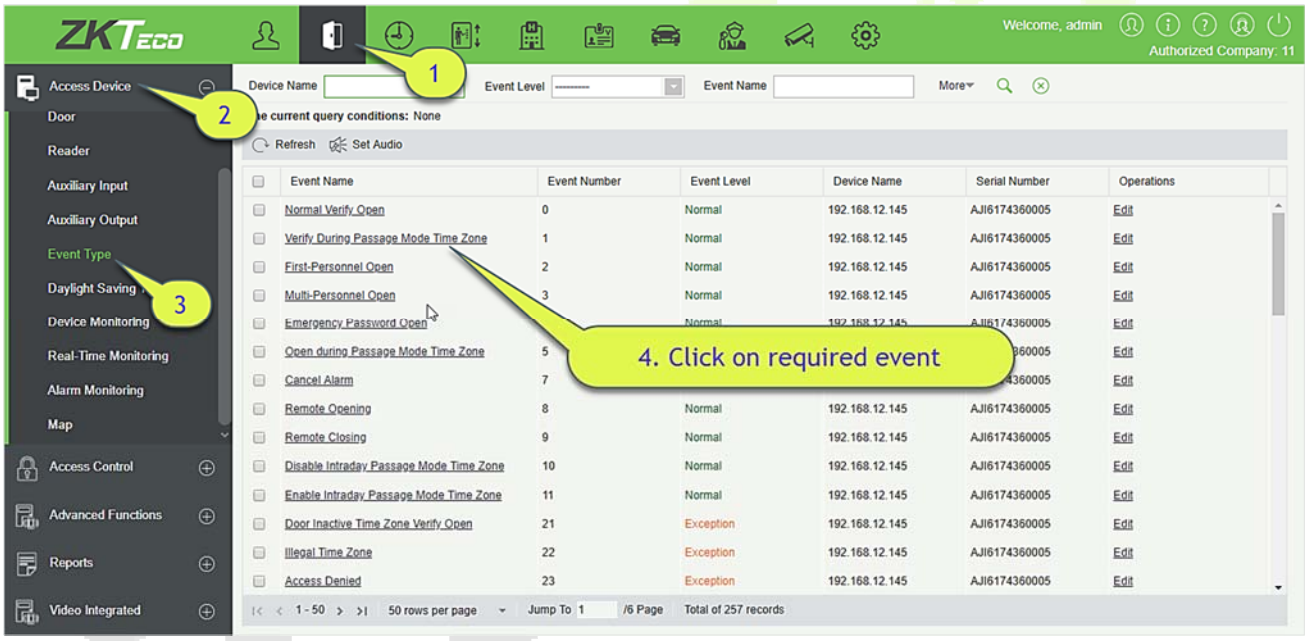
✍**Note:** Only Name, Passage Mode Time Zone and Remarks can be modified.

3. Click [**OK**] to save the name and remark and exit.

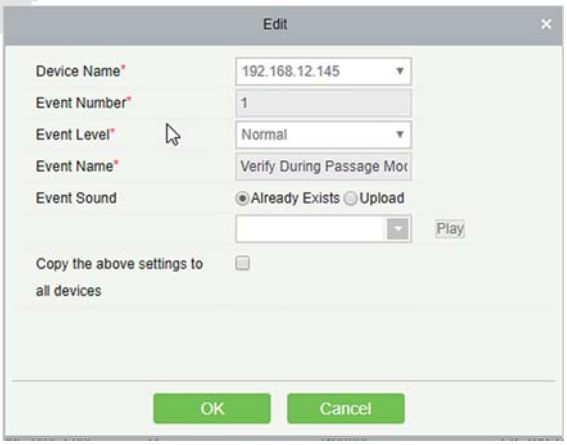
4.1.7 Event Type

It will display the event types of the access devices.

1. Click [**Access Device**] > [**Event**] to access the following page:



2. Click [**Edit**] or click the event type name to edit:



Fields are as follows:

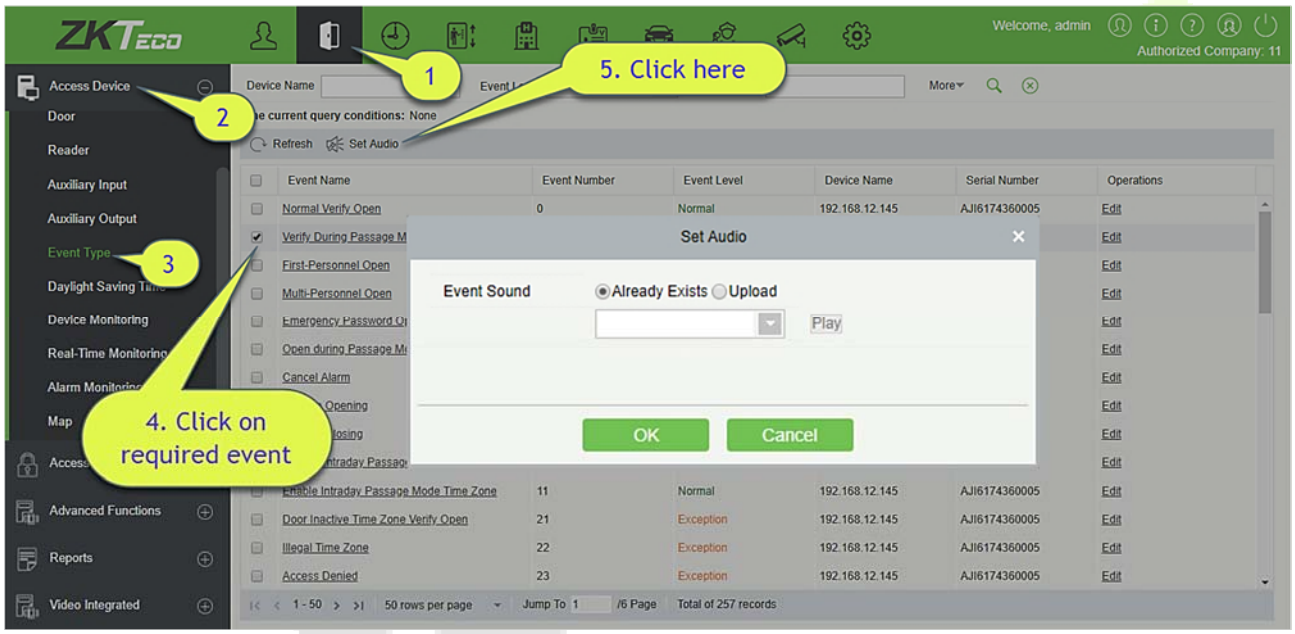
Event Level: Normal, Exception, and Alarm are available.

Event Name: It can't be modified.

Event Sound: You can set custom sound being played when the event occurs in real-time monitoring.

Copy the above settings to all devices: This event will be applied to all current devices within the purview of the same user event number.

Set Audio: Same as the event sound. Click [**Set Audio**]:



You can upload an audio from your local PC. The file must be in wav or mp3 format, and it must not exceed 10MB.

For more details about Event Type, please refer to Access Event Type.

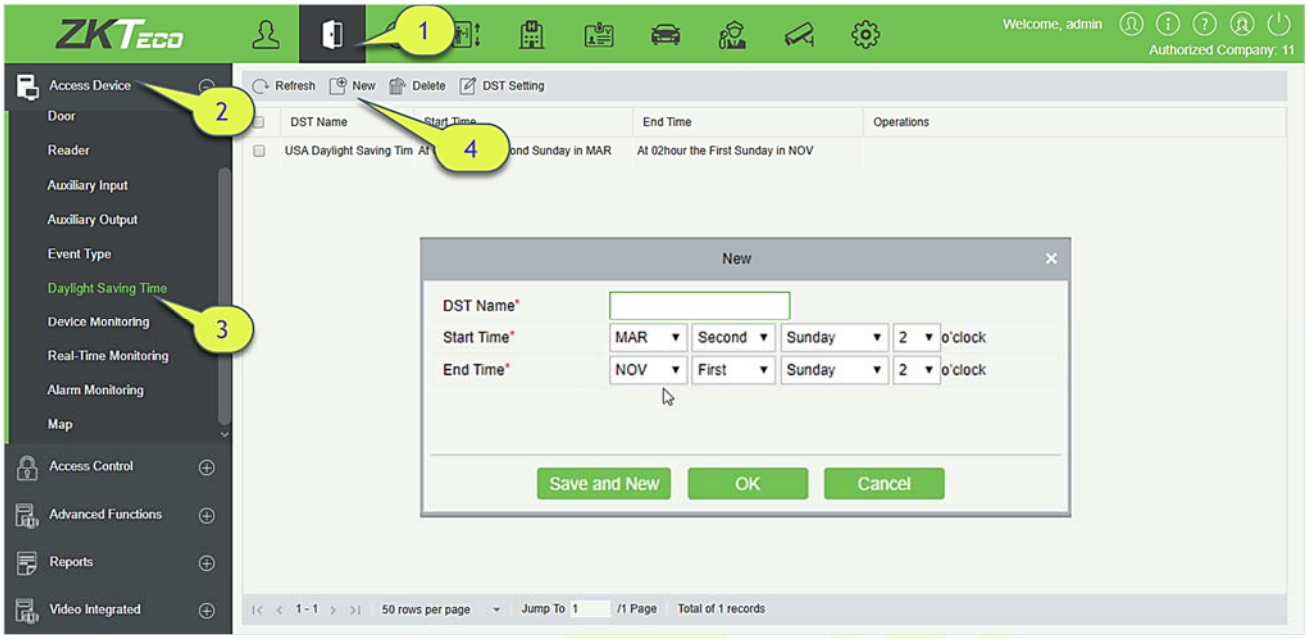
4.1.8 Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. The regulations are different in different countries. At present, nearly 70 countries adopt DST.

To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

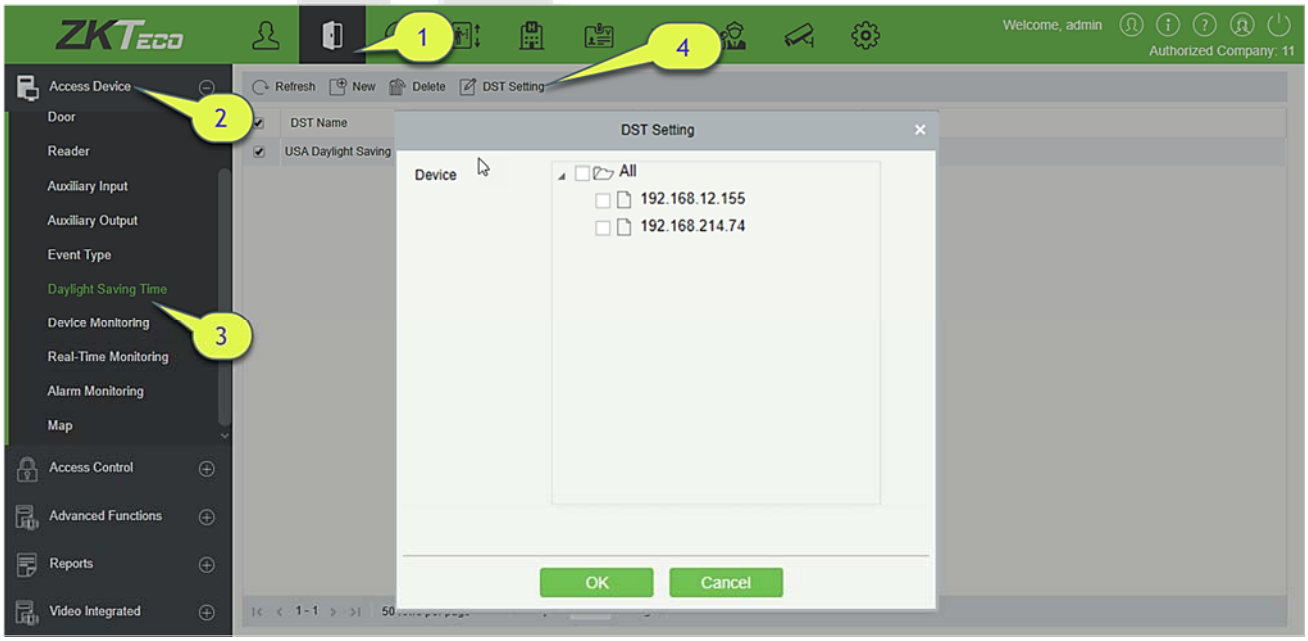
Add DST

1. Click [**Access Device**] > [**Daylight Saving Time**] > [**New**]:



Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as “second Monday in March, 02:00”. The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Use a DST



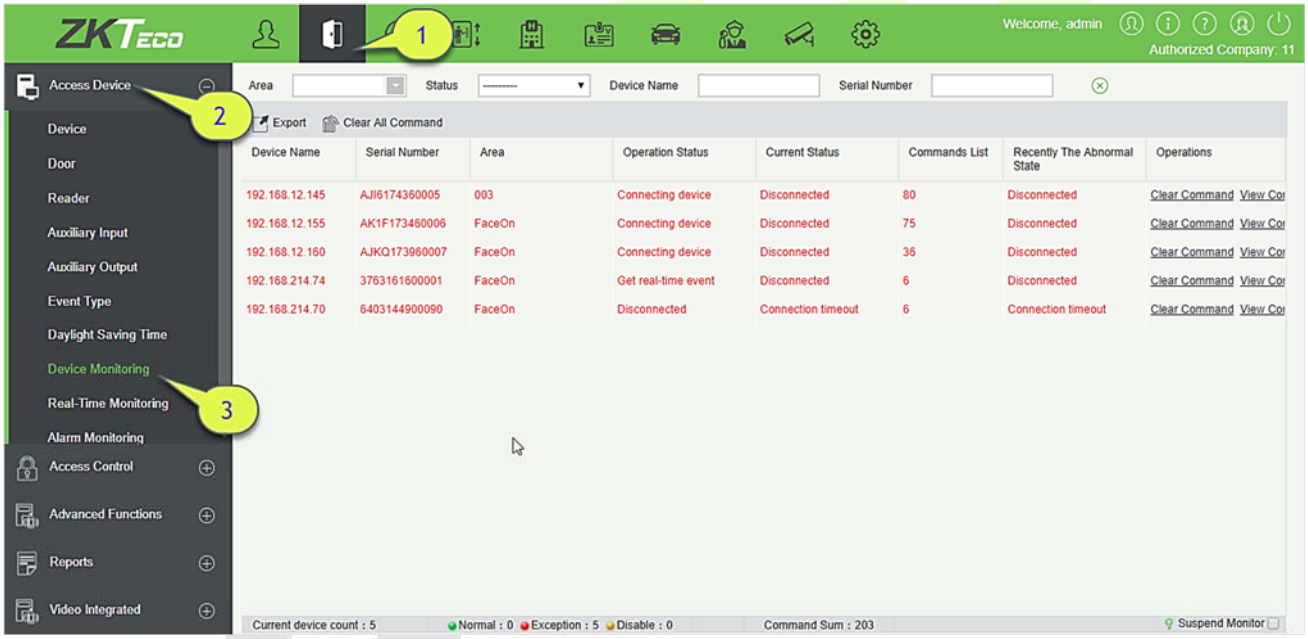
The user can enable the DST setting on a device: In the DST interface, select a DST setting, and click [**DST Setting**], select the device to apply the DST setting to and click [**OK**] to confirm.

✍Notes:

- If a DST setting is in use, it cannot be deleted. Stop the DST before deleting.
- If a DST setting is in use, the latest modification will be sent to the device. Disconnection of the relevant device will lead to transmission failure, and it will resume at the next connection.
- In the Door Management module of the access control system, you can enable or disable DST function. If you enable DST setting, the system will be advanced one hour at the start time. The system will go back to the original time at the end time. If you did not set a DST in the device, the system will prompt "The Daylight Saving Time hasn't been set in this device" when you disable the function.

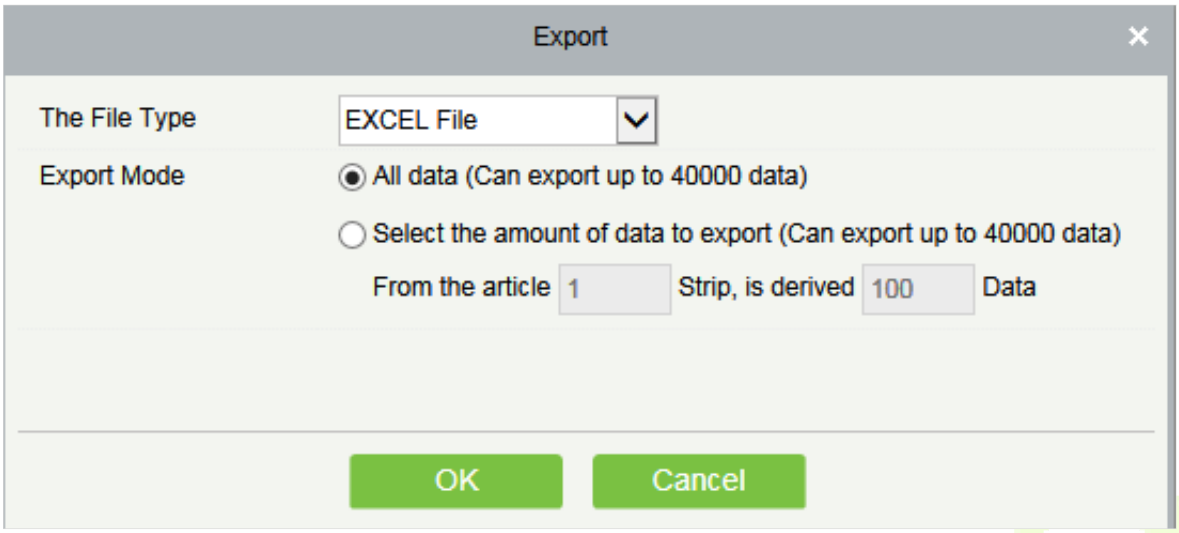
4.1.9 Device Monitoring

By default, it monitors all devices within the current user's level. You may click [**Access Device**] > [**Device Monitoring**] to view a list of operation information of devices: Device Name, Serial No., Area, Operation Status, Current status, Commands List, and Related Operation.



- **Export**

Device commands can be exported in EXCEL, PDF, CSV file format.

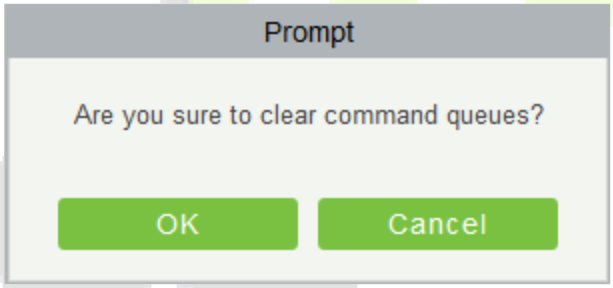


ZKTECO

Device Monitoring

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State
192.168.218.60	20100501999	Area Name	Get real-time event	Normal	0	None

You may clear the command as needed. Click [**Clear Command**] in operations column:



Click [**OK**] to clear.

✍Notes:

- After the implementation of Clear Command, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you can replace the current device with a higher-capacity one or delete the rights of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.
- Operate State is the content of communications equipment of current device, mainly used for debugging.
- The number of commands to be performed is greater than 0, indicating that the data is not yet synchronized to the device, so wait for the synchronization to complete.

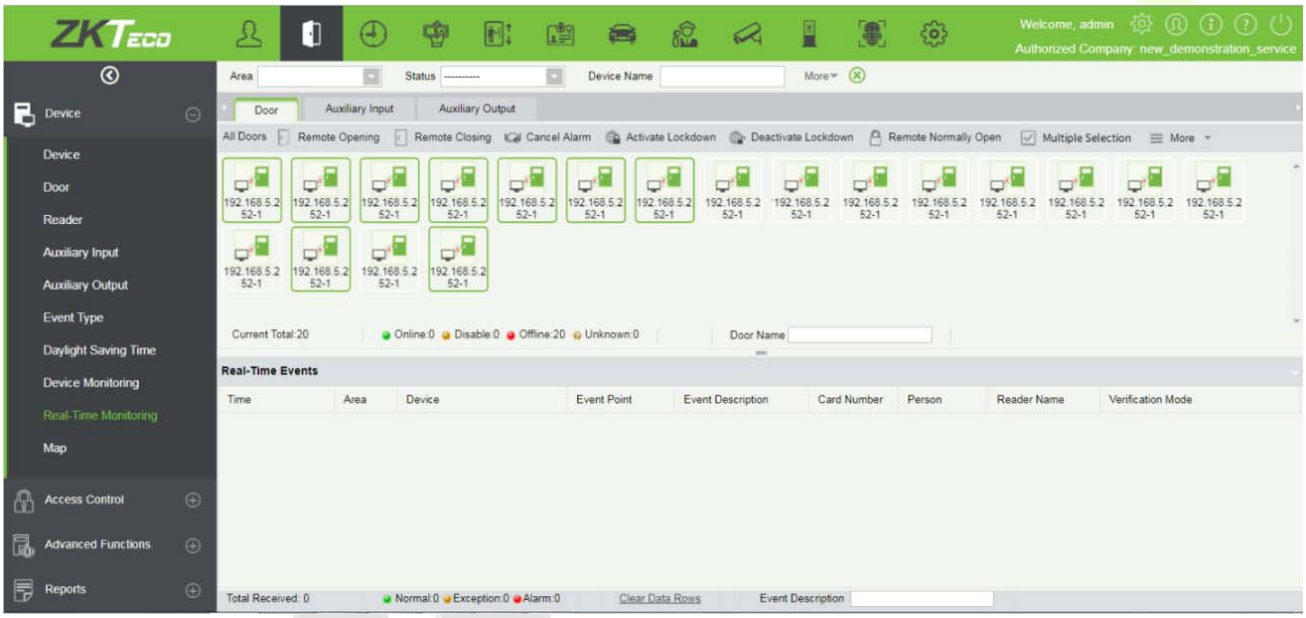
4.1.10 Real-Time Monitoring

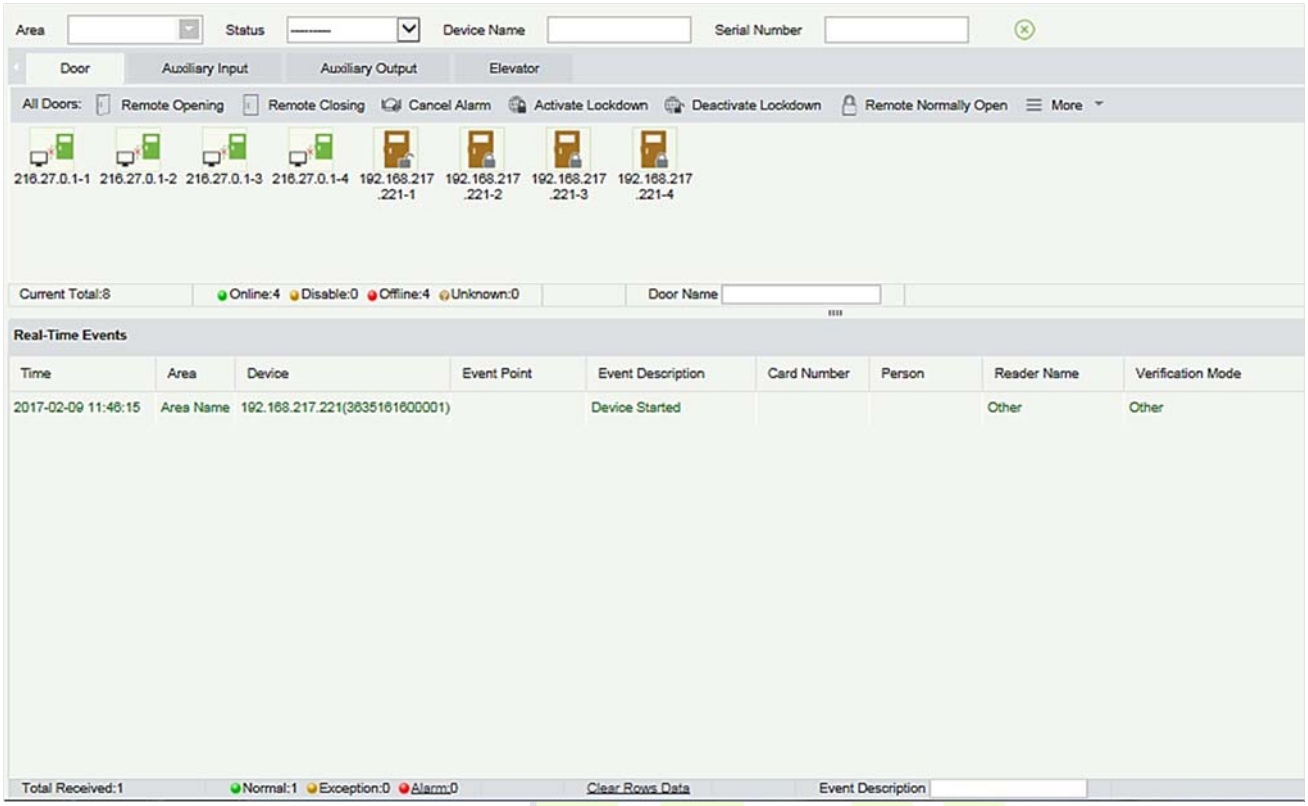
Click [**Access Device**] > [**Real-Time Monitoring**].

It will monitor the status and real-time events of doors under the access control panels in the system in real-time, including normal events and abnormal events (including alarm events).

The Real-Time Monitoring interface is shown as follows:

Click a door to enable the selection mode. You can perform operations such as batch selection, batch remote opening, remote closing, activate lockdown, deactivate lockdown, and remote normally open.





Different icons represent status as followed:

Icons	Status	Icons	Status
	Device banned		Door Offline
	Door sensor unset, Relay closed /Without relay status		Door sensor unset, Relay opened/Without relay status
	Online status Door closed, Relay closed/Without relay status		Online status Door closed, Relay opened/Without relay status
	Online status Door opened, Relay closed/Without relay status		Online status Door opened, Relay opened/Without relay status
	Door opened alarming, Relay closed		Door opened alarming, Relay opened
	Door opening timeout, Relay closed /Without relay status, Door Sensor Opened		Door opening timeout, Relay opened/Without relay status
	Door opening timeout, Relay closed/ Door Sensor Closed		Door opening timeout, Relay opened/ Door Sensor Closed

/	Door closed alarming, Relay closed/Without relay status	/	Door closed alarming, Relay opened/Without relay status
	Door sensor unset, Door alarming, Relay closed		Door sensor unset, Door alarming, Relay opened
	Door opening timeout, Without relay status/Door Sensor Closed		Door locking
✍**Note:** Without relay status, indicates that the current firmware does not support "detect relay status" function.			

1. Door

- **Monitoring All**

By default, the home page displays all doors of the panels within the user's level. User may monitor door(s) by setting the Area, Access Control or Door.

Remote Opening/Closing: It can control one door or all doors.

To control a single door, right click over it, and click [**Remote Opening/ Closing**] in the pop-up dialog box. To control all doors, directly click [**Remote Opening/ Closing**] behind Current All.

In remote opening, user can define the door opening duration (The default is 15s). You can select [**Enable Intraday Passage Mode Time Zone**] to enable the intraday door passage mode time zones, or set the door to Normal Open, then the door will not be limited to any time zones (open for 24 hours).

To close a door, select [**Disable Intraday Passage Mode Time Zone**] first, to avoid enabling other normal open time zones to open the door, and then select [**Remote Closing**].

✍**Note:** If [**Remote Opening /Closing**] fails, check whether the devices are disconnected or not. If disconnected, check the network.

Cancel the alarm: Once an alarming door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click [**Remote Opening/Closing**] in the menu. To control all doors, directly click [**Remote Opening/Closing**] behind Current All.

✍**Note:** If [**Cancel the alarm**] fails, check if any devices are disconnected. If found disconnected, check the network.

Remote Normally Open: It will set the device as normal open by remote.

Activate Lockdown: It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

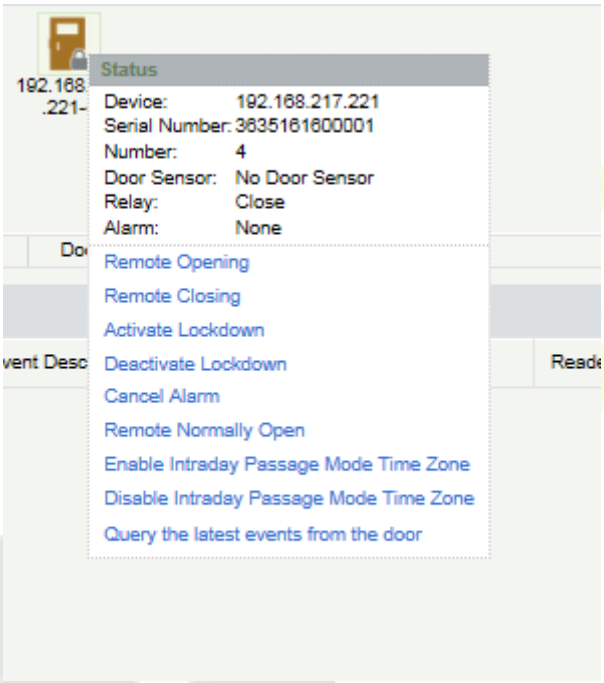
Deactivate Lockdown: It will unlock a locked door. This function is supported only by certain devices.

Personnel photo display: If a Real-Time Monitoring event contains personnel activity, the monitor will display the person photo (if no photo is registered, the monitor will display default photo). The event name, time and date are displayed.

Play Audio: If this option is selected, it plays an audio after an alarming event occurs.

- **Quick Management of Doors**

If you move the cursor to a door's icon; you can perform the above operations in a quick way. In addition, you can query the latest events from the door.



Query the latest events from the door: Click to quickly view the latest events happened on the door.

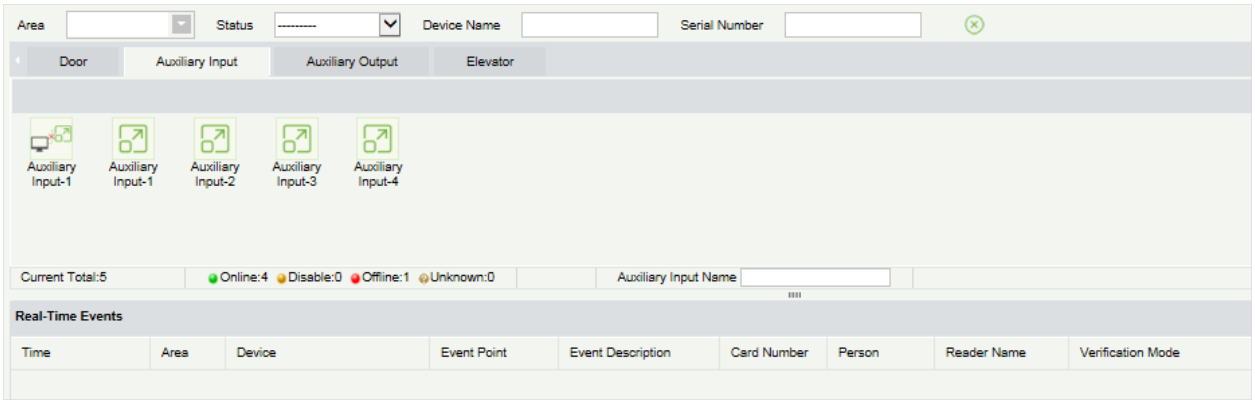
Issue card to person: If you swap an unregistered card, a record with a card number will pop-up in real-time monitoring interface. Right click that card number, and a menu will pop-out. Click "Issue card to person", to assign that card to one person.

- **Event monitoring**

The system will automatically acquire records of devices being monitored (by default, display 200 records), including normal and abnormal access control events (including alarm events). Normal events will appear in green; alarm events will appear in red; other abnormal events will appear in orange.

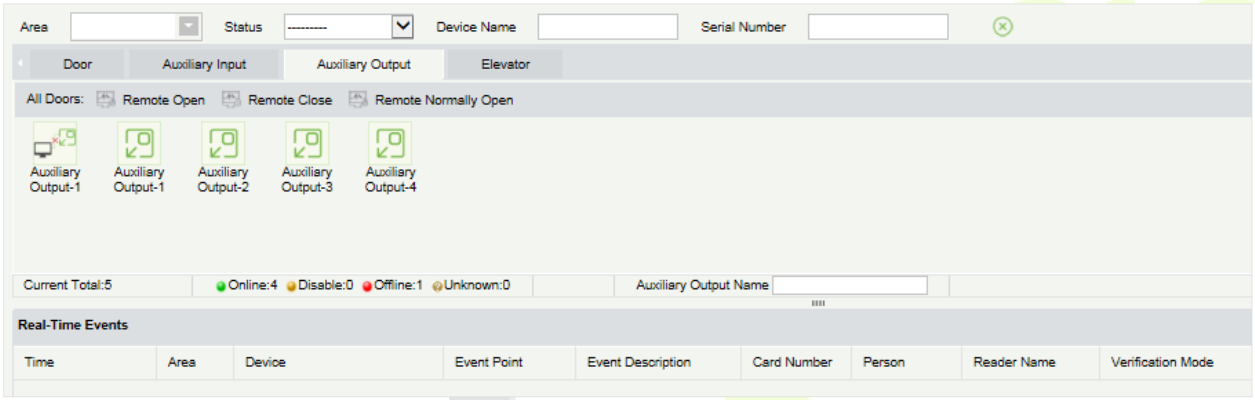
2. Auxiliary Input

It monitors current auxiliary input events in real-time.



3. Auxiliary Output

Here you can perform Remote open, Remote Close, Remote Normally Open.

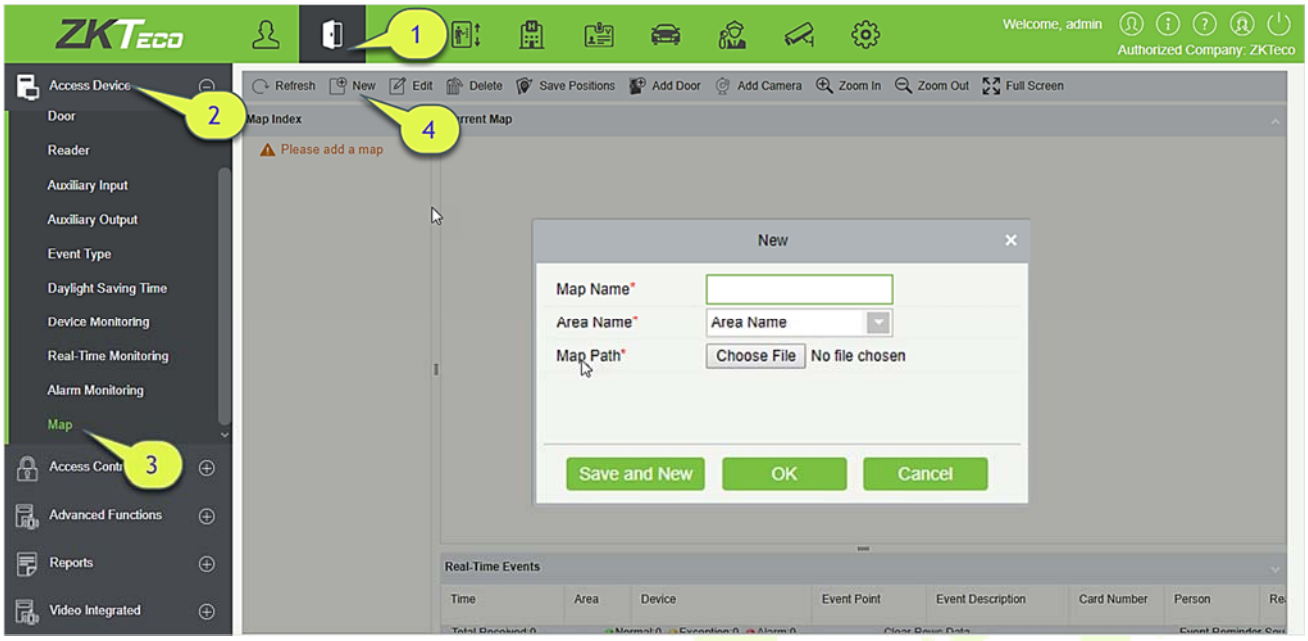


4. Elevator

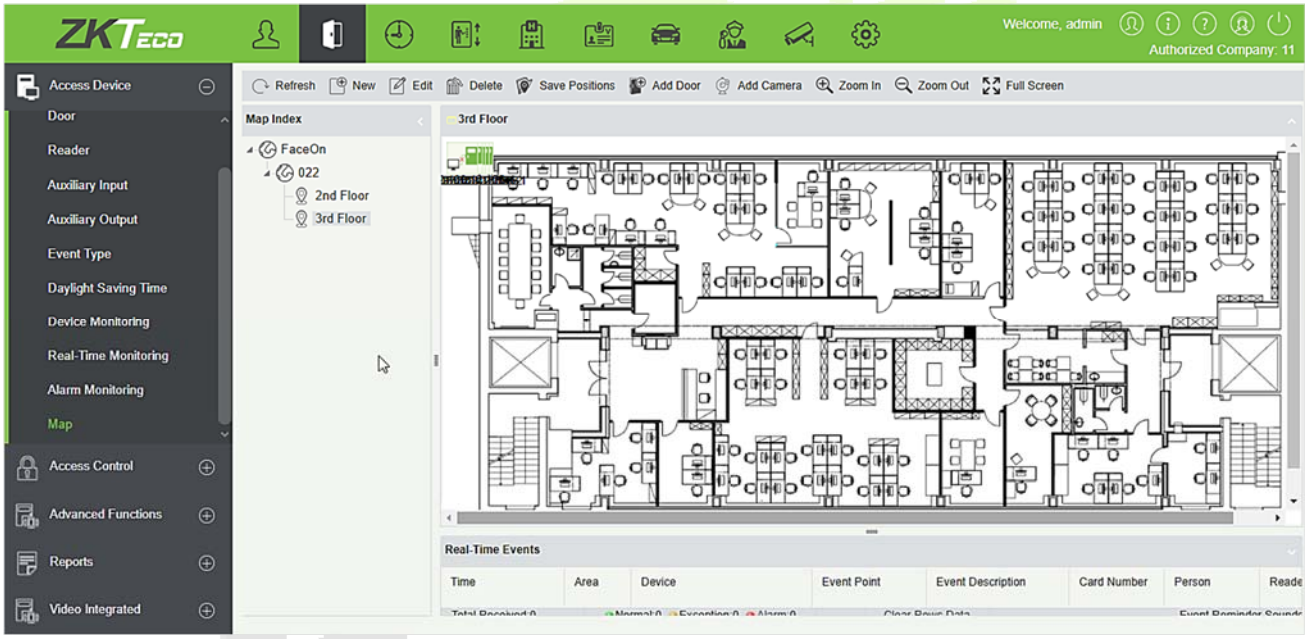
About the real-time monitoring of elevators, please refer to Real-Time Monitoring.

4.1.11 Map

Click [**Access Device**] > [**Map**] > [**New**] to add a map.



After adding, users can add door on the map, perform zoom-in, zoom-out, etc. If users relocated or modified the map, click [**Save Positions**] to save. The user can view the new setting at next visit.



Add/Delete Map: Users can add or delete a map as needed.

Edit Map: Users can edit map name, change map or the area it belongs to.

Adjust map (includes door): Users can add a door on the map or delete an existing one (right click the door icon, and select [**Delete Door**]), or adjust the map or position(s) of the door or camera icons (by dragging the door or camera icons), adjust the size of the map (click [**Zoom in**] or [**Zoom out**] or click [**Full Screen**]).

Door operation: If you move the cursor to a door, the system will automatically filter and displays the operation according to the door status. Users can do remotely open/close doors, cancel alarms, etc.

Levels control:

1) Users need to select the relevant area for the map when adding levels. The area will be relevant to the user access levels, users can only view or manage the map within levels. If the relevant area of a map is modified, all doors on the map will be cleared. Users need to add the doors manually again.

2) When an administrator is adding a new user, he can set the user operation rights in role setting, such as Save positions, Add Door, Add Camera, etc.

✍Notes:

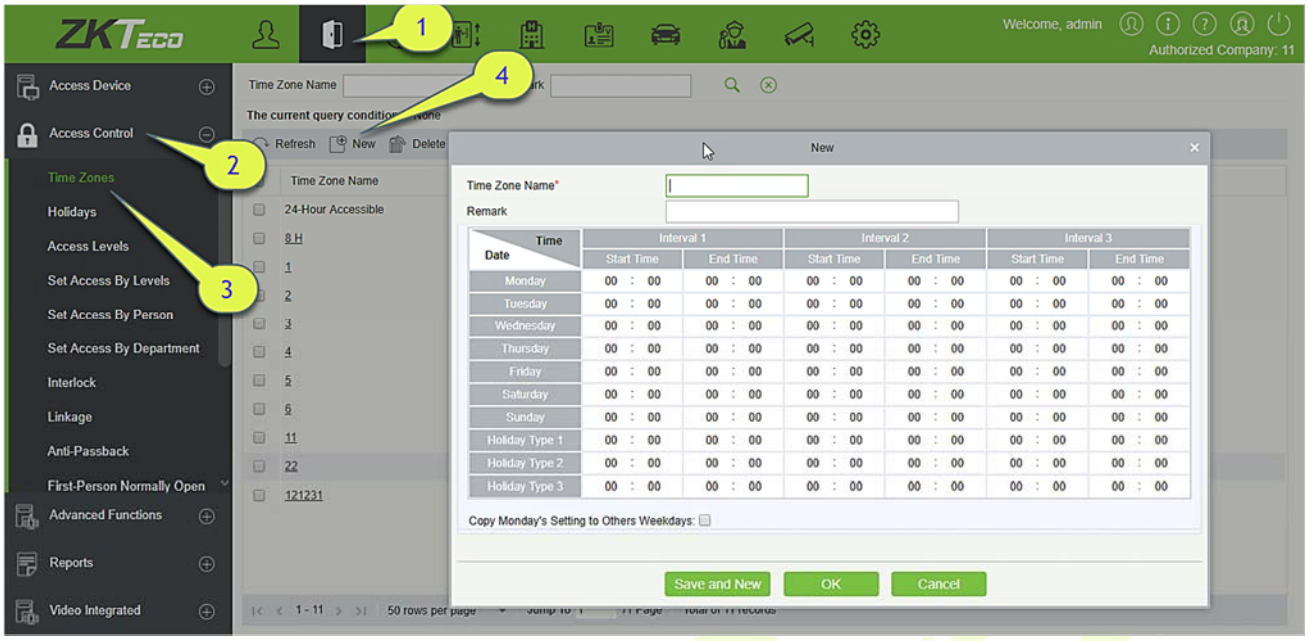
- In map modification, users can choose to modify the map name but not the path. Users only need to check the box to activate the modification option.
- The system supports adding multi doors at the same time. After adding the doors, users need to set the door position on the map and click [**Save**].
- When modifying door icon, especially when users zoomed out the map, the margin for top and left shall not be smaller than 5 pixels, or system will prompt error.
- Users are recommended to add a map size under 1120 * 380 pixels. If several clients access the same server, the display effect will be different according to resolutions of screen and the settings of browsers.

4.2 Access Control Management

4.2.1 Time Zones

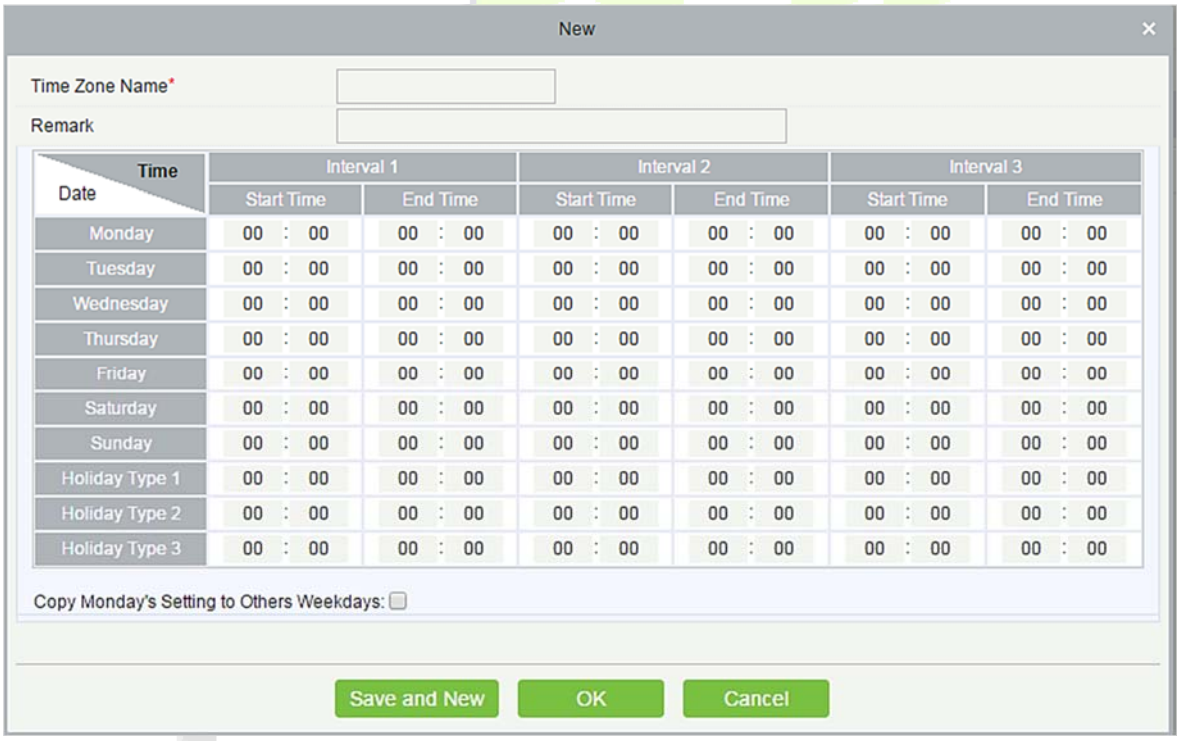
It sets usage time of a door; the reader is usable during valid time periods of certain doors and unusable during other time periods. Time Zone can also be used to set Normal Open time periods or set access levels so that specified users can only access specified doors during specified time periods (including access levels and First-Person Normally Open).

The system controls access according to Time Zones (up to 255 time zones). The format of each interval for a time zone: HH: MM-HH: MM. Initially, by default, the system has an access control time zone named [24 hours Accessible]. This time period cannot be modified and deleted. The user can add new Access Control Time Zones that can be modified or deleted.



1. Add Access Control Time Zone

1) Click [**Access Control**] > [**Time zones**] > [**New**] to enter the time zone setting interface:



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 30 characters.

✍**Remarks:** Detailed description of the current time zone, including explanation of current time zone and primary applications. Users can input up to 50 characters in this field.

Interval and Start/ End Time: One Access Control Time Zone includes 3 intervals for each day in a week,

and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as interval 1, and 00:00-00:00 as interval 2/3. If the interval is Normal Close: all inputs will be 00:00-00:00. If users use only one interval, they just need to fill in interval 1, and interval 2/3 will be the default value. Similarly, when users only use the first two intervals, the third interval will be the default value. When using two or three intervals, users need to ensure that the two or three intervals do not overlap, and the time shall not cross the days. Or the system will prompt error.

Holiday Type: Three holiday types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access purpose. The holiday type is optional. If the user does not enter one, the system will use the default value.

Copy on Monday: You can quickly copy the settings of Monday to other weekdays.

2) After setting, click [**OK**] to save, and it will display in the list.

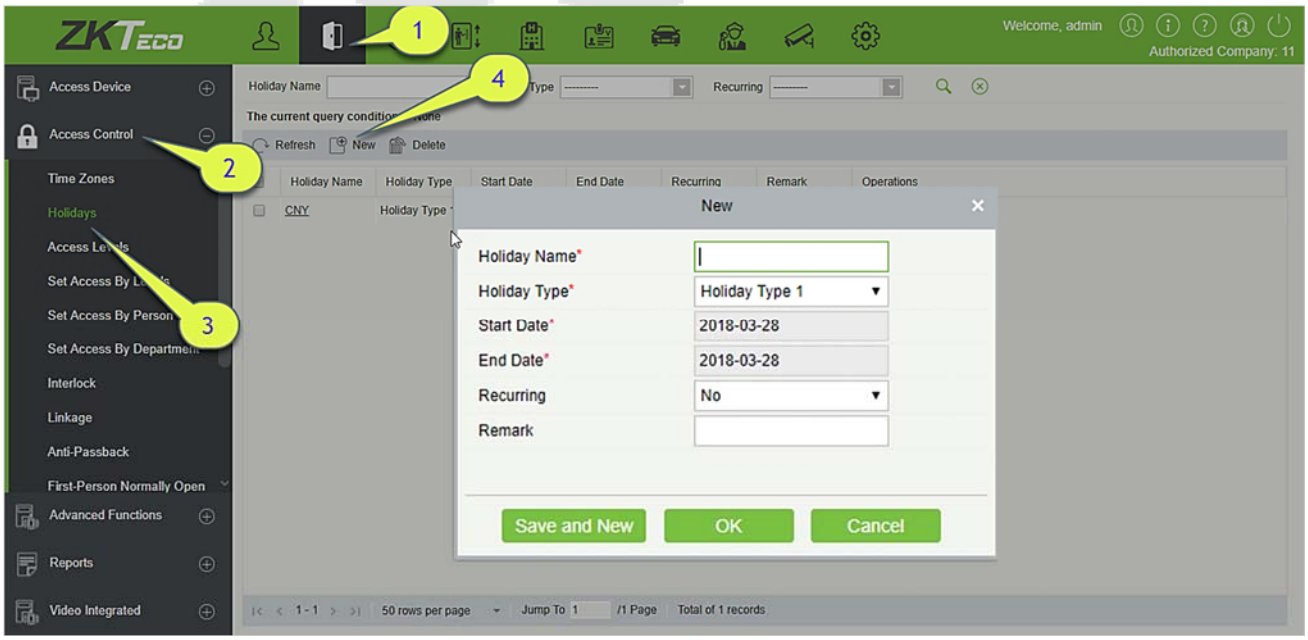
2. Maintenance of Access Control Time Zones

Edit: Click the [**Edit**] button under Operation to enter the edit interface. After editing, click [**OK**] to save.

Delete: Click the [**Delete**] button under Related Operation, then click [**OK**] to delete, or click [**Cancel**] to cancel the operation. A time zone in use cannot be deleted. An alternative way is to tick the check boxes before one or more time zones in the list, and click the [Delete] button over the list, then click [**OK**] to delete, and click [C**ancel**] to cancel the operation.

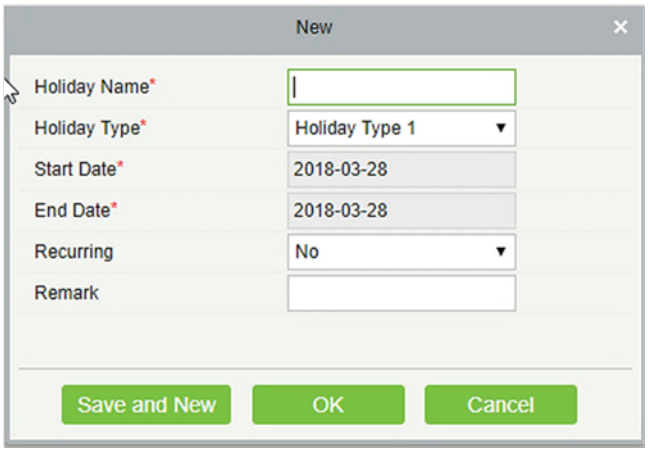
4.2.2 Holidays

Access Control Time of a holiday may differ from that of a weekday. The system provides access control time setting for holidays. Access Control Holiday Management includes Add, Modify and Delete.



- **Add**

1) Click [**Access Control**] > [**Holidays**] > [**New**] to enter edit interface:



Fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/End Date: The date format: 2010-1-1. Start Date cannot be later than End Date, otherwise the system will prompt an error message. The year of Start Date cannot be earlier than the current year, and the holiday cannot be set across two different years.

Recurring: It refers a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

2) After editing, click [**OK**] button to save, and it will display in the holiday list.

- **Modify**

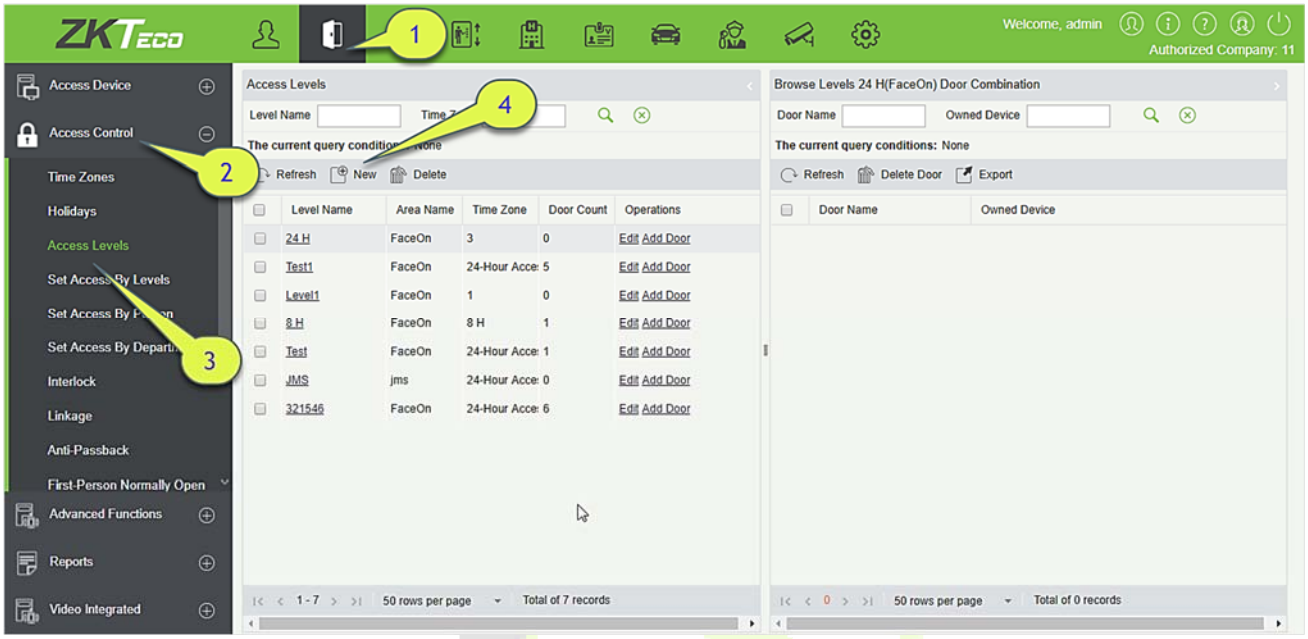
Click Holiday Name or [**Edit**] button under Operations to enter the edit interface. After modification, click [**OK**] to save and quit.

- **Delete**

In the access control holiday list, click [**Delete**] button under Operations. Click [**OK**] to delete, click [**Cancel**] to cancel the operation. An Access Control Holiday in use cannot be deleted.

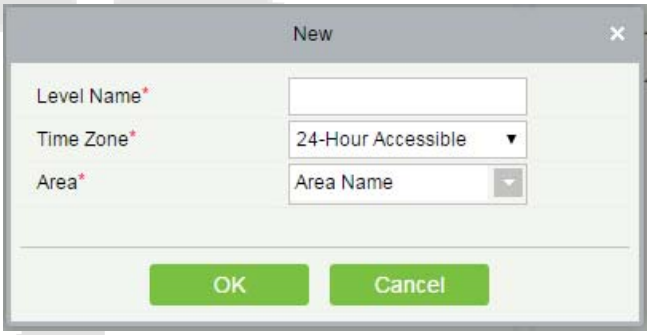
4.2.3 Access Levels

Access levels indicate that one or several selected doors can be opened by verification of a combination of different person within certain time zone. The combination of different person set in Personnel Access Level option.



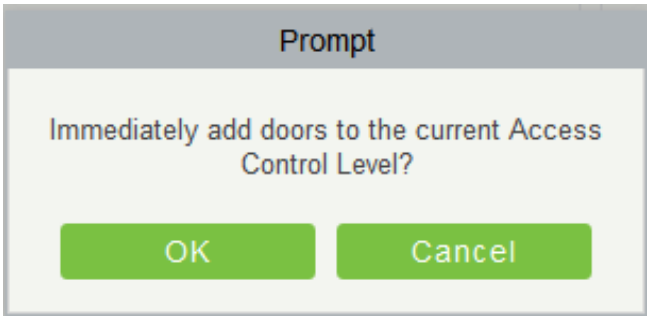
- **Add**

1. Click [**Access Control**] > [**Access Levels**] > [**New**] to enter the Add Levels editing interface:



2. Set each parameter: Level Name (unrepeatable), Time Zone.

3. Click [**OK**], the system prompts "Immediately add doors to the current Access Control Level", then click [**OK**] to add doors, then click [**Cancel**] to return the access levels list. The added access level is displayed in the list.



✍**Note:** Different doors of different panels can be selected and added to an access level.

4.2.4 Set Access by Levels

Add/Delete Personnel for Selected Levels:

1) Click [**Access Control**] > [**Access Levels**] > [**Set Access By Levels**] to enter the edit interface, then click an Access level in the list on the left, personnel having right of opening doors in this access level will be displayed in list on the right.

2) In the left list, click [**Add Personnel**] under Operations to pop up the Add Personnel box; select personnel (multiple) and click > to move to the selected list on the right, then click [**OK**] to save and exit.

3) Click the level to view the personnel in the list on the right. Select personnel and click [**Delete Personnel**] above the list on the right, then Click [**OK**] to delete.

4.2.5 Set Access by Person

Add selected personnel to selected access levels or delete selected personnel from the access levels.

Add/Delete levels for Selected Personnel:

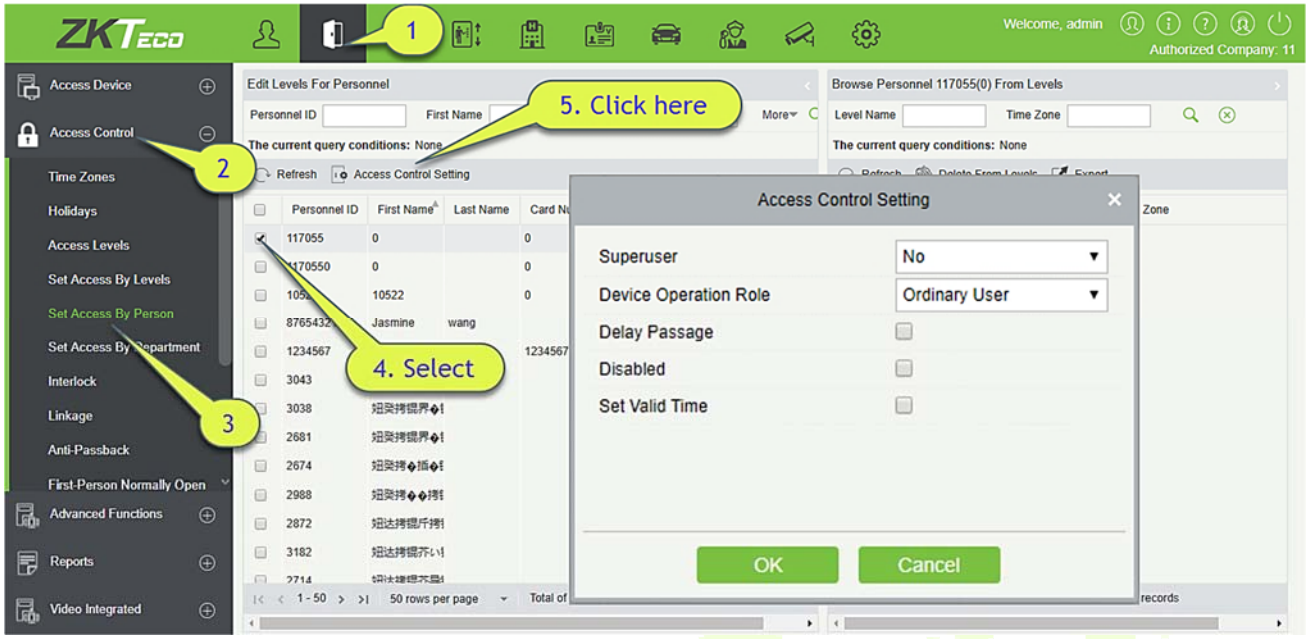
1) Click [**Access Control**] > [**Access Levels**] > [**Set Access By Person**], click Employee to view the levels in the list on the right.

2) Click [**Add to Levels**] under Related Operations to pop up the Add to Levels box, select Level (multiple) and click > to move it to the selected list on the right; then click [**OK**] to save.

3) Select Level (multiple) in the right list and click [Delete from levels] above the list, then click [**OK**] to delete the selected levels.

Setting Access Control for Selected Personnel:

A. Select a person in the list on the left and click [**Access Control Setting**].



B. Set access control parameters and then click [**OK**] to save the settings.

4.2.6 Set Access by Department

Add the selected department to the selected access levels or delete the selected department from the access levels. The access of the staff in the department will be changed.

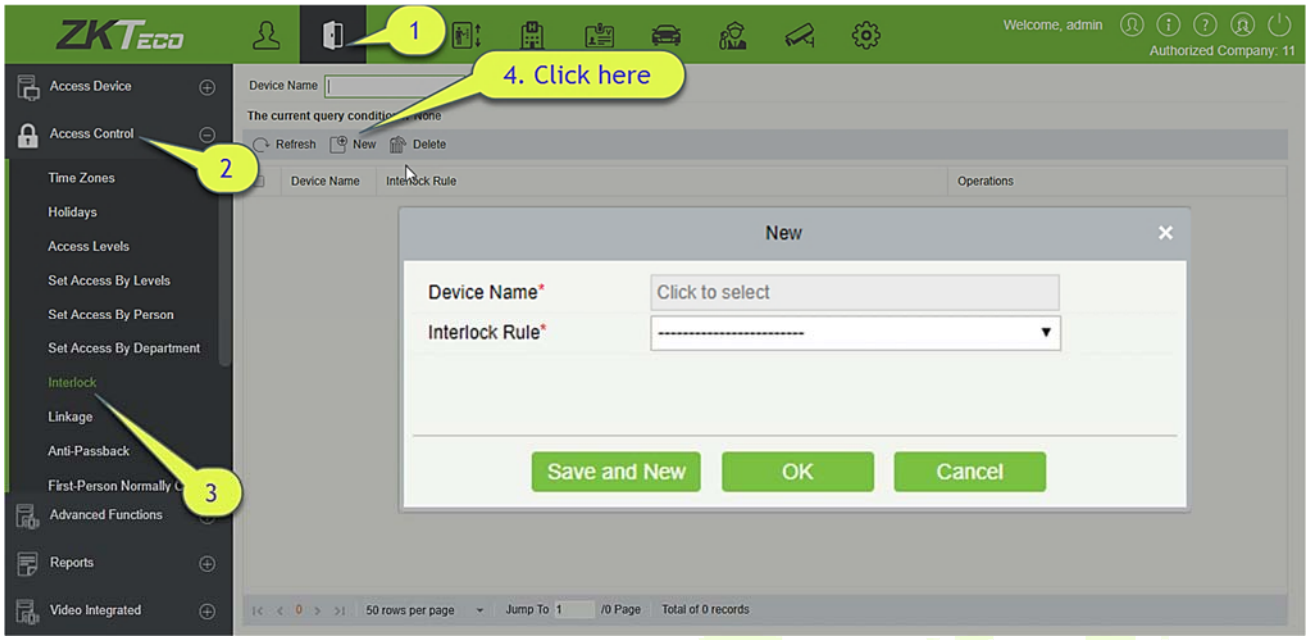
4.2.7 Interlock

Interlock can be set for two or more locks belonging to one access controller. When one door is opened, the others will be closed, or you cannot open the door.

Before setting the interlock, please ensure that the access controller is connected with door sensor, which has been set as NC or NO state.

- **Add Interlock**

1. Click [**Access Control**] > [**Interlock**] > [**New**] to enter the edit interface:



2. Select Device Name. When users are adding devices, interlocked devices cannot be seen in the dropdown list. After deleting established interlock information, the corresponding device will return to the dropdown list. Interlock setting will vary with the number of doors controlled by selected devices:

- A one-door control panel has no interlock settings.
- A two-door control panel: 1-2 two-door interlock settings.
- A four-door control panel: 1-2 two-door interlock; 3-4 two-door interlock; 1-2-3 three-door interlock; 1-2-3-4 four-door interlock.

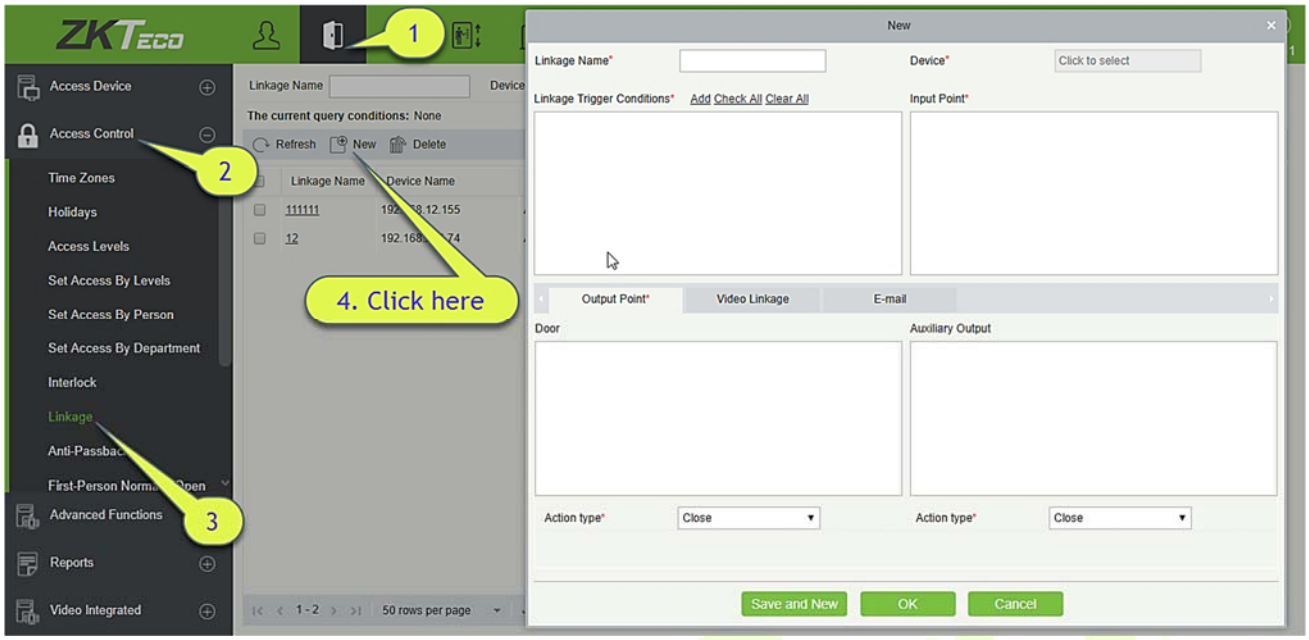
3. Select Interlock Rule, tick an item, then click [**OK**] to complete. The new added interlock settings will be shown in the list.

✍**Note:** During editing, the device cannot be modified, but the interlock settings can be modified. If the interlock settings are not required for the device any more, the interlock setting record can be deleted. If users delete a device record, its interlock setting record, if any, will be deleted.

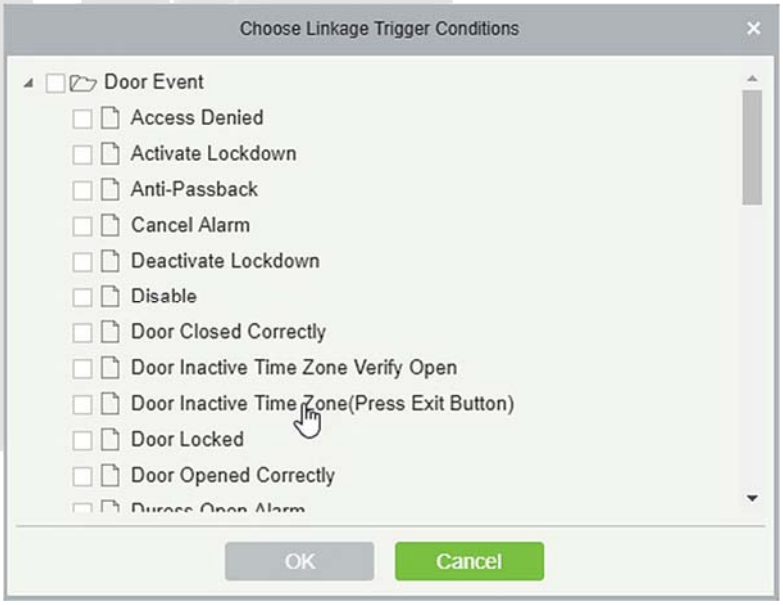
4.2.8 Linkage

Linkage setting means when an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control events such as verification, opening, alarm and abnormal of system, and list them in the corresponding monitoring view.

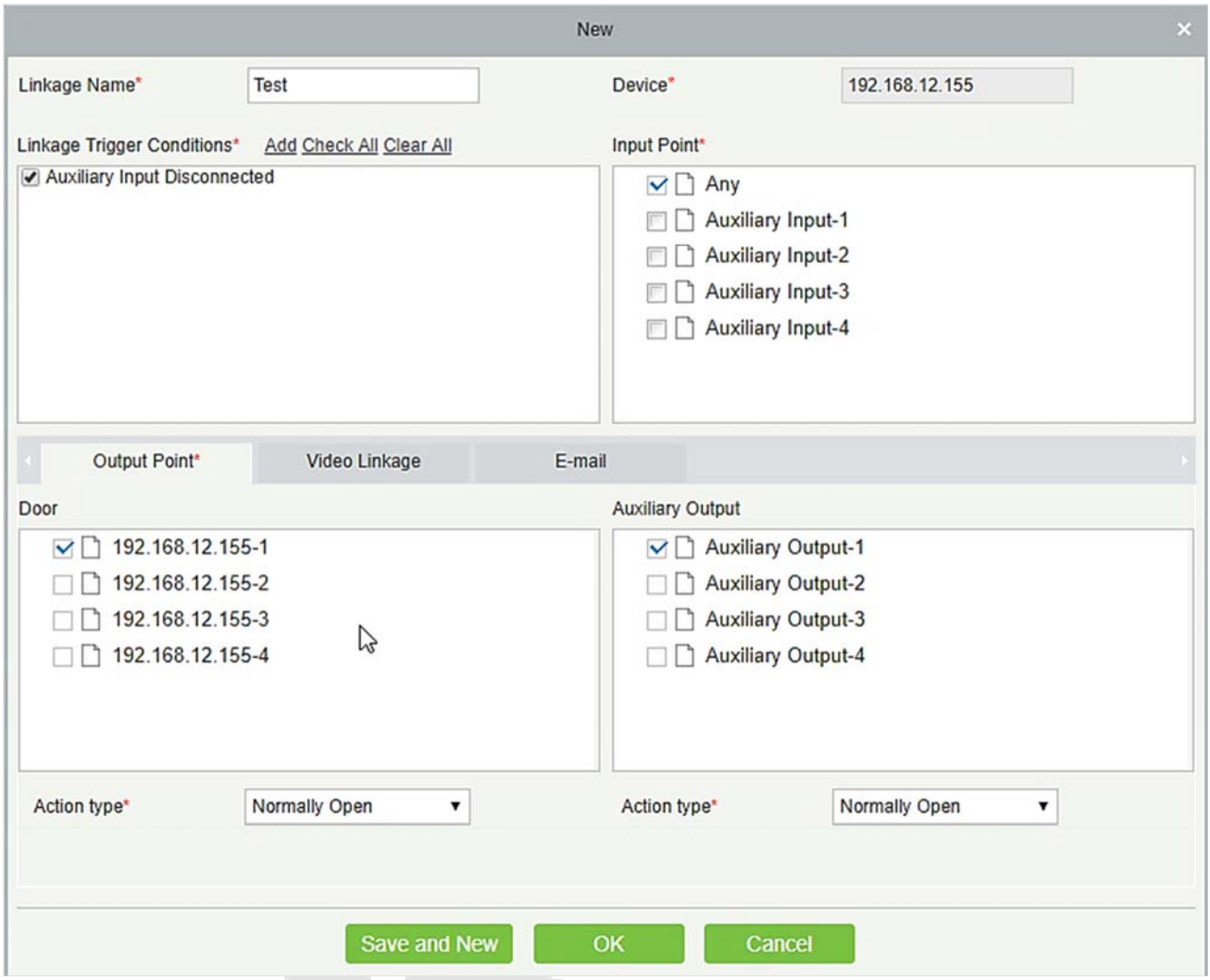
Add Linkage setting:



1. Click [**Access Control**] > [**Linkage**] > [**New**].
2. Enter the linkage name, select a linkage device, linkage trigger conditions, input point, output point, then set linkage action, video linkage and other parameters.
3. After selecting devices, corresponding linkage settings will be displayed. The System will first judge whether the device is successfully connected and has read extended parameters. If there is no available extended parameters, the system cannot set any linkage. If there is an available extended parameter(s), the system will show linkage settings according to the door quantity, auxiliary input and output quantity of currently selected device:



✍**Note:** Linkage Trigger Conditions contain Door Event and Auxiliary Input Event. And "Fail to connect server", "Recover connection", "Device connection off" will be filtered from Door Event.



4. Select the Input Point and Output Point, Linkage Action, Video Linkage and Email Address.

The fields are as follows:

Linkage Name: Set a linkage name.

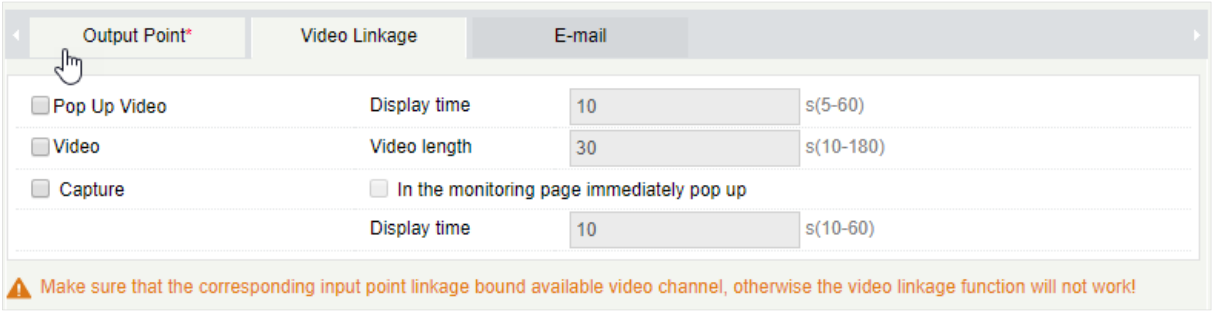
Linkage Trigger Condition: Linkage Trigger Condition is the event type of selected device. Except Linkage Event Triggered, Enable/Disable Auxiliary Output, and Device Start. All events could be trigger condition.

Input Point: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refers to specific device parameters).

Output Point: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, and Auxiliary Output 10 (the specific output point please refers to specific device parameters).

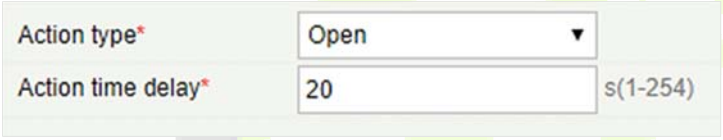
Action Type: Close, Open, Normal Open, Lock, Unlock. The default is Close. To open, delay time or Normal Open shall be set.

Video Linkage:



- Pop up video: Whether to set the pop-up preview page in real-time monitoring, and set the pop-long.
- Video: Enable or disable background video recording and set the duration of background video recording.
- Capture: Enable or disable background snapshots.

Delay: Ranges from 1~254 second (This item is valid when Action type is Open).



5. After editing, click [**OK**] to save and quit, then the added linkage setting will be shown in the list.

For example, if users select Normal Punching Open Door as trigger condition, then the input point is Door 1, output point is Lock 1, action type is Open, delay is 60 second. When Normal Punching Open Door occurs at Door 1, the linkage action of Open will occur at Lock 1, and the door will be open for 60 second.

✍**Note:** During editing, you cannot modify the device, but modify the linkage setting name and configuration. When delete a device, its linkage setting record, if any, will be deleted.

If the device and trigger condition are the same, and system has linkage setting record where the input point is a specific door or auxiliary input, it will not allow users to add (or edit) a linkage setting record where the input point is any.

On the contrary, if the device and trigger condition are the same, and the system has linkage setting record where the input point is 'Any', it will not permit user to add (or edit) a linkage setting record where the input point is a specific door or auxiliary input.

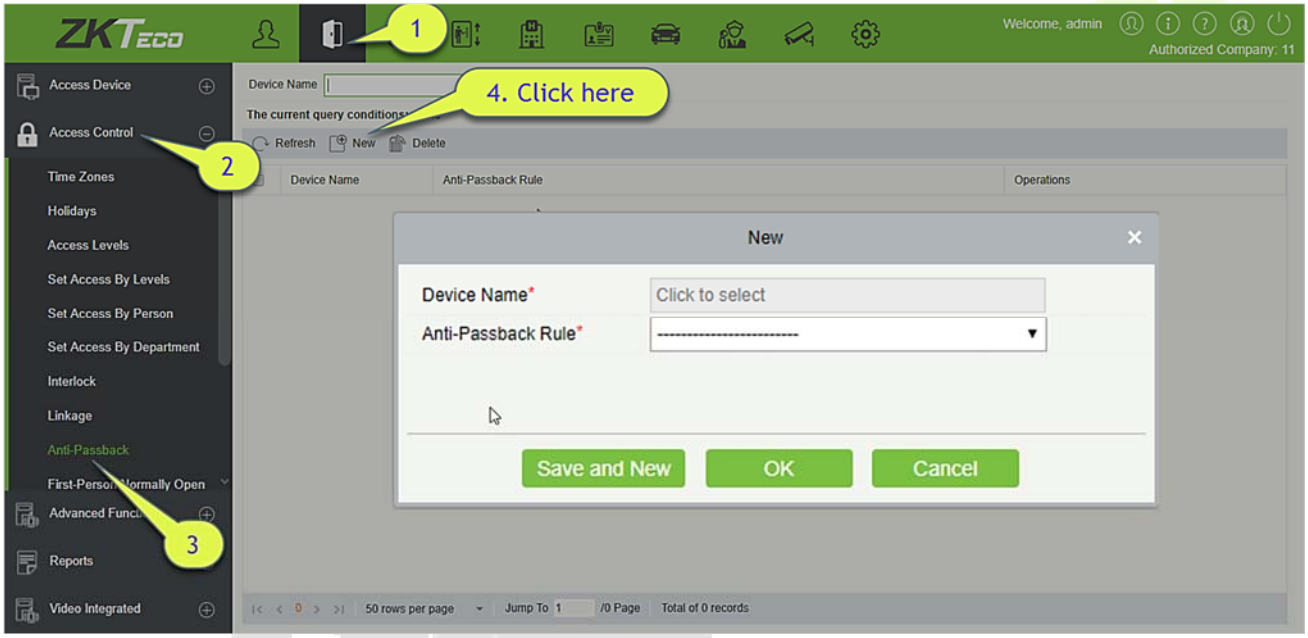
In addition, same linkage setting at input point and output point is not allowed. The same device permits consecutive logical linkage settings. The system allows to set several trigger conditions for a linkage setting at a time.

4.2.9 Anti-Passback

Currently anti-passback settings support in and out anti-passback. In some special occasions, it is required that the cardholders who entered from a room by card swiping at a door device must swipe the cards over a device at the same door when leaving to keep the entry and exit records strictly consistent. The user can use this function just by enabling it in the settings. This function is normally used in prisons, the army, national defense, scientific research, bank vaults, etc.

Add Anti-Passback Settings:

1. Click [**Access Control**] > [**Anti-Passback**] > [New] to show the edit interface:



2. Select devices. When users are adding Anti-Passback Rules, devices with anti-passback settings cannot be seen in the dropdown list. When deleting established anti-passback information, the corresponding device will appear in the dropdown list again. The settings vary with the number of doors controlled by the device.

- Anti-passback settings of a one-door control panel: Anti-passback between door readers.
- Anti-passback settings of a two-door control panel: Anti-passback between readers of door 1; anti-passback between readers of door 2; anti-passback between door 1 and door 2.
- Anti-passback settings of a four-door control panel: Anti-passback of door 1 and door 2; anti-passback of door 3 and door 4; anti-passback of door 1/2 and door ¾; anti-passback of door 1 and door 2/3; anti-passback of door 1 and door 2/3/4; Anti-passback between readers of door 1/2/ 3/ 4.

✍**Note:** The door reader mentioned above includes Wiegand reader that connected with access controller and InBio reader. The single and two door controller with Wiegand reader includes out and in reader. There is only “In reader” for four door control panel. The reader number of 1, 2 (that is RS485 address or

device number, the same below) is for door 1, the reader number of 3, 4 is for door 2, etc. No need to consider if it is a Wiegand reader or InBio reader when you are setting the anti-passback between doors or between readers, just make sure the in or out reader is set according to the actual requirements. For the reader number, odd number is for in reader, and even number is for out reader.

3. Select Anti-Passback Rule, and tick one item, click [**OK**] to complete, then the added anti-passback settings will be shown in the list.

✍**Note:** When editing, you cannot modify the device, but can modify anti-passback settings. If anti-passback setting is not required for the device any more, the anti-passback setting record can be deleted. When you delete a device, its anti-passback setting record, if any, will be deleted.

4.2.10 First-Person Normally Open

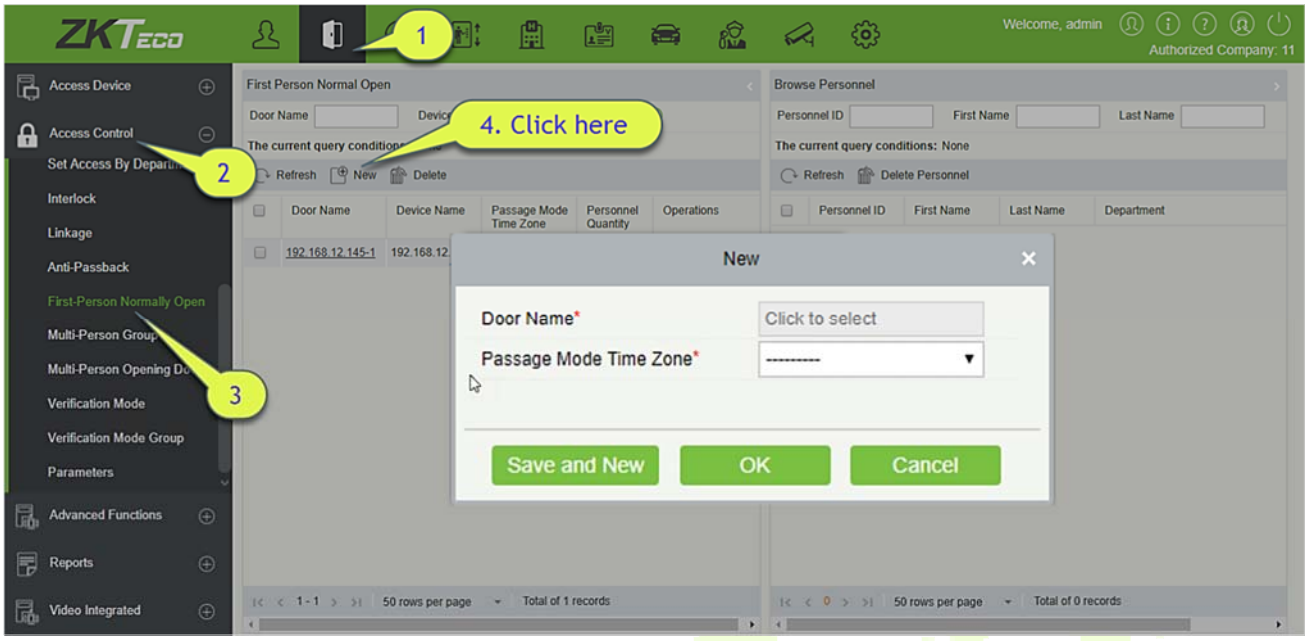
First-Person Normally Open: During a specified interval, after the first verification by the person having First-Person Normally Open level, the door will be Normal Open, and will automatically restore closing after the valid interval has expired.

Users can set First-Person Normally Open for a specific door (the settings include door, door opening time zone and personnel with First-Person Normally Open level). A door can set First-Person Normally Open for multiple time zones. The interface of each door will show the number of existing First-Person Normally Open.

When adding or editing First-Person Normally Open settings, you may only select door and time zones. After successful adding, add personnel that can open the door. You can browse and delete the personnel on the right of the interface.

Operation steps are as follows:

1. Click [**Access Control**] > [**First-Person Normally Open**] > [**New**], select Door Name and Passage Mode Time, and click [**OK**] to save the settings.

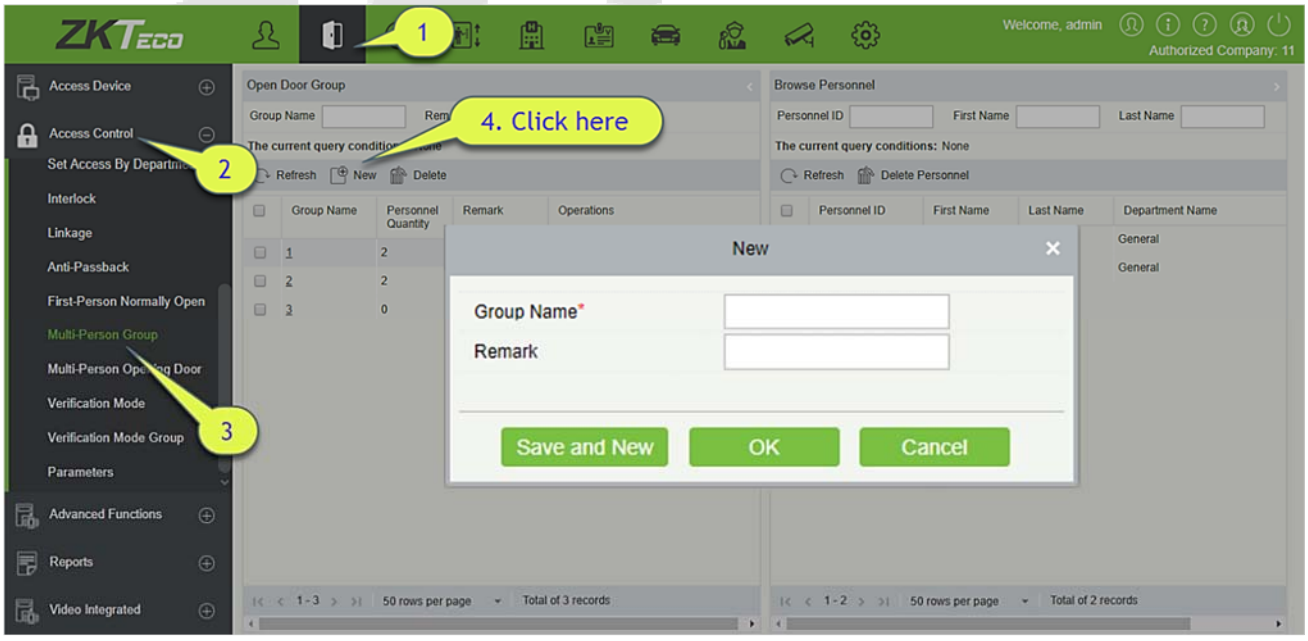


2. Click [**Add Personnel**] under Related operation to add personnel having First-Person Normally Open level (these personnel must have access control level), then click [**OK**] to save.

4.2.11 Multi-Person Group

The door will open only after the consecutive verification of multiple people. Any person verifying outside of this combination (even if the person belongs to other valid combination) will interrupt the procedure and you need to wait 10 seconds to restart verification. It will not open by verification by only one of the combination.

1. Click [**Access Control**] > [**Multi-Person Group**] > [**New**] to access the following edit interface:



Group name: Any combination of up to 30 characters that cannot be identical to an existing group name.

After editing, click [**OK**] to save and return. The added Multi-Person Personnel Group will appear in the list.

2. Click [**Add personnel**] under Related Operations to add personnel to the group.
3. After selecting and adding personnel, click [**OK**] to save and return.

✍**Note:** A person can only be grouped into one group.

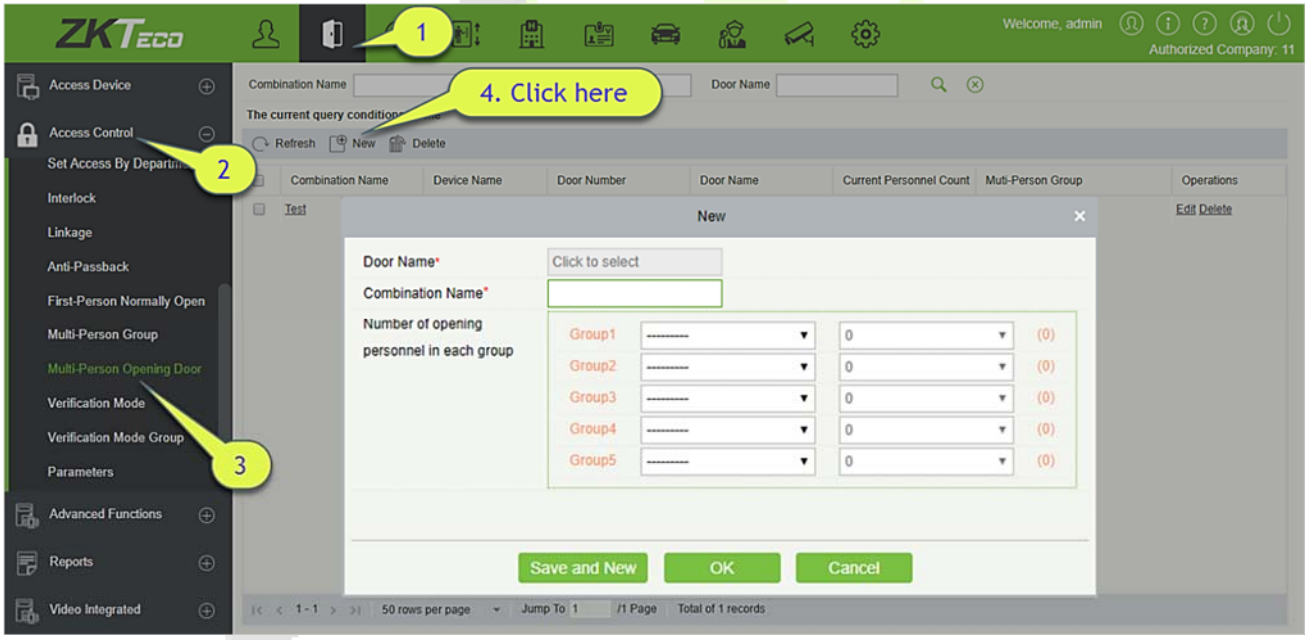
4.2.12 Multi-Person Opening Door

Set levels for personnel in Multi-Person Personnel Group.

It is a combination of the personnel in one or more Multi-Person Personnel Groups. When setting the number of people in each group, you can configure one group (such as combined door opening by two people in one group) or multiple groups (such as combined door opening by four people, including 2 people in group 1 and 2 people in group 2), and at least one group shall consist of number of door opening people instead of 0, and the total number shall not be greater than 5. In addition, if the number of people entered is greater than that in the current group, Multi-Person Opening Door will be disabled.

Multi-Person Opening Door Settings:

1. Click [**Access Control**] > [**Multi-Person Opening Door**] > [**New**]:



2. The maximum number of multi-person opening door people for combined door opening is 5. That in the brackets is the current actual number of people in a group. Select the number of people for combined door opening in a group, and click [**OK**] to complete.

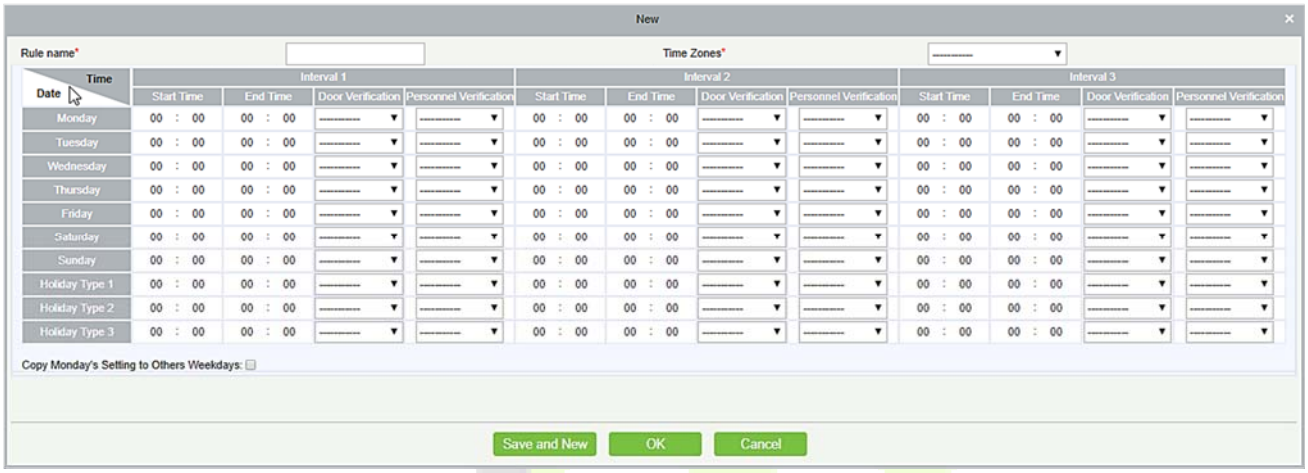
✍**Note:** The default Credit Card Interval is 10 seconds, it means that the interval of two personnel's verification must not exceed 10 seconds. You can modify the interval if the device supports.

4.2.13 Verification Mode Group

Verification Mode: You can set verification modes for doors and personnel separately in a specified time segment.

- **Add**

1. Click [**Access Control**] > [**Verification Mode**] > [**New**] to go to the page for adding a verification mode rule.



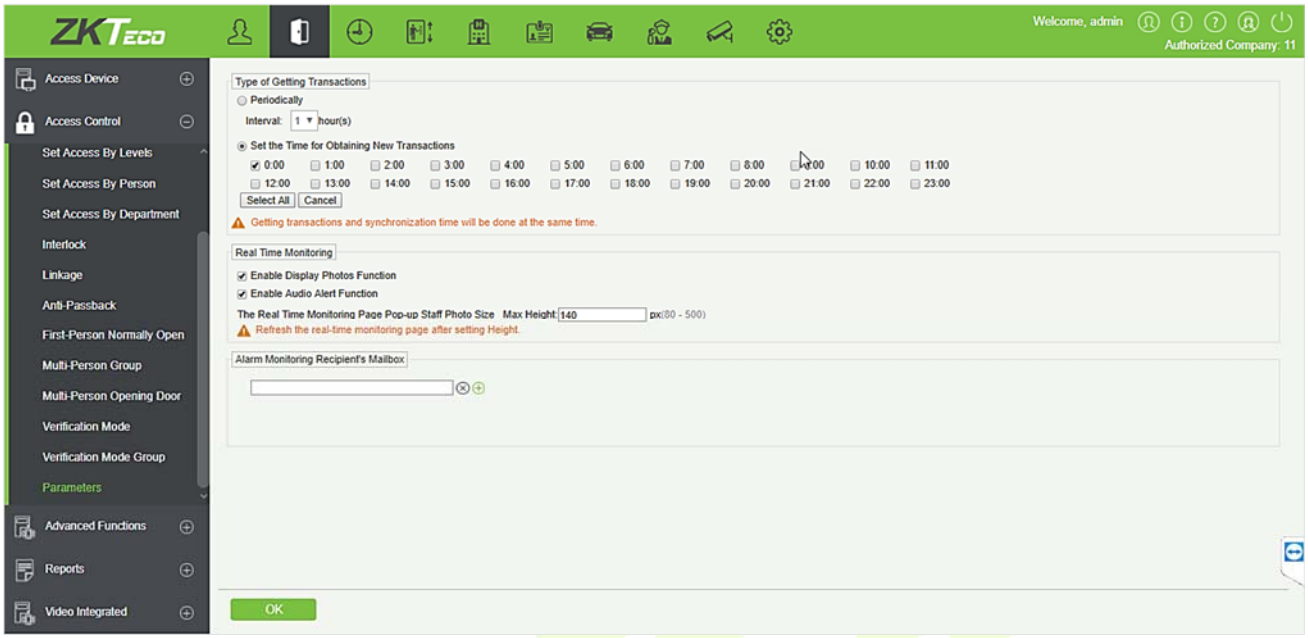
2. Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.
3. Click [**OK**] to finish the setting.
4. On the list page, you can add or delete doors in the verification mode rule.

✍**Note:** If a rule includes the verification mode for personnel, you cannot select doors with the RS485 readers when adding doors. You can modify only the configuration on the reader setting page before adding doors.

Verification Mode Group: Set appropriate personnel for configured verification mode rule.

4.2.14 Parameters

Click [**Access Control**] > [**Parameters**] to enter the parameter setting interface:



Type of Getting Transactions

- **Periodically**

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

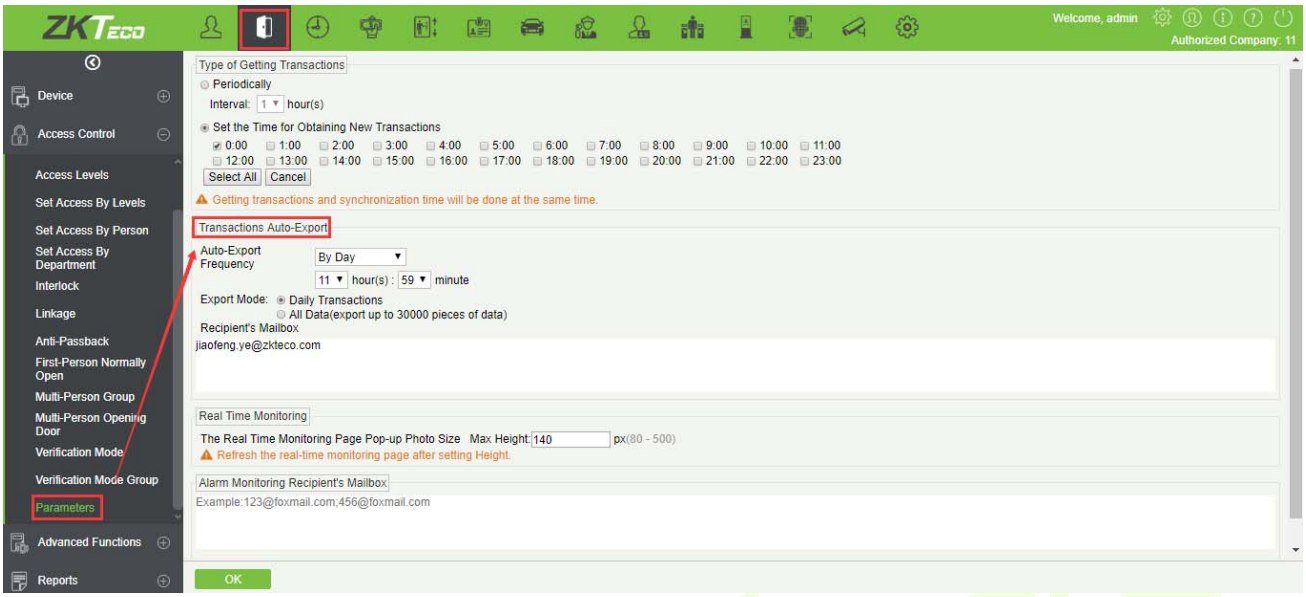
- **Set the Time for Obtaining New Transactions**

The selected Time is up, the system will attempt to download new transactions automatically.

Transaction Auto-Export

The user can choose the export frequency and the data to be exported each time. If the export frequency is selected as **"By day"**, you must set the time to export the data. You must also select the mode of export. It can be daily transactions or all the system data(30000 data units can be sent at a time.

If the export frequency is selected as **"By Month"**, you must select the day to export the data. It can be the first day of the month or you can specify any particular date. Then select the export frequency as Daily Data or all System data. Finally, add the recipient's mail address to send the transaction data.



The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

Alarm Monitoring Recipient Mailbox: The system will send email to alarm monitoring recipient's mailbox if there is any event.

4.3 Advanced Functions

Advanced Access control is optional function. If needed, please contact business representative or pre-sales engineer, you can use these functions after obtaining license and activating.

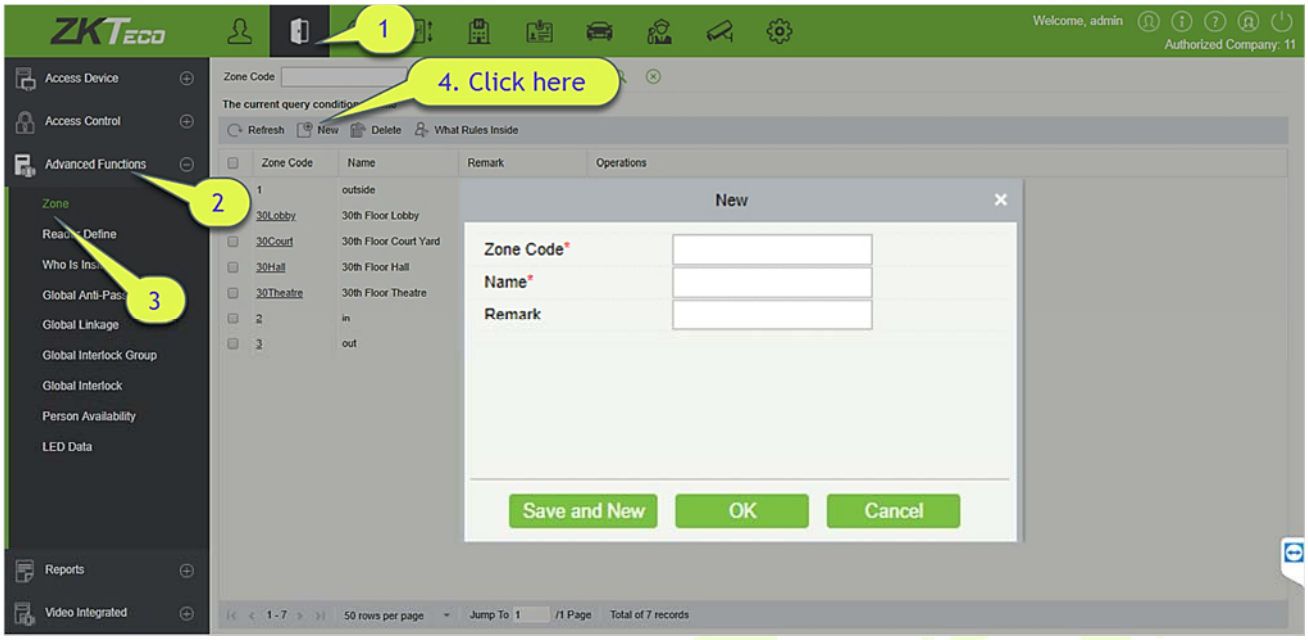
✍**Note:** Except Global Linkage, to use other advanced functions you need to enable Background Verification. For detail, please see Device Operation.

4.3.1 Zone

It mainly uses partition Zones in advanced access control. When using such advanced functions as Global Zone APB, you must define Access Zones.

- **Add**

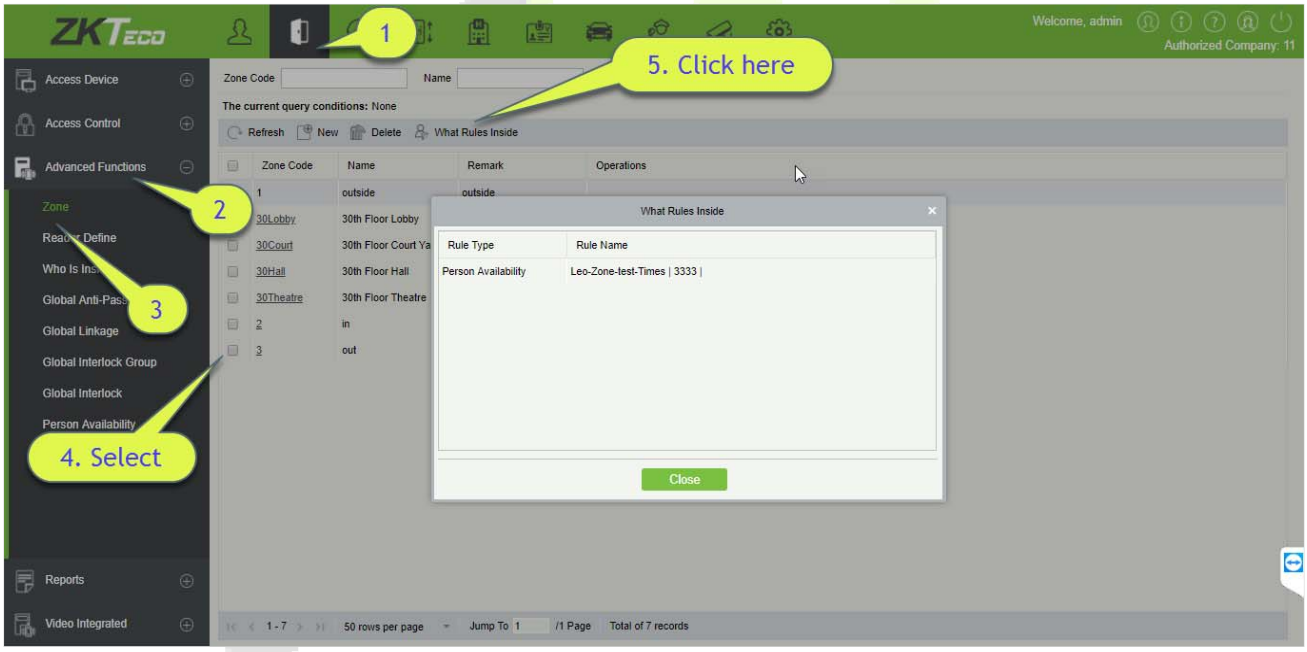
1. Click [**Advanced Functions**] > [**Zone**] > [**New**] to enter the Add Zone interface:



2. Set Zone Code, Name, Parent Zone and Remark as required.

3. Click [**OK**] to save and quit. The added Zone will appear in the list.

What rules inside:

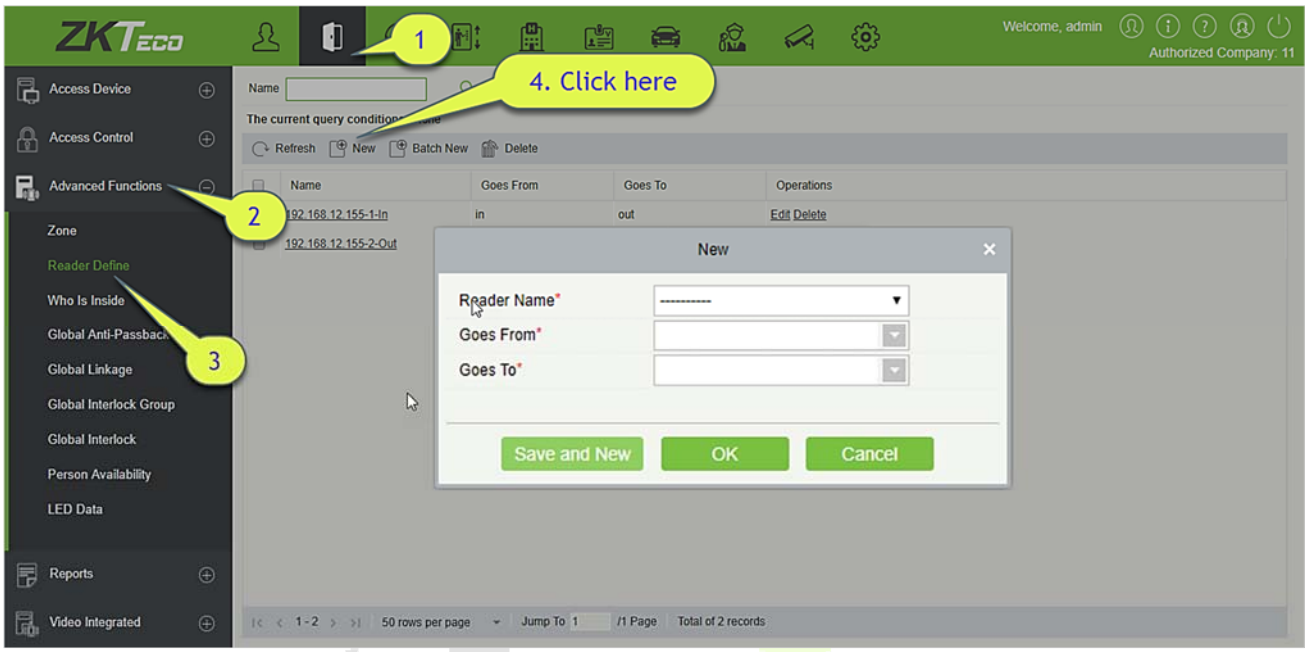


4.3.2 Reader Define

Reader Define indicates that Reader control from one access zone to another one, it is based on access zone. If advanced functions are needed, you shall set the Reader Define.

- **Add**

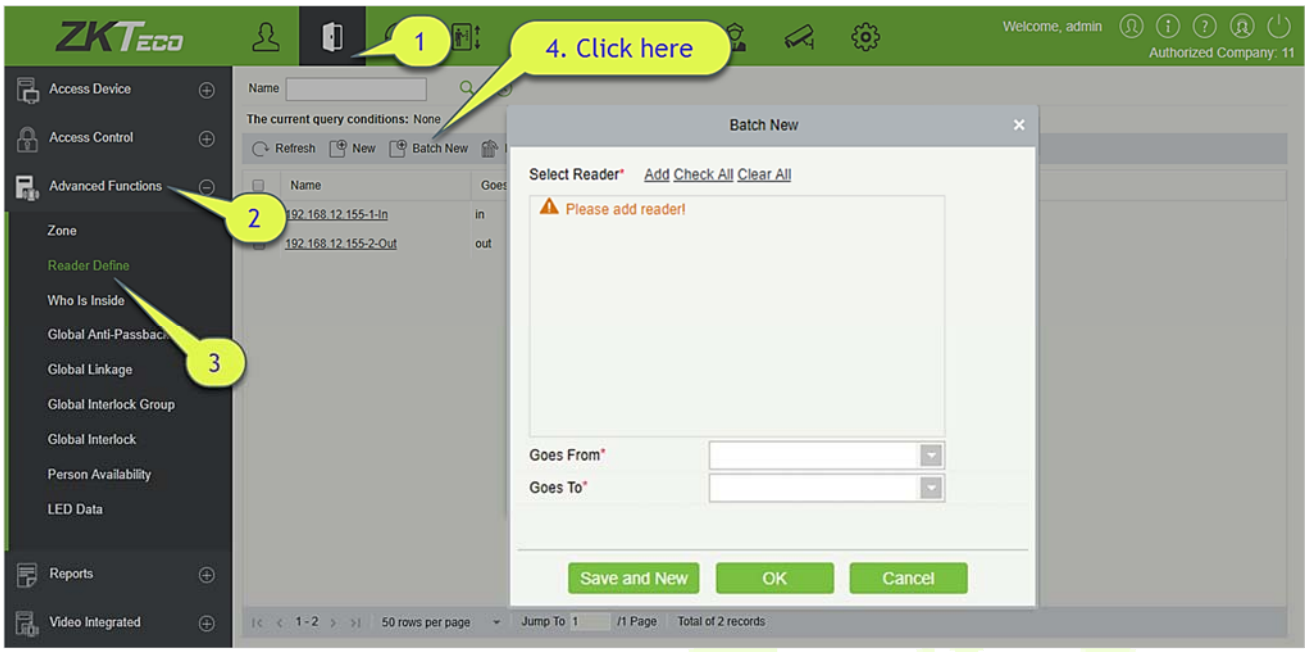
1. Click [**Advanced Functions**] > [**Reader Define**] > [**New**] to enter the add interface:



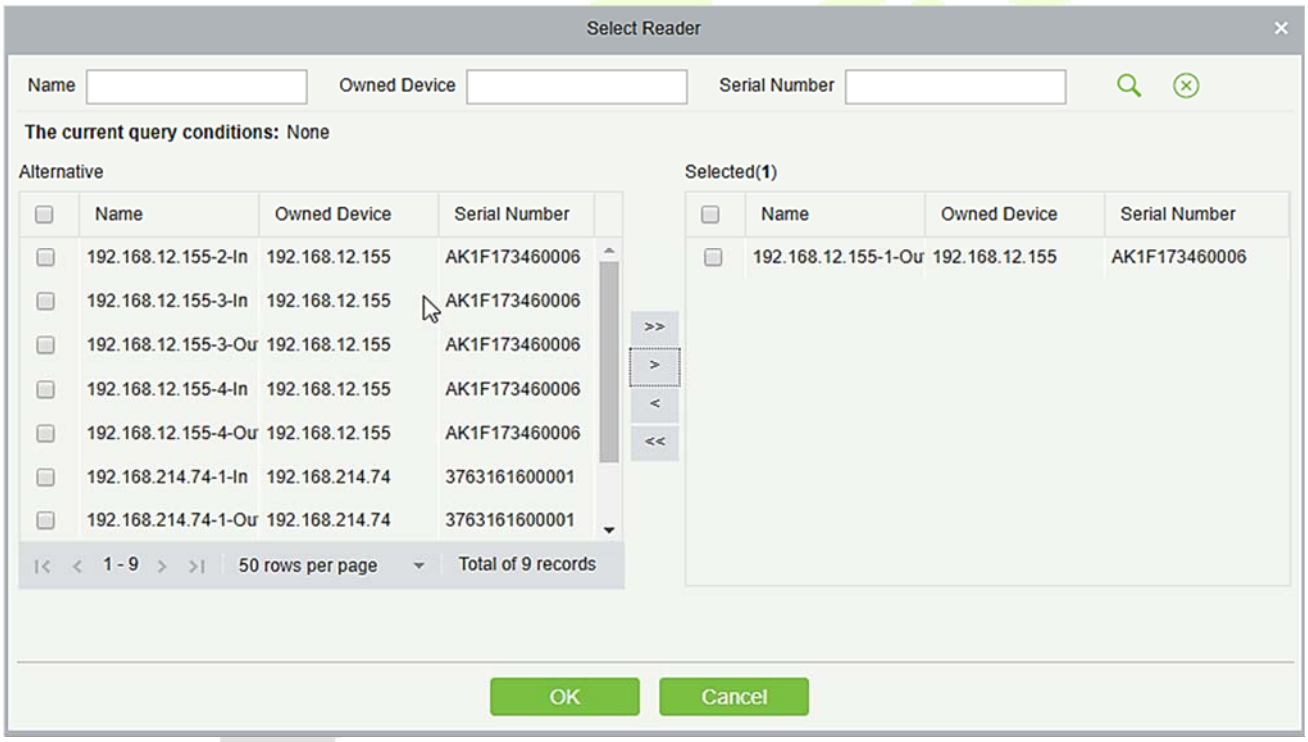
2. Set Reader Name, Goes From and Goes To as required.
3. Click [**OK**] to save and quit. The added Reader Define will appear in the list.

- **Batch New**

1. Click [**Advanced Functions**] > [**Reader Define**] > [**Batch New**] to enter the batch add interface:



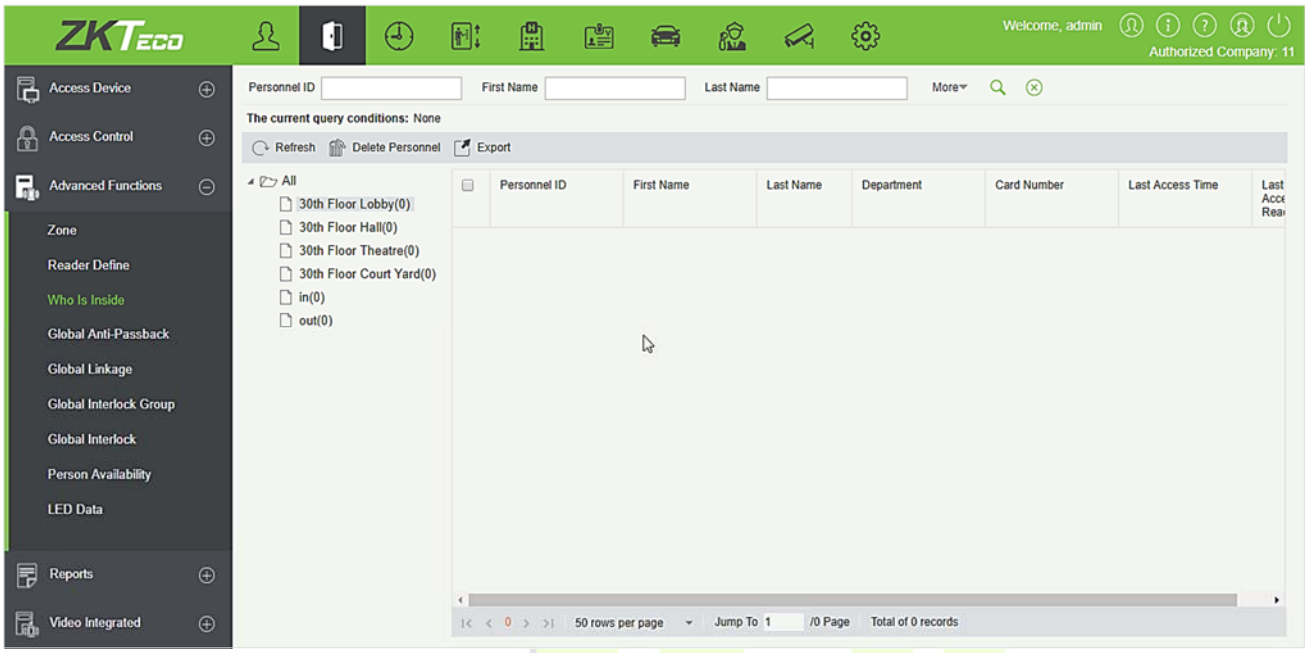
2. Click [**Add**], select Reader(s) and move towards right and click **[OK]**.



3. Set Goes from and Goes to as required and press [**OK**].

4.3.3 Who is Inside

After entering the zone, you can view all personnel status in the zone by zone tree.



- **Delete Personnel**

Deleting personnel in the selected area will clear the global anti-passback status of the personnel.

- **Export**

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

ZKTECO

Total People 10

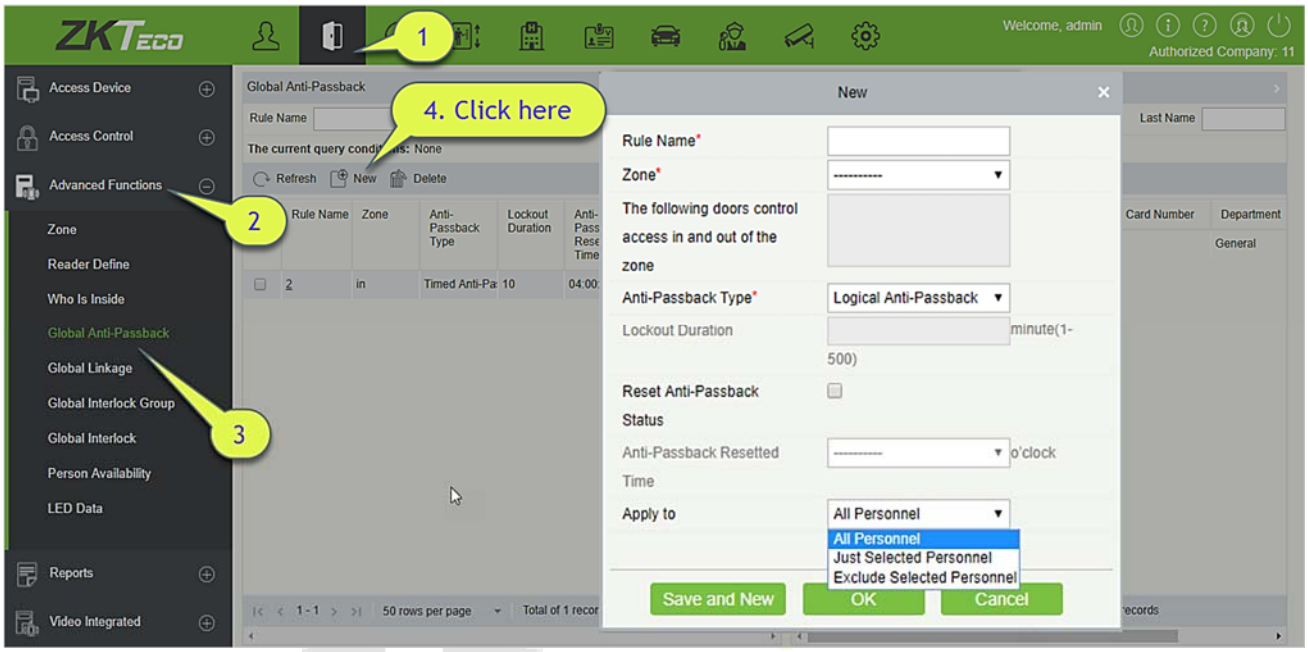
Personnel ID	First Name	Last Name	Department	Card Number	Last Access Time	Last Access Reader
1	Jerry	Wang	General	4461253	2017-12-18 09:29:31	192.168.218.60-2-In
2	Lucky	Tan	Development Department	6155266	2017-12-18 09:27:12	192.168.218.60-1-In
2940	Sherry	Yang	Hotel	1411237	2017-12-18 09:55:52	192.168.218.60-1-In
3	Leo	Hou	Financial Department	13271770	2017-12-18 09:34:57	192.168.218.60-2-In
4	Berry	Cao	General	13592341	2017-12-18 09:55:58	192.168.218.60-1-In
5	Necol	Ye	Marketing Department	13260079	2017-12-18 09:34:18	192.168.218.60-1-In
6	Amber	Lin	Financial Department	4628036	2017-12-18 09:25:29	192.168.218.60-1-In
7	Jacky	Xiang	General	6323994	2017-12-18 09:27:18	192.168.218.60-2-In
8	Glori	Liu	Marketing Department	6189166	2017-12-18 09:34:20	192.168.218.60-2-In
9	Lilian	Mei	Development Department	9505930	2017-12-18 09:27:22	192.168.218.60-1-In

4.3.4 Global Anti-Passback

Global Zone APB can set Anti-Passback across devices; you can use this function after setting Global Anti-passback. You must set Access Zone and Reader Define before using, and also the device that has set Anti-Passback shall issue background verification parameters.

- **Add**

1. Click [**Advanced Functions**] > [**Global Anti-passback**] > [**New**] to enter the add interface:



2. Set Rule Name (Unrepeatable), Zone, Anti-passback Type, Lockout Duration, Reset Anti-passback Status and When to Reset the Anti-passback as required.

Zone: Select an option from the dropdown list, Corresponding doors will display in the text box of "The following doors control access in and out of the zone". At the same time, the doors obey the rule of one door cannot set as the boundary of two independent Anti-passback.

Anti-passback Type: Logical Anti-passback, Timed Anti-passback or Timed Logic Anti-passback.

- Logical Anti-passback: The door will not open if the entry and exit records is not in consistent with Anti-passback zone.
- Timed Anti-passback: In specified time period, user can enter Anti-passback zone only once. After the Time period has expired, user state will be cleared, and allow user to enter this zone again.
- Timed Logic Anti-passback: In Specified time period, Users who enter Anti-passback zone must obey the rule of Logical Anti-passback. If users exceed timed period, system will time again.

Lockout Duration: Only select Timed Anti-passback and Timed Logic Anti-passback in Anti-passback Type. Lockout Duration can be set.

Reset Anti-passback Status: Tick it to clear Anti-passback status of personnel in the system, and recover initial state. Only tick this option. When to Reset the Anti-passback can be select. After the reset time of the anti-passback has expired, system will clear all the Anti-passback status of personnel in zone.

When to Reset the Anti-passback: Select time to reset Anti-passback.

Apply to: All Personnel, Just Selected Personnel and Exclude Selected Personnel three types.

- Apply to All Personnel: Can only edit and does not support select personnel.
- Apply to Just Selected Personnel: The anti- passback is only effective for these selected personnel.
- Apply to Exclude Selected Personnel: The anti- passback only effective for these exclude selected personnel.

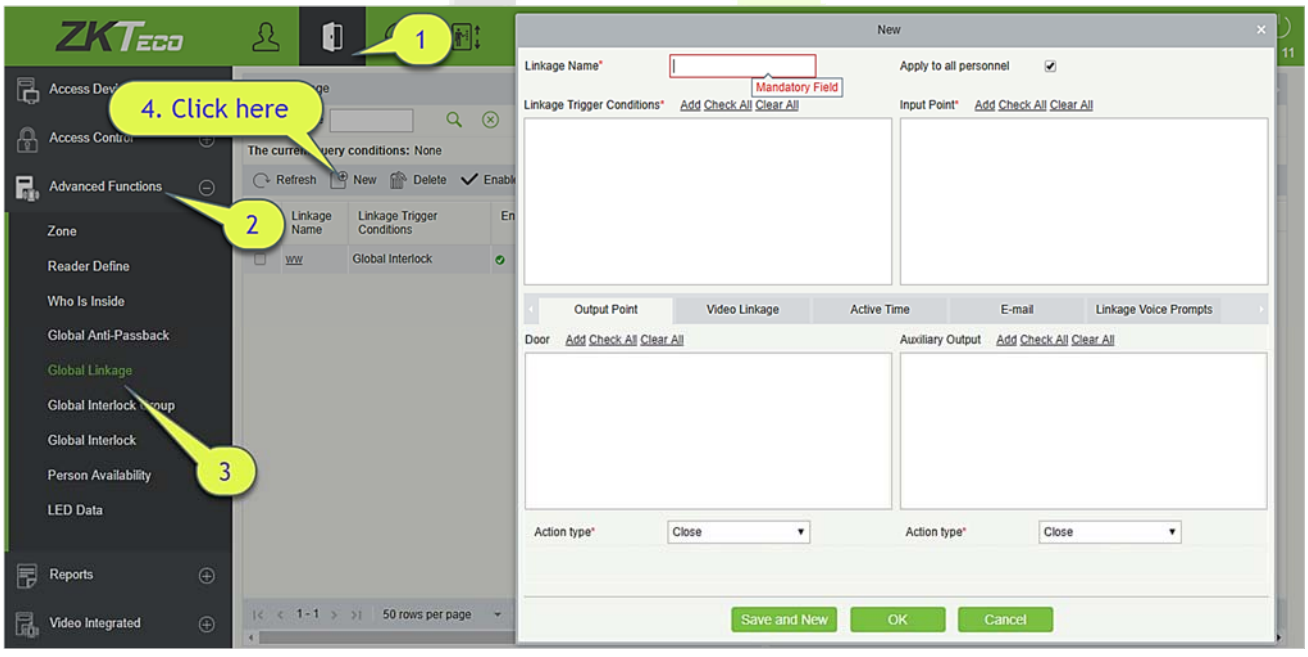
3. Click [**OK**] to save and quit. The added Global Zone APB will display in the list.

4.3.5 Global Linkage

The global linkage function allows you to configure data across devices. Only push devices support this function.

- **Add**

1. Click [**Advanced Functions**] > [**Global Linkage**] > [**New**]:



Apply to all personnel: If this option is selected, this linkage setting is effective for all personnel.

Active Time: Set the active time of the linkage setting.

2. Choose Global Linkage trigger conditions, the input point (System will filter devices according to the choice in first step) and the output point, Set up linkage action. For more details about these parameters, please refer to Linkage Setting.

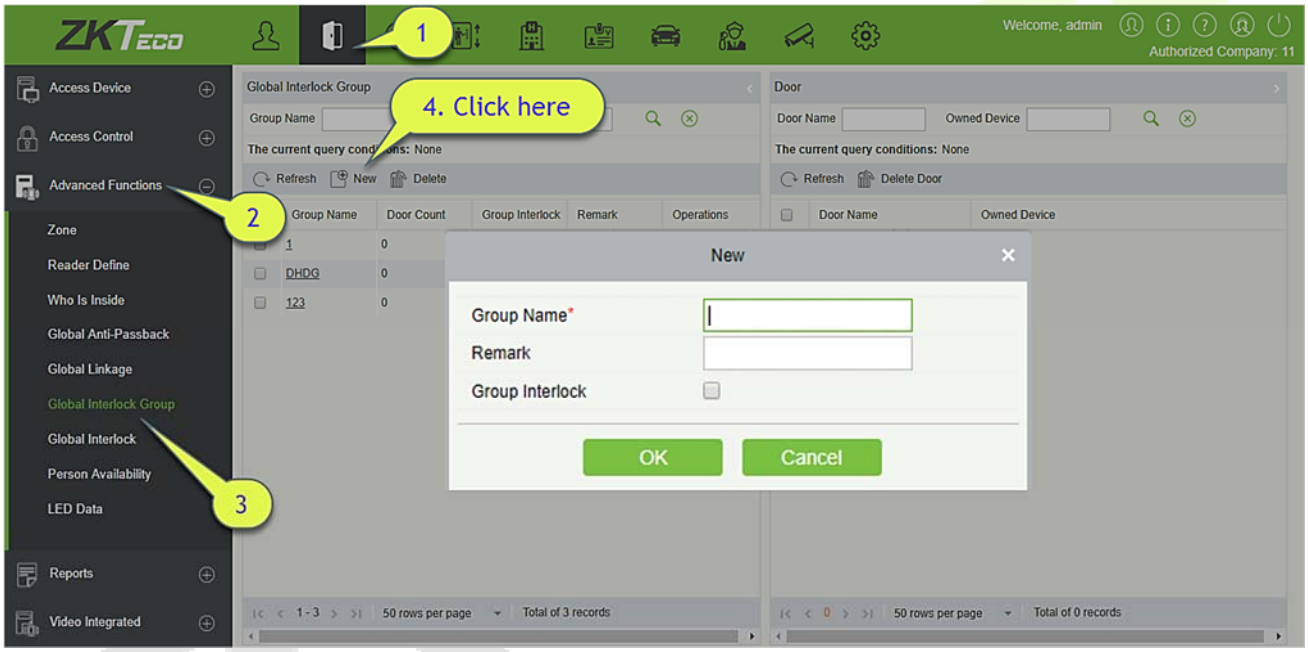
✍**Note:** You can select multiple Door Events, but "Fail to connect server", "Recover connection" and "Device connection off" will be filtered automatically from Door Event.

3. Click [**OK**] to save and quit. The added Global Linkage will display in the list.

4.3.6 Global Interlock Group

The global interlock group groups the doors in the global interlock, but to use the global interlock function, the device must be enabled with background authentication.

Click [**Advanced Functions**] > [**Global Interlock Group**]> [**New**]:



Group Name:

Any combination of up to 30 characters that cannot be identical to an existing group name.

1. After editing, click [**OK**] to save. After confirming that add the door immediately, the information of added door will appear in the list.
2. Click [**Add Door**] under Related Operations to add door to the group.
3. After selecting and adding personnel, click [**OK**] to save and return.

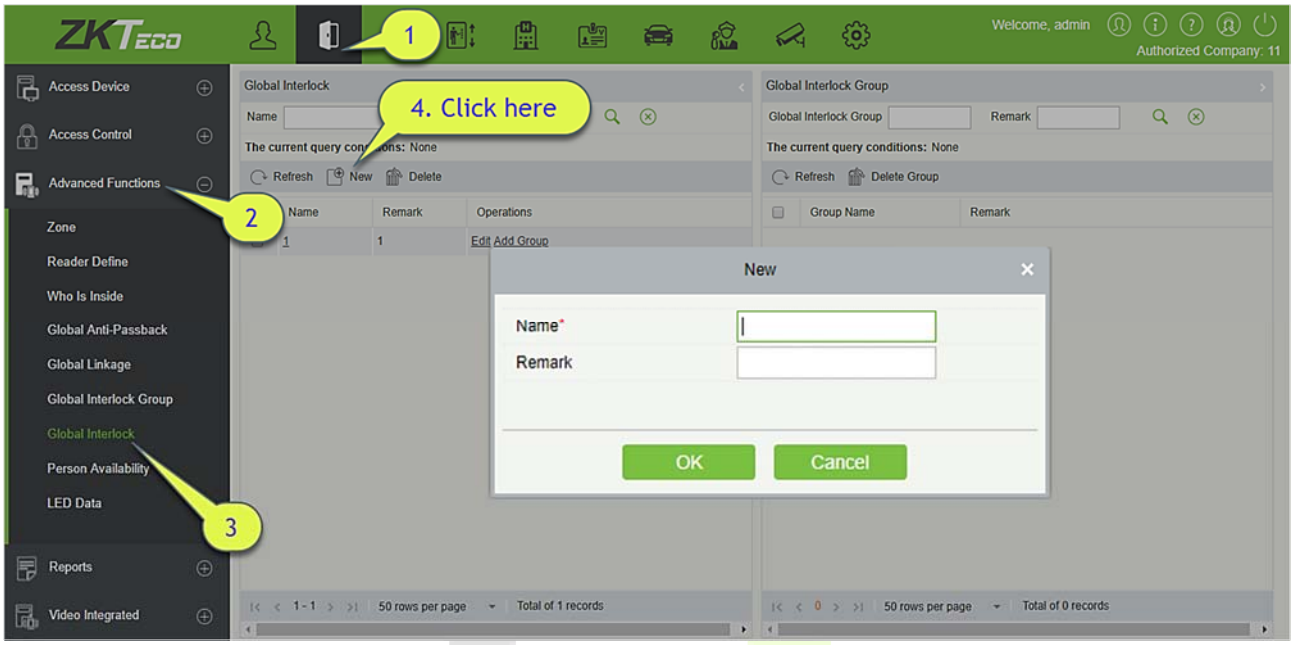
Group Interlock: If the option is selected, set global interlock rule for the interlocking group.

4.3.7 Global Interlock

The global interlock function allows you to configure data across devices. Only push devices support this function.

Multi-Person Opening Door Setting:

Click [**Advanced Functions**] > [**Global Interlock**]> [**New**]:



Name:

1) Any combination of up to 30 characters that cannot be identical to an existing name.
2) After editing, click [**OK**] to save. After confirming that add the group immediately, the information of add group will appear in the list.
3) Click [**Add Group**] under Related Operations to add door to the group.
4) After selecting and adding group, click [**OK**] to save and return.

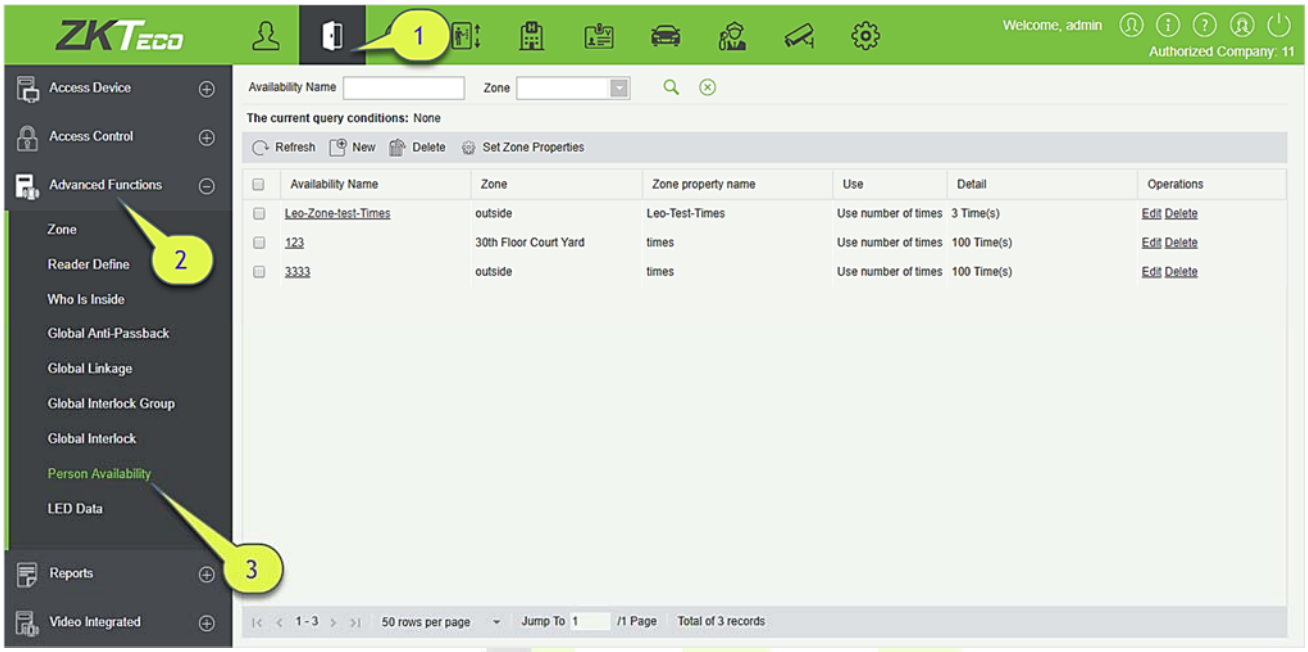
Group Interlock: If the option is selected, set global interlock rule for the interlocking group.

Notes:

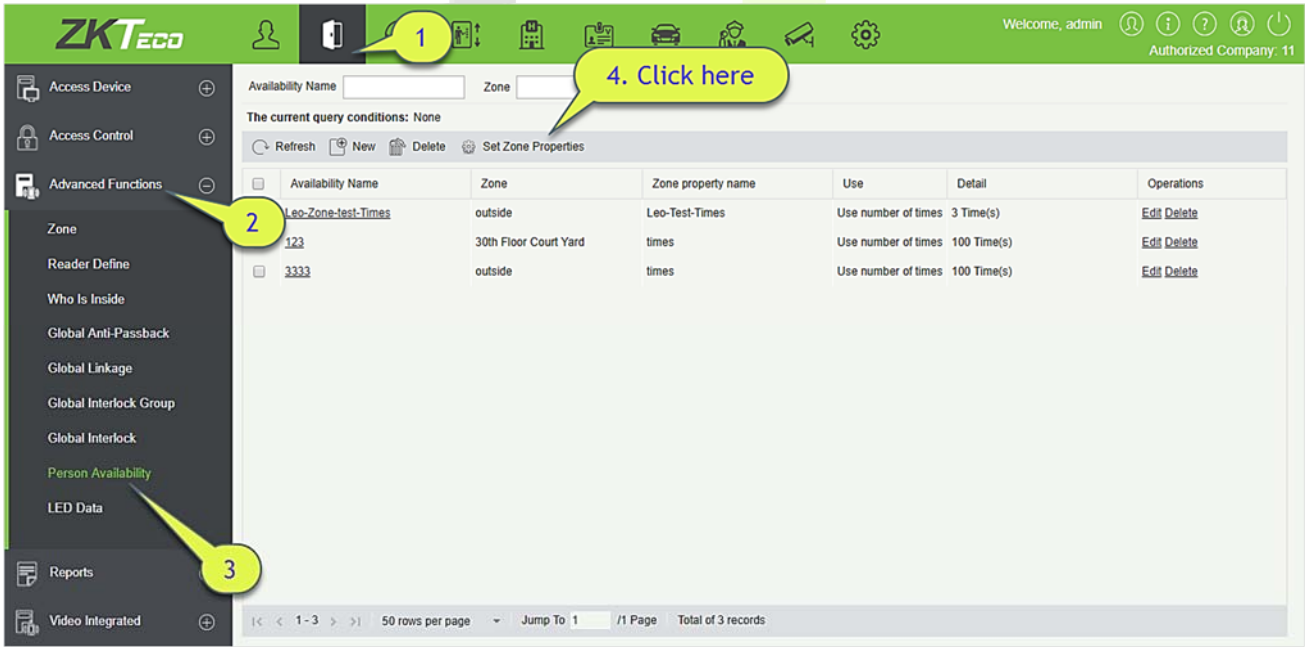
- In the same interlock, all the doors in the group cannot be duplicated.
- If the interlock group exists in the interlock function, it cannot be deleted directly.

4.3.8 Person Availability

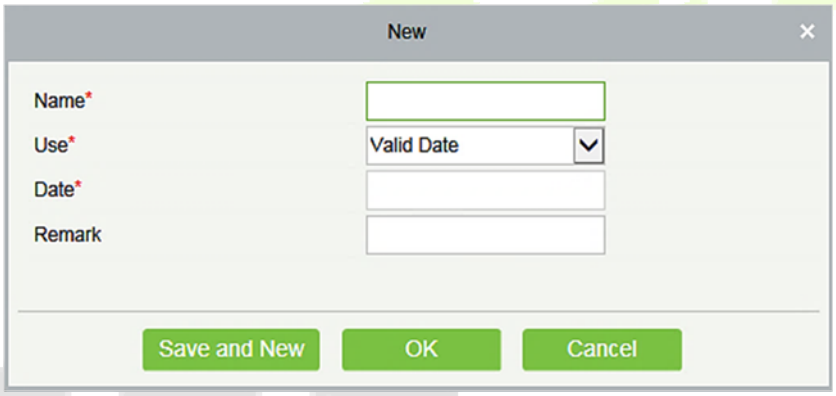
It is mainly used to limit valid date/ after the first use of valid days/ use number of times of personnel in advanced access control area.



- **Set Zone Properties**

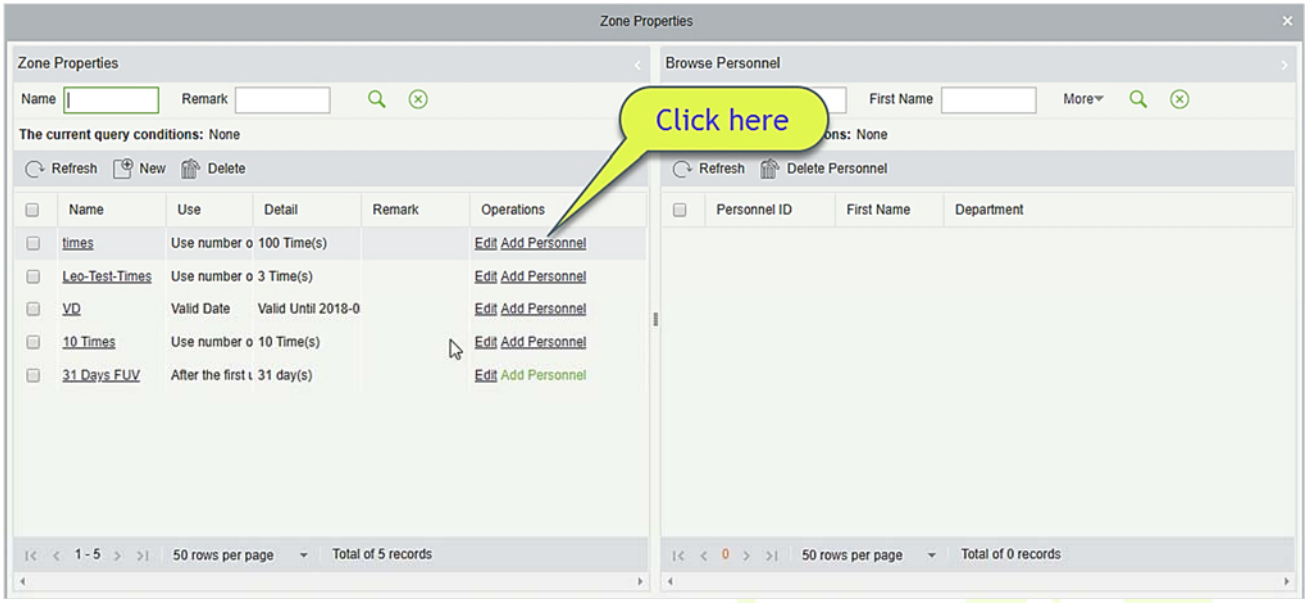


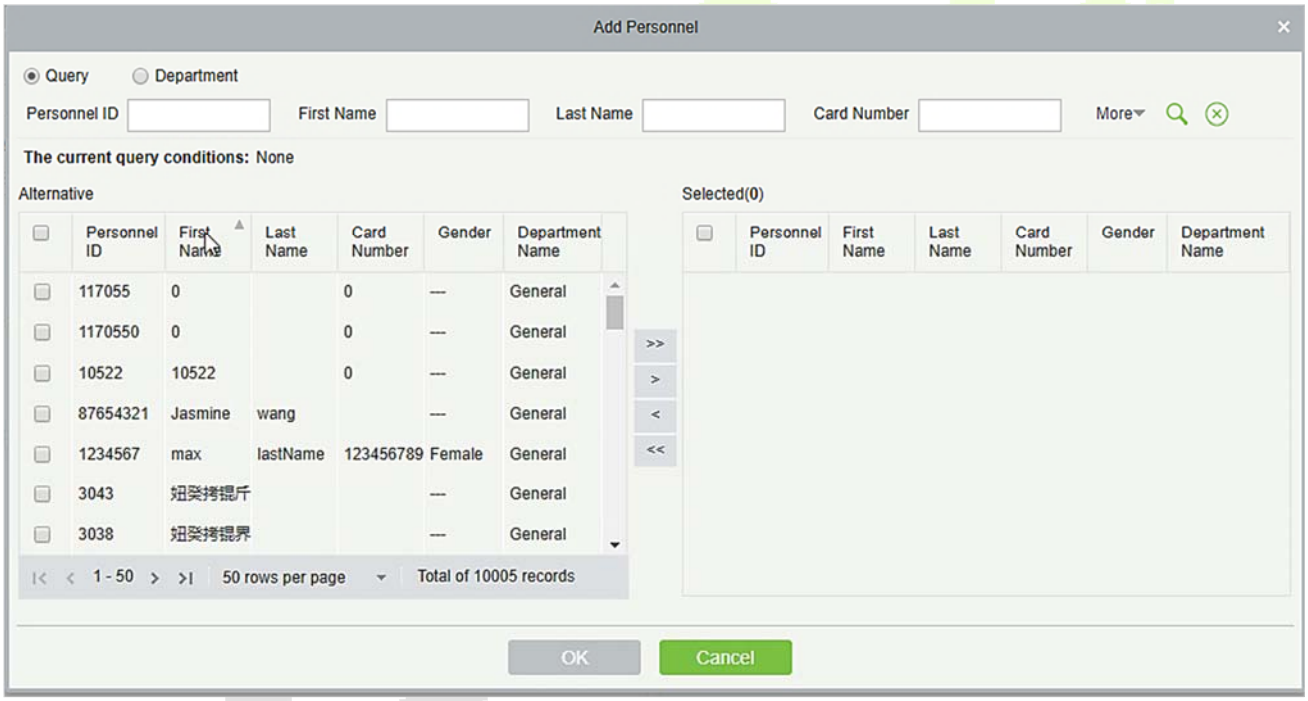
1. Click [**Advanced Functions**] > [**Person Availability**] > [**Set Zone Properties**] > [**New**], the following interface will be shown:



Use: It is divided into Valid Date, after the first use of valid days and Use number of times, corresponding to Date, Days and Times.

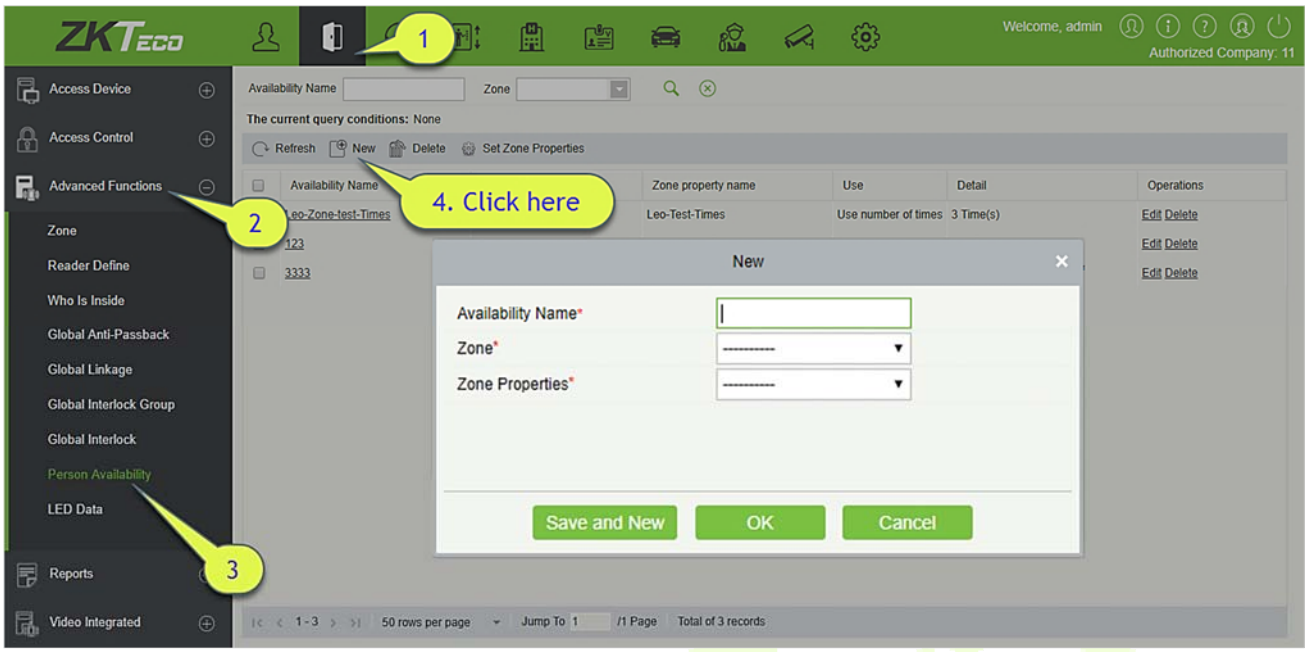
2. Click [**Advanced Functions**] > [**Person Availability**] > [**Set Zone Properties**] > [**Add Personnel**], apply the zone properties to the specified personnel.





New

Click [**Advanced Functions**] > [**Person Availability**] > [**New**], the following interface will be shown:



Select the Zone and Zone Properties to control the person availability.

- **Delete**

Click [**Advanced Functions**] > [**Person Availability**], select an Availability Name, click [**Delete**] > [**OK**] to delete.

4.4 Access Reports

Includes “All transactions”, “Events from Today”, “All Exception Events” and so on. You can export after query.

You can generate statistics of relevant device data from reports, including card verification information, door operation information, and normal punching information, etc.

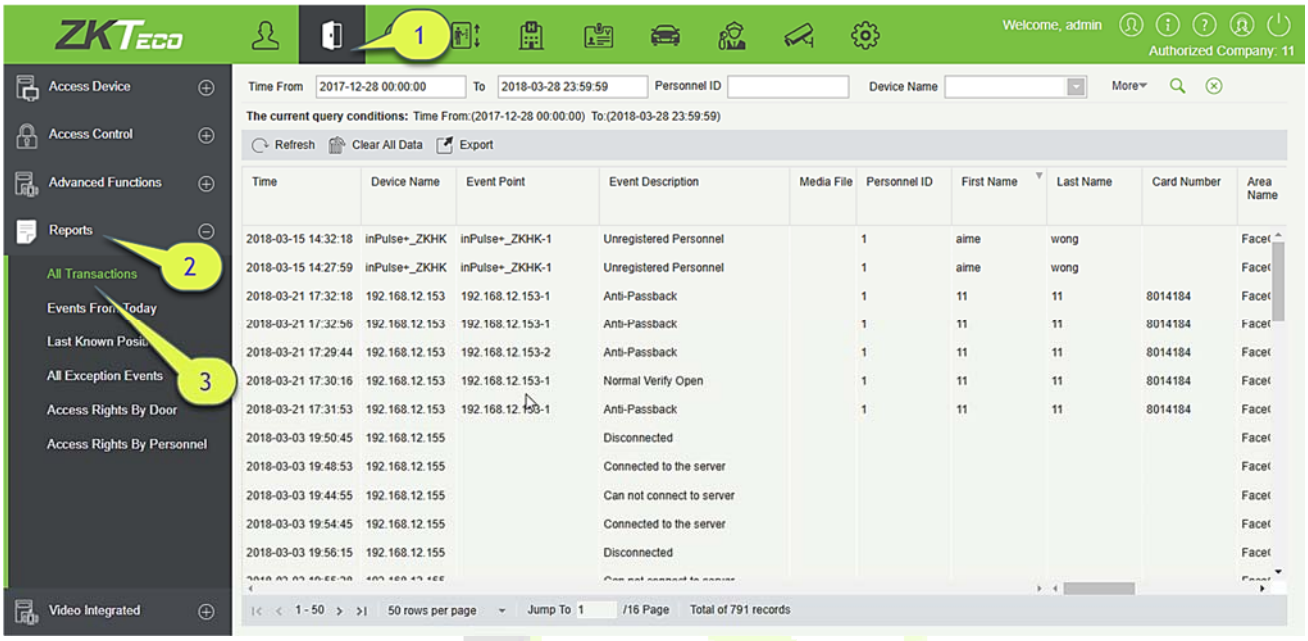
About the Normal and abnormal event please refer to Real-Time Monitoring for details.

Verify mode: Only Card, Only Fingerprint, Only Password, Card plus Password, Card plus Fingerprint, Card or Fingerprint and etc.

✍**Note:** Only event records generated when the user uses emergency password to open doors will include only password verification mode.

4.4.1 All Transactions

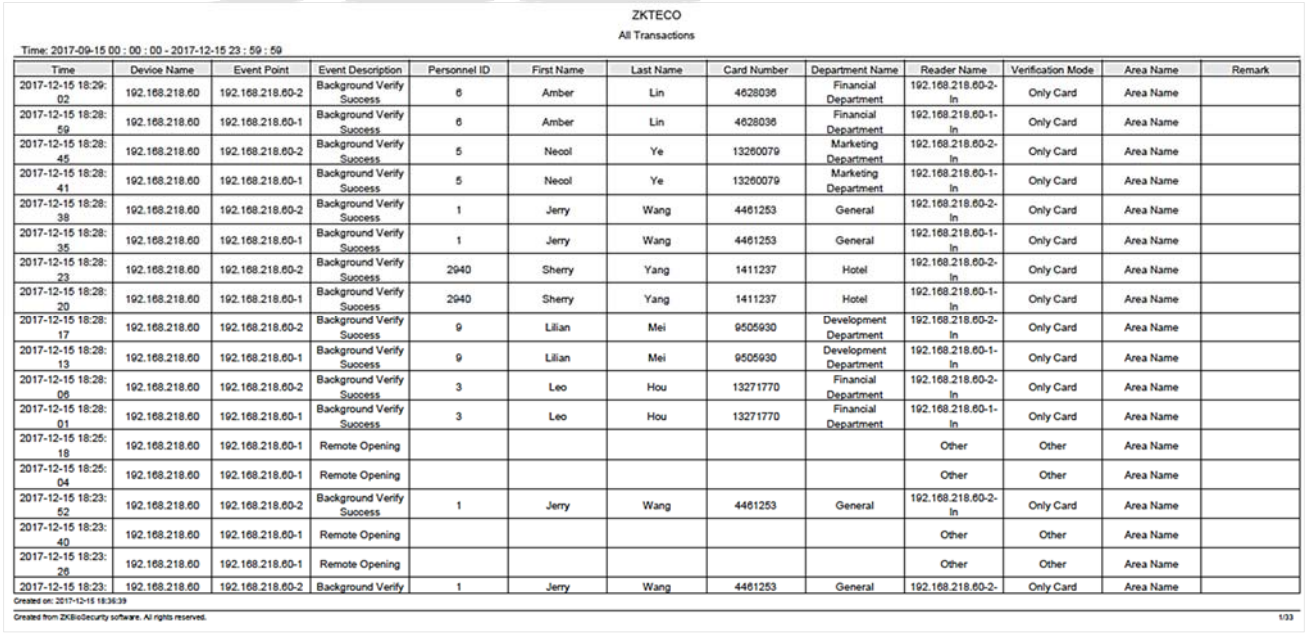
Because the data size of access control event records is large, you can view access control events as specified condition when querying. By default, the system displays latest three months transactions. Click [**Reports**] > [**All Transactions**] to view all transactions:



Media File: You can view or download the photos and videos created in the video system.

Clear All Data: Click [**Clear All Data**] to pop up prompt and click [**OK**] to clear all transactions.

Export: You can export all transactions in Excel, PDF, CSV format.



ZKTECO

All Transactions

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
2017-12-15 18:29:02	192.168.218.60	192.168.218.60-2	Background Verify Success	6	Amber	Lin	4628036	Financial Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:59	192.168.218.60	192.168.218.60-1	Background Verify Success	6	Amber	Lin	4628036	Financial Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:45	192.168.218.60	192.168.218.60-2	Background Verify Success	5	Neool	Ye	13260079	Marketing Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:41	192.168.218.60	192.168.218.60-1	Background Verify Success	5	Neool	Ye	13260079	Marketing Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:38	192.168.218.60	192.168.218.60-2	Background Verify Success	1	Jerry	Wang	4461253	General	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:35	192.168.218.60	192.168.218.60-1	Background Verify Success	1	Jerry	Wang	4461253	General	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:23	192.168.218.60	192.168.218.60-2	Background Verify Success	2940	Sherry	Yang	1411237	Hotel	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:20	192.168.218.60	192.168.218.60-1	Background Verify Success	2940	Sherry	Yang	1411237	Hotel	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:17	192.168.218.60	192.168.218.60-2	Background Verify Success	9	Lilian	Mei	9505930	Development Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:13	192.168.218.60	192.168.218.60-1	Background Verify Success	9	Lilian	Mei	9505930	Development Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:06	192.168.218.60	192.168.218.60-2	Background Verify Success	3	Leo	Hou	13271770	Financial Department	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:01	192.168.218.60	192.168.218.60-1	Background Verify Success	3	Leo	Hou	13271770	Financial Department	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:25:18	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:25:04	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:52	192.168.218.60	192.168.218.60-2	Background Verify Success	1	Jerry	Wang	4461253	General	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:40	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:26	192.168.218.60	192.168.218.60-1	Remote Opening						Other	Other	Area Name	
2017-12-15 18:23:	192.168.218.60	192.168.218.60-2	Background Verify	1	Jerry	Wang	4461253	General	192.168.218.60-2-	Only Card	Area Name	

Created on: 2017-12-15 18:36:39

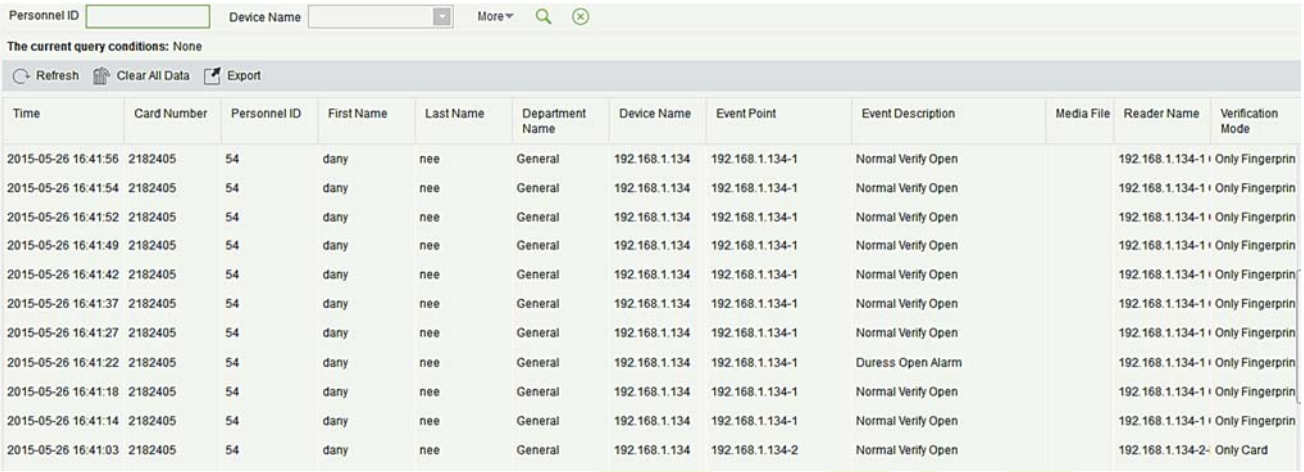
Created from ZKBioSecurity software. All rights reserved.

1/33

4.4.2 Events from Today

Check out the system record today.

Click [**Reports**] > [**Events from Today**] to view today's records. You can export all events from today in Excel, PDF, CSV format.



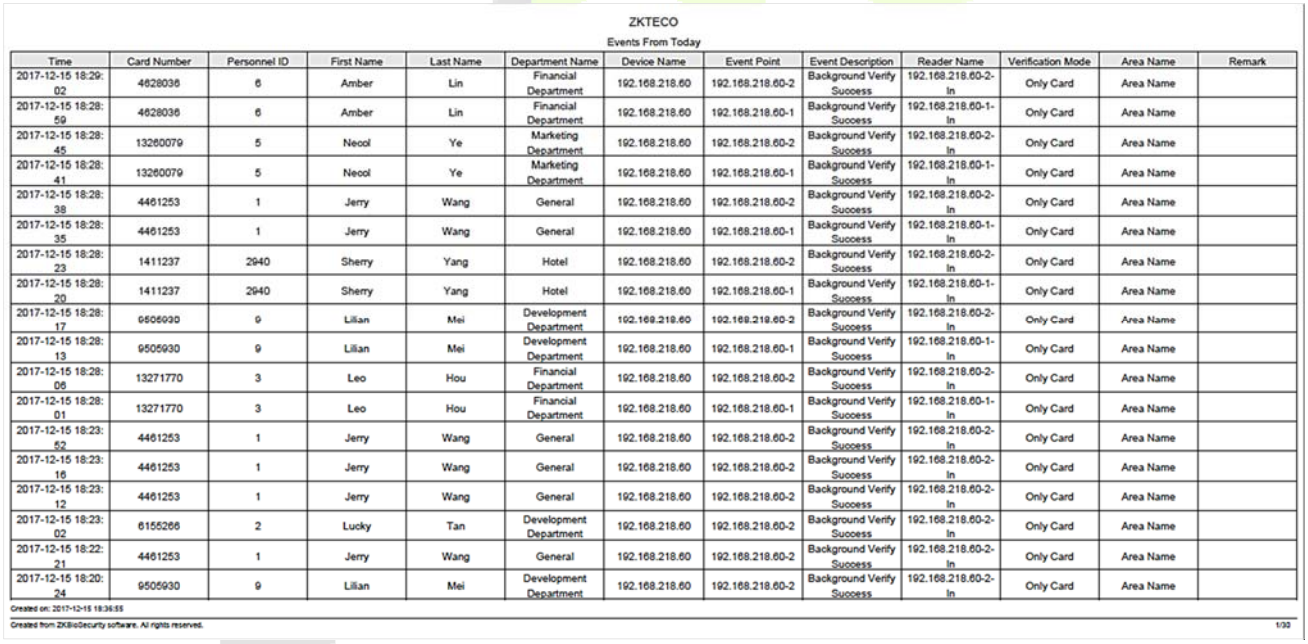
Personnel ID | Device Name | More

The current query conditions: None

Refresh | Clear All Data | Export

Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Media File	Reader Name	Verification Mode
2015-05-26 16:41:56	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:54	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:52	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:49	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:42	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:37	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:27	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:22	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Duress Open Alarm		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:18	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:14	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-1	Normal Verify Open		192.168.1.134-1	Only Fingerprin
2015-05-26 16:41:03	2182405	54	dany	nee	General	192.168.1.134	192.168.1.134-2	Normal Verify Open		192.168.1.134-2	Only Card

You can export all events from today in Excel, PDF, CSV format.



ZKTECO

Events From Today

Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name	Remark
2017-12-15 18:29:02	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:59	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:45	13260079	5	Necol	Ye	Marketing Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:41	13260079	5	Necol	Ye	Marketing Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:38	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:35	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:23	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:20	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:17	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:13	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:06	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:01	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:23:52	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:16	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:12	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:02	6155266	2	Lucky	Tan	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:22:21	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:20:24	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	

Created on: 2017-12-15 18:36:55

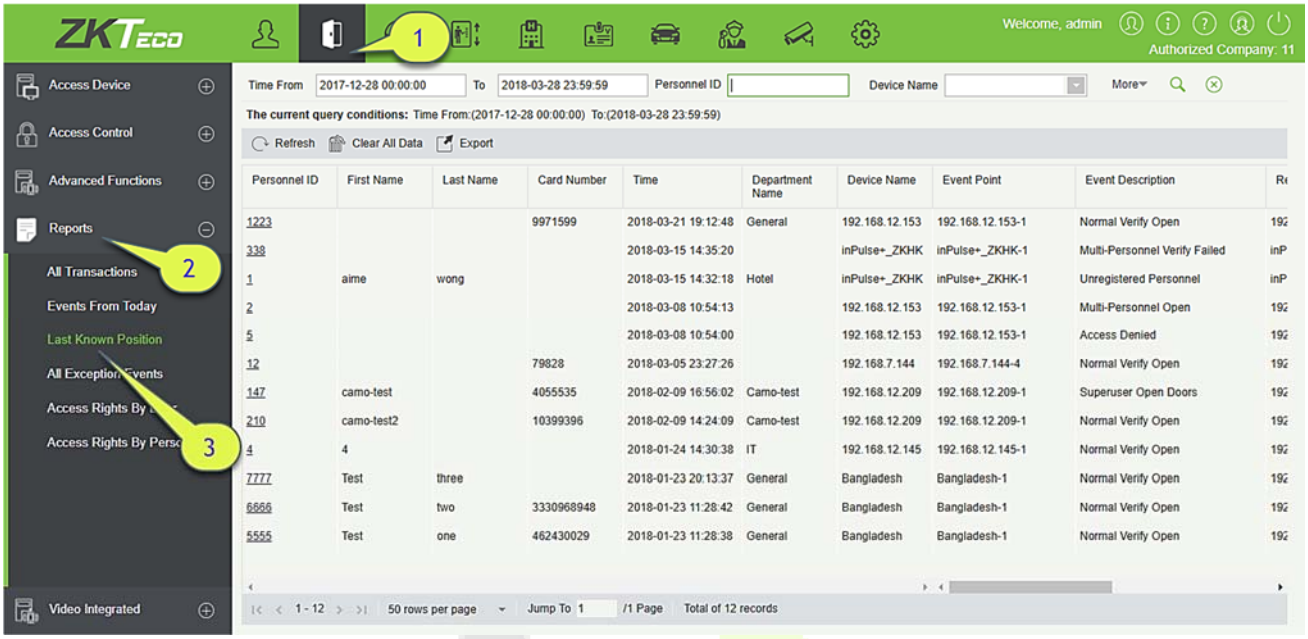
Created from ZKBioSecurity software. All rights reserved.

1/30

4.4.3 Last Known Position

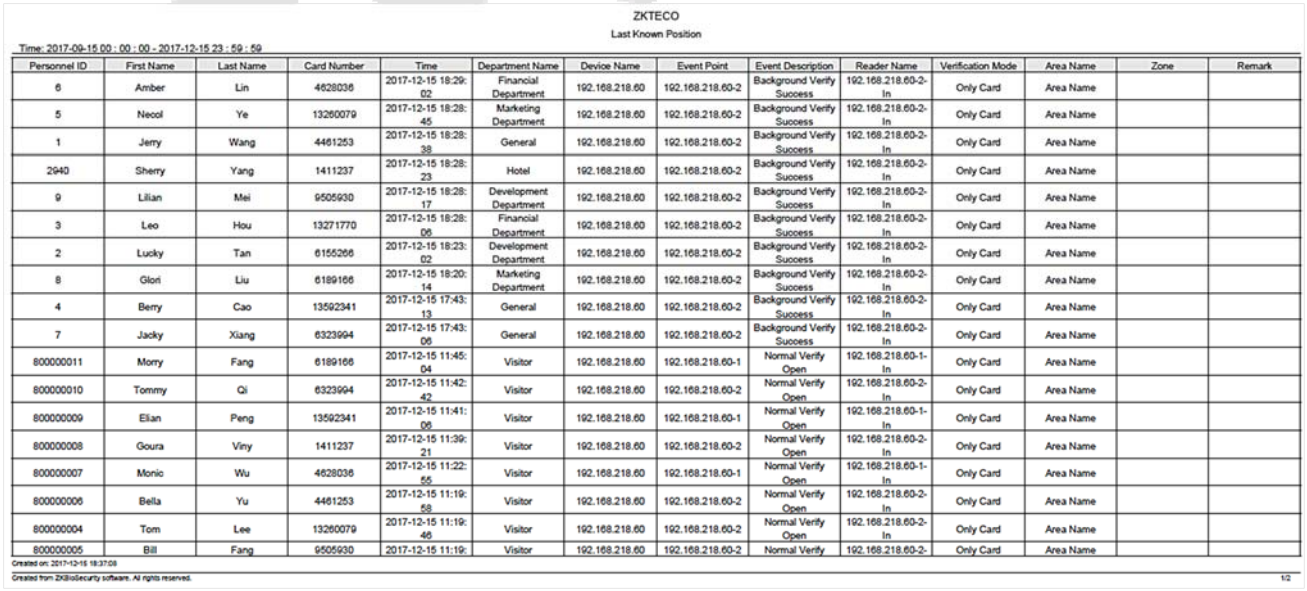
Check out the final position of personnel who has access privileges to access. It is convenient to locate a person.

Click [**Reports**] > [**Last Know Position**] to check out.



Locate the location of personnel: Personnel with electronic map authority, click on the corresponding [**Personnel ID**], you can locate the specific location of the personnel in the electronic map by the way of flashing the door.

You can export all personnel final position data in Excel, PDF, CSV format.



ZKTECO

Last Known Position

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Personnel ID	First Name	Last Name	Card Number	Time	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name	Zone	Remark
6	Amber	Lin	4628036	2017-12-15 18:29:02	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
5	Neool	Ye	13260079	2017-12-15 18:28:45	Marketing Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
1	Jerry	Wang	4461253	2017-12-15 18:28:38	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
2940	Sherry	Yang	1411237	2017-12-15 18:28:23	Hotel	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
9	Lilian	Mei	9505930	2017-12-15 18:28:17	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
3	Leo	Hou	13271770	2017-12-15 18:28:06	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
2	Lucky	Tan	6155266	2017-12-15 18:23:02	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
8	Glori	Liu	6189166	2017-12-15 18:20:14	Marketing Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
4	Berry	Cao	13592341	2017-12-15 17:43:13	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
7	Jacky	Xiang	6323994	2017-12-15 17:43:06	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name		
800000011	Morry	Fang	6189166	2017-12-15 11:45:04	Visitor	192.168.218.60	192.168.218.60-1	Normal Verify Open	192.168.218.60-1-In	Only Card	Area Name		
800000010	Tommy	Qi	6323994	2017-12-15 11:42:42	Visitor	192.168.218.60	192.168.218.60-2	Normal Verify Open	192.168.218.60-2-In	Only Card	Area Name		
800000009	Elian	Peng	13592341	2017-12-15 11:41:06	Visitor	192.168.218.60	192.168.218.60-1	Normal Verify Open	192.168.218.60-1-In	Only Card	Area Name		
800000008	Goura	Viny	1411237	2017-12-15 11:39:21	Visitor	192.168.218.60	192.168.218.60-2	Normal Verify Open	192.168.218.60-2-In	Only Card	Area Name		
800000007	Monic	Wu	4628036	2017-12-15 11:22:55	Visitor	192.168.218.60	192.168.218.60-1	Normal Verify Open	192.168.218.60-1-In	Only Card	Area Name		
800000006	Bella	Yu	4461253	2017-12-15 11:19:58	Visitor	192.168.218.60	192.168.218.60-2	Normal Verify Open	192.168.218.60-2-In	Only Card	Area Name		
800000004	Tom	Lee	13260079	2017-12-15 11:19:46	Visitor	192.168.218.60	192.168.218.60-2	Normal Verify Open	192.168.218.60-2-In	Only Card	Area Name		
800000005	Bill	Fang	9505930	2017-12-15 11:19:	Visitor	192.168.218.60	192.168.218.60-2	Normal Verify	192.168.218.60-2-	Only Card	Area Name		

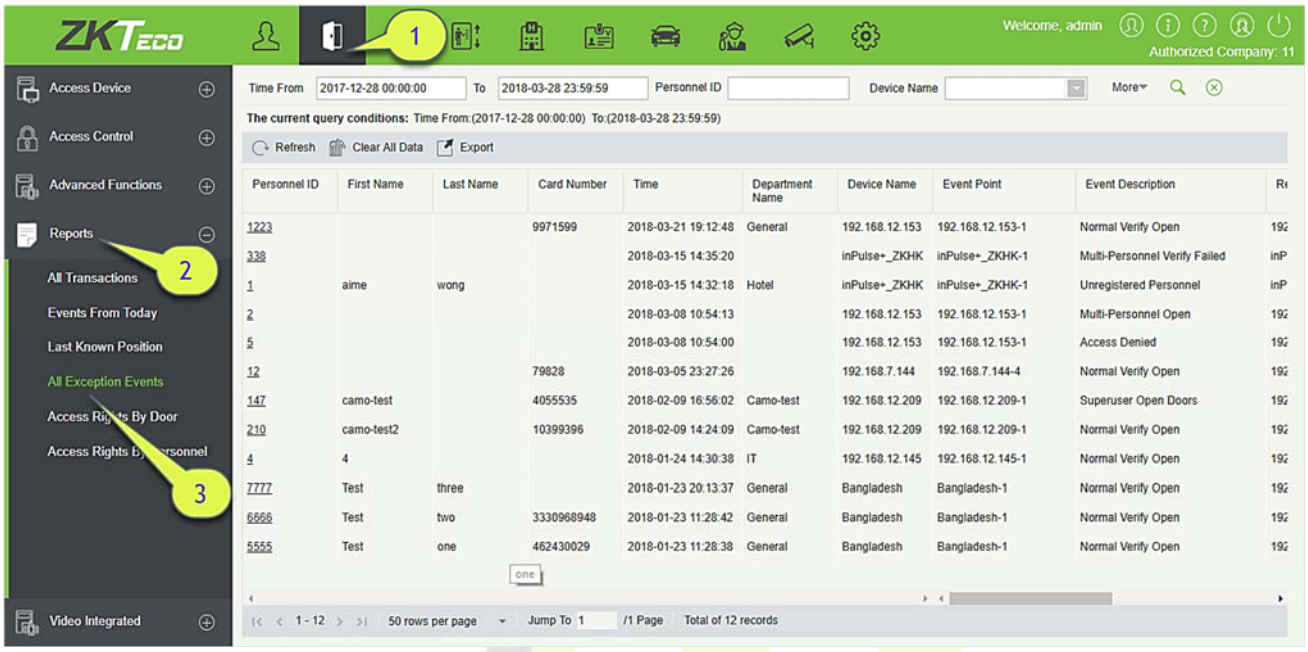
Created on: 2017-12-15 18:37:08

Created from ZKBioSecurity software. All rights reserved.

1/2

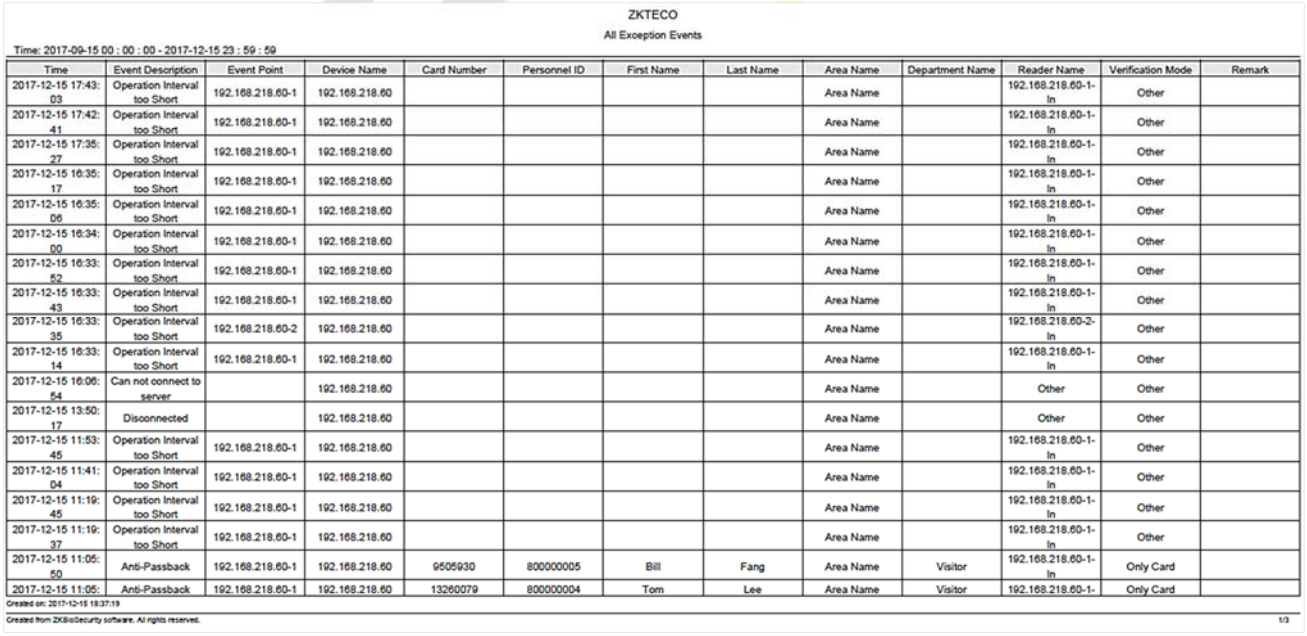
4.4.4 All Exception Events

Click [**Reports**] > [**All Exception Events**] to view exception events in specified condition. The options are same as those of [**All Transactions**].



Clear All Data: Click [**Clear All Data**] to pop up prompt, and then click [**OK**] to clear all exception events.

Export: You can export all exception events in Excel, PDF, CSV format.



ZKTECO

All Exception Events

Time: 2017-09-15 00 : 00 : 00 - 2017-12-15 23 : 59 : 59

Time	Event Description	Event Point	Device Name	Card Number	Personnel ID	First Name	Last Name	Area Name	Department Name	Reader Name	Verification Mode	Remark
2017-12-15 17:43:03	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 17:42:41	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 17:35:27	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:35:17	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:35:06	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:34:00	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:52	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:43	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:33:35	Operation Interval too Short	192.168.218.60-2	192.168.218.60					Area Name		192.168.218.60-2-In	Other	
2017-12-15 16:33:14	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 16:06:54	Can not connect to server		192.168.218.60					Area Name		Other	Other	
2017-12-15 13:50:17	Disconnected		192.168.218.60					Area Name		Other	Other	
2017-12-15 11:53:45	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:41:04	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:19:45	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:19:37	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1-In	Other	
2017-12-15 11:05:50	Anti-Passback	192.168.218.60-1	192.168.218.60	9505930	800000005	Bill	Fang	Area Name	Visitor	192.168.218.60-1-In	Only Card	
2017-12-15 11:05:	Anti-Passback	192.168.218.60-1	192.168.218.60	13260079	800000004	Tom	Lee	Area Name	Visitor	192.168.218.60-1-	Only Card	

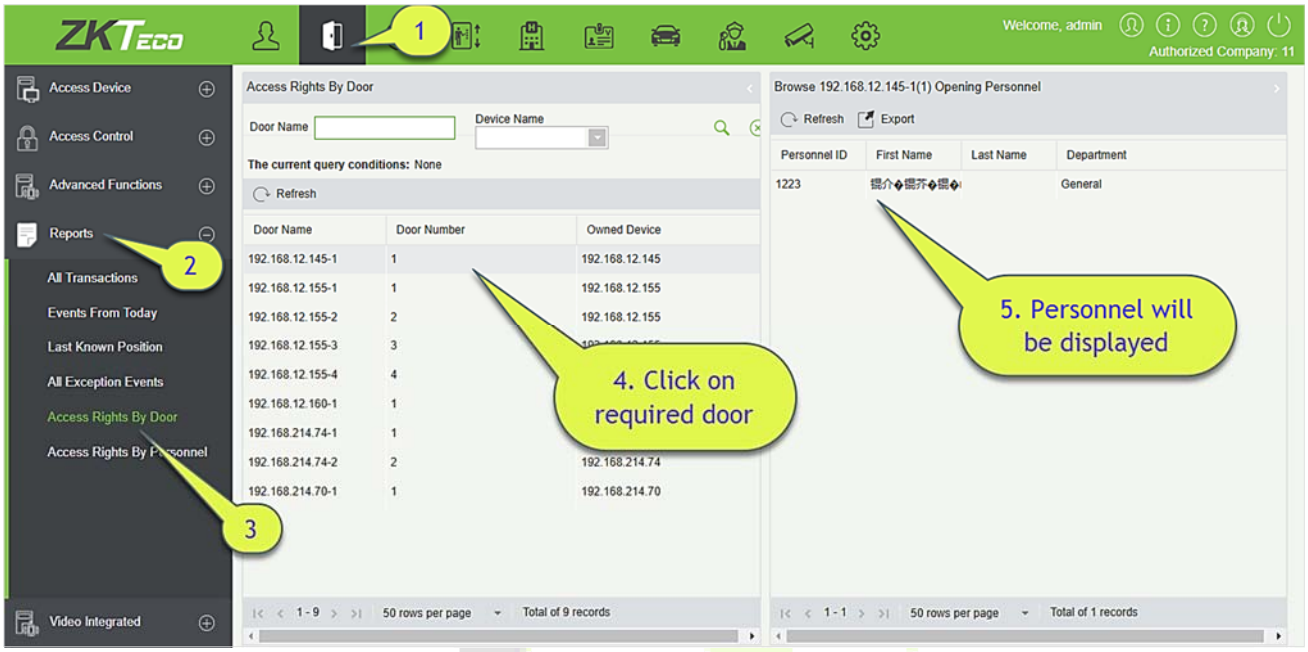
Created on: 2017-12-15 18:37:19

Created from ZKBioSecurity software. All rights reserved.

1/3

4.4.5 Access Rights by Door

View related access levels by door. Click [**Reports**] > [**Access Rights By Door**], the data list in the left side shows all doors in the system, select a door, the personnel having access levels to the door will be displayed on the right data list.



You can export all the personnel having access levels to the door data in Excel, PDF, CSV format.

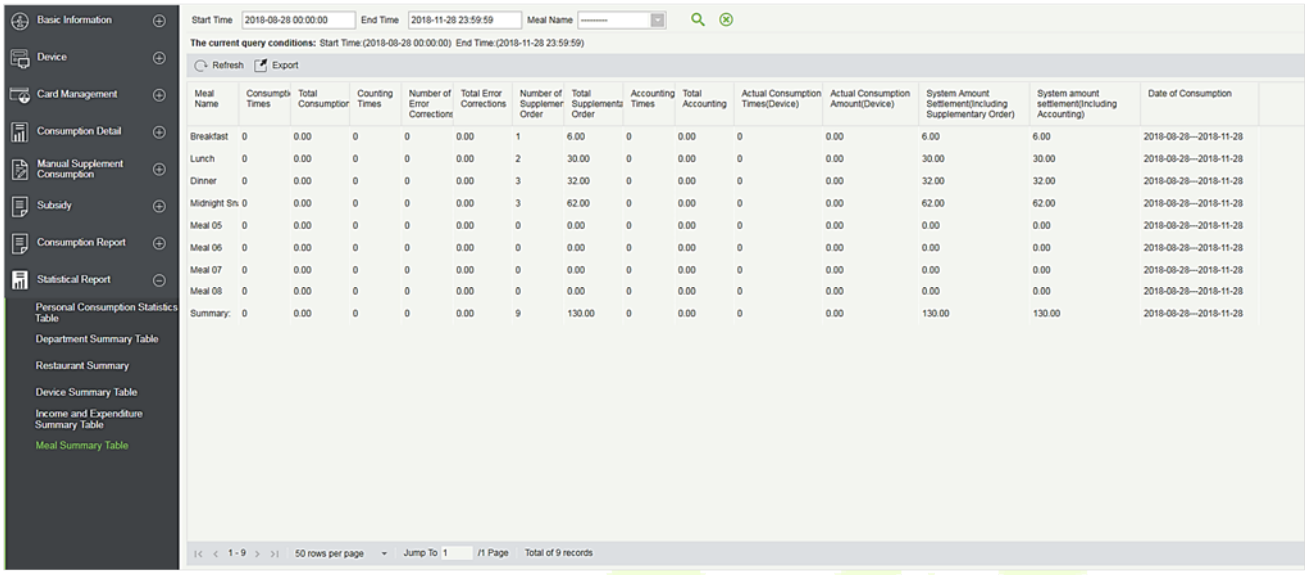
ZKTECO

192.168.218.60-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
4	Berry	Cao	General
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
7	Jacky	Xiang	General
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department

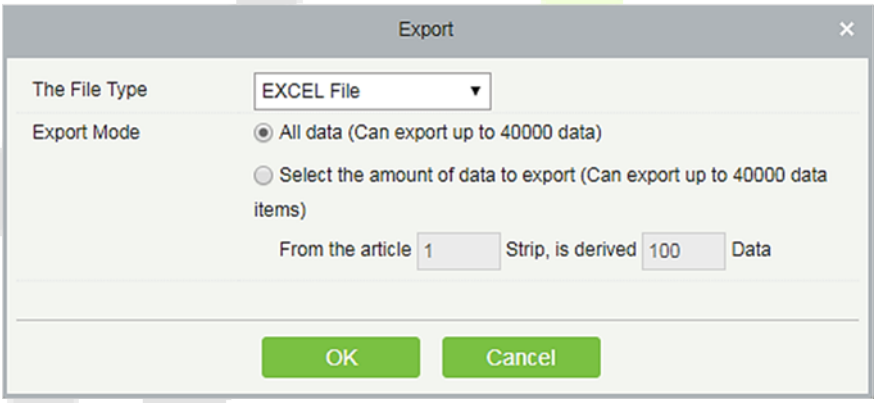
6.8.6 Meal Summary Table

Click **[Statistical Report]** > **[Meal Summary Table]**, as shown below:



- **Export**

Click the **[Export]** button at the top of the list to open an export dialog box, as shown below. Click **[OK]** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

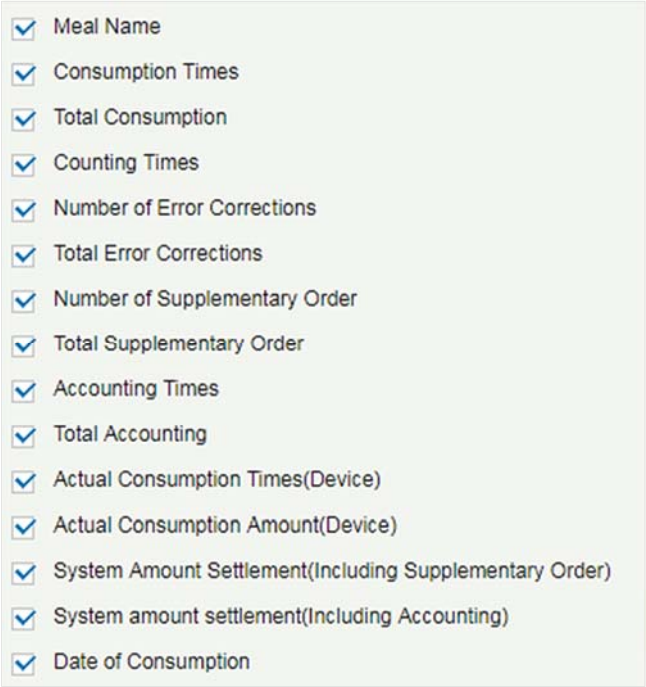


- **Refresh**

Click **[Refresh]** to load the latest meal summary table data.

✍**Note:** If there is more data in the page meal summary table, you can also enter the device name, name, and consumption time in the search field, and click [🔍] to search for it.

The data statistics column includes:



The following is the calculation formula of the specific column.

Consumption times = Total number of count the particular type is consumed.

Total consumption = Total amount of money consumed for the particular type.

Counting times = Total number of times the type is counted.

Number of error corrections = Total number of error correction for the particular type name.

Total error correction = Total amount of error correction for the particular type name.

Times of supplementary order = Total count of supplementary order for the particular type.

Total supplementary order = Total amount of supplementary order for the particular type.

Accounting times = Total count of billing for the particular type.

Total Accounting = Total amount of money billed for the particular type.

Actual Consumption Times (device) = [Consumption times - Number of error corrections].

Actual Consumption Amount (device) = [Total Consumption - Total Error Correction].

System Amount Settlement (including supplementary order) = [Total Consumption - (Total Error Correction + Total Supplementary Order)].

System Amount Settlement (including billing) = [Total Consumption - (Total Error Correction + Total Supplementary Order + Total Accounting)].

7 Elevator

The following is the manual of online elevator control. If you are using offline elevator control, please refer to Offline Elevator Control Manual.

The Elevator Control System is mainly used to set device parameters (such as the swiping interval for taking elevators and elevator key drive duration), manage personnel's rights to floors and elevator control time, and supervise elevator control events. You can set registered users' rights to floors. Only authorized users can reach certain floors within a period of time after being authenticated.

7.1 Elevator Device

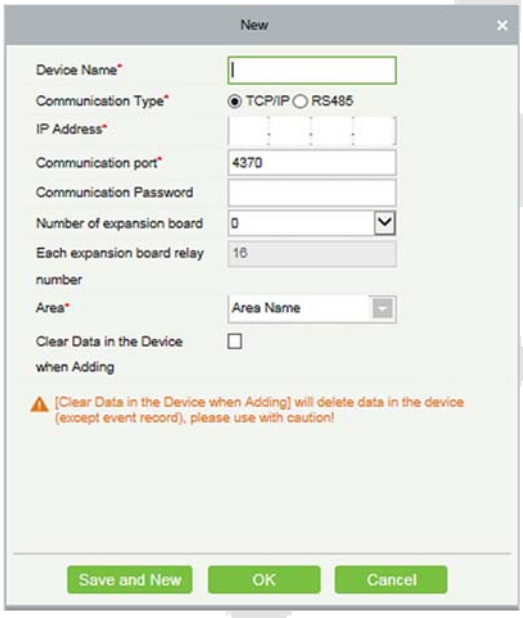
7.1.1 Device

There are two ways to add Elevator Devices.

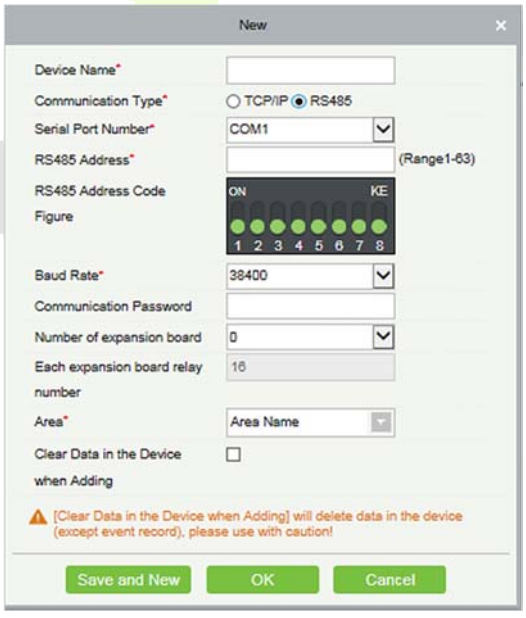
- **Add Device manually**

1. Click [**Elevator Device**] > [**Device**] > [**New**] on the Action Menu, the following interface will be shown:

TCP/ IP communication mode



RS485 communication mode



IP Address: Enter the IP Address of the elevator device.

Communication port: The default is 4370.

Serial Port No.: COM1~COM254.

RS485 Address: The machine number, range 1-255. When Serial Port No. is same, it is not allowed to set repeated RS485 addresses.

Baud Rate: Same as the baud rate of the device. The default is 38400.

RS485 Address Code Figure: Display the code figure of RS485 address.

Common options:

Device Name: Any character, up to a combination of 20 characters.

Communication Password: The max length is 6 with numbers or letters. The initialized device's communication password is blank.

✍**Note:** You do not need to input this field if it is a new factory device or just after the initialization.

Number of expansion board: The expansion board number of elevator device controlling.

Each expansion board relay number: Each expansion board has 16 relays.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-Time Monitoring.

Clear Data in the Device when Adding: Tick this option, after adding device, the system will clear all data in the device (except the event logs). If you add the device just for demonstration or testing, there is no need to tick it.

Extended Device Parameters: Includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity etc.

2. After editing, click [**OK**], and the system will start to connect the current device.

If successfully connected, it will read the corresponding extended parameters of the device and save.

✍**Note:** When deleting a new device, the software will clear all user information, time zones, holidays, and elevator access levels settings from the device, except the events record (unless the information in the device is unusable, or it is recommended not to delete the device in used to avoid loss of information).

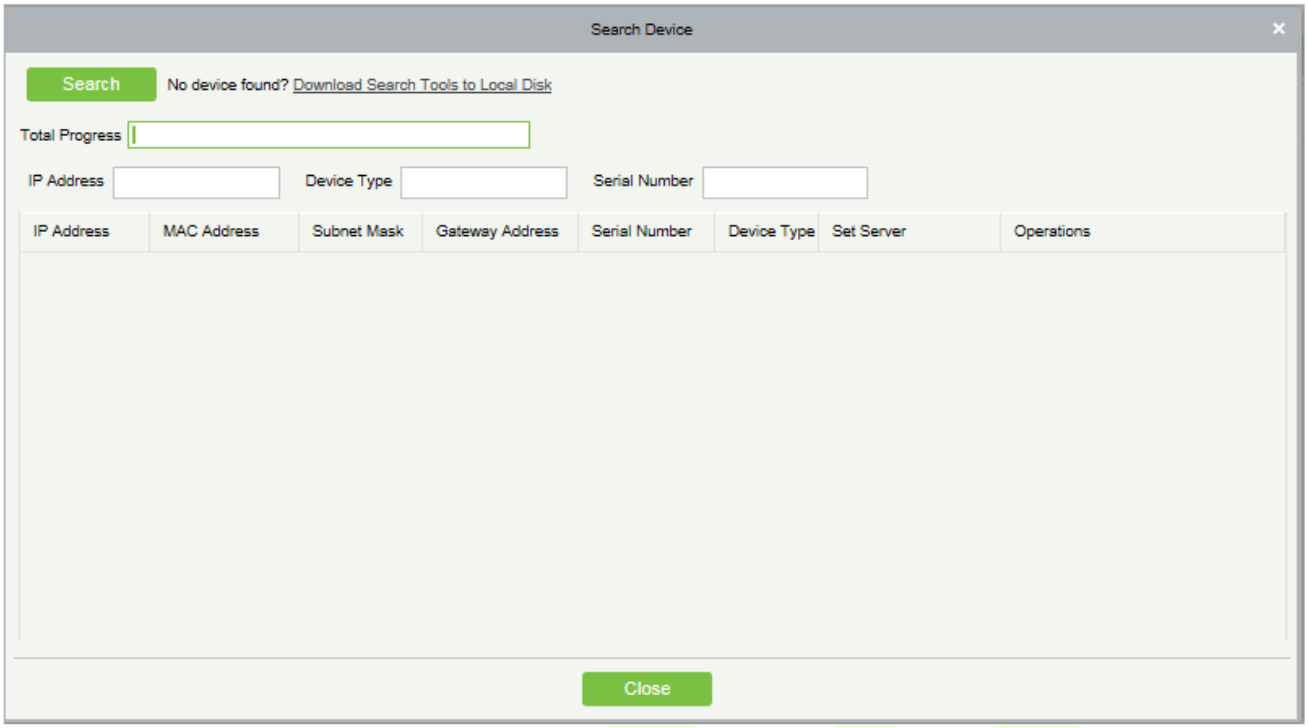
Elevator Controller Settings:

- TCP/ IP Communication Requirements
- Support and enable TCP/ IP communication, directly connect device to the PC or connect to the local network, query IP address and other information of the device;
- RS485 Communication Requirements
- Support and enable RS485 communication, connect device to PC by RS485, query the serial port number, RS485 machine number, baud rate and other information of the device.

- **Add Device by Searching Elevator Controllers**

Search the elevator device in the Ethernet.

1) Click [**Elevator Device**] > [**Device**] > [**Search Device**], to show the Search interface.
2) Click [**Search**], and it will prompt [searching……].
3) After searching, the list and total number of elevator devices will be displayed.



✍**Note:** Here we use UDP broadcast mode to search elevator devices, this mode cannot perform cross-Router function. IP address can be cross-net segment, but must belong to the same subnet, and needs to be configured the gateway and IP address in the same net segment.

4) Click [**Add Device**] behind the device, and a dialog box will pop up. Enter self-defined device name, and click [**OK**] to complete device adding.

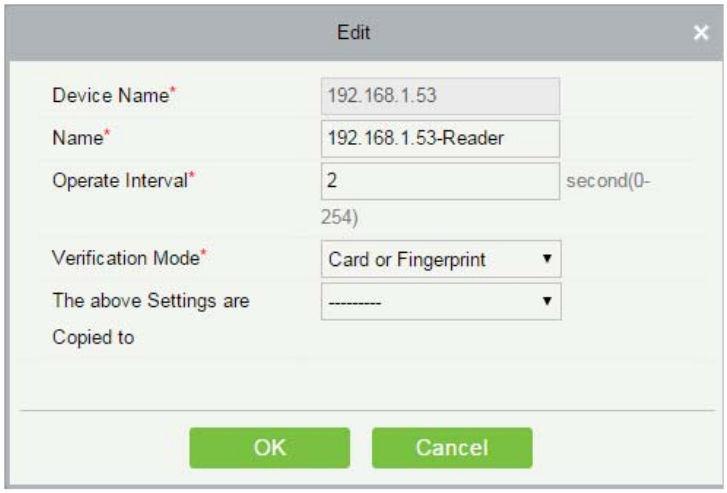
5) The default IP address of the elevator device may conflict with the IP of a device on the Local network. You can modify its IP address: Click [**Modify IP Address**] behind the device and a dialog box will open. Enter the new IP address and other parameters (**Note:** Configure the gateway and IP address in the same net segment).

✍**Note:** The system cannot add Elevator Devices automatically.

7.1.2 Reader

Each elevator device has a reader, the reader information can be set.

Click **[Elevator Device]** > **[Reader]**, select a reader name in the reader list:



Fields are as follows:

Device Name: It is not editable.

Name: The default format is "Device Name - Reader", it is editable within 30 characters.

Operate Interval: The interval between two verifications. The default value is 2 seconds, the range is 0~254 seconds.

Verification Mode: The default setting is "Card or Fingerprint". The Wiegand reader supports "Only Card", "Only Password", "Card or Password", "Card and Password", "Card or Fingerprint". The RS485 reader supports "Card or Fingerprint". Make sure the reader has a keyboard when the verification mode is "Card and Password".

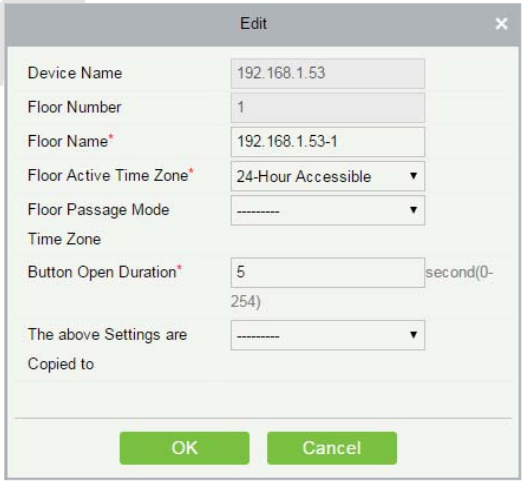
The above Settings are Copied to:

All Readers of All Devices: Apply the above settings to all readers within the current user's level.

Click [**OK**] to save and exit.

7.1.3 Floor

Click **[Elevator Device]** > **[Floor]**, select a floor name in the list to click **[Edit]**:



Fields are as follows:

Device Name: It is not editable.

Floor Number: The system automatically numbered according to the number of relays.

Floor Name: The default setting is "Device Name- Floor Number"; it is editable within 30 characters.

Floor Active Time Zone, Floor Passage Mode Time Zone: The default setting is Null. The Floor Active Time Zones that are initialized or newly added by users will be displayed here so that users can select a period. When editing a floor, the Floor Active Time Zone must be specified. The key for closing the related floor can be released continuously only after the effective periods of this floor are specified. Floor Passage Mode Time Zone takes effect only within the floor effective period. It is recommended that the floor continuous release period be included in the floor effective period.

Button Open Duration: It is used to control the time period to press floor button after verification. The default value is 5 seconds; the range is 0~254 seconds.

The above Settings are Copied to: Including below two options.

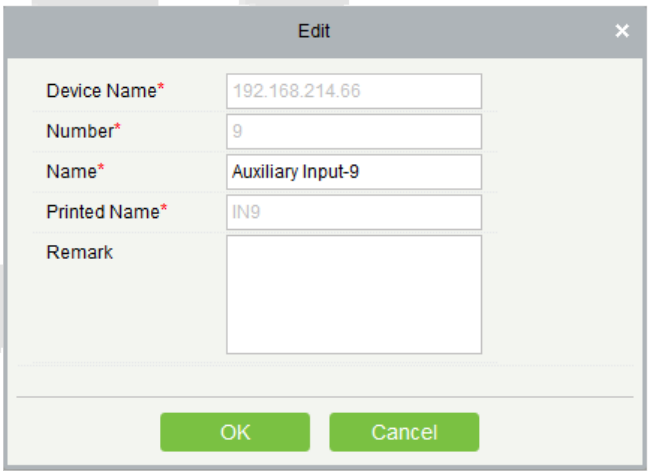
- All Floors of Current Device: To apply the above settings to all floors of the current elevator device.
- All floors of all Devices: To apply the above settings to all floors within the current user's level.

7.1.4 Auxiliary Input

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

Click [**Elevator Device**] > [**Auxiliary Input**] on the Action Menu, enter into the following page:

Click [**Edit**] to modify the parameters:



Fields are as follows:

Name: You can customize the name according to your preference.

Printed Name: The printing name in the hardware, for example IN9.

Click [**Edit**] to modify the name and remark. Others are not allowed to edit here.

7.1.5 Event Type

Display the event types of the elevator devices. Click [**Elevator Device**] > [**Event**], the following page is displayed:

Refresh

Event Name	Event No.	Event Level	Device Name	Serial No.
Normal Punch Open	0	Normal	192.168.90.235	0013130700074
Punch during Passage Mode Time Zone	1	Normal	192.168.90.235	0013130700074
Open during Passage Mode Time Zone	5	Normal	192.168.90.235	0013130700074
Remote Release	8	Normal	192.168.90.235	0013130700074
Remote Locking	9	Normal	192.168.90.235	0013130700074
Disable Intraday Passage Mode Time Zone	10	Normal	192.168.90.235	0013130700074
Enable Intraday Passage Mode Time Zone	11	Normal	192.168.90.235	0013130700074
Normal Fingerprint Open	14	Normal	192.168.90.235	0013130700074
Press Fingerprint during Passage Mode Time Zc	16	Normal	192.168.90.235	0013130700074
Operate Interval too Short	20	Exception	192.168.90.235	0013130700074
Button Inactive Time Zone(Punch Card)	21	Exception	192.168.90.235	0013130700074
Illegal Time Zone	22	Exception	192.168.90.235	0013130700074
Access Denied	23	Exception	192.168.90.235	0013130700074
Disabled Card	27	Exception	192.168.90.235	0013130700074
Card Expired	29	Exception	192.168.90.235	0013130700074
Password Error	30	Exception	192.168.90.235	0013130700074
Press Fingerprint Interval too Short	31	Exception	192.168.90.235	0013130700074

More details about Event Type, please refer to Elevator Event Type.

7.1.6 Device Monitoring

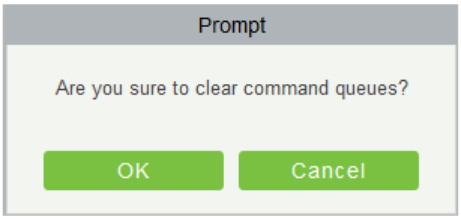
By default, it monitors all devices within the current user's level, click **[Elevator Device]** > **[Device Monitoring]**, and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, and Related Operation.

Area Status --------- Device Name Serial Number

Export

Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State	Operations
192.168.214.66	0013130700074	Area Nameaa	Get real-time event	Normal	0	None	Clear Command View Command

You can clear command as required. Click [**Clear Command**] behind the corresponding device:



Click [**OK**] to clear.

✍Notes:

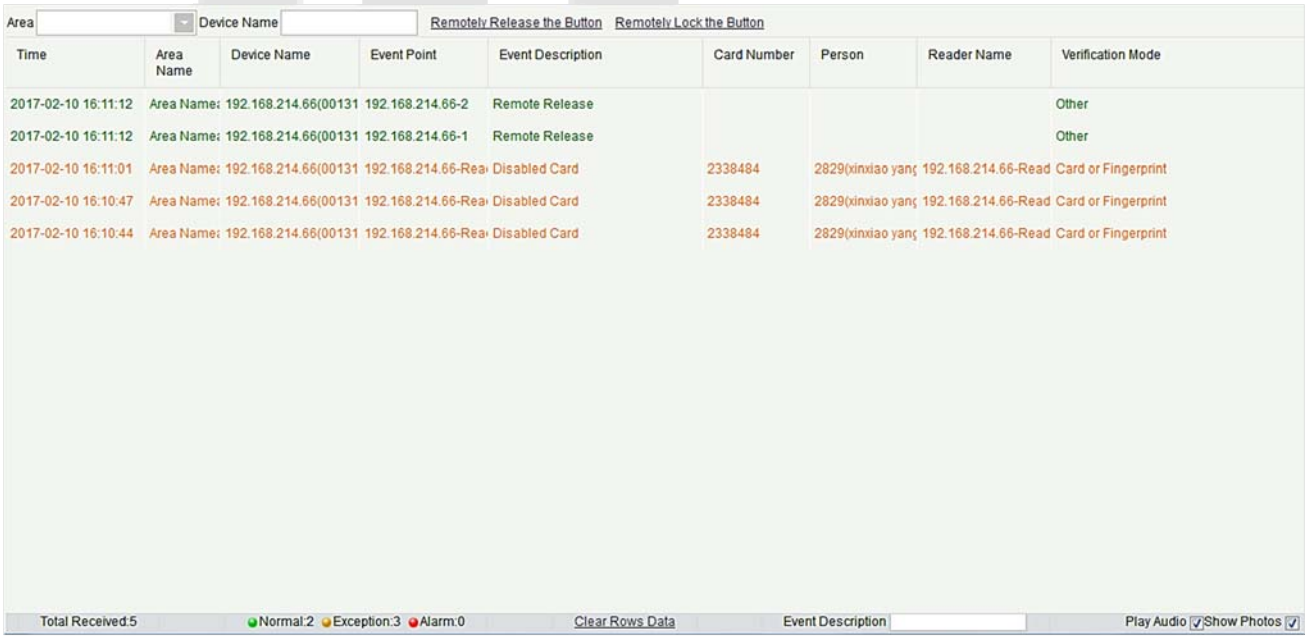
1) After the Clear Command is executed, you can perform the Synchronize All Data to Devices operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you can replace the current device with a large-capacity one, or delete the right of some personnel to access this device, and then perform the Synchronize All Data to Devices operation.

2) Operate State is the content of communications equipment of current device, mainly used for debugging.

3) The number of commands to be performed is greater than 0, indicating that data is not synchronized to the device, just wait.

7.1.7 Real-Time Monitoring

Click [**Elevator Device**] > [**Real-Time Monitoring**], real-time monitor the status and real-time events of elevator controllers in the system, including normal events and abnormal events (including alarm events). Real-Time Monitoring interface is shown as follows:



1. Event Monitoring

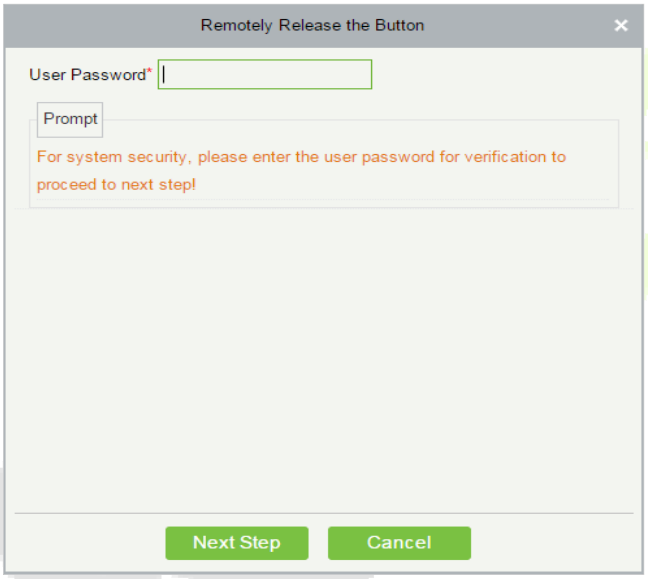
System automatically acquires monitored device event records (by default, display 200 records), including normal and abnormal elevator control events (including alarm events). Normal events appear in green, alarm events appear in red, other abnormal events appear in orange.

Monitor Area: All floors with elevator controller in the system is monitored by default, you can target to monitor one or more floors by Area, Status, Device Name and Serial NO.

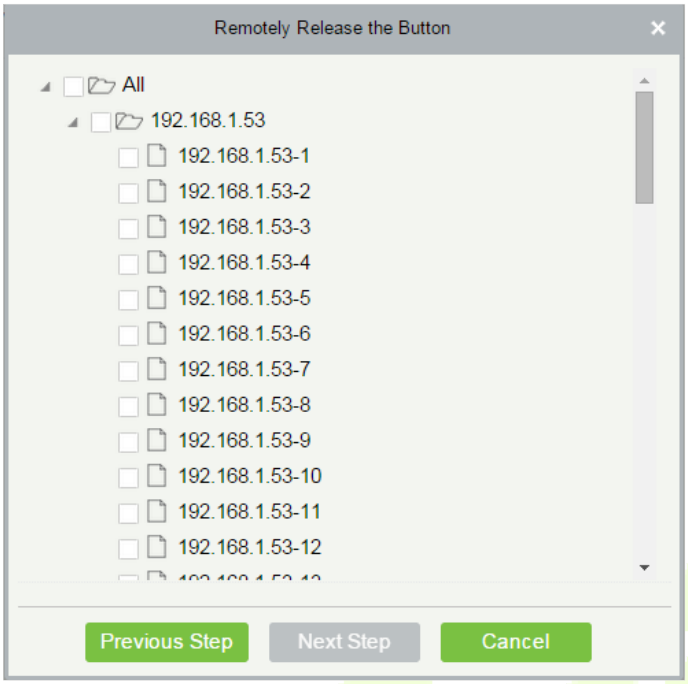
Show Photos: If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

2. Remotely Release Button

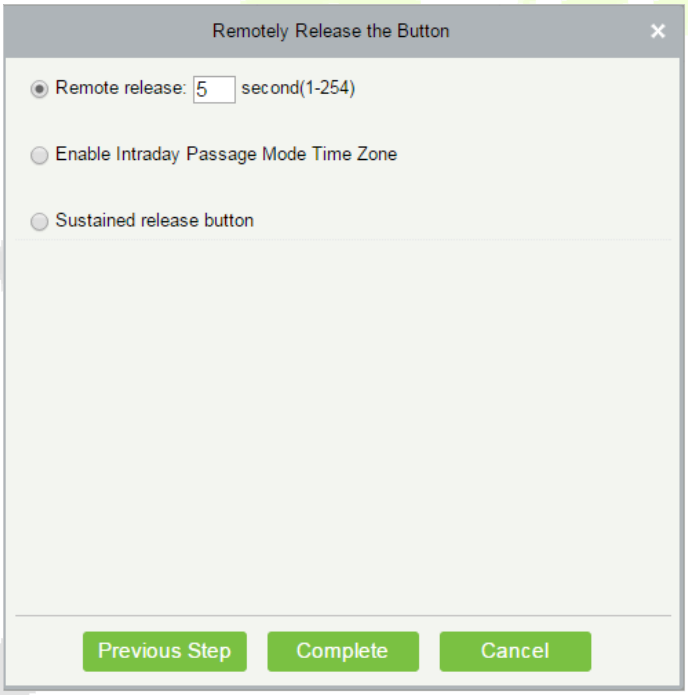
Click [**Remotely Release Button**]:



Input the user password (the system logging password), click [**Next Step**]:



Select the floor, and click [**Next Step**]:



Fields are as follows:

Remote Release: It determines whether the corresponding key to the selected floor can be pressed. You can customize the key release duration (15s by default), or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

Enable Intraday Passage Mode Time Zone: To close a floor, you must first set Disable Intraday Passage

Mode Time Zone to prevent the case that the floor is opened because other continuous open periods take effect. Then, you need to set to close the Remote Lock Button.

Sustained Release Button: The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

✍**Note:** If a failure message is always returned for the remote release key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

Select the options, click [**Complete**] to finish enabling the button.

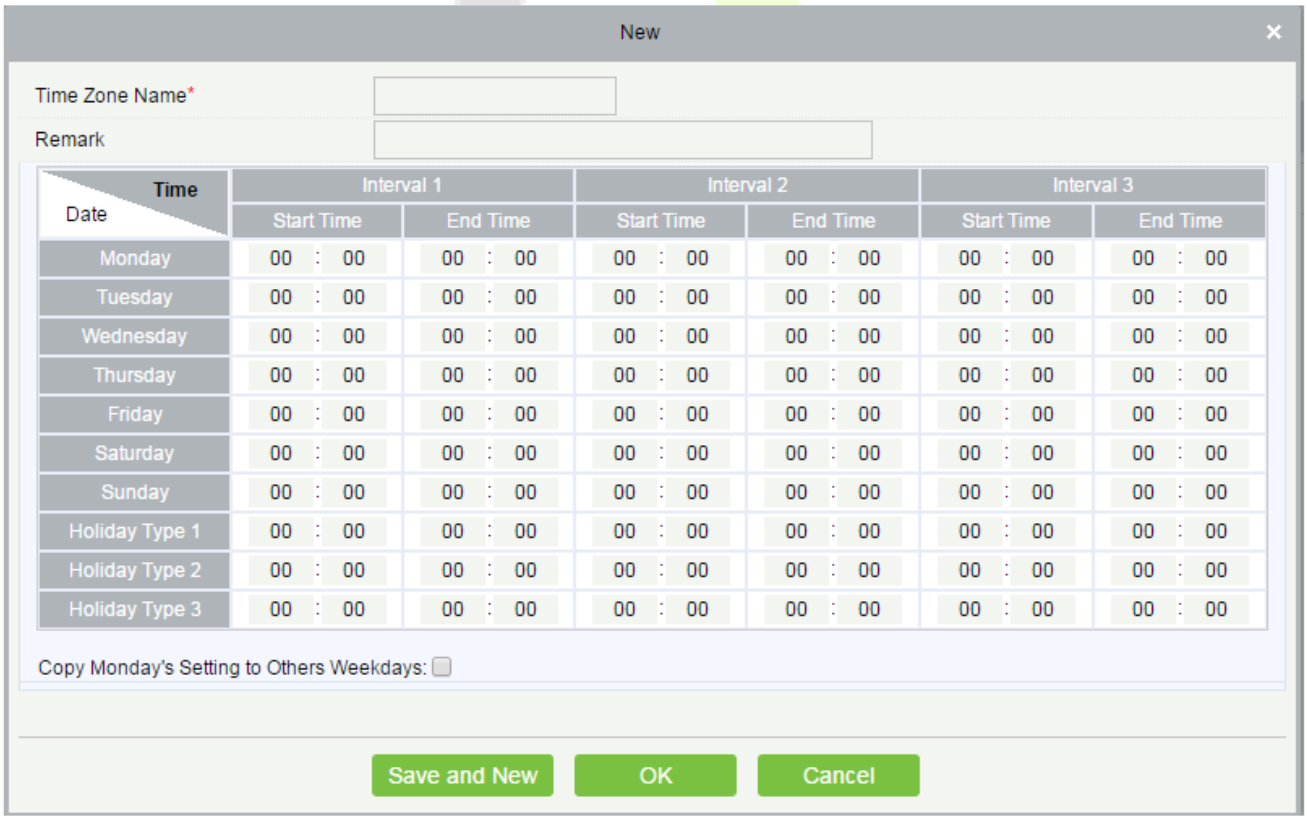
7.2 Elevator Rules

It can control buttons of a common elevator and implement unified management on people going in or on access and exits of each floor through the elevator controller on the computer management network. You can set the rights of registered personnel for operating floor buttons on the elevator.

7.2.1 Time Zones

- **Add Elevator Control Time Zone**

1. Click [**Elevator**] > [**Time Zones**] > [**New**] to enter the time zone setting interface:



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 30 characters.

Remarks: Detailed description of the current time zone, including explanation of current time zone and primary applications. The field is up to 50 characters.

Interval and Start/End Time: One Elevator Control Time Zone includes 3 intervals for each day in a week, and 3 intervals for each of the three Holidays. Set the Start and End Time of each interval.

Setting: If the interval is Normal Open, just enter 00:00-23:59 as the interval 1, and 00:00-00:00 as the interval 2/3. If the interval is Normal Close: All are 00:00-00:00. If only using one interval, user just needs to fill out the interval 1, and the interval 2/3 will use the default value. Similarly, when only using the first two intervals, the third interval will use the default value. When using two or three intervals, user needs to ensure two or three intervals have no time intersection, and the time shall cross over to 2nd day, or the system will prompt error.

Holiday Type: Three holiday types are unrelated to the day of a week. If a date is set to a holiday type, the three intervals of the holiday type will be used for access. The holiday type is optional. If the user does not enter one, system will use the default value.

Copy on Monday: You can quickly copy the settings of Monday from Tuesday to Sunday.

2. After setting, click [**OK**] to save, and it will display in the list.

- **Maintenance of Elevator Time Zones**

Edit: Click the [**Edit**] button under operation to enter the edit interface. After editing, click [**OK**] to save.

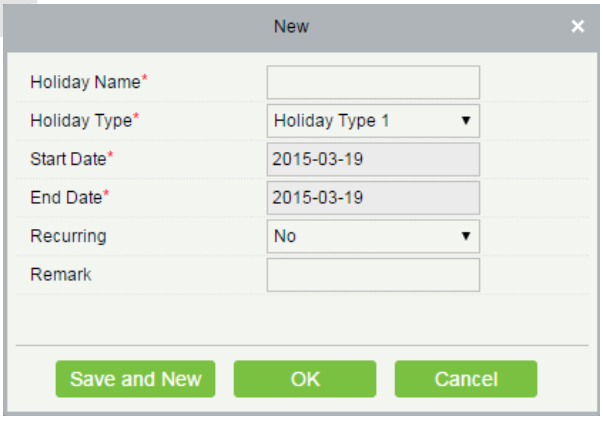
Delete: Click the [**Delete**] button under Related Operation, then click [**OK**] to delete, or click [**Cancel**] to cancel the operation. A time zone in use cannot be deleted. Or tick the check boxes before one or more time zones in the list, and click the [**Delete**] button over the list, then click [**OK**] to delete, click [**Cancel**] to cancel the operation.

7.2.2 Holidays

Elevator Control Time of a holiday may differ from that of a weekday. The system provides elevator control time setting for holidays. Elevator Holiday Management includes Add, Modify and Delete.

- **Add**

Click [**Elevator**] > [**Holidays**] > [**New**] to enter edit interface:



Fields are as follows:

Holiday Name: Any character, up to a combination of 30 characters.

Holiday Type: Holiday Type 1/2/3, namely, a current holiday record belongs to the three holiday types and each holiday type includes up to 32 holidays.

Start/End Date: The date format: 2010-1-1. Start Date cannot be later than End Date otherwise system error will occur. The year of Start Date cannot be earlier than the current year, and the holiday cannot span years.

Recurring: It means that a holiday whether to require modification in different years. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. The Mother's Day is on the second Sunday of each May; this date is not fixed and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Friday, but the Access Control Time of Holiday Type 1.

After editing, click **[OK]** button to save, and it will display in holiday list.

- **Modify**

Click Holiday Name or **[Edit]** button under Operations to enter the edit interface. After modification, click **[OK]** to save and quit.

- **Delete**

In the access control holiday list, click **[Delete]** button under Operations. Click **[OK]** to delete, click **[Cancel]** to cancel the operation. An Elevator Holiday in use cannot be deleted.

7.2.3 Elevator Levels

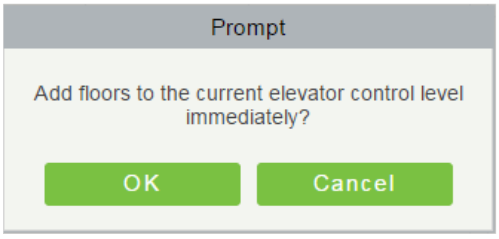
Elevator levels indicate that one or several selected doors can be opened by verification of a combination of multi person within certain time zone. The combination of multi-person set in Personnel Access Level option.

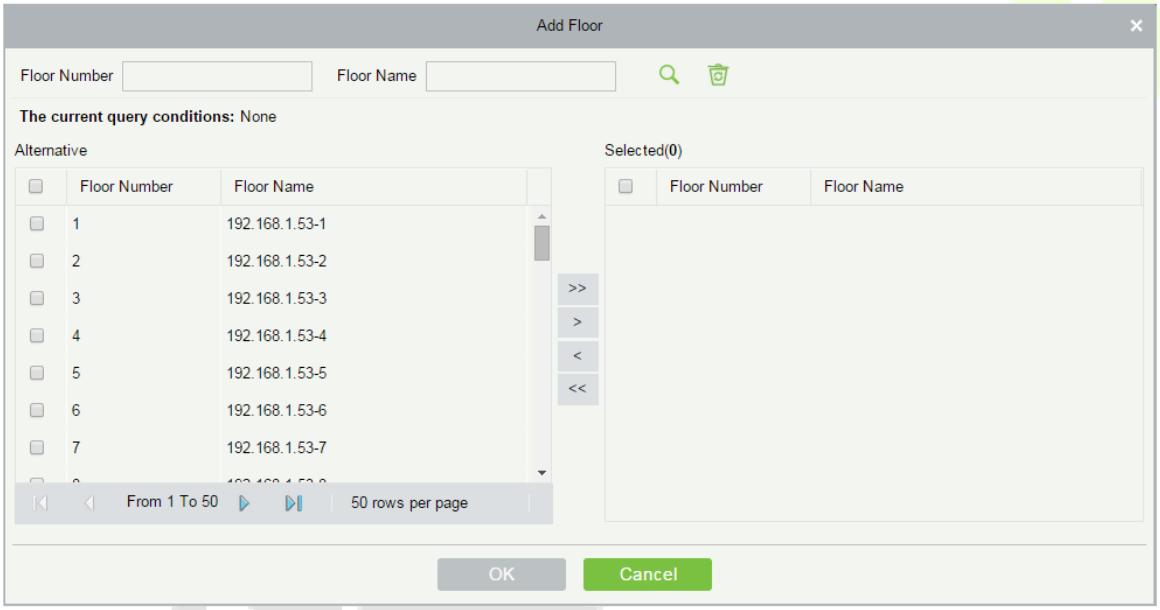
- **Add**

1. Click [**Elevator**] > [**Access Levels**] > [**New**] to enter the Add Levels editing interface:

2. Set each parameter: Level Name (unrepeatable), Time Zone and Area.

3. Click [**OK**], the system prompts "Add floors to the current elevator control level immediately", click [**OK**] to add floors, click [Cancel] to return the elevator levels list. The added level is displayed in the list.





✍**Note:** Different floors of different elevator controllers can be selected and added to an elevator level.

7.2.4 Set Access by Levels

Add/Delete Personnel for Selected Levels:

1) Click [**Elevator**] > [**Set By Levels**] to enter the edit interface, Click an Elevator level in left list, personnel having right of opening door in this access level will display on right list.

2) In the left list, click [**Add Personnel**] under Operations to pop-up the Add Personnel box; select personnel (multiple) and click > to move it to the right selected list, then click [**OK**] to save and complete.

3) Click the level to view the personnel in the right list. Select personnel and click [**Delete Personnel**] above the right list, then Click [**OK**] to delete.

7.2.5 Set Access by Person

Add selected personnel to selected elevator levels, or delete selected personnel from the elevator levels.

- **Add/Delete levels for Selected Personnel:**

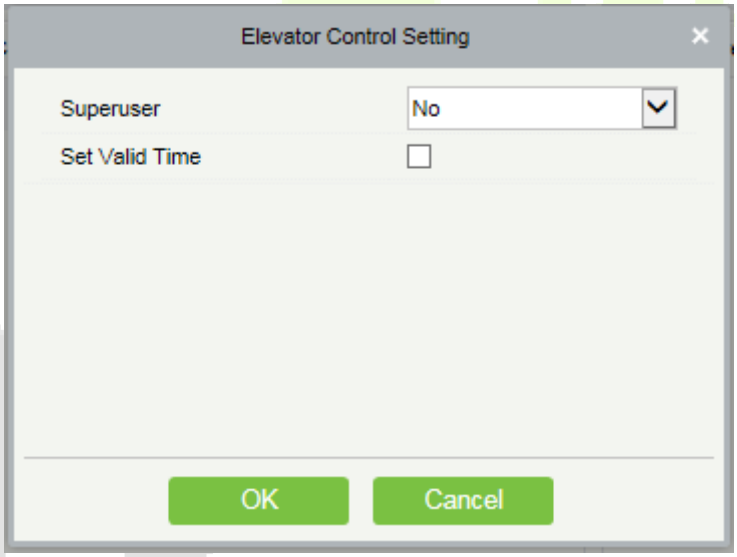
1) Click [**Elevator**] > [**Elevator Levels**] > [**Set By Person**], click employee to view the levels in the right list.

2) Click [**Add to Levels**] under Operations to pop-up the Add to Levels box, select Level (multiple) and click > to move it to the right selected list; click [**OK**] to save and complete.

3) Select Level (multiple) in the right list, and click [**Delete from levels**] above the list, then click [**OK**] to delete the selected levels.

- **Setting levels for Selected Personnel:**

1) Select a person in the list on the left and click [**Elevator Control Setting**]. The following page is displayed:



2) Set access control parameters and click [**OK**] to save the setting.

7.2.6 Set Access by Department

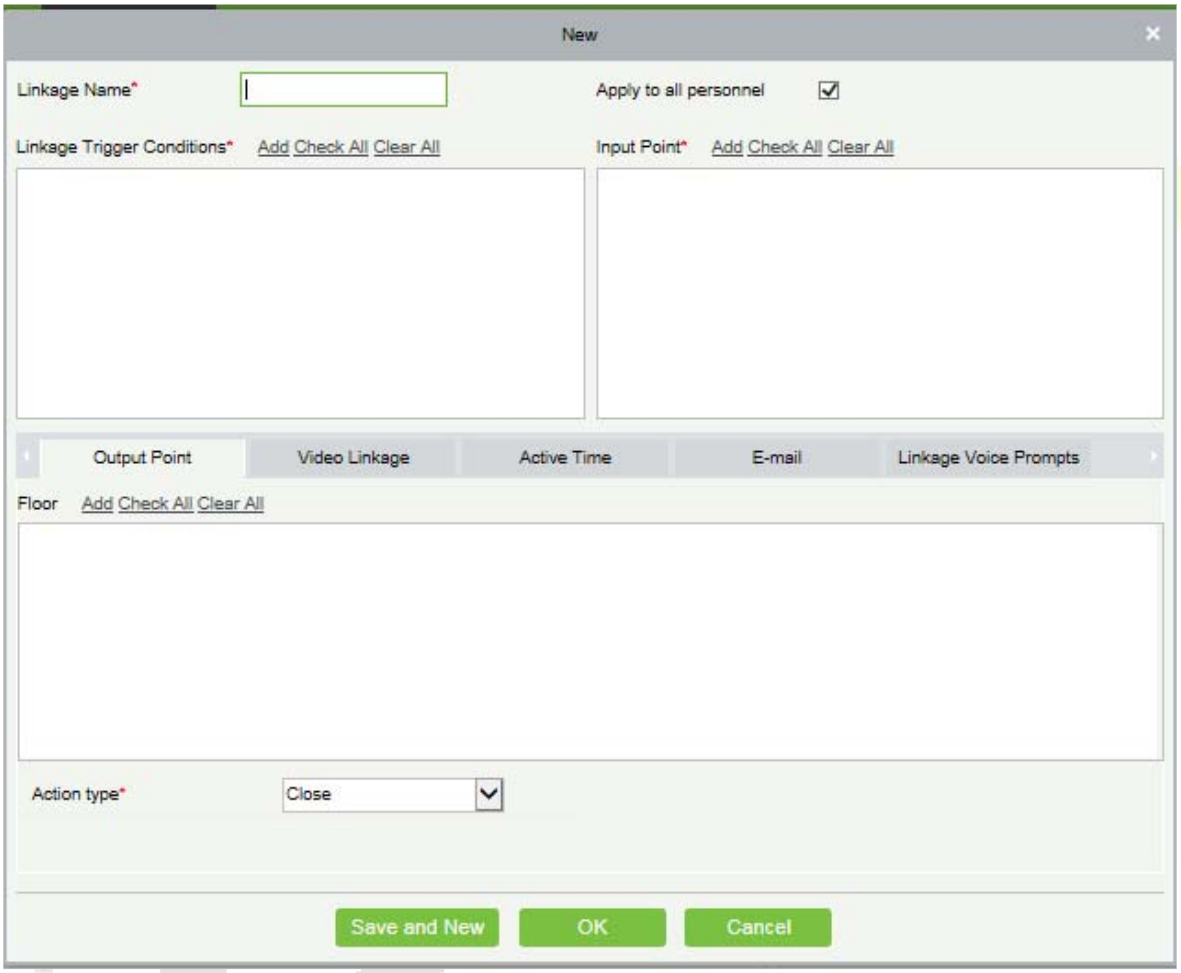
Add selected department to selected elevator levels, or delete selected department from the elevator levels. The access of the staff in the department will be changed.

7.2.7 Global Linkage

The global linkage function enables you to configure data across devices. Only push devices support this function.

- **Add**

1) Click [**Elevator**] > [**Elevator**] > [**Global Linkage**] > [**New**]:



The fields are as follows:

Linkage Name: Set a linkage name.

Linkage Trigger Condition: Linkage Trigger Condition is the event type of selected device. Except Linkage Event Triggered, Cancel Alarm, Enable/Disable Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (the specific input point please refers to specific device parameters).

Output Point: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, and Auxiliary Output 10 (the

specific output point please refers to specific device parameters).

Linkage Action: Close, Open, Normal Open. The default is closed. To open, delay time shall be set, or select Normal Close.

Video Linkage:

- Pop up video: Whether to set the pop-up preview page in real-time monitoring, and set the pop-long.
- Video: Enable or disable background video recording, and set the duration of background video recording.
- Capture: Enable or disable background snapshot.

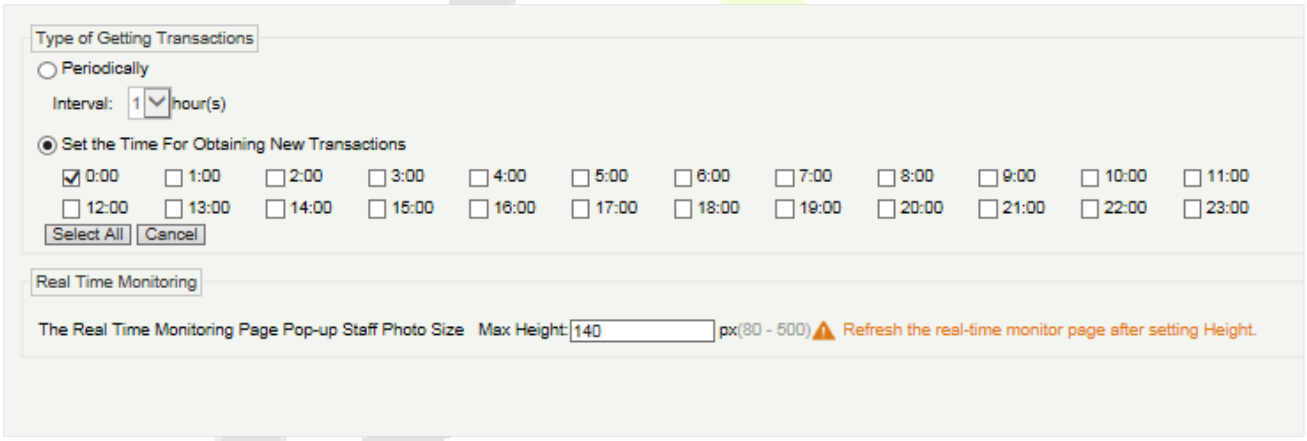
Delay: Ranges from 1~254s (This item is valid when Action type is Open).

2) Click [**OK**] to save and quit. The added Global Linkage will display in the list.

✍**Note:** It is not allowed to set the same linkage setting at input point and output point. The same device permits consecutive logical linkage settings. The system allows you to set several trigger conditions for a linkage setting one time.

7.2.8 Parameters

Click **[Elevator]** > **[Elevator]** > **[Parameters]**:



Type of Getting Transactions:

- **Periodically**

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

- **Set the Time For Obtaining New Transactions**

The selected Time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up, set the size of the pop-up photos, the range is 80-500px.

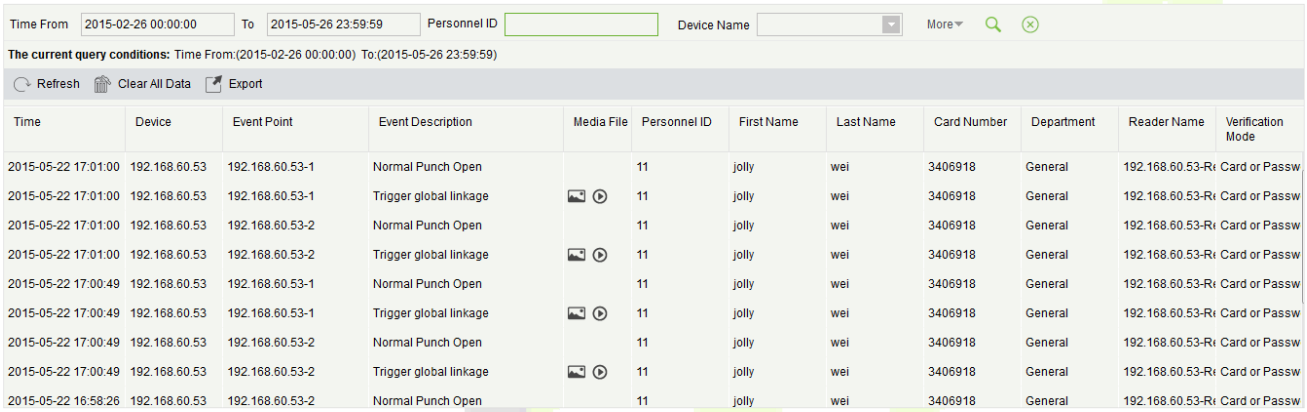
7.3 Elevator Reports

Includes “All transactions” and “All Exception Events”. You can export after querying.

7.3.1 All Transactions

Because the data size of elevator access control event records is large, you can view elevator access control events as specified condition when querying. By default, the system displays the latest three months transactions.

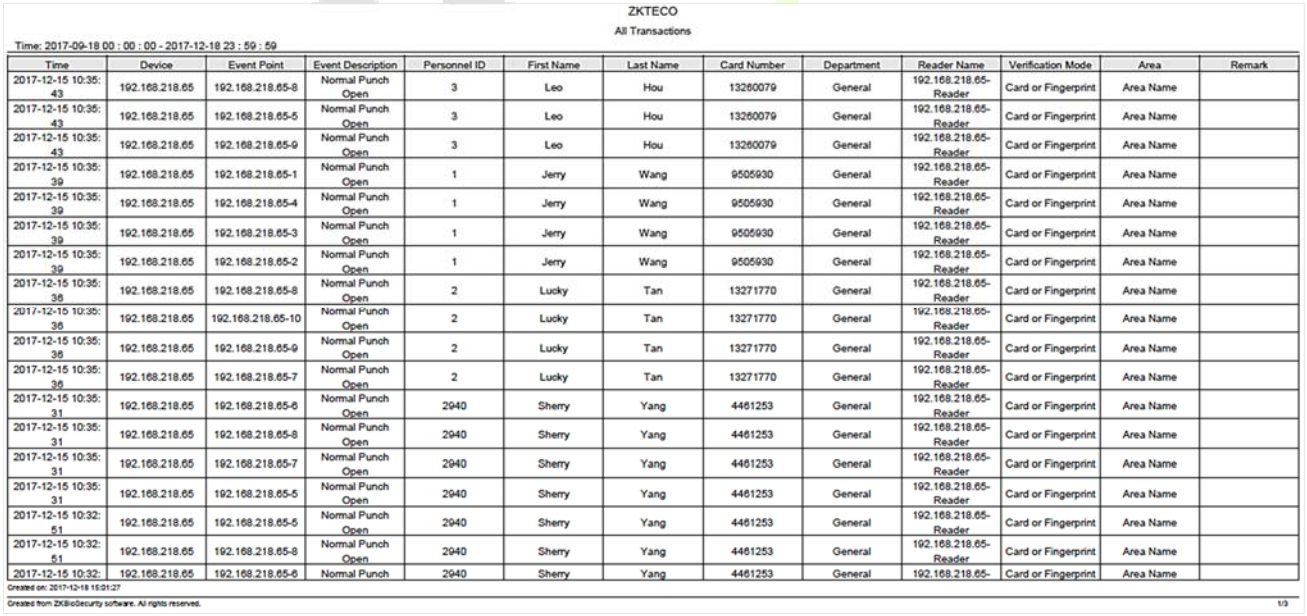
Click **[Reports]** > **[All Transactions]** to view all transactions:



Time	Device	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Trigger global linkage		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw
2015-05-22 16:58:26	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-R	Card or Passw

Clear All Data: Click **[Clear All Data]** to pop up prompt and click **[OK]** to clear all transactions.

Export: You can export all transactions in Excel, PDF, CSV format.



ZKTECO

All Transactions

Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

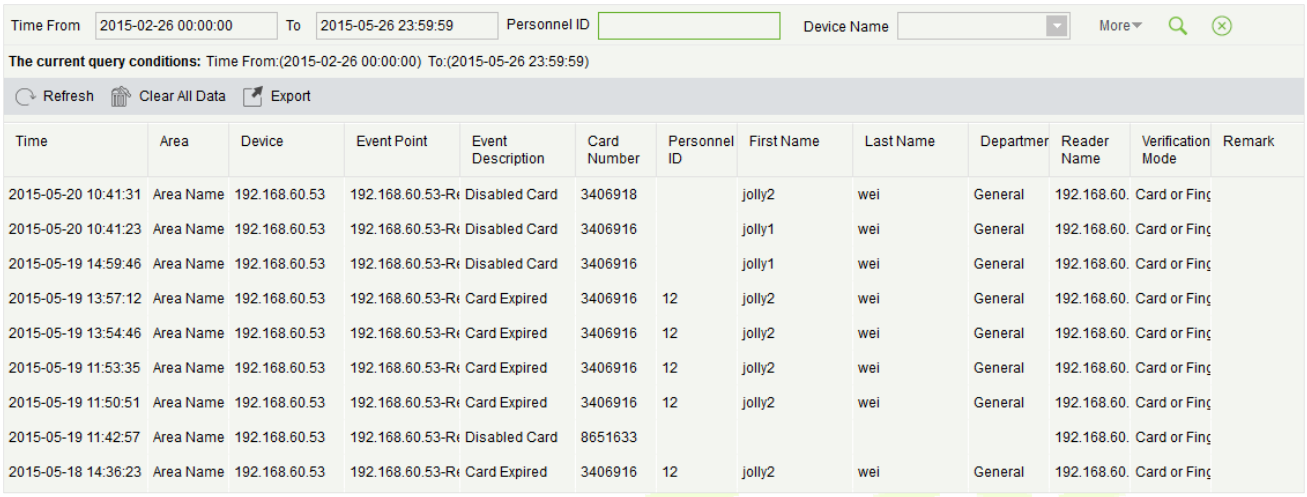
Time	Device	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area	Remark
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-8	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-5	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:43	192.168.218.65	192.168.218.65-9	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-1	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-4	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-3	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:39	192.168.218.65	192.168.218.65-2	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-8	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-10	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-9	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:36	192.168.218.65	192.168.218.65-7	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-6	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-7	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35:31	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:51	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65-Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32:	192.168.218.65	192.168.218.65-6	Normal Punch	2940	Sherry	Yang	4461253	General	192.168.218.65-	Card or Fingerprint	Area Name	

Created on: 2017-12-18 15:01:27

Created from ZKBioSecurity software. All rights reserved. 1/3

7.3.2 All Exception Events

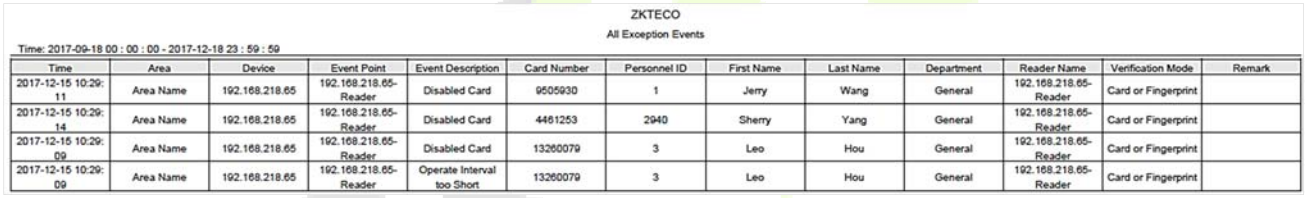
Click **[Reports]** > **[All Exception Events]** to view exception events in specified condition. The options are same as those of **[All Transactions]**.



Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Departmer	Reader Name	Verification Mode	Remark
2015-05-20 10:41:31	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406918		jolly2	wei	General	192.168.60.	Card or Finç	
2015-05-20 10:41:23	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406916		jolly1	wei	General	192.168.60.	Card or Finç	
2015-05-19 14:59:46	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	3406916		jolly1	wei	General	192.168.60.	Card or Finç	
2015-05-19 13:57:12	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Finç	
2015-05-19 13:54:46	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Finç	
2015-05-19 11:53:35	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Finç	
2015-05-19 11:50:51	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Finç	
2015-05-19 11:42:57	Area Name	192.168.60.53	192.168.60.53-R	Disabled Card	8651633					192.168.60.	Card or Finç	
2015-05-18 14:36:23	Area Name	192.168.60.53	192.168.60.53-R	Card Expired	3406916	12	jolly2	wei	General	192.168.60.	Card or Finç	

Clear All Data: Click **[Clear All Data]** to pop up prompt, click **[OK]** to clear all exception events.

Export: You can export all exception events in Excel, PDF, CSV format.



ZKTECO

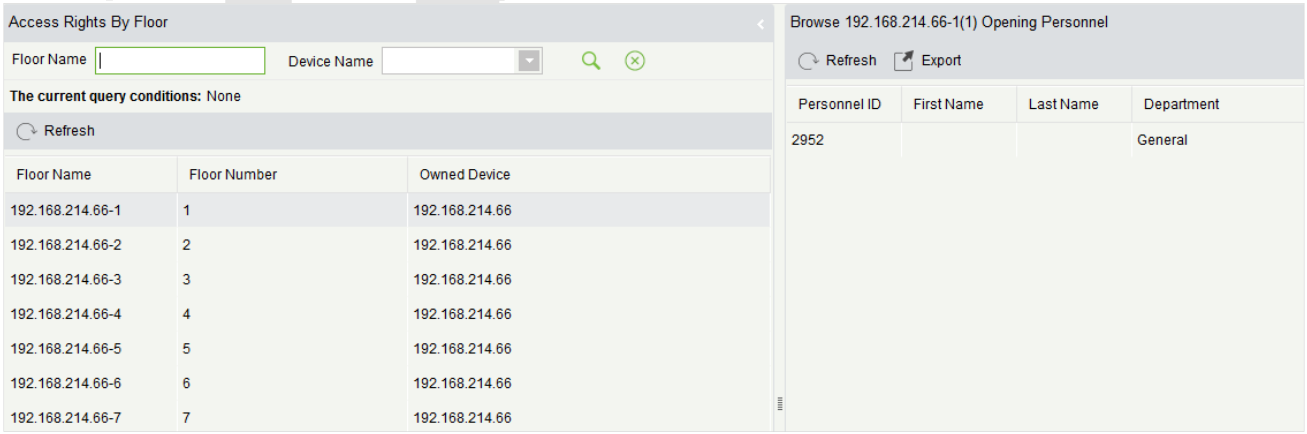
All Exception Events

Time: 2017-09-18 00 : 00 : 00 - 2017-12-18 23 : 59 : 59

Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Department	Reader Name	Verification Mode	Remark
2017-12-15 10:29:11	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	9505930	1	Jerry	Wang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:14	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	4461253	2940	Sherry	Yang	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Disabled Card	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	
2017-12-15 10:29:09	Area Name	192.168.218.65	192.168.218.65-Reader	Operate Interval too Short	13260079	3	Leo	Hou	General	192.168.218.65-Reader	Card or Fingerprint	

7.3.3 Access Rights by Floor

View related access levels by door. Click **[Reports]** > **[Access Rights By Floor]**, the data list in the left side shows all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.



Floor Name	Floor Number	Owned Device
192.168.214.66-1	1	192.168.214.66
192.168.214.66-2	2	192.168.214.66
192.168.214.66-3	3	192.168.214.66
192.168.214.66-4	4	192.168.214.66
192.168.214.66-5	5	192.168.214.66
192.168.214.66-6	6	192.168.214.66
192.168.214.66-7	7	192.168.214.66

Personnel ID	First Name	Last Name	Department
2952			General

You can export all the personnel having access levels to the floor data in Excel, PDF, CSV format.

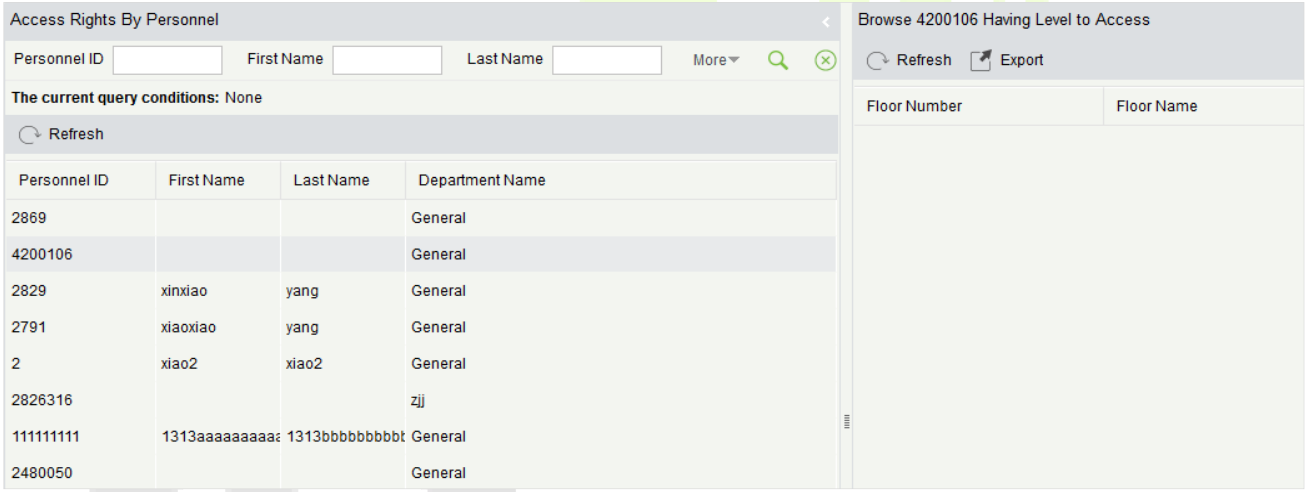
ZKTECO

192.168.218.65-1(1) Opening Personnel

Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
5	Necol	Ye	Marketing Department
6	Amber	Lin	Financial Department
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Development Department

7.3.4 Access Rights by Personnel

Click **[Reports]** > **[Access Rights By Personnel]**, the data list in the left side show all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.



You can export all the floor information in Excel, PDF, CSV format.

ZKTECO

2940(Sherry) Having Level to Access

Floor Number	Floor Name
1	192.168.218.65-1
2	192.168.218.65-2
3	192.168.218.65-3
4	192.168.218.65-4
5	192.168.218.65-5
6	192.168.218.65-6
7	192.168.218.65-7
8	192.168.218.65-8
9	192.168.218.65-9
10	192.168.218.65-10

11 Video (Video Linkage)

The system supports video linkage of access elevator control. You can achieve the management of DVR/ NVR/IPC, real-time video preview, video records query and automatically popping up of linkage events.

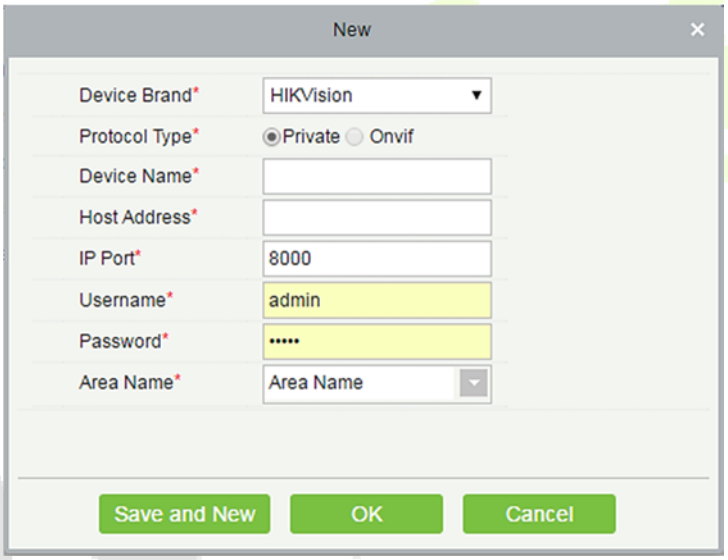
You need to add video device, set linkage function in Linkage Setting and Global Linkage in advanced.

✍**Note:** The current software only supports HIKVision, ZKIVision and Dahua devices. For more details about the devices models, please contact technical support personnel to confirm.

11.1 Video Device

- **Add a Video device**

Click **[Video]** > **[Video Device]** > **[Video Device]** > **[New]**:



Fields are as follows:

Device Brand: The current software version only supports ZKTeco, HIKVISION, Dahua, Axis, Panasonic and Geovision brands. For each brand supporting models, please refer to the Hardware Support List for Video Module.

Protocol Type: The Private or Onvif protocol is automatically selected after Device Brand is specified.

Device Name: Any characters within a length of 30.

Host Address: Input the device's IP address.

IP Port: The default corresponding IP Port will display after select Device Brand.

User Name: Any characters within a length of 15 (mandatory).

Password: Any characters within a length of 32 (mandatory).

Area Name: Divide area for the device.

✍**Note:** After adding device, only the device name and area name can be modified again, other options cannot be modified.

- **Enable/Disable a Video Device**

Select a video device in the list and click [**Enable] or [Disable**].

- **Edit/Delete Video a Device**

Select a video device in the list and click [**Edit**] or [**Delete**].

- **Communication Settings**

When the communication parameters are modified in the device, the modification must be synchronized to the software to keep consistency, otherwise all the channels of the video device will not work normally.

Select a device, click [**Communication Settings**]:

- **Video Linkage Operation Guide**

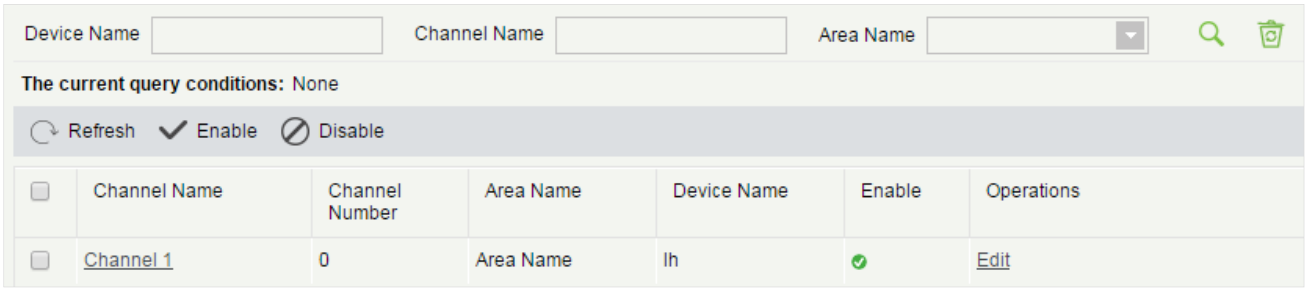
Click **[Video Linkage Operation Guide]**, guide users to add video equipment, binding cameras for access control equipment and set the linkage.

11.2 Video Channel

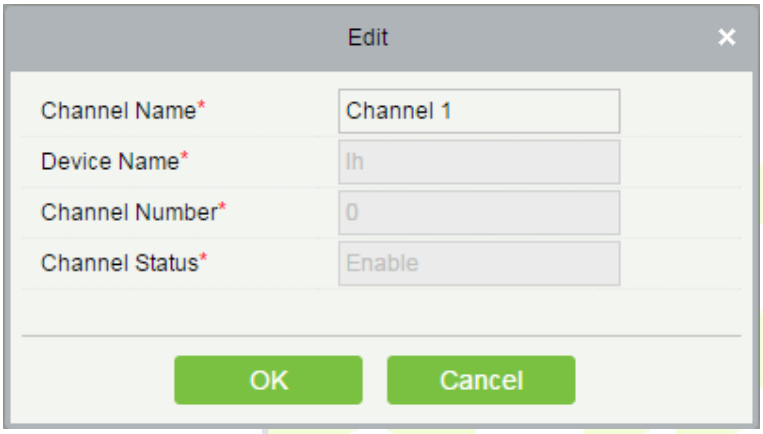
When adding a video device, the system will automatically detect the number of cameras on this device, that is, the number of channels, and generate a number of channels accordingly. For example, a video device has 16 cameras. After adding this device, the system will generate 16 channels, and name the channels by default using the format "Device name-channel No.".

- **Enable/Disable Video Device**

Click **[Video]** > **[Video Device]** > **[Channel]**:



Click [**Edit**] below Operations in the list:



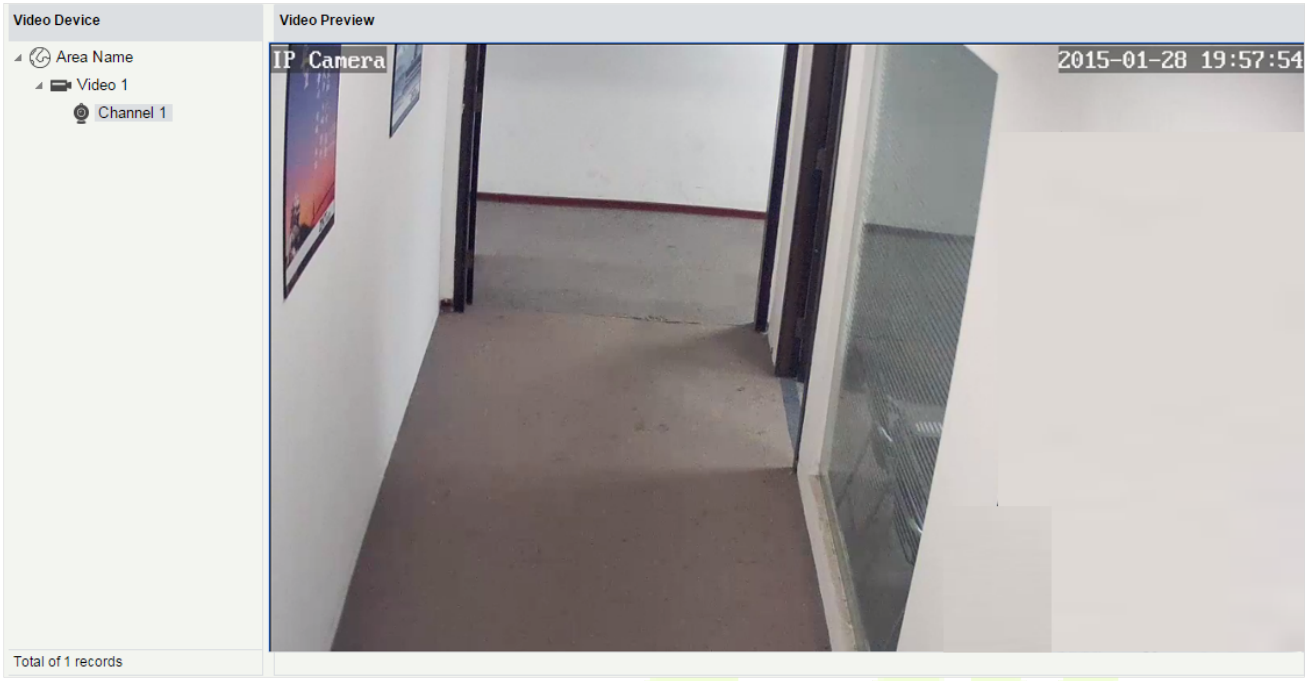
Fields are as follows:

Channel Name: Any characters within a length of 30.

Device Name, Channel Number and Channel Status are not editable in this page. You can modify them in Video Device. The channel number is the channel number in video device.

11.3 Video Preview

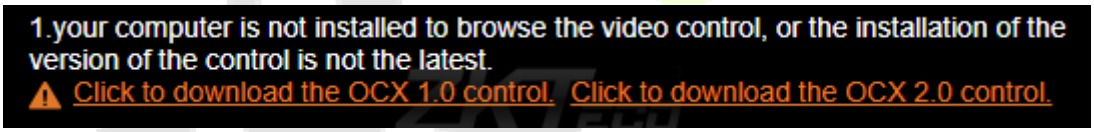
Click **[Video]** > **[Video Device]** > **[Video Preview]**, the left side is the device and channel lists, click a channel to view the monitor screen.



Re-click the channel to shut down the screen.

✍Notes:

- A video can allow five users to preview at the same time. In chronological order, the exceeded users cannot preview the video normally, and the page will be grey.
- If there are no video controls in the system, the below prompts will be displayed:

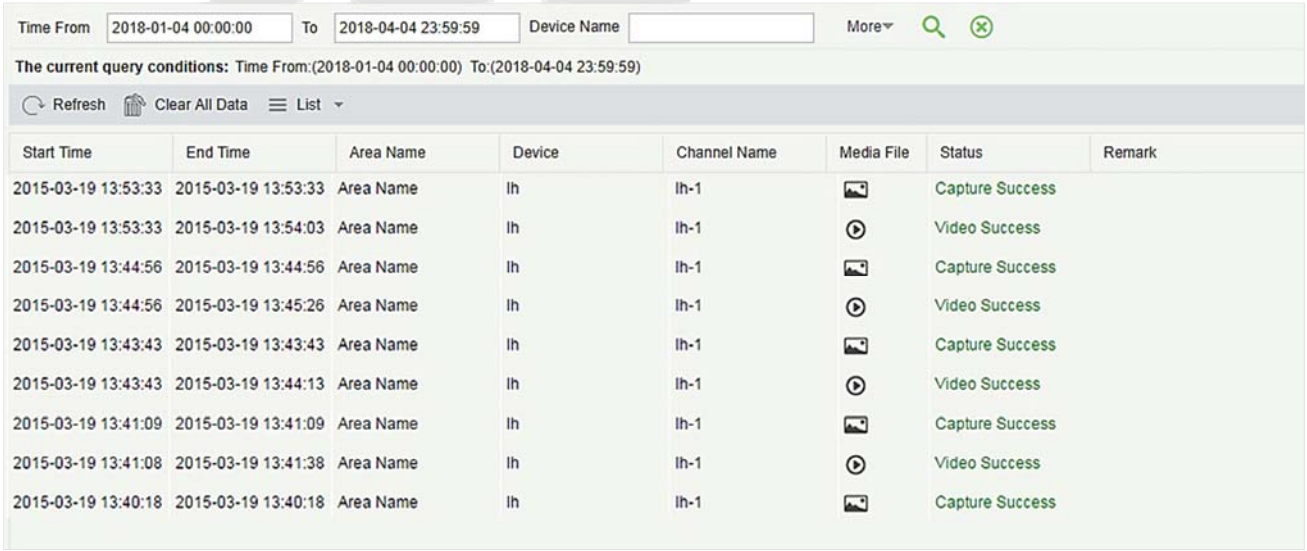


Click to download both the controls. Install the controls, and refresh the page, you can view the monitor screen normally. To prevent abnormal video display, please install the controls that ZKBioSecurity offers.

11.4 Video Event Record

View the records of catching pictures and videos.

Click [**Video**] > [**Video Device**] > [**Video Event Record**]:



Start Time	End Time	Area Name	Device	Channel Name	Media File	Status	Remark
2015-03-19 13:53:33	2015-03-19 13:53:33	Area Name	Ih	Ih-1		Capture Success	
2015-03-19 13:53:33	2015-03-19 13:54:03	Area Name	Ih	Ih-1		Video Success	
2015-03-19 13:44:56	2015-03-19 13:44:56	Area Name	Ih	Ih-1		Capture Success	
2015-03-19 13:44:56	2015-03-19 13:45:26	Area Name	Ih	Ih-1		Video Success	
2015-03-19 13:43:43	2015-03-19 13:43:43	Area Name	Ih	Ih-1		Capture Success	
2015-03-19 13:43:43	2015-03-19 13:44:13	Area Name	Ih	Ih-1		Video Success	
2015-03-19 13:41:09	2015-03-19 13:41:09	Area Name	Ih	Ih-1		Capture Success	
2015-03-19 13:41:08	2015-03-19 13:41:38	Area Name	Ih	Ih-1		Video Success	
2015-03-19 13:40:18	2015-03-19 13:40:18	Area Name	Ih	Ih-1		Capture Success	

The media file is:

: Indicates that the linkage type is “Video”, you can click to download this file. Please choose a third

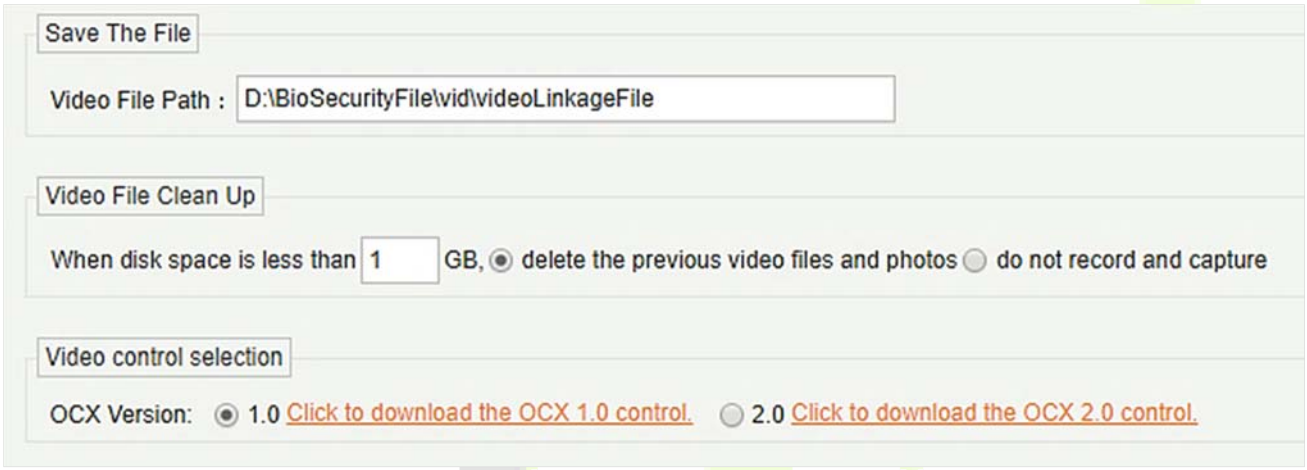
part of video player to play the file, or else it cannot be played normally.

: Indicates that the linkage type is “Capture”, you can click to view this file.

✍**Note:** If the “Video” and “Capture” are both selected, there will be 2 records. For more details about the way to set the linkage type, please refer to Linkage Setting.

11.5 Parameters

Click [**Video**] > [**Video Device**] > [**Parameters**]:



Video File Path: Path for storing files when the server records videos or captures images.

Video File Clean Up: When the disk space for storing video files is smaller than the pre-set value, you can choose to delete the old video files or not to record videos or capture images. If you choose Delete, the software will delete the video files that are generated in the earliest day and continue to record videos; otherwise, the software does not record videos.

Video Control selection: It can set whether to download OCX 1.0 or OCX 2.0.

11.6 Solutions of Exceptions

A. Client browser cannot playback video, preview, or Real-Time Monitoring page has no video pops-up:

Firstly, ensure IE11 or above version browser is available, client and Video Server are on the same network segment and the video ActiveX installation is successful. If the ActiveX installation fails, above all, uninstall the video ActiveX that were originally installed, run the "regsvr32-u NetVideoActiveX23.ocx"command, and then in the browser, set all the options in "Tools -> Internet Options -> Security -> Custom Level" on the ActiveX to "Enable or Prompt", re-open the browser, re-login screen and open the video preview page, run the button "all add items of the site".

B. The network or power of video device is shut off while previewing the video screen.

Check whether the network or power is connected normally. Refresh the page after ensuring that the connection is normal, refresh the page, and re-open the video preview.

C. In the E-Map, no video pops-up after clicking the camera icon:

Make sure to use IE11 and above version browser, client and Video Server on the same network segment and the video ActiveX installation is successful. Also, view whether the browser is preventing the temporary window pops up, if it is change to allow window pops up to the site.

D. Video linkage is triggered, the video server does not have video or size of the video file that the client downloads from the Video Server is 0kb:

First, ensure that the software server has set Time Server (keep the Windows time service and has set the NTP function of the video server), it is recommended to set the time interval of the video server smaller to ensure accurate synchronization software server and video server time, so as to keep the time consistent between software server and controllers. It is recommended set Linkage Recording Time more than 5 seconds, to avoid executing video linkage commands delay, which may lead to the downloaded 0kb video file.

E. The Video system is not normal to use in windows server 2008:

Desktop Experience feature needs to be added in windows server2008 before the normal use of the video.

Step 1: Run" services.msc" to open the "Service Manager".

Step2: Set the start type of "Windows Audio" and "Themes" as Automatically Start.

Step3: Run the service manager, click **[Add functions]**, check the "Desktop Experience" box and click **[Install]**. Reboot the server after the installation is finished.

F. The video downloaded to local cannot be played:

Please choose a third part of video player to play the file, or else it cannot be played normally.

G. When the browser is chrom42 or above version, the system will prompt you to install video controls though you have already installed.

The old NPAPI controls are disabled in chrom42 or above version. You should open the browser and enter "chrome://flags/#enable-npapi" in address bar to enable the controls.

12 Video (VMS)

12.1 Video Device

On the **VMS module**, click **Video Device** to go to the Video Device module.

12.1.1 Add a Video Device

On the **Video Device** module, click **Video Device**, and then click **New** to manually add the video device.

- **Fill in the relevant fields with the corresponding values:**

Host Address: Enter the IP address of your system.

IP Port: Enter the Port number.

Device Name: Enter the Device Name.

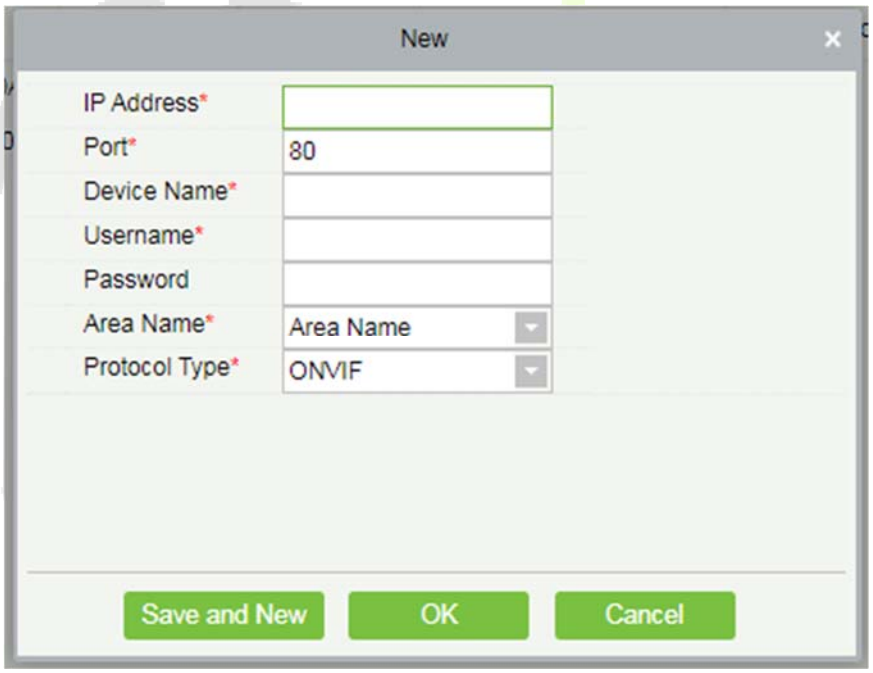
Username: Enter the Username.

Password: Enter a unique password.

Area Name: Select the Area name from the drop-down list.

Protocol Type: Select the protocol from the drop-down list for transmitting the data.

Click [**OK**] to add the device.

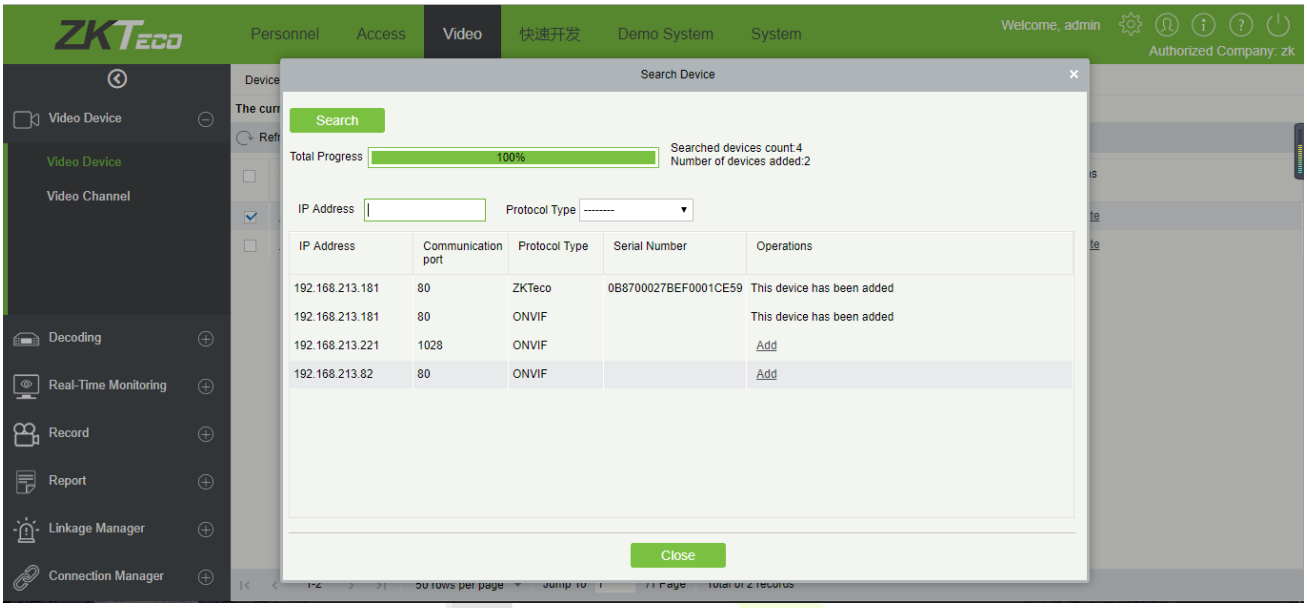


Search and Add Video Device

On the **Video Device** interface, click **Search Device** to search and add the Video Device.

On the **Search Device** window, click the **Search button** on the upper left corner and it will list the search results.

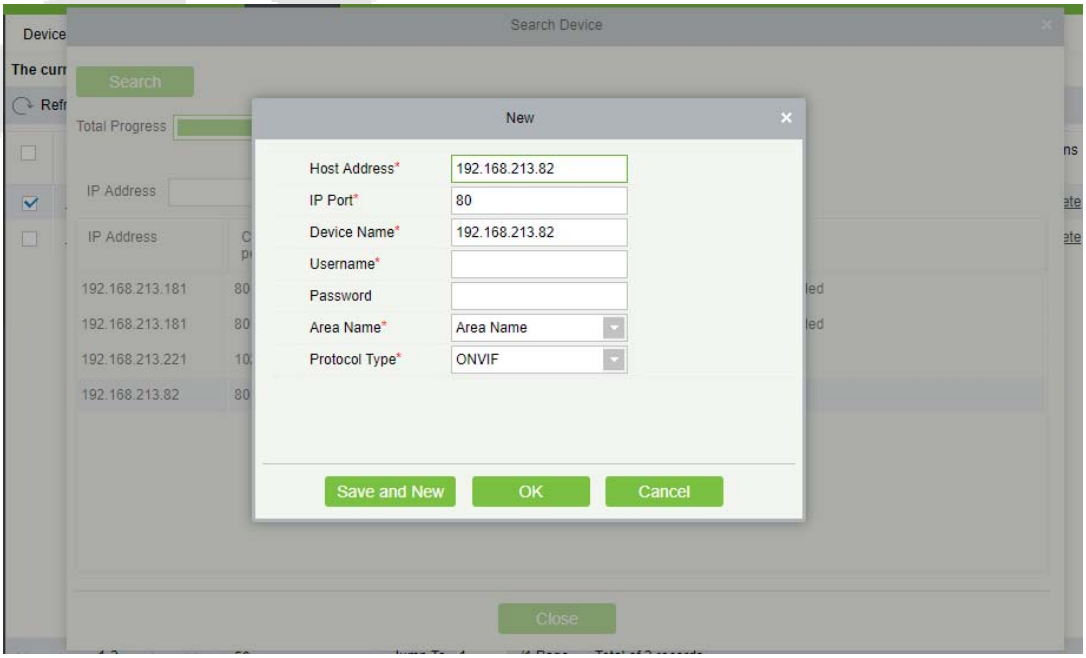
During the search process the device with "**ONVIF**" protocol type will not display the serial number, and it can be viewed only after adding the device.



On the **Search** list, the Add operation will not be available for the devices that have been already added.

On the **Search** list, click **Add** to add the required devices.

On the **New** window, enter the **Username** and the **Password**.



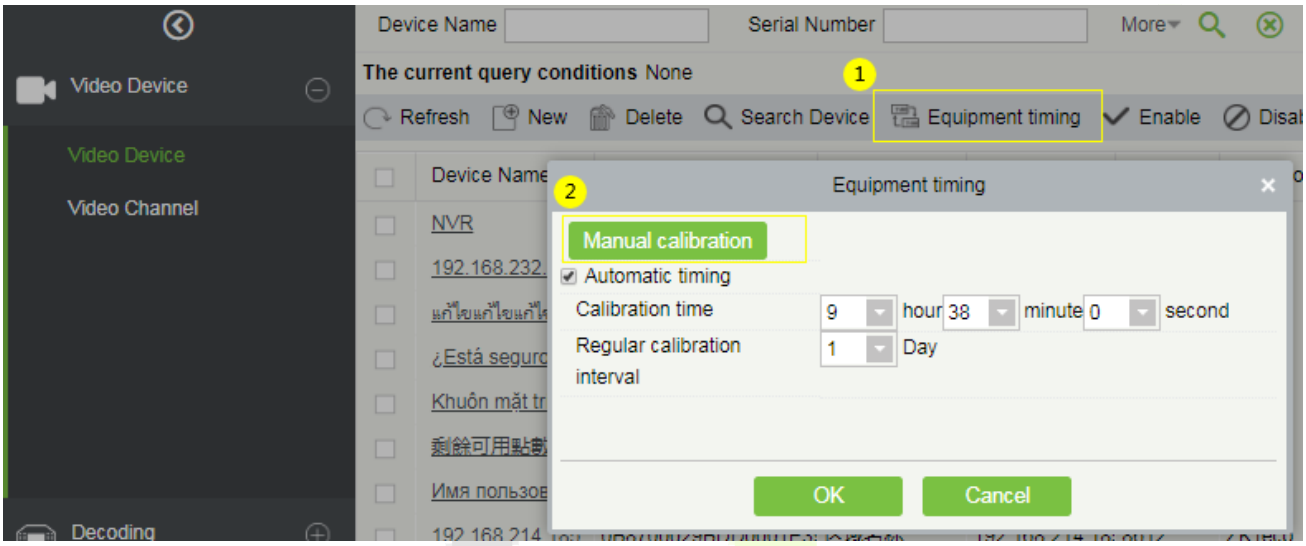
✍Note:

On the **New** window the other information (Host address, IP Port, Device Name, Area Name, and the Protocol Type) will get automatically updated by the software.

- **Equipment Timing**

On the **Video Device** interface, click **Equipment timing** to set the timing.

On the **Equipment timing** window, you can either select the Manual calibration and set the time or can select the Automatic timing.

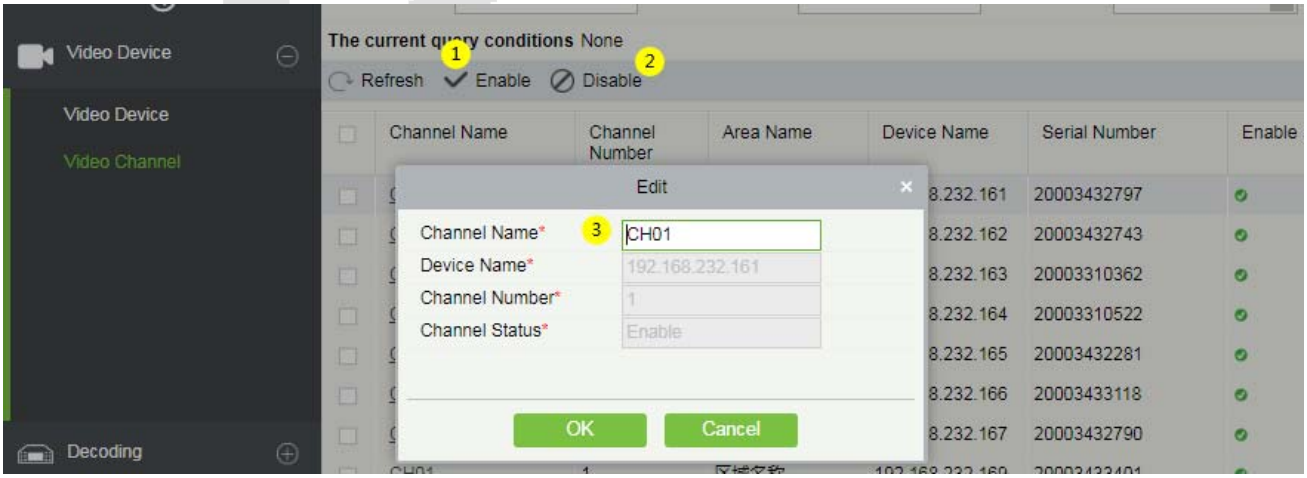


12.1.2 Video Channel

On the **Video Device** module, click **Video Channel** to go to the Video Channel interface.

- **Enable/Disable Channel**

On the **Video Channel** interface, you can edit the channel name, and enable or disable the required video channel.



12.2 Decoding

The decoder can transmit the video images to the screen, which is used to set the TV wall and other such features.

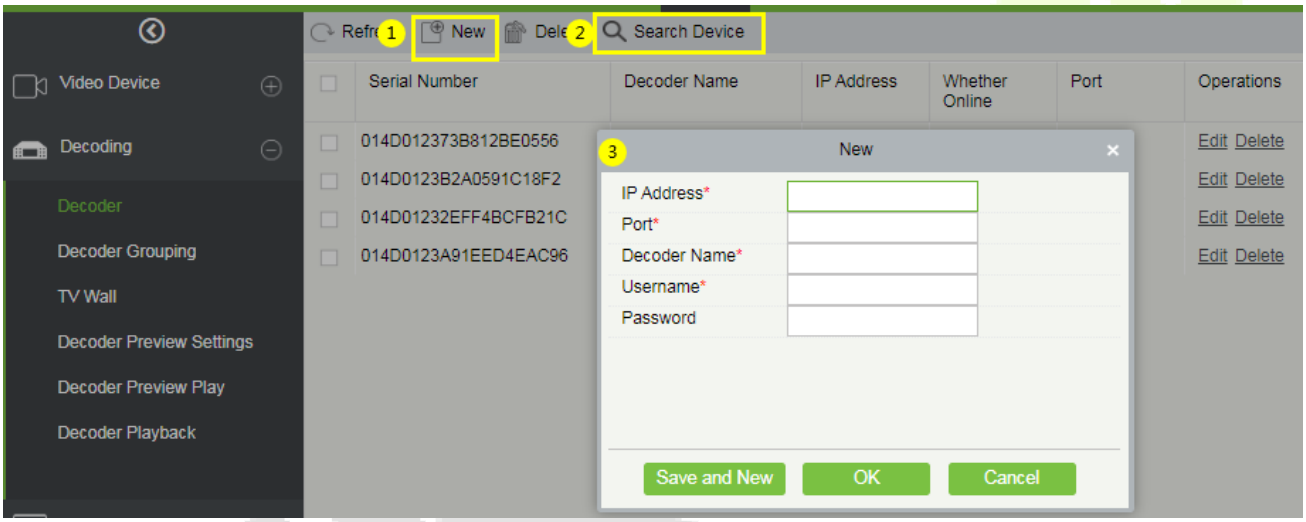
On the **Video** module, click **Decoding** to go the Decoding module.

12.2.1 Decoder

On the **Decoding** module, click **Decoder** to go to the Decoder interface.

- **Add a new Decoder**

On the Decoder interface, click **New** or **Search Device** to add a new decoder.

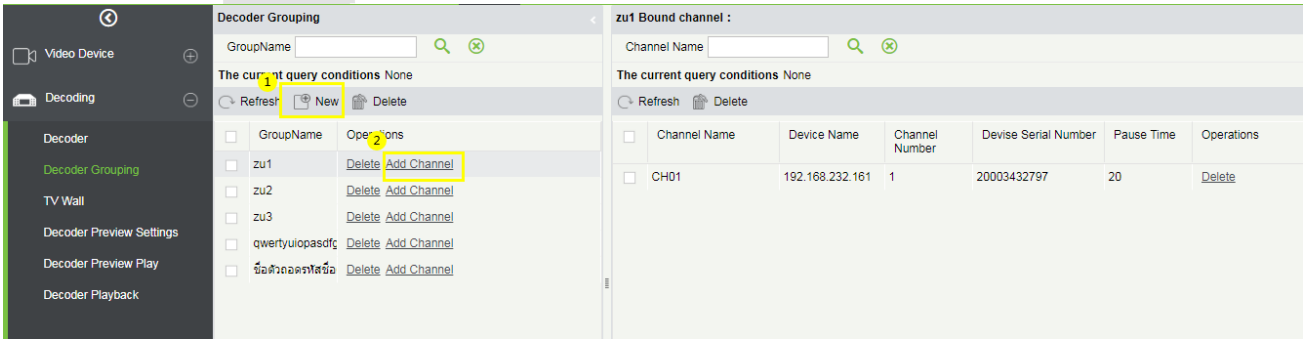


12.2.2 Decoder Grouping

The grouping of Decoder can be set for different video channels.

On the **Decoding** module, click **Decoder Grouping** to group the decoder.

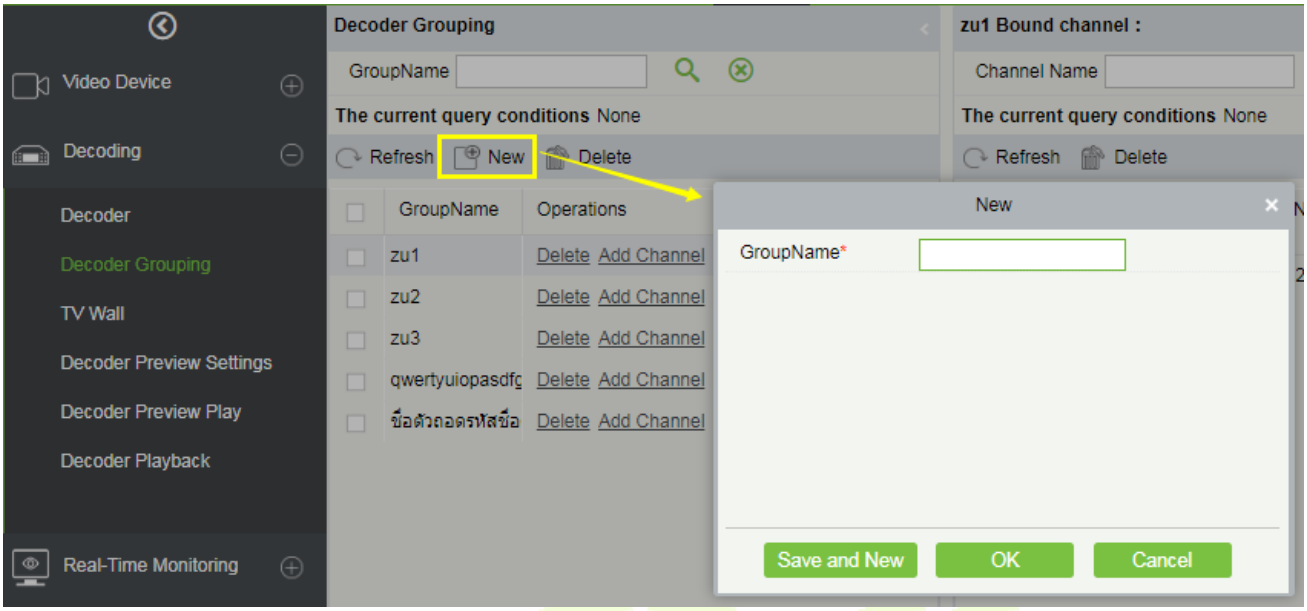
The left side of the **Decoder Grouping** interface displays the Group list and the right side of the interface displays the video channel corresponding to the group.



Add a New Decoder Group

On the **Decoder Grouping** interface, click **New** to add a new decoder group.

On the **New** window, enter the group name.

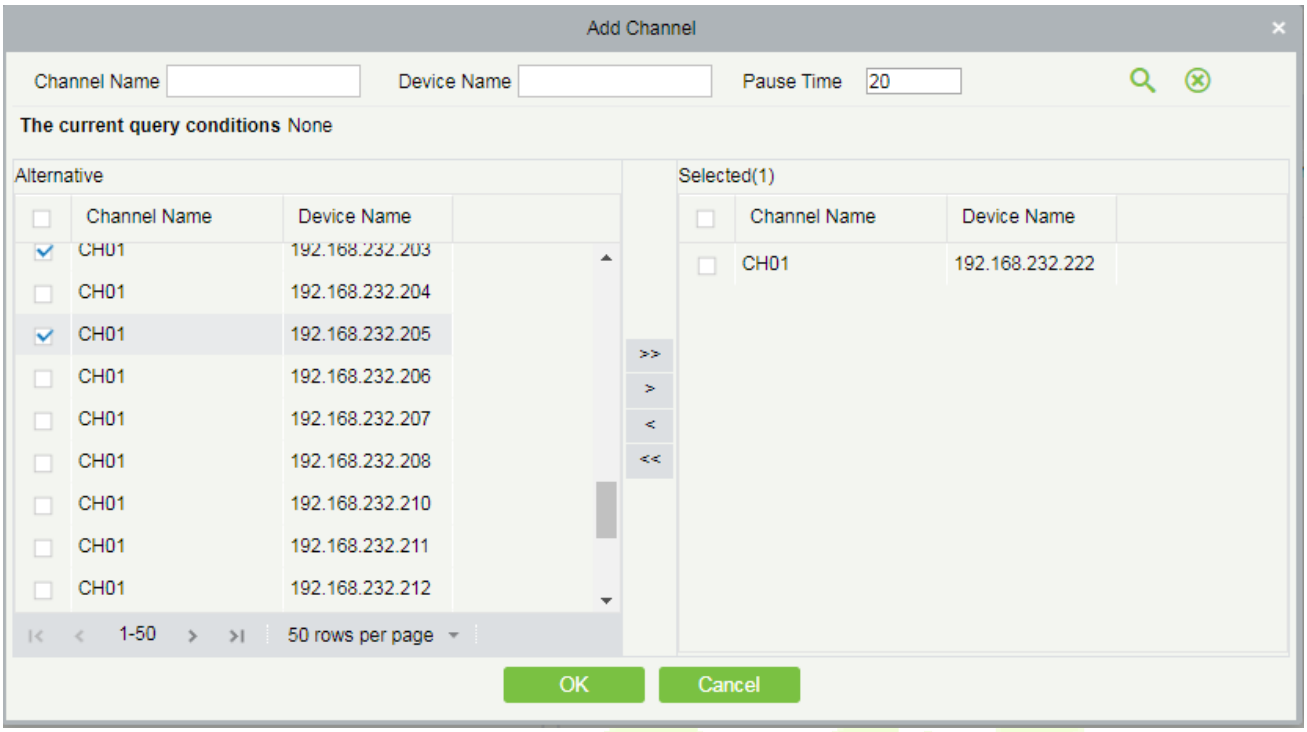


Add Channel:

Click **Add Channel** to add a video channel to the decoder group.

On the **Add Channel** window, select the video channel to be added to the group from the list on the left side of the window.

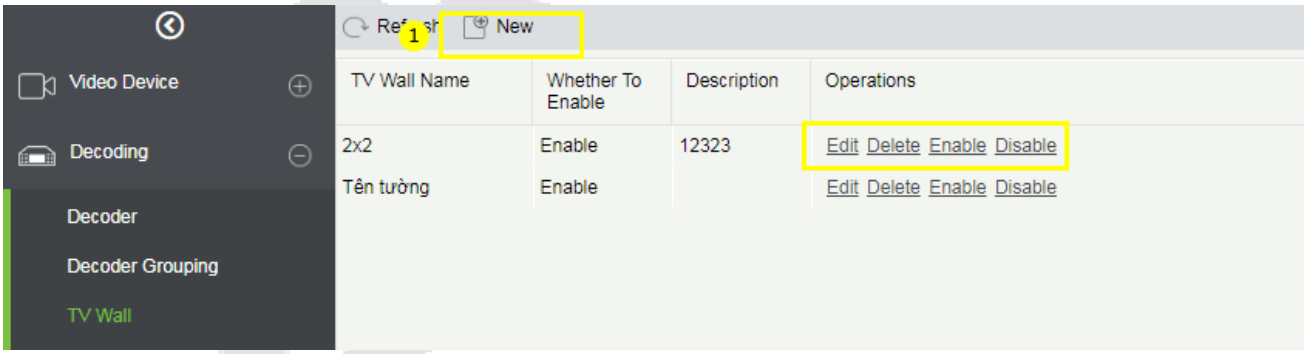
The selected video channel will be reflected on the right side of the window.



12.2.3 TV Wall

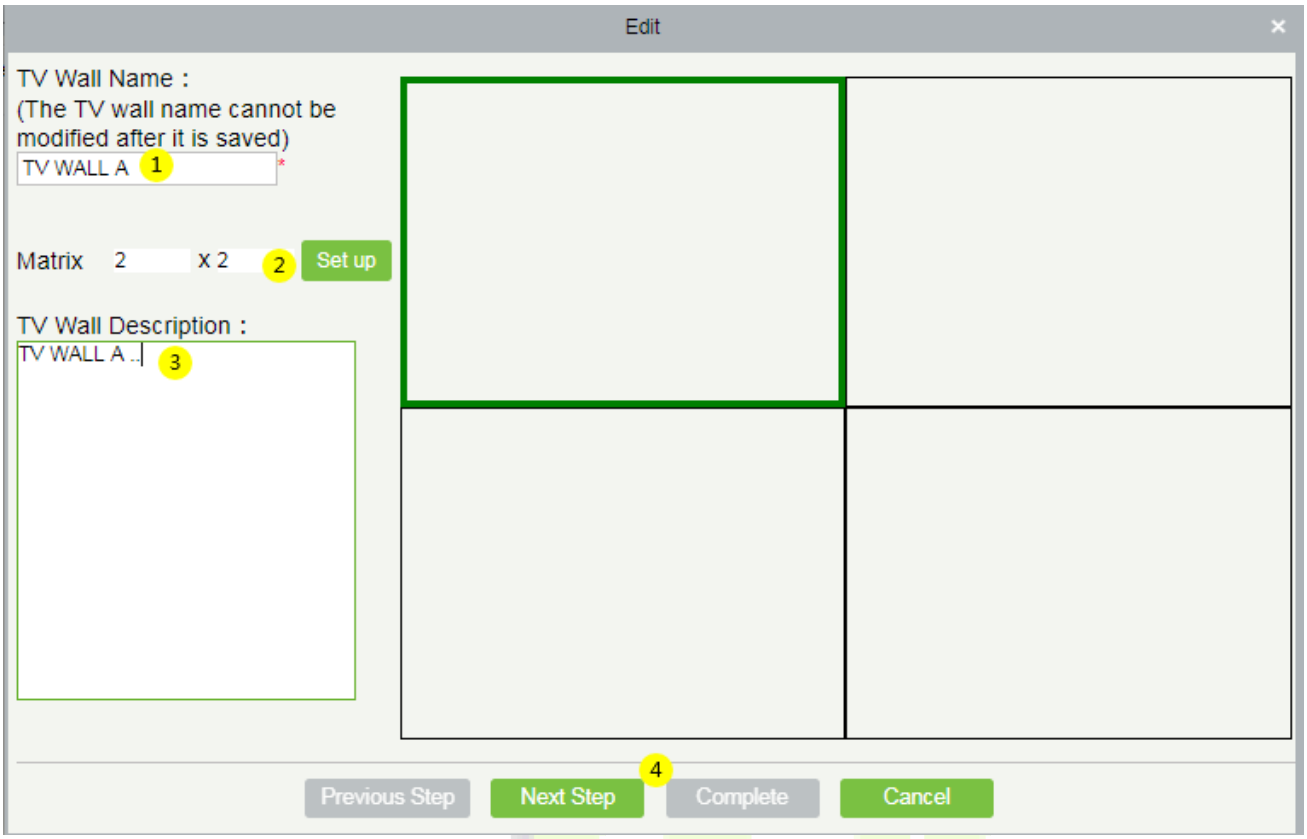
The TV wall is used for setting the size of the video display that is joined together by the display screen. It can be added, edited, enabled, or disabled in the TV Wall menu.

On the **Decoding** module, click **TV Wall** to go to the TV Wall interface.



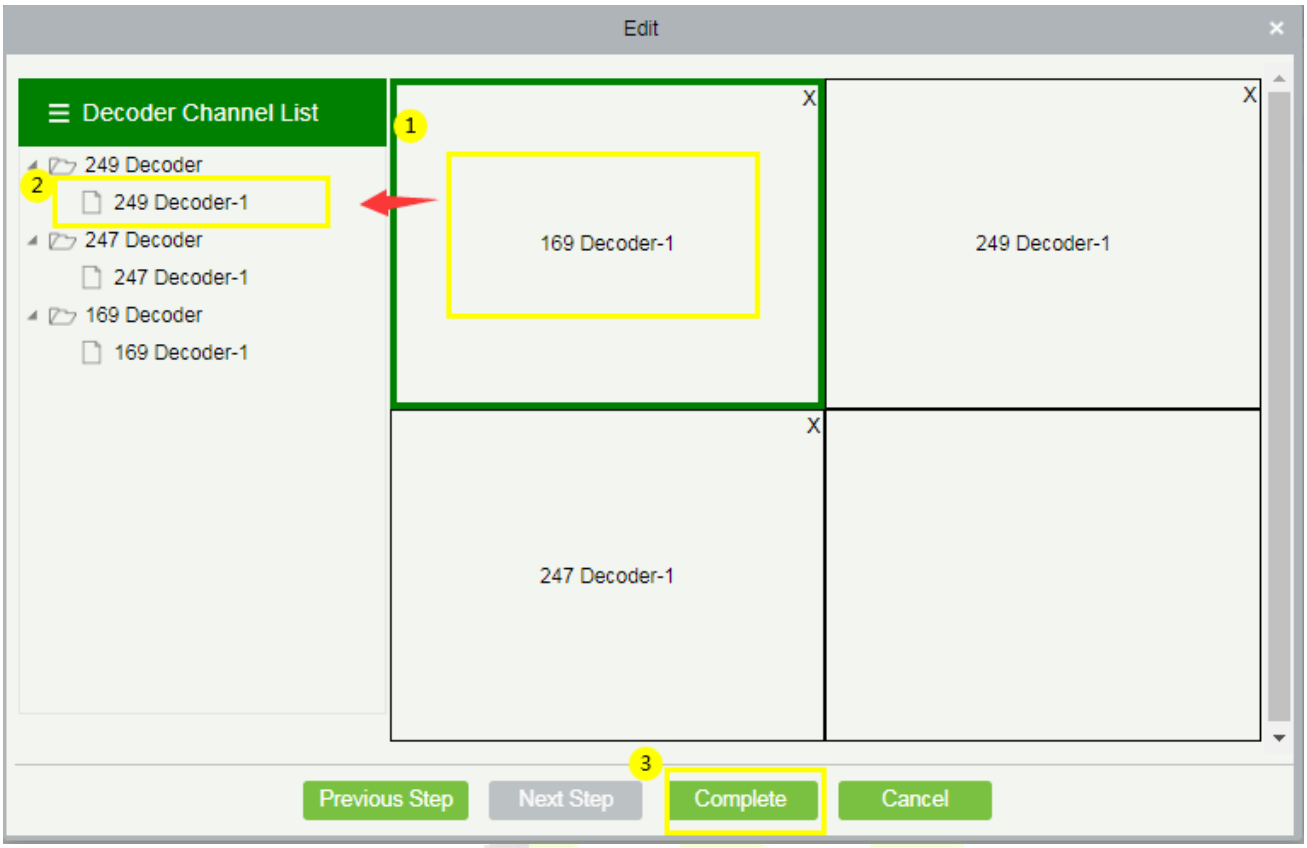
- **Add a new TV Wall Settings:**

1. On the TV Wall interface, click New to add new TV wall settings.
2. Fill in a unique name for the TV wall, where the names cannot be changed once saved.
3. Set the Matrix (here, the matrix refers to the number of rows and columns of the TV wall).
4. Add a description for the TV wall.
5. Click Next Step to go to the next setting.



On this Next window, perform the below action to set the TV Wall.

Click the required ① screen from the matrix on the right side of the window, then select a ② decoder to be displayed, and then click ③ Complete to update the TV Wall settings.



12.2.4 Decoder Preview Settings

The Decoder Preview settings facilitates in setting up the video preview screen.

On the **Decoding** module, click **Decoder Preview Settings** to go to the Decoder Preview Settings interface.

- **Features available on the Decoder Preview Settings:**

TV Wall: On the top right corner of the interface, select the type of TV wall to be previewed from the drop-down option.

Save: Click **Save** to save the preview settings plan.

Save As: Click **Save As** to save the preview settings in a different location or name.

Delete: Click **Delete** to delete the preview settings.

Stop Plan: Click **Stop Plan** to stop the plan.

Start the plan round: Click **Start the plan round** to initiate the plan.

Plan Setting: Click **Plan Setting** to set a new decoder plan.

Exit Plan Editing: Click **Exit Plan Editing** to exit from editing the existing plan.

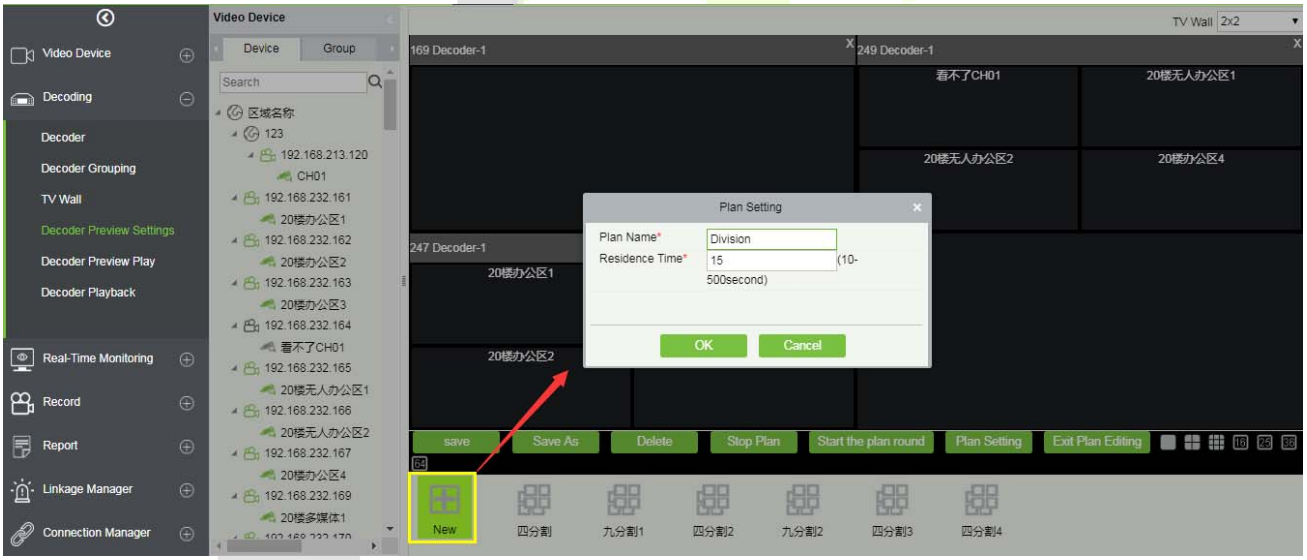
New: Click **New** to create a new preview plan.

Create a New plan

To set the preview, it is essential to create a plan first if there is no existing plan.

On the **Decoder Preview Settings** interface, click **New** to create a new plan.

On the **Plan Setting** window, enter the **Plan Name** (e.g. Division) and **Residence Time** (e.g. 15), and then click **OK** to save.



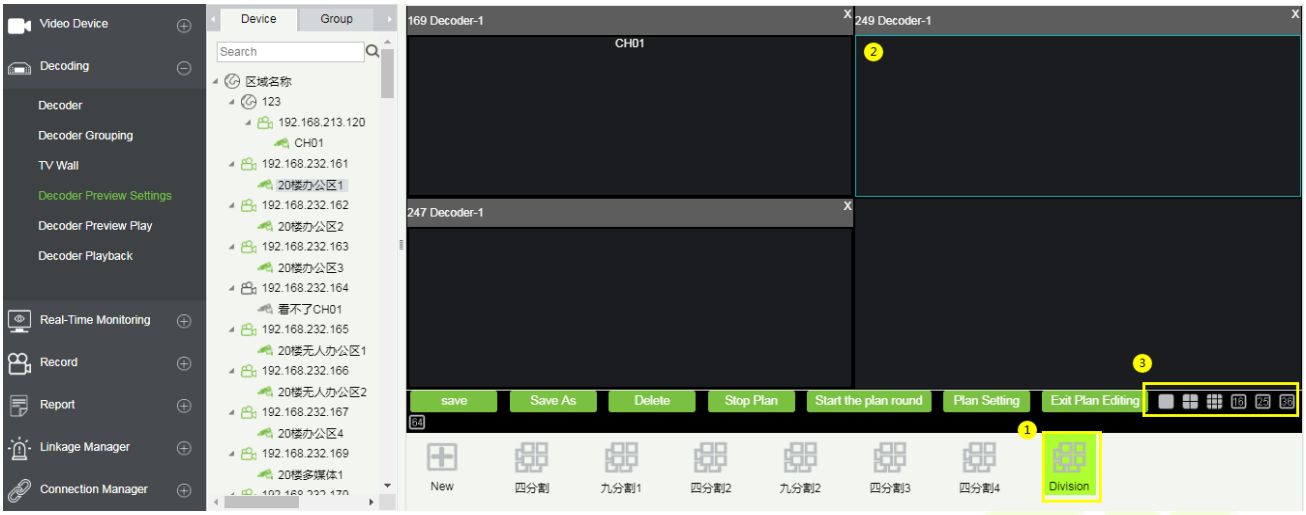
Division (Created/Existing Plan Name)

The newly created or the existing plan name will be displayed at the bottom of the interface as shown in the below image.

To Divide the Decoder Screen

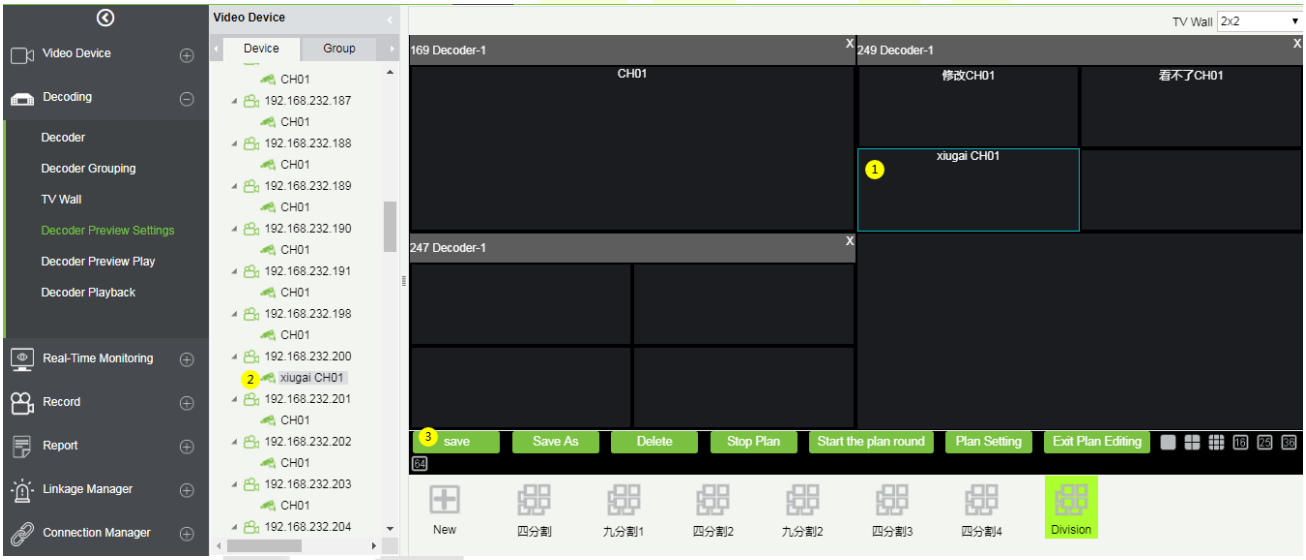
On the **Decoder Preview Settings** interface, click **Division** (plan name), and then select the required decoder screen from the matrix.

Then select any one of the matrix screens from the options to further divide the selected decoder screen.



Add the Video to the Screen

On the divided decoder screen matrix, select any one of split screen, then select the required video channel from the list on the left, and then click ③ **Save** to update the plan settings.

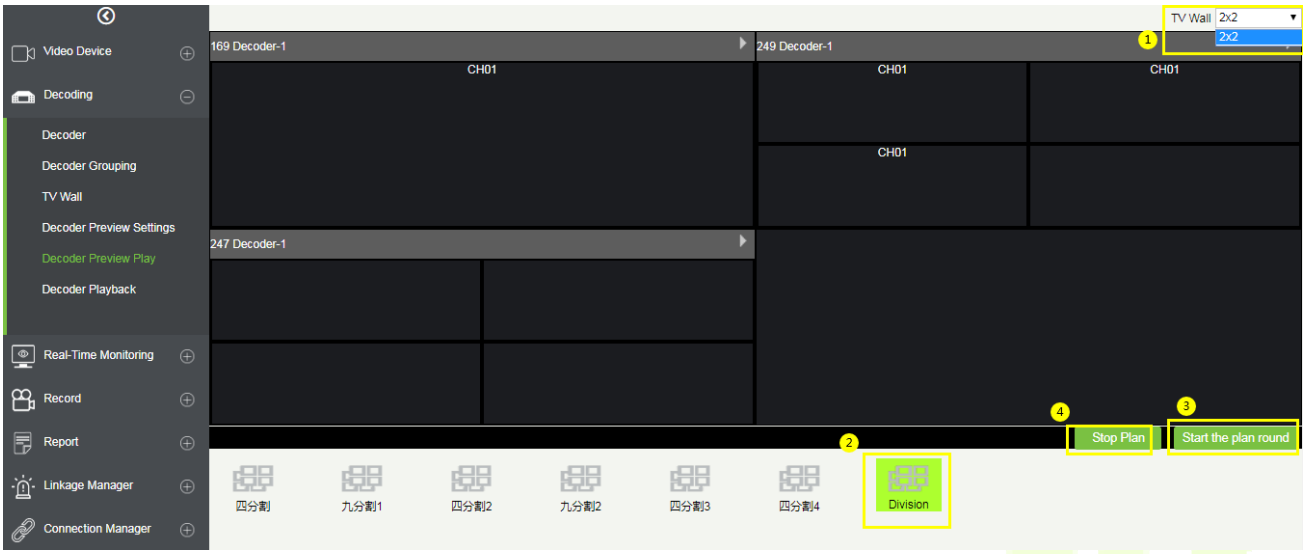


12.2.5 Decoder Preview Play

On the **Decoding** module, click **Decoder Preview Play** to go to the Decoder Preview Play interface.

1. Select a TV wall type from the drop-down list.
2. Click Division (the plan name) to initiate the preview.
3. Click Start the plan round and the display connected to the decoder will perform the video roving.

Note: There is no default video available in the software.



12.2.6 Decoder Playback

On the **Decoding** module, click **Decoder Playback** to go to the Decoder Playback interface.

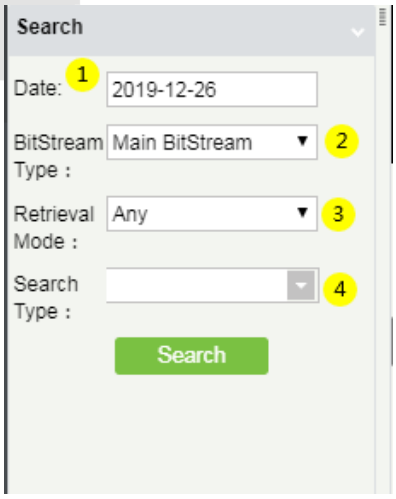
- **Functions and Operations**

1. **TV Wall** - The upper right corner is the TV wall, and the binding relationship between the TV wall and the video device can be selected.
2. **Device and Storage Server** - Select the required video from the Device or the Storage server on the left upper column of the interface.
3. **Search**:

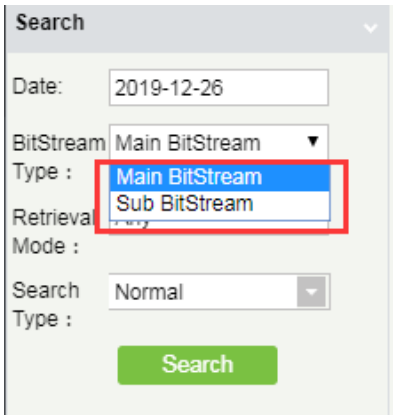
Search the video channels in the bottom left of the interface, which filters the search video types.

You can search for different videos according to four different conditions.

Date: Search by the required date.



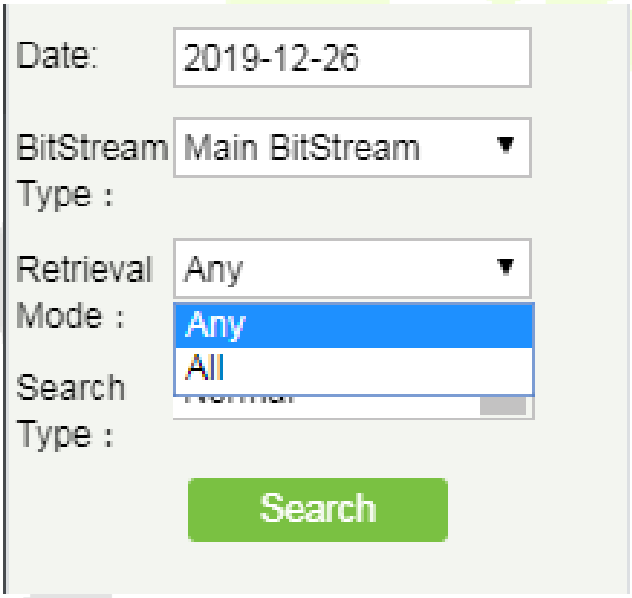
Bitstream Type: Select either Main BitStream or Sub BitStream from the drop- down list.



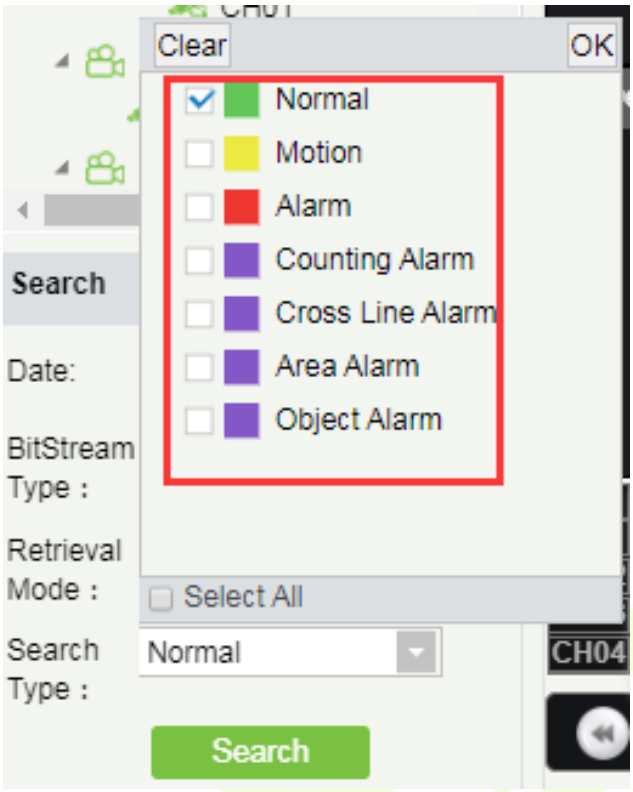
Retrieval Mode: Select either **Any** or **All** from the drop- down list.

All: If the Retrieval mode is **All**, then all the alarm options will be selected in the **Search type** field, and the **Search** function searches and retrieves the videos that meet all the alarm options.

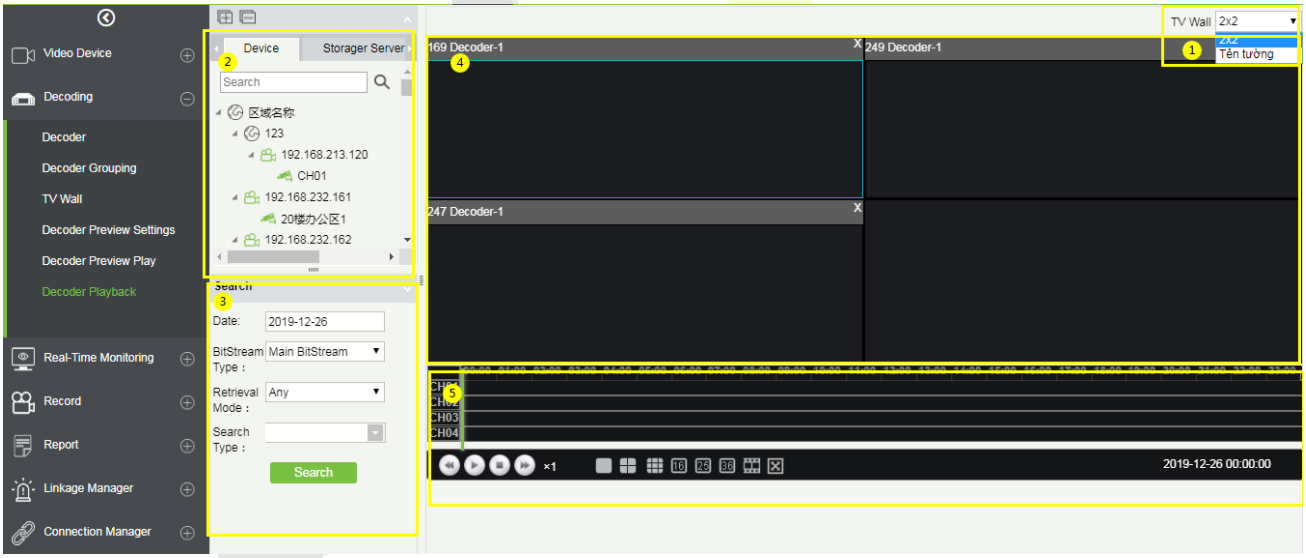
Any: If the Retrieval mode is **Any**, then the **Search** function searches and retrieves only the videos that meet the checked-in alarm options.



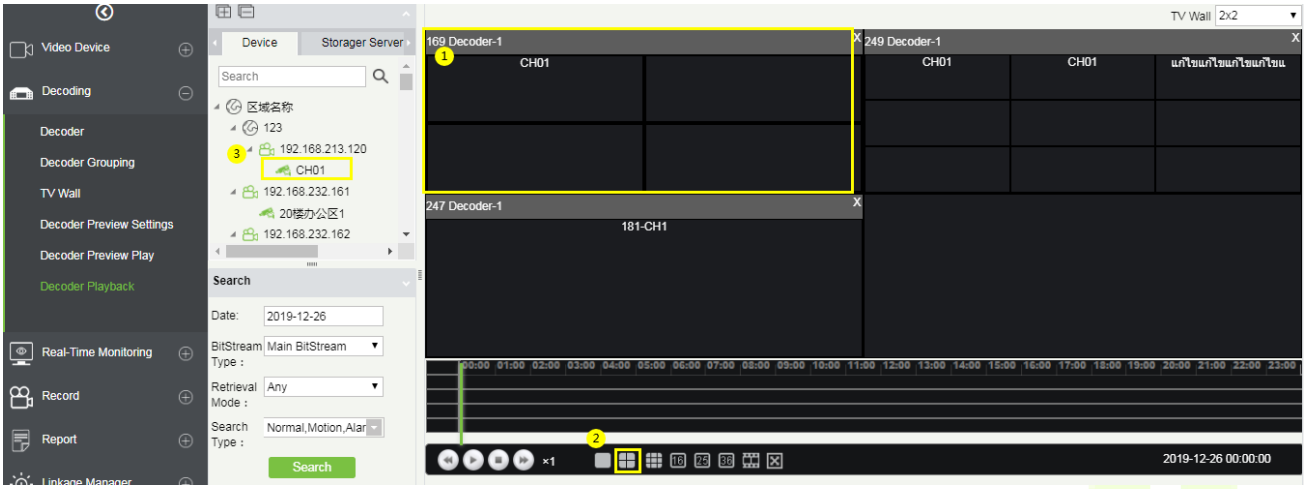
Search Type: You can choose Normal, Motion, Alarm, Counting Alarm, Cross Line Alarm, Area Alarm and Object Alarm.



4. The Decoder displays the selected video.
5. The lower right corner is the playback control panel.



You can even split the screen by choosing the matrix option below and then add the video channel to the corresponding split screen.



12.3 Face Recognition

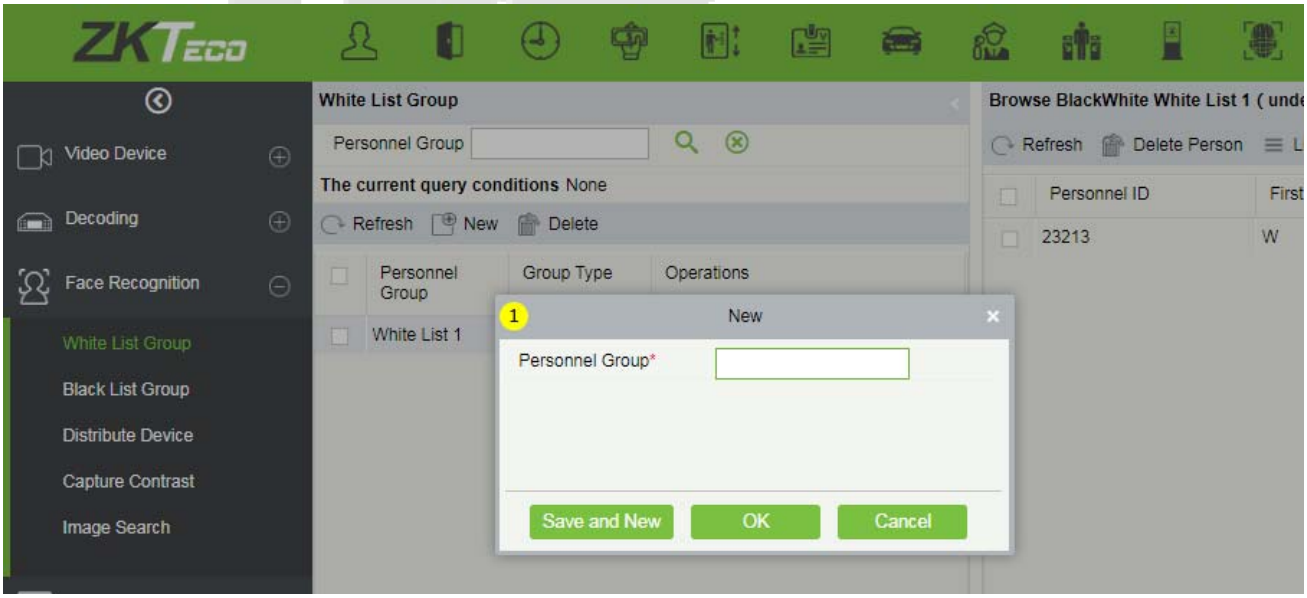
The face recognition module is mainly used to manage the face NVR function, which can be used for the control and monitoring of black and white list. It can view the results of the camera capture, identify in real time, and can support the image search.

12.3.1 White List Group

- **White List Group Management of Personnel:**

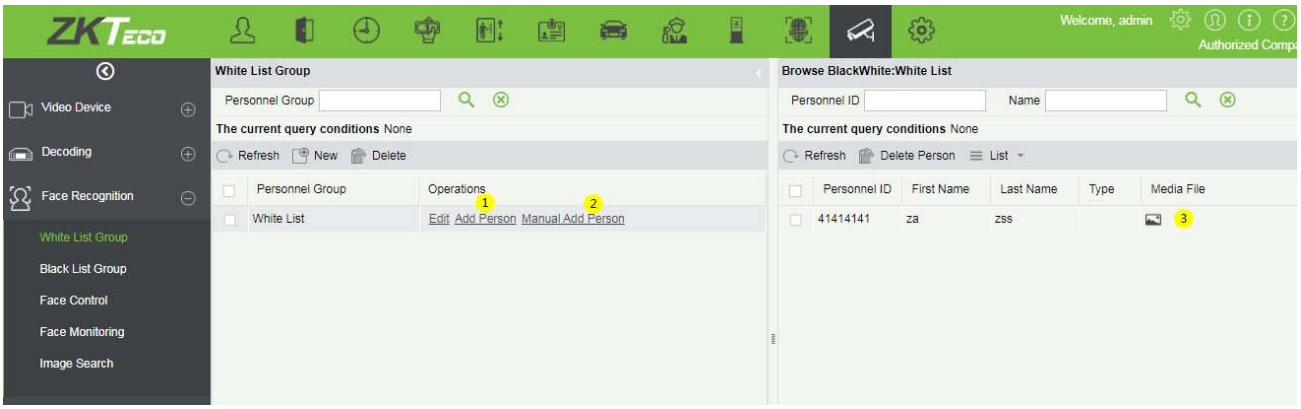
On the **Video Device** interface, click **Face Recognition**, then click **White List Group**, and then click **New** to add a new white list group.

Enter the Personnel Group name and click **OK**.

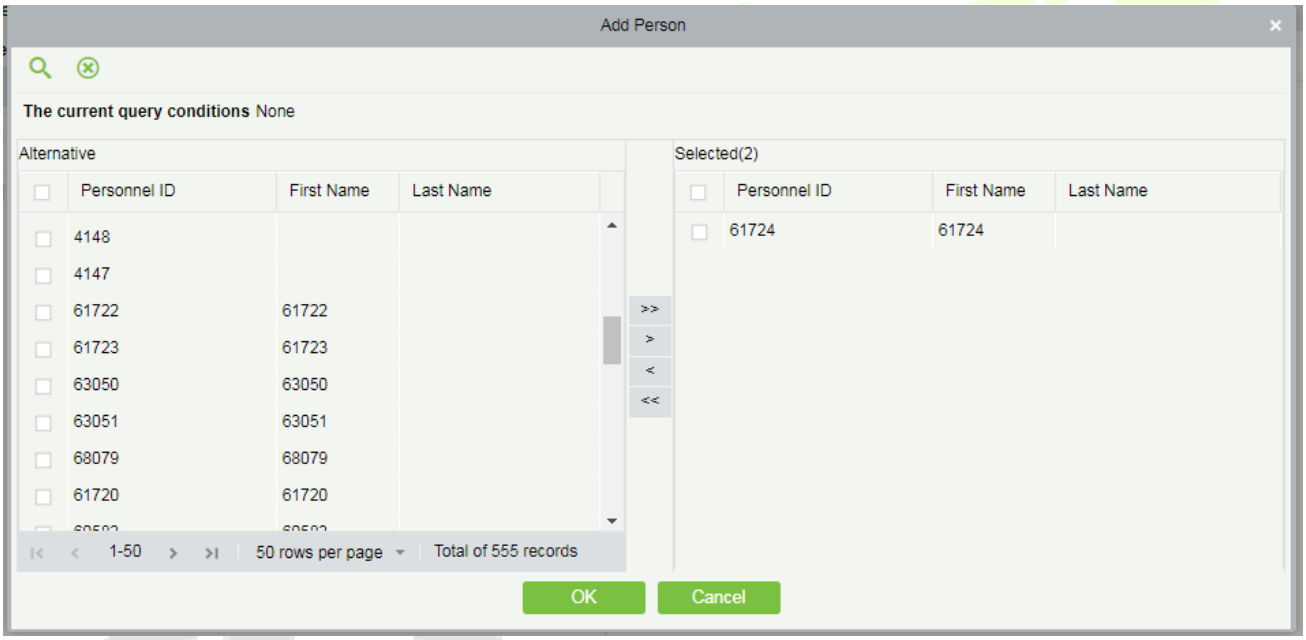


- **Add Person**

On the **White List Group** interface, click **Add Person** to add the personnel to the white list group.



On the **Add Person** window, select the required Personnel ID from the left side, then click the > button to move the selected Personnel to the right side of the Add Person, and then click **OK** to update the selected Personnel ID to the White List Group.

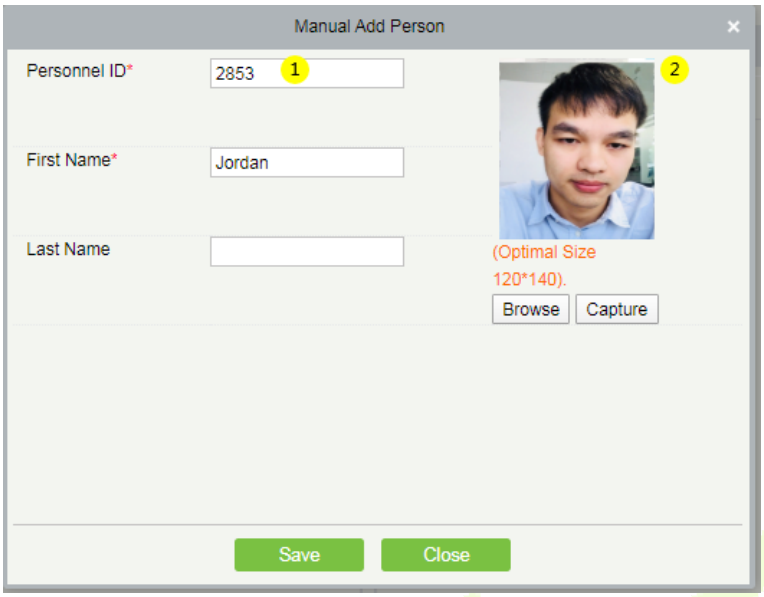


Manual Add Person

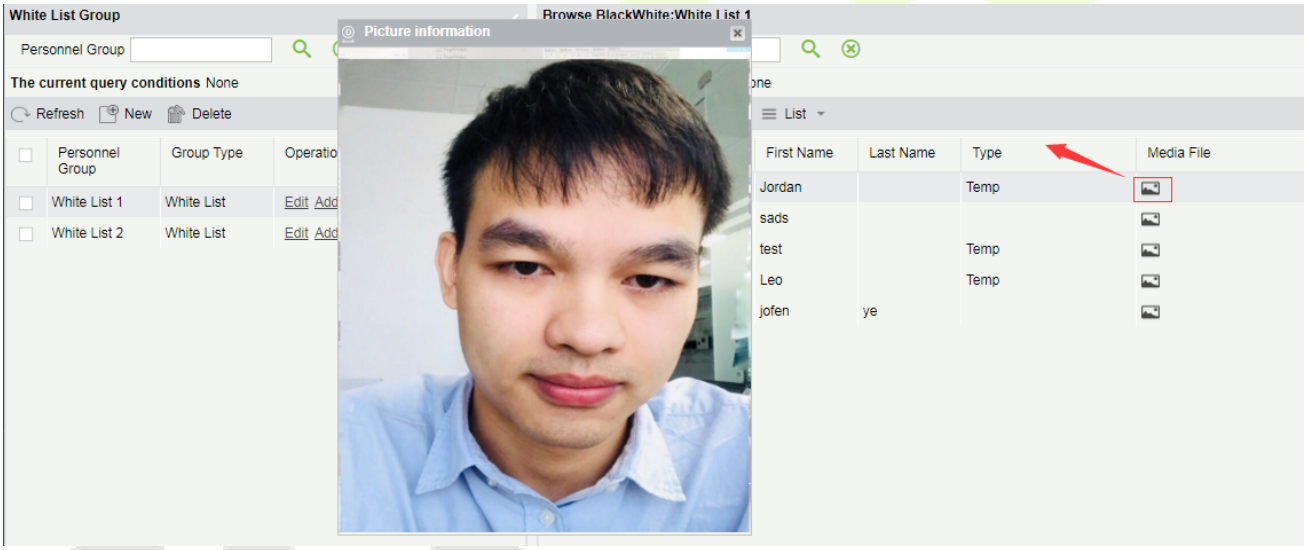
On the White List Group interface, click **Manual Add Person** to temporarily add the personnel to the white list group.

On the **Manual Add Person** window, enter the required Personnel ID, First Name, Last Name, and then click **Save** to manually update the Personnel ID to White List Group.

The temporarily added personnel will not be synchronized to the personnel module of the system, so the Personnel ID can be same as the system personnel. To add a temporary whitelist, you must select a photo of the person.



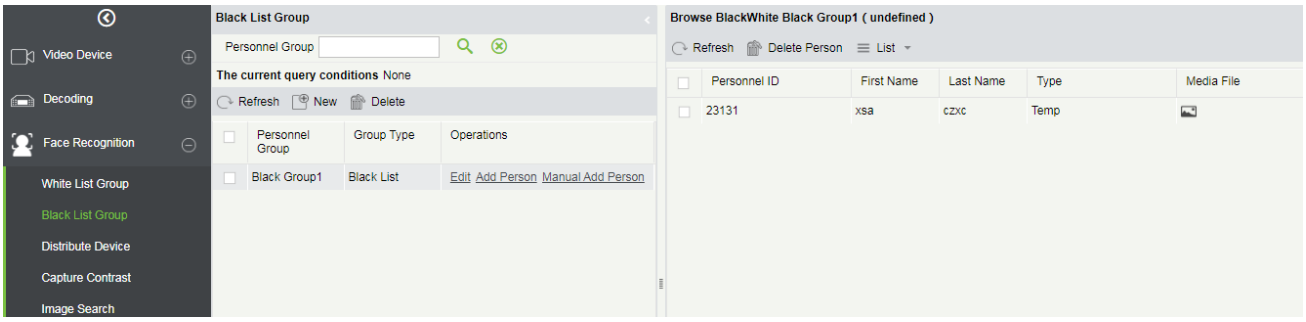
Click the image button to enlarge and view the photos of whitelist.



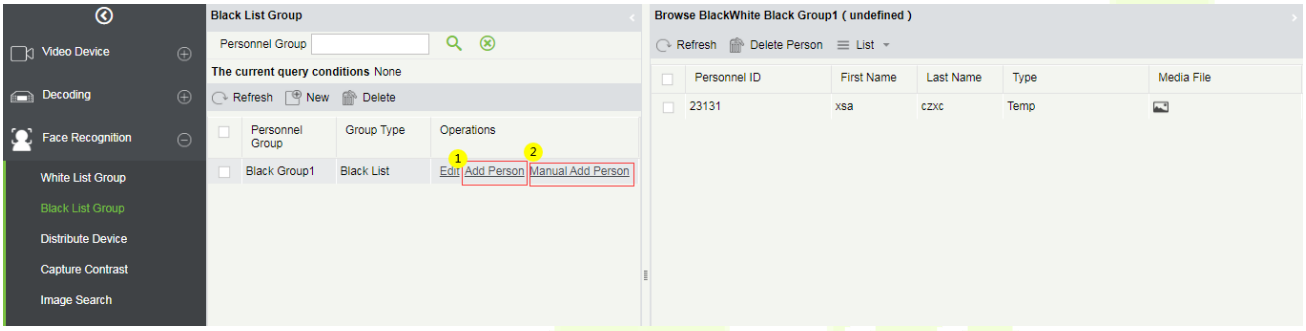
12.3.2 Black List Group

Blacklist group management of personnel:

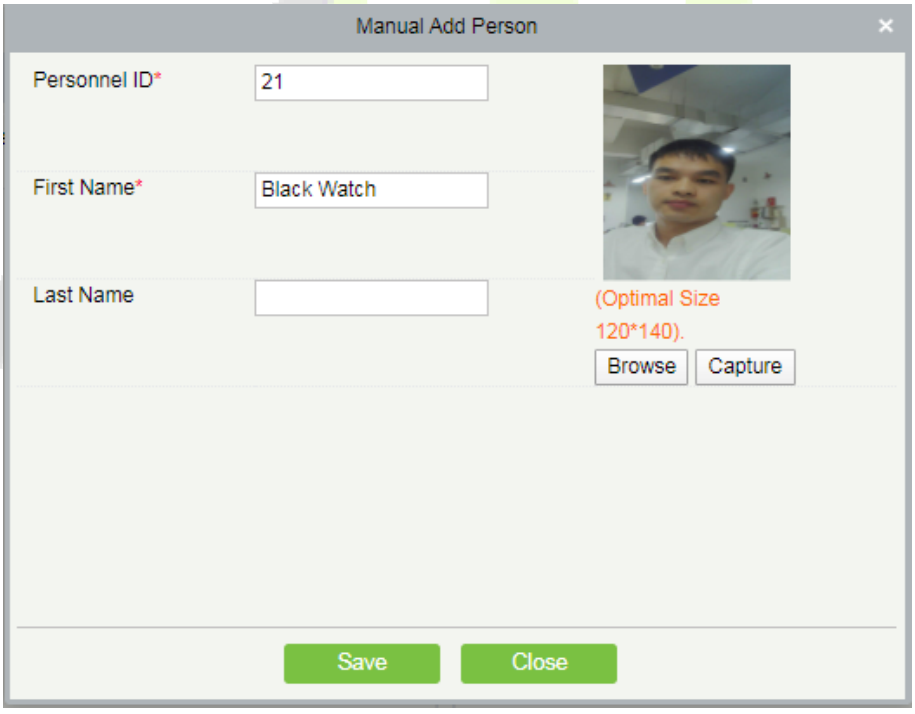
On the **Video Device** interface, click **Face Recognition**, then click **Face Recognition** -> **Black List Group** -> **New**, add a new group, fill in the group name, and click **OK** to confirm.



To manage blacklist personnel, you can ① add existing personnel in the ZKBioSecurity system to the blacklist group; ② you can temporarily add personnel to the blacklist group for control.

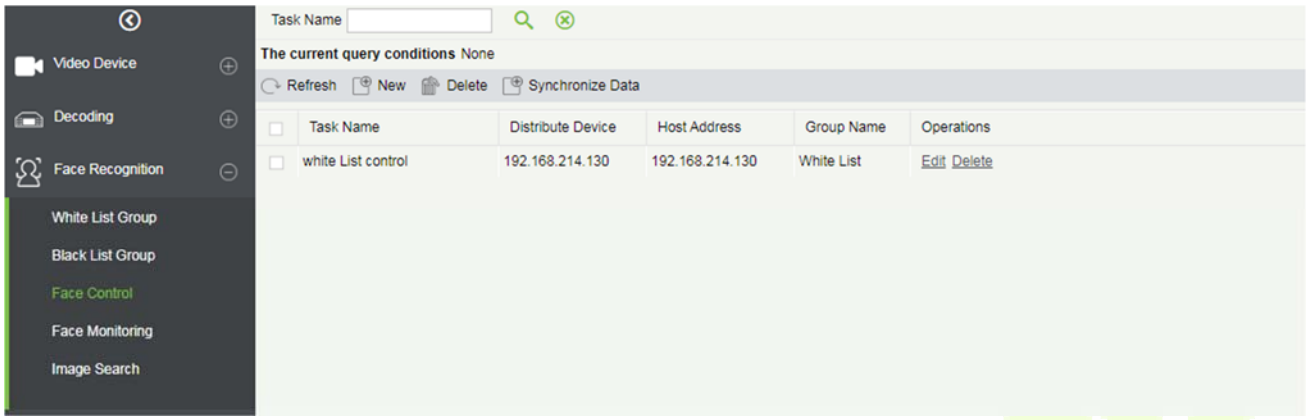


Click ② to temporarily add a blacklist. To temporarily add a blacklist, you must add a photo.



12.3.3 Face Control

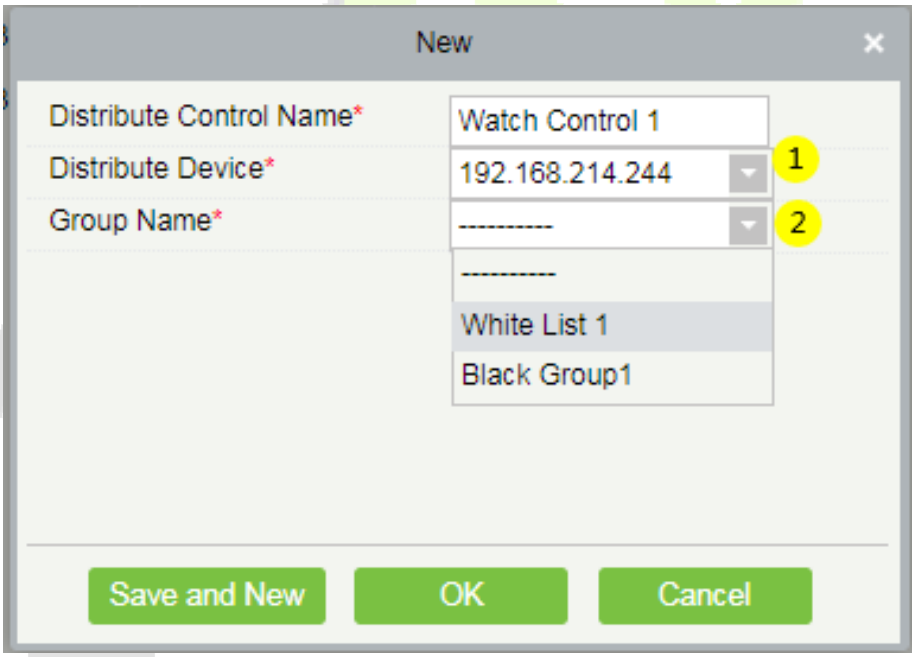
It is used to deliver black and white list groups to NVR devices that support face recognition.



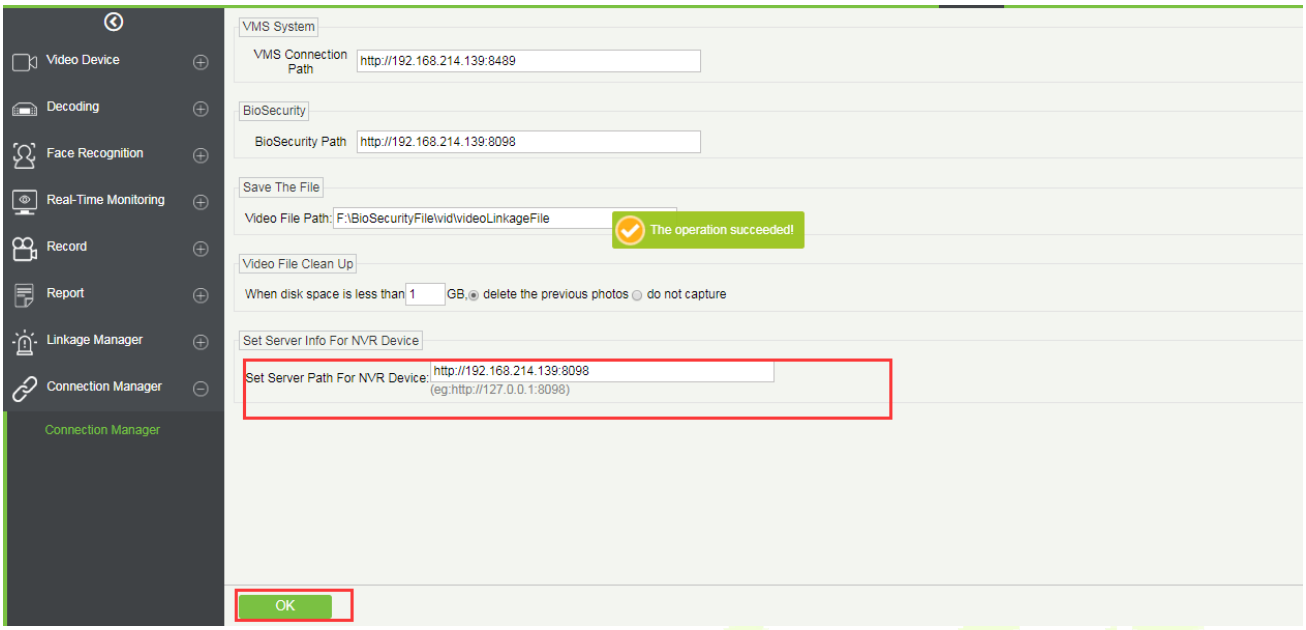
Click **Face Recognition** > **Distribute Device** > **New** to add a device group for black and white list assignment.

①Select the NVR device that needs to send the black / white list.

②Select the black / white list group that needs to be sent.



✍**Note:** When adding new NVR to server each time, it is required to click [OK] again, to save the Server info for NVR device on the "Connection Manager" interface, so that the black and white list can be sent to the corresponding new face NVR.



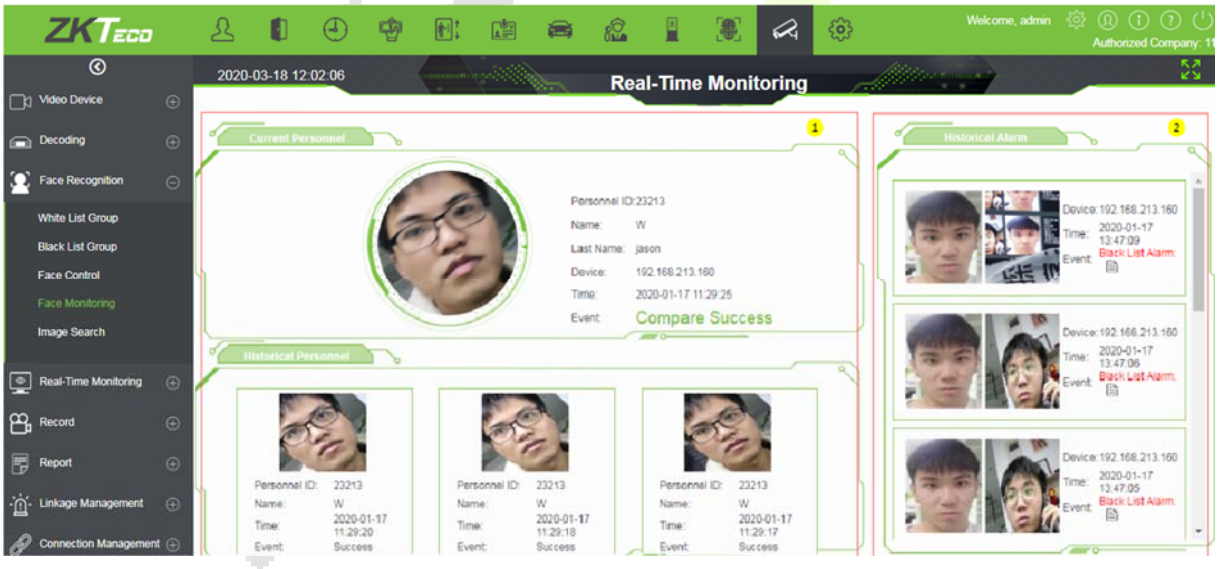
12.3.4 Face Monitoring

Real-time monitoring of NVR and its camera to capture and contrast the black and white list personnel.

①Monitors and displays the Whitelist Personnel List.

②Monitors and displays the Blacklist Personnel List.

③Full screen monitoring.



Note: If the person is neither in the white list group nor in the black list group, then the person will appear on the alarm list on the right with "Stranger Alarm".

Click the button on the Black List Alarm list to view specific alarm details.

Click ① to view the real-time monitoring screen; click ② to view the video alarm recording.

- Real-Time Monitoring Screen.

- View the video record within 10 seconds before and after the Alarm.

①Play the video in the device.

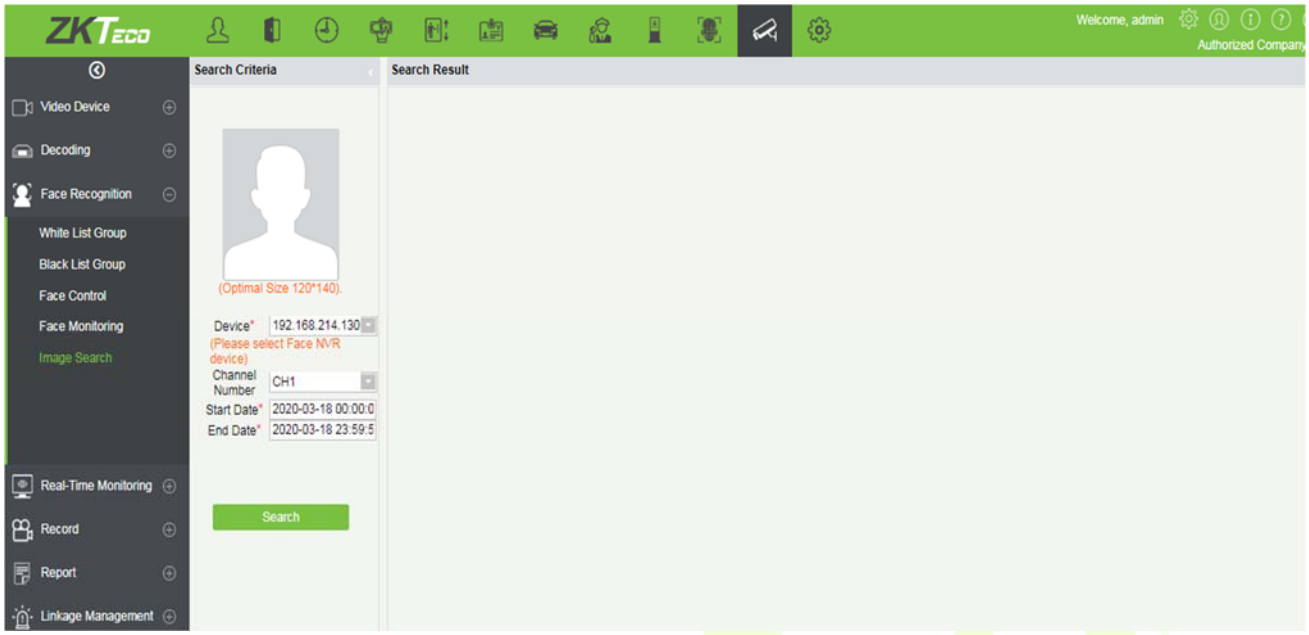
②Play the video in the storage server;

③View the video in full screen.

④Click Download to download the video.

12.3.5 Image Search

You can search for matching faces captured by related NVR and camera devices by uploading photos of personnel.

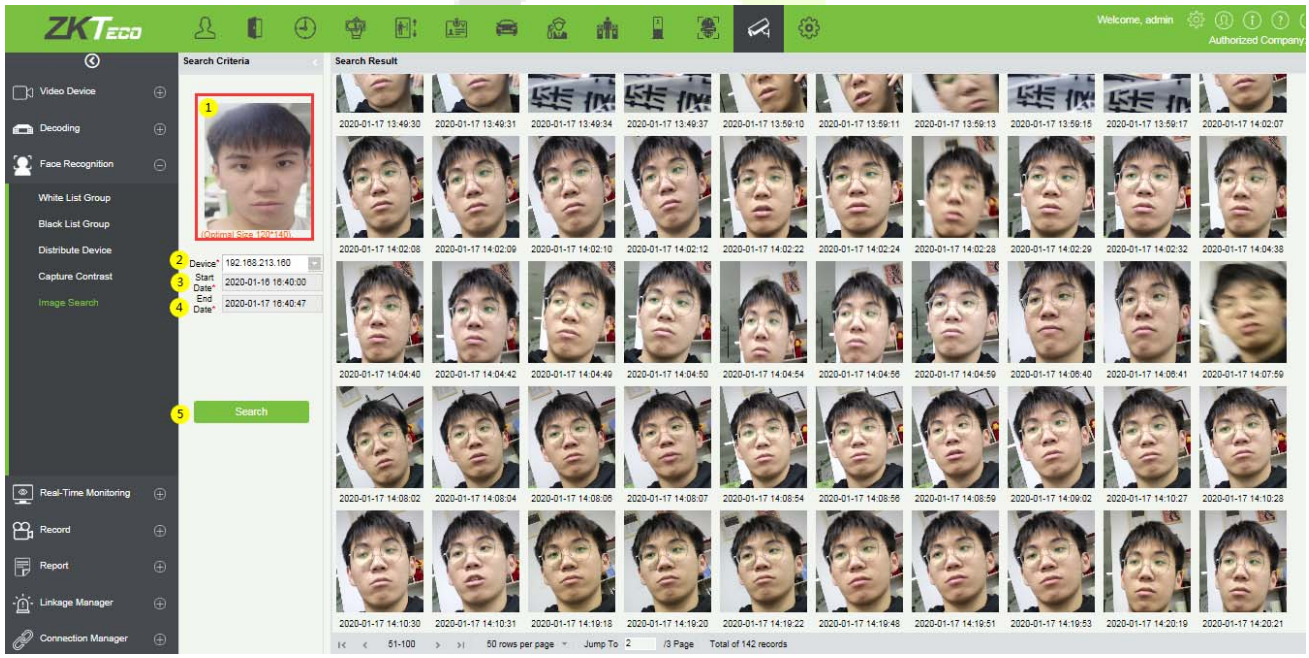


Upload Image: Click to upload photos of personnel who needs to be searched.

Device: Select the devices to be searched from the drop-down list.

Start Date and End Date: Enter the start and end date to search, and then click **Search** to search.

The results will be listed on the right side of the interface.



12.4 Real-Time Monitoring

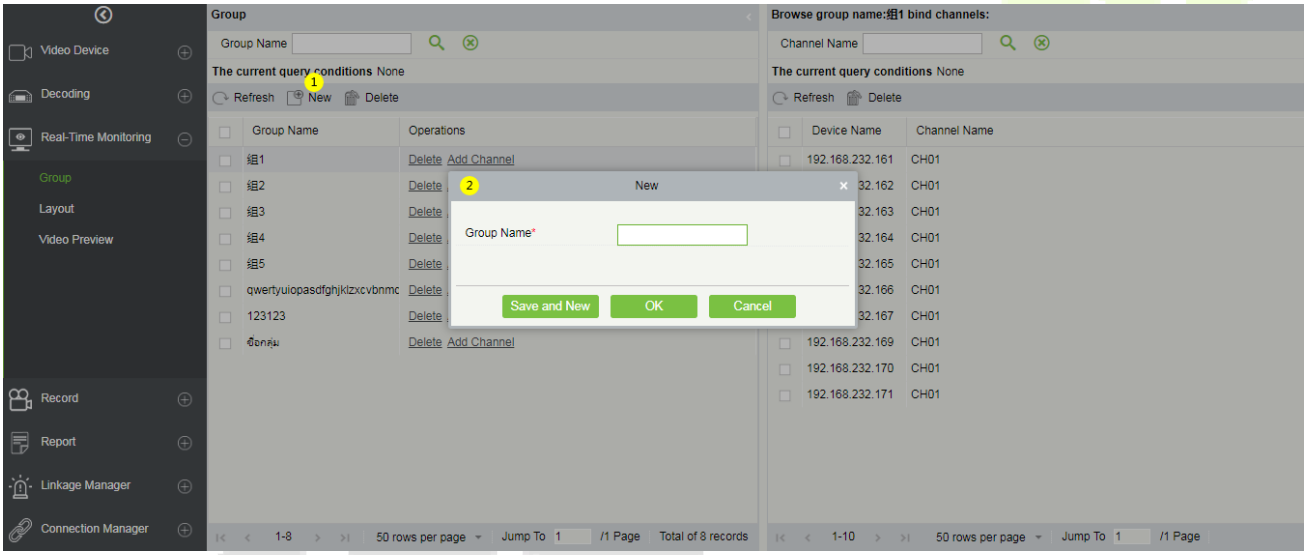
The real-time monitoring menu has three sub-menus, Group, Layout, and Video Preview.

The group and layout settings are for the third menu-preview. You can choose to preview in the form of group and layout.

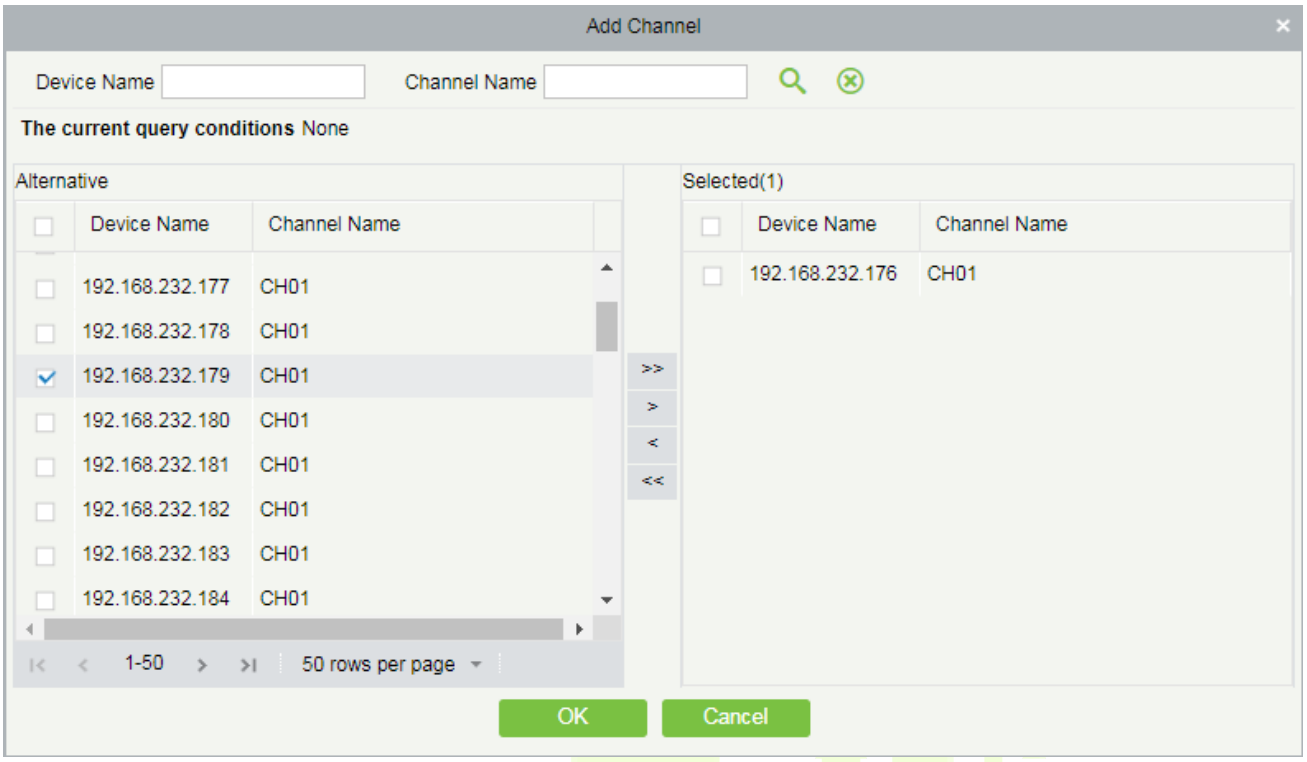
12.4.1 Group

It can manage video channels in groups.

Click **[Group]** > **[New]** to add a new group, fill in the **Group Name,** and click **[OK]** to confirm.



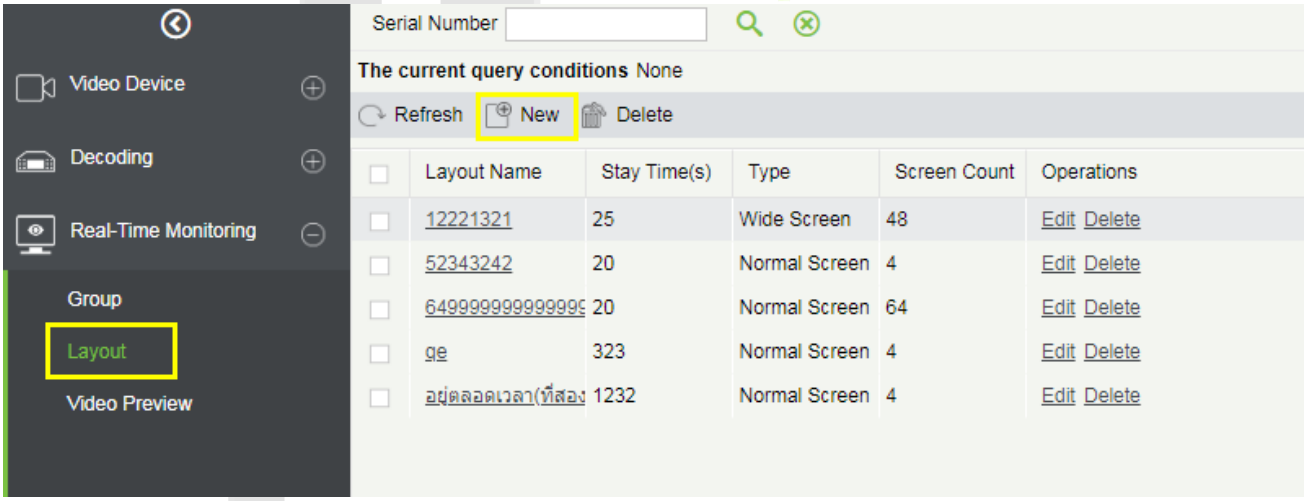
Click [**Add Channel**] to add video channels to this group.



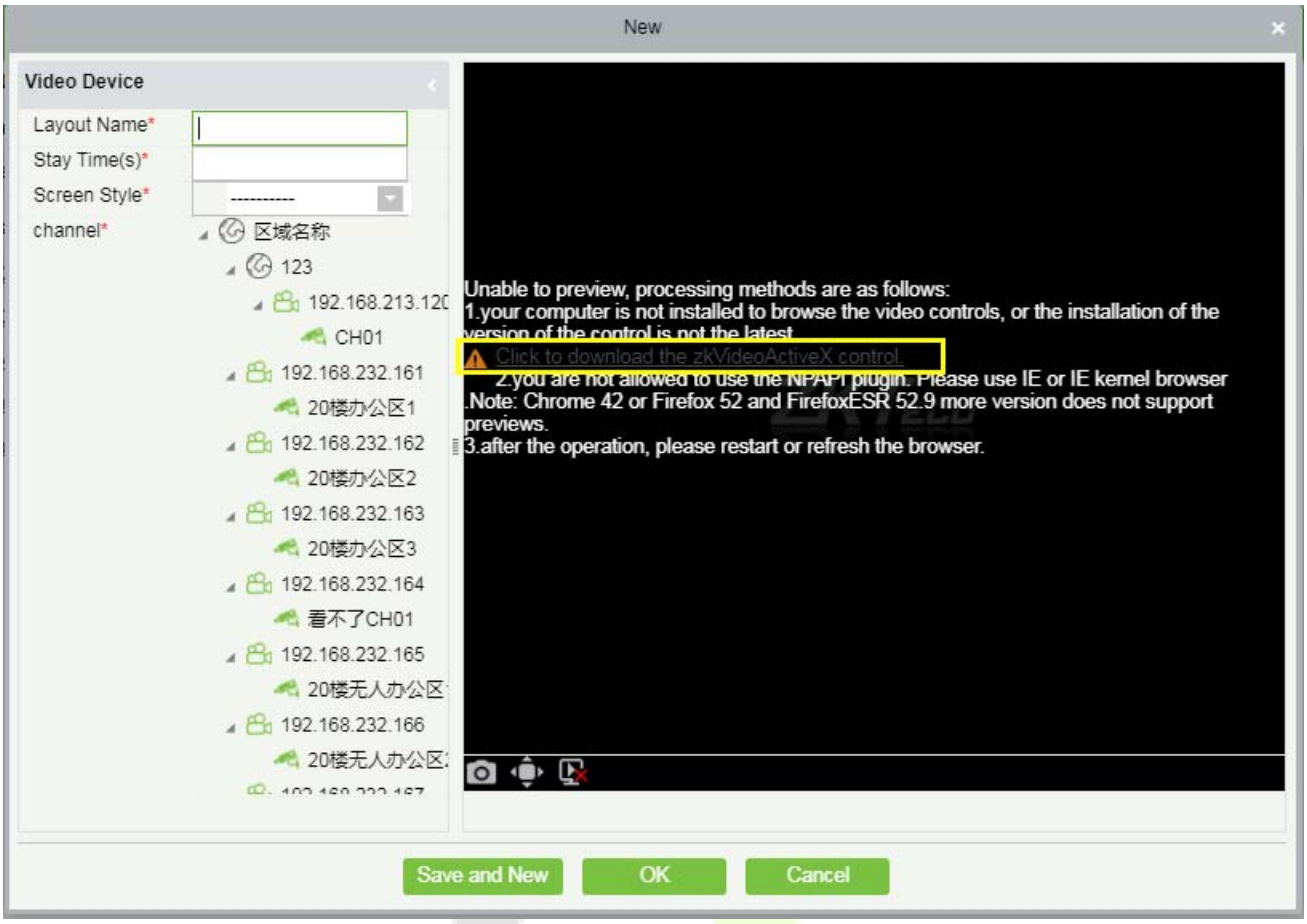
12.4.2 Layout

It sets the display style of the OCX and displays the bound video channels.

Click **[Layout]** -> **[New]** to add layout settings.



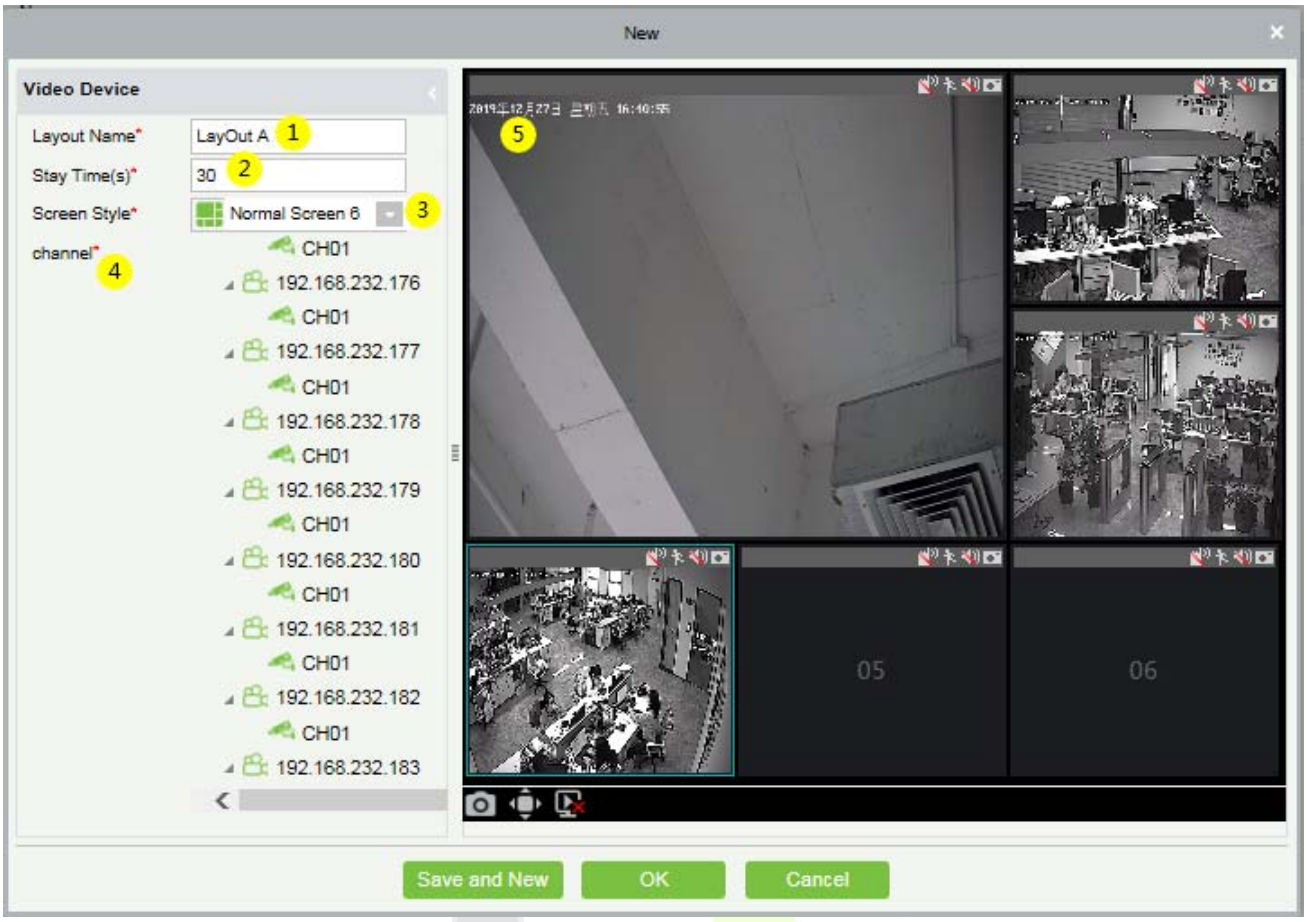
For the first time users, click "**Click to download**." and install the "zkVideoActiveX" plugin.



- **Add layout settings:**

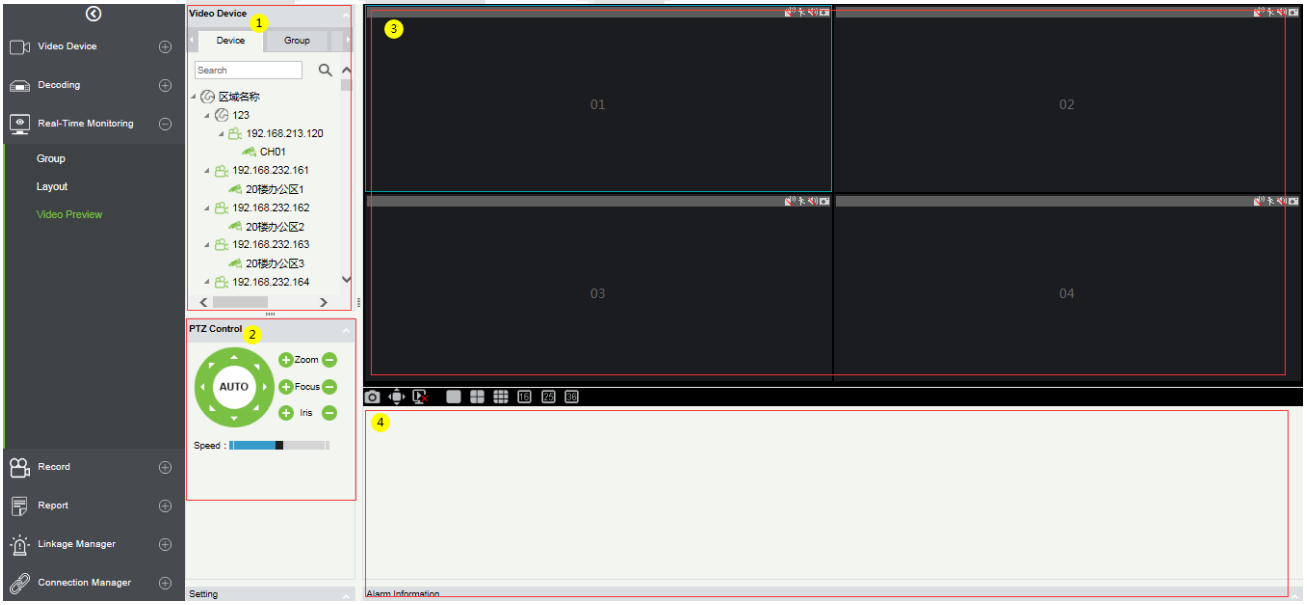
① Fill in the **Layout Name** on the left, ② Fill in the **Stay Time**, the preview time of the video channel set by this layout. ③ Select the **Screen Style** of the layout. There are **Normal Screen** and **Wide Screen** and a variety of screen options.

④ Click on the video **channel** on the left to bind it to the screen on the right ⑤. After binding the screen, a screen will be displayed, click **[OK]** to save.



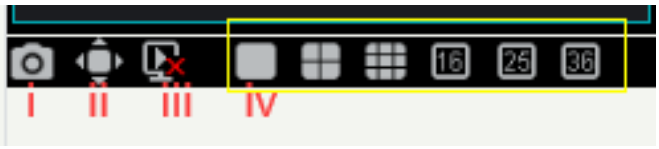
12.4.3 Video Preview

Click **[Real-Time Monitoring]** -> **[Video Preview]** to enter the video preview interface. The video preview interface is divided into four parts.



① Video device selection area.

② Video preview display interface.



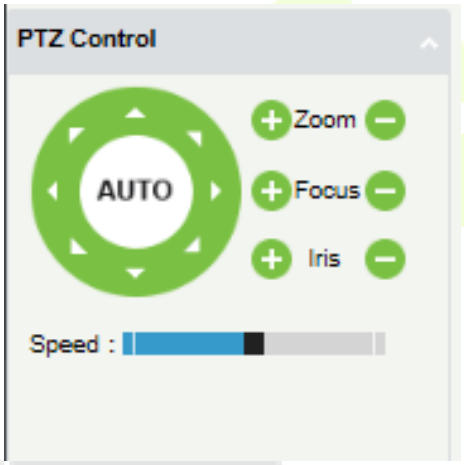
i: Takes a screenshot within the blue frame of the selected screen,

ii: Displays the screen in the full screen preview.

iii: Stops all the preview screens,

iv: Different split screen options.

③ PTZ Control: This function is only available for dome camera.



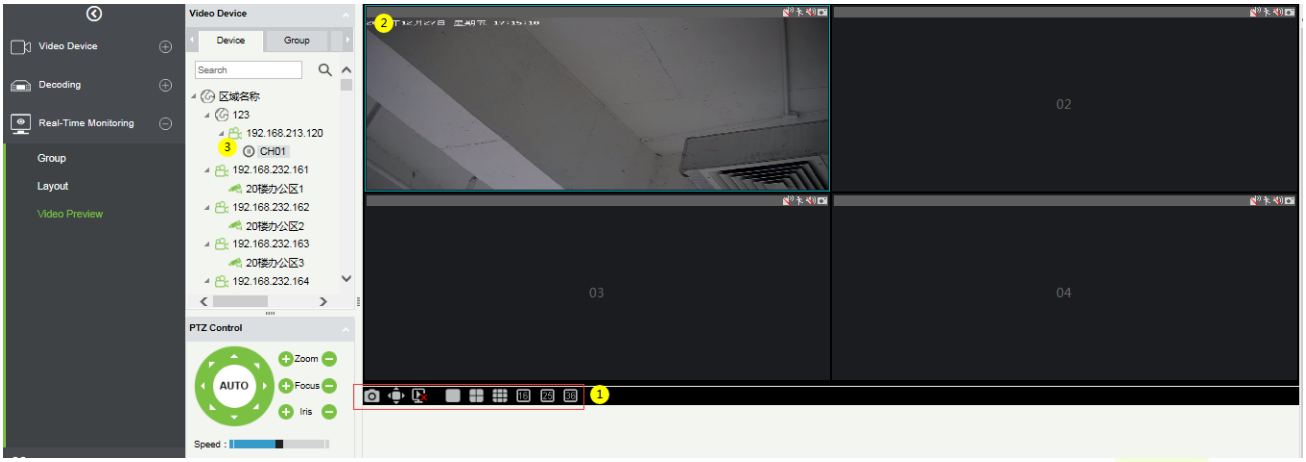
④ Alarm Information list.

There are three tabs in the video device selection area, which are device list, group, and layout.

Online devices are green and offline are gray.

- **Video list for video preview:**

The device list has three levels, which are area, device, and channel. ① Select the layout to be previewed. ② ③ Left-click an online channel to play the corresponding channel's screen on the right preview window (blue frame). Click again to stop playback.



Group Video Preview:

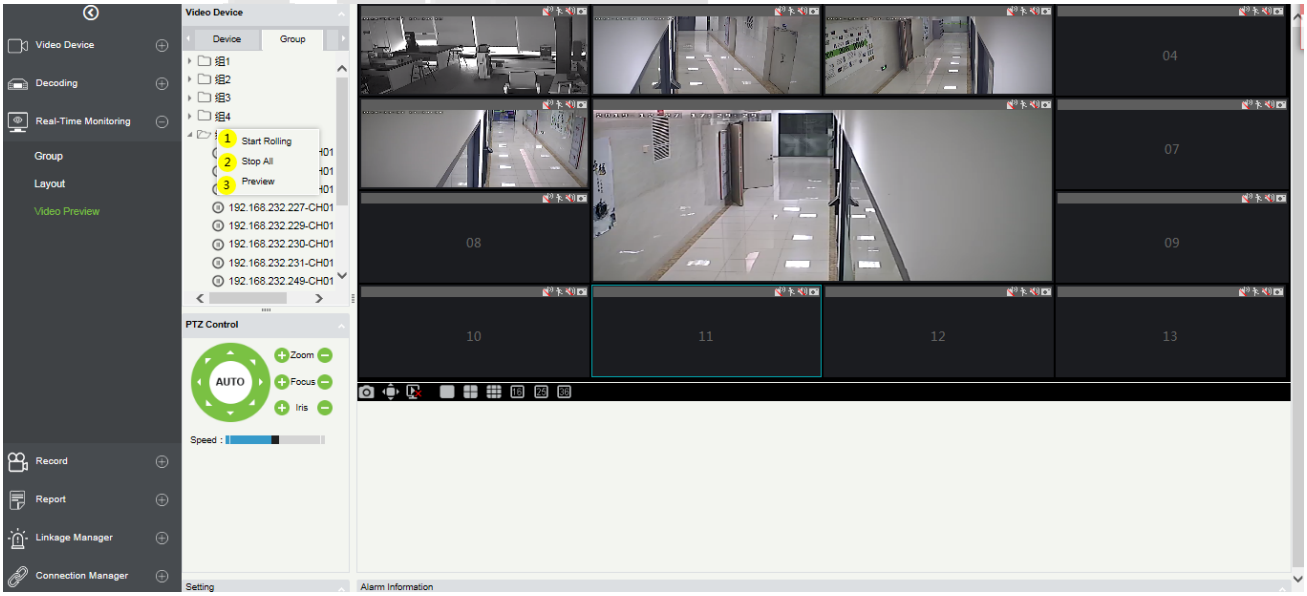
Click [**Group**] in the tab page, here is a list of all the groups set in the [**Group**] menu. Right-click a group and three options will appear, which are [**Start Rolling**], [**Stop All**], and [**Preview**].

① **Start Rolling:** After the round starts, it will automatically start timing (15 seconds) to start the group switching preview from the selected group.

For example, group 5 is currently selected. The preview screen on the right will preview this group first, and then switch to preview group 1 after 15 seconds, and then preview group 2, group 3 group 5 group 1 after 15 seconds and keeps looping.

② **Stop All:** Click to stop rolling and preview.

③ **Preview:** Play the group monitoring screen on the preview screen on the right. Offline devices will not display the preview screen.



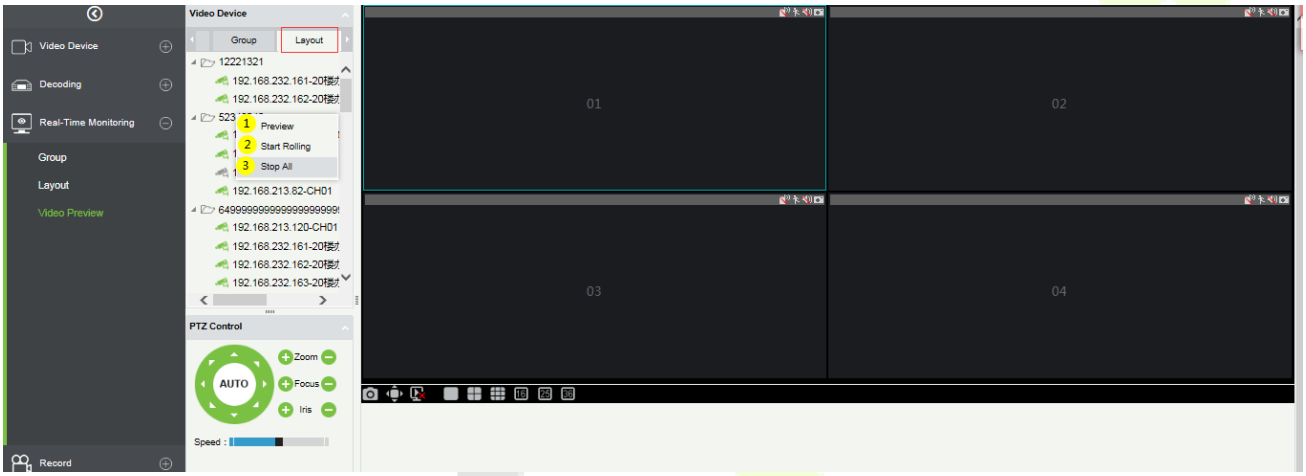
- **Layout Video Preview**

Click [**Layout**] in the tab page, here is a list of all the layout settings that have been set in the [**Layout**] menu. Right-click a layout and three options will appear: [**Preview**], [**Start Rolling**], and [**Stop All**].

① **Preview:** Play the layout monitoring screen on the preview screen on the right. The offline devices will not display the preview screen.

② **Stop all:** Click to stop rolling and preview.

③**Start Rolling:** After the round starts, it will automatically start timing (can be set in Layout) to start the layout switching preview from the selected layout and keep looping.



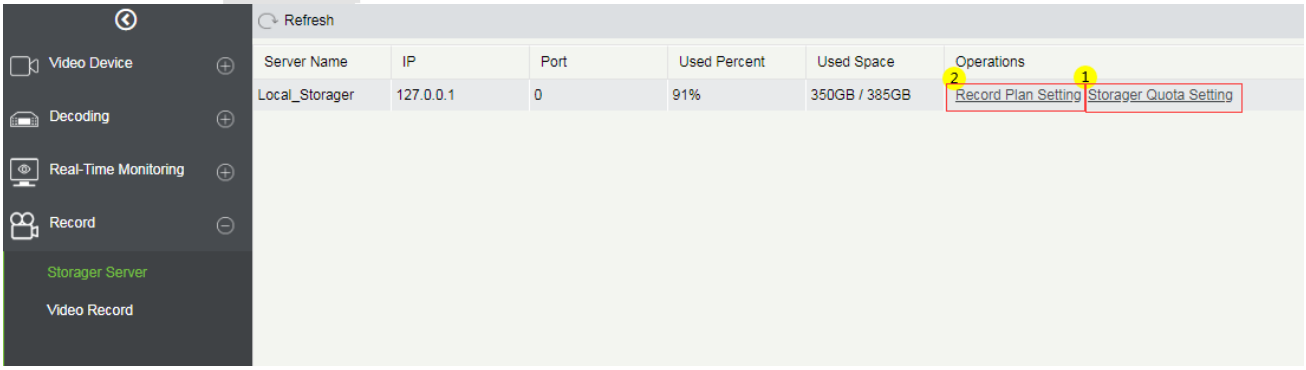
12.5 Record

The record function is mainly used to configure the record plan and view the related video records of the device.

12.5.1 Storage Server

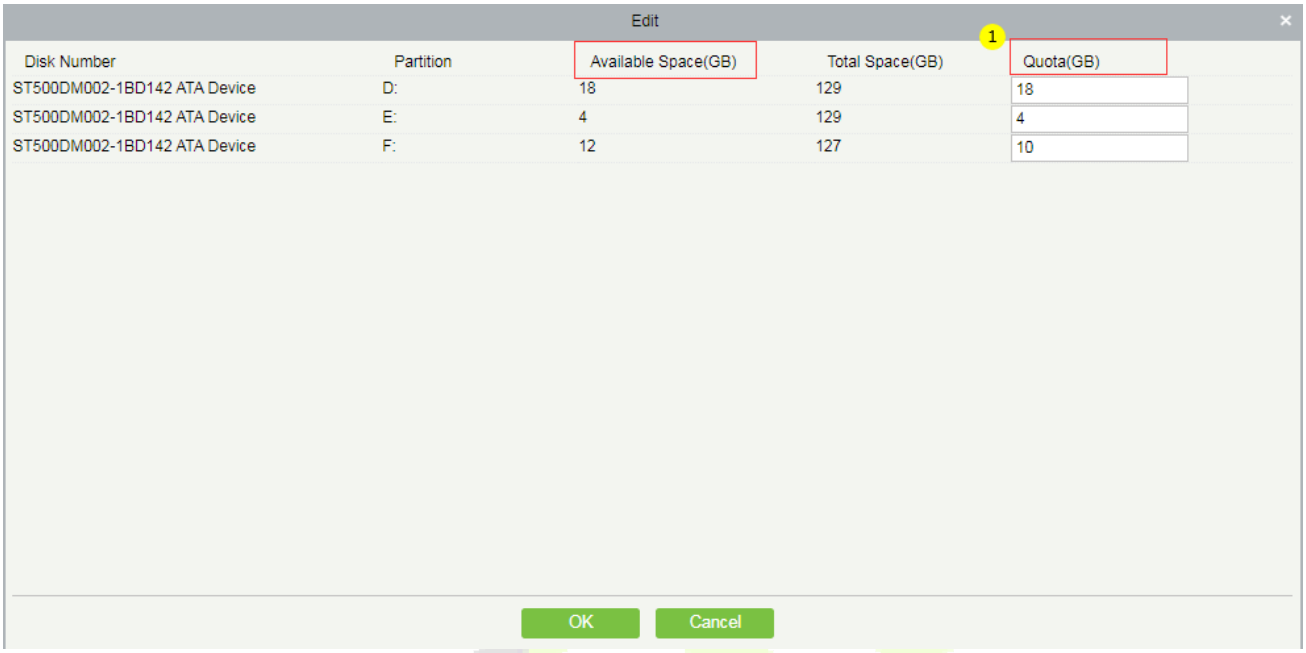
- **Configure the record plan**

Before setting the record plan, you must first configure the storage capacity, otherwise the corresponding records will not be generated.



Click ① **[Storage Server]** -> **[Storage Quota Setting]** to configure the record storage capacity of the VMS server.

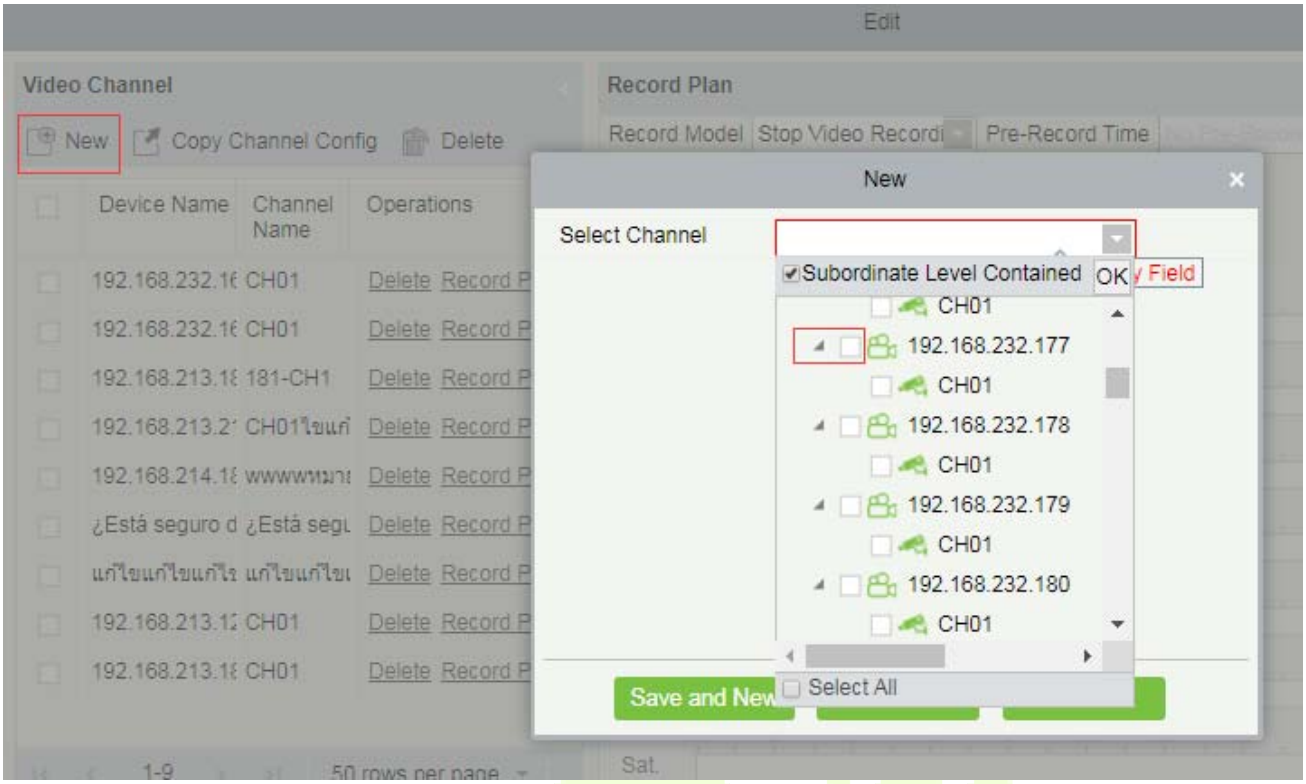
It will obtain the available capacity of the hard disks on the VMS server other than the system disk and configure the disk space for storing videos.



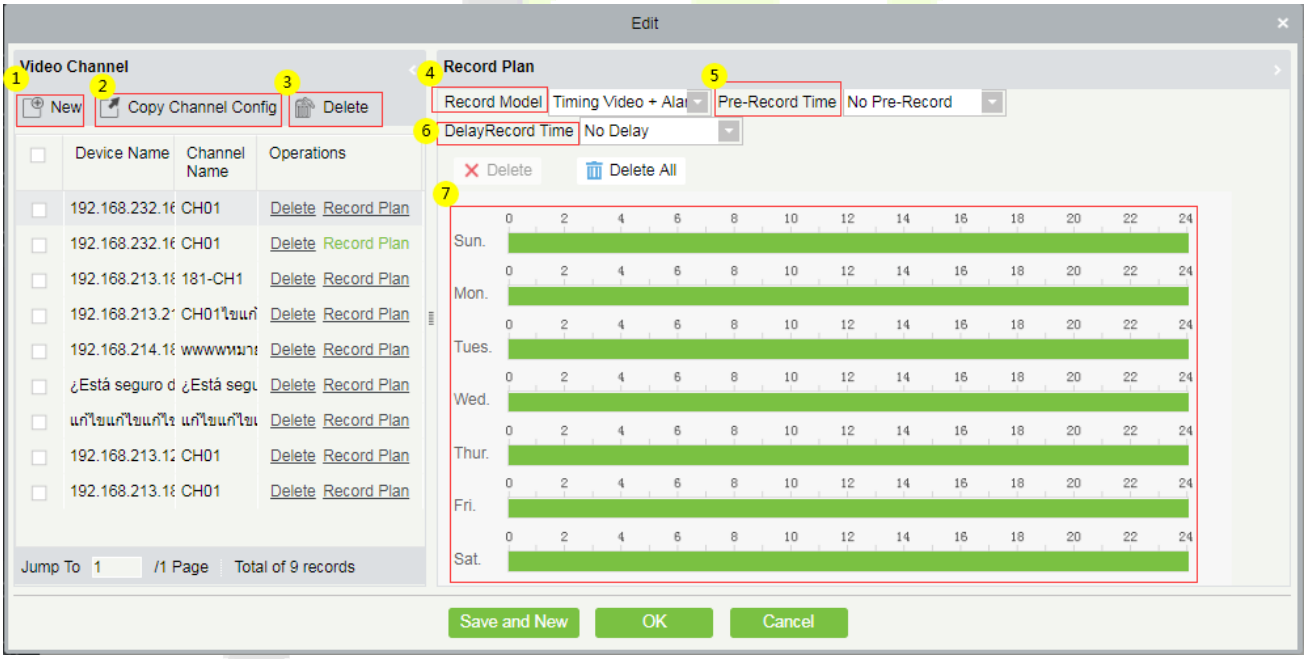
- **Record Plan Setting**

Click ② **[Record Plan Setting]** to enter the record plan setting page.

Click **[New]** to select a video channel to set the record plan.



After selecting the video channel, you can set the corresponding record plan, as shown below:



① Add a record video channel.

② **Copy Channel Config** can copy the record plan of the ⑦ weekly record panel to the selected video channel.

③ Delete the selected record plan;

④ Record Model:

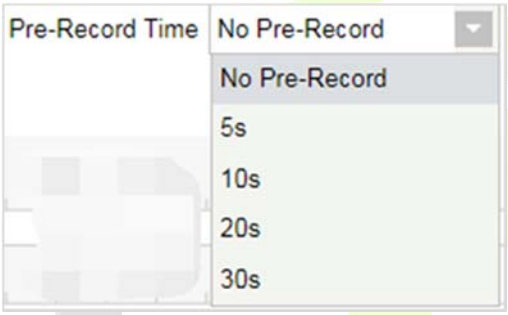
i: Stop Video Recording.

Ii: Timing Video.

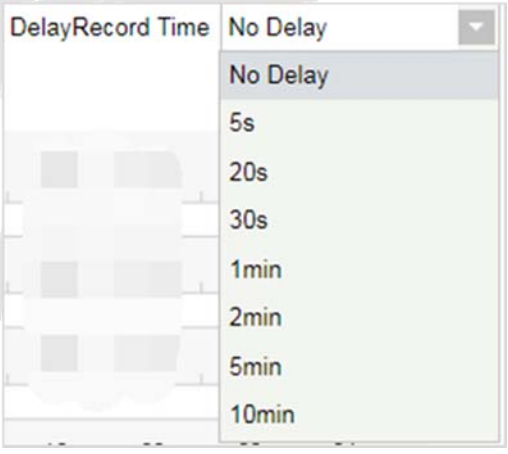
Iii: Alarm Video.

Iv: Timing Video + Alarm Video.

⑤ Select Pre-Record Time: When the record model is in **Stop Video Recording** or in **Timing Video**, the pre-record time should be "**No Pre-Record**" by default.



⑥ Select Delay Record Time: When the recording type is Stop Video Recording and Timing Video, the default delay record time can only be "**No Delay**".



⑦ Record plan panel, drag to select the record time.

12.5.2 Video Record

Video playback can be viewed on the **[Video Record]** interface.

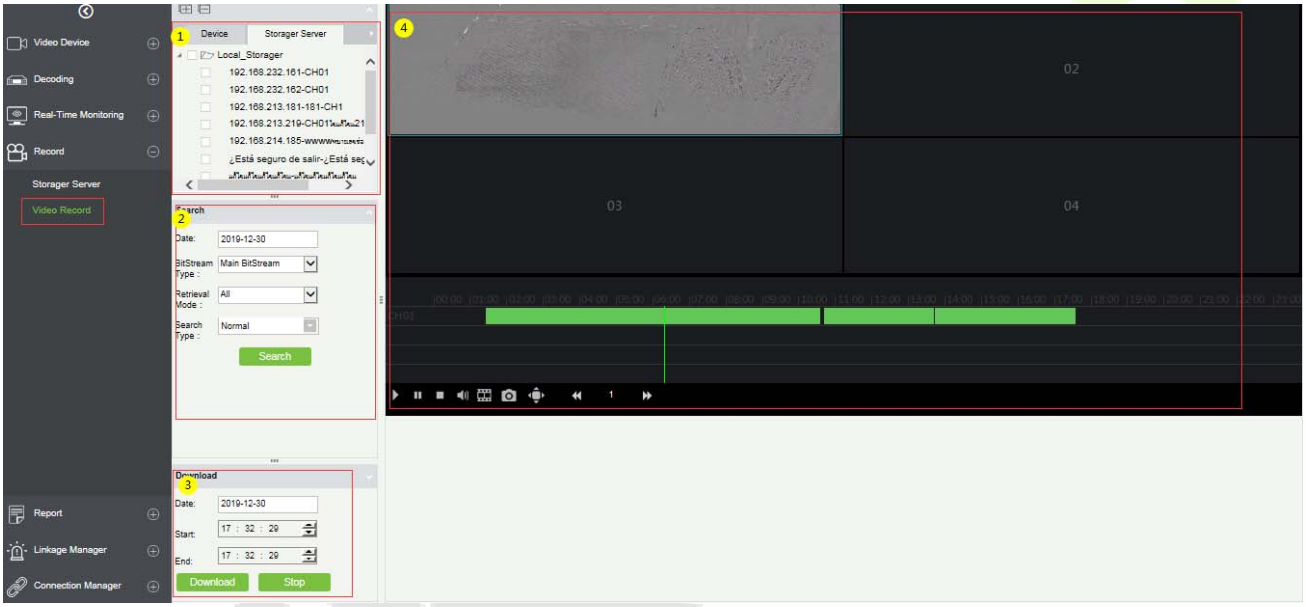
The video playback interface is divided into four areas:

① in the device area, there are two-tab pages, the device list interface and the local storage server.

② Video search area.

③ Video download area.

④ Video playback area.



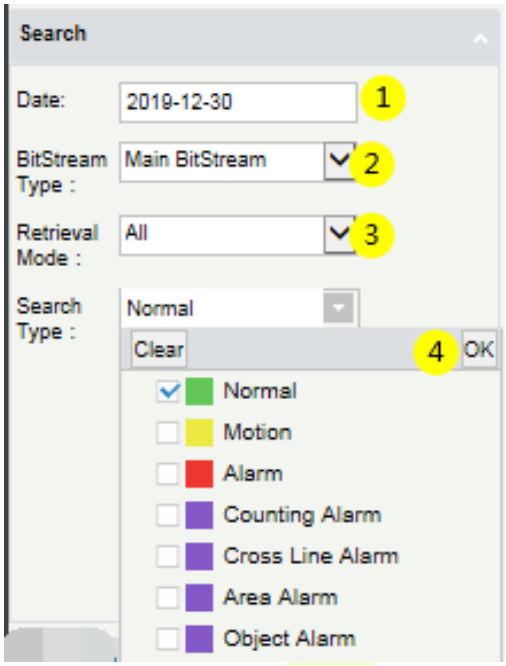
- **Device area:**

Video device selection area, there are 2-tab pages, which are device and local storage server. Online devices are shown in green and offline devices are shown in gray.

Select the video channel to be searched in ①, select the conditions for video search in ②, and click **[Search]** to search for video. If there is a video, it will display the video segment that can be played; if there is no video, it will pop up **[No data]**.

- **Video search conditions:**

There are four search filter conditions: ①Date, ②BitStream Type (Main or sub BitStream), ③Retrieval Mode (Any and All), ④Search Type (there are 7 options, multiple options can be selected).



- **Video download area:**

Before downloading, select the device in the device area, select the date and start/end time of the video ①②③, click Download, if there is no data, it will pop up **[No data]**; If there is a video will directly start to download and show the ④ download progress. After the download is completed, the progress will display **[Download Completed]**.

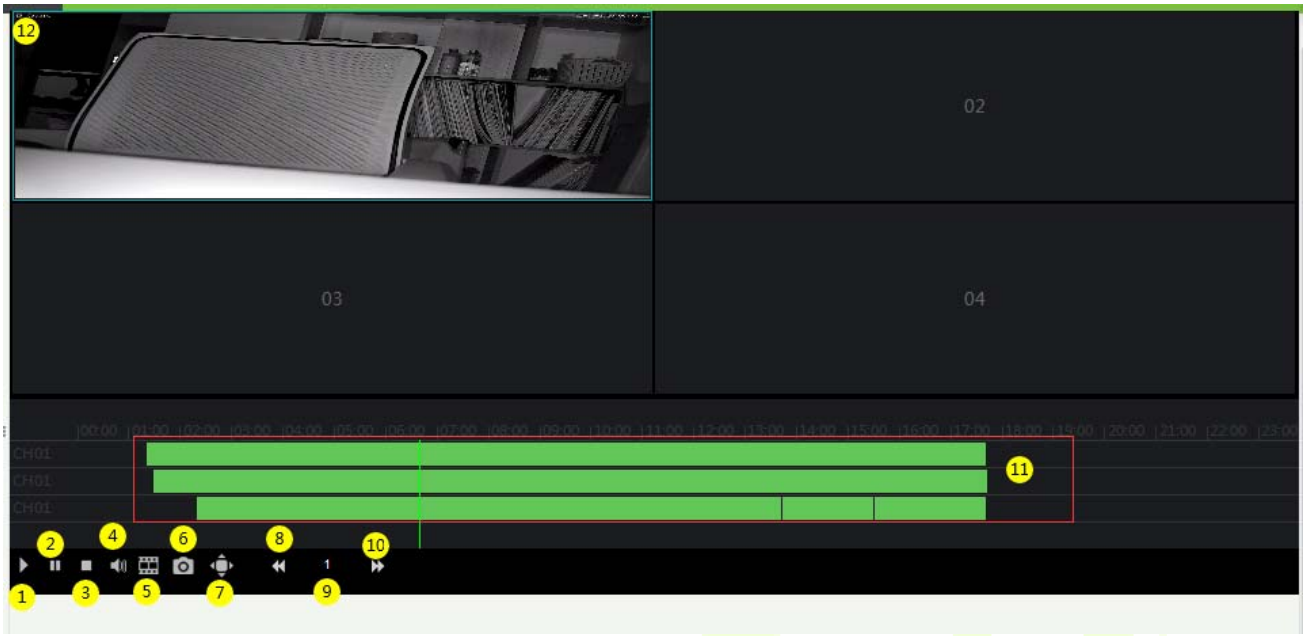
- **Video playback area:**

① Play button; ② Pause button; ③ Stop button; ④ Mute button; ⑤ Play by frame; ⑥ Screenshot button.

⑦ Full screen playback button; ⑧⑨⑩ Double speed adjustment button.

⑪ Play video clips; ⑫ Video playback window.

Note: The video playback area can only play up to 4 videos at the same time.



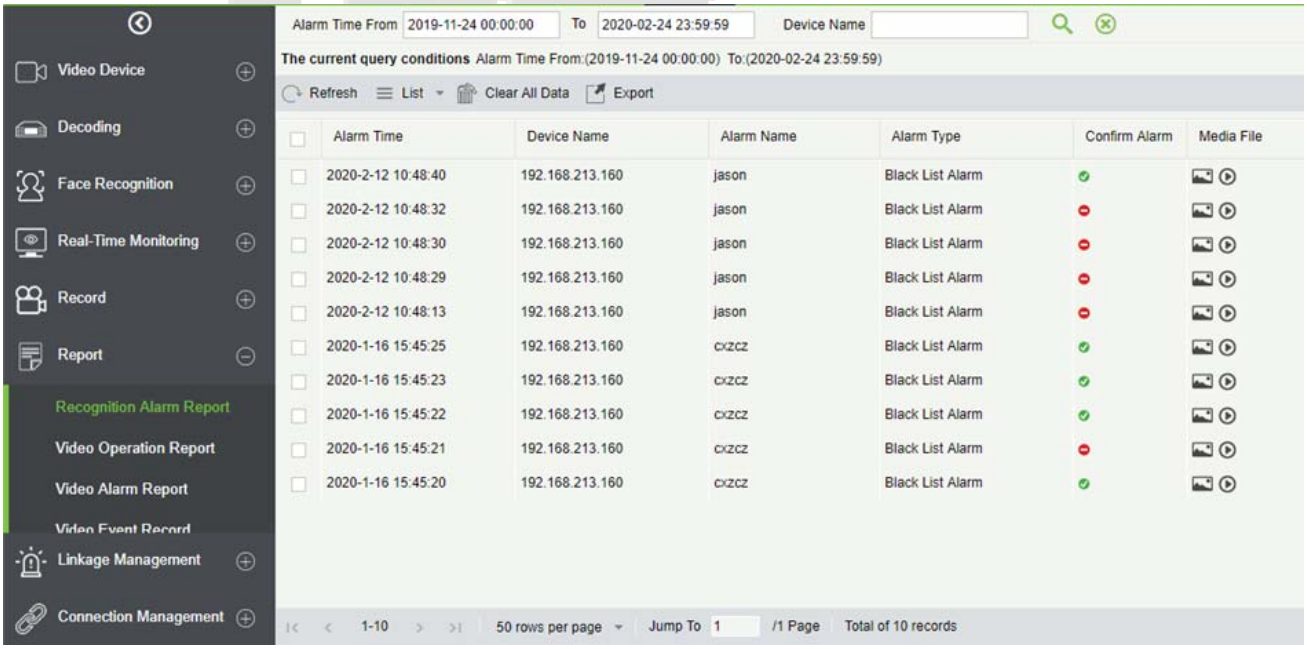
12.6 Report

The report function of the video module can query operation records of the system user on the video device, the video alarm records, facial recognition alarm report, and the video linkage records.

12.6.1 Recognition Alarm Report

It is mainly used to show the facial recognition alarm report.

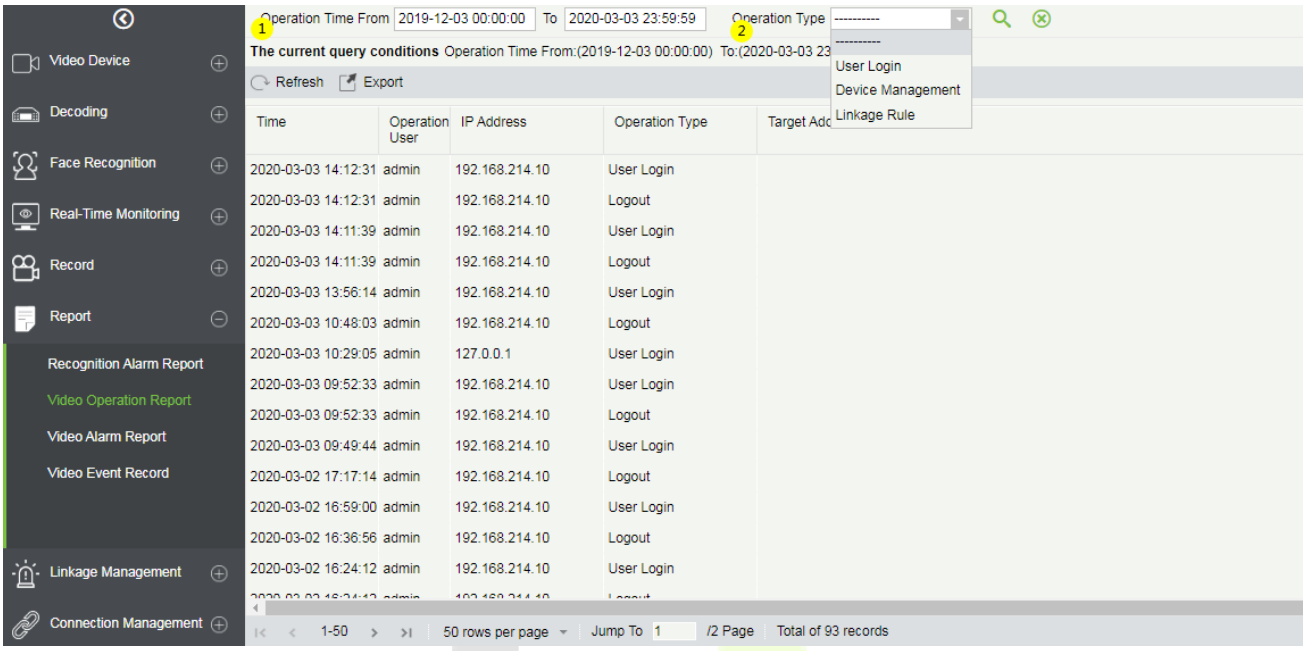
Include three alarm type: White List Alarm, Black List Alarm, Stranger Alarm.



12.6.2 Video Operation Report

It is mainly used to list the operation records of the system users on video device.

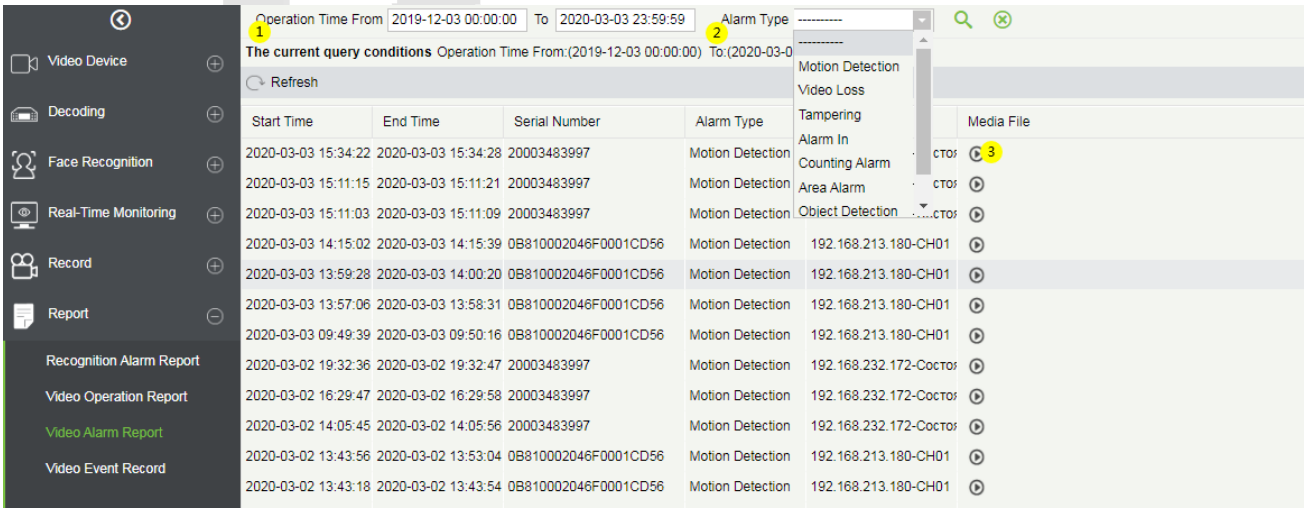
You can choose ① start time, ② operation type (User Login/Device Management/Linkage Rule) and other conditions to filter the report.



12.6.3 Video Alarm Report

It is mainly used to list all the video alarm record reports.

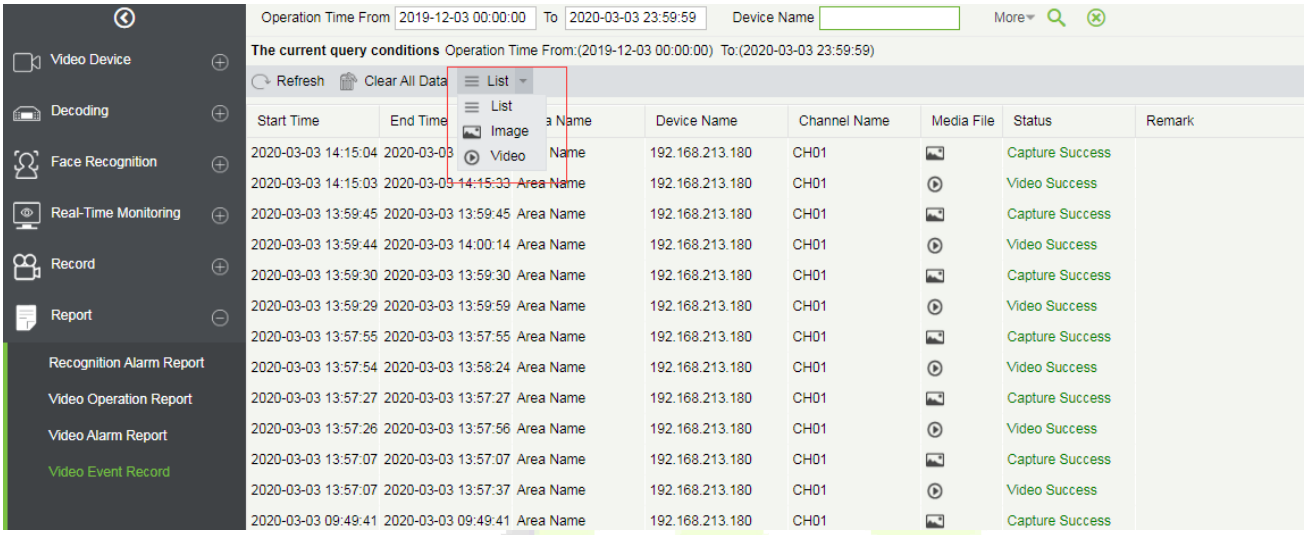
You can select ① the start time, the serial number of the video channel, and ② different alarm types to filter the report. There are 8 types of alarms that can be filtered: Motion Detection, Video Loss, Video Occlusion, Alarm Inputs, Counting Detection, Area Detection, Item Detection, Cross-Line Detection. Click ③**Media File** to view the alarm video.



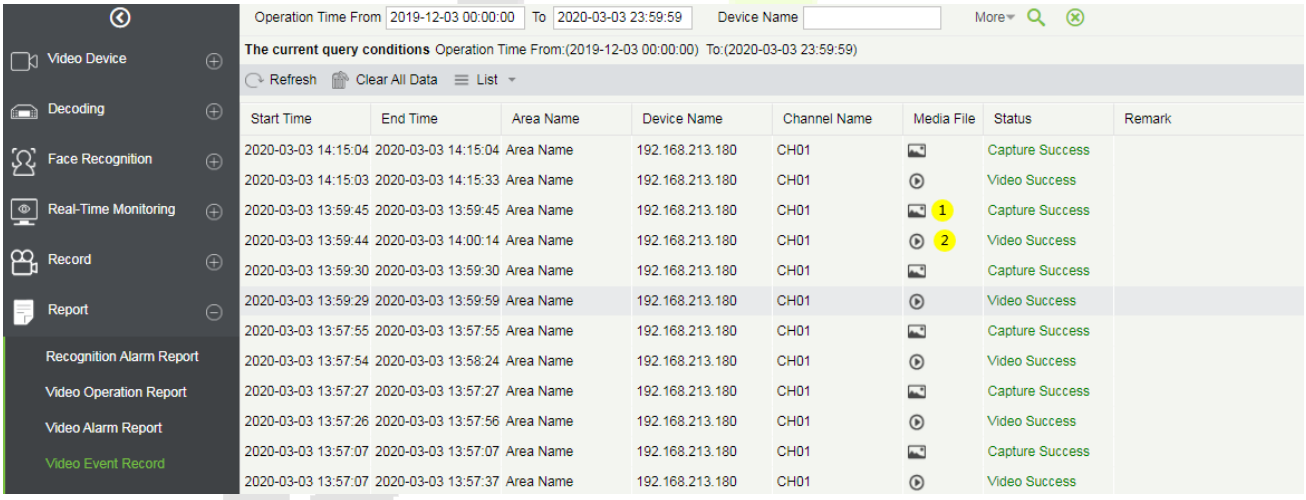
12.6.4 Video Event Report

The video event report data comes from the capture and the video recording data generated by the linkage between the access control and the video module.

Search event report data based on the time period and device name. You can select any one option to display data types: List, Image, Video.



①Click on the location of the image to display it; ② Click on the video play button to play it.



12.7 Linkage Management

Alarm linkage management is mainly used to configure the alarm linkage trigger conditions and action types of video device in the management system.

12.7.1 Linkage Management

Click [**Linkage Management**] to enter the linkage management interface and click [**New**] to add an alarm management.

①Enter Rule Name.

②Alarm Type, there are 8 options (Motion Detection, Video Loss, Video Occlusion, Alarm Inputs, Counting Detection, Area Detection, Item Detection, Cross-Line Detection).

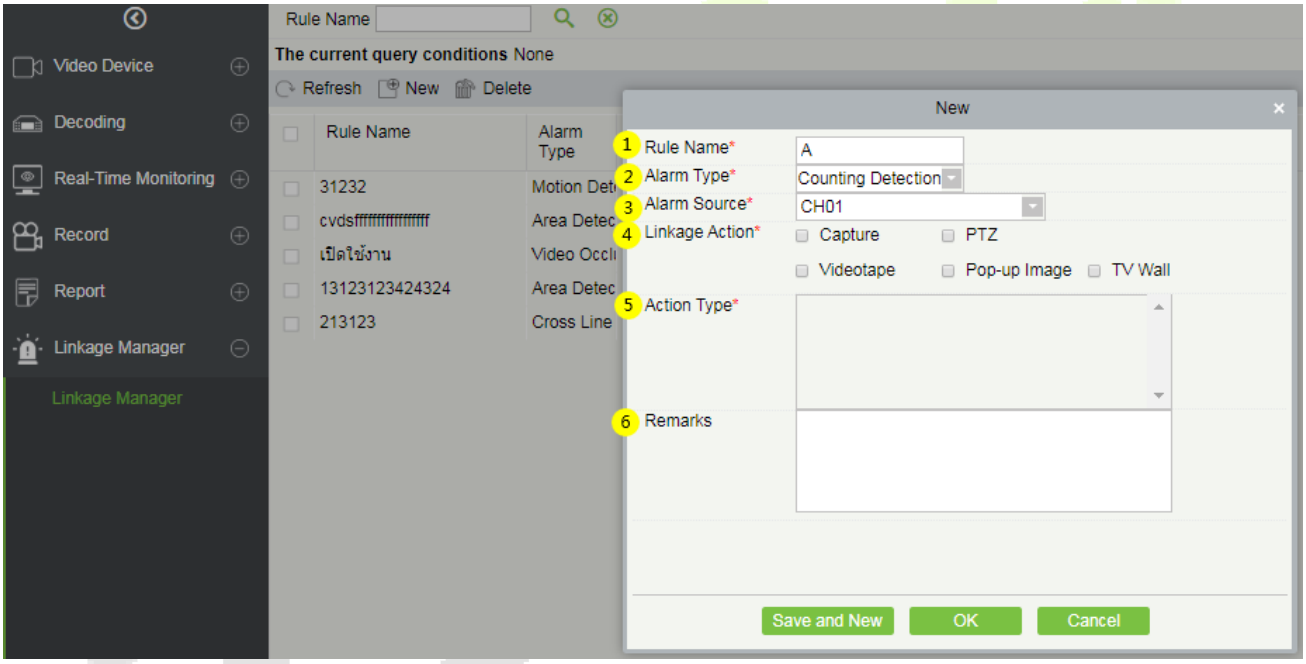
③Select the Alarm Source, that is, select a video channel.

④Linkage Action: there are five options: Capture, PTZ, Videotape, Pop-up image, TV wall.

⑤Action type.

⑥Remarks.

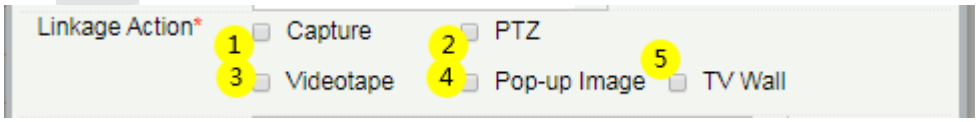
Note: When the alarm type is selected as Alarm inputs, the pull-down option of the alarm source will become the alarm input. Not all devices have alarm inputs. There are two types of alarm input: local alarm source and network alarm source. IPC devices have only local alarm source and no network alarm source. NVR devices have network alarm source.



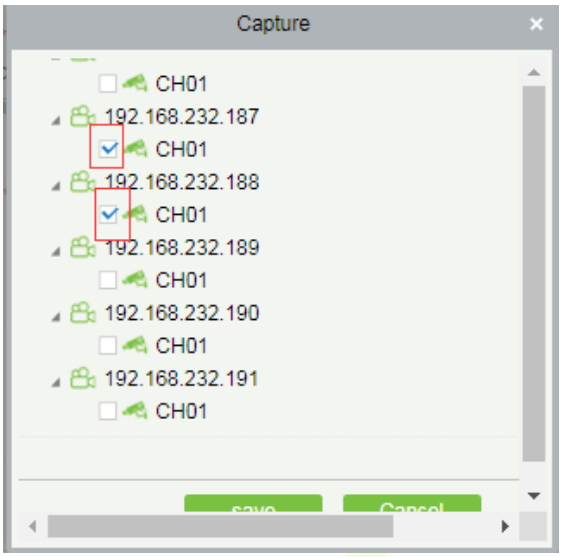
There are five options for linkage actions:

①Capture, ② PTZ, ③ Videotape, ④ Pop-up Image, ⑤ TV Wall.

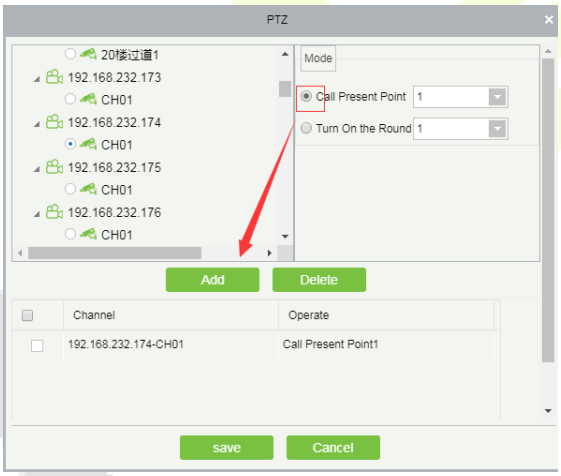
You can select multiple options, but you can configure the actions one by one only.



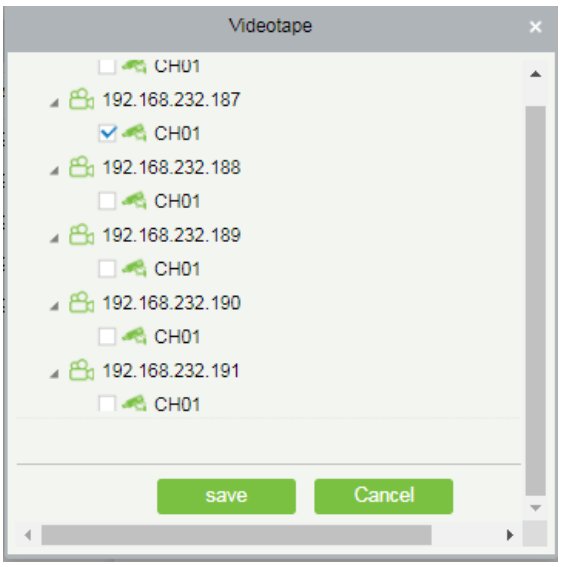
- When selecting **Capture**, select the video channel that needs to be captured.



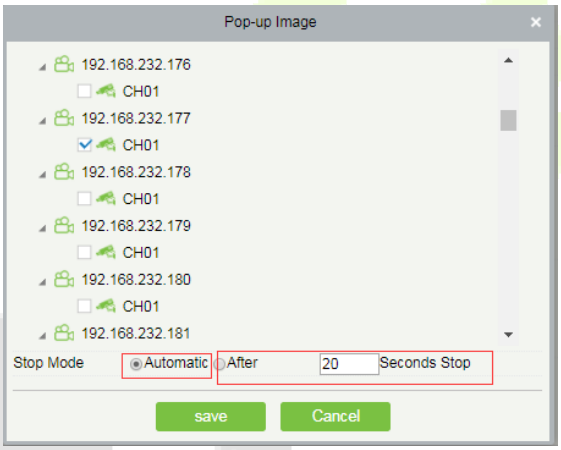
- When selecting **PTZ**, you can choose to call the present point or turn on the round.



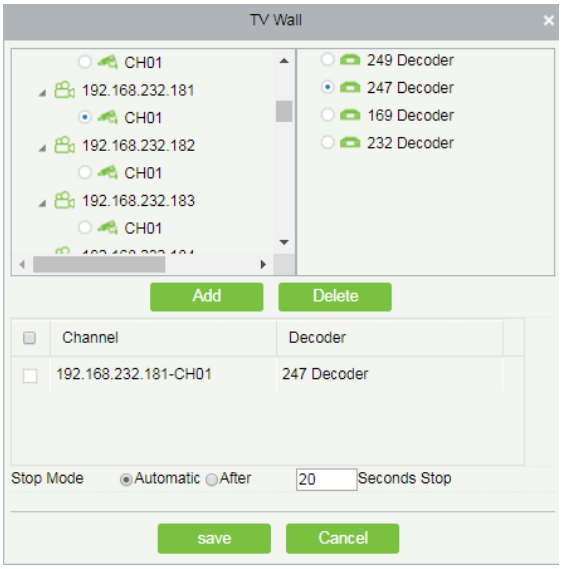
- When selecting **Videotape**, select the video channel that needs video; multi-channel can be selected.



- When **Pop-up image** is selected, select the output channel and set the duration of the pop-up image. There are Automatic (stop when the alarm stops) and pop-up time setting.



- When **TV-Wall** is selected, you can select the corresponding alarm linkage output video channel. You need to add a decoder first.



12.8 Connection Manager

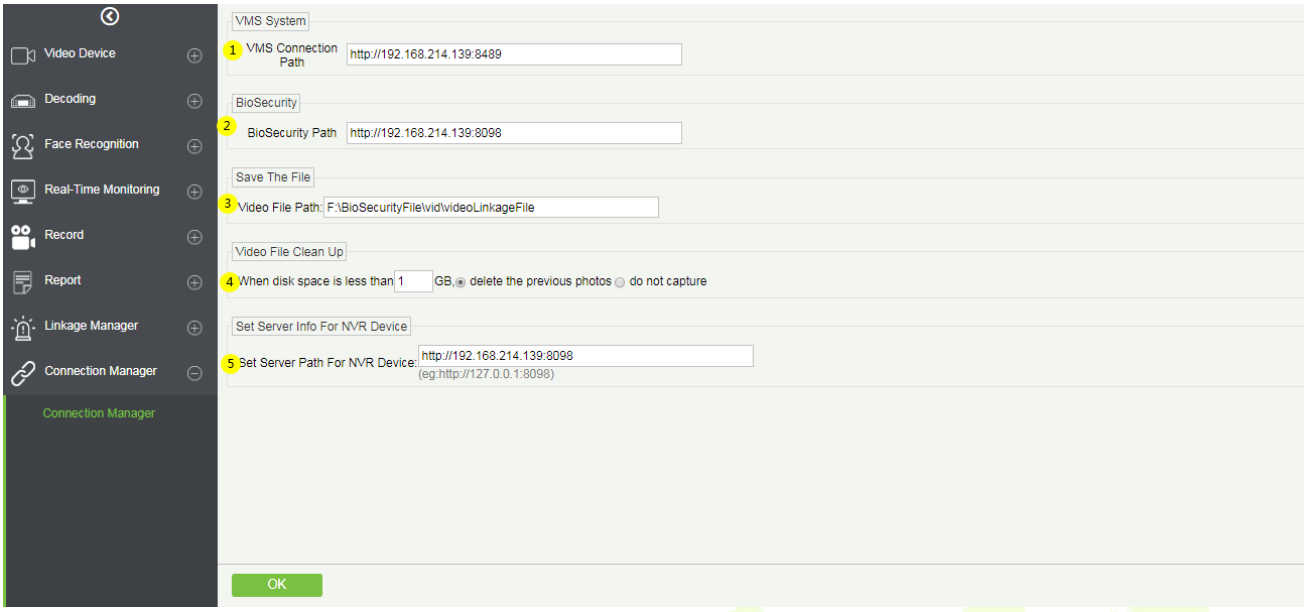
12.8.1 Connection Manager

Click **[Connection Manager]** to enter the connection management configuration interface:

1. The address and port number of the VMS client.

Note: The VMS Client must be installed and configure the connection with VMS Server.

2. Configure the access address of ZKBioSecurity.
3. Configure the storage address of the video linkage captured pictures and video files.
4. Configure the size of the space where the video linkage media files are stored. When the media file capacity reaches the configured space size, there are two options: "Delete old files" and "No longer capture".
5. Set and save the server info for NVR Device.



12.9 Access Control Module and VMS-Video Linkage Function Description

12.9.1 Access Control and Video Linkage Function

VMS video function can replace the original Video module to make a video linkage with the access control module. The setting method is the same as the original setting linkage method of access control and video module.

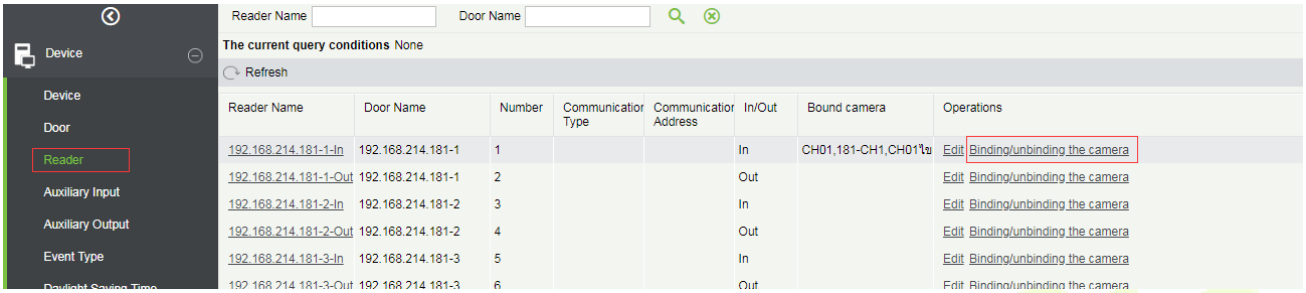
The steps to set up the linkage between access control and VMS video are as follows:

1. Under VMS device interface, add video device.

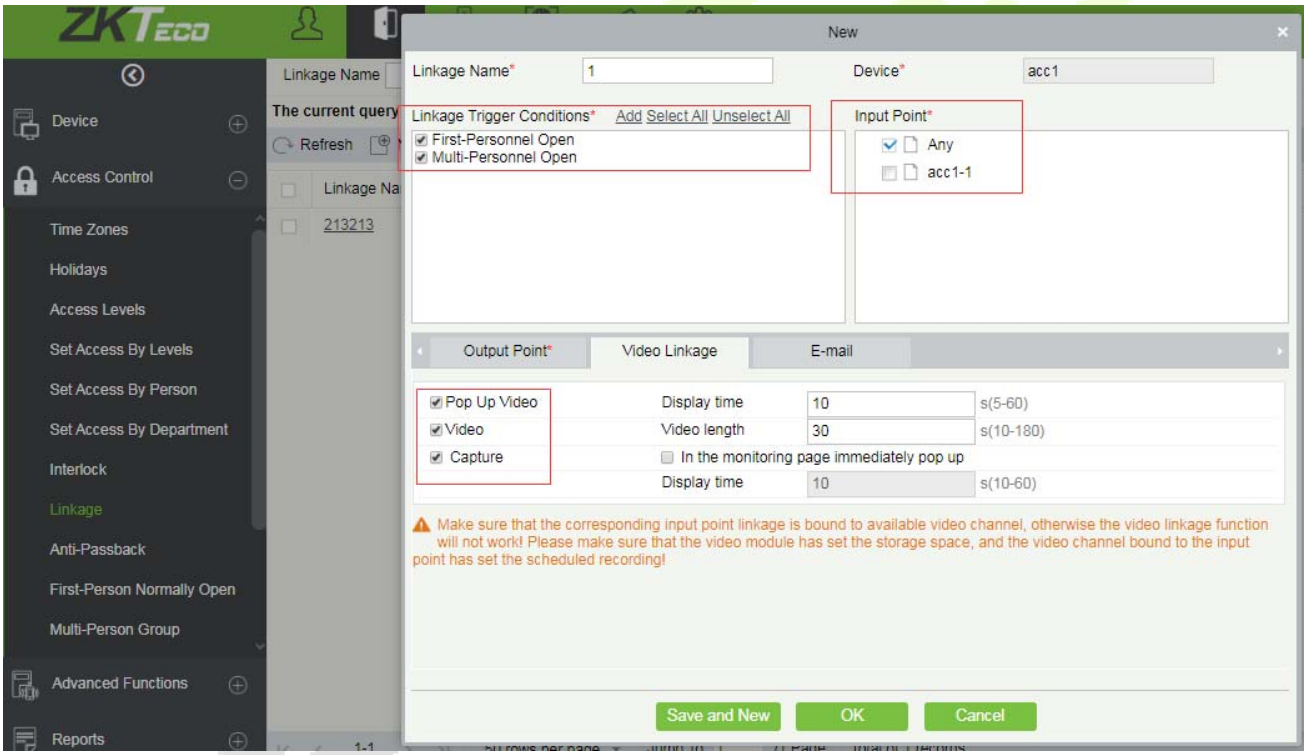
2. Add the access control device under the device interface of the access control module.

3. Under the Reader interface of the access control module, bind the reader of the access control device to the VMS video channel that needs video linkage. A reader can bind up to 5 video channels.

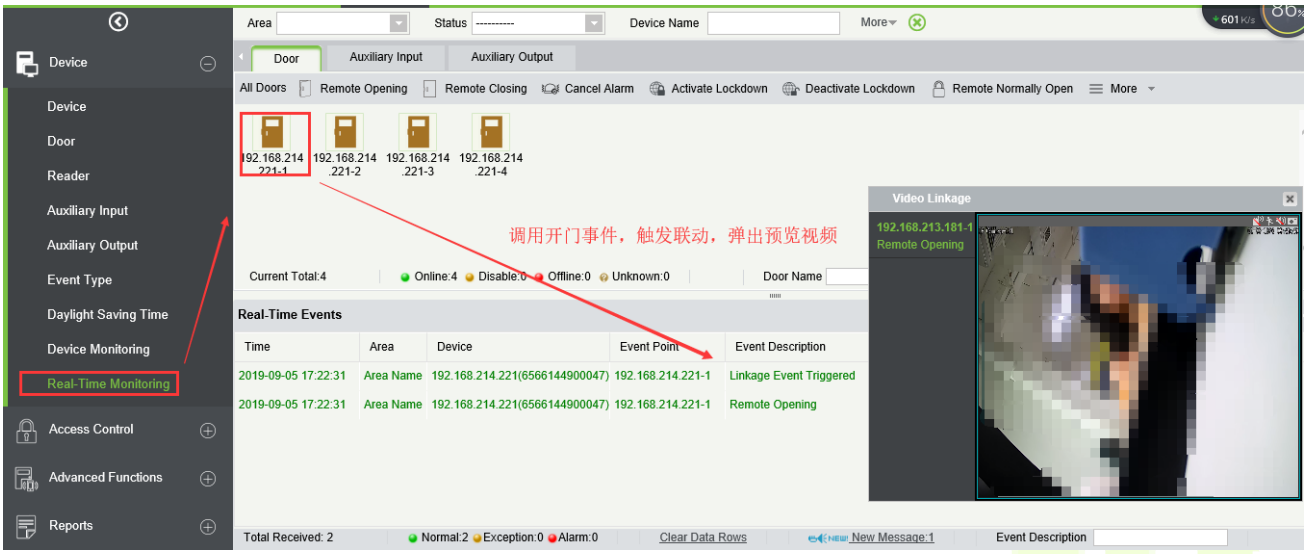
Note: The combined channel must first set the alarm video in the Storage Server-Record Plan Setting, so that the access control linkage can produce the video.



4. Set the linkage trigger conditions, input point, output point, etc., click [**OK**] to save. For details, please refer to [**Linkage**] setting instructions of access control module.



5. Real-time monitoring interface preview linkage effect is as follows: linkage triggered, pop up the video playback window.

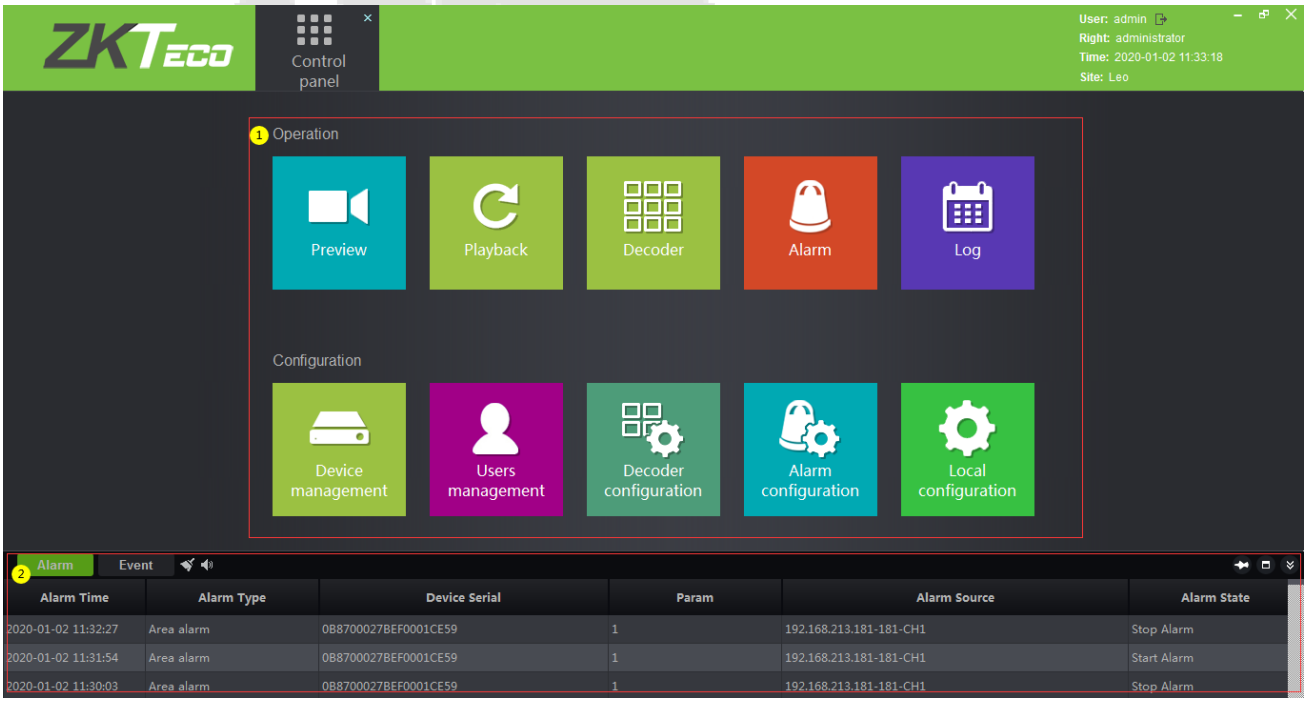


12.10 VMS Client Instructions

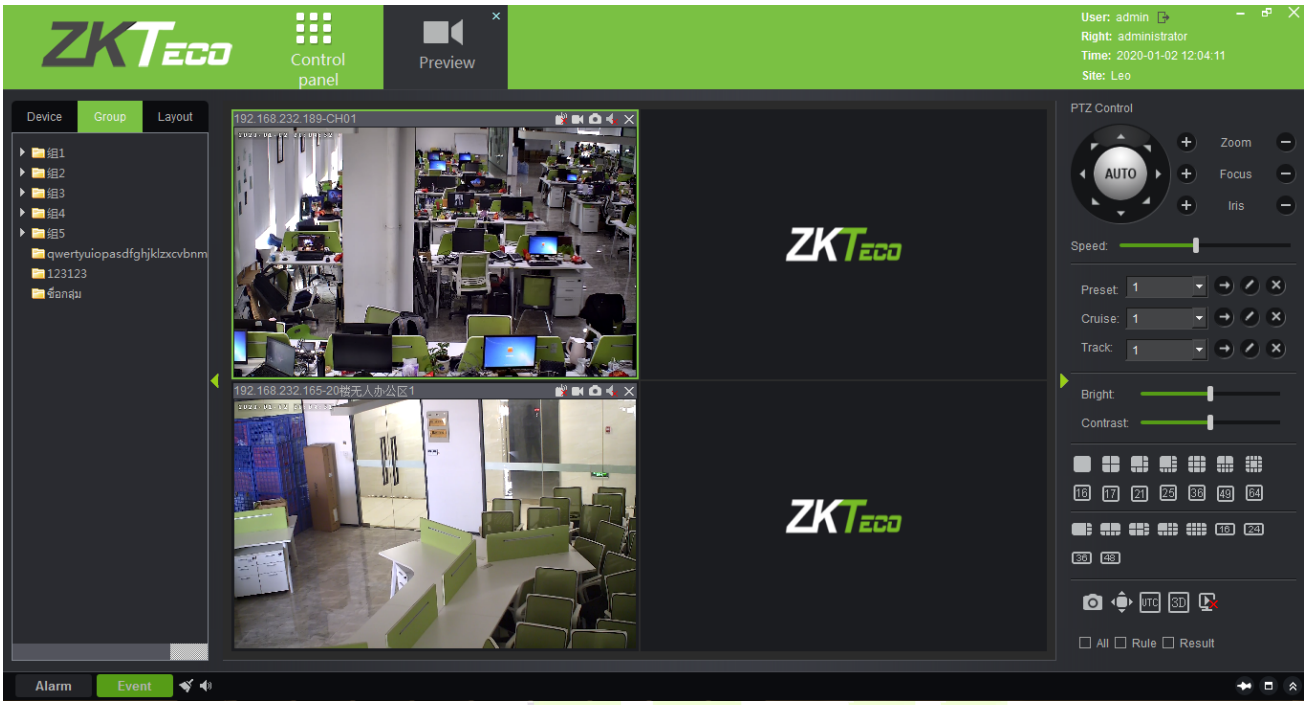
12.10.1 VMS Client

The VMS client is called ZKBioSecurity VMS Plugin, and its functionality is similar to that of the VMS server. After logging into the VMS client, the control panel lists as follows. ①10 common function modules (Preview, Playback, Decoder, Alarm, Log, Device management, User management, Decoder configuration, Alarm configuration and Local configuration) and ② Alarm event center.

Click the  icon in the upper right corner to log out of the system.

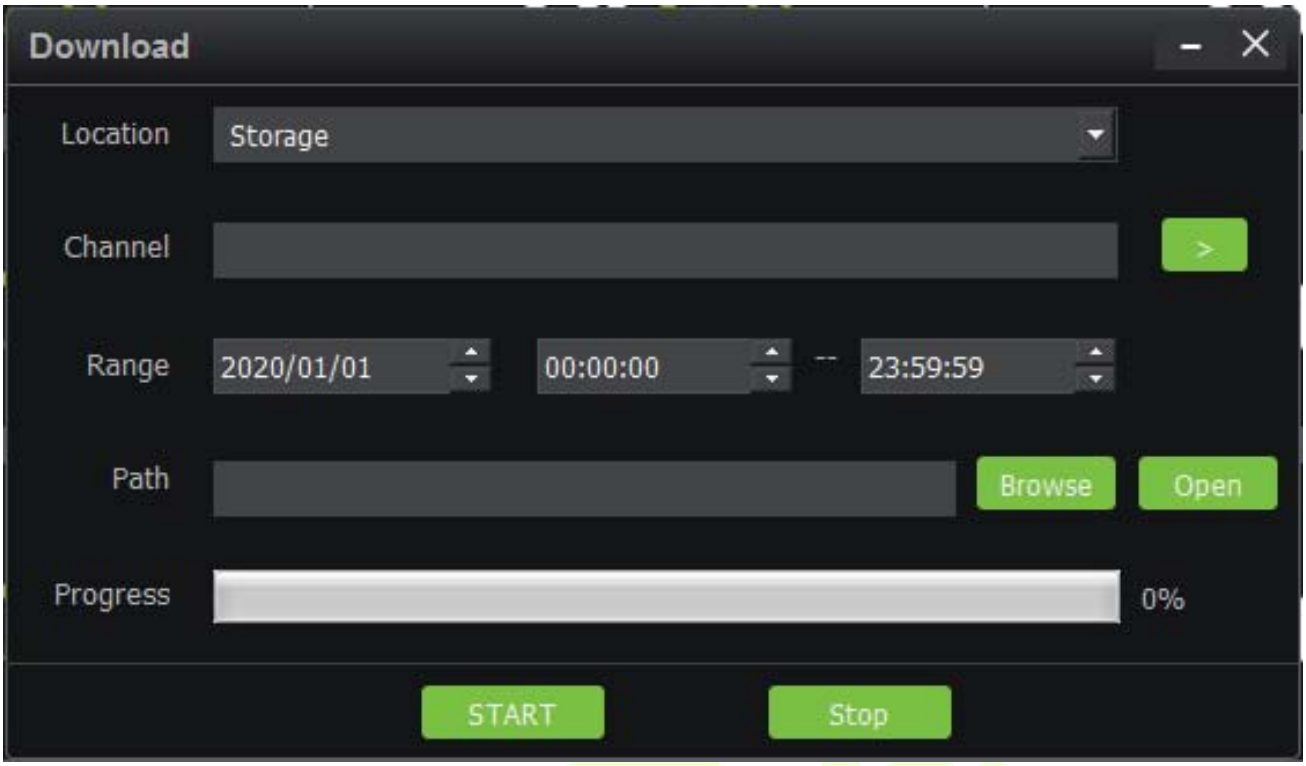


Click **[Preview]** to open the client preview interface, and you can select video channel, group and layout for screen preview. For the operation of preview interface, please refer to 12.4.3 Video Preview.



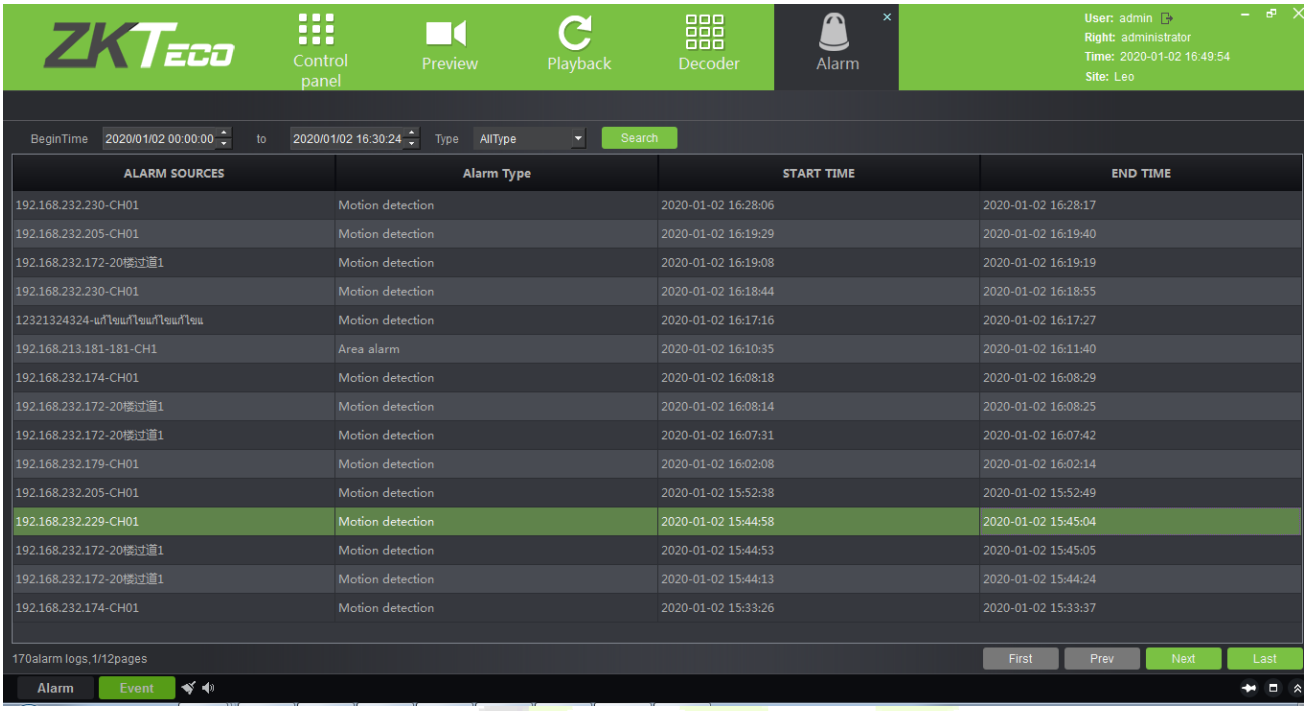
Click **[Playback]** to open the client playback interface. The function of the playback interface is basically the same as that of the VMS server. Please refer to 12.5.2 Video Record for the operation method.

There are two differences: ① on the client side, you can replay nine video channels at the same time, while on the server, you can only replay four channels at the same time. ② Add a download configuration interface.

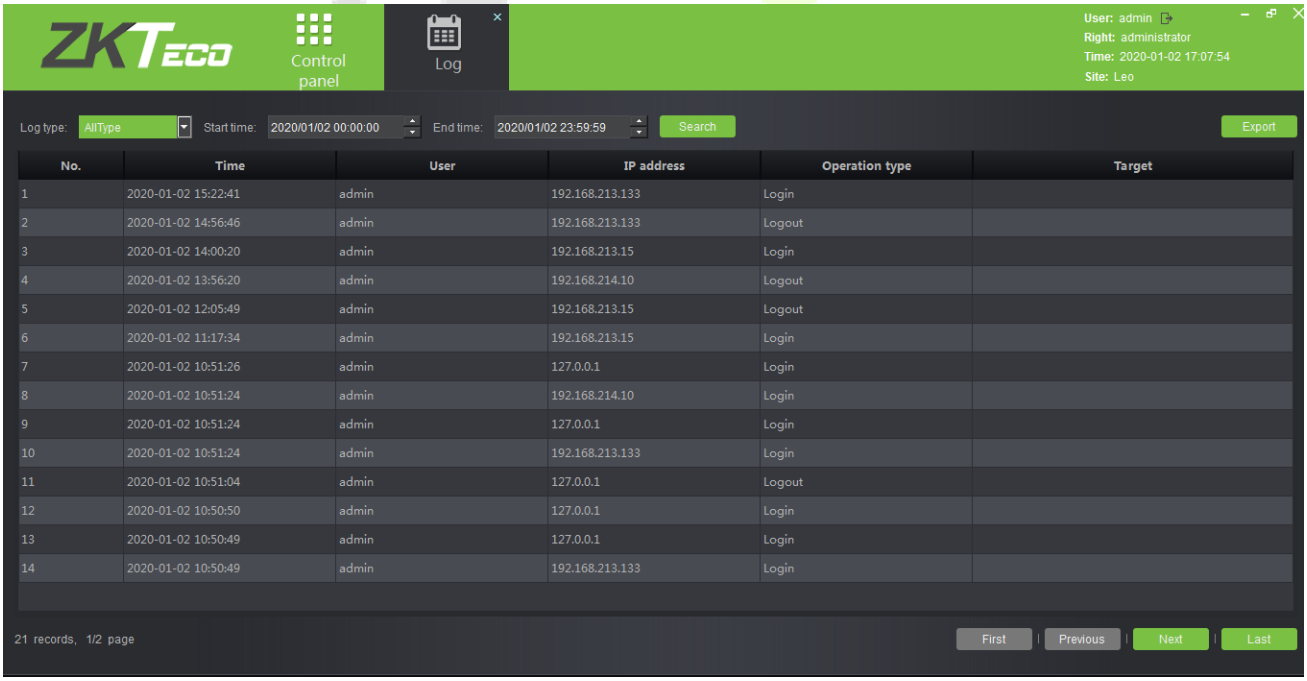


Click **[Decoder]** to enter the decoder operation interface. The decoder interface of the VMS client integrates the three functions of decoder preview settings, decoder preview play and decoder playback on the VMS server into one interface. Please refer to 12.2.4 Decoder Preview Settings, 12.2.5 Decoder Preview Play and 12.2.6 Decoder Playback.

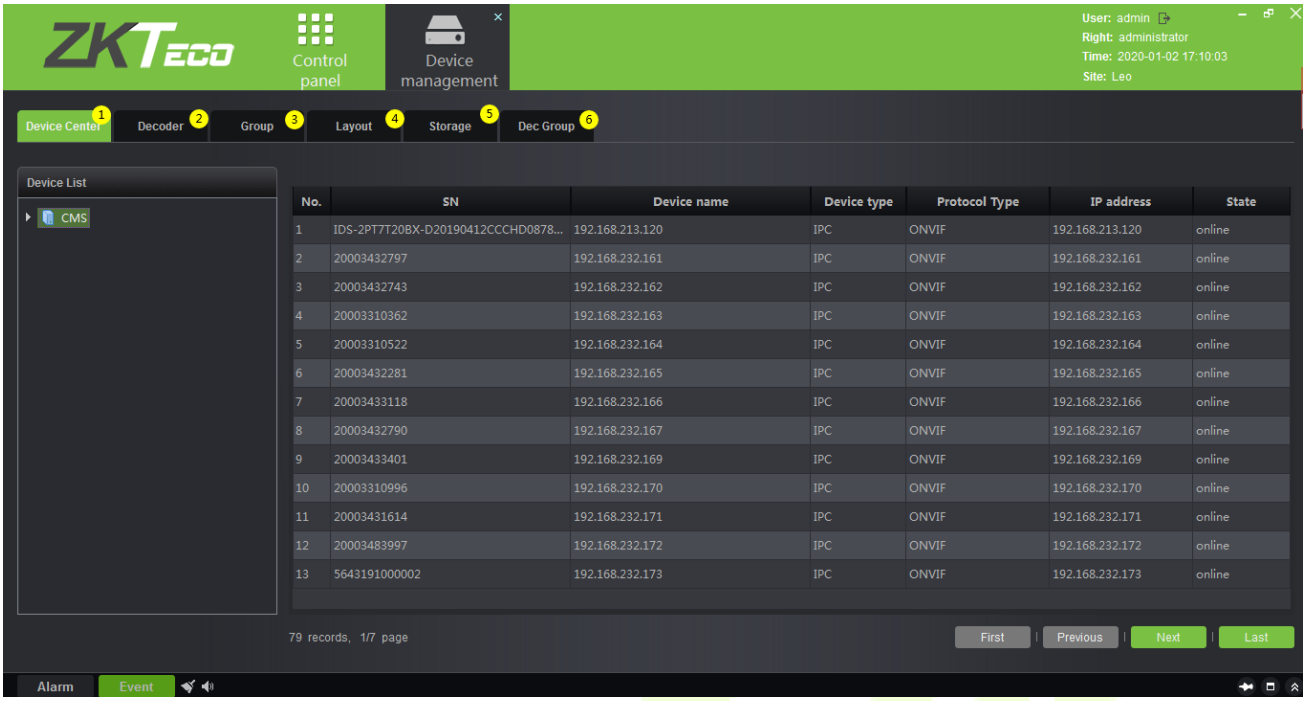
Click **[Alarm]** to enter the alarm report interface. It is the same as the report on VMS, except you can't immediately view the alarm video. If you need to view the alarm video, you can go to the 12.6.3 Video Alarm Report on the VMS server.



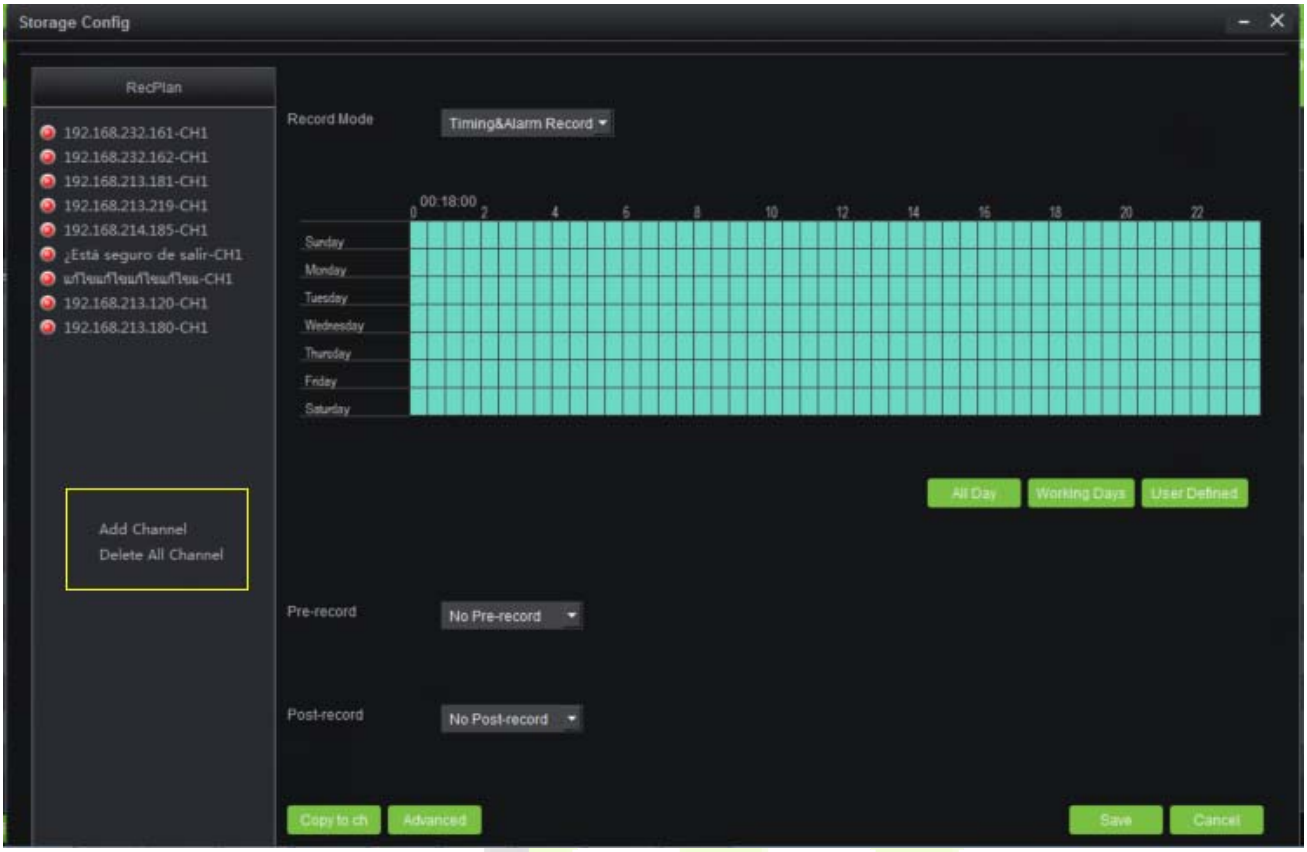
Click **[Log]** to query the user's operation record of the video device. The content is the same as that seen in the 12.6.2 Video Operation Report.



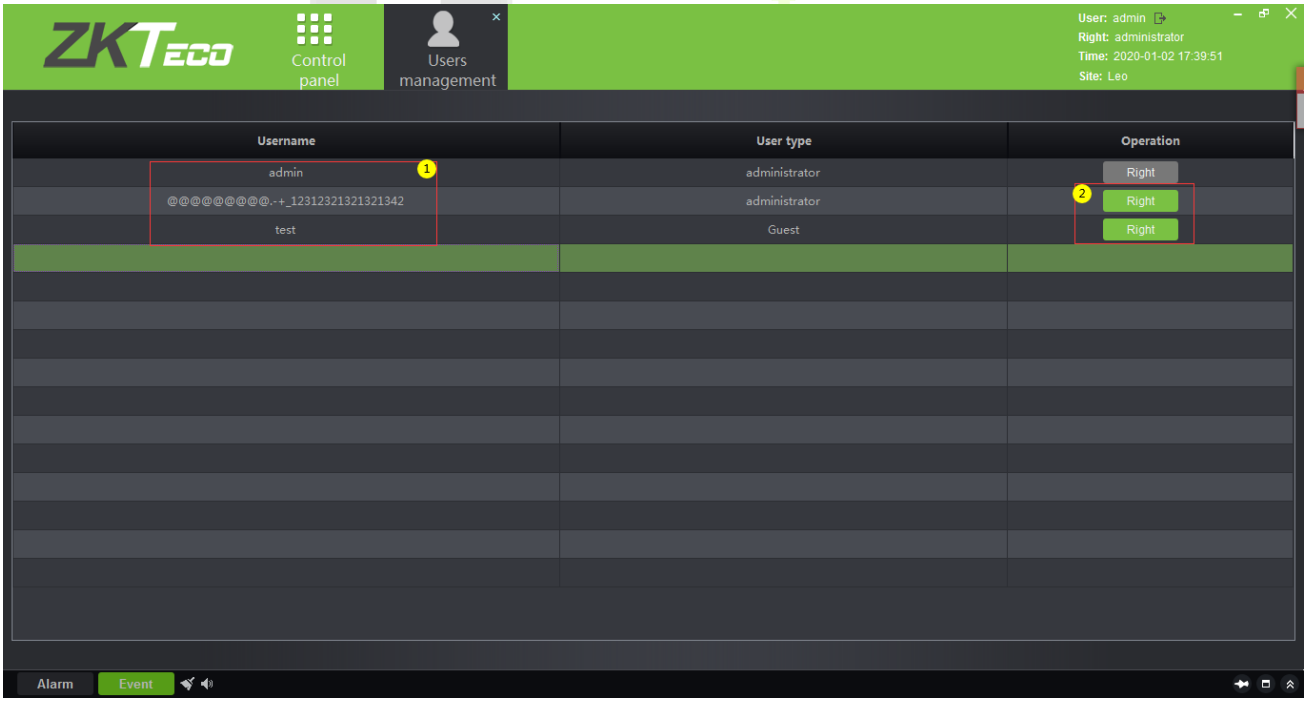
Click **[Device management]** to enter the device management interface of VMS client.

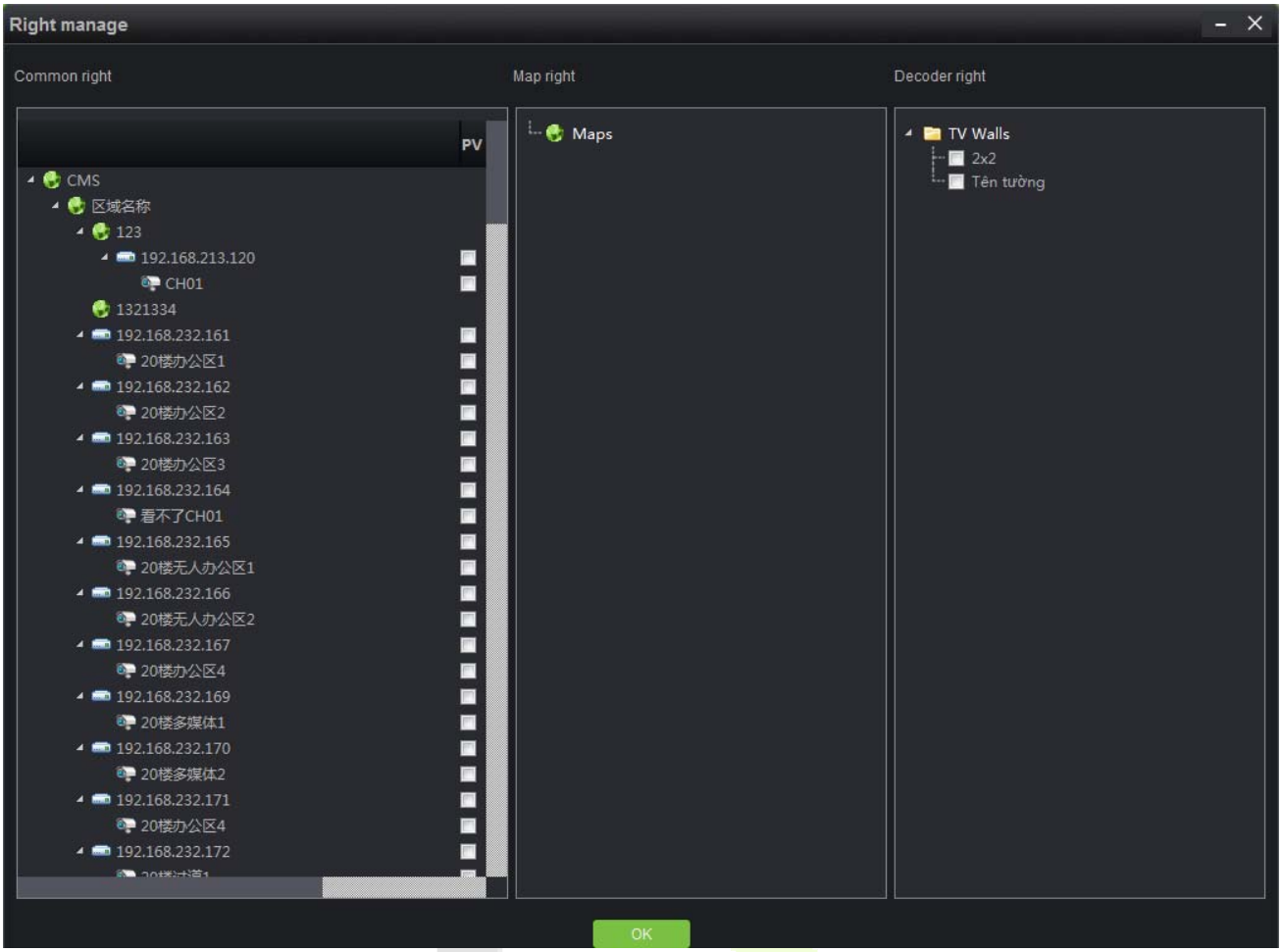


Including: ① is the Device monitoring interface, which is the same as the information listed in the Video Device interface on the VMS server. ②Decoder management interface, the same as the content of 12.2.1 Decoder. ③ Video group management interface, please refer to 12.4.1 Group. ④ Video channel layout management interface, please refer to 12.4.2 Layout. ⑤ Storage service configuration interface, please refer to 12.5.1 Storage Server. In the record plan module, right-click to add or delete the record plan. See figure 1 below. ⑥Decoder group, please refer to 12.2.2 Decoder Grouping.

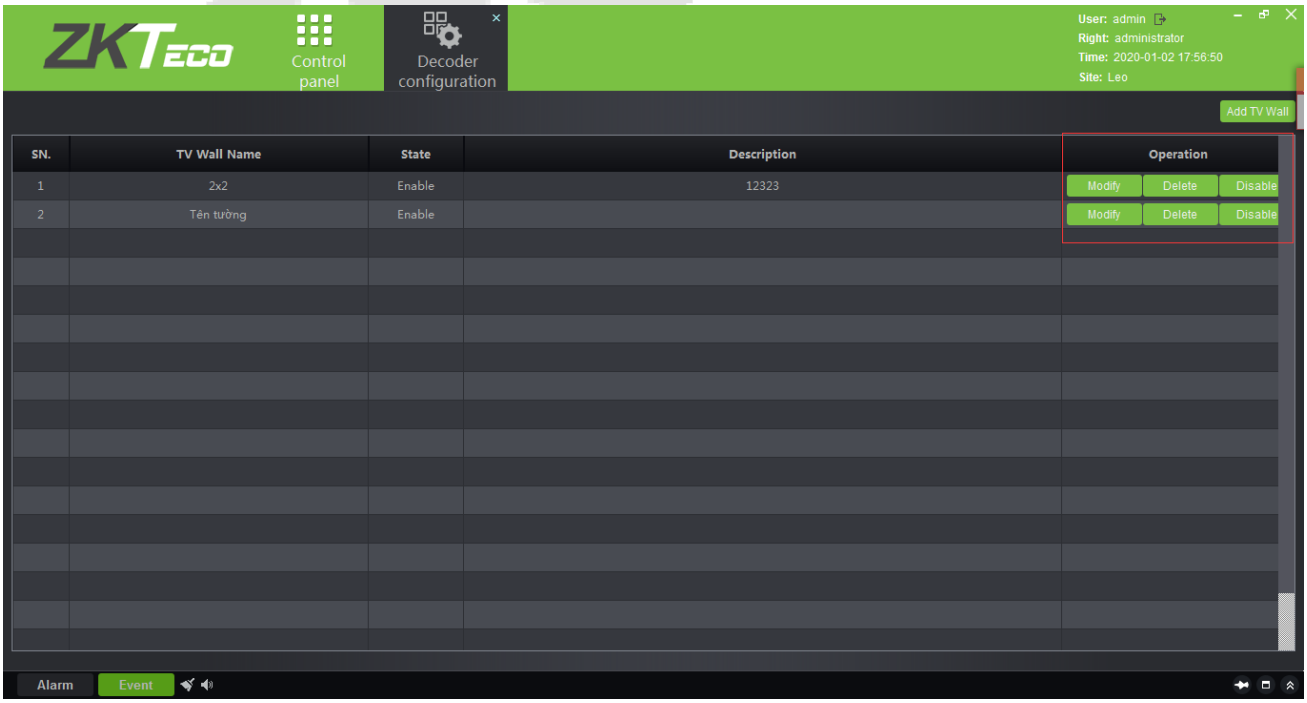


Click **[User management]** to enter the user management interface of the system. This interface lists ① all the users of VMS system, click ② to set different permissions for each user to access the device, map, TV wall. The admin has all permissions by default.

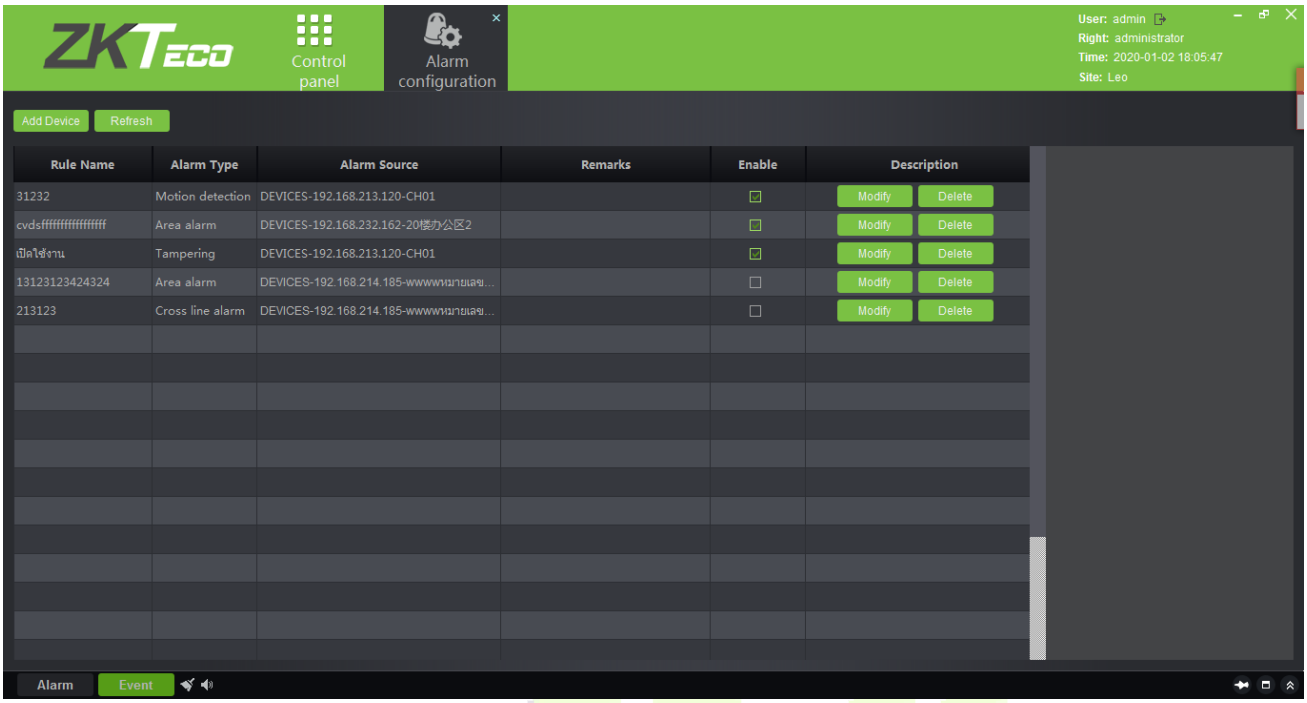




Click **[Decoder configuration]** to enter the management interface of TV wall. Please refer to 12.2.3 TV Wall for specific setting steps.

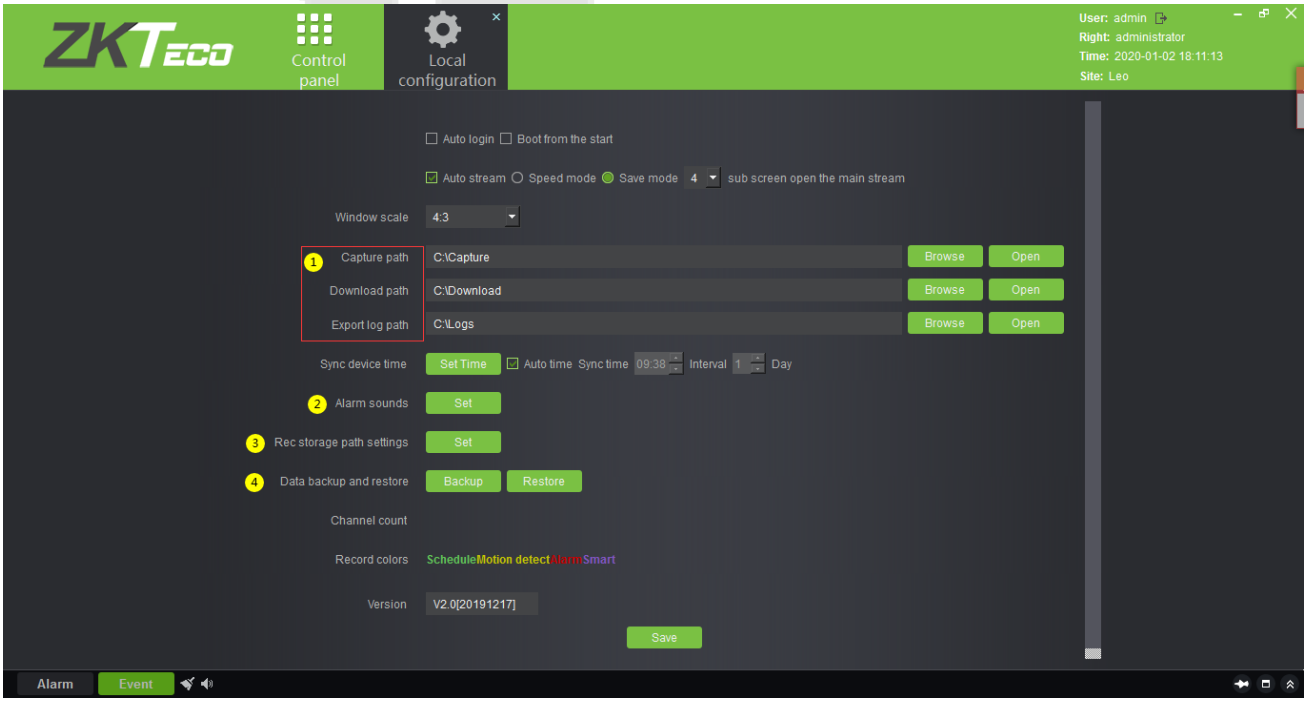


Click **[Alarm configuration]** to enter the alarm linkage management interface of the client, and the alarm linkage setting is the same as 12.7.1 Linkage Management.



Click **[Local configuration]** to enter the system configuration interface of the client. ① Capture, download, export log path can be set. ② Different alarm sounds can be set. ③The record storage path can be set. ④ The client database can be backed up and restored.

Click **[Save]** to save the configuration.



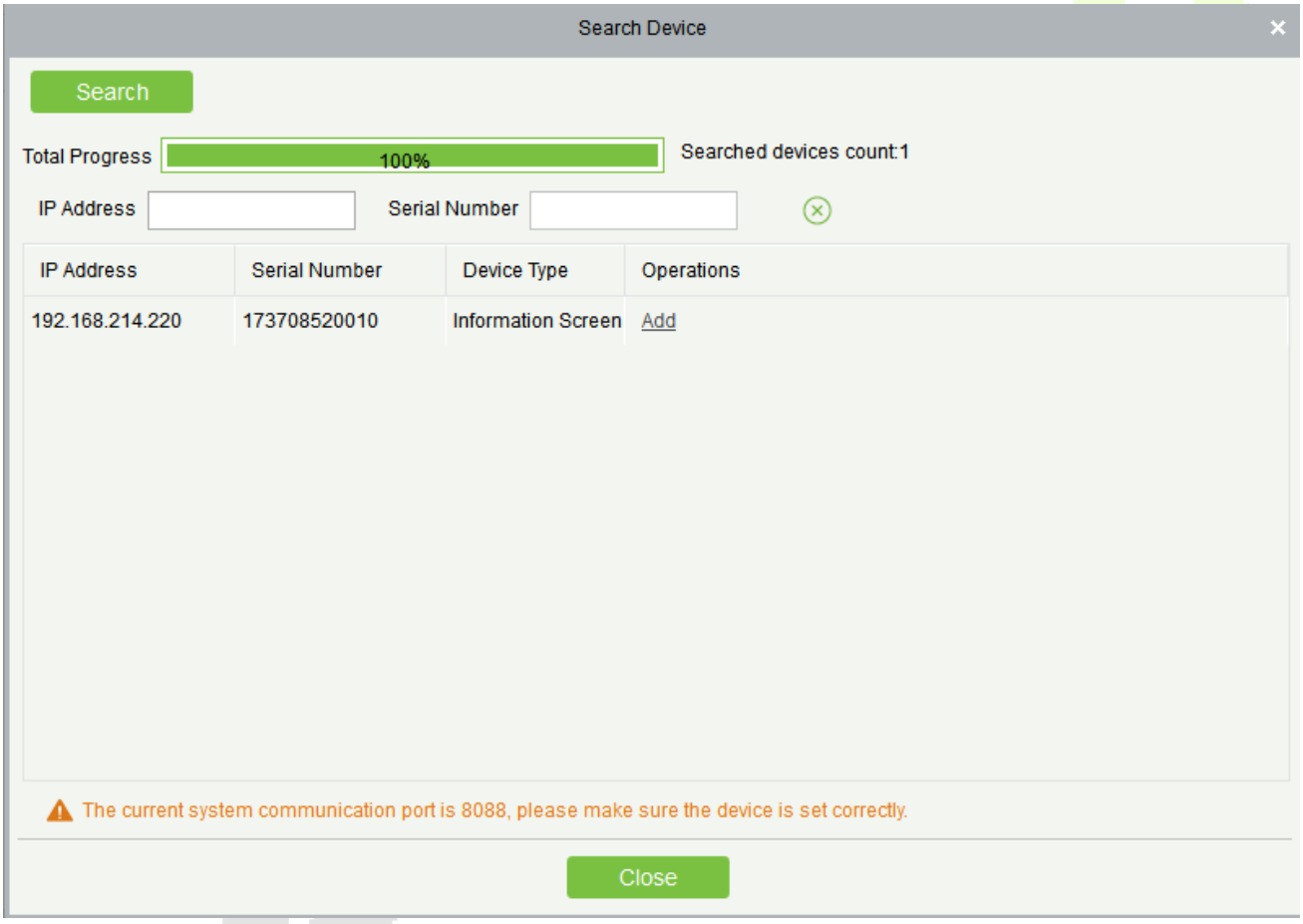
13 FaceKiosk

13.1 FaceKiosk

13.1.1 Device

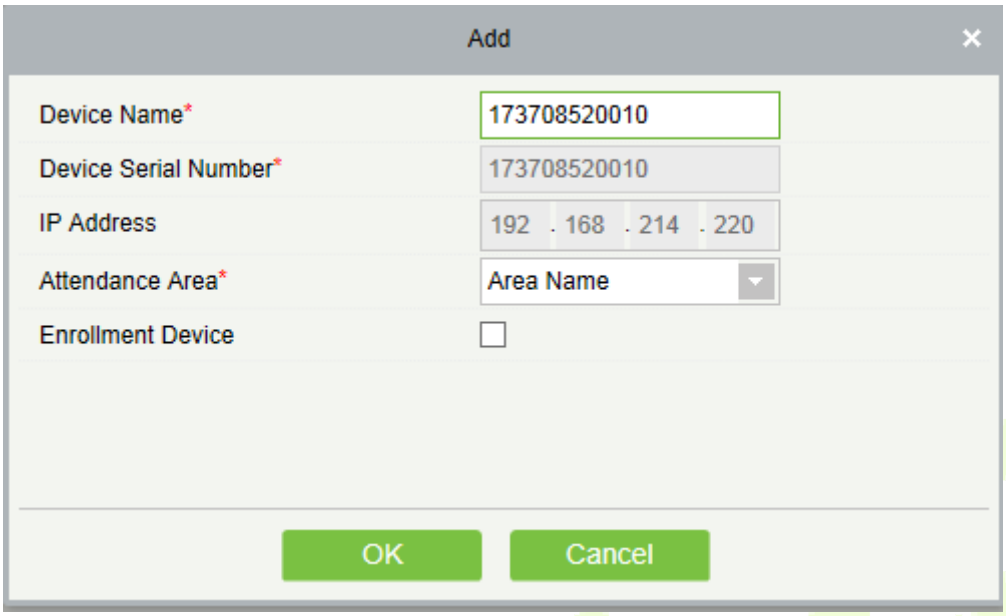
Search Device: In the tool bar, select the "Search device" menu. Add the device to the software server

✍**Note:** User need to entry the hardware deivce and setting some paramter which is support to setting the software server address.



- **Add Device**

Click the **[Add]**, the system will show the menu, user can typing the important information, click the **[OK]** button.



Device Name: FaceKiosk Device name.

Device Serial Number: Just support to show the default value, It can't support to edit.

IP Address: Belong to the device parameter and used to communication with the software server.

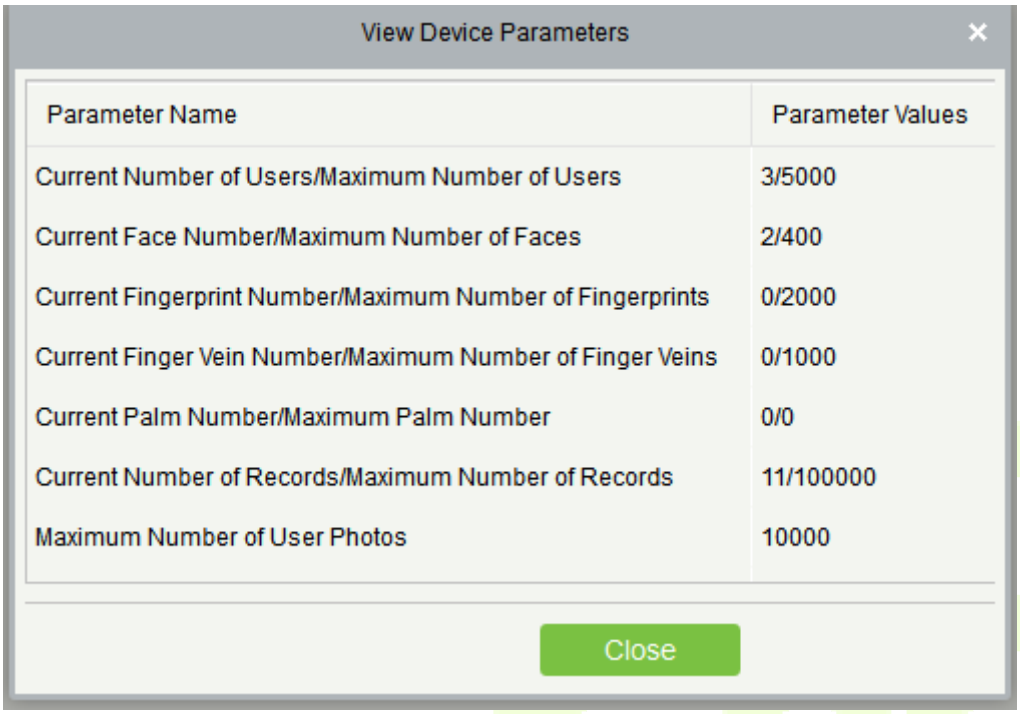
Attendance Area: Which area the FaceKiosk device belong to.

Enrollment Device: Support to setting as the registration device.

Enable/Disable: Select device, click [**Disable/Enable**] to stop/start using the device. When communication between the device and the system is interrupted or device fails, the device may automatically appear in disabled status. After adjusting local network or device, click [**Enable**] to reconnect the device and restore device communication.

Synchronize software Data to the Device: Synchronize data of the system to the device. Select device, click [**Synchronize All Data to Devices**] and click [**OK**] to complete synchronization.

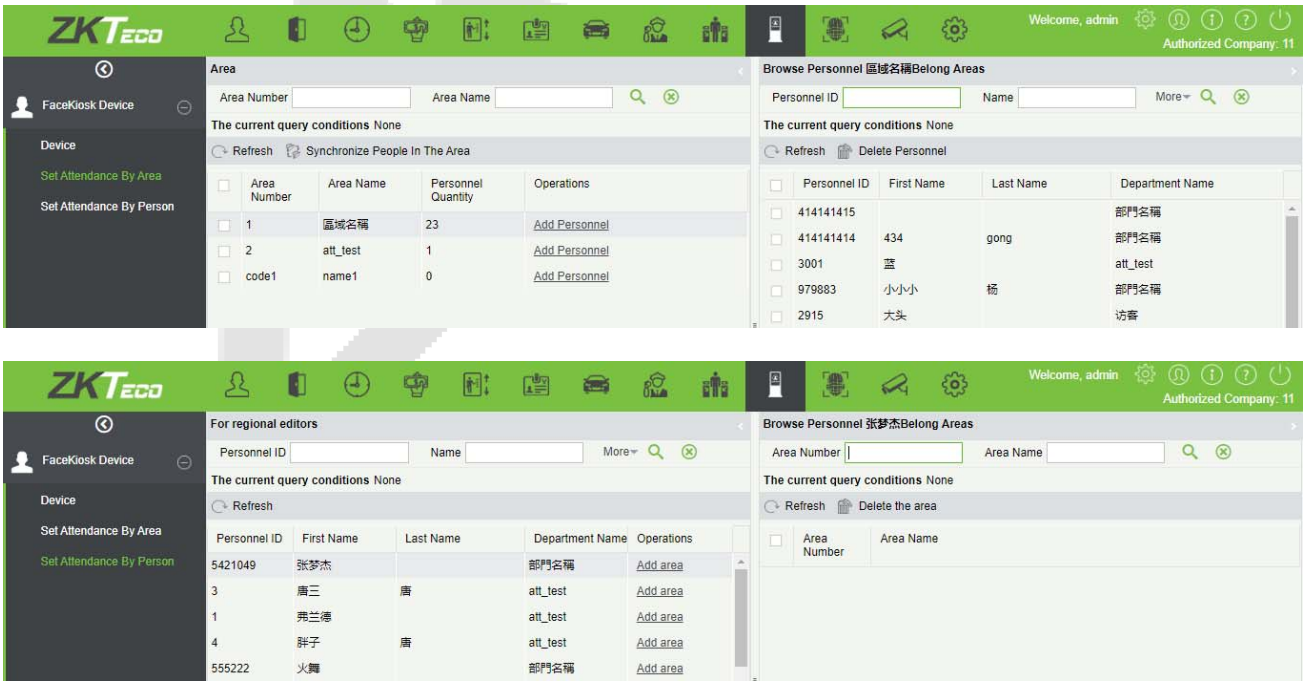
View Device Parameters: Show the capacity detail.



13.1.2 Area

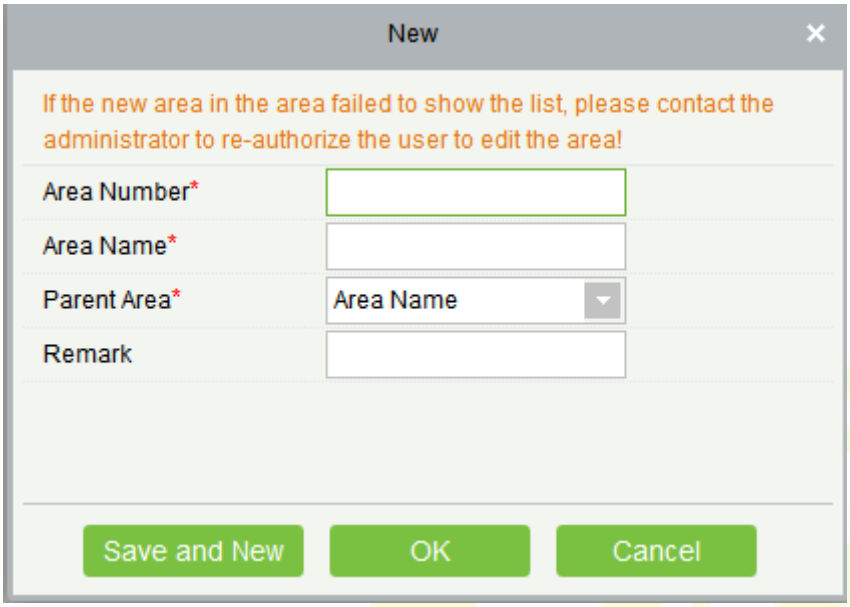
Set Attendance by Area/Person

The area is unified to the system management for maintenance, and the Facekoisk is displayed by area and by person. It displays each area and the personnel belonging to each area in area settings, and display the area to which the personnel belongs in person settings.



- **New**

[Area] -> **[new].**



After you finish the input value, click the submit button [**Save and new**] or [**OK**].

Area Number: It just can support typing the number and alphabet.

Area Name: It can support typing anything alphabet, but can't typing the comman.

Parent Area: The default parent area is Area name. User can select any area.

Remark: It can support to typing anything.

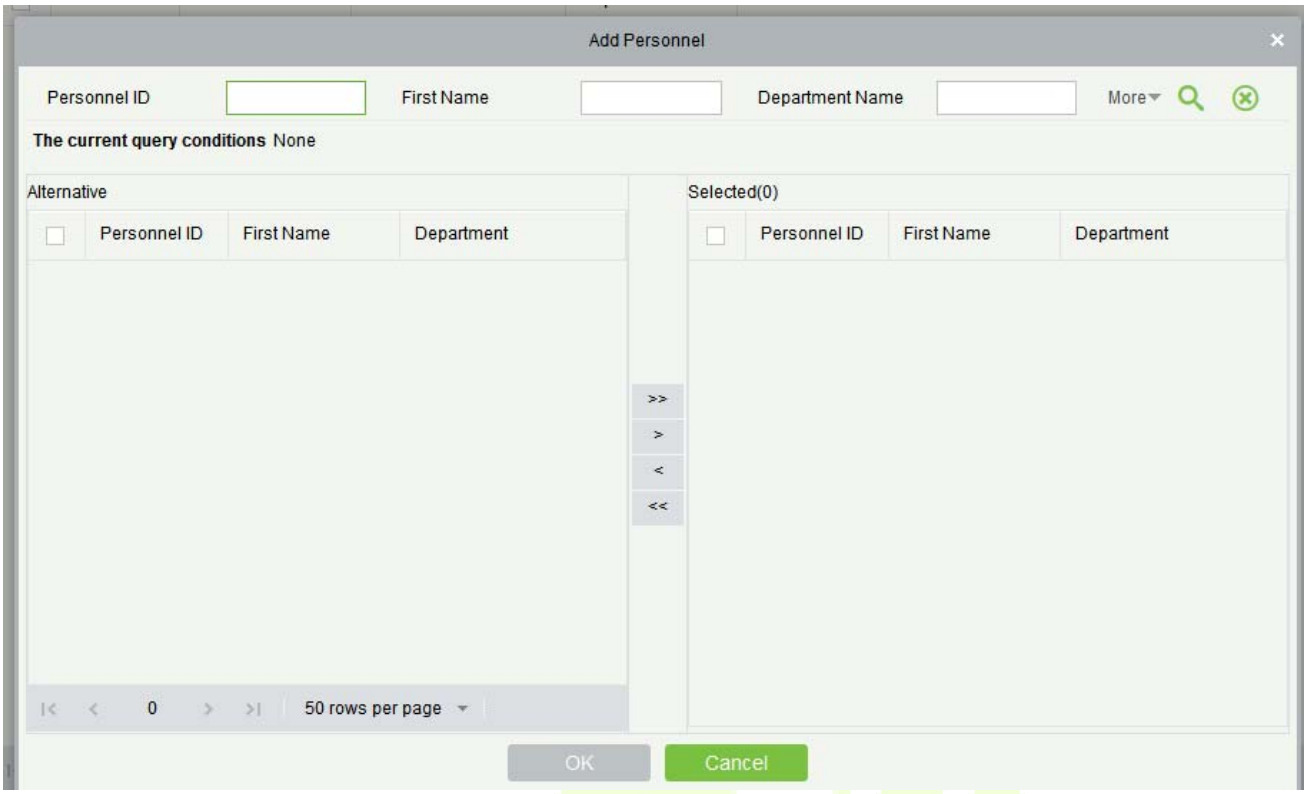
✍**Note:** This area contact with the system area. Which is under the system module.

✍**Note:** If some persons belong to the area, so that this area can't support to delete.

13.1.3 Personnel Area Setting

- **Regional Add Staff**

Select a **[Area]** and click the **[Regional add staff]** to this area.



Delete: Select person which is the user want to delete, the system will automatic to delete this user from the device.

Resynchronize to Device: Synchronized the personnel information to the device by manual.

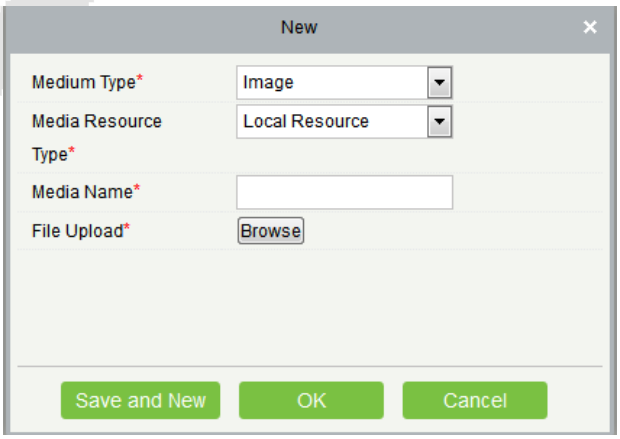
13.2 Media Advertising

13.2.1 Advertisement Resources

In the Advertisement resources module, it can support to create/edit/delete advertisement resources.

Refresh: Refresh the data which is show on the table.

New: Support to upload some new advertisement resources to software server.



Medium Type: It have both value to choice. Image and video.

Media Resource Type: It Support to upload some file to server form the local computer. Or setting the link from the network.

Media Name: It can support the used defined the media name which is used for user remenber.

File Upload: It can support select the file from the local computer. Which is will be uploaded.

Edit: It can support to edit and fixed the information.

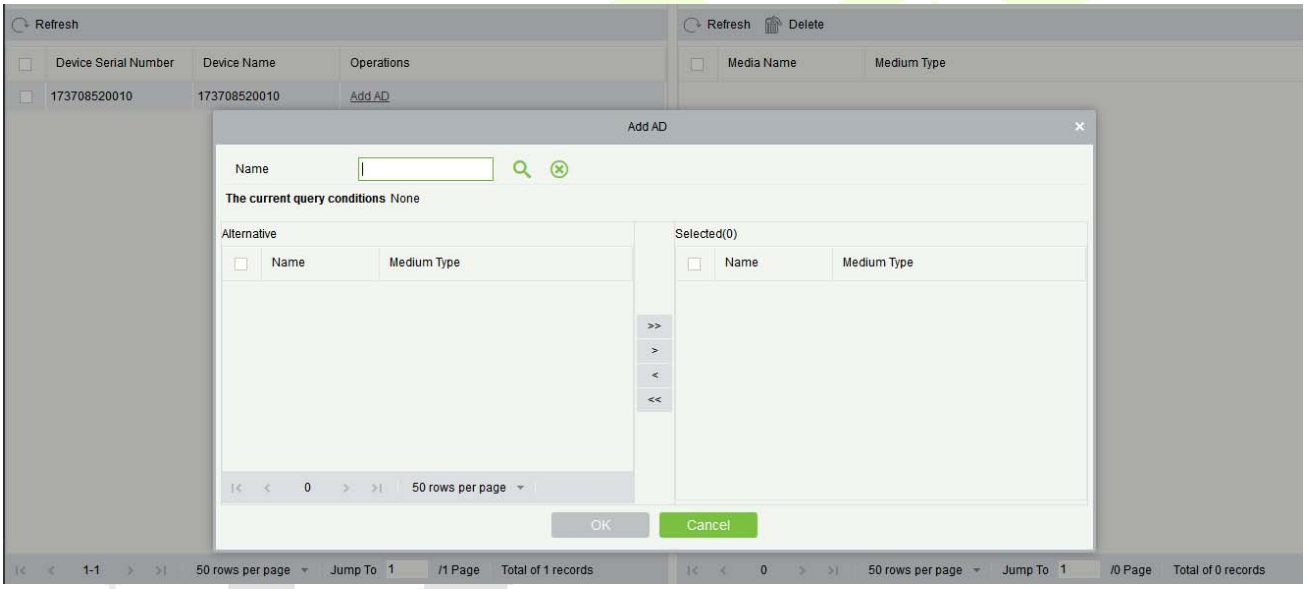
Delete: It can support to be deleted.

13.2.2 Advertising Setting

Click [**Advertising Setting**], this module support to create/edit/delete the advertising.

Add AD:

Open [**Advertising Setting**], Click [**Add AD**].

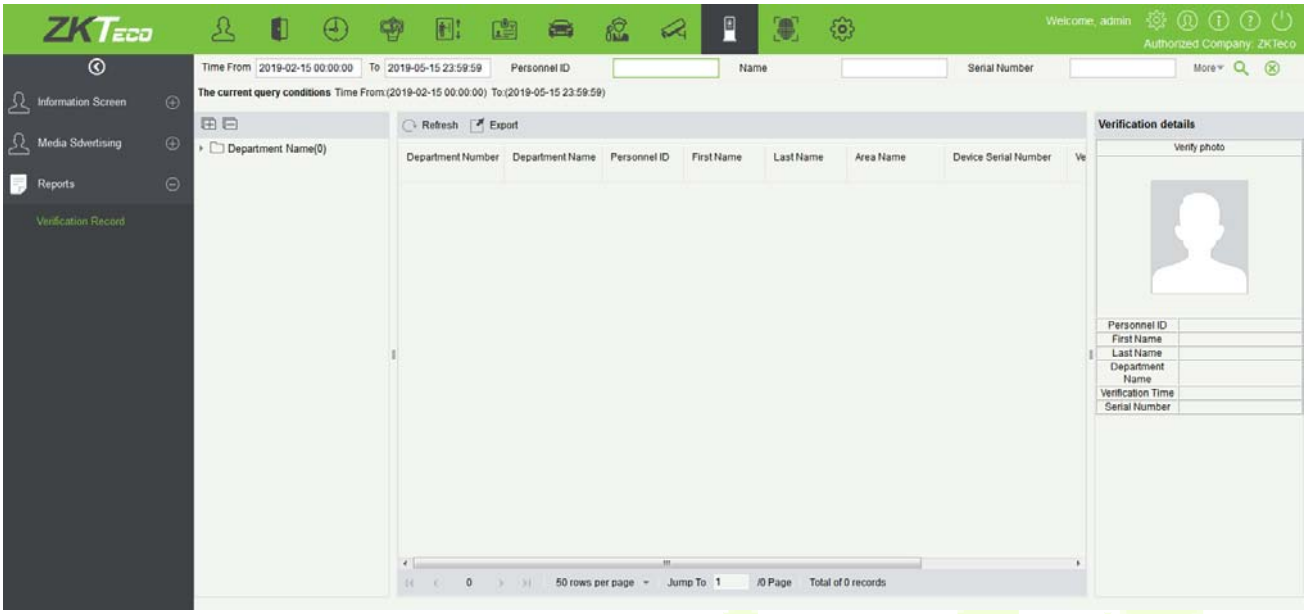


Delete: It can support to delete the advertising.

13.3 Reports

13.3.1 Verification Record

Click [**Reports**] > [**Verification Record**] to view specified events in specified condition. The options are same as those of [**Verification Record**].



14 Face Intellect

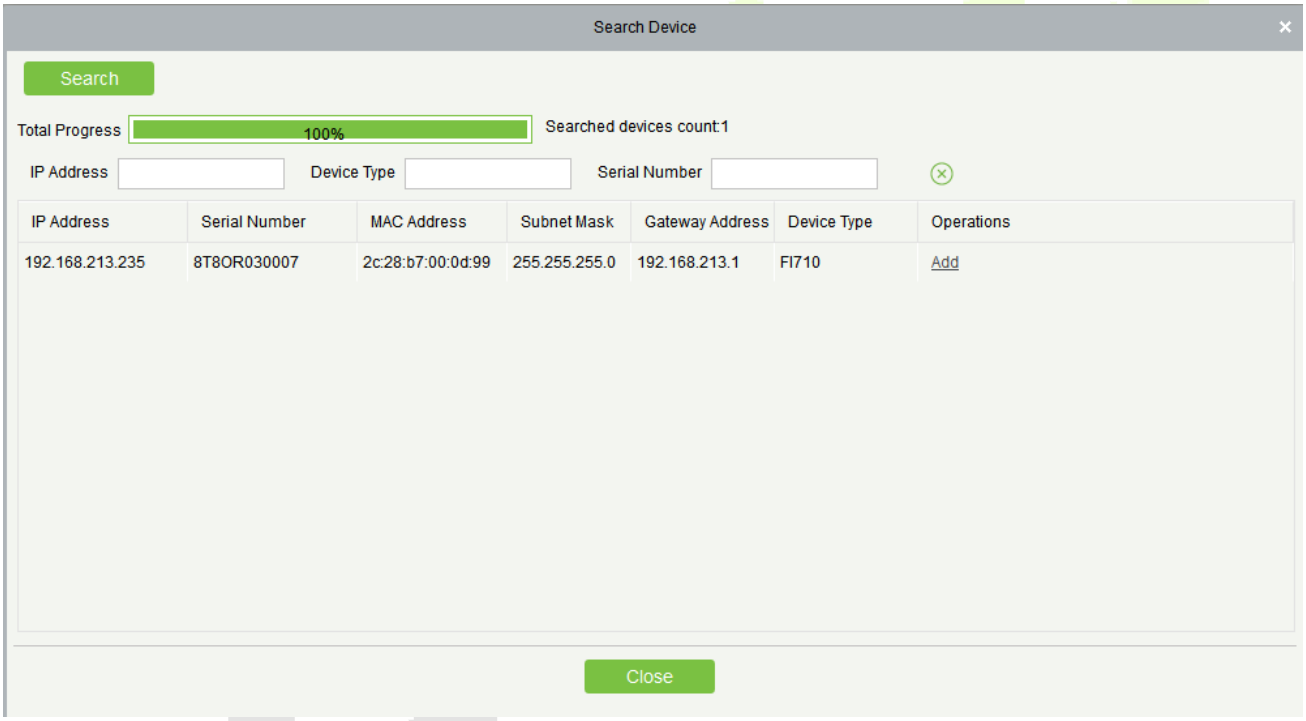
Face Intellect Device used the push protocol to communication with the software. It can support to setting the Face Intellect device as the reader , and then used the Face Intellect device to verification the user facial ,according the verification result to make the decision whether if open door.

14.1 Face Intellect Device

14.1.1 Device

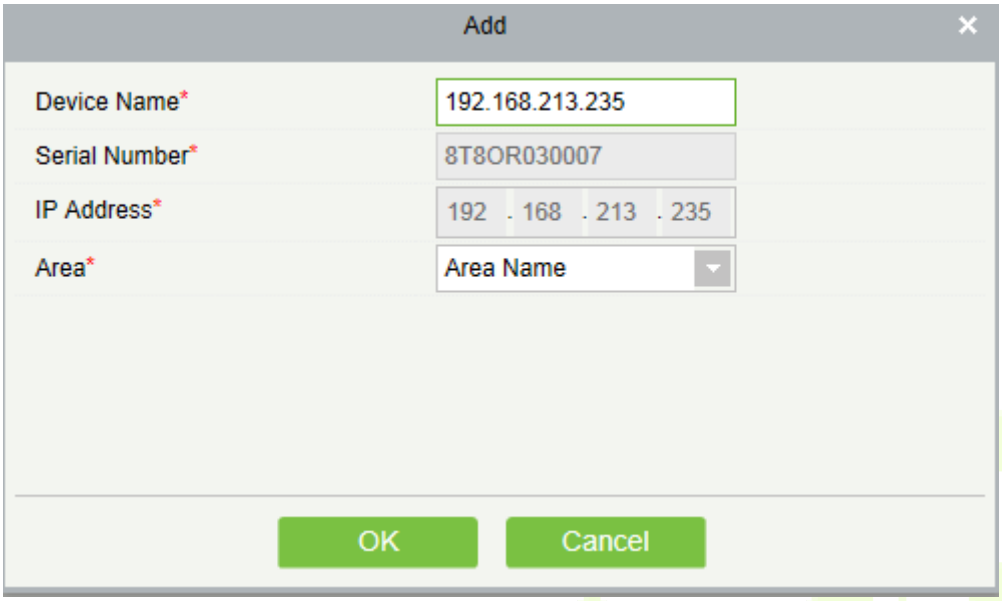
Search Device

Click **[Face Intellect Device]** > **[Device]** > **[Search Device]**:



Add Device

Click the **[Add]**, the system will show the menu, user can typing the important information, click the **[OK]** button.



Upgrade Firmware

Tick the device that needs to be upgraded, click **[Upgrade firmware]** to enter edit interface, then click **[Browse]** to select firmware upgrade file (named emfw.cfg) provided by Access software, and click **[OK]** to start upgrading.

✍**Note:** The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware or upgrade it following the instructions of the distributor. Unauthorized upgrade may affect normal operations.

Synchronize Time

It will synchronize device time with server's current time.

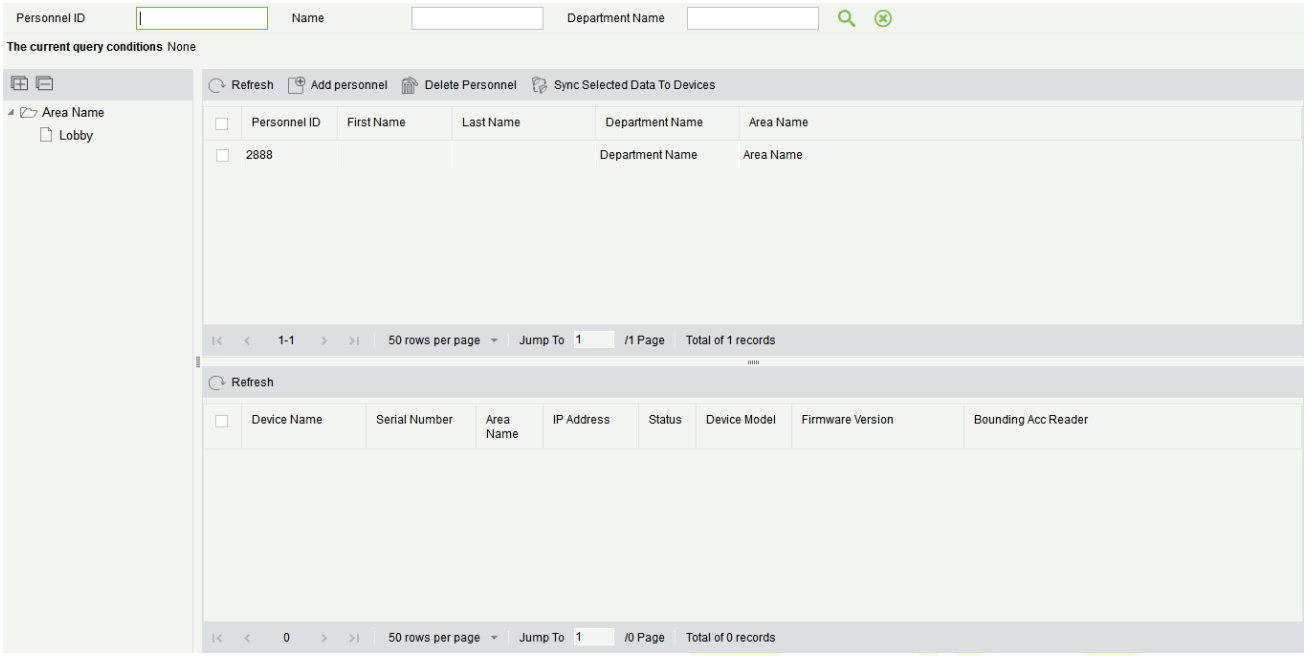
Synchronize All Data to Devices

Synchronize data of the system to the device. Select device, click **[Synchronize All Data to Devices]** and click **[OK]** to complete synchronization.

14.1.2 Personnel in Area

Add Personnel

Click **[Personnel in Area]** > **[Area]** > **[Add Person]**:



Delete Personnel

Click **[Personnel in Area]** > **[Area]** >select the person > **[delete Person]**:

Sync Selected Data to Devices

Synchronize selected data to the device. Select area, click **[Sync Select Data to Devices]** and click **[OK]** to complete synchronization.

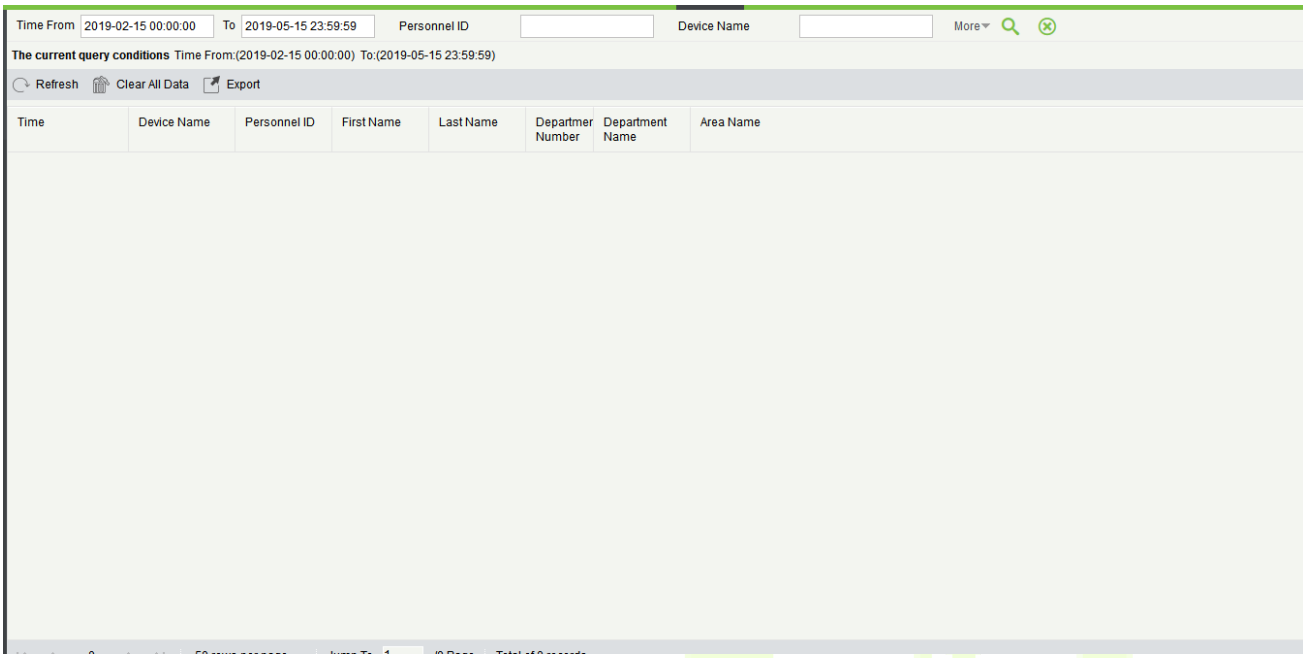
14.2 Reports

14.2.1 All Transactions

✍**Note:** Here have two cases.

1) If the user setting the Face Intellect device connect with the lock directly, Once the validation is successful, the record is displayed in the report

2) If the user setting the Face Intellect device as the reader with the access device. All the record will be show on the access module. And can't show on this report.



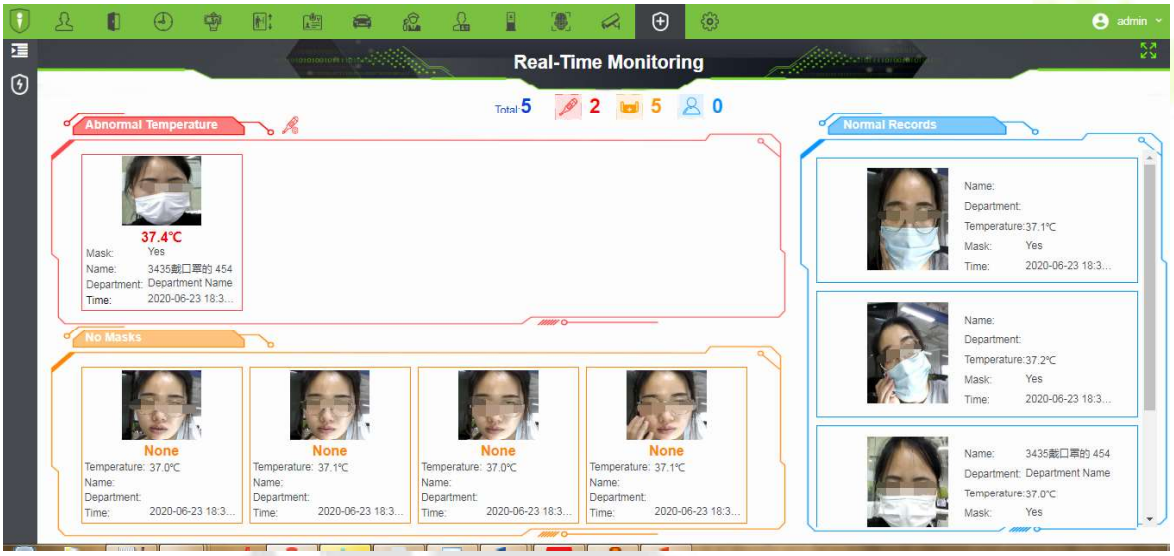
16 Temperature Detection

MTD (Mask and Temperature Detection) module is primarily designed to work with the access control devices which have body temperature detection and mask detection features. It provides real-time monitoring of temperature and mask detection of all the users and various analysis reports.

16.1 Temperature Management

16.1.1 Real-Time Monitoring

Click [**Temperature Detection**] > [**Temperature Management**] > [**Real-Time Monitoring**].



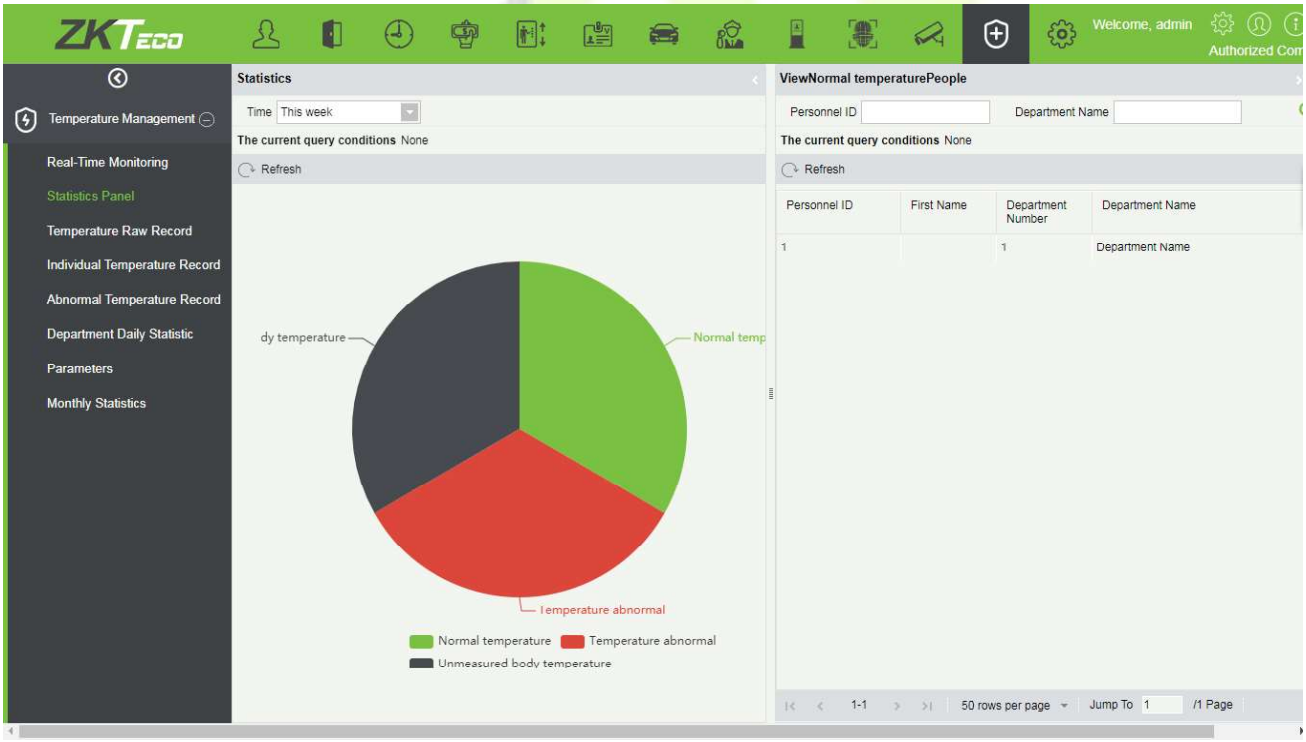
The Real-Time Monitoring interface allows the user to monitor the body temperature of the users with their image captured during verification. The mask and temperature data is collected at every entry and exit point of the premises if the personnel is registered in the device. There are 3 different categories of records that are displayed on the monitoring page. They are:

- Personnel with abnormal temperature (masked or unmasked).
- Personnel without a mask.
- Personnel with normal body temperature and mask.

The system allows the users to set the body temperature threshold which determines the category that the user data will be recorded i.e Abnormal Temperature or Normal Temperature.

16.1.2 Statistic Panel

Click [**Temperature Detection**] > [**Temperature Management**] > [**Statistic Panel**].



The statistics panel provides statistical data for the Administrators to analyze the number of users with normal body temperature, abnormal temperature, and unmeasured body temperature in a specific time period. The statistics can be filtered by time i.e., Today, This Week, and This Month.

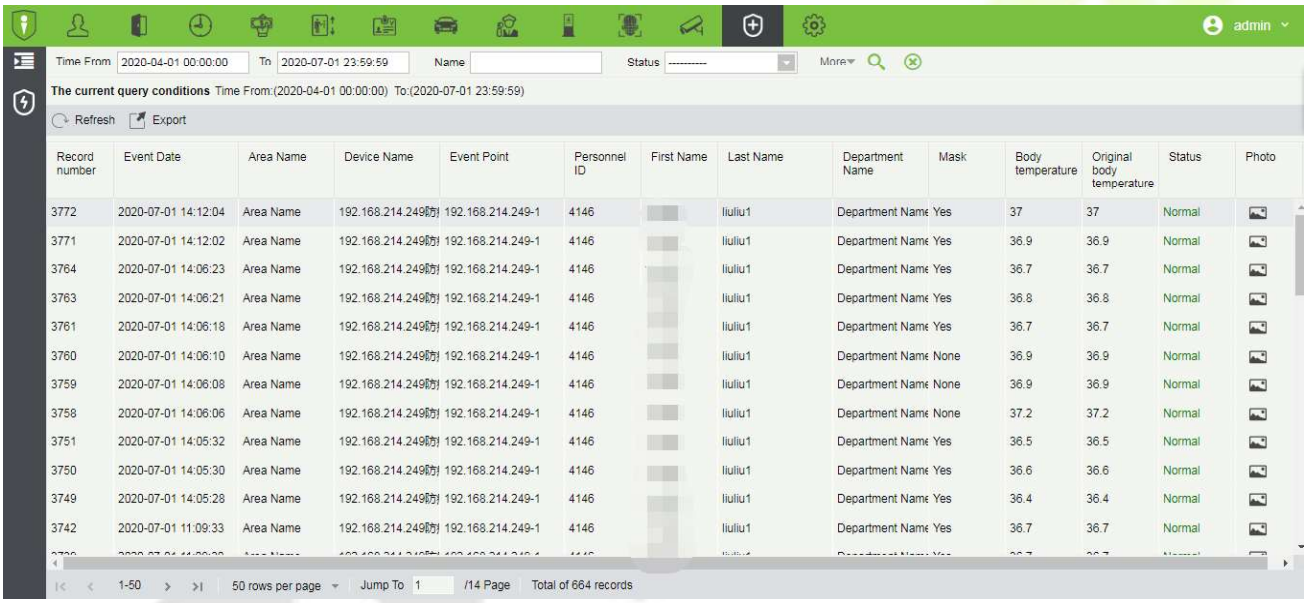
You can also click on any category on the Pie-chart and the corresponding personnel details will be displayed on the right side of the interface. Also, personnel can be searched by entering the Personnel ID or Department Name on the top-right corner of the interface.

✍**Note:** The statistics are only available for system personnel.

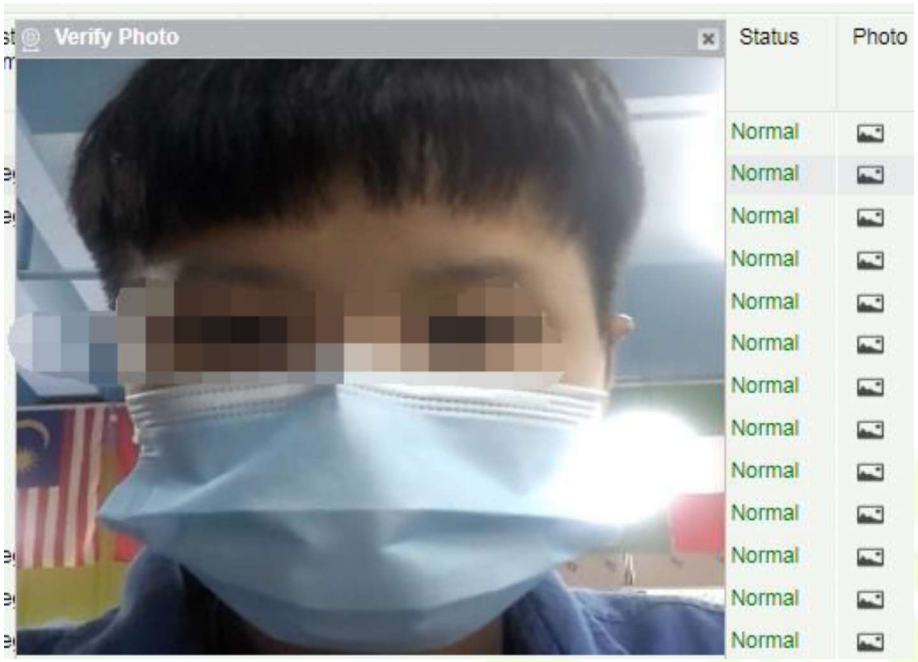
16.1.3 Temperature Raw Record

Click [**Temperature Detection**] > [**Temperature Management**] > [**Temperature Raw Record**].

The **Temperature Raw Record** displays the reports in event-time order i.e. sequentially as it happens regardless of Normal Temperature/Abnormal Temperature/Department/Masked/Unmasked. It also displays the Department Name, Body Temperature, Status, and Photo which a user can check instantly after verification.



Click the **IMAGE** icon to view the captured photo.



Export

Temperature+Raw+Record

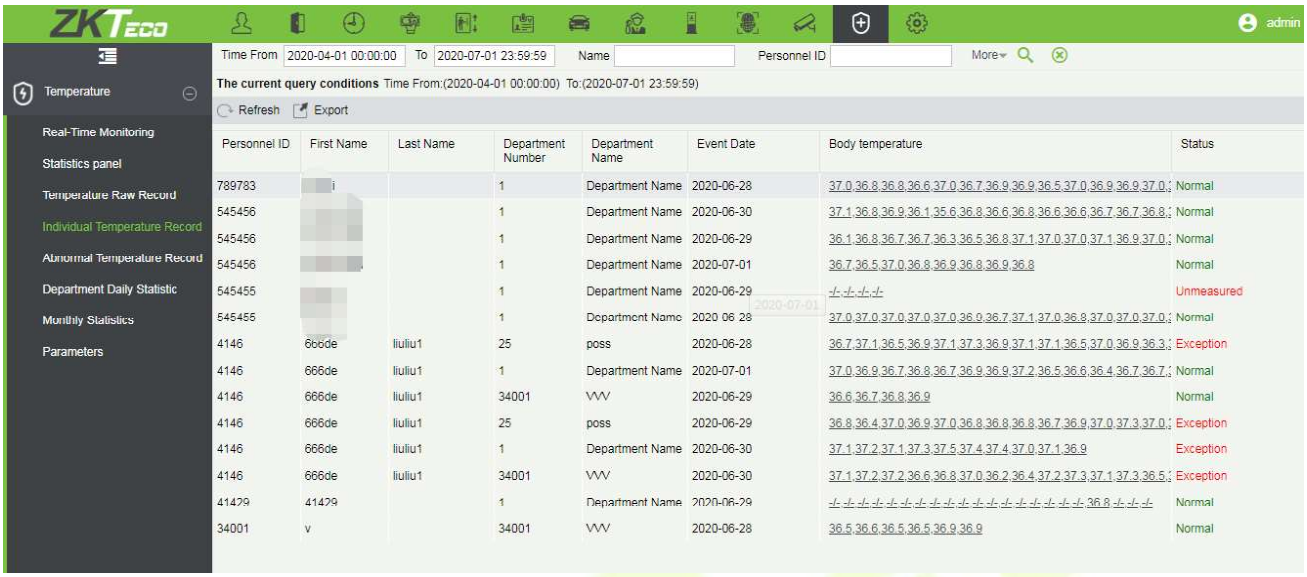
Record number	Event Date	Area Name	Device Name	Event Point	Personnel ID	First Name	Last Name	Department Name	Mask	Body temperature	Original body temperature	Sta
3772	2020-07-01 14:12:04	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	37.0	37.0	Nor
3771	2020-07-01 14:12:02	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.9	36.9	Nor
3764	2020-07-01 14:06:23	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.7	36.7	Nor
3763	2020-07-01 14:06:21	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.8	36.8	Nor
3761	2020-07-01 14:06:18	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.7	36.7	Nor
3760	2020-07-01 14:06:10	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	None	36.9	36.9	Nor
3759	2020-07-01 14:06:08	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	None	36.9	36.9	Nor
3758	2020-07-01 14:06:06	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	None	37.2	37.2	Nor
3751	2020-07-01 14:05:32	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.5	36.5	Nor

✍Note:

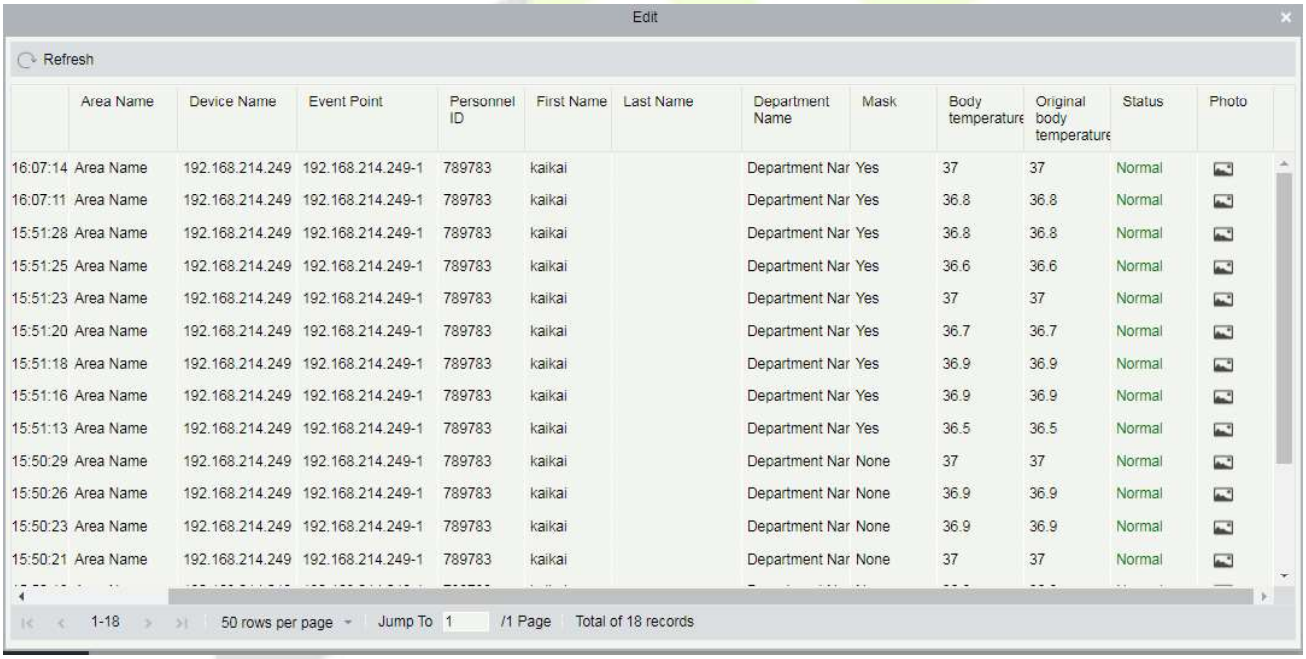
- If the Personnel ID field is blank, it represents a Visitor.
- The "Original body temperature" is usually measured by the device, and it can't be modified. But the "Body Temperature" can be revised in "Abnormal Temperature Record".

16.1.4 Individual Temperature Record

This report displays all the body temperature details of a User or Personnel daily.



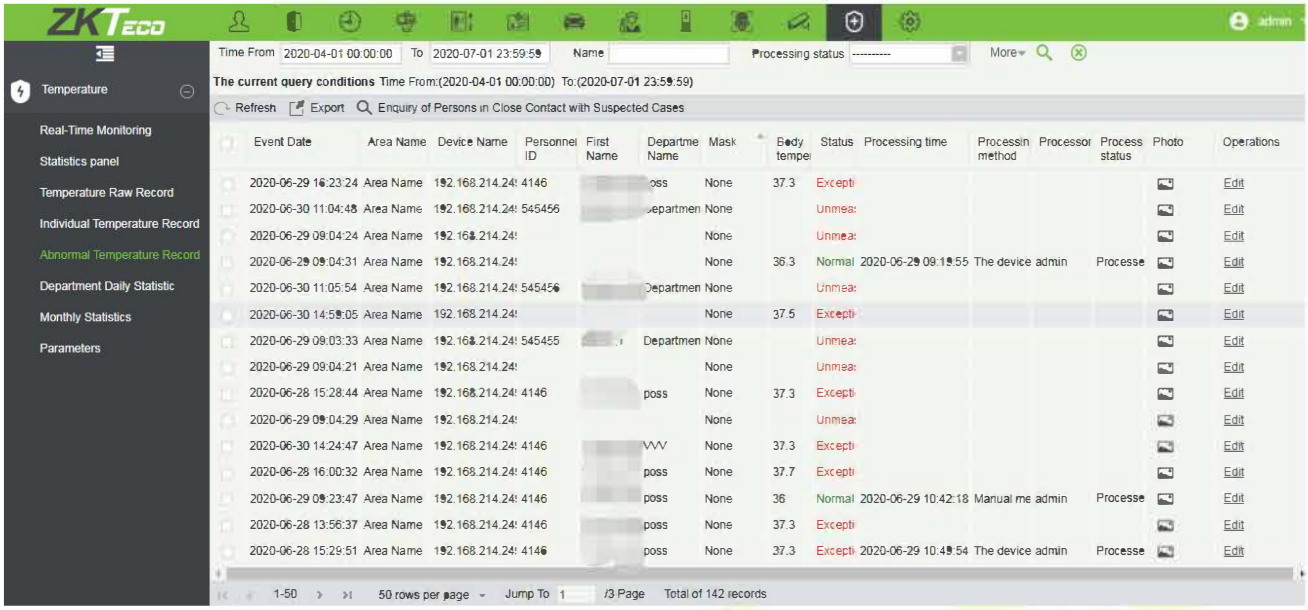
Click **Body Temperature** to view the details of each record.



16.1.5 Abnormal Temperature Record

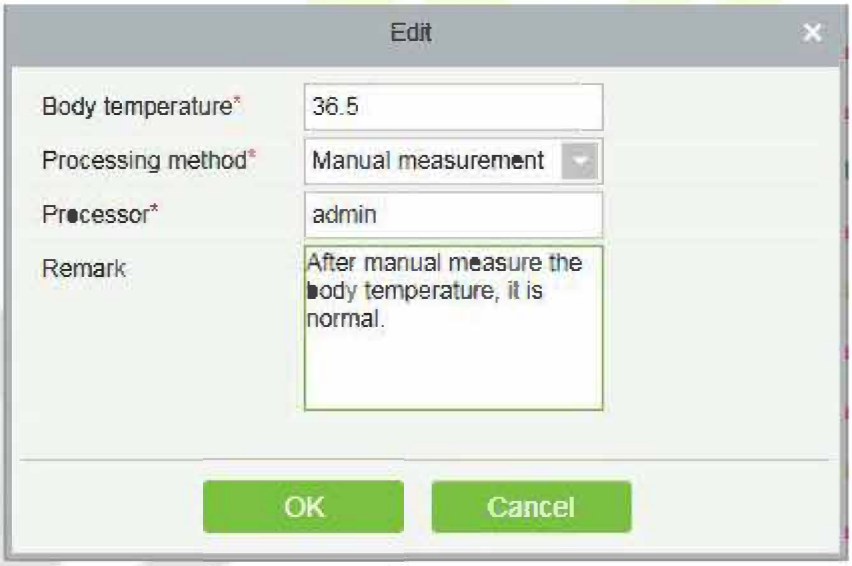
It displays the record of exceptional body temperatures i.e. above the body temperature threshold and the temperature of personnel which is not detected.

Click **[Temperature Detection]** > **[Temperature Management]** > **[Abnormal Temperature Record]**.



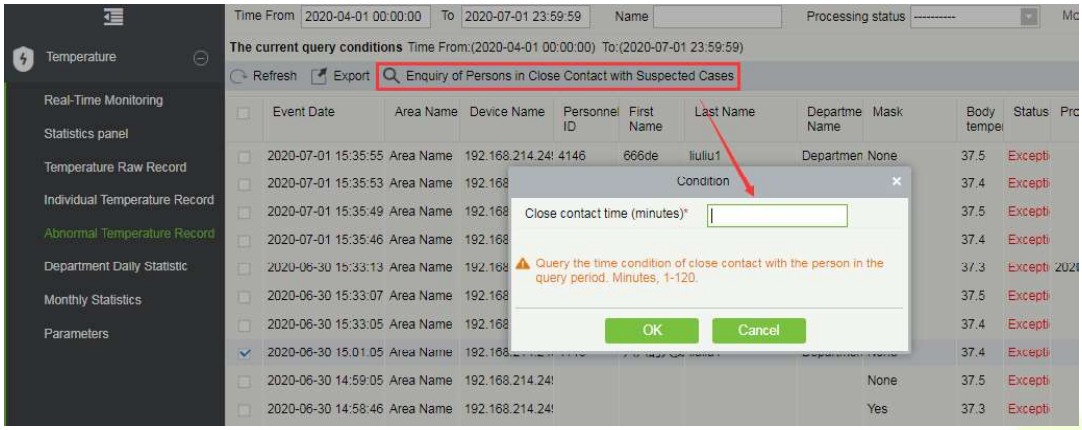
Edit

Click the **Edit** option to revise the user's body temperature by manual detection. The edit window pops-up as shown below:

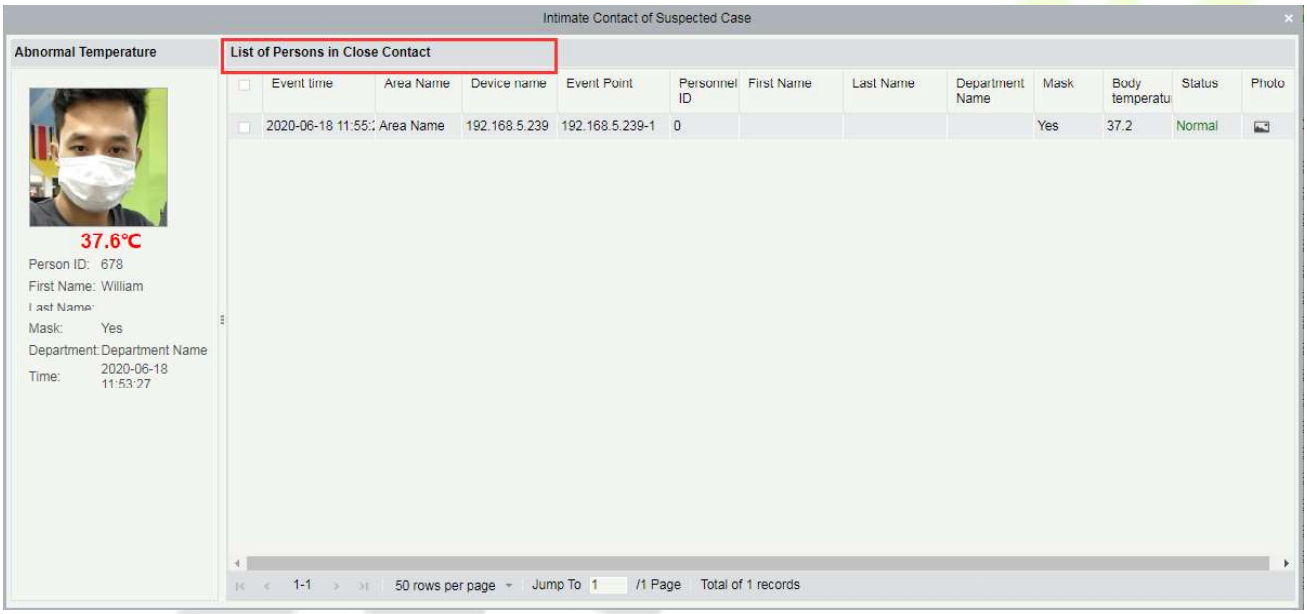


Inquiry of Persons in Close Contact with Suspected Cases

It will help the user to check the personnel who had contact with any suspected persons. Enter the contact time, 1 to 120 minutes is applicable.

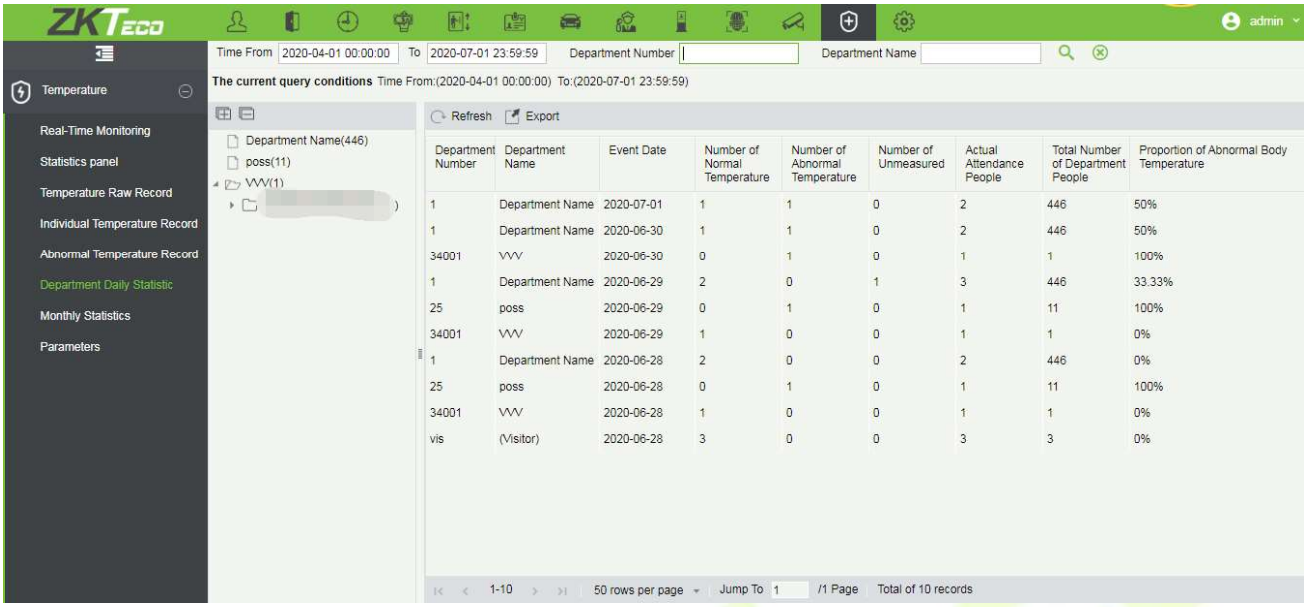


Click **OK** to view the search results.



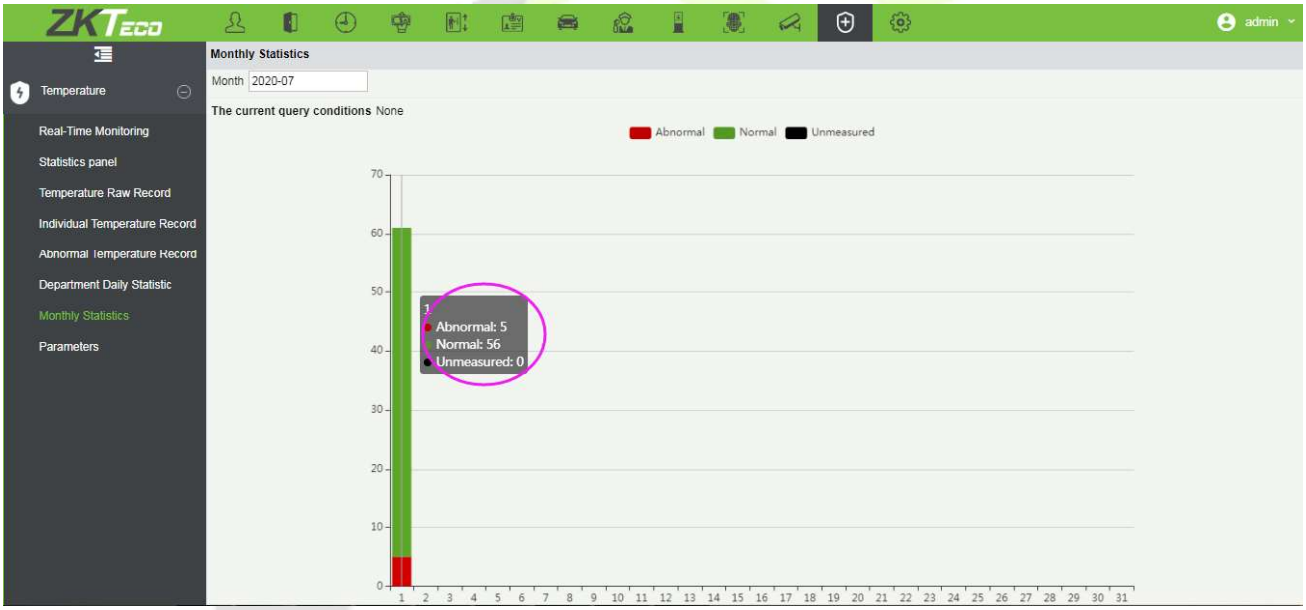
16.1.6 Department Daily Statistics

It displays the department-wise temperature detection records. A user can select a department from the list of departments in the left panel which displays the number of persons with normal temperature, abnormal temperature, and unmeasured in the specific department daily. It also displays the proportion of abnormal body temperature.



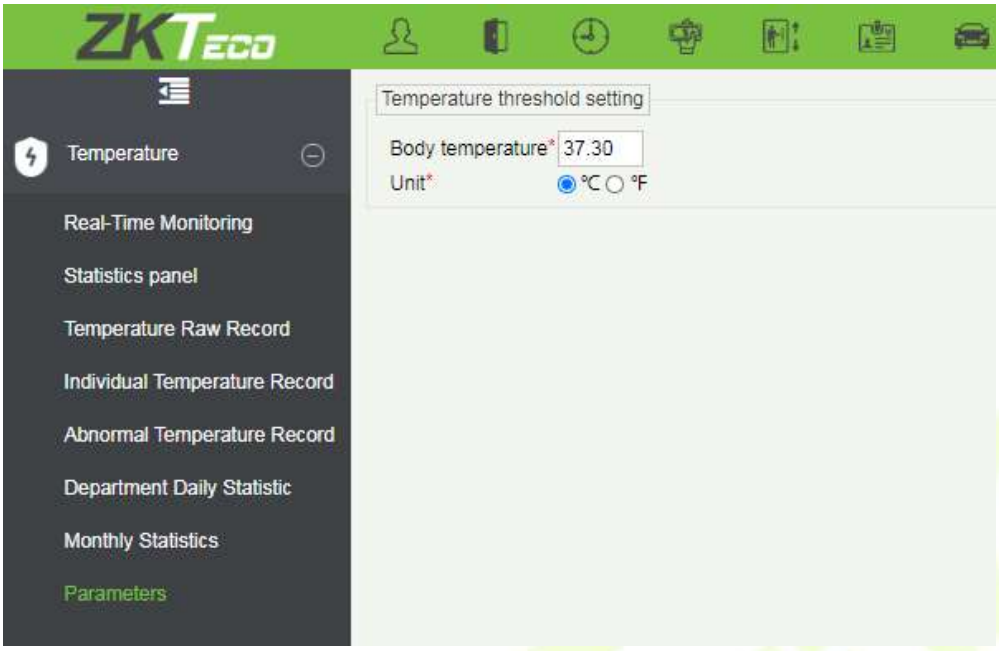
16.1.7 Monthly Statistics

Click **[Temperature Detection]** > **[Temperature Management]** > **[Monthly Statistic]** to view the infographics of monthly temperature detection.



16.1.8 Parameters

It allows the user to set the body temperature threshold which determines the category to which the recorded temperature falls-in i.e Abnormal Temperature or Normal Temperature. For example, assume that the threshold temperature is set to 37.3°C. If the recorded temperature is 37°C, it will be saved as "Normal Temperature" and if the recorded temperature is 38°C, it will be saved as "Abnormal Temperature". The temperature unit can also be chosen between °C or °F.



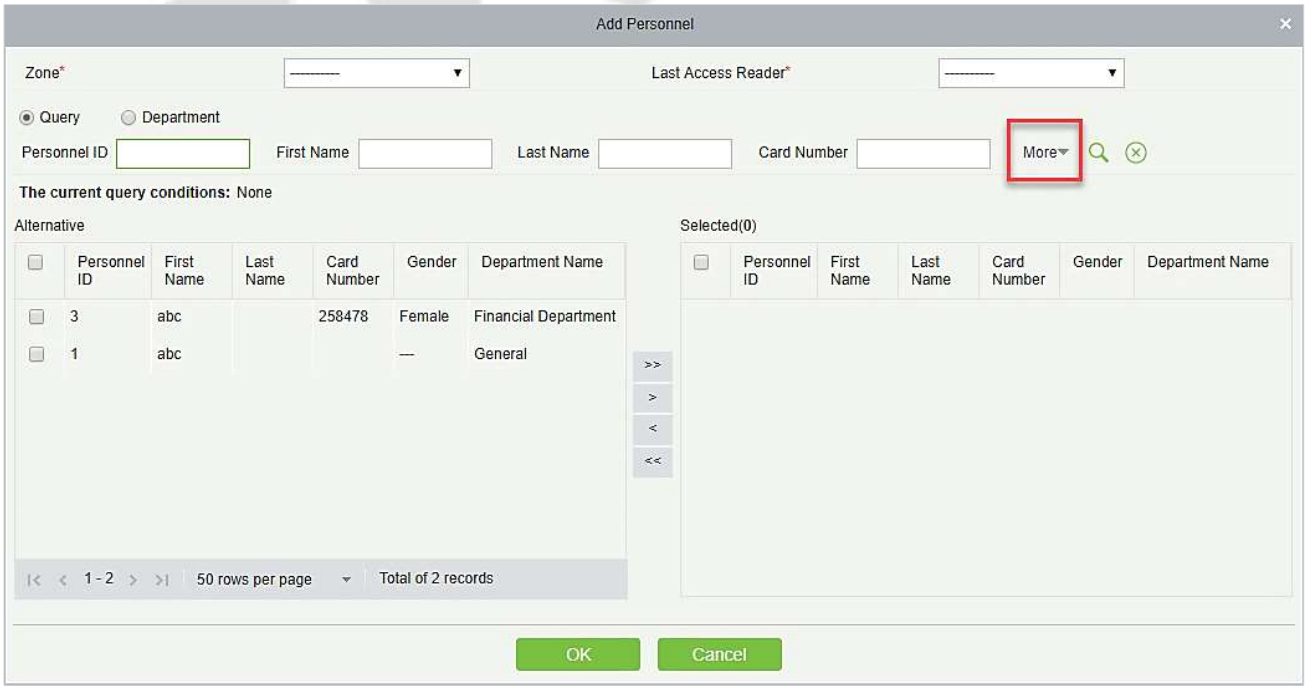
✍**Note:** After setting the body temperature threshold, the Real-Time Monitoring Page will refresh, and the persons will be categorized according to the new threshold temperature.

17 Appendices

Common Operations

- **Select Personnel**

The selected personnel page in the system is as below:



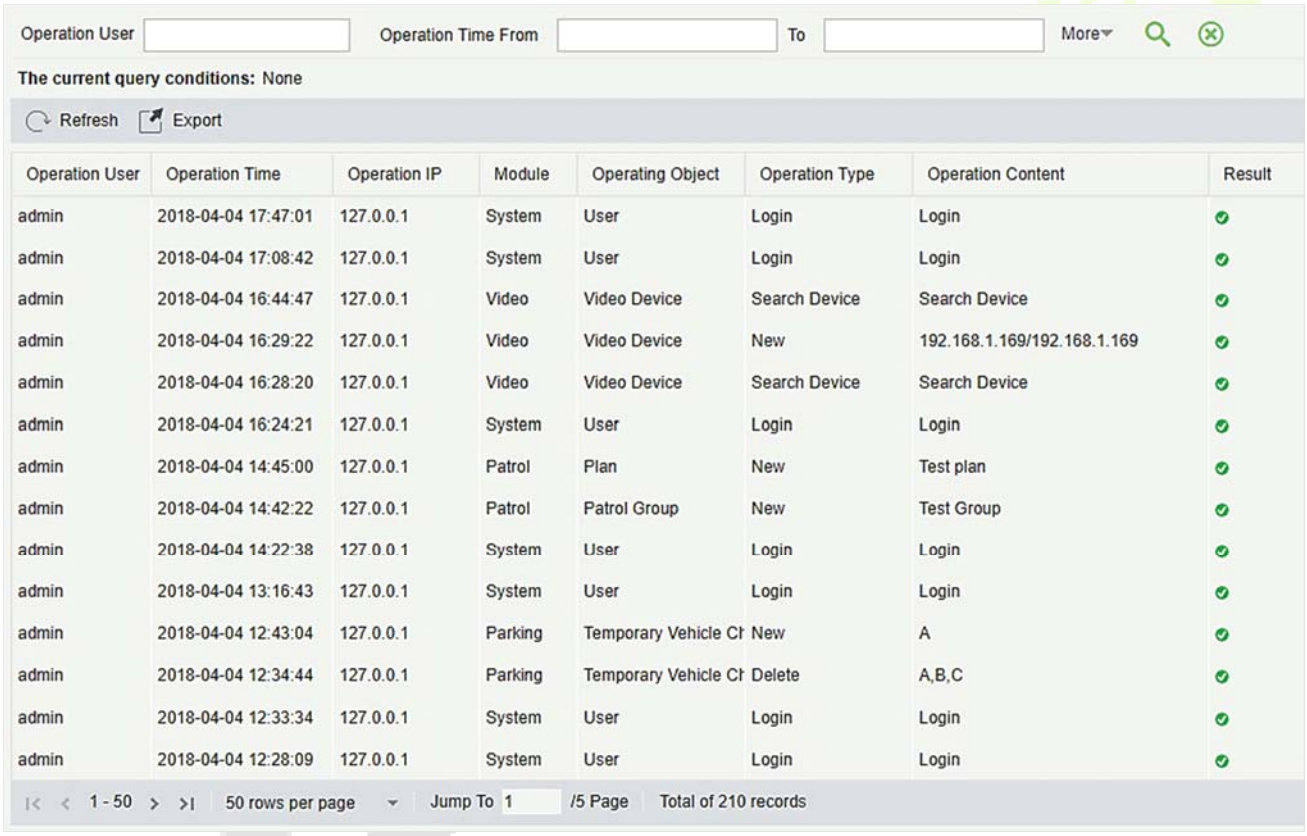
15 System Management

System settings primarily include assigning system users (such as company management user, registrar, access control administrator) and configuring the roles of corresponding modules, managing database, setting system parameters and view operation logs, etc.

15.1 Basic Management

15.1.1 Operation Log

Click [**System**] > [**Basic Management**] > [**Operation Log**]:



All operation logs are displayed in this page. You can query specific logs by conditions.

Export: Export the operation log records, save to local. You can export to an Excel, PDF, or CSV file. See the following figure.

ZKTECO

Operation Log

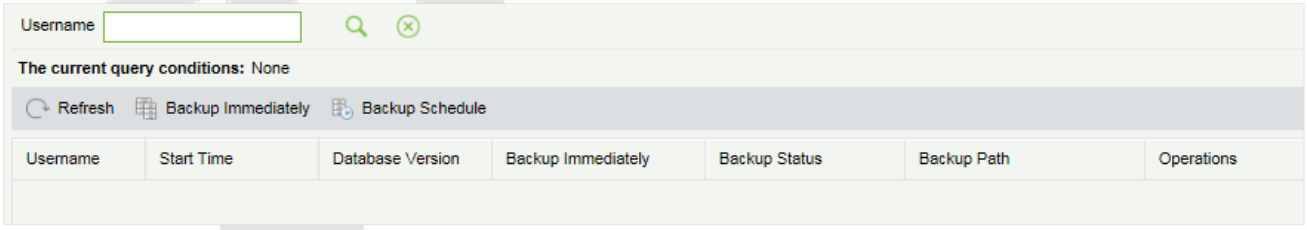
Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result
admin	2017-12-18 15:06:35	127.0.0.1	Visitor	Visitor	Export	Export	Succeed
admin	2017-12-18 15:03:40	127.0.0.1	Elevator	Access Rights By Personnel	Export	Export	Succeed
admin	2017-12-18 15:03:17	127.0.0.1	Elevator	Access Rights By Floor	Export	Export	Succeed
admin	2017-12-18 15:02:59	127.0.0.1	Elevator	All Exception Events	Export	Export	Succeed
admin	2017-12-18 15:01:27	127.0.0.1	Elevator	All Transactions	Export	Export	Succeed
admin	2017-12-18 14:25:34	127.0.0.1	Attendance	Appended Receipt	Export	Export	Succeed
admin	2017-12-18 14:24:41	127.0.0.1	Attendance	Leave	Export	Export	Succeed
admin	2017-12-18 14:24:05	127.0.0.1	Attendance	Leave	Export	Export	Succeed
admin	2017-12-18 14:23:45	127.0.0.1	Attendance	Business Trip	Export	Export	Succeed
admin	2017-12-18 14:23:25	127.0.0.1	Attendance	Go Out	Export	Export	Succeed
admin	2017-12-18 14:22:26	127.0.0.1	Attendance	Overtime	Export	Export	Succeed
admin	2017-12-18 14:13:29	127.0.0.1	Attendance	Overtime	Export	Export	Succeed
admin	2017-12-18 14:06:58	127.0.0.1	Attendance	Adjust and Append	Export	Export	Succeed
admin	2017-12-18 14:04:21	127.0.0.1	Attendance	Adjust Shift	Export	Export	Succeed
admin	2017-12-18 14:02:21	127.0.0.1	Attendance	Adjust Shift	New	5	Succeed
admin	2017-12-18 14:00:27	127.0.0.1	Attendance	Adjust Shift	New	4;3	Succeed
admin	2017-12-18 13:56:27	127.0.0.1	Attendance	Adjust Shift	New	3	Succeed
admin	2017-12-18 13:55:40	127.0.0.1	Attendance	Adjust and Append	New	3;;3	Succeed

Created on: 2017-12-18 15:07:23

 1/25

15.1.2 Database Management

Click [**System**] > [**Basic Management**] > [**Database Management**]:



All history operation logs about database backup are displayed in this page. You can refresh, backup and schedule backup database as required.

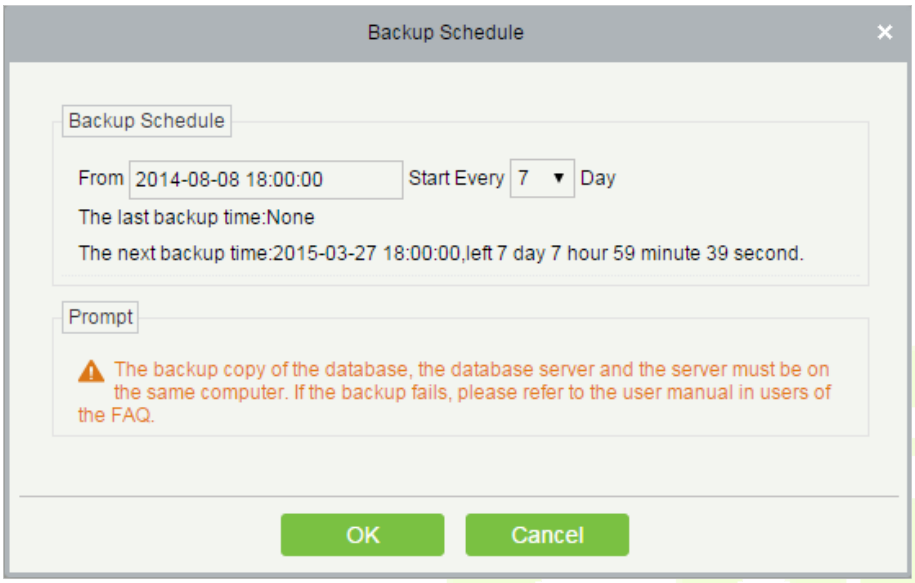
- **Backup Immediately**

Backup database to the path set in installation right now.

✍**Note:** The default backup path for the system is the path selected during the software installation. For details, refer to '*Software Installation Guide*'.

Backup Schedule

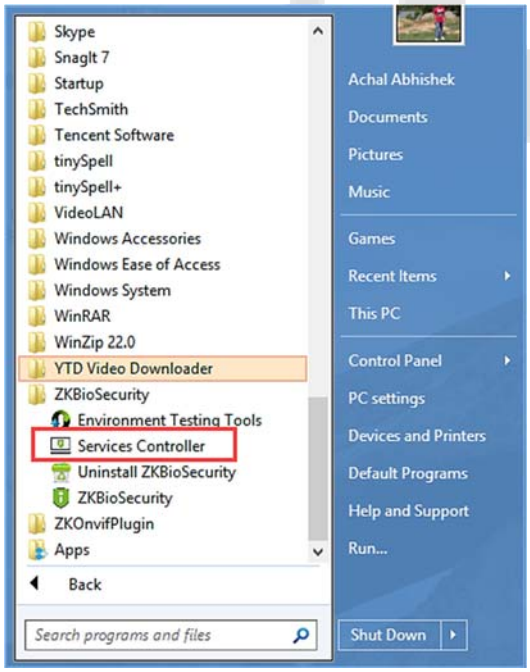
Click **[Backup Schedule]**:

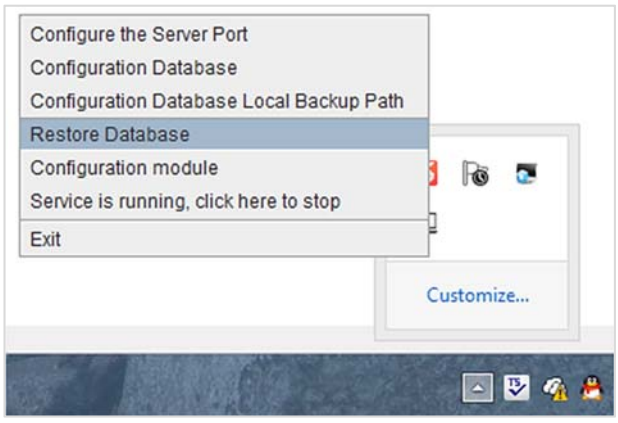


Set the start time, set interval between two automatic backups, click **[OK]**.

Restore Database

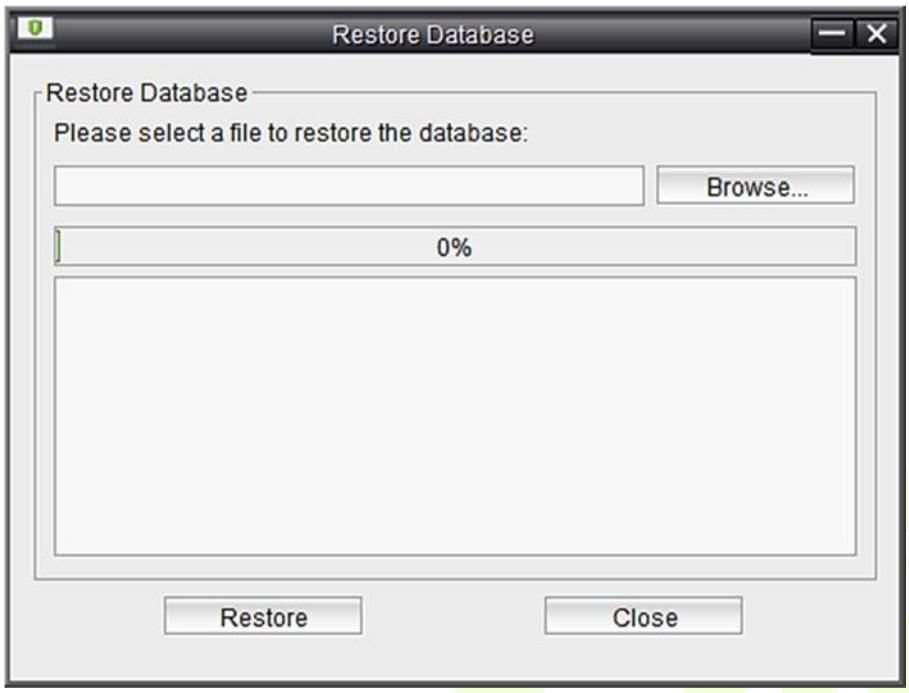
1) Click the start menu of the PC > [**All programs**] > [**ZKBioSecurity**] > Then run "Services Controller", and you can find out the icon of "Services Controller" in Taskbar as follow, right click that icon, then left click "Restore Database".





2) In the popup window, click "Browse" to choose the backup file to restore the database.

✍**Note:** Before restoring a database, it is recommended that you back up the current database to avoid data loss.



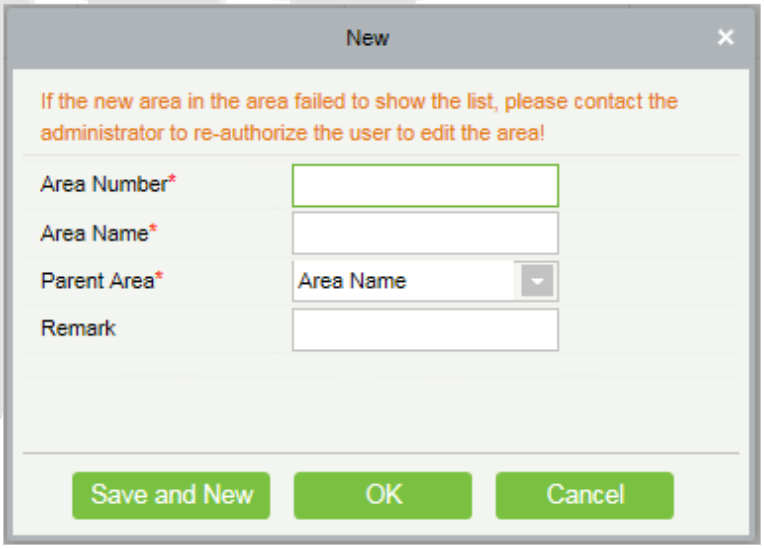
15.1.3 Area Setting

Area is a spatial concept which enables the user to manage devices in a specific area. After area setting, devices (doors) can be filtered by area upon real-time monitoring.

The system, by default, has an area named **[Headquarters]** and numbered **[1]**.

- **Add an Area**

Click **[System]** > **[Area Setting]** > **[Area]** > **[New]**:



Fields are as follows:

Area Number: It must be unique.

Area Name: Any characters with a length less than 30.

Parent Area: Determine the area structure of system.

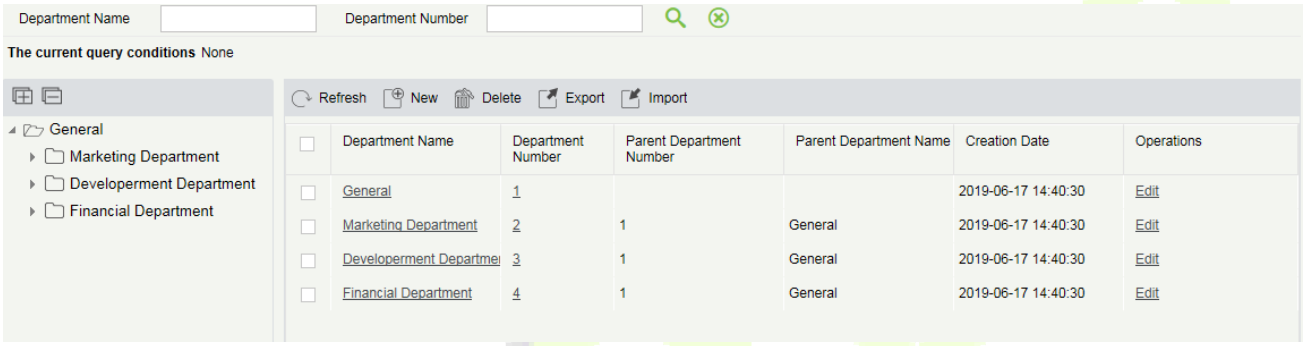
Click [**OK**] to finish adding.

- **Edit/Delete an Area**

Click [**Edit**] or [**Delete**] as required.

15.1.4 Department

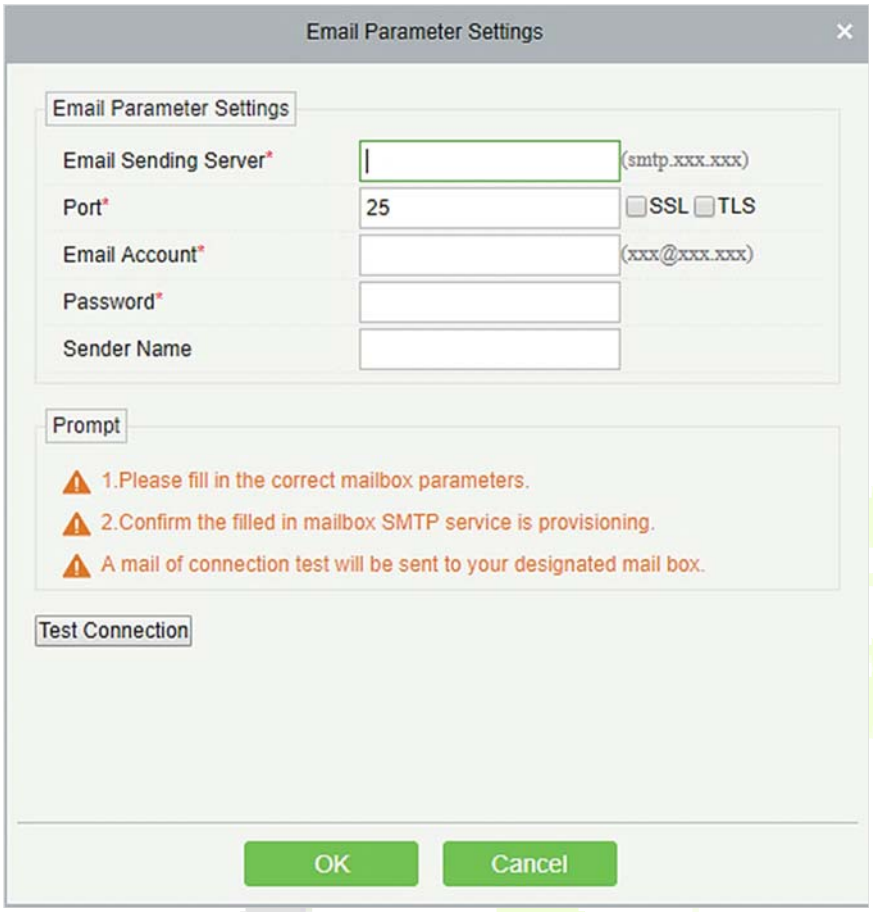
Click [**System**] > [**Department**] to manage the department information:



15.1.5 E-mail Management

Set the email sending server information. The recipient e mail should be set in Linkage Setting.

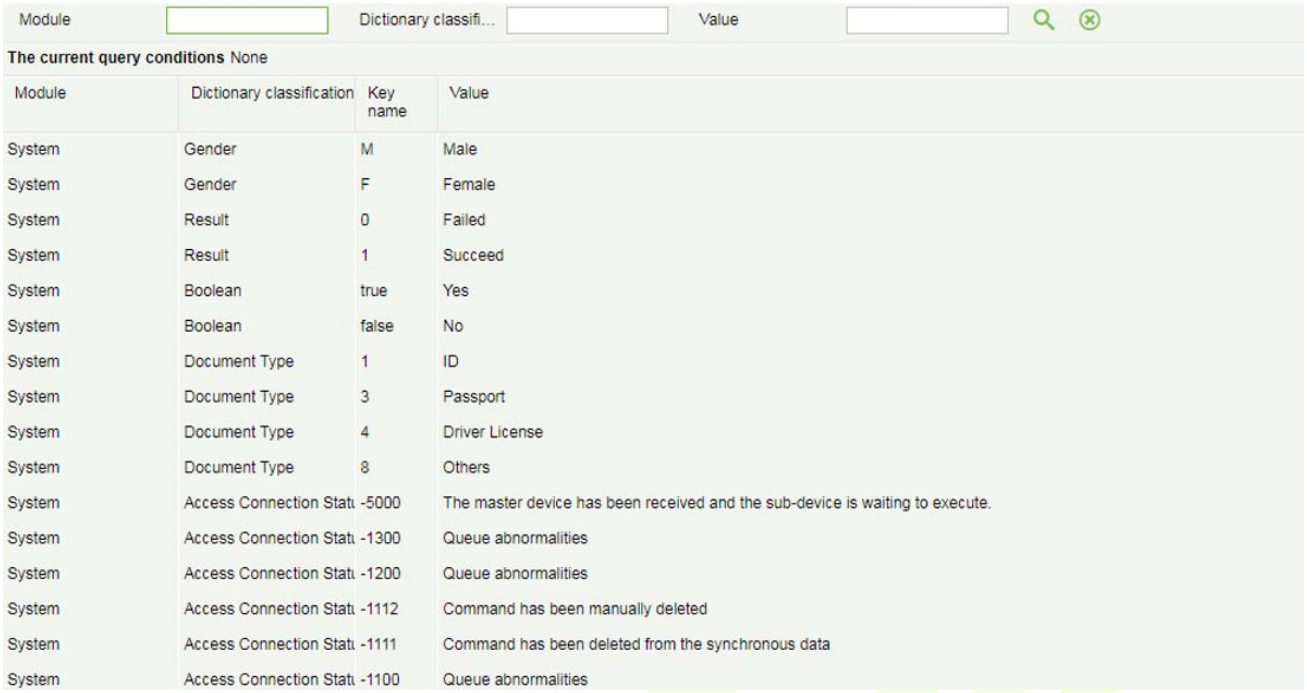
Click **[Basic Management]** > **[Email Management]** > **[Email Parameter Settings]**:



✍**Note:** The domain name of E-mail address and E-mail sending sever must be identical. For example, the Email address is: test@gmail.com, and the E-mail sending sever must be: smtp.gmail.com.

15.1.6 Dictionary Management

Data dictionary management function, users can find the meaning of error code and self-check software errors.



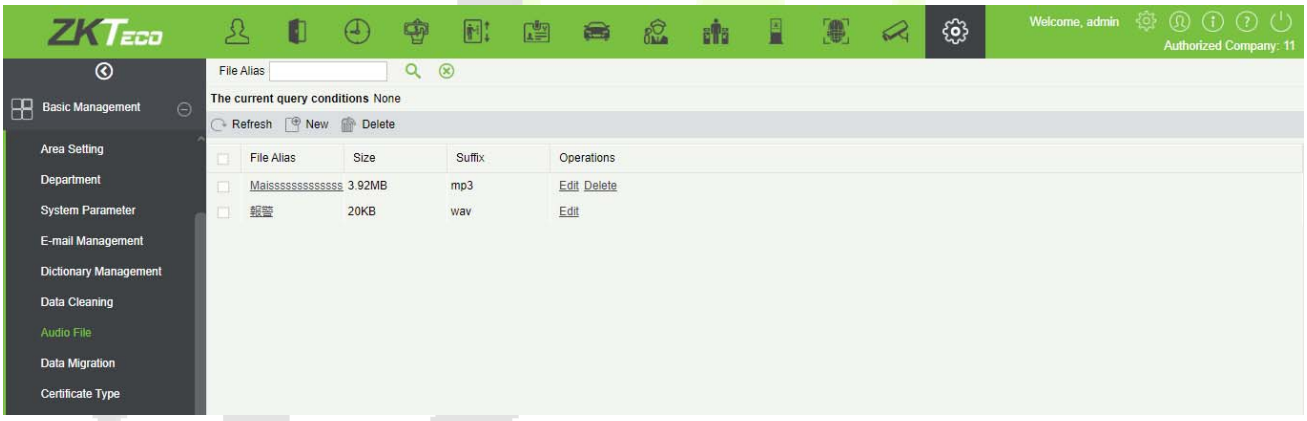
Module | Dictionary classifi... | Value

The current query conditions None

Module	Dictionary classification	Key name	Value
System	Gender	M	Male
System	Gender	F	Female
System	Result	0	Failed
System	Result	1	Succeed
System	Boolean	true	Yes
System	Boolean	false	No
System	Document Type	1	ID
System	Document Type	3	Passport
System	Document Type	4	Driver License
System	Document Type	8	Others
System	Access Connection Stati	-5000	The master device has been received and the sub-device is waiting to execute.
System	Access Connection Stati	-1300	Queue abnormalities
System	Access Connection Stati	-1200	Queue abnormalities
System	Access Connection Stati	-1112	Command has been manually deleted
System	Access Connection Stati	-1111	Command has been deleted from the synchronous data
System	Access Connection Stati	-1100	Queue abnormalities

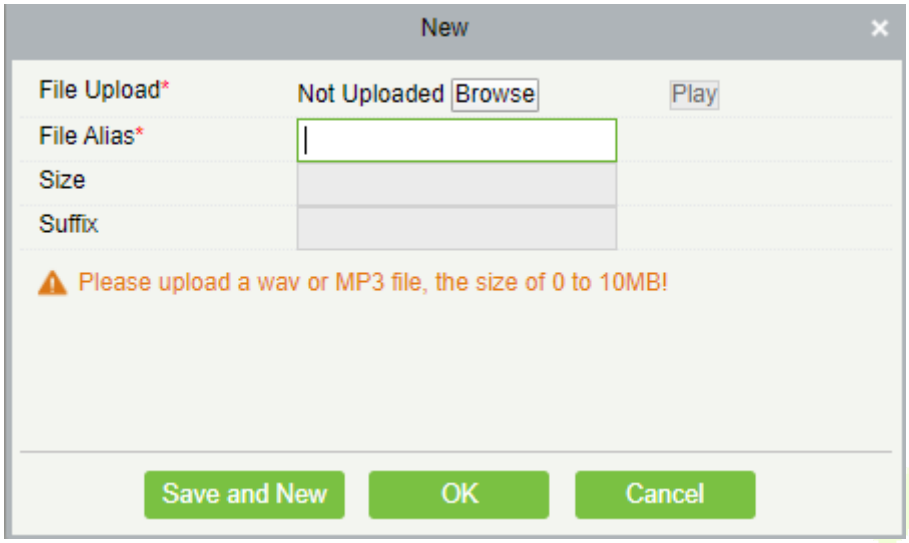
15.1.7 Audio File

Click **[System]>[Basic Management]>[Audio File]** to open the following interface:



- **Add**

1) Click [**System**]>[**Basic Management**]>[**Audio File**]>[**New**], the following window appears:



2) Click [**Browse**] to upload an audio file locally. The file format must be in WAV or mp3 format and must not exceed 10M in size.

File Alias(Name): Any character, up to 30 characters.

Size: After uploading the file, the file size is automatically generated.

Suffix: After uploading the file, the suffix of the file is automatically generated.

- **Edit**

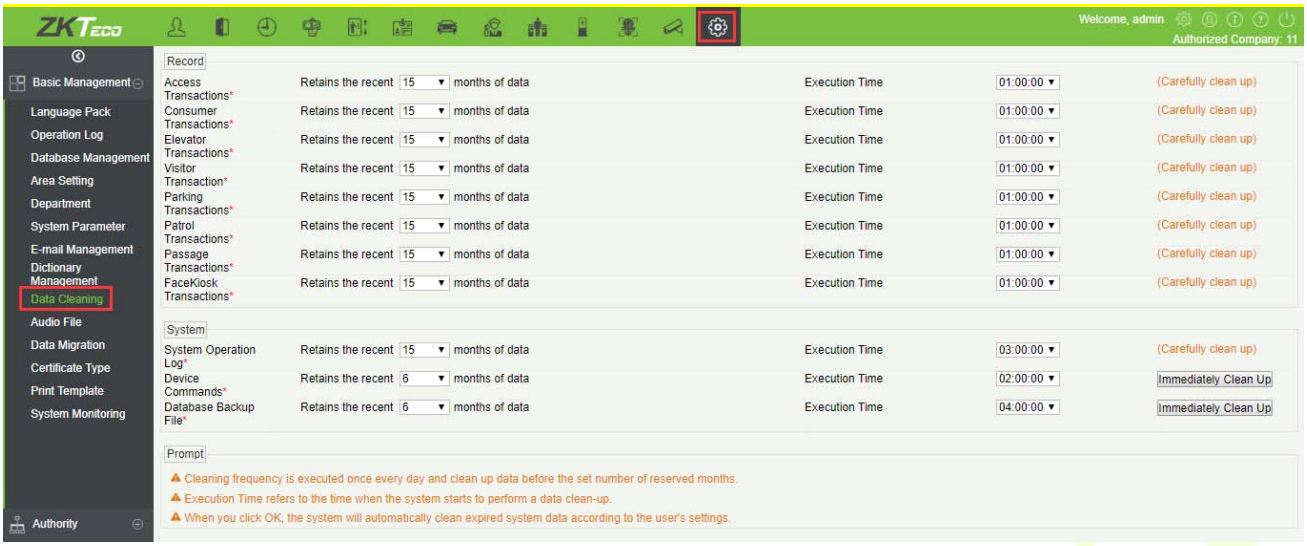
Click the file name or [**Edit**] to edit the audio file details which supports replacing the audio files and editing the file name.. The "size" and "suffix" automatically change depending on the size and type of audio file being uploaded. After editing, click [**OK**] and exit.

- **Delete**

Select the specified audio file to delete and click [Delete].

15.1.8 Data Cleaning

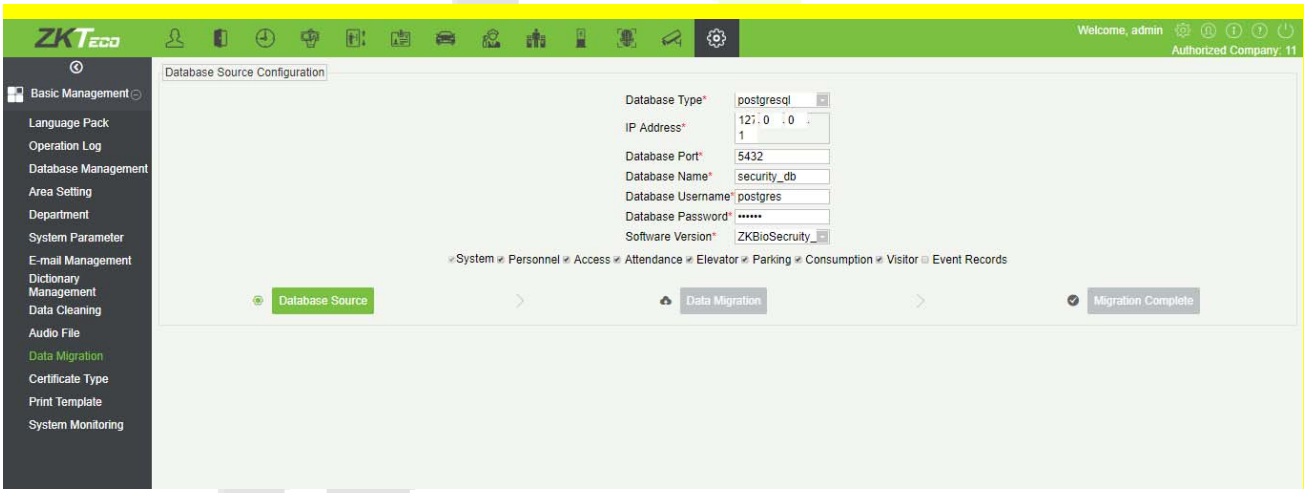
To save the disk storage space, the expired data generated by the system must be cleaned up regularly. Click [**System**]> [**Basic Management**]> [**Data Cleaning**].



15.1.9 Data Migration

The Software supportsmigration from 3150 to V5000, including various modules and events (except the patrol module). Here, you have to configure the Database type, IP address, database port, database name, database user name, database password, and software version. Select the modules to be migrated for automatic migration.

Click [**System Management**]> [**Basic Management**]> [**Data Migration**].



✍Notes:

1. 3150 and V5000 are installed on the same server.

① Before installing V5000, you need to close the 3150 Tomcat service as well as the WatchDog service and remove the environment variable SEC.

② When installing, make sure the 3150 and V5000 communication ports are the same.

③ The first migration must be thePersonnel module.

④ Check the event records (not checked by default): The access, elevator, attendance, patrol and video modules need to select the event records to transfer the records. There is no need to check the event records for visitor, parking, consumption modules and the event record will be migrated by default.

⑤ After all the modules are migrated, the parameter settings for each module need to be set again.

⑥ Personnel comparison photos, access records photos, linkage photos and videos, attendance photos, parking photos, visitors photos and so on are all need to be copied because they are not transferred.

⑦After the migration is successful, restart the software service.

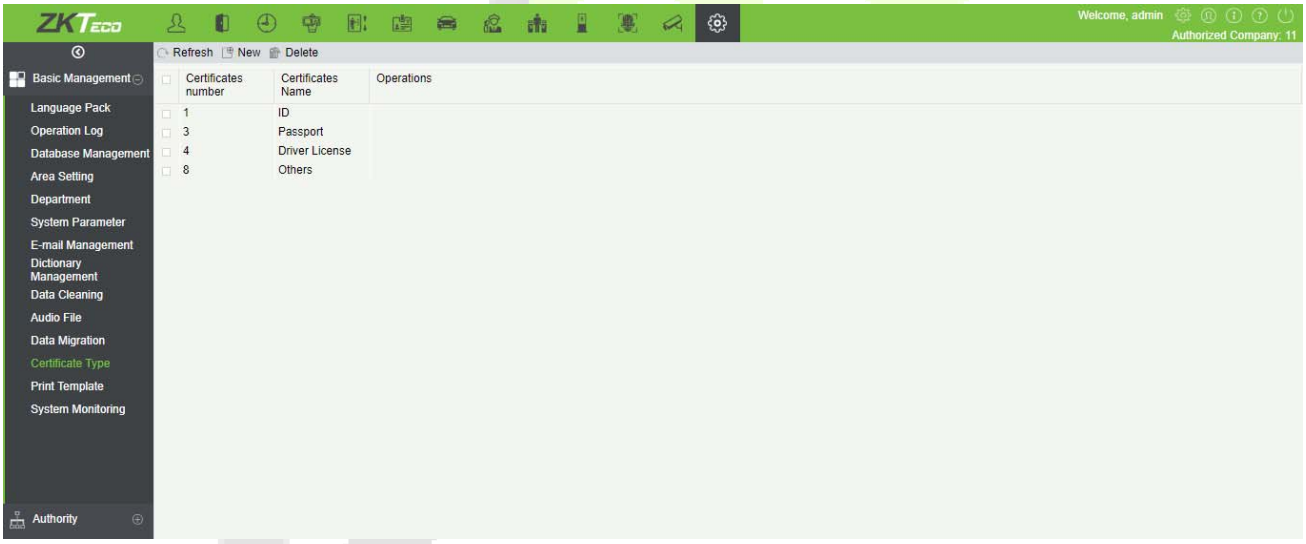
2. 3150 and V5000 installed on different servers:

① Install the V5000 service, the communication port is consistent with the communication port of 3150. After installation, the computer IP of V5000 needs to be changed to 3150 service address IP.

15.1.10 Certificate Type

The system initializes 9 certificate types. User can add the required certificate type for personnel and visitor registration.

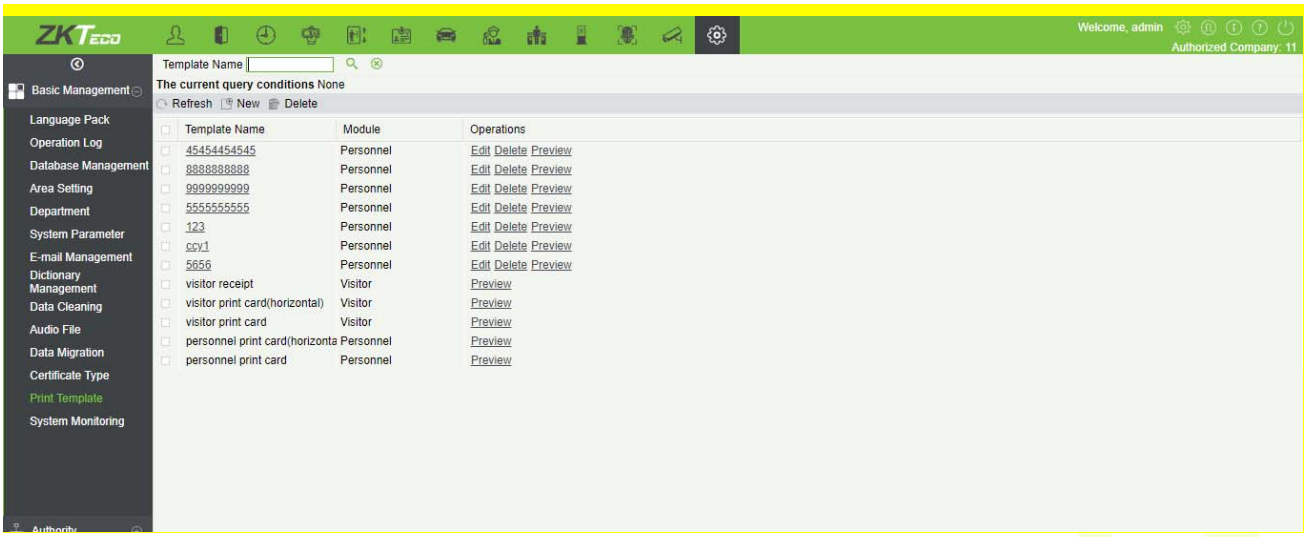
Click [**System**]> [**Basic Management**]>[**Certificate Type**].



15.1.11 Print Template

You can manage the template for different cards: Personnel card template, Visitor receipt template/Card template are all configured here. The system initializes 5 types of personnel and visitor print templates.

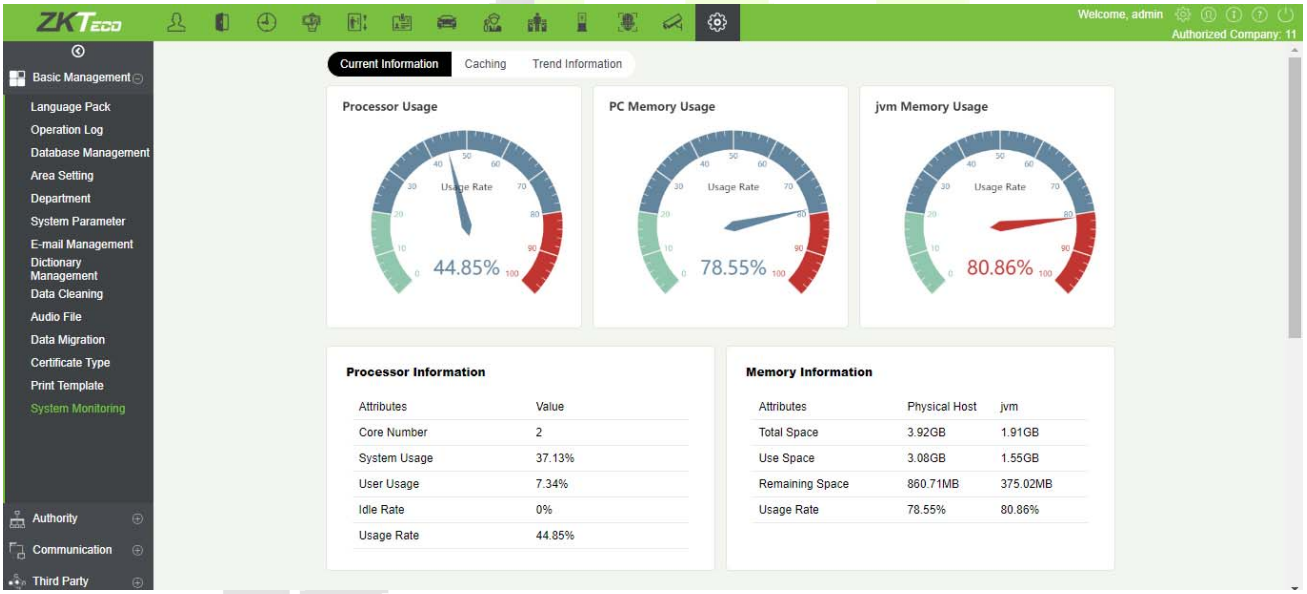
Click [**System**]> [**Basic Management**]> [**Print template**].



15.1.12 System Monitoring

The system monitoring function displays the server processor usage, host memory usage, processor information, memory information, java virtual machine memory usage and other information.

Click [**System**]> [**Basic Management**]>[**System Monitoring**].

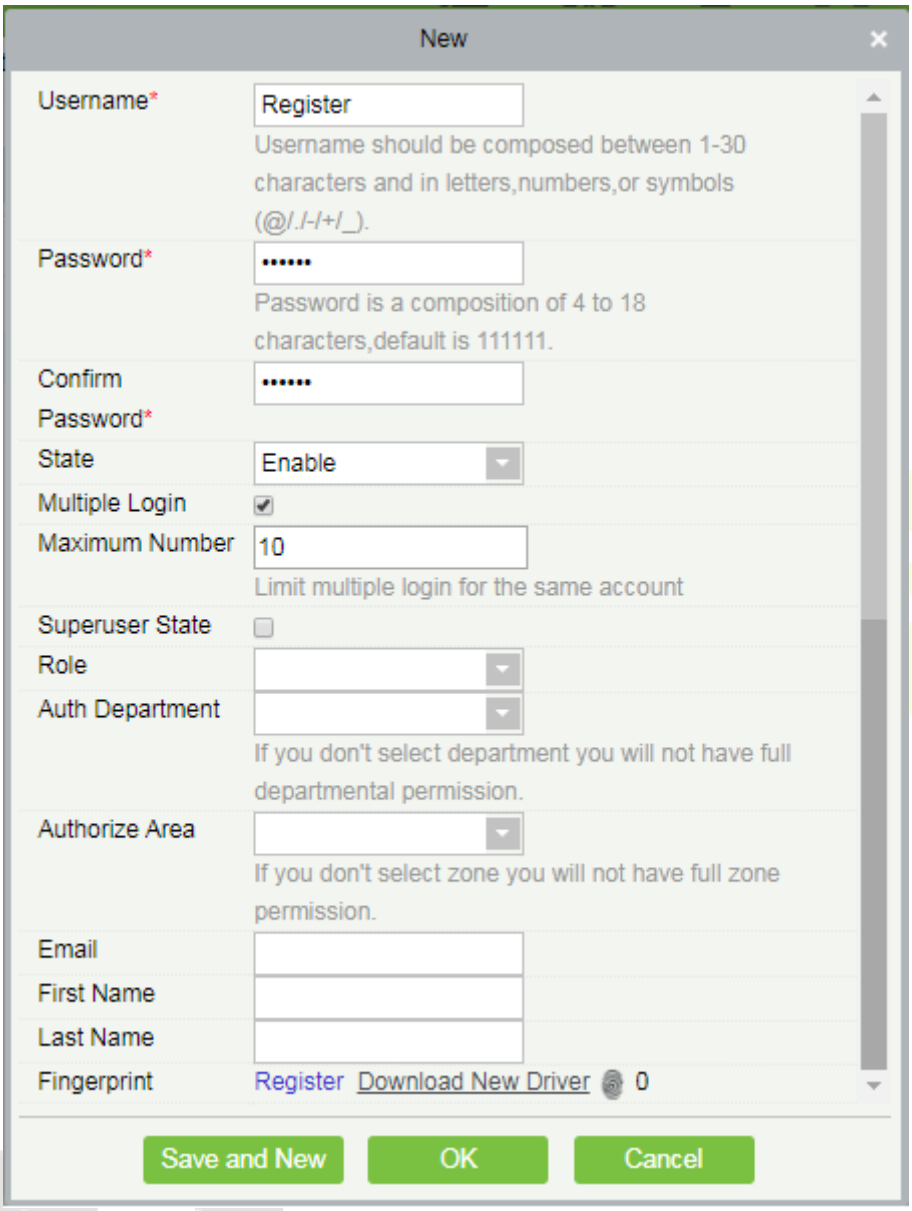


15.2 Authority Management

15.2.1 User

Add new user and implement levels for the user in the system.

1) Click [**System Management**] > [**Authority Management**] > [**User**] > [**New**]:



Fields are as follows:

Username: Any characters within a length of 30.

Password: The length must be more than 4 digits and less than 18 digits. The default password is 111111.

State: Enable or disable the user to operate the system.

Multiple Login: Enable if multiple users want to login to the same software simultaneously.

Maximum Number: Set the maximum number of users who can login at a time. The range is 1 to 100.

Super User State: Enable or disable the user to have the superuser's levels.

Role Group: Non-super user needs to choose a role group to get the levels of the group. The role group must be set in advanced in Role Group.

Auth Department: If no department is selected, then the user will have all department rights by default.

Authorize Area: No area selected means the user possesses all area rights by default.

Email: Type your email in the correct format.

First Name/Last Name: Type your initials.

Fingerprint: Enroll the user fingerprint or duress fingerprint. The user can login the system by pressing the enrolled fingerprint. If the user presses the duress fingerprint, it will trigger the alarm and send the signal to the system.

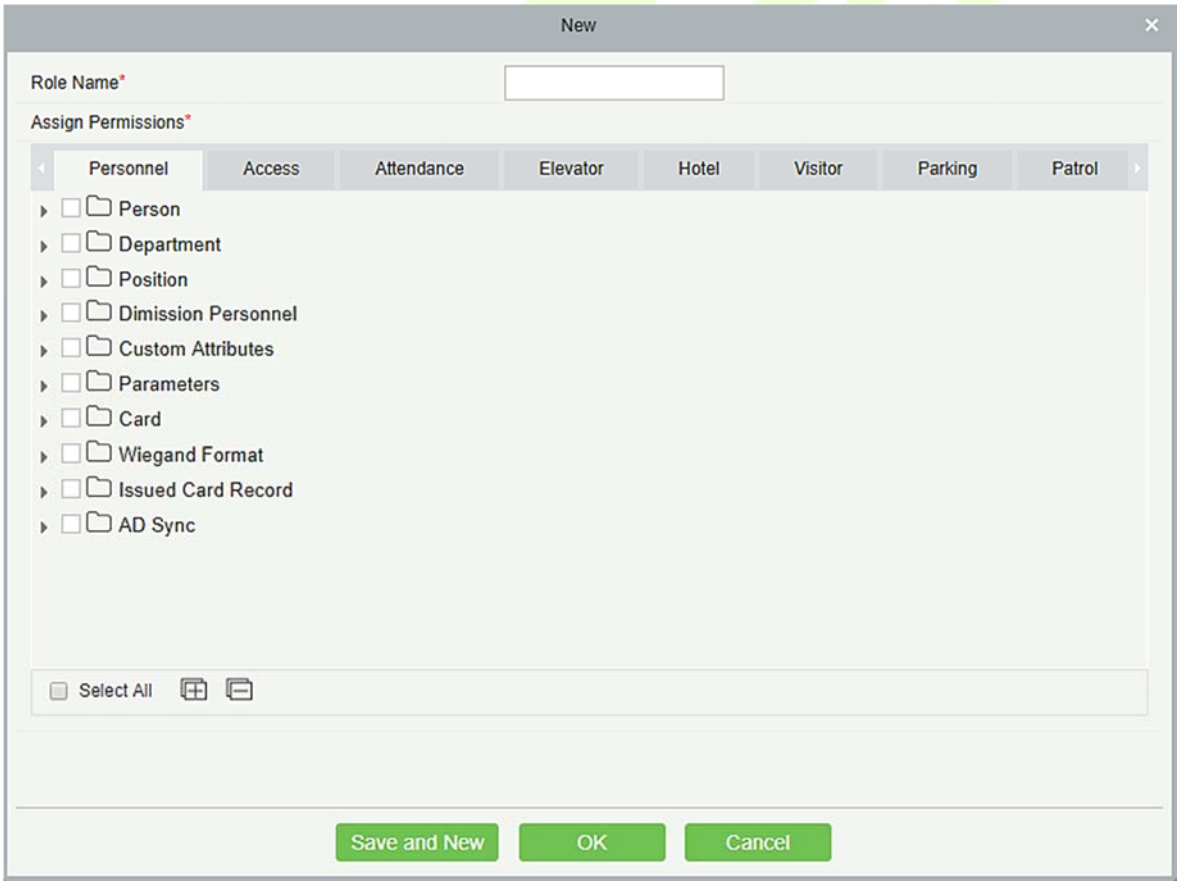
2) After editing, click [**OK**] to complete user adding, and the user will be shown in the list.

Click [**Edit**] or [**Delete**] as required.

15.2.2 Role

When using the system, the super user needs to assign different levels to new users. To avoid setting users one by one, you can set roles with specific levels in role management and assign appropriate roles to users when adding users. A super user has all the levels, can assign rights to new users and set corresponding roles (levels) according to requirements.

1) Click [**System**] > [**Authority Management**] > [**Role**] > [**New**]:



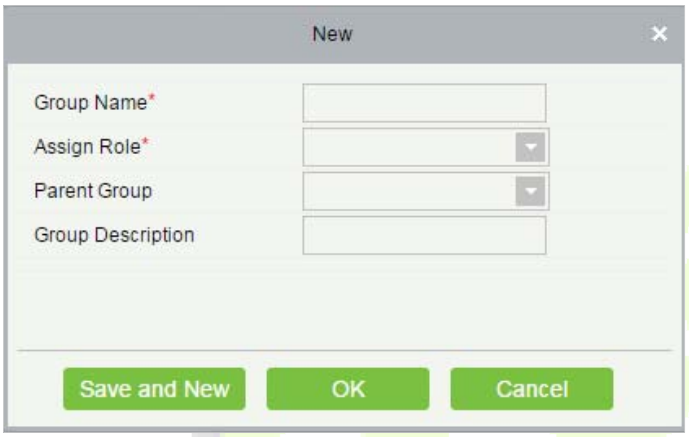
2) Set the name and assign permissions for the role.

3) Click [**OK**] to save.

15.2.3 Role Group

You can add role groups to the system. A role group has all the levels assigned to roles within the group. An appropriate role group can be directly assigned to a newly-added user. Include all the levels for using all the service modules of the system and the system setup module. The default super user of the system has all the levels, can assign rights to new users and set corresponding role groups (levels) according to requirements.

1) Click [**System Management**] > [**Authority Management**] > [**Role Group**] > [**New**]:

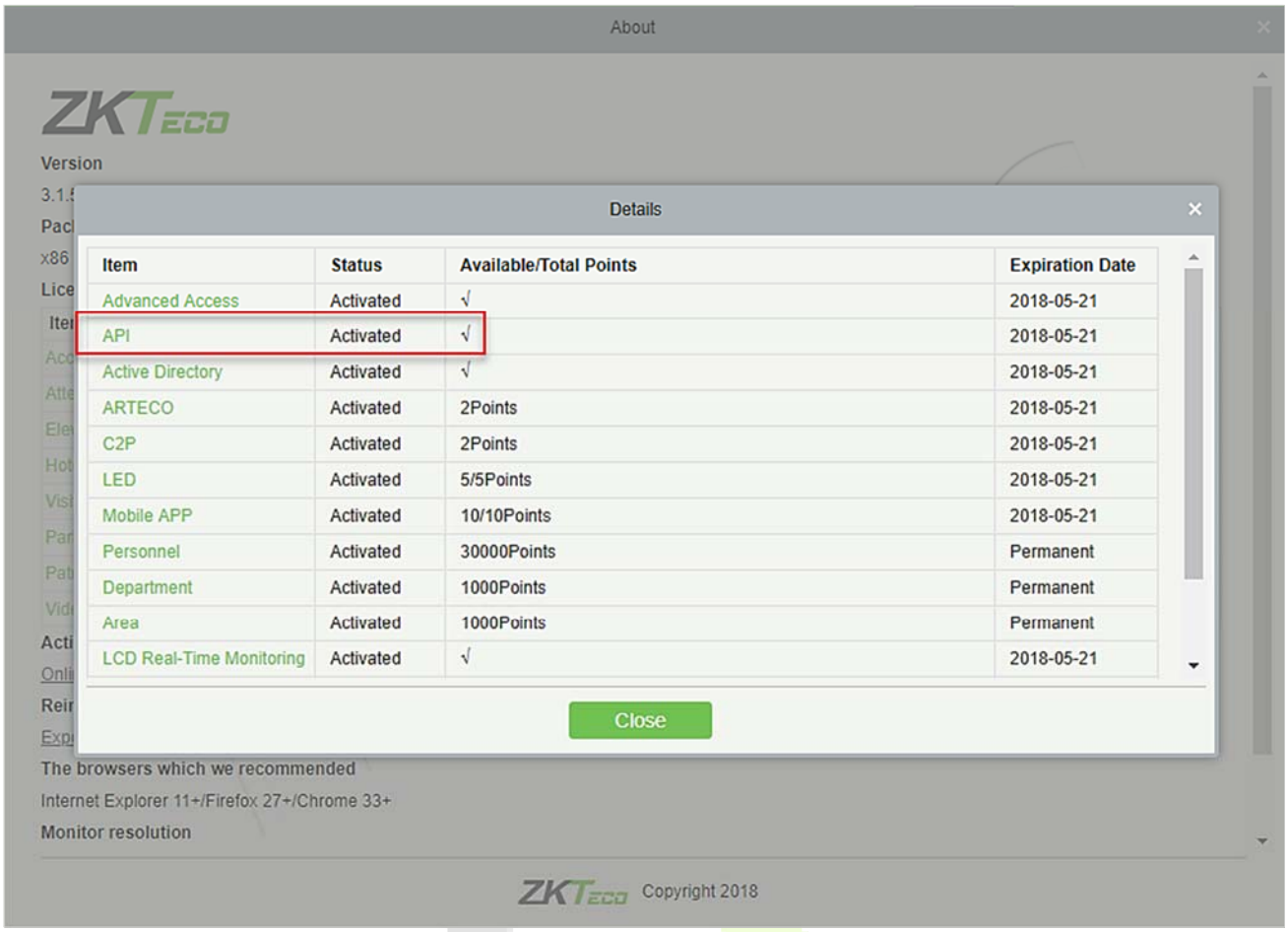


2) Set the name and parent group, assign role for the group.

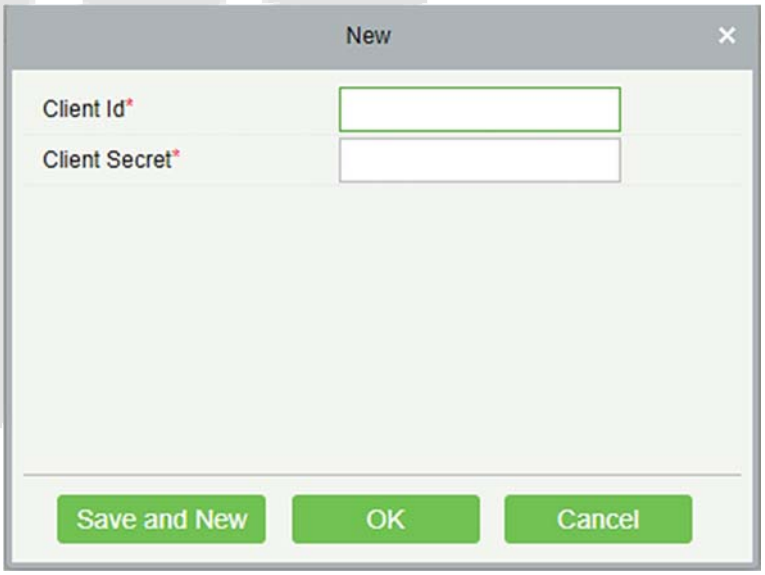
3) Click [**OK**] to save.

15.2.4 API Authorization

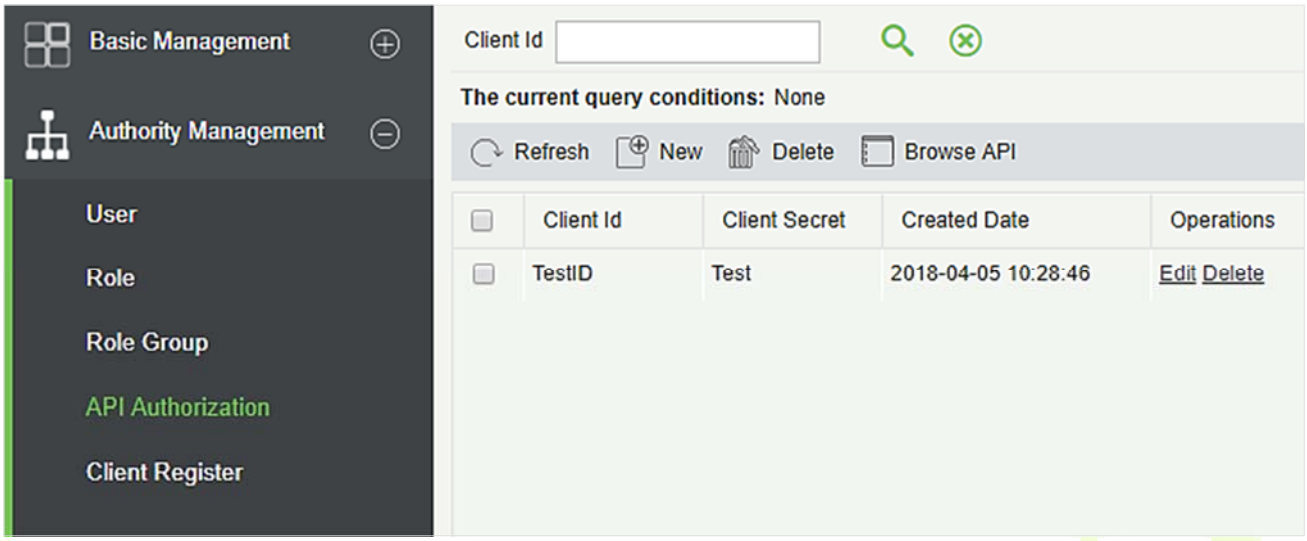
1. Activate the API through authorization. You can check whether the API has been activated on the About page (The API Authorization menu is displayed in System Management only when the API is activated). API is shown in License details below:



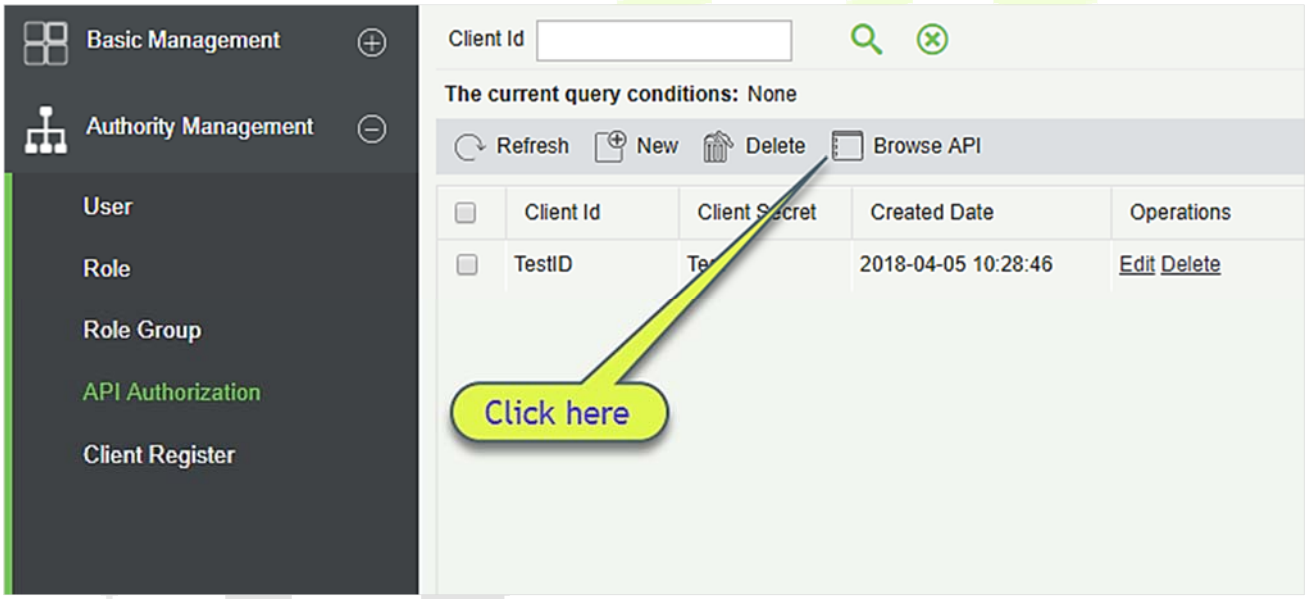
2. Log in to the system (as the super user, for example, admin) to enter the software. Click [**System Management**] > [**Authority Management**] > [**API Authorization**]. Add a client ID, which must be unique, and a client secret, which will be used when the API is invoked.

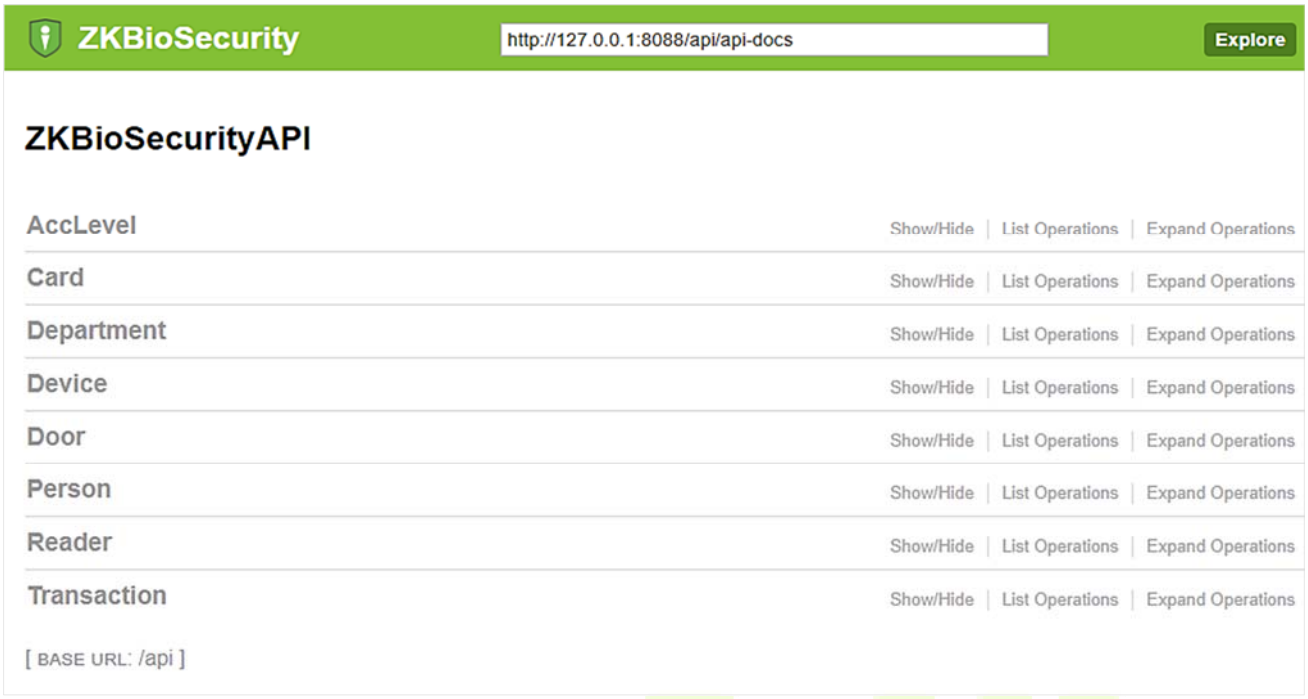


3. Only when the client ID and secret are added can the next API operation page be displayed normally. Otherwise, the access is abnormal):

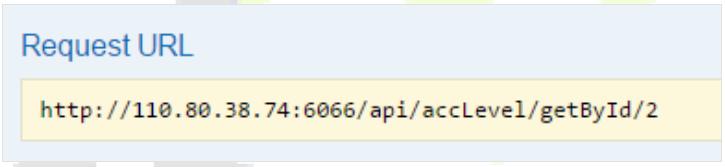


4. After the client ID and secret are added, click Browse API on the API Authorization page to skip to the API operation page (The page of the ZKBioSecurity system must be open for normal access of the API operation page). This page provides multiple APIs:





When APIs are invoked, URLs of all request APIs must contain the access_token parameter, whose value is determined by the client key configured on the background (if there are multiple keys, only one is selected), for example:

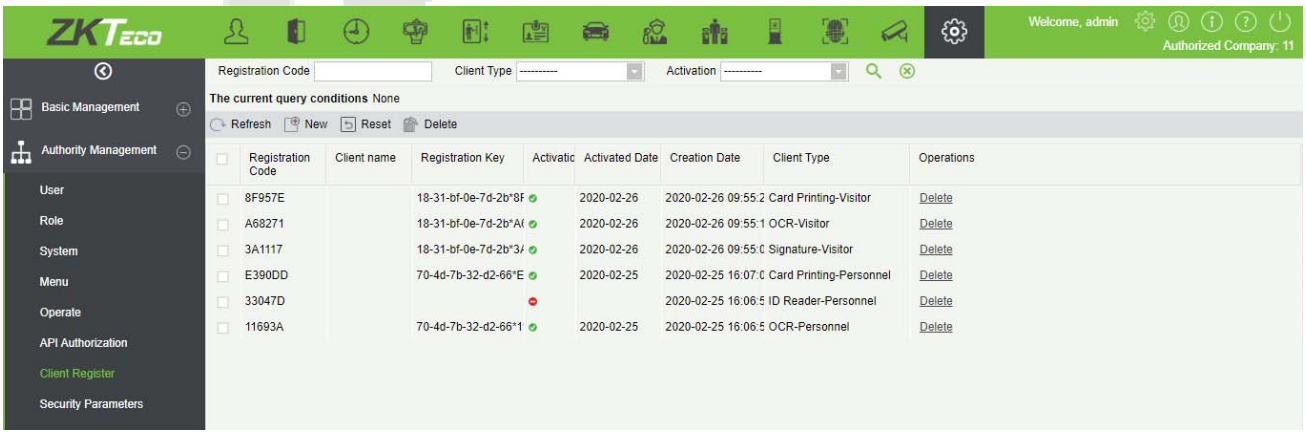


The access_token parameter must be added when the API is invoked (one request URL can be invoked):

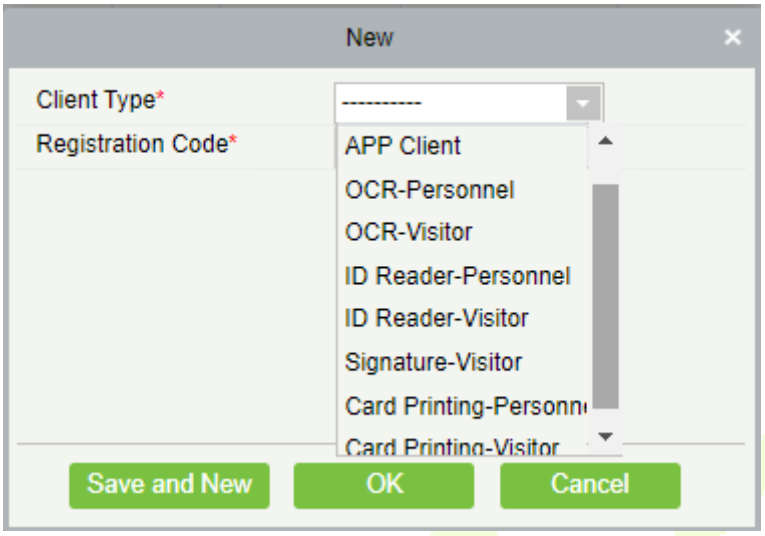
http://110.80.38.74:6066/api/accLevel/getById/2.

15.2.5 Client Register

You can add client types for the system and generate registration codes for client registrations of each module function. The number of allowed clients is controlled by the number of allowed points.



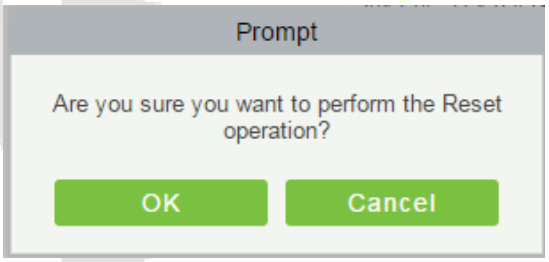
Click **[System Management]** > **[Authority Management]** > **[Client Authorization]** > **[New] to go to the [New]** page:



Client Type: The value can be APP Client, OCR-Personnel, OCR-Visitor, ID Reader-Personnel, ID Reader-Visitor or Signature- Visitor, Card Printing- Personnel, Card Printing-Visitor

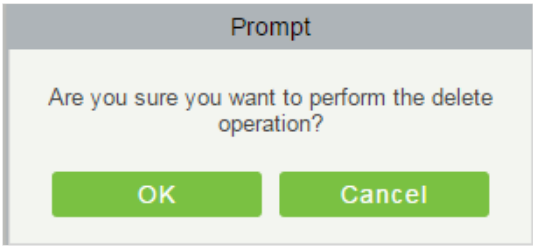
Registration Code: The registration code for **[APP Client]** is used under **[Network Settings]** on the APP login page and that for **[Print Card-Personnel]** is used under **[Parameter Settings]** > **[Client Registration]**. Only new registration codes added on the server are authorized and one registration code can be used by only one client.

1. To reset a client, select the client and click [**Reset**].



Click [**OK**] to reset the client.

2. To delete a client, select the client and click [**Delete**].

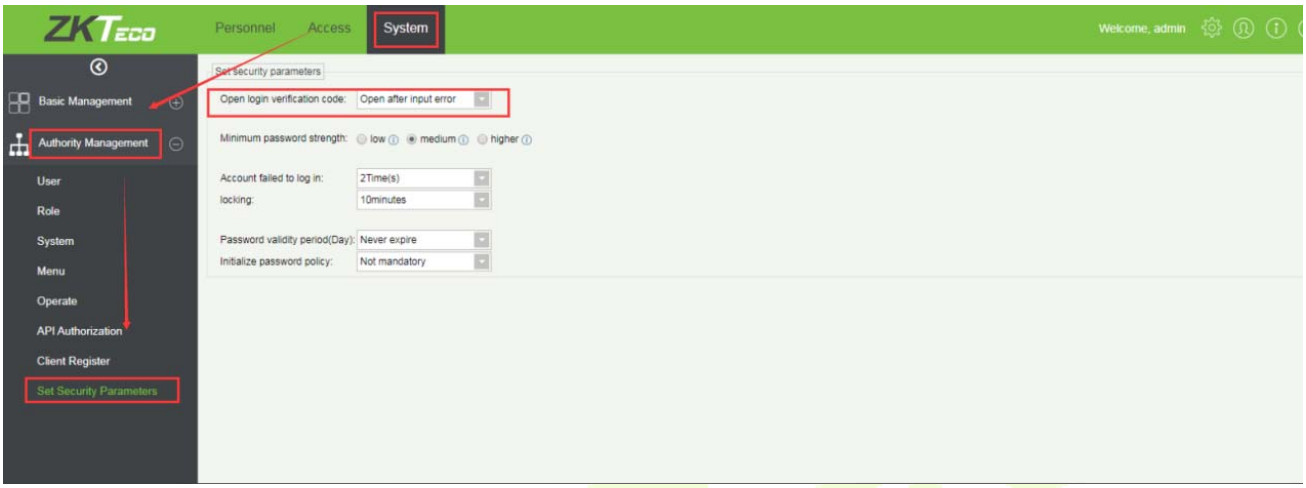


Click [**OK**] to delete the client.

15.2.6 Security Parameters

1) Login Verification Code Setting: It includes None, Always prompt verification code, Prompt after entering an error.

There are three login verification modes which can be selected.

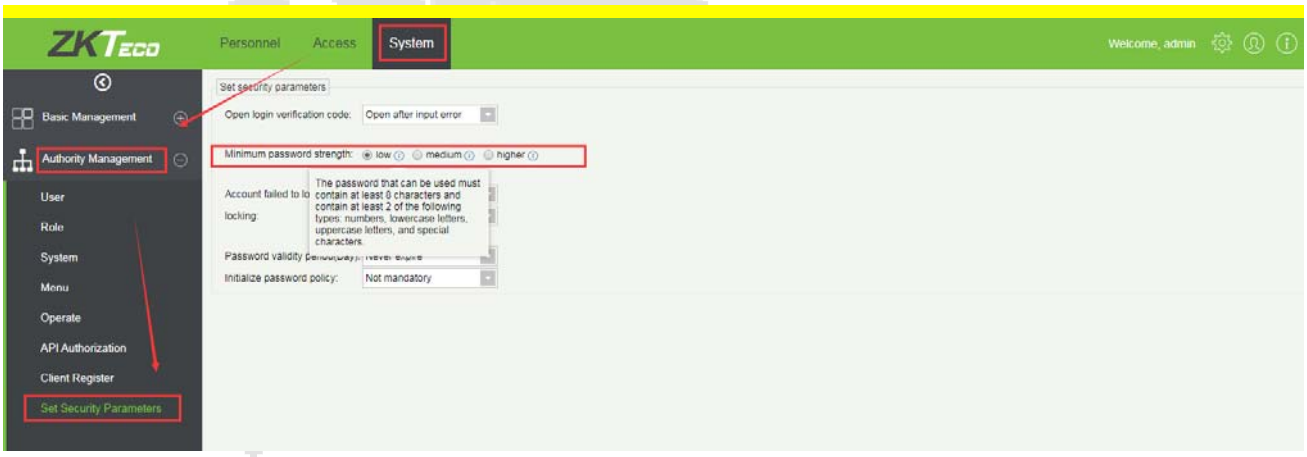


Do not open verification code: The system allows no verification code

Open verification code: Users must fill in the verification code when logging in to the software.

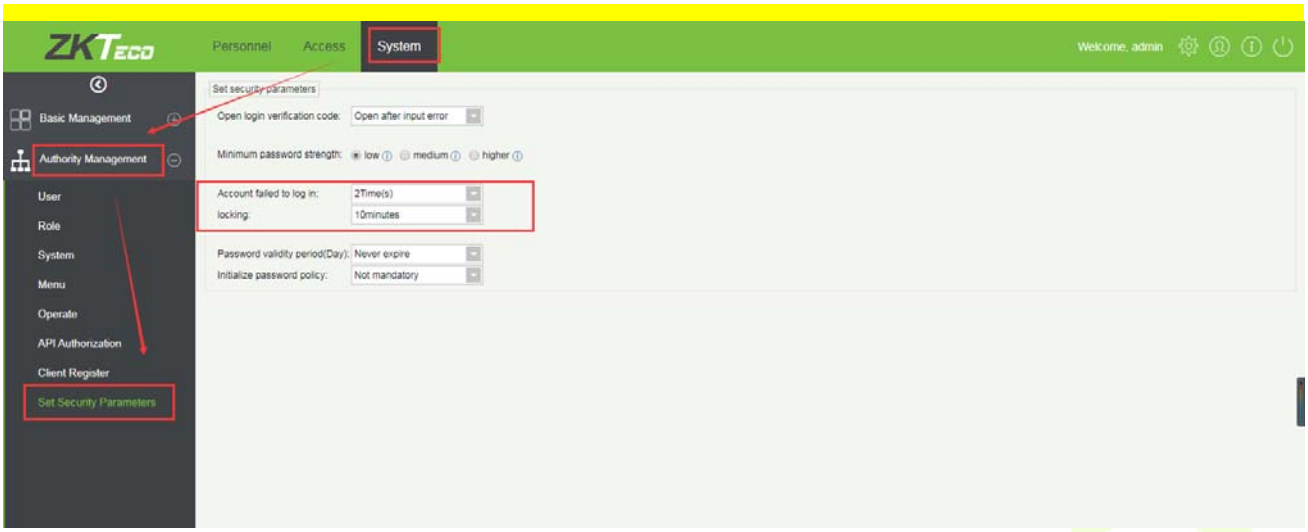
Open after input error: The system will pop-up a verification box after filling in the wrong Username and password.

2) Password Strength Setting: The path is **[System] -> [Authority Management]-> [Set Security Parameter].**

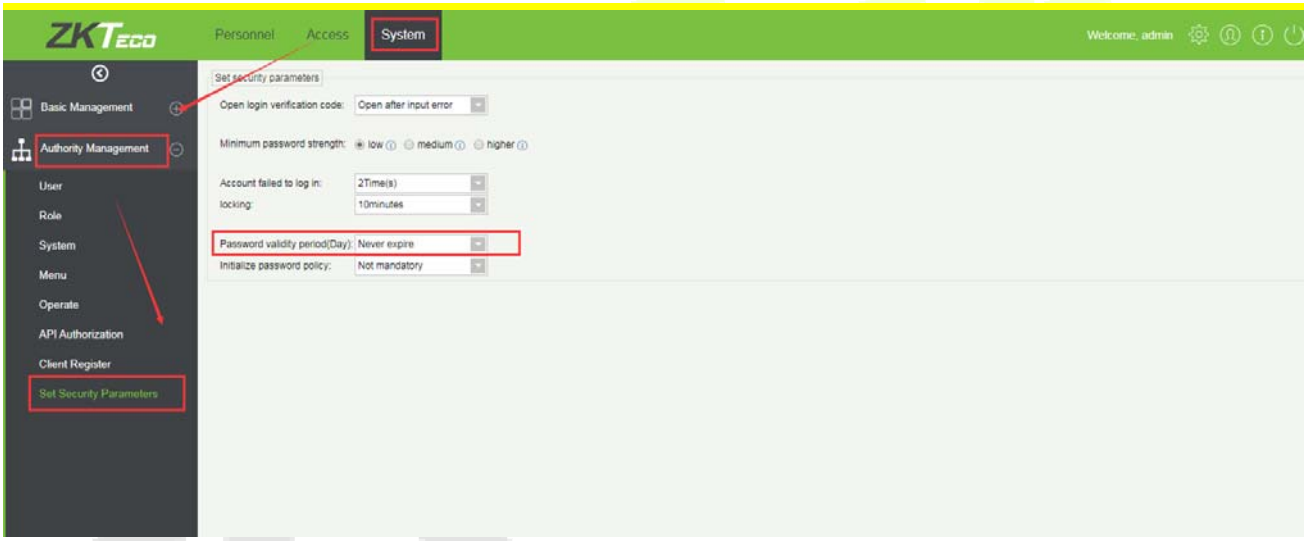


3) Lock account: The path is **[System] -> [Authority Management] -> [Set Security Parameter].**

The account will be locked if user fails to login the system as per the software setting. For example, if the system allows user fill in wrong username and password for 2 times. The system will be locked for 10 minutes after exceeding 2 times of operation.



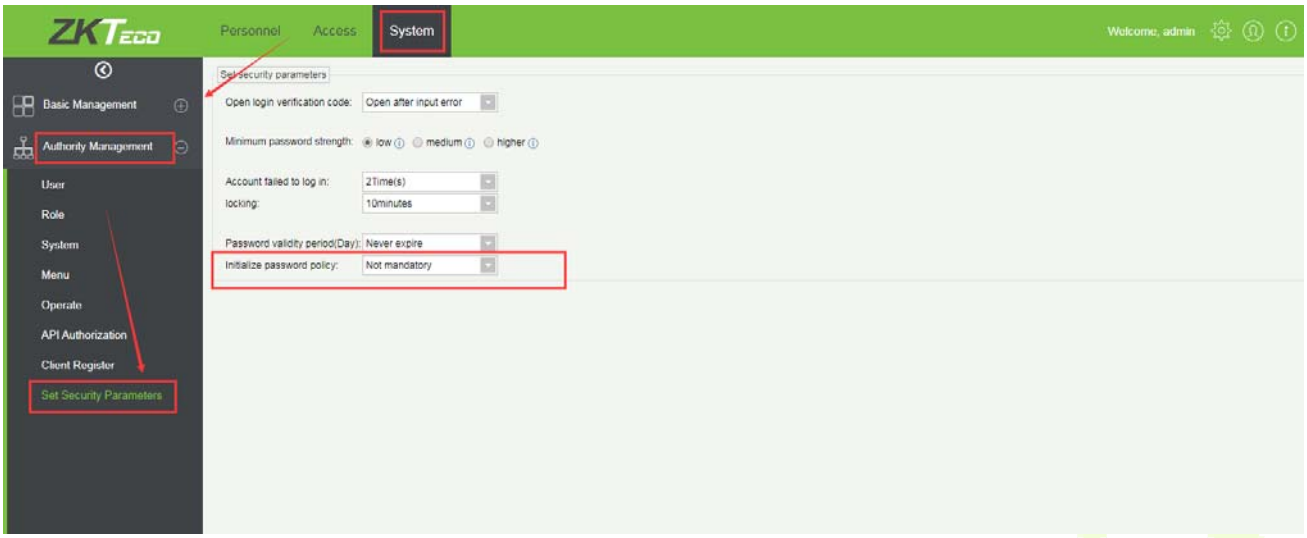
4) Password valid day(s): The path is **[System[-> [Authority Management] -> [Set Security Parameter].** Users can set the validity as 30days, 60daysor permanent. If password gets expired, user cannot login to the system.



5) Password Modification: The path is **[System] -> [Authority Management] -> [Set Security Parameter].** There are 2 options that user can set. Not mandatory andForced to modify the next time you login.

Not mandatory: The system does not need to modify the initial password.

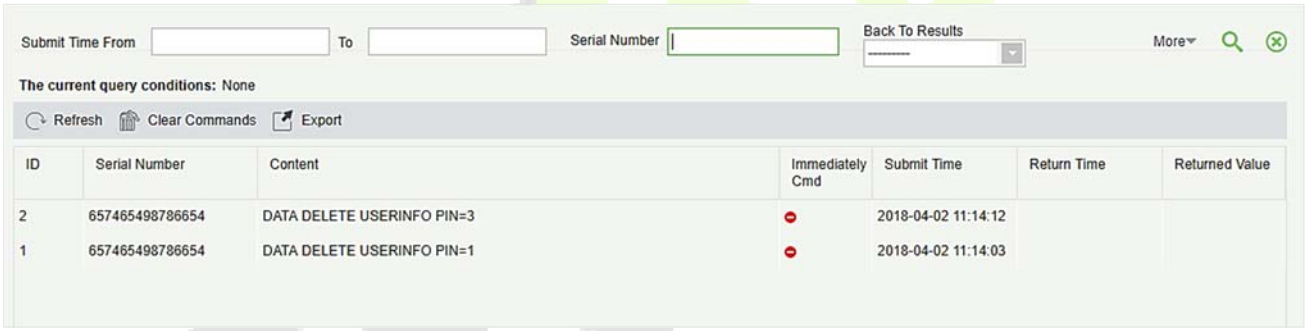
Forced to modify the next time you login: It is compulsory to modify the initial password after the second login.



15.3 Communication

15.3.1 Device Commands

Click **[System]** > **[Communication]** > **[Device Commands]**, the commands lists will be displayed.



If the returned value is more than or equal to 0, the command is successfully issued. If the returned value is less than 0, the command is failed to be issued.

Clear Commands: Clear the command lists.

Export: Export the command lists to local host. You can export to an Excel file. See the following figure.

			Device Commands			
ID	Serial Number	Content	Immediately Cmd	Submit Time	Return Time	Returned Value
1504	20100501999	DATA UPDATE userauthorize Pin=2AuthorizeTimezoneId=1AuthorizeDoorId=1 Pin=1AuthorizeTimezoneId=1AuthorizeDoorId=1 ...	false	2017-12-18 10:51:15	2017-12-18 10:51:21	0
1502	20100501999	DATA UPDATE mulcarduser Pin=2CardNo=5dec02LossCardFlag=0CardType=0 Pin=1CardNo=4412c5LossCardFlag=0CardType=0 ...	false	2017-12-18 10:51:14	2017-12-18 10:51:21	0

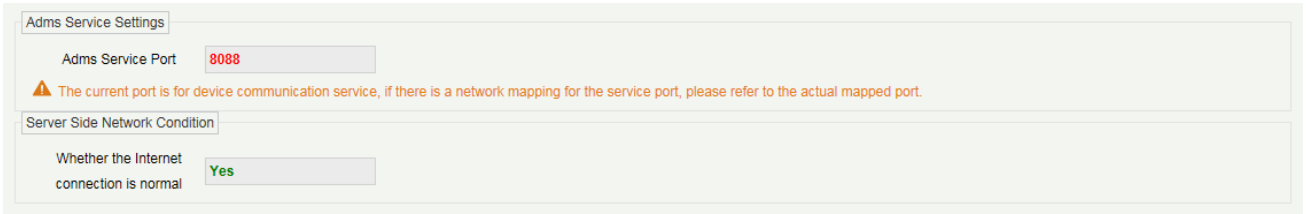
15.3.2 Communication Device

Click **[System]** > **[Communication]** > **[Communication Device]**, you can view all equipment information and communication in the system. Detailed information such as accessed module, serial number, firmware version, IP address, communication status and command execution can be viewed.

View authorized device: View the authorized device information.

15.3.3 Communication Monitor

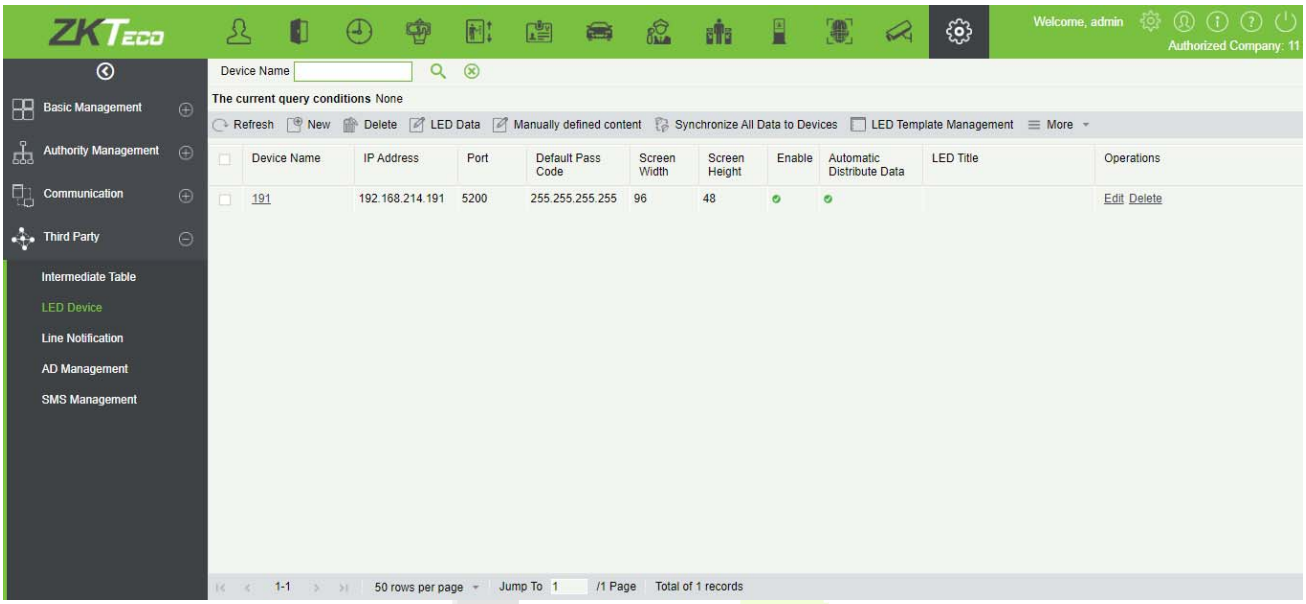
Click **[System]** > **[Communication]** > **[Communication Monitor]** to check the adms communication port of the current server and check whether the Internet connection of the server is normal.



15.4 Third Party

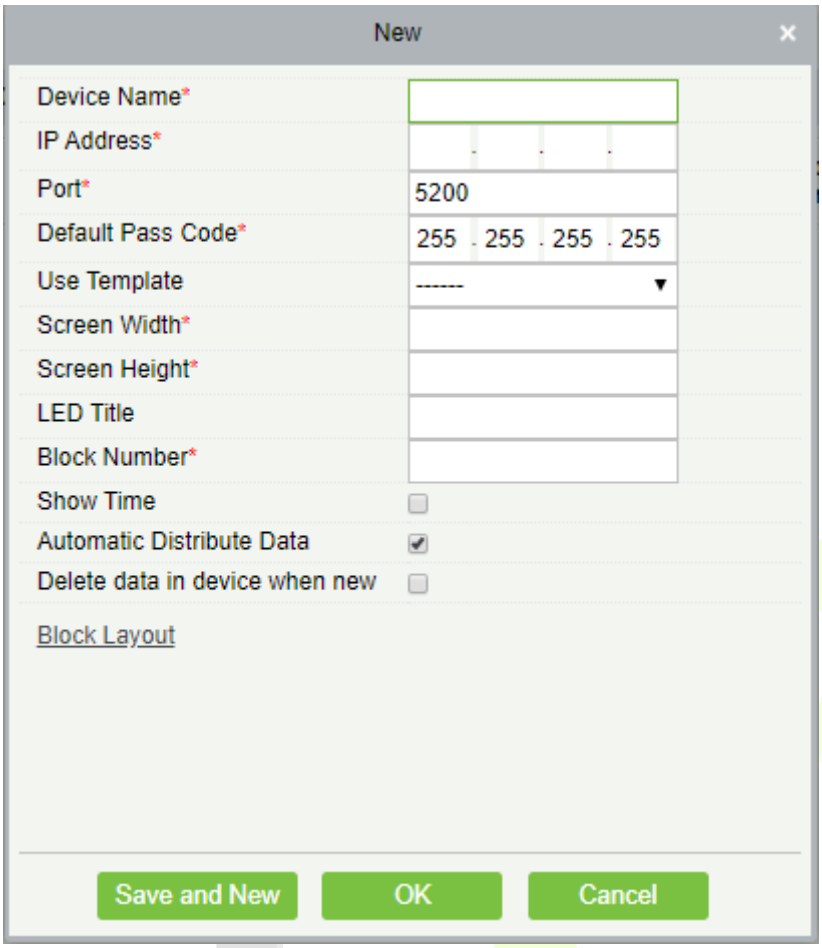
15.4.1 LED Device

The system integrated outsourcing LED equipment (control card: lumens 3200/4200), provides a window to display data; it can provide customers personnel in the access area quantity statistics, real-time information about personnel going in and out and personnel information in the area, etc.



- **Add**

Click **[System]**> **[Extended Management]**> **[LED Device]**> **[New]**. The page is displayed as follows:



Fields are as follows:

Device Name: Name of the LED device.

IP Address: IP address of the LED device.

Port: The default communication port is 5200.

Default Pass Code: The default value is 255.255.255.255.

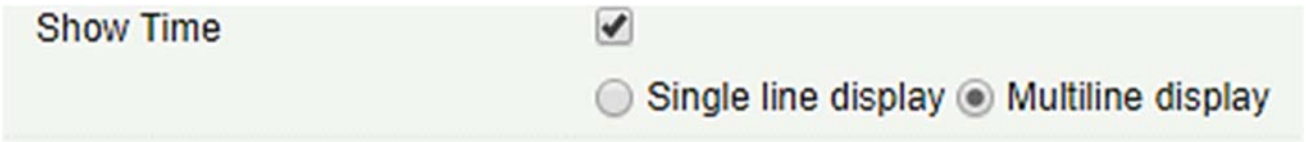
Screen Width: Width of the dot matrix (resolution).

Screen Height: Height of the dot matrix (resolution).

LED Title: Select whether to display the title. If the parameter is left blank, the title is not displayed.

Block Number: Number of blocks that the LED is divided into (Note that the blocks do not contain the title and system time blocks).

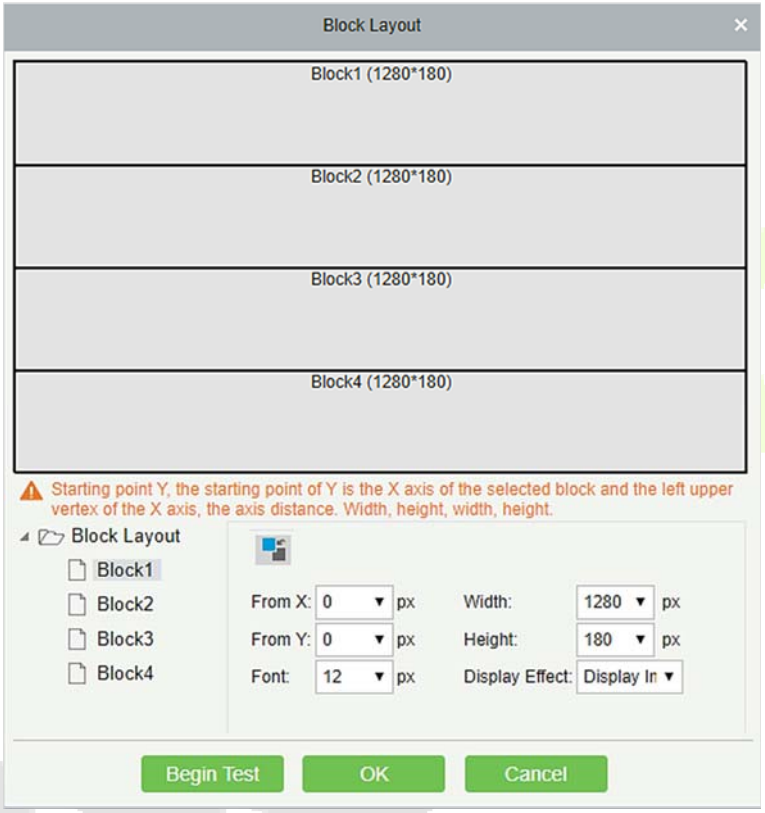
Show Time: It will display time on the LED screen. Once you select it, you will find two options to choose from; Single Line and Multiline Display. Choose according to your choice.



Automatic Distribute Data: By default, this parameter is selected. You send data to the LED in the access control module only when you select this parameter. Otherwise, the content to be sent needs to be manually defined.

Delete data in device when new: Delete the original data in the device when adding LED device.

Block Layout: After you click Block Layout, the following box is displayed:



✍Notes:

- Parameters must be set for each block.
- The height of each block must be equal to or larger than 12. Otherwise, the letters cannot be completely displayed.
- The total height of all blocks cannot be larger than the screen height.

- **Edit**

Click a device name or **[Edit]** under **[Operation]** to go to the edit page. After editing the device, click **[OK]** to save the setting.

- **Delete**

Click a device name or **[Delete]** under **[Operation]** in the device list and click **[OK]** to delete the device or click **[Cancel]** to cancel the operation. Select one or more devices and click **[Delete]** above the list and click **[OK]** to delete the selected device(s) or click **[Cancel]** to cancel the operation.

- **Enable and Disable**

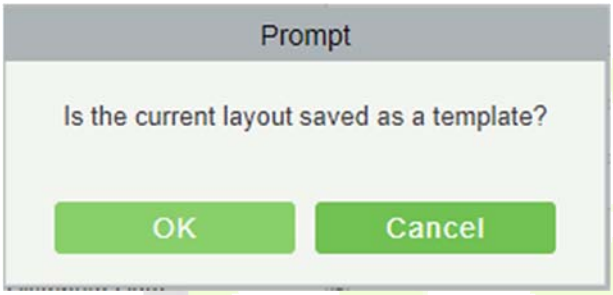
Select a device and click **[Enable/Disable]** to start/stop using the device. If the device is enabled, data is transmitted to the device. Otherwise, no data is transmitted to the device.

- **Synchronize All Data To Devices**

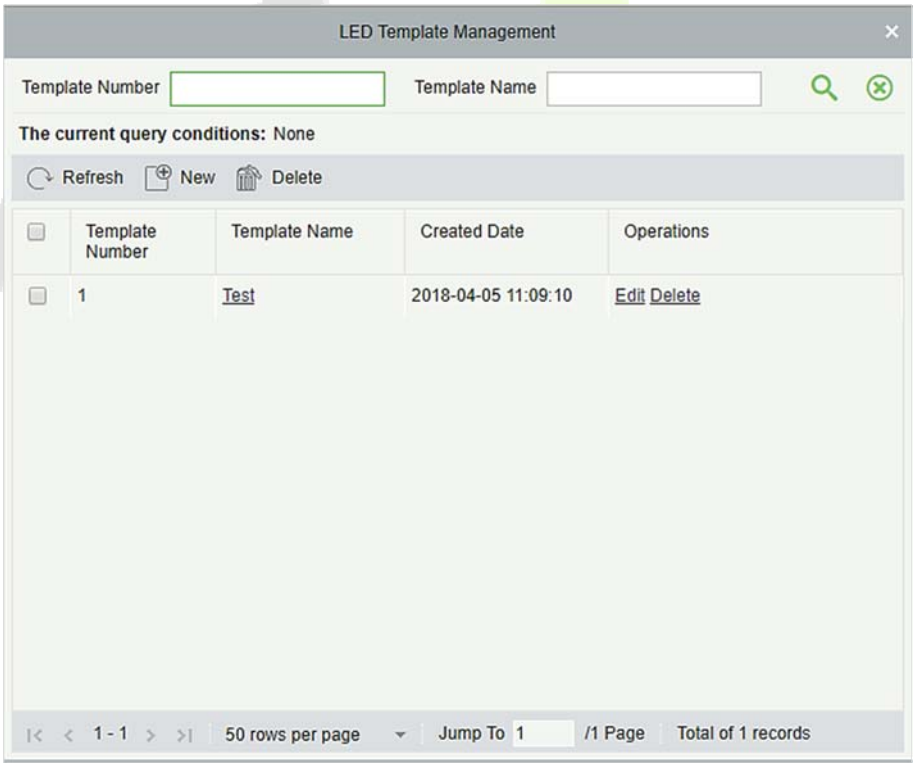
Synchronize the LED block layout and LED data setting in the system to the device. Select a device, click **[Synchronize All Data To Devices]**, and then click **[Synchronize]** to synchronize the data.

- **LED Template Management**

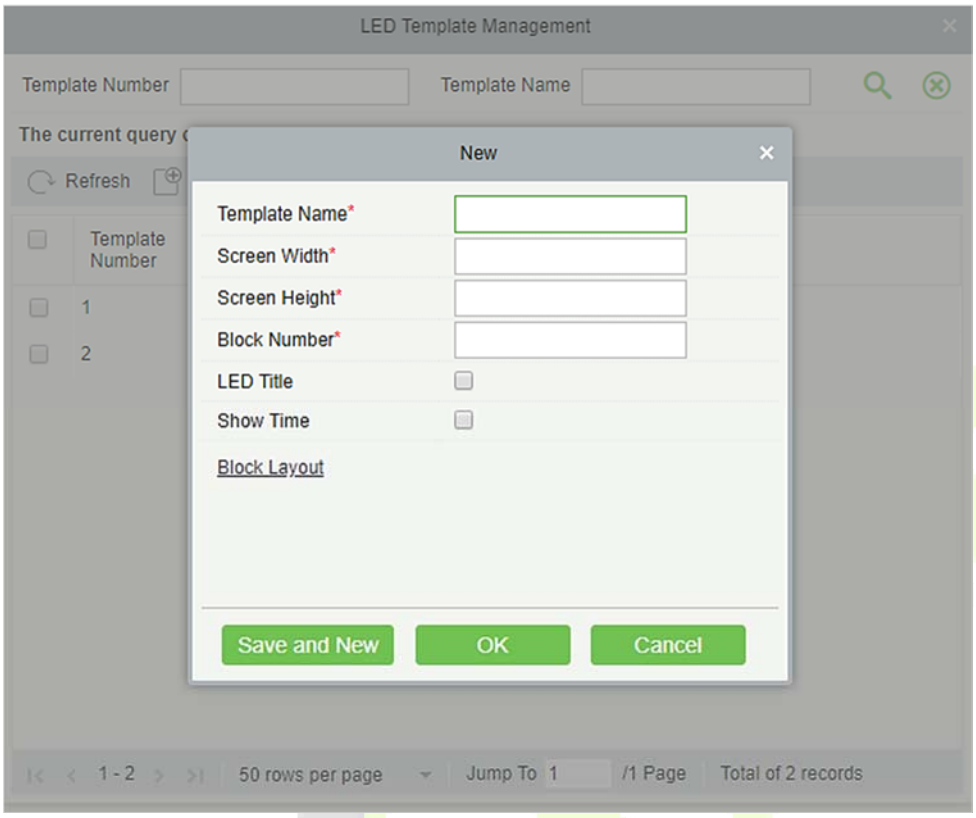
Through this function you can create a template for the blocks. This template you can directly use at the time of adding LED device. When you are adding LED device, then after defining the blocks dimensions, you will be prompted to save the template as shown below:



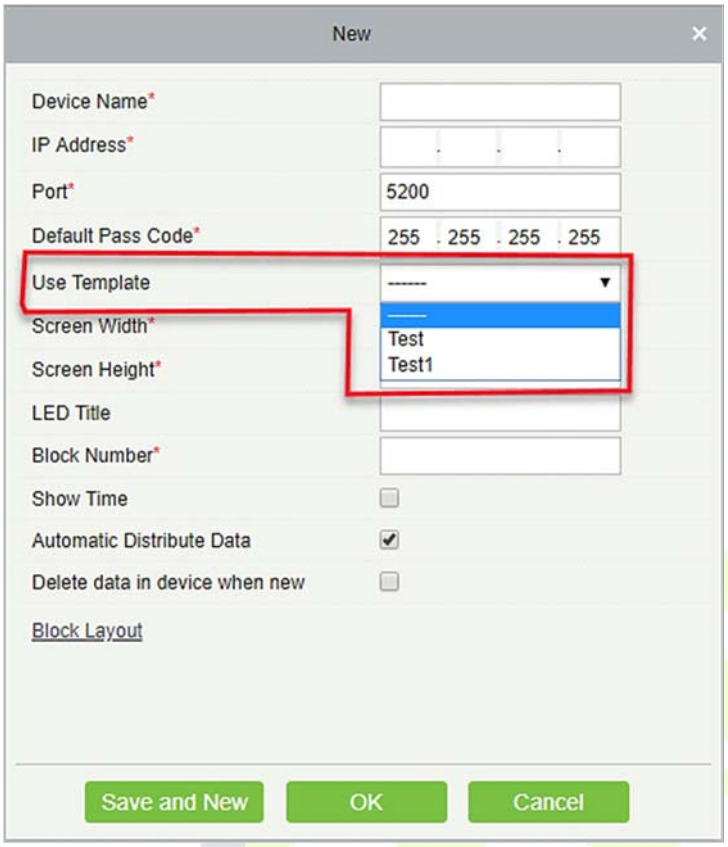
If you save it, then this template will be displayed in the LED Template Management list as shown below:



You can directly create the blocks by clicking on **[New]** in above interface.



Fill all the required details and save. Once saved, you will find this template at the LED device adding interface.



- **Restart**

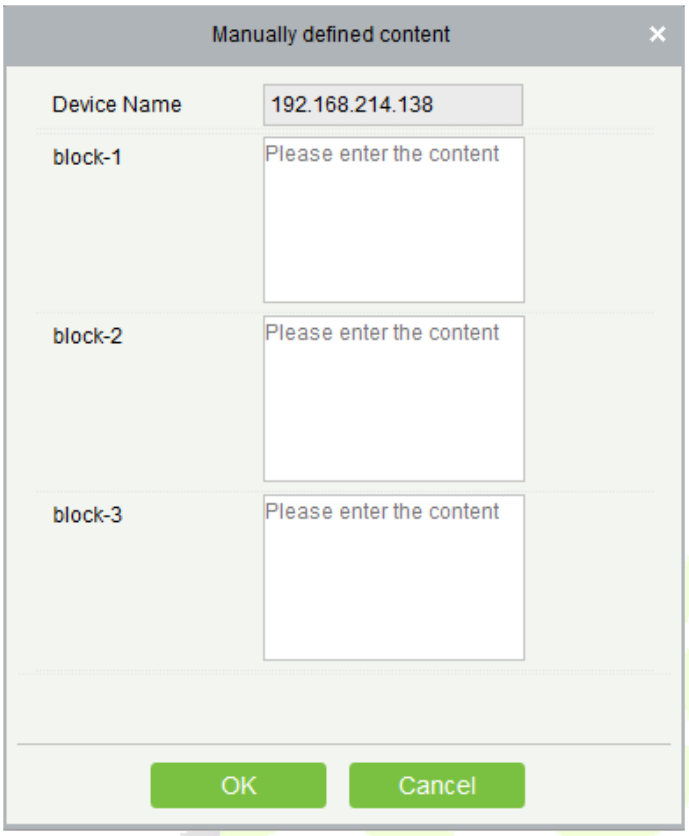
After you restart the device, the LED control card system will be restarted, data on the screen is cleared and data saved in the system is restored. After the device is successfully restarted, click **[Synchronize All Data To Devices]** to display all distributed content on the LED screen.

- **Modify IP address**

Modify the IP address of the device. The default IP address of the control card is 192.168.1.222.

- **Manually defined content**

Select a device and click **[Manually defined content]**. The page is displayed as follows:



✍Notes:

- At least one block must be selected for distribution of manually defined content.
- After the manually defined content is selected, the access control module cannot send data to the LED device.

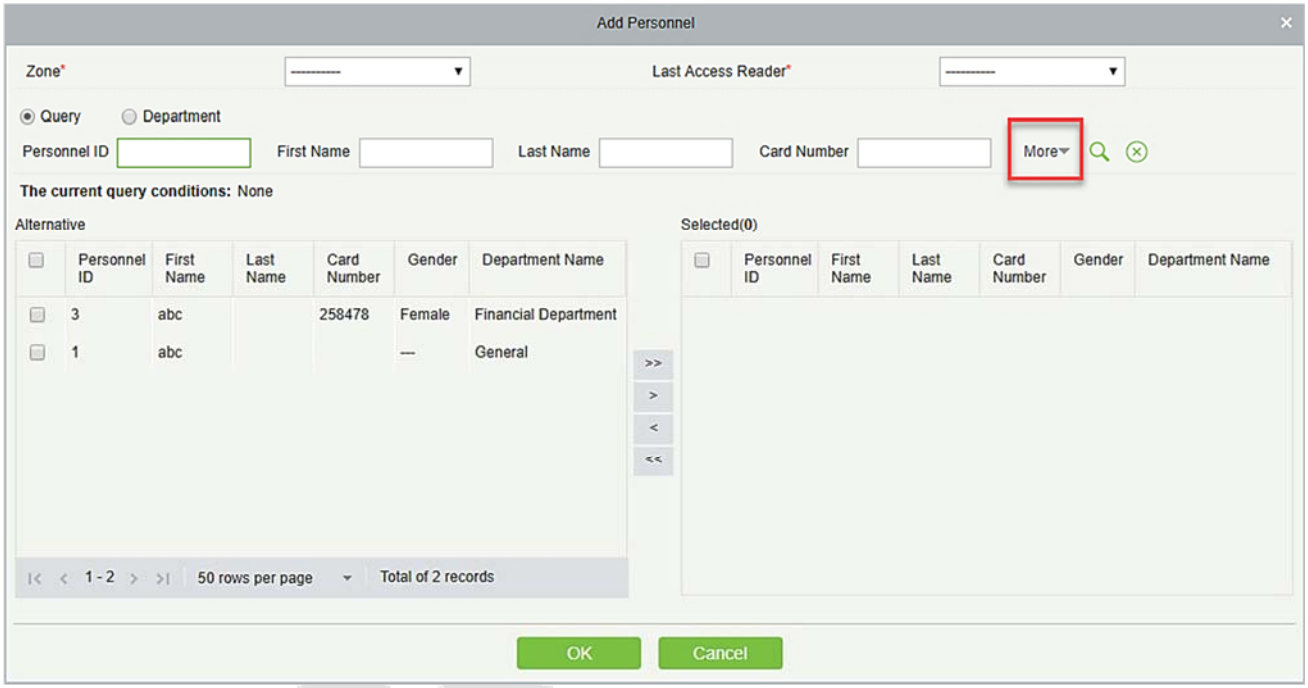
✍Notes: Contact the technical support team for intermediate table, line notification, active directory page and other materials.

16 Appendices

Common Operations

Select Personnel

The selected personnel page in the system is as below:

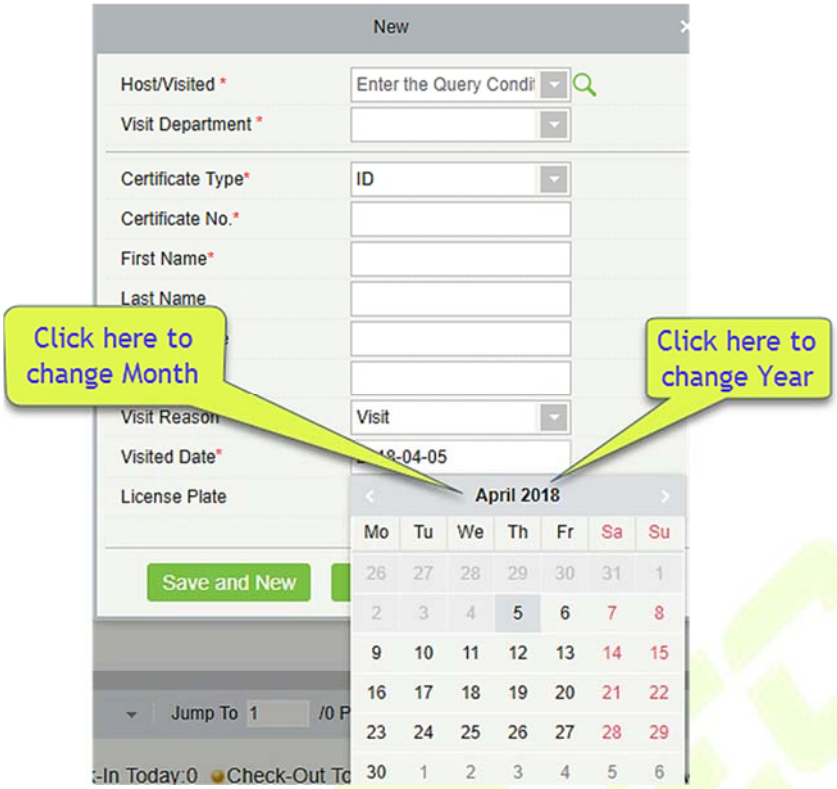


You can select the personnel from list generated, or you can also click **[More]** to filter by gender or department.

Click > to move the selected personnel in to the selected lists. If you want to cancel the movement, click <.

Set Date and Time

Click the date and time box:

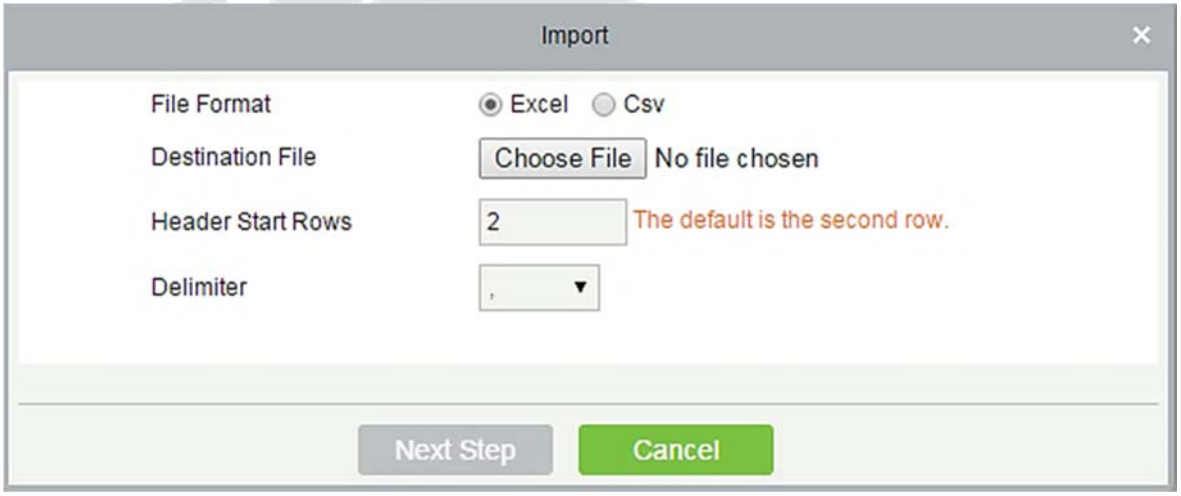


Click on the Year to select by clicking or . Click the Month and Date to select directly.

- **Import (take the personnel list importing as an example)**

If there is a personnel file in your computer, you can Import it into the system.

1) Click [**Import**]:



Fields are as follows:

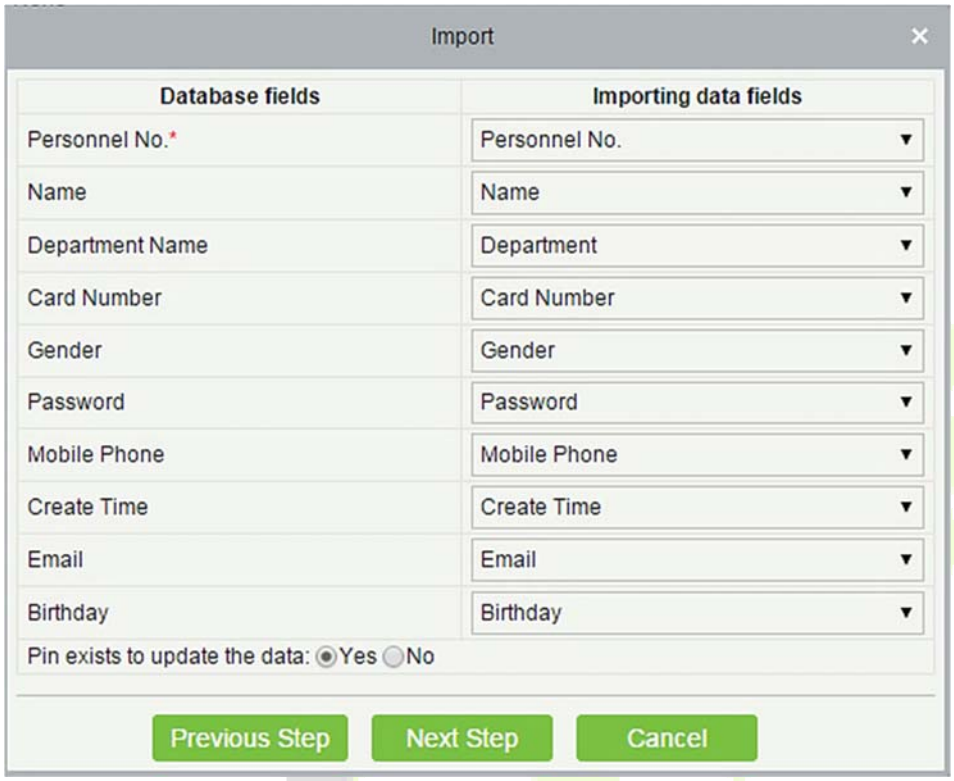
File Format: Select the file format to be imported.

Destination File: Choose file to be imported.

Head Start Rows: which row is the first row to be imported.

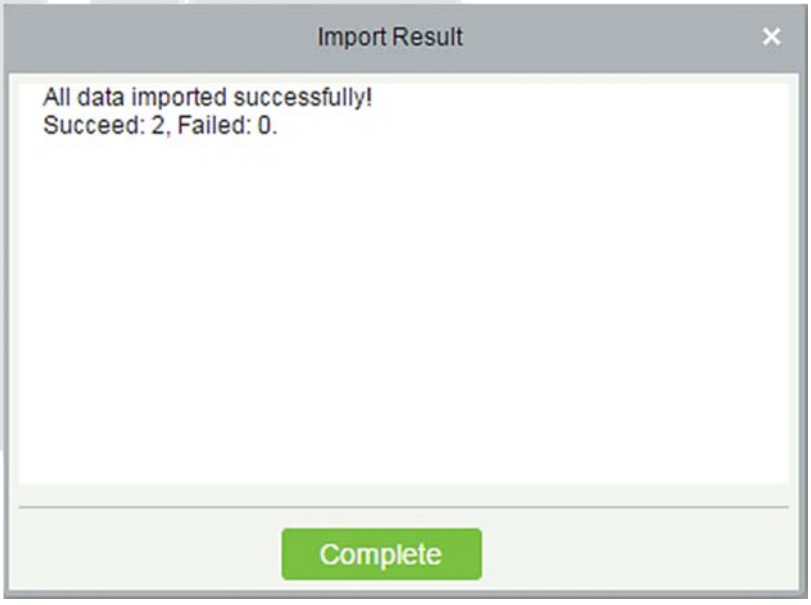
Delimiter: The delimiter of CSV format file, only "." and "-" are available.

2) Click [**Next Step**]:



3) Select the feeds to be imported to the system. "----------" indicates the fields will not be imported.

4) Click [**Next Step**]:



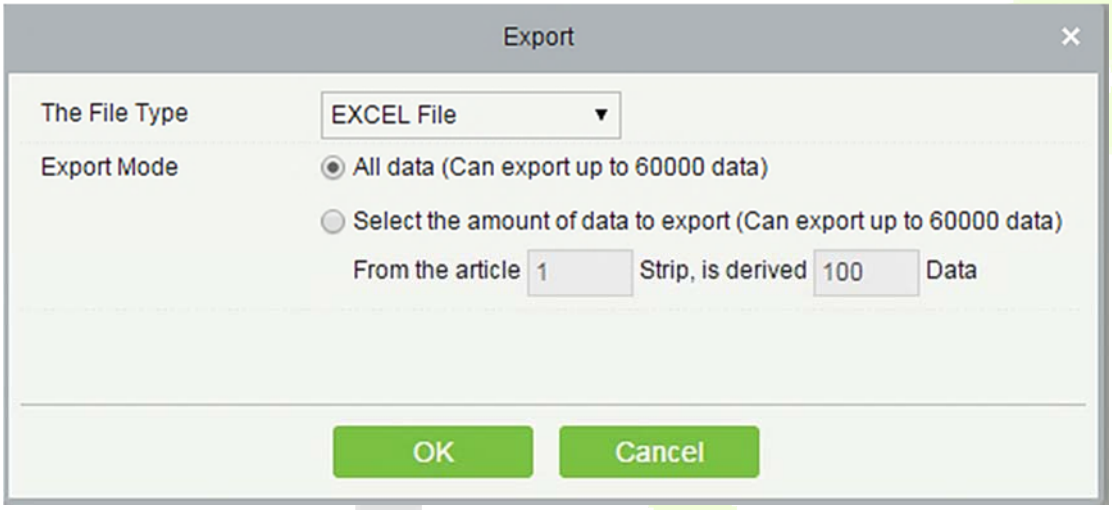
The data is imported successfully.

✍**Notes:**

- When importing department table, department name and department number must not be empty, the parent department can be empty. Duplicated number does not affect the operation, it can be modified manually.
- When importing personnel table, personnel number is required. If the personnel number already exists in the database, it will not be imported.

- **Export (take the personnel list exporting as an example)**

1) Click [**Export**]:



2) Select the file format and export mode to be exported. Click [**OK**].

3) You can view the file in your local drive.

✍**Note:** 10000 records are allowed to export by default, you can manually input as required.

Access Event Type

- **Normal Events**

Normal Punch Opening: In **[Only Card]** verification mode, the person having open door levels punch card at valid time period, open the door, and trigger the normal event.

Normal Press Fingerprint Opening: In **[Only Fingerprint]** or **[Card or Fingerprint]** verification mode, the person having open door levels press fingerprint at valid time period, the door is opened, and trigger the normal event.

Card and Fingerprint Opening: In **[Card and Fingerprint]** verification mode, the person having the open permission, punch the card and press the fingerprint at the valid time period, and the door is opened, and trigger the normal event.

Exit button Open: press the exit button to open the door within the door valid time zone, and trigger this normal event.

Trigger the exit button (locked): indicates the normal event triggered by pressing the exit button when the exit button is locked.

Punch during Normal Open Time Zone: At the normal open period (set normal open period for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission punch effective card at the opened door to trigger this normal event.

Press Fingerprint during Normal Open Time Zone: At the normal open period (set normal open period for a single door or for first-person normally open), or through the remote normal open operation, the person having open door permission press the effective fingerprint at the opened door to trigger this normal event.

First-Person Normally Open (Punch Card): In **[Only Card]** verification mode, the person having first-person normally open permission, punch at the setting first-person normally open time period (the door is closed), and trigger the normal event.

First-Person Normally Open (Press Fingerprint): In **[Only Fingerprint]** or **[Card plus Fingerprint]** verification mode, the person having first-person normally open permission, press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

First-Person Normally Open (Card plus Fingerprint): In **[Card plus Fingerprint]** verification mode, the person having first-person normally open permission, punch the card and press the fingerprint at the setting first-person normally open period (the door is closed), and trigger the normal event.

Normal Open Time Zone Over: After the normal open time zone over, the door will close automatically.

Remote Normal Opening: When set the door state to normal open in the remote opening operation, this normal event is triggered.

Cancel Normal Open: When Punch the valid card or use remote opening function to cancel the current door normal open state, this normal event is triggered.

Disable Intraday Passage Mode Time Zone: In door normal open state, punch effective card for five times (must be the same user), or select **[Disable Intraday Passage Mode Time Zone]** in remote closing operation, and this normal event is triggered.

Enable Intraday Passage Mode Time Zone: If the intraday passage mode time zone is disabled, punch effective card for five times (must be the same user), or select **[Enable Intraday Passage Mode Time Zone]** in remote opening operation, and this normal event is triggered.

Multi-Person Opening Door (Punching): In **[Only Card]** verification mode, Multi-Person combination can be used to open the door. After the last card is verified, the system triggers this normal event.

Multi-Person Opening Door (Press Fingerprint): In **[Only Fingerprint]** or **[Card plus Fingerprint]** verification mode, Multi-Person combination can be used to open the door. After the last fingerprint is verified, the system triggers this normal event.

Multi-Person Opening Door (Card plus Fingerprint): In **[Card plus Fingerprint]** verification mode, Multi-Person combination can be used to open the door. After the last card plus fingerprint is verified, the system triggers this normal event.

Emergency Password Opening Door: Emergency password (also known as super password) set for the current door can be used for door open. This normal event will be triggered after the emergency password is verified.

Opening Door during Normal Open Time Zone: If the current door is set a normally open period, the door will open automatically after the setting start time has expired, and this normal event will be triggered.

Linkage Event Triggered: After linkage configuration takes effect, this normal event will be triggered.

Cancel Alarm: When the user cancels the alarm of corresponding door successfully, this normal event will be triggered.

Remote Opening: When the user opens a door by **[Remote Opening]** successfully, this normal event will be triggered.

Remote Closing: When the user closes a door by **[Remote Closing]** successfully, this normal event will be triggered.

Open Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Open for Action Type, this normal event will be triggered when the linkage setting takes effect.

Close Auxiliary Output: In linkage setting, if the user selects Auxiliary Output for Output Point, selects Close for Action Type, or closes the opened auxiliary output by **[Door Setting]** > **[Close Auxiliary Output]**, this normal event will be triggered.

Door Opened Correctly: When the door sensor detects the door has been properly opened, triggering this normal event.

Door Closed Correctly: When the door sensor detects the door has been properly closed, triggering this normal event.

Auxiliary Input Point Disconnected: Will be triggered auxiliary input point is disconnected.

Auxiliary Input Point Shorted: When the auxiliary input point short circuit, trigger this normal event.

Device Start: Will be triggered if device starts (This event of PULL devices will not appear in real-time monitoring and can be viewed only in event records of reports).

- **Abnormal Events**

Too Short Punch Interval: When the interval between two punching is less than the set time interval, this abnormal event will be triggered.

Too Short Fingerprint Pressing Interval: When the interval between two fingerprints pressing is less than the set time interval, this abnormal event will be triggered.

Door Inactive Time Zone (Punch Card): In **[Only Card]** verification mode, if the user having the door open permission punch but not at door effective period of time, this abnormal event will be triggered.

Door Inactive Time Zone (Press Fingerprint): If the user having the door open permission, press the fingerprint but not at the door effective time period, this abnormal event will be triggered.

Door Inactive Time Zone (Exit Button): If the user having the door open permission, press exit button but not at the effective period of time, this abnormal event will be triggered.

Illegal Time Zone: If the user with the permission of opening the door, punches during the invalid time zone, this abnormal event will be triggered.

Illegal Access: If the registered card without the permission of current door is punched to open the door, this abnormal event will be triggered.

Anti-Passback: When the anti-pass back takes effect, this abnormal event will be triggered.

Interlock: When the interlocking rules take effect, this abnormal event will be triggered.

Multi-Person Verification (Punching): When Multi-Person combination opens the door, the card verification before the last one (whether verified or not), this abnormal event will be triggered.

Multi-Person Verification (Press Fingerprint): In **[Only Fingerprint]** or **[Card or Fingerprint]** verification mode, When Multi-Person combination opens the door, the fingerprint verification before the last one (whether verified or not), this abnormal event will be triggered.

Unregistered Card: If the current card is not registered in the system, this abnormal event will be triggered.

Unregistered Fingerprint: If the current fingerprint is not registered or it is registered but not synchronized with the system, this abnormal event will be triggered.

Opening Door Timeout: If the door sensor detects that it is expired the delay time after opened, if not close the door, this abnormal event will be triggered.

Card Expired: If the person with the door access level, punches after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Fingerprint Expired: If the person with the door access permission, presses fingerprint after the effective time of the access control and cannot be verified, this abnormal event will be triggered.

Password Error: If using **[Card plus Password]** verification mode, duress password or emergency password to open door, this abnormal event will be triggered.

Failed to Close door during Normal Open Time Zone: If the current door is in normal open state, but the user cannot close it by **[Remote Closing]**, this abnormal event will be triggered.

Verification Mode Error: If the user opening door mode is inconsistent with that set for current door, this abnormal event will be triggered.

Background Verification Failed: If the background verification fails, this abnormal event will be triggered.

Background Verification Success: If the background verification succeeds, this abnormal event will be triggered.

Background Verification Timeout: If no background verification result is returned in the specified period, this abnormal event will be triggered.

Multi-Person Verification Failed: When Multi-Person combination opens the door, the verification is

failed, and triggers this abnormal event.

- **Alarm Events**

Duress Password Opening Door: Use the duress password of current door for verifying successfully and trigger this alarm event.

Duress Fingerprint Opening Door: Use the duress fingerprint of current door for verifying successfully and trigger this alarm event.

Duress Opening Door Alarm: Use the duress password or duress fingerprint set for current door for verifying successfully and trigger this alarm event.

Opened Accidentally: Except all normal events, if the door sensor detects that the door is opened, and this alarm event will be triggered.

Door-open timeout: This alarm event is triggered when the opened door is not locked at closing door time.

Tamper-Resistant Alarm: This alarm event will be triggered when AIO device is tampered.

Server Connection Failed: This alarm event will be triggered when the device is disconnected from the server.

Mains power down: Inbio5 series controller events, external power down.

Battery power down: Inbio5 series controller event, built-in battery power-down.

Invalid card alarm: Alarm event trigger when invalid card swiping five consecutively.

✍**Notes:** The user can customize the level of each event (Normal, Abnormal, and Alarm).

Elevator Event Type

- **Normal Events**

Normal Punch Open: This normal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card and passed the verification.

Punch during passage mode time zone: This normal event is triggered if a valid card is punched after a user with the floor opening right sets the Normally Open periods for a specific floor, or sets the floor to the Normally Open state through the remote opening floor operation.

Open during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific floor, or sets the floor to the Normally Open state through the remote opening floor operation.

Remote release: This normal event is triggered if a user remotely releases a button successfully.

Remote locking: This normal event is triggered if a user remotely locks a button successfully.

Disable intraday passage mode time zone: This normal event is triggered if a user performs this operation on the Remotely Release Button page when a floor is in Normally Open state.

Enable intraday passage mode time zone: This normal event is triggered if the user performs this operation on the Remotely Lock Button page when the Normally Open periods of the floor are prohibited on the day.

Normal fingerprint open: This normal event is triggered if a user with the button releasing right presses his/her fingerprint in the "Card or fingerprint" verification mode and the verification is passed.

Press fingerprint during passage mode time zone: This normal event is triggered if a fingerprint is pressed after a user with the floor opening right sets the Normally Open periods for a specific door, or sets the door to the Normally Open state through the remote opening door operation.

Passage mode time zone over: When the preset Normally Open period arrives, the button is automatically locked.

Remote normal opening: This normal event is triggered if a user selects the continuously releasing button to set the button in continuously released state on the page for remotely opening the floor.

Device started: This normal event is trigger upon startup of the device. (This event will not appear in the real-time monitoring, and can only be viewed through the event records in the report.)

Password open: This normal event is triggered if a user with the button releasing right presses the password in the "Password only" or "Card or fingerprint" verification mode and the verification is passed.

Superuser open buttons: This normal event is triggered if the super user remotely releases a button successfully.

Start the fire floor: Release all buttons in the case of emergency so that users can select floors.

Superuser close buttons: This normal event is triggered if the super user remotely closes floors (locks the buttons) successfully.

Enable elevator control button: Restart the elevator control function.

Disable elevator control button: Temporarily disable the elevator control function.

Auxiliary input disconnected: This normal event is triggered if the auxiliary input point is disconnected.

Auxiliary input shorted: This normal event is triggered if the auxiliary input point is short circuited.

- **Abnormal Events**

Operate interval too short: This abnormal event is triggered if the actual interval between two times of card punching is smaller than the interval that is set for this floor.

Press fingerprint interval too short: This abnormal event is triggered if the actual interval between two times of fingerprint pressing is smaller than the interval that is set for this floor.

Button inactive time zone (punch card): This abnormal event is triggered if the verification mode is associated with cards, and a user with the floor opening right punches his/her card beyond the effective periods.

Illegal time zone: This abnormal event is triggered if a user with the floor opening right punches his/her card beyond the effective periods.

Access denied: This abnormal event is triggered if a registered card is punched before the elevator control right of the current floor is set for this card.

Disabled card: This event is triggered if the current card number is not registered in the system yet.

Card expired: This event is triggered if a person, for whom the elevator control effective time is set, punches his/her card beyond the elevator control effective periods and verification fails.

Fingerprint expired: This event is triggered if a person, for whom the elevator control effective time is set, presses his/her fingerprint beyond the elevator control effective periods and verification fails.

Password error: This event is triggered if the verification mode is associated with the password and the password verification fails.

Disabled fingerprint: This event is triggered if the current fingerprint is not registered in the system or has been registered but not synchronized to the device.

Button inactive time zone (press fingerprint): This abnormal event is triggered if a user with the floor opening right presses his/her fingerprint beyond the effective periods of the floor.

Failed to close during passage mode time zone: This abnormal event is triggered if the current floor is in Normally Open state and the button cannot be locked by performing the Remotely Locking Button operation.

Wiegand format error: This abnormal event is triggered if a card is punched and the Wiegand format of this card is incorrectly set.

✍**Note:** User can self-define the level of each event (normal, abnormal and alarm).

Offline Elevator Control Manual

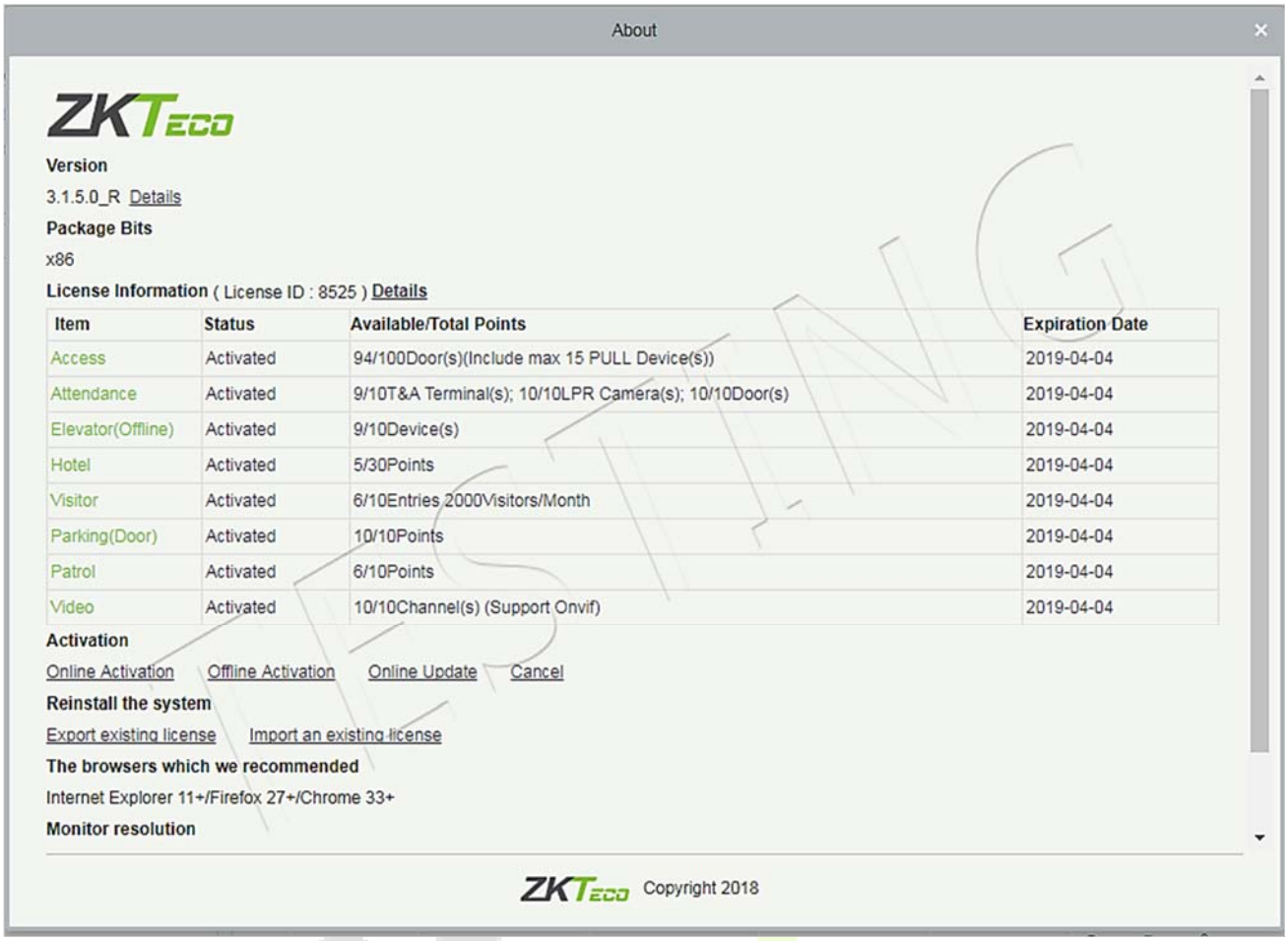
To use offline elevator control mode, you must use an offline elevator control license.

Offline Elevator Device

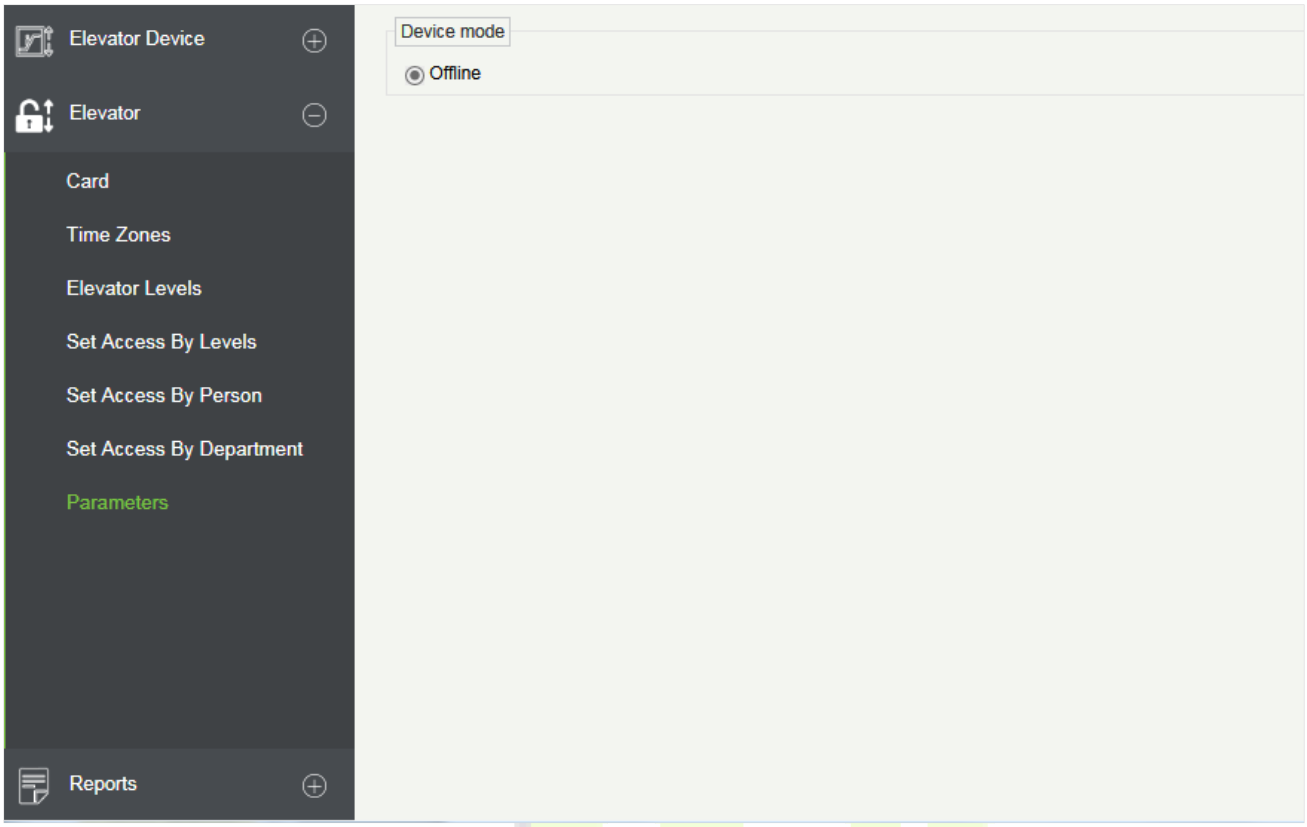
Add the offline elevator control device to facilitate user management of device in the software. Among them, rights management is the same as online elevator control, offline elevator control module does not support most of the functions, such as synchronization data, equipment monitoring, real-time monitoring. Compared with the online elevator control, the following functions are missing: event type, device monitoring, real-time monitoring, holidays, global linkage, all records, all abnormal records, currently only supports synchronization time and modify button open duration and card writing operation.

New offline elevator devices:

System authorization

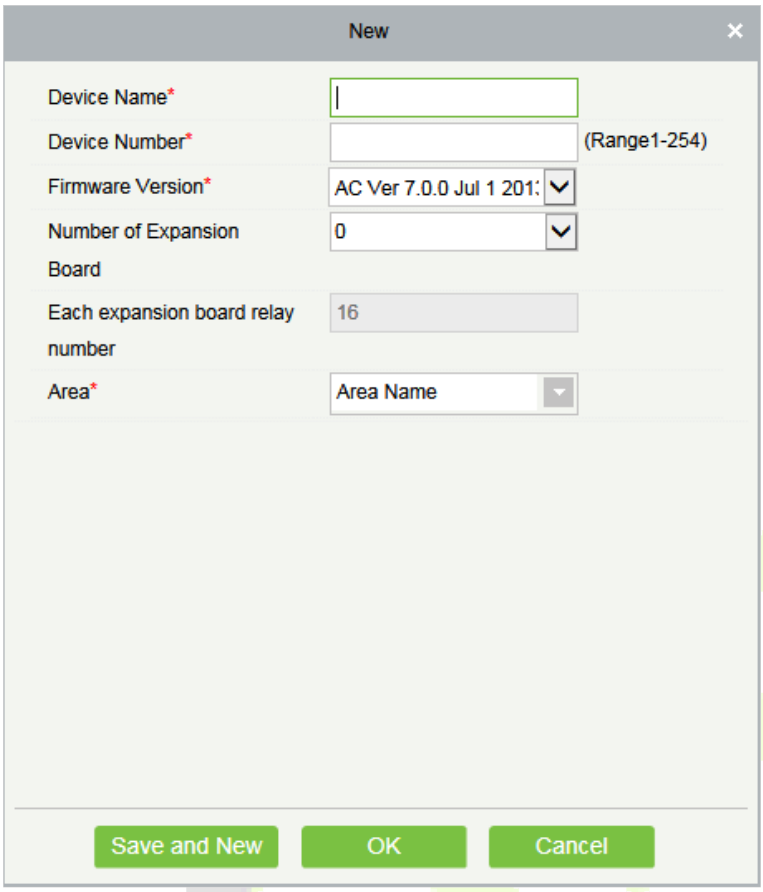


After offline elevator control is authorized, the default software and device mode in elevator parameter setting is offline and cannot be changed.



- **Add devices by manually**

Click **[Elevator Device]** > **[Device]** > **[New]** on the Action Menu, the following interface will be shown:



Fields are as follows:

Device Name: Any character, up to a combination of 20 characters.

Device Number: Range 1 ~ 254, the machine number cannot be repeated.

Firmware Version: Firmware version number of elevator control device.

Number of Expansion Board: Expands the number of floors that the elevator control device can control.

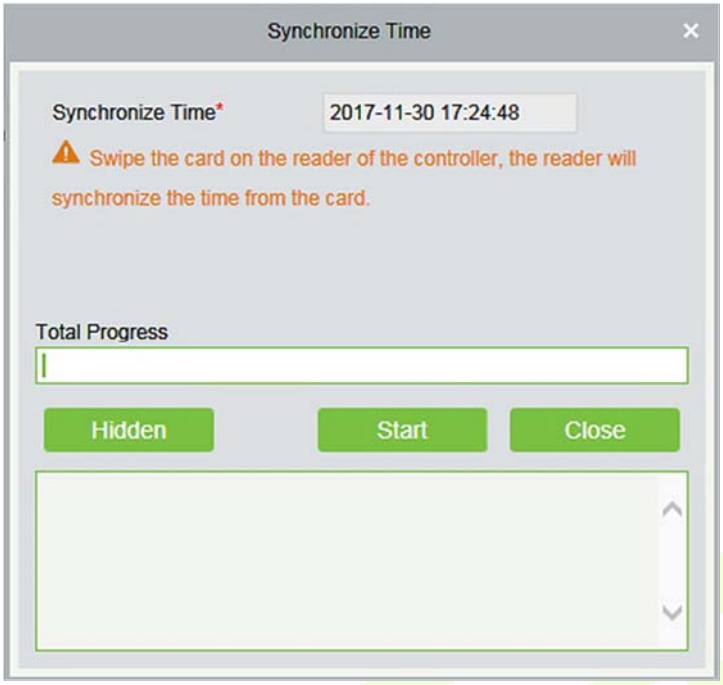
Each expansion board relay number: 16 relays per expansion board.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-Time Monitoring.

✍**Note:** When adding a device, the device number in the software should be the same as the 485 address setting number on the device.

- **Synchronize Time**

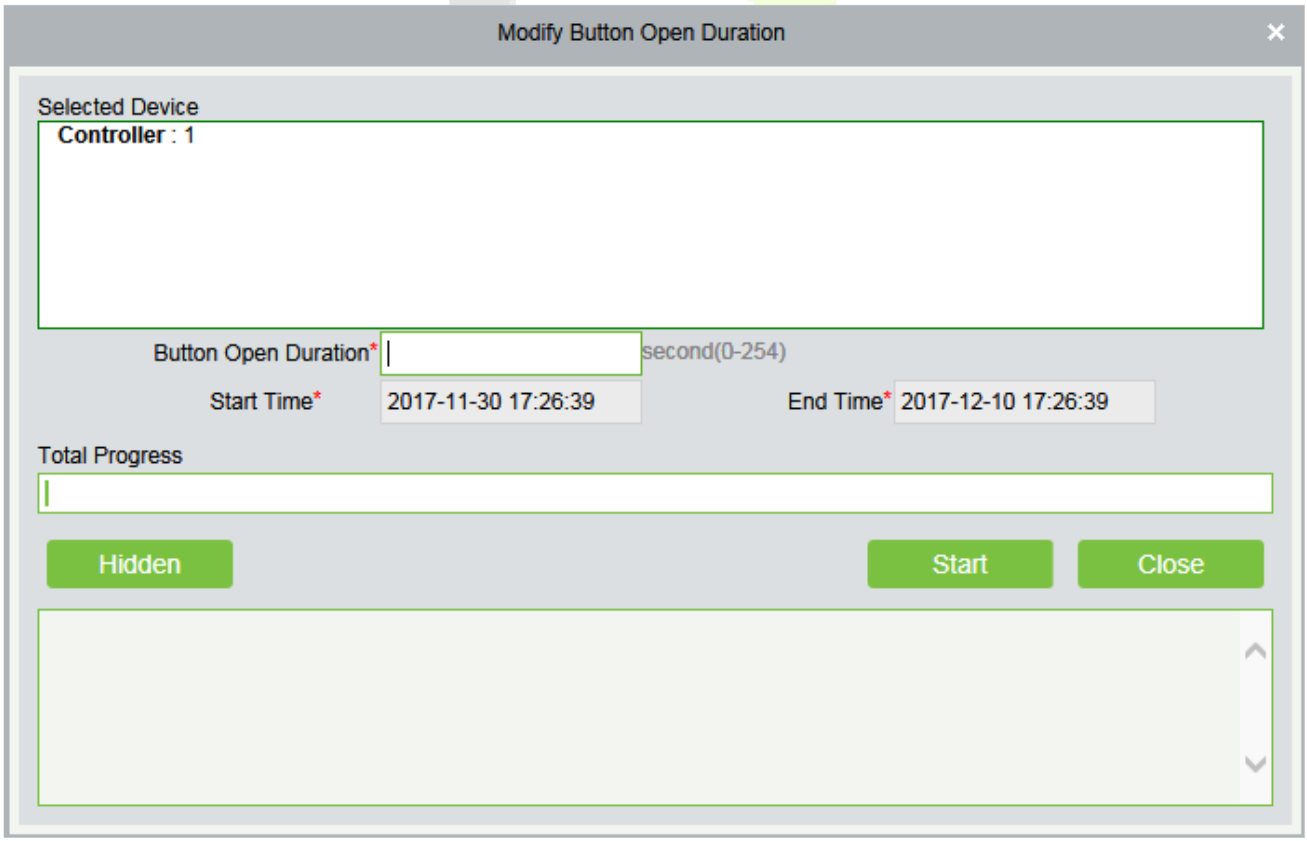
Click **[Elevator Device]** > **[Device]** > **[Synchronize Time]** on the Action Menu, the following interface will be shown:



Synchronize device time with current server time.

- **Modify Button Open Duration**

Click **[Elevator Device]** > **[Device]** > **[Modify Button Open Duration]** on the Action Menu, the following interface will be shown:

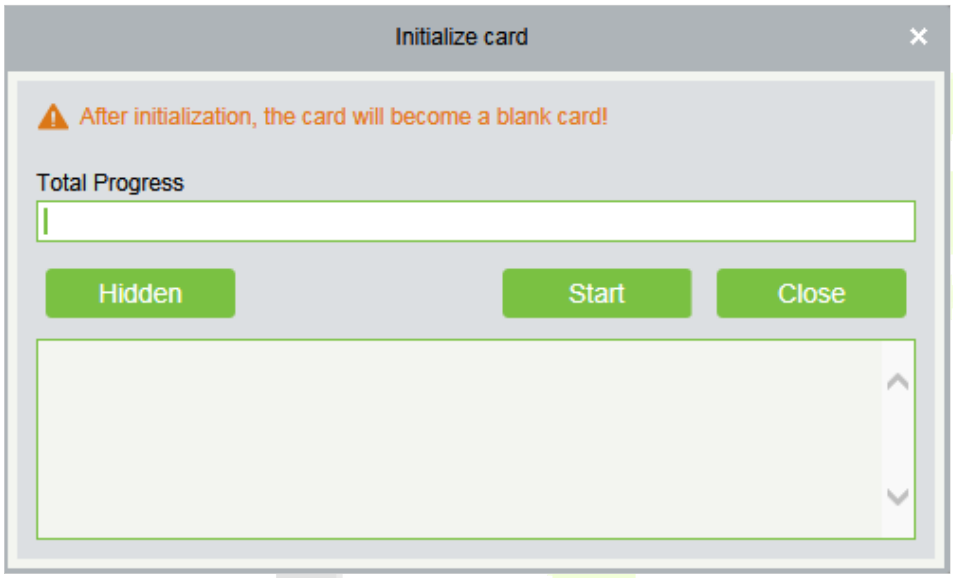


Button Open Duration: It is used to control the time period to press floor button after verification. The default value is 5 seconds; the range is 0~254 seconds.

Initialize Card

Users can initialize the card to restore the default password and sector operation.

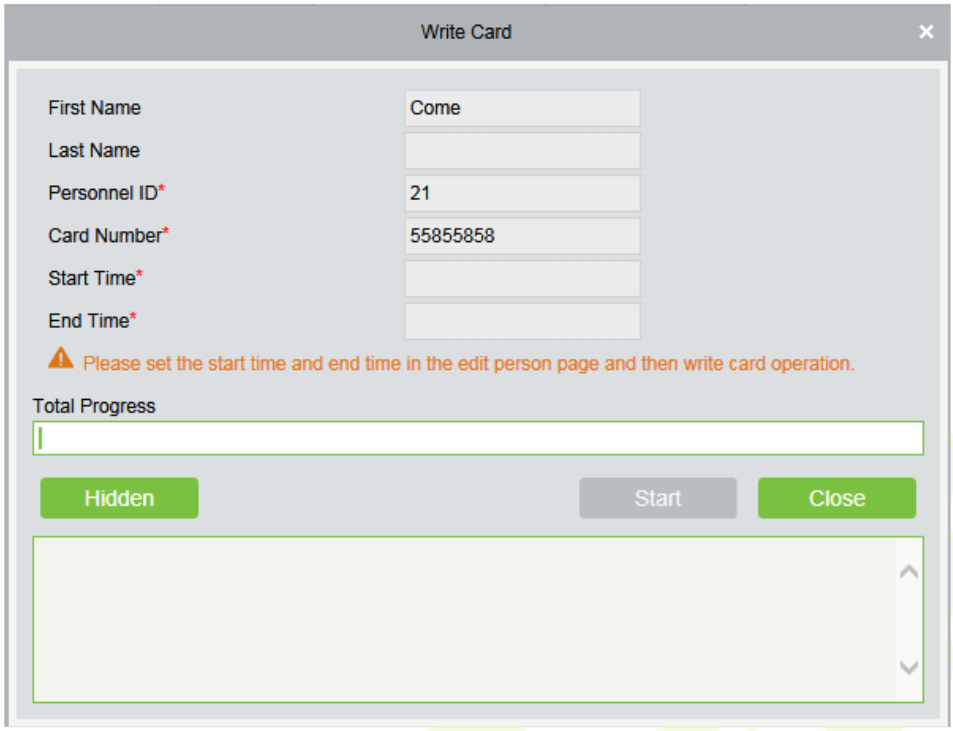
Click **[Elevator Device]** > **[Card]** > **[Initialize Card]** on the Action Menu, the following interface will be shown:



Write Card

Write device number, personnel ID, personnel password, personnel authority, start time, end time, card number (calculated logic card number) and other related information to the card.

Click **[Elevator Device]** > **[Card]** > **[Write Card]** on the Action Menu, the following interface will be shown:



Fields are as follows:

First/Last Name: The maximum length cannot exceed 50, does not support comma; value sources Personnel field, cannot add, modify, delete.

Personnel ID: The default maximum length of personnel ID is 9, the effective range is 1-799999999, which can be configured according to the actual situation. Value sources Personnel field, cannot be added, modified or deleted.

Card number: Card number cannot be repeated, the maximum length of 10; value sources Personnel field, cannot add, modify, delete.

Start time: The effective starting time of the card; value sources Personnel field, cannot add, modify, delete.

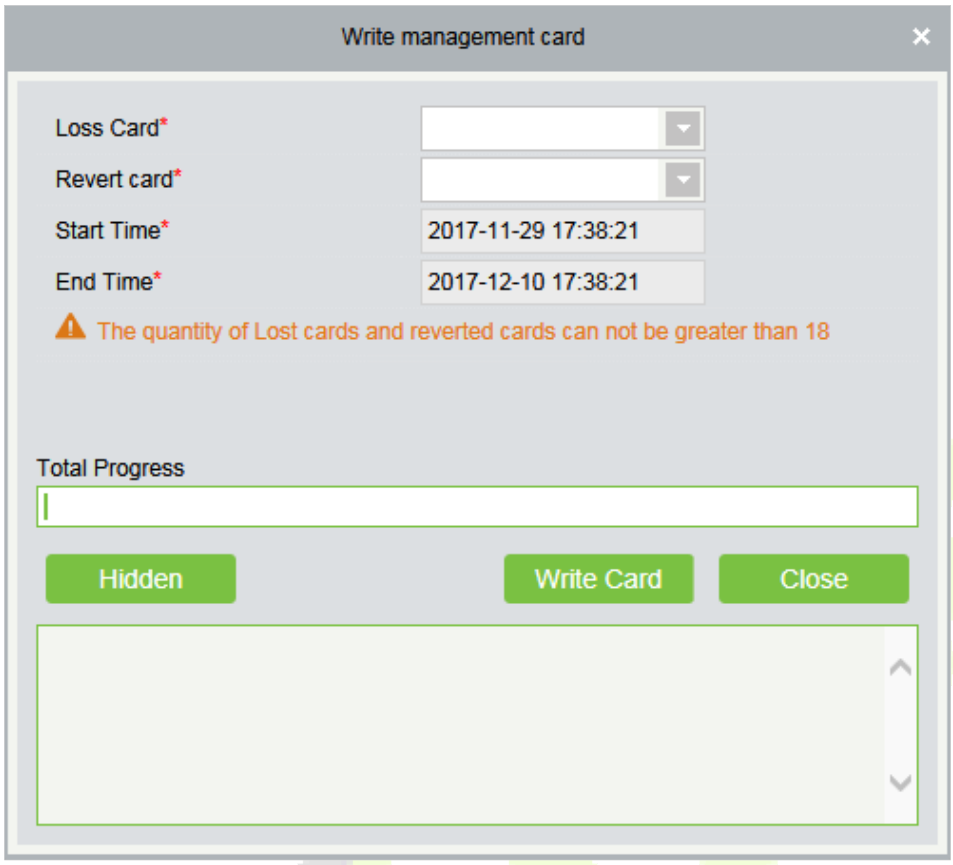
End time: The effective cut-off time of the card; value sources Personnel field, cannot add, modify, delete.

✍**Note:** Personnel related authority (elevator levels), card number and related data can only be written when the personnel editing page is completely filled in. The card number is calculated logical card number; the logical card number stored in the database shall prevail.

Write management card

Management card is mainly used to loss and revert card. When the card is lost or reverted, you need to write the card information into the management card, thus loss and revert card take effect.

Click **[Elevator Device]** > **[Card]** > **[Write management card]** on the Action Menu, the following interface will be shown:



Fields are as follows:

Function selection: Management card is used to write the loss and revert card data in the software system to the management card and then loss and revert card by brushing the management card on the device.

Loss Card: Lost Card collection, drop-down selection.

Revert card: Revert Card collection, drop-down selection.

Start Time: The effective starting time of the card; value sources Personnel field, cannot add, modify, delete.

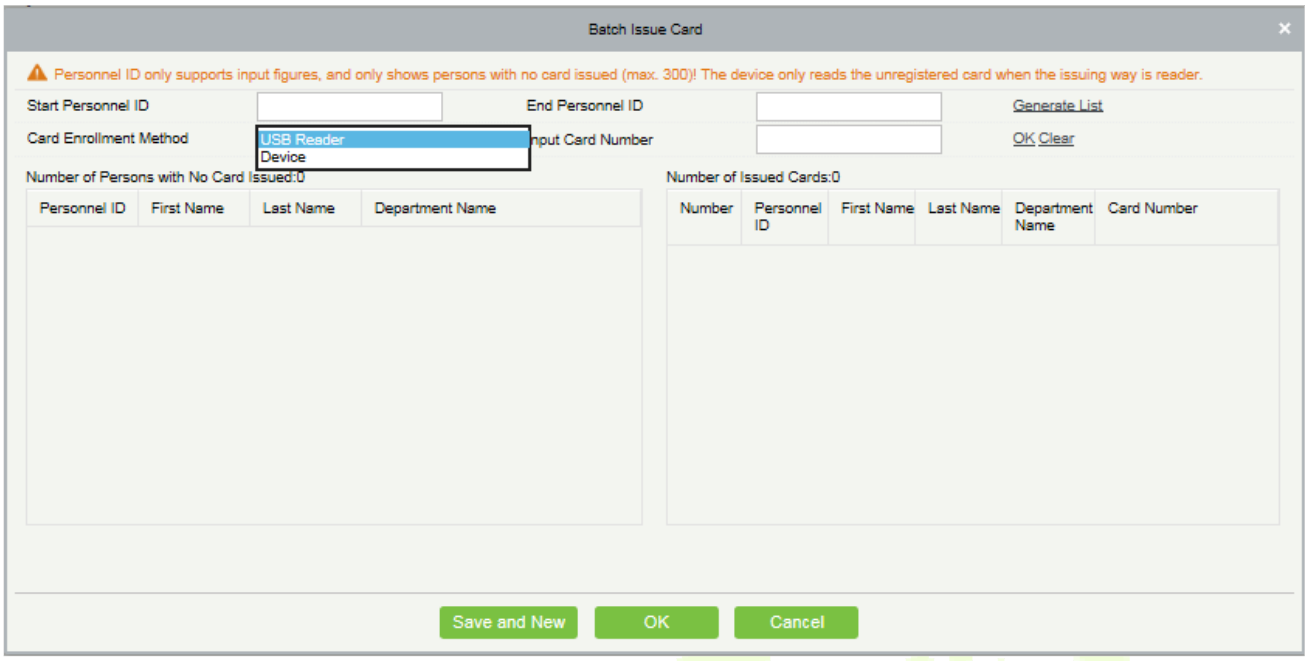
End Time: The effective deadline of the card; value sources Personnel field, cannot add, modify, delete.

Personnel System - Card

Check the list of cards in the system and batch issue card, assigning cards to personnel.

- **Batch Issue Card**

Click **[Personnel]** > **[Card Manage]** > **[Card]** > **[Batch Issue Card]**:



Card Enrollment Method: USB Reader or device.

Input Card Number: It can be generated by swiping an ID card on the USB reader and device, or entering it manually. The card manually entered may be IC card.

- **Report Lost Card**

Click **[Personnel]** > **[Card Manage]** > **[Card]** > **[Report Lost Card]**:

✍**Note:** Report Lost Card is applicable to all functional modules, not to the offline elevator module. After the report of loss, the status of the card becomes invalid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **[Write management card]** (**[Elevator Device]** > **[Card]** > **[Write management card]**).

- **Reactivate Lost Card**

Click **[Personnel]** > **[Card Manage]** > **[Card]** > **[Reactivate Lost Card]**:

✍**Note:** Reactivate Lost Card is applicable to all functional modules, not to the offline elevator module. After reactivating lost card, the status of the card becomes valid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **[Write management card]** (**[Elevator Device]** > **[Card]** > **[Write management card]**).

FAQs

Q: How to use a card issuer?

A: Connect the card issuer to PC through USB port, and then select individual personnel card issue or batch card issue. Move the cursor to the card number input box, and punch the card on the card issuer, then the card number will be automatically shown in the input box.

Q: What is the use of role setting?

A: Role setting has the following uses: 1. To set unified level for the same type of users newly added, just directly select this role when adding users; 2. When setting system reminder and determine which roles can be viewed.

Q: How to operate if I want to set accounts for all personnel of the Company's Financial Department?

A: First, create a new role in system setting and configure the functions to be used for this role. Then add a user, set user information, and select the user's role, thus adding a new account. For other accounts, do the same.

Q: In Windows Server 2003, why the IE browser displayed error when access the system, how to solve it?

A: This problem occurs because that Server 2003 has **[Security Configuration Option]** settings. If you want to access the system, please configure it as follows: click Start - Control Panel - Add or Remove Program, select **[Add and remove Windows components]** in the interface and click **[Internet Explorer Enhanced Security Configuration]** option, cancel the tick before it. Then click [Next] to remove it from the system. Open the system again the browser will access the system properly.

Q: If backing up or restoring the database fails, the possible reason?

A:

Backup fails: Please check the system environment variables, please go to Properties > Advanced to set the environment variables as "C:\Program Files\ZKBioSecurity3.0\MainResource\postgresql\bin:". "C:\Program Files" is the system installation path, you can modify by your actual situation.

Restore fails: There are several reasons: The system version is too high or too low, or the database has been damaged, you need to follow the prompts to change the system version or repair the system, re-install the database.

END-USER LICENSE AGREEMENT

Important - read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this Software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights: Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse Engineering, Recompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components.

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Software Transfer.

You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Termination.

Without prejudice to any other rights, the Author of this Software may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.
Distribution.

The SOFTWARE PRODUCT may not be sold or be included in a product or package which intends to receive benefits through the inclusion of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT may be included in any free or non-profit packages or products.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT(including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by the Author of this Software. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes.

LIMITED WARRANTY

NO WARRANTIES.

The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or no infringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

NO LIABILITY FOR DAMAGES.

In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the Author of this Software has been advised of the possibility of such damages.

Acknowledgment of Agreement.

I have carefully read and understand this Agreement, ZKTeco, Inc.'s Privacy Policy Statement.

If YOU ACCEPT the terms of this Agreement:

I acknowledge and understand that by ACCEPTING the terms of this Agreement.

IF YOU DO NOT ACCEPT the terms of this Agreement.

I acknowledge and understand that by refusing to accept these terms, I have rejected this license agreement and therefore have no legal right to install, use, or copy this Product or the Licensed Software that it incorporates.

ZKTeco USA LLC

1600 Union Hill Road

Alpharetta, GA 30005

(862) 505 2101 | info@zktecousa.com | www.zktecousa.com