# USER MANUAL

## ZKBioAccess

Version: 1.0

Date: January 2019

Software Version: 1.0.0

# Important Statement

Thank you for choosing our product. Before using this product, please read this manual carefully. Proper operations of the product will result in better performance and faster verification.

None of the content of this document shall be copied or delivered in any forms or by any means without the prior written consent of our company.

The product described in the manual may include the software whose copyrights are shared by licensors, including our company. No one shall copy, distribute, revise, modify, extract, decompile, disassemble, decrypt, reverse engineer, lease, transfer, sub-license the software, or perform other acts of copyright infringement, unless such restrictions are prohibited by applicable laws or such actions are approved by respective copyright holders.

Information provided in this manual may differ from actual technical specifications due to the constant development of products. Our company claims no responsibility for any disputes arising out of any discrepancy between actual technical parameters and those described in this document. The document is subject to change without prior notice.

# 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 ZKBioAccess, that helps customers to integrate operations of safety procedures on one platform. The system is divided into three modules, namely: **Personnel**, **Access**, and **System**.

### ❖ Features

- ➢ It can manage around 2000 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 10GB or above. We recommend using NTFS hard disk partition as the software installation directory.
- ➢ Monitor Resolution of 1024 x 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: PostgreSQL
- ➢ 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

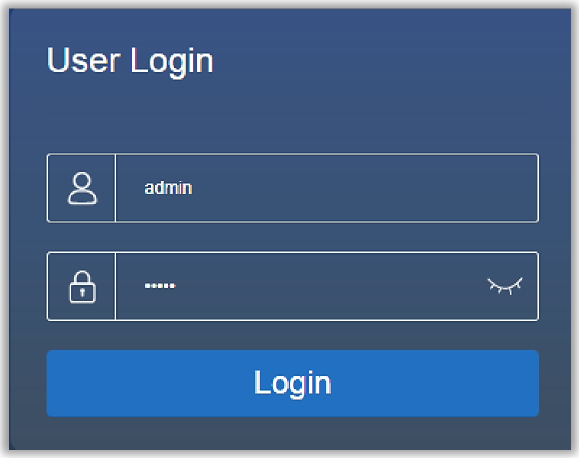
This module is a web-based management system which enables normal access control functions, management of networked access control panel via computer, and unified personnel access management. The access control system sets door opening time and levels for registered users.

## 1.3 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



User Login

admin

•••••

After installing the software, double-click the ZKBioAccess 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://127.0.0.1:8088 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 super user is [admin], and the password is [admin], then click [**Login**]. After the first login to the system, please reset the password in [Personal Information].

✍**Note:**

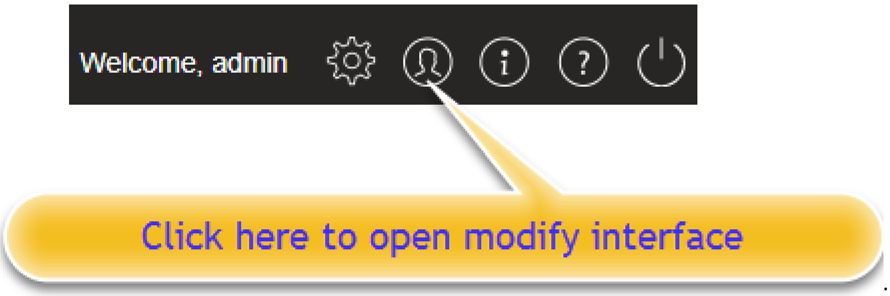
The user name of the super user is [admin], and the password is [admin]. After the first login to the system, please reset the password in [Personal Information].

## 2.2 Activate the System

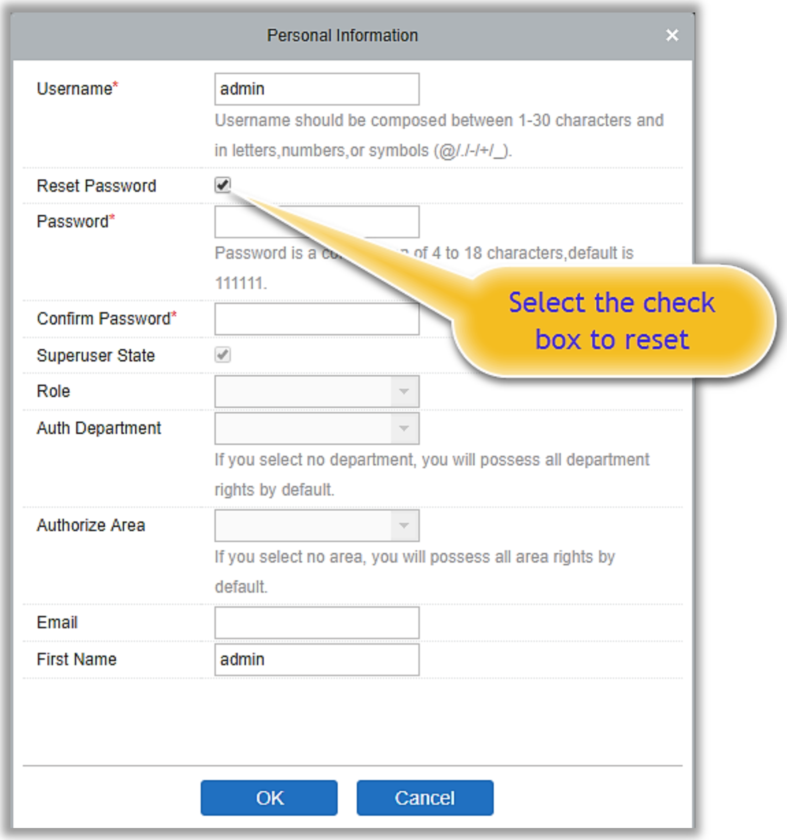
Please refer to the corresponding license activation document.

## 2.3 Modify Password

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



:



Personal Information ×

| | |
|---|---|
| Username* | admin<br>Username should be composed between 1-30 characters and in letters,numbers,or symbols (@/./-/+/_). |
| Reset Password | ☑ |
| Password* | <br>Password is a co n of 4 to 18 characters,default is 111111. |
| Confirm Password* | |
| Superuser State | ☑ |
| Role | |
| Auth Department | <br>If you select no department, you will possess all department rights by default. |
| Authorize Area | <br>If you select no area, you will possess all area rights by default. |
| Email | |
| First Name | admin |

OK Cancel

Select [Reset Password] check box to modify the password.

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

## 2.4 About

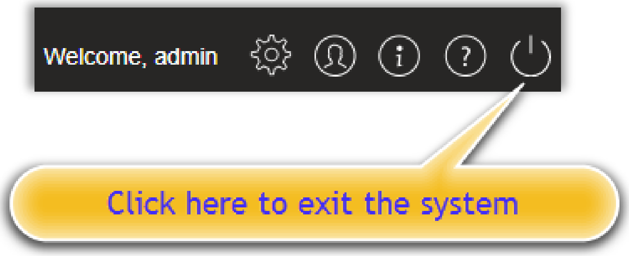
Click the [**About**] button ⓘ to check all the software version and license information.

## 2.5 Help

Click the [**Help**] button ? on the top right corner of the interface to get user manual.

## 2.6 Exit the system

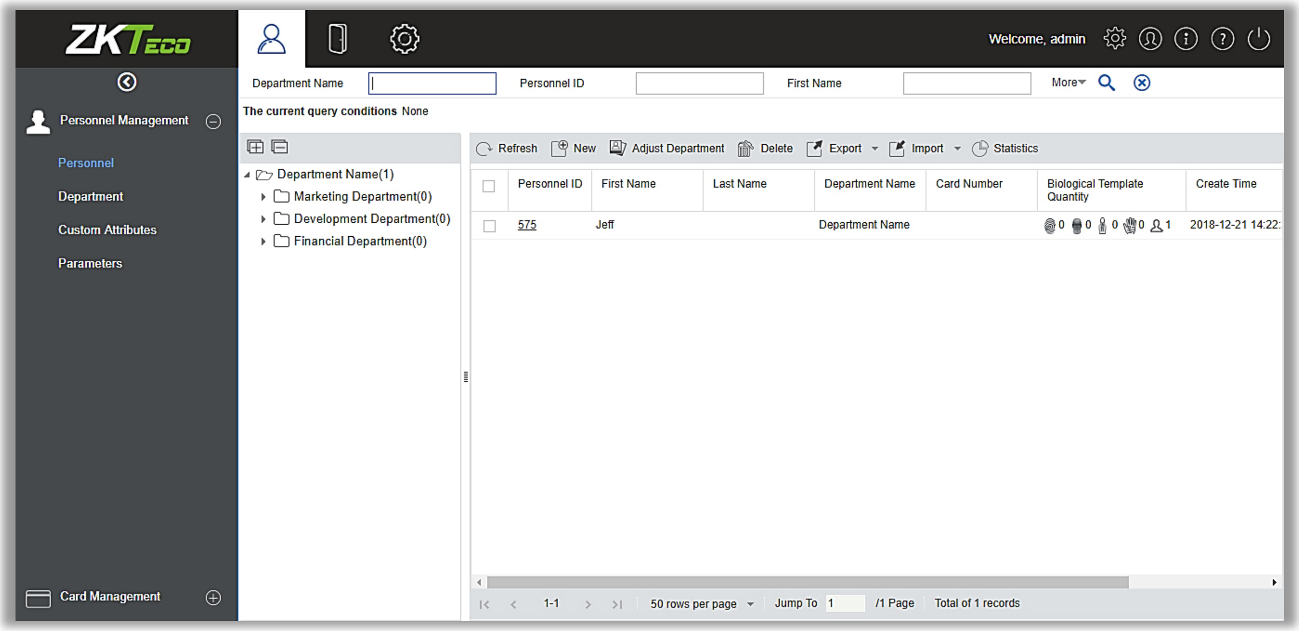
Click the [**Logout**] button ⏻ on the upper right corner of the interface to exit the system.



Click here to exit the system

# 3. Personnel

Please configure the Personnel Management and Card Management.



The current query conditions None

| □ | Personnel ID | First Name | Last Name | Department Name | Card Number | Biological Template Quantity | Create Time |
|---|---|---|---|---|---|---|---|
| □ | 575 | Jeff | | Department Name | | 0 0 0 0 1 | 2018-12-21 14:22: |

1-1 | 50 rows per page | Jump To 1 | /1 Page | Total of 1 records

## 3.1 Personnel Management

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

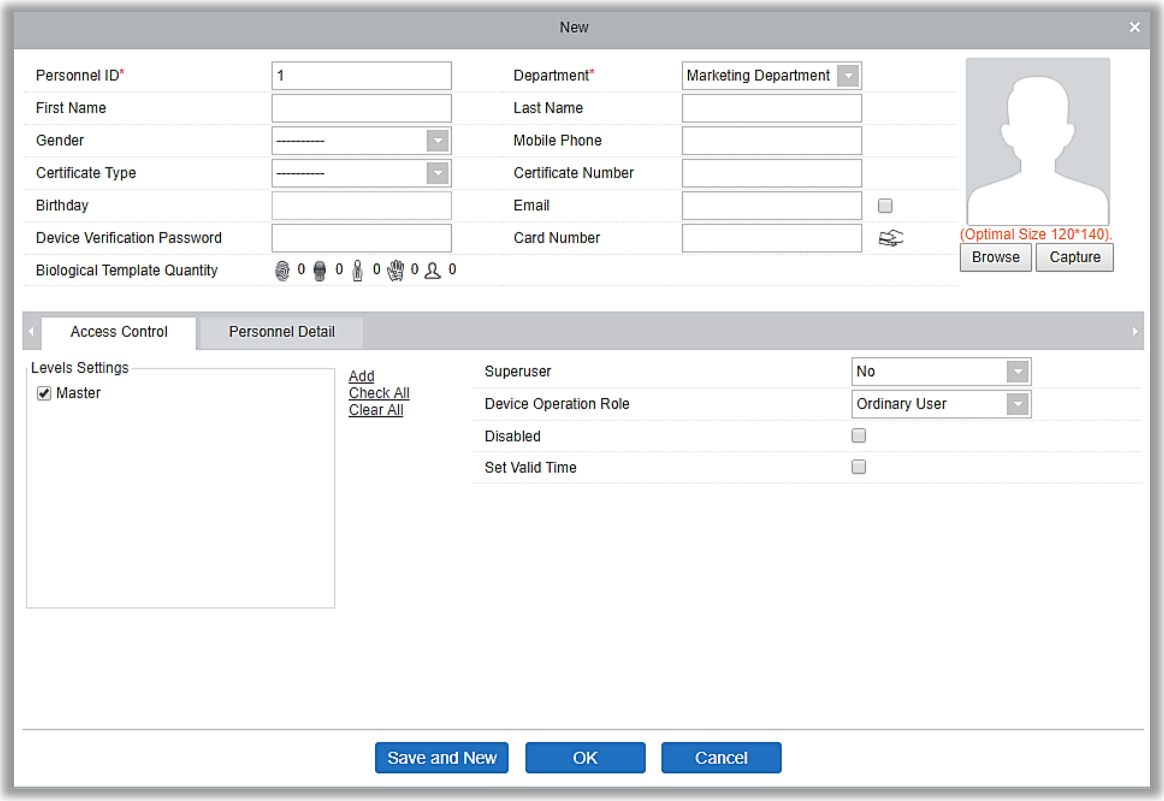
### 3.1.1 Personnel

When using this management program, the user shall register personnel in the system, or import personnel information from other software or file 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 Management] > [Personnel] > [New]:



| | | | |
|---|---|---|---|
| Personnel ID* | 1 | Department* | Marketing Department |
| First Name | | Last Name | |
| Gender | ---------- | Mobile Phone | |
| Certificate Type | ---------- | Certificate Number | |
| Birthday | | Email | □ |
| Device Verification Password | | Card Number | |
| Biological Template Quantity | 0 0 0 0 0 | | |

(Optimal Size 120*140).

Levels Settings

☑ Master

| | |
|---|---|
| Superuser | No |
| Device Operation Role | Ordinary User |
| Disabled | □ |
| Set Valid Time | □ |

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 characters is 50.

Gender: Set the gender of personnel.

Mobile Phone: Input the phone number of the user.

Certificate Type: There are four types of certificates: ID, Passport, Driver License and Others.

Certificate Number: Enter the ID number.

Birthday: Input employee’s actual birthday.

Email: Input employee’s Email ID. The max length is 30.

Device Verification Password: Set password for verifying on device using personnel accounts. It can only contain up to 6-digits. It cannot be the same with other user's password and the duress password.

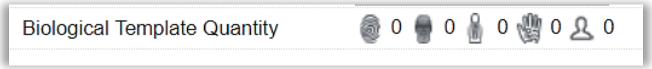
Card number: The max length is 10, and it should not be repeated.

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 photo on your local drive 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, Palm, or Face. To trigger the alarm and send the signal to the system, scan the Duress Fingerprint.

How to register fingerprint:

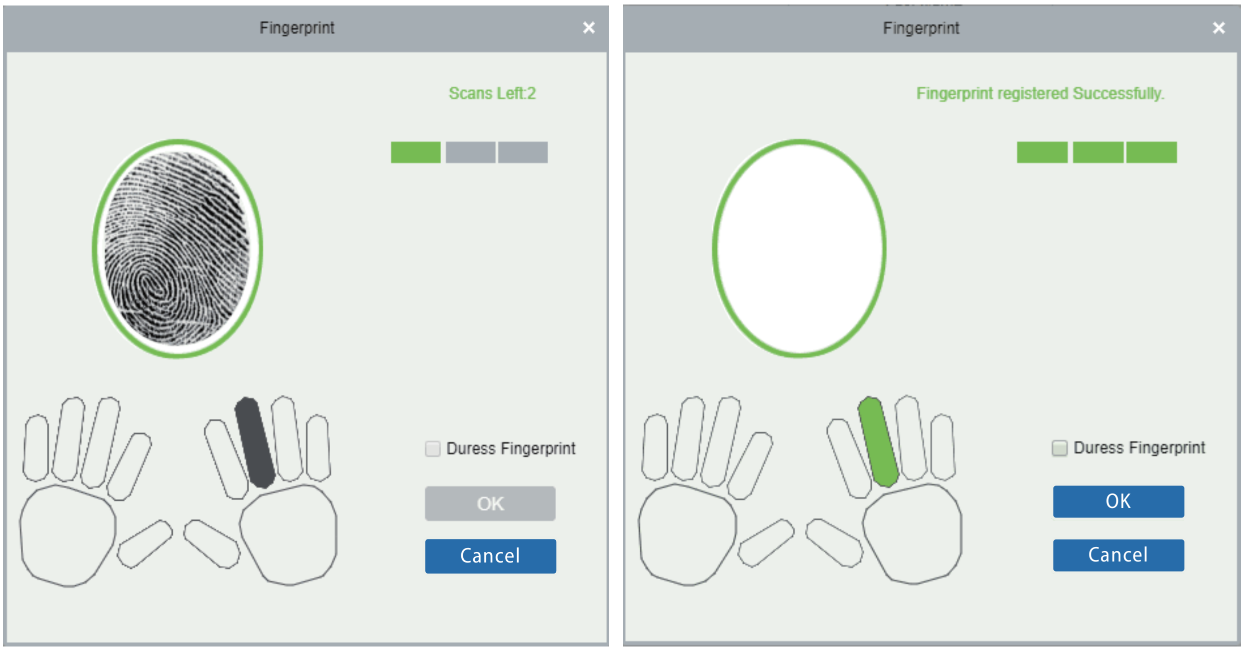


Biological Template Quantity 0 0 0 0 0

(1) Move the cursor to the fingerprint icon position, a registration pop-up or driver download dialog box will appear, click [Register].

(2) Select a fingerprint, press the finger on the sensor three times, then "Fingerprint registered Successfully" will be prompted.

(3) Click [OK] to complete registration.



Fingerprint

Scans Left:2

□ Duress Fingerprint

Fingerprint

Fingerprint registered Successfully.

□ Duress Fingerprint

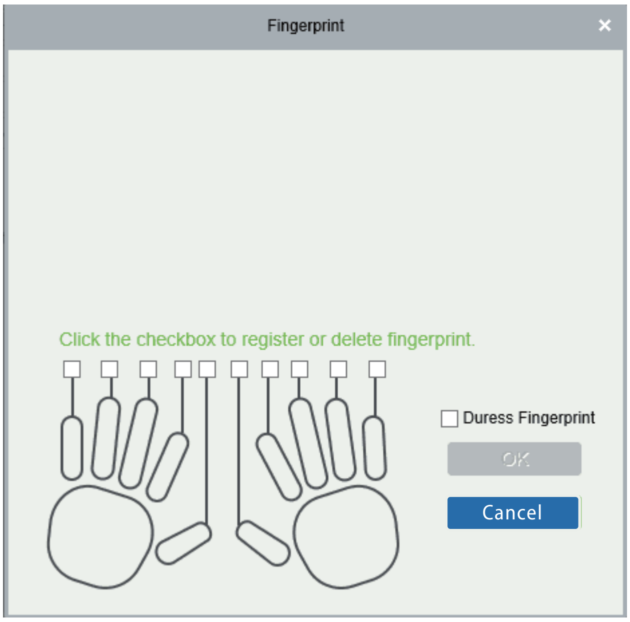
Click a fingerprint to delete. If you need to register a duress fingerprint, select the Duress Fingerprint check box.

✍**Notes:**

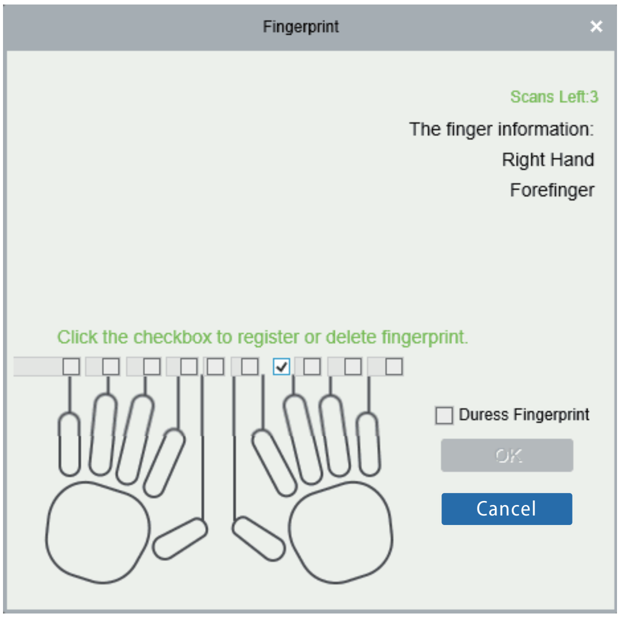
- If fingerprints are duplicated, "Don't repeat the fingerprint entry" will be prompted.

- 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 Internet Explorer, click [Tools] → [Internet Options] → [Security] → [Credible Sites], add http://localhost to the credible sites, then restart the Internet Explorer.
  2) In Internet Explorer, click [Tools] → [Internet Options] → [Advanced] → [Reset] to pop up a dialog of Reset Internet Explorer Settings, click [Reset] to confirm; then restart the Internet Explorer (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 select [Check for server certificate revocation], then restart IE.

4) If the browser is below IE8, the fingerprint registration page will be different:



Click the checkbox to register or delete fingerprint.

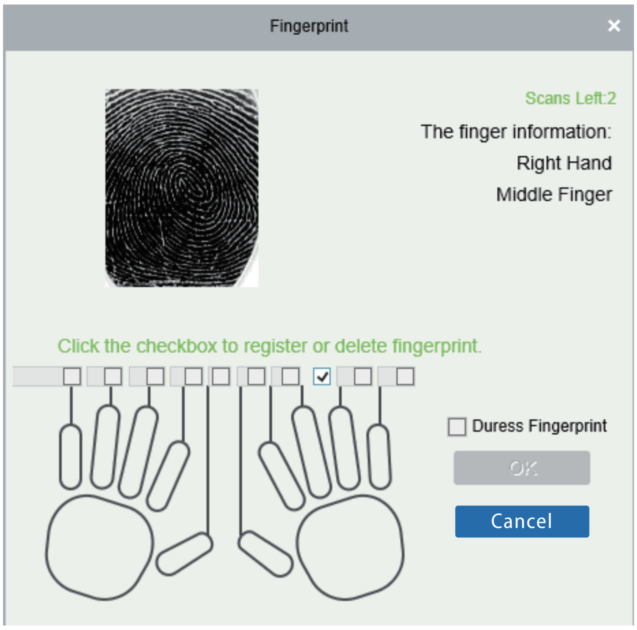


Scans Left:3

The finger information:
Right Hand
Forefinger

Click the checkbox to register or delete fingerprint.

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

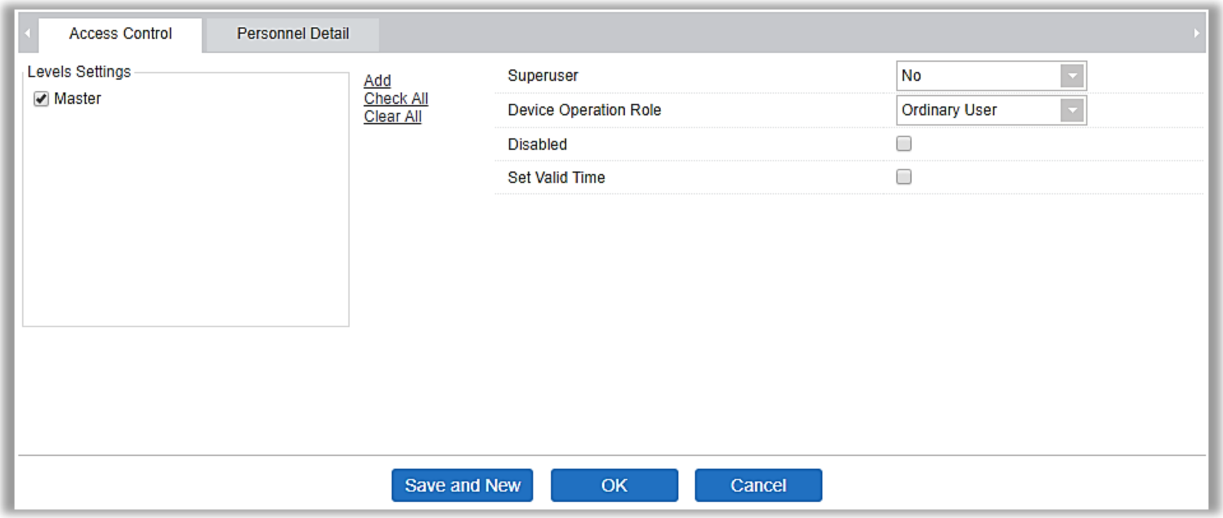


Scans Left:2

The finger information:
Right Hand
Middle Finger

Click the checkbox to register or delete fingerprint.

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



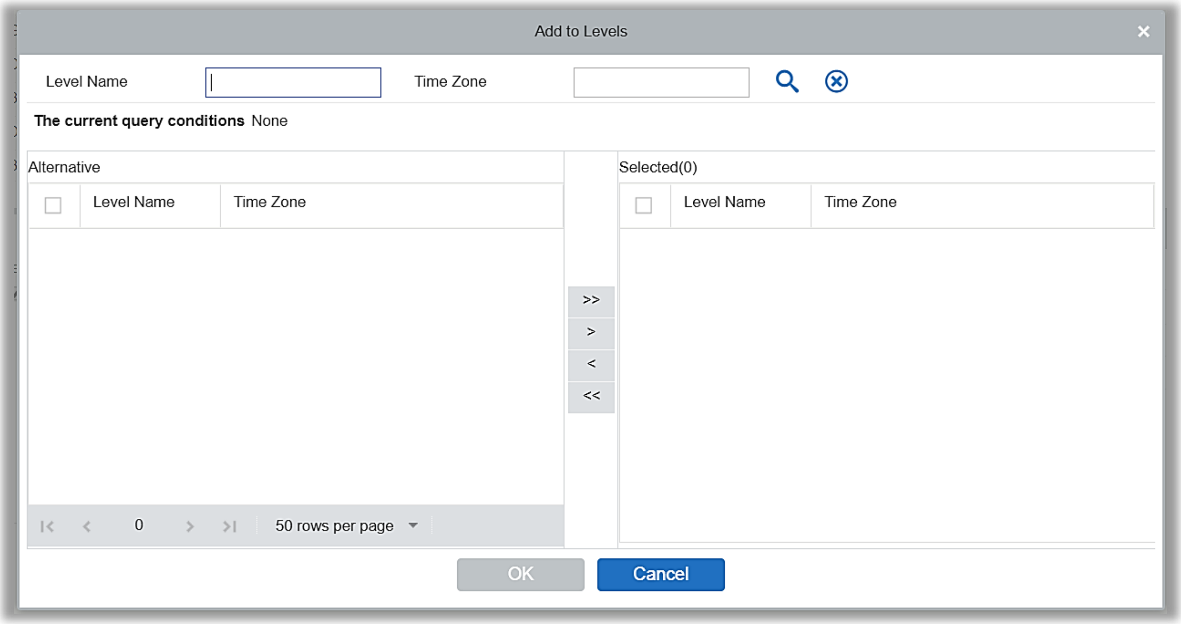
Levels Settings

☑ Master

| | |
|---|---|
| Superuser | No |
| Device Operation Role | Ordinary User |
| Disabled | □ |
| Set Valid Time | □ |

Fields are as follows:

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



The current query conditions None

| □ | Level Name | Time Zone |
|---|---|---|

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

Device Operation Role: It will define the authority level in device of the user.

Disabled: Temporarily disable the personnel’s access level.

Set Valid Time: Doors can be set to open only within certain time periods. If the check box is not selected, the door is always active.

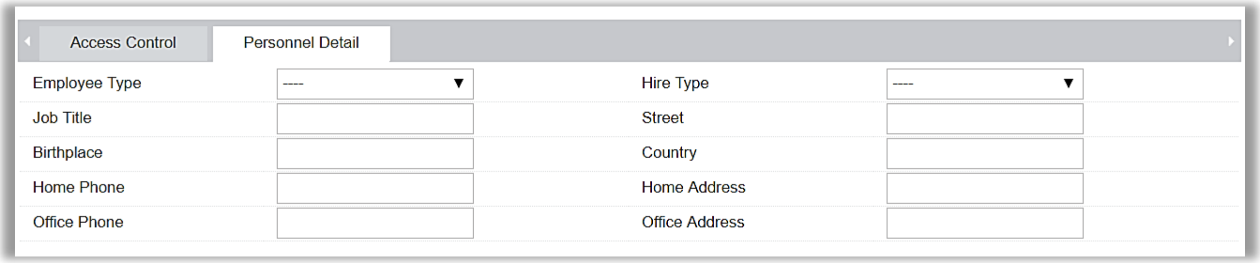
✍**Note:** The system will automatically search for the relevant numbers in the departure library during verification.

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 or not. Please upgrade the device to use this function.
- Not all the devices support the ”Set Valid Time” function. 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 or not. Please upgrade the device to use this function.

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



| | | | |
|---|---|---|---|
| Employee Type | ---- ▼ | Hire Type | ---- ▼ |
| Job Title | | Street | |
| Birthplace | | Country | |
| Home Phone | | Home Address | |
| Office Phone | | Office Address | |

4. 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].

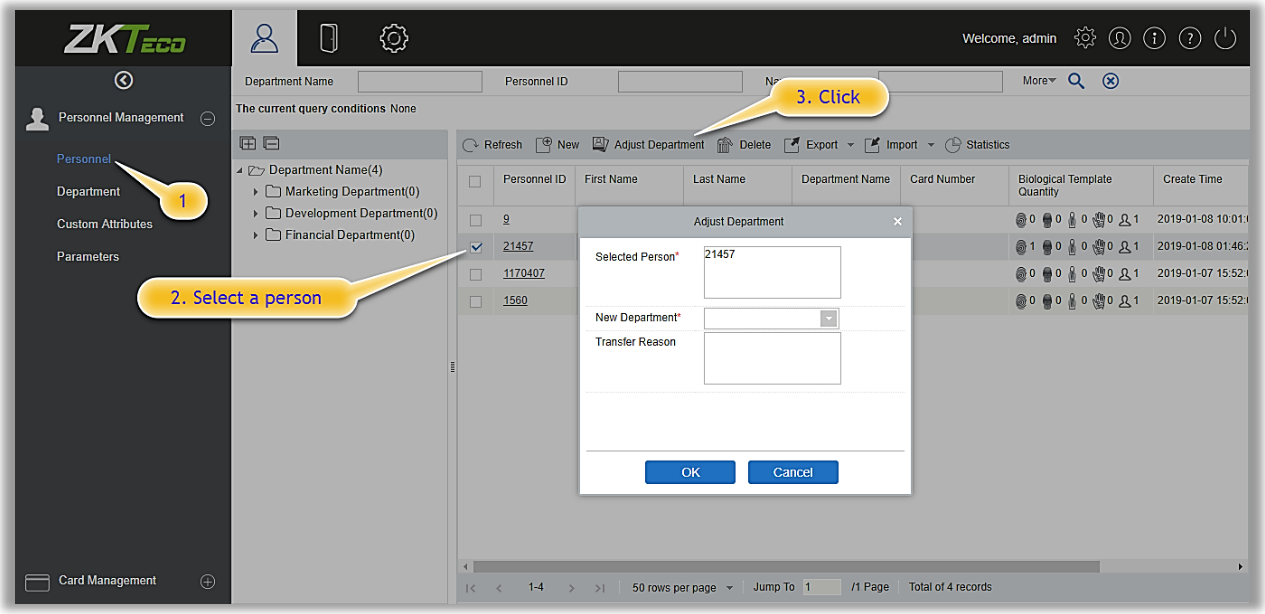
### ➢ Delete Personnel

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

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

### ➢ Adjust Department

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



1

2. Select a person

3. Click

| Personnel ID | Create Time |
|---|---|
| 9 | 2019-01-08 10:01: |
| ☑ 21457 | 2019-01-08 01:46: |
| 1170407 | 2019-01-07 15:52: |
| 1560 | 2019-01-07 15:52: |

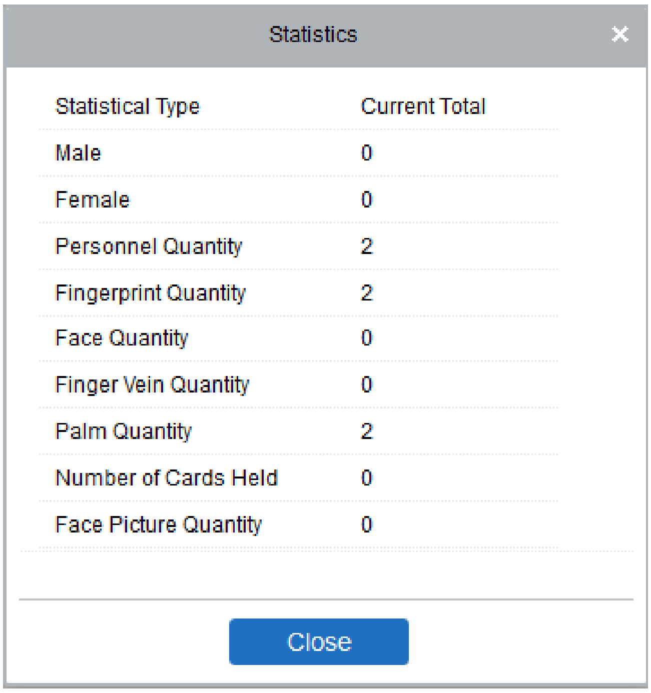
Selected Person*: 21457

2. Select from the dropdown list of “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.

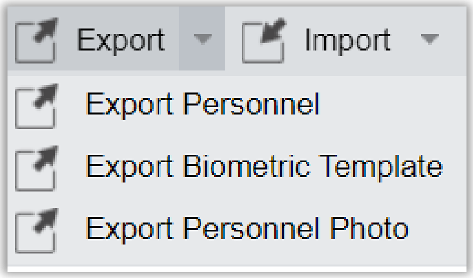


Statistics

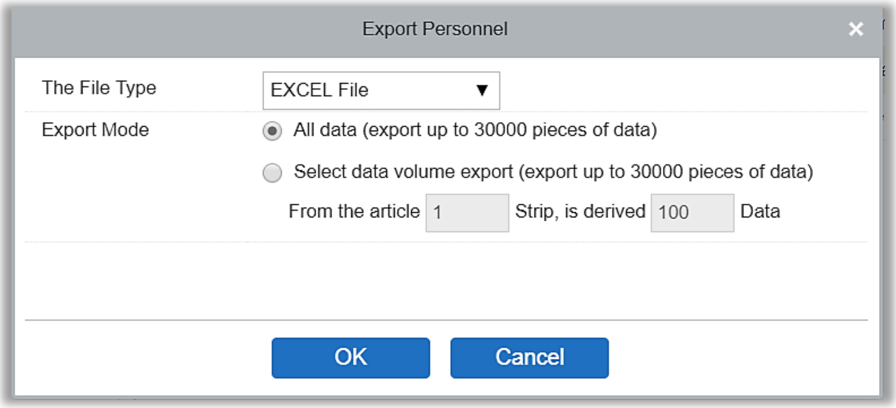
| Statistical Type | Current Total |
|---|---|
| Male | 0 |
| Female | 0 |
| Personnel Quantity | 2 |
| Fingerprint Quantity | 2 |
| Face Quantity | 0 |
| Finger Vein Quantity | 0 |
| Palm Quantity | 2 |
| Number of Cards Held | 0 |
| Face Picture Quantity | 0 |

## ➢ Export

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



1) Select the type of file and Export mode as required.



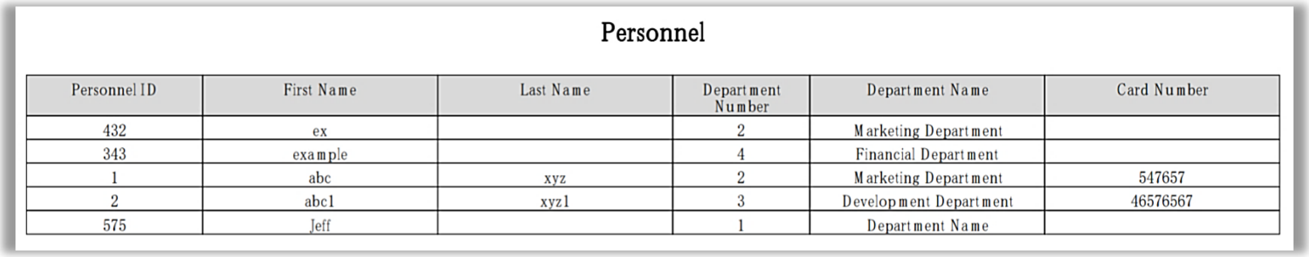
Export Personnel

The File Type: EXCEL File ▼

Export Mode: ● All data (export up to 30000 pieces of data)

○ Select data volume export (export up to 30000 pieces of data)

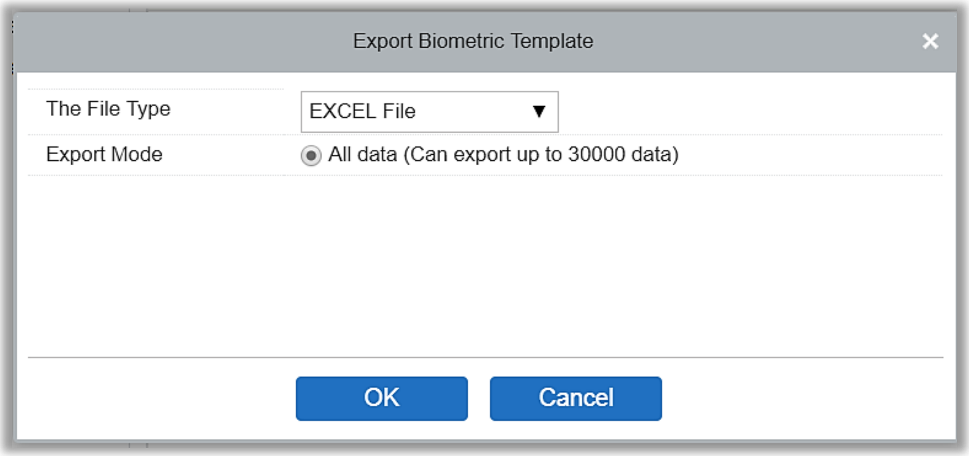
From the article 1 Strip, is derived 100 Data



Personnel

| Personnel ID | First Name | Last Name | Department Number | Department Name | Card Number |
|---|---|---|---|---|---|
| 432 | ex | | 2 | Marketing Department | |
| 343 | example | | 4 | Financial Department | |
| 1 | abc | xyz | 2 | Marketing Department | 547657 |
| 2 | abc1 | xyz1 | 3 | Development Department | 46576567 |
| 575 | Jeff | | 1 | Department Name | |

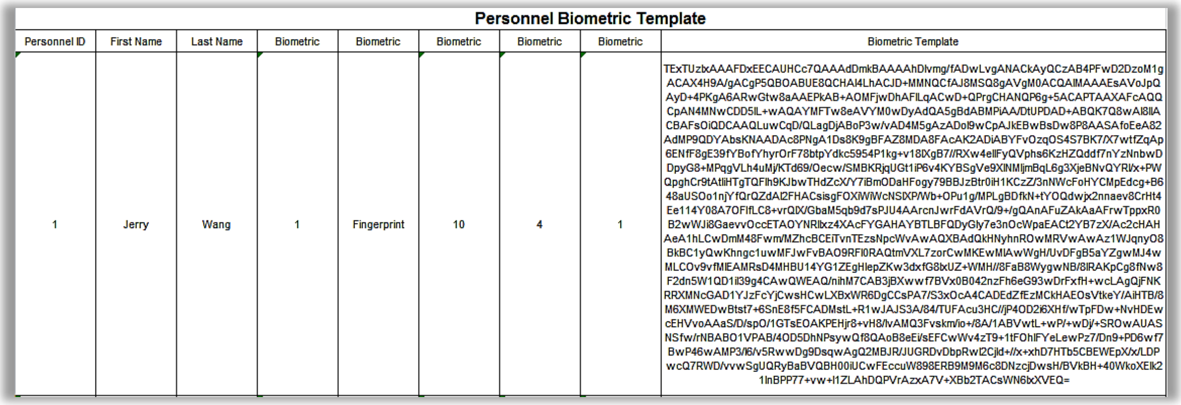
2) Export the Biometric Template.



Export Biometric Template

The File Type: EXCEL File ▼

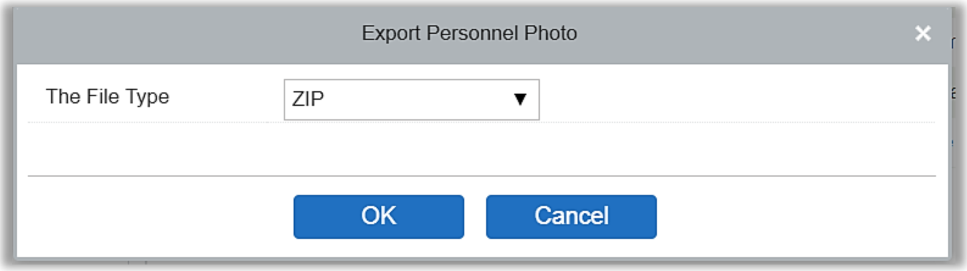
Export Mode: ● All data (Can export up to 30000 data)



Personnel Biometric Template

| Personnel ID | First Name | Last Name | Biometric | Biometric | Biometric | Biometric | Biometric | Biometric Template |
|---|---|---|---|---|---|---|---|---|
| 1 | Jerry | Wang | 1 | Fingerprint | 10 | 4 | 1 | TExTUzlxAAAFDxEECAUHCc7QAAAdDmkBAAAAhDlvmg/fADwLvgANACkAyQCzAB4PFwD2DzoM1gACAX4H9A/gACgP5QBOABUE8QCHAl4LhACJD+MMNQCfAJ8MSQ8gAVgM0ACQAlMAAAEsAVoJpQAyD+4PKgA6ARwGtw8aAAEPkAB+AOMFjwDhAFlLqACwD+QPrgCHANQP6g+5ACAPTAAXAFcAQQCpAN4MNwCDD5lL+wAQAYMFTw8eAVYM0wDyAdQA5gBdABMPiAA/DtUPDAD+ABQK7Q8wAl8lIACBAFsOiQDCAAQLuwCqD/QLagDjABoP3w/vAD4M5gAzADol9wCpAJkEBwBsDw8P8AASAfoEeA82AdMP9QDYAbsKNAADAc8PNgA1Ds8K9gBFAZ8MDA8FAcAK2ADiABYFvOzqOS4S7BK7/X7wtfZqAp6ENfF8gE39fYBofYhyrOrF78btpYdkc5954P1kg+v18lXgB7//RXw4ellFyQVphs6KzHZQddf7nYzNnbwDDpyG8+MPqgVLh4uMj/KTd69/Oecw/SMBKRjqUGt1iP6v4KYBSgVe9XlNMljmBqL6g3XjeBNvQYRl/x+PWQpghCr9tAtliHTgTQFlh9KJbwTHdZcX/Y7iBmODaHFogy79BBJzBtr0iH1KCzZ/3nNWcFoHYCMpEdcg+B648aUSOo1njYfQrQZdAl2FHACsisgFOXiWiWcNSlXP/Wb+OPu1g/MPLgBDfkN+tYOQdwjx2nnaev8CrHt4Ee114Y08A7OFlfLC8+vrQlX/GbaM5qb9d7sPJU4AArcnJwrFdAVrQ/9+/gQAnAFuZAkAaAFrwTppxR0B2wWJi8GaevvOccETAOYNRlbxz4XAcFYGAHAYBTLBFQDyGly7e3nOcWpaEACt2YB7zX/Ac2cHAHAeA1hLCwDmM48Fwm/MZhcBCEiTvnTEzsNpcWvAwAQXBAdQkHNyhnROwMRVwAwAz1WJqnyO8BkBC1yQwKhngc1uwMFJwFvBAO9RFl0RAQtmVXL7zorCwMKEwMlAwWgH/UvDFgB5aYZgwMJ4wMLCOv9vfMlEAMRsD4MHBU14YG1ZEgHlepZKw3dxfG8lxUZ+WMH//8FaB8WygwNB/8lRAKpCg8fNw8F2dn5W1QD1il39g4CAwQWEAQ/nihM7CAB3jBXwwf7BVx0B042nzFh6eG93wDrFxfH+wcLAgQjFNKRRXMNcGAD1YJzFcYjCwsHCwLXBxWR6DgCCsPA7/S3xOcA4CADEdZfEzMCkHAEOsVtkeY/AiHTB/8M6XMWEDwBtst7+6SnE8f5FCADMstL+R1wJAJS3A/84/TUFAcu3HC//jP4OD2i6XHf/wTpFDw+NvHDEwcEHVvoAAaS/D/spO/1GTsEOAKPEHjr8+vH8/lvAMQ3Fvskm/io+/8A/1ABVwtL+wP/+wDj/+SROwAUASNSfw/rNBABO1VPAB/4OD5DhNPsywQf8QAoB8eEi/sEFCwWv4zT9+1tFOhlFYeLewPz7/Dn9+PD6wf7BwP46wAMP3/l6/v5RwwDg9DsqwAgQ2MBJR/JUGRDvDbpRwl2Cjld+//x+xhD7HTb5CBEWEpX/x/LDPwcQ7RWD/vvwSgUQRyBaBVQBH00iUCwFEccuW898ERB9M9M6c8DNzcjDwsH/BVkBH+40WkoXElk21lnBPP77+vw+l1ZLAhDQPVrAzxA7V+XBb2TACsWN6lxXVEQ= |

3) Export Personnel Photo.

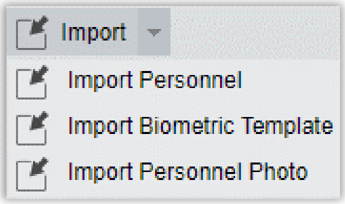


Export Personnel Photo

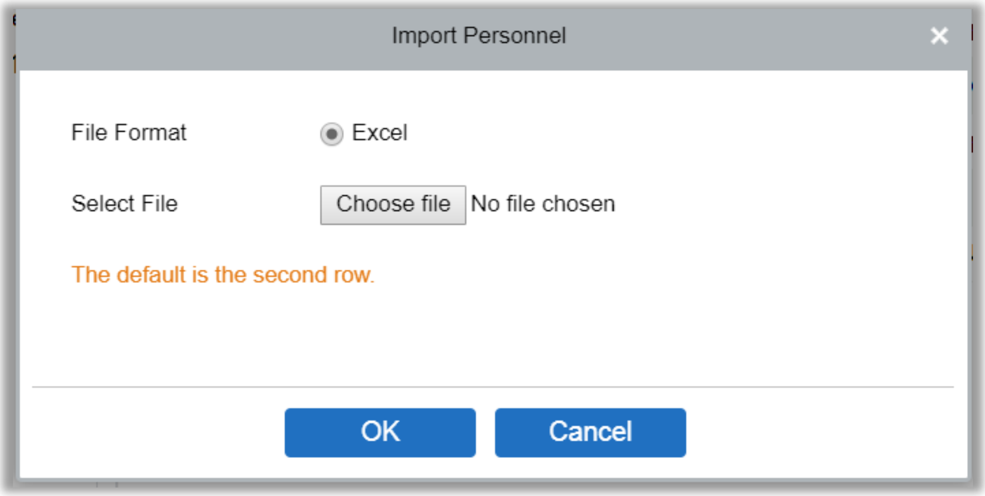
The File Type: ZIP ▼

➢ 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.

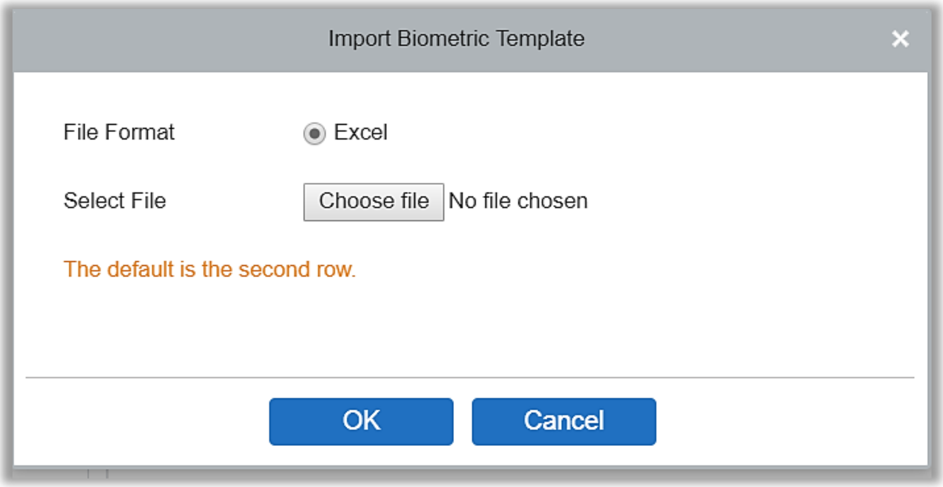

Import Personnel

File Format ● Excel

Select File Choose file No file chosen

The default is the second row.

2) Import Biometric Template.

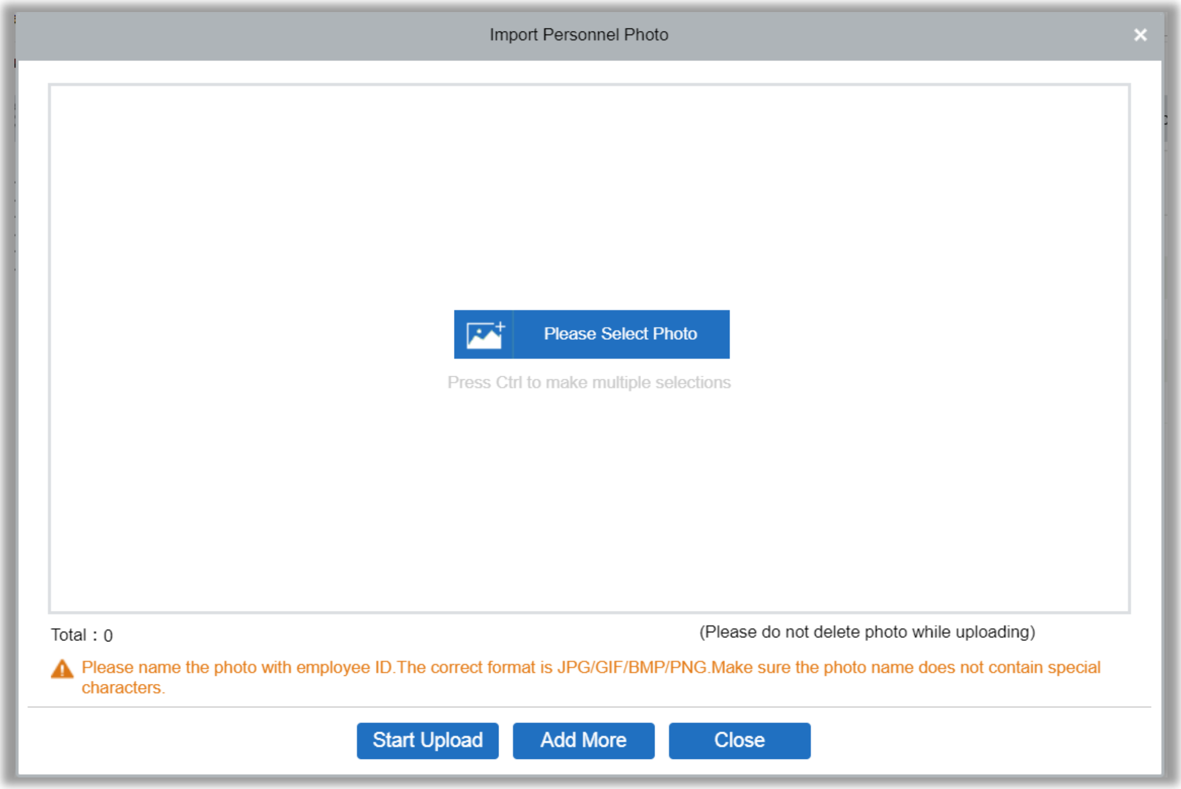

Import Biometric Template

File Format ● Excel

Select File Choose file No file chosen

The default is the second row.

3) Import Personnel Photo: The personnel photo needs to be named by personnel ID, supporting common picture formats, such as jpg, jpeg, png, gif, etc.



Total : 0

(Please do not delete photo while uploading)

Please name the photo with employee ID.The correct format is JPG/GIF/BMP/PNG.Make sure the photo name does not contain special characters.

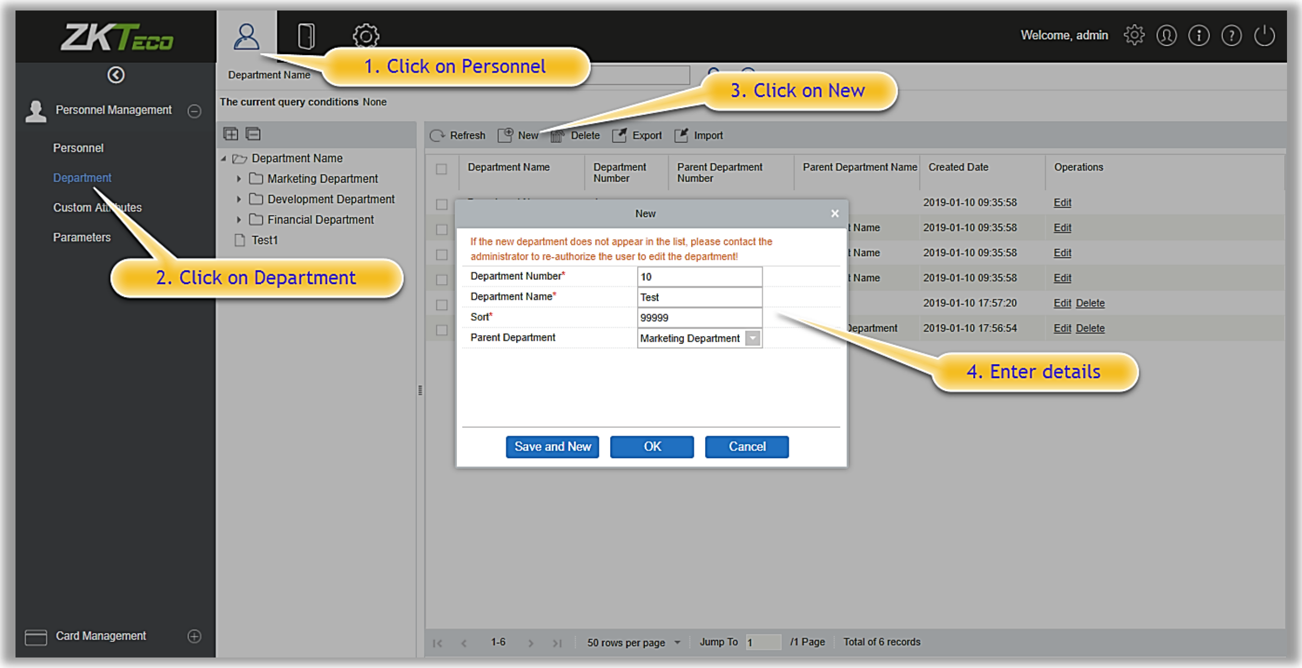
### 3.1.2 Department

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 Management] > [Department] > [**New**]:



New

If the new department does not appear in the list, please contact the administrator to re-authorize the user to edit the department!

| | |
|---|---|
| Department Number* | 10 |
| Department Name* | Test |
| Sort* | 99999 |
| Parent Department | Marketing Department |

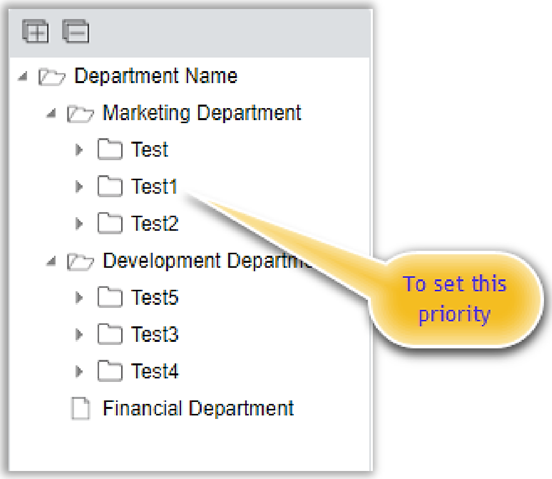
Save and New · OK · Cancel

Fields are as followed:

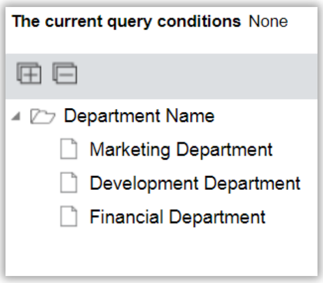
Department Number: Letters and numbers are available. It cannot be identical to the number of another department. The number shall not exceed 30 digits.

Department Name: Combination of characters up to 100. In case of different levels, the department names can be repeated.

Sort: It is used to set the priority (level) of a department within a parent department. The smaller the number of department sort is, the higher ranks such department have. You can set any number from 1 to 999999.



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.



**The current query conditions** None

- Department Name
  - Marketing Department
  - Development Department
  - Financial Department

2. After filling the details, you can click [OK] to complete adding; or click [Cancel] to cancel it, or click [Save and new] to save and continue adding new department.

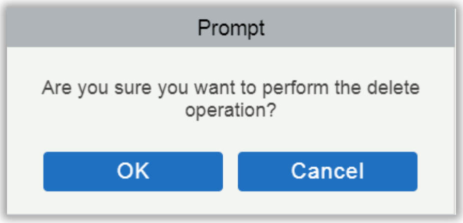
To add a department, you can also choose [Import] to import department information from other software or other documents into this system. For details, see Common Operations.

### ➢ Edit a Department

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

### ➢ Delete a Department

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



Prompt

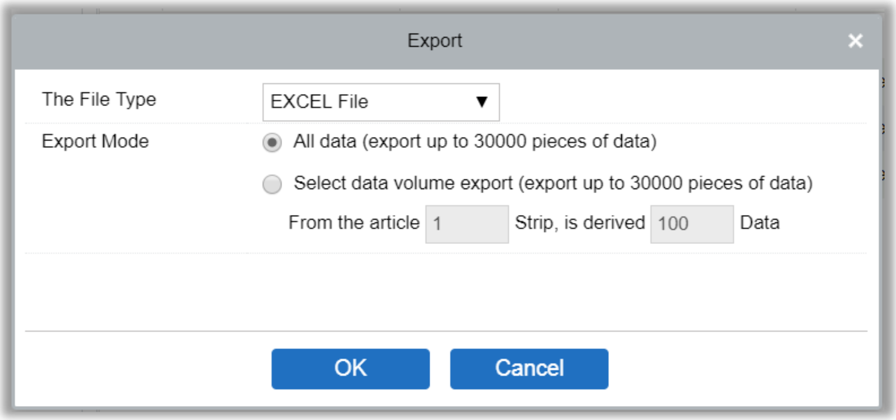
Are you sure you want to perform the delete operation?

2. Click [OK] to delete.

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

### ➢ Export

a) It can be exported in EXCEL, PDF, CSV file format.



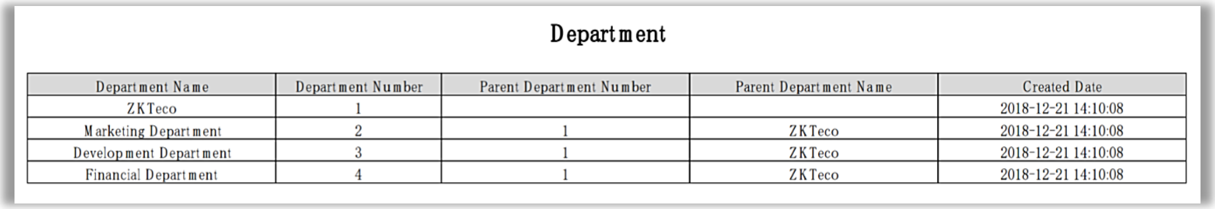
Export

The File Type: EXCEL File ▼

Export Mode: ● All data (export up to 30000 pieces of data)

○ Select data volume export (export up to 30000 pieces of data)

From the article 1 Strip, is derived 100 Data

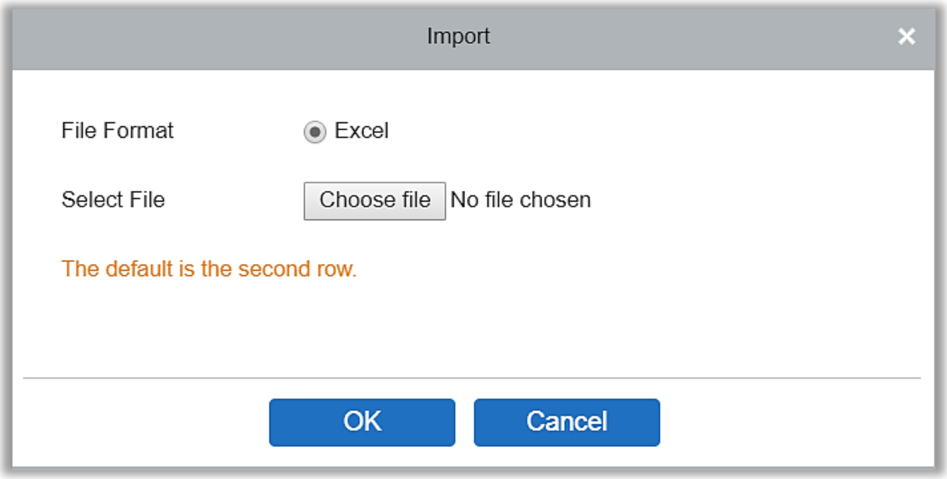


Department

| Department Name | Department Number | Parent Department Number | Parent Department Name | Created Date |
|---|---|---|---|---|
| ZKTeco | 1 | | | 2018-12-21 14:10:08 |
| Marketing Department | 2 | 1 | ZKTeco | 2018-12-21 14:10:08 |
| Development Department | 3 | 1 | ZKTeco | 2018-12-21 14:10:08 |
| Financial Department | 4 | 1 | ZKTeco | 2018-12-21 14:10:08 |

- Import

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



File Format ● Excel

Select File Choose file No file chosen

The default is the second row.

2) Import department information: can import EXCEL, CSV format files.

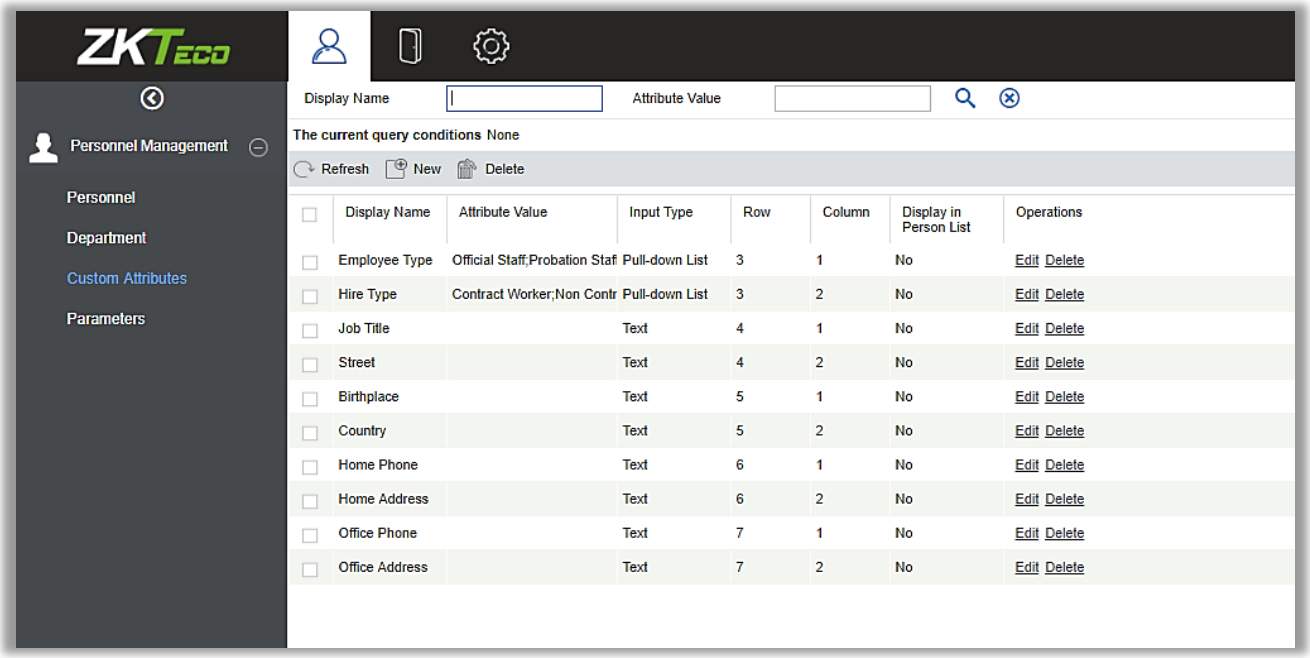
3) After importing the file, the system will match the imported report field and the data segment field automatically.

### 3.1.3 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

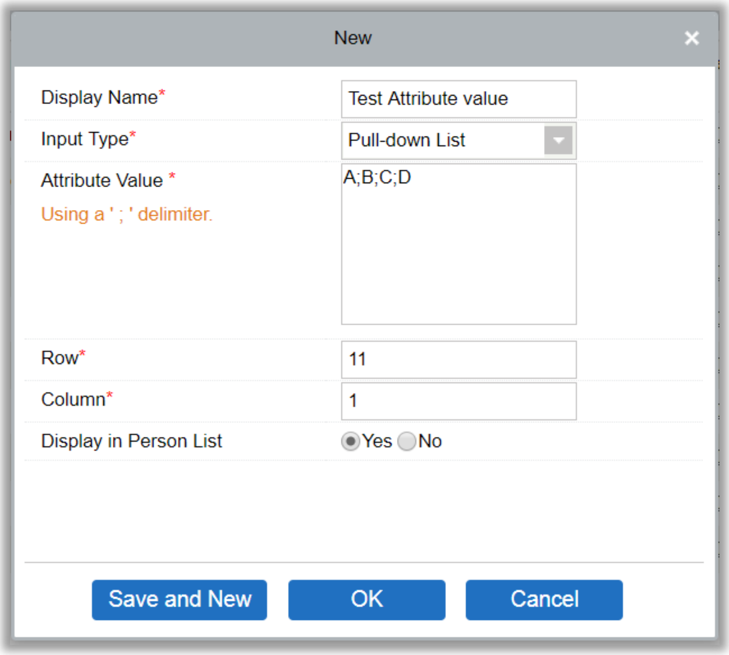
Click [Personnel] > [Personnel Management] > [Custom Attributes] > [New], then edit the parameters and click [OK] to save and exit.



Display Name | Attribute Value

The current query conditions None

| □ | Display Name | Attribute Value | Input Type | Row | Column | Display in Person List | Operations |
|---|---|---|---|---|---|---|---|
| □ | Employee Type | Official Staff;Probation Staf | Pull-down List | 3 | 1 | No | Edit Delete |
| □ | Hire Type | Contract Worker;Non Contr | Pull-down List | 3 | 2 | No | Edit Delete |
| □ | Job Title | | Text | 4 | 1 | No | Edit Delete |
| □ | Street | | Text | 4 | 2 | No | Edit Delete |
| □ | Birthplace | | Text | 5 | 1 | No | Edit Delete |
| □ | Country | | Text | 5 | 2 | No | Edit Delete |
| □ | Home Phone | | Text | 6 | 1 | No | Edit Delete |
| □ | Home Address | | Text | 6 | 2 | No | Edit Delete |
| □ | Office Phone | | Text | 7 | 1 | No | Edit Delete |
| □ | Office Address | | Text | 7 | 2 | No | Edit Delete |



Display Name*: Test Attribute value

Input Type*: Pull-down List

Attribute Value *: A;B;C;D

Using a ' ; ' delimiter.

Row*: 11

Column*: 1

Display in Person List: ● Yes ○ No

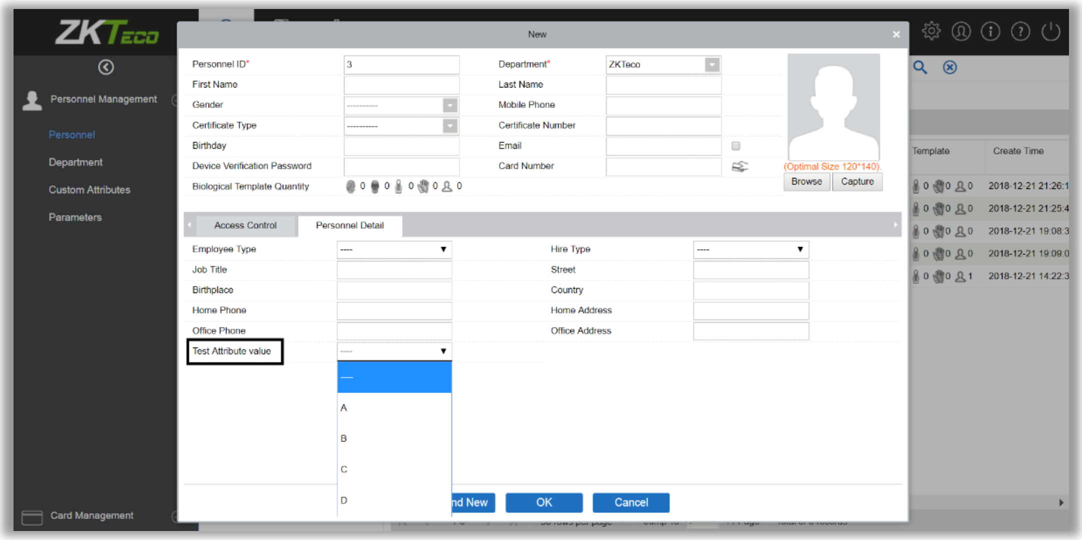
## Fields are as follows:

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 can be either 1 or 2, and the row number can only be 3 to 20. 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.



Personnel ID*: 3

First Name:

Gender: ----------

Certificate Type: ----------

Birthday:

Device Verification Password:

Biological Template Quantity: 0 0 0 0 0

Department*: ZKTeco

Last Name:

Mobile Phone:

Certificate Number:

Email:

Card Number:

### ➢ Editing a Custom Attribute

Click [Edit] to modify the corresponding attributes.

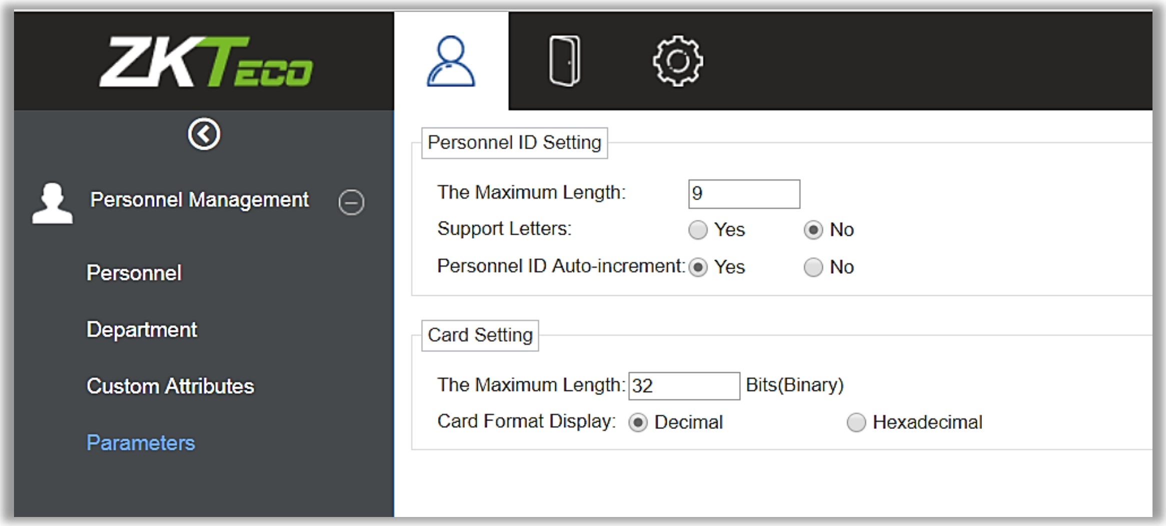
### ➢ Deleting a Custom Attribute

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.

## 3.1.4 Parameters

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



Personnel ID Setting

The Maximum Length: 9

Support Letters: ○ Yes ● No

Personnel ID Auto-increment: ● Yes ○ No

Card Setting

The Maximum Length: 32 Bits(Binary)

Card Format Display: ● Decimal ○ Hexadecimal

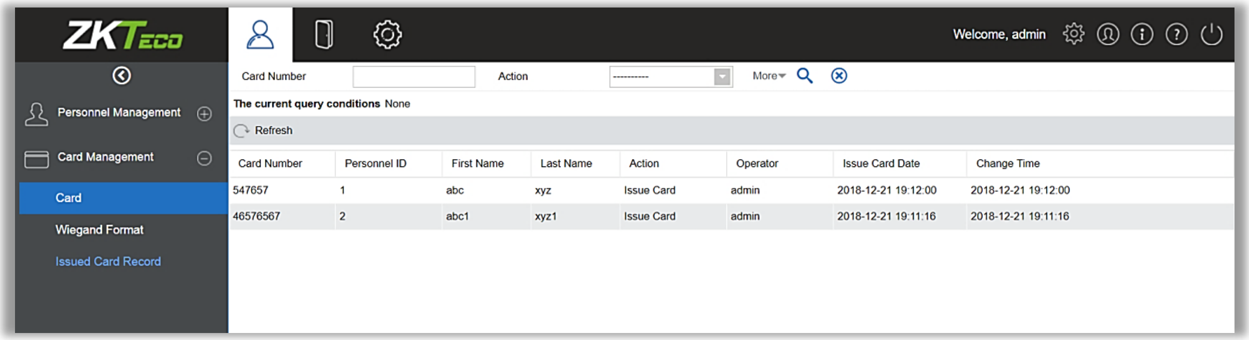
2. You can set the maximum length for a Personnel ID and whether it will support letters or not. If Personnel ID Auto increment is selected as Yes, then while adding personnel, the ID in field automatically updates to the next succeeding new number.
3. Set the maximum length (binary number) of the card number that the current system will support.
4. Set the card format currently used in the system. The card format cannot be switched once it is set up.
5. Click [OK] to save the settings and exit.

## 3.2 Card Management

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

### 3.2.1 Card

It shows the cards issued in the system with their status.

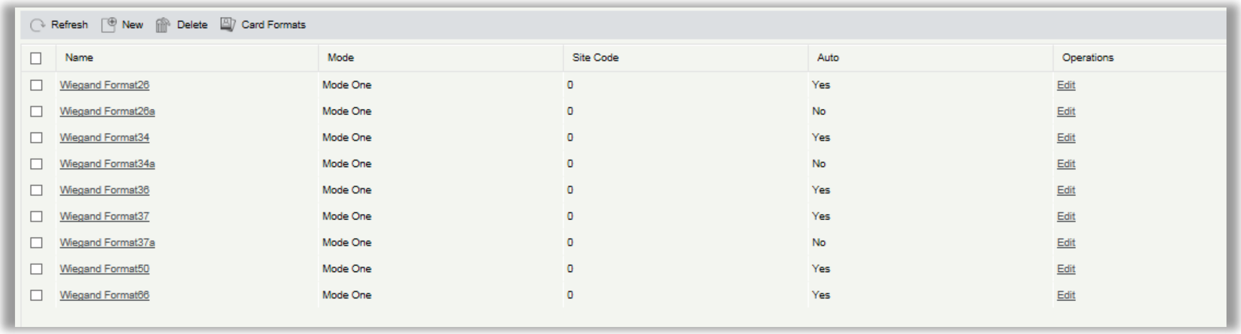


The current query conditions None

| Card Number | Personnel ID | First Name | Last Name | Action | Operator | Issue Card Date | Change Time |
|---|---|---|---|---|---|---|---|
| 547657 | 1 | abc | xyz | Issue Card | admin | 2018-12-21 19:12:00 | 2018-12-21 19:12:00 |
| 46576567 | 2 | abc1 | xyz1 | Issue Card | admin | 2018-12-21 19:11:16 | 2018-12-21 19:11:16 |

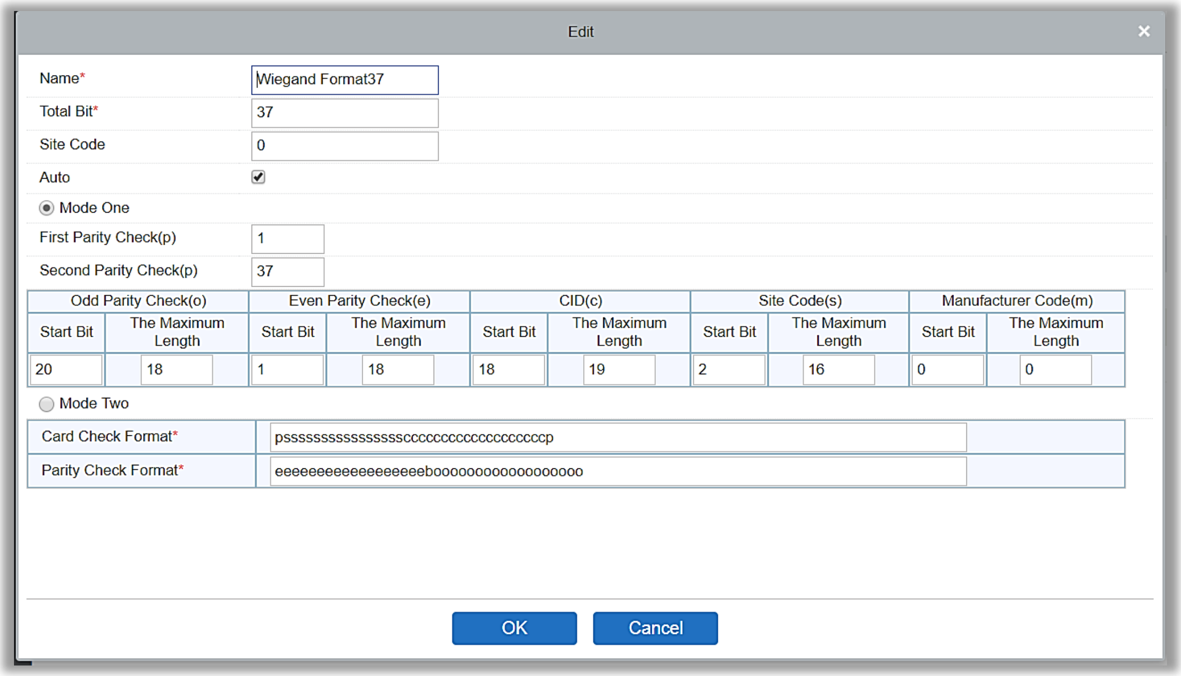
### 3.2.2 Wiegand Format

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 Format26 | Mode One | 0 | Yes | Edit |
| □ | Wiegand Format26a | Mode One | 0 | No | Edit |
| □ | Wiegand Format34 | Mode One | 0 | Yes | Edit |
| □ | Wiegand Format34a | Mode One | 0 | No | Edit |
| □ | Wiegand Format36 | Mode One | 0 | Yes | Edit |
| □ | Wiegand Format37 | Mode One | 0 | Yes | Edit |
| □ | Wiegand Format37a | Mode One | 0 | No | Edit |
| □ | Wiegand Format50 | Mode One | 0 | Yes | Edit |
| □ | Wiegand Format66 | Mode One | 0 | Yes | Edit |

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



Edit

Name*: Wiegand Format37

Total Bit*: 37

Site Code: 0

Auto: ☑

● Mode One

First Parity Check(p): 1

Second Parity Check(p): 37

| Odd Parity Check(o) | | Even Parity Check(e) | | CID(c) | | Site Code(s) | | Manufacturer Code(m) | |
|---|---|---|---|---|---|---|---|---|---|
| Start Bit | The Maximum Length | Start Bit | The Maximum Length | Start Bit | The Maximum Length | Start Bit | The Maximum Length | Start Bit | The Maximum Length |
| 20 | 18 | 1 | 18 | 18 | 19 | 2 | 16 | 0 | 0 |

○ Mode Two

Card Check Format*: psssssssssssssssscccccccccccccccccccp

Parity Check Format*: eeeeeeeeeeeeeeeeeebooooooooooooooooooo

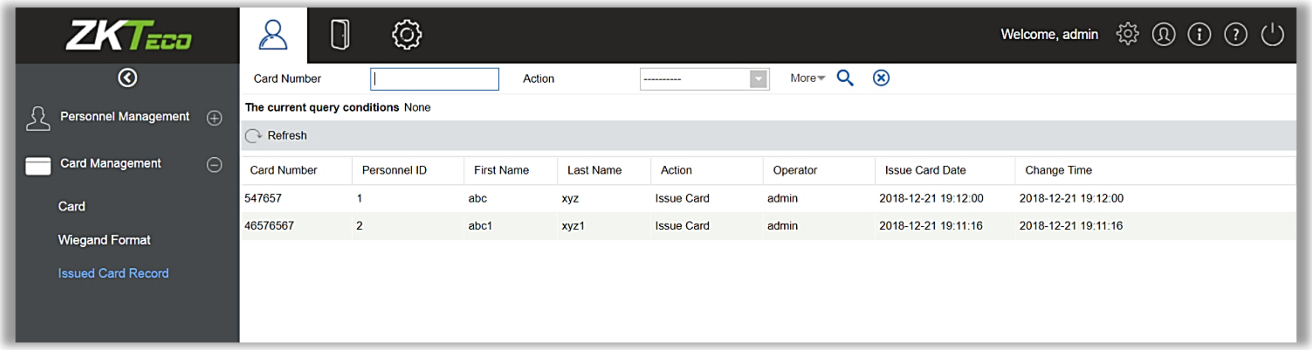
## Format Specifying:

"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 "eeeeeeeeeeeeeeeeee"; the second parity bits check "ooooooooooooooooooo". 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 will display the operations performed on the card.



Card Number: | Action: ----------

The current query conditions None

| Card Number | Personnel ID | First Name | Last Name | Action | Operator | Issue Card Date | Change Time |
|---|---|---|---|---|---|---|---|
| 547657 | 1 | abc | xyz | Issue Card | admin | 2018-12-21 19:12:00 | 2018-12-21 19:12:00 |
| 46576567 | 2 | abc1 | xyz1 | Issue Card | admin | 2018-12-21 19:11:16 | 2018-12-21 19:11:16 |

✍**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.

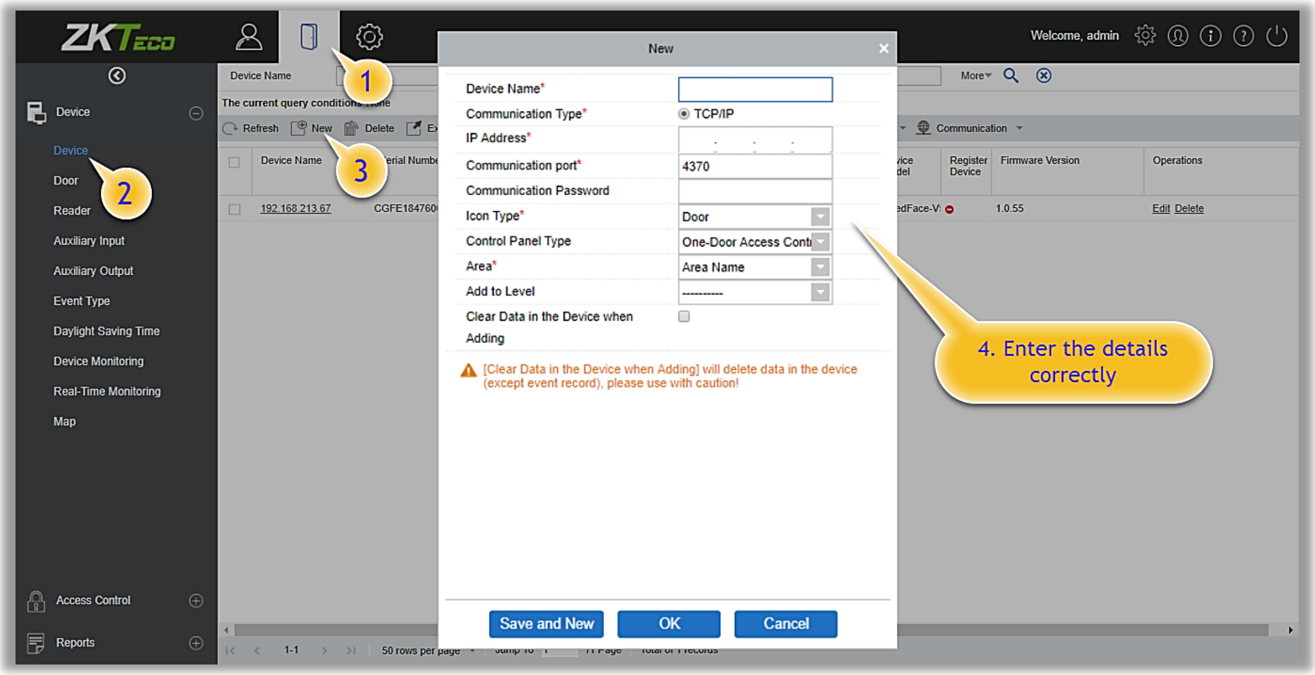
### 4.1.1 Device

- Add Device

There are two ways to add Access Devices.

1. Add Device manually

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



New

Device Name*

Communication Type* ● TCP/IP

IP Address*

Communication port* 4370

Communication Password

Icon Type* Door

Control Panel Type One-Door Access Contr

Area* Area Name

Add to Level ----------

Clear Data in the Device when Adding □

⚠ [Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

Fields are as follows:

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

IP Address: Enter the IP Address of the device.

Communication port: The default value is 4370.

Communication Password: A Password should be a combination of number and letters of 6 digits.

Common options:

✍**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 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 and 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.

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 select it.

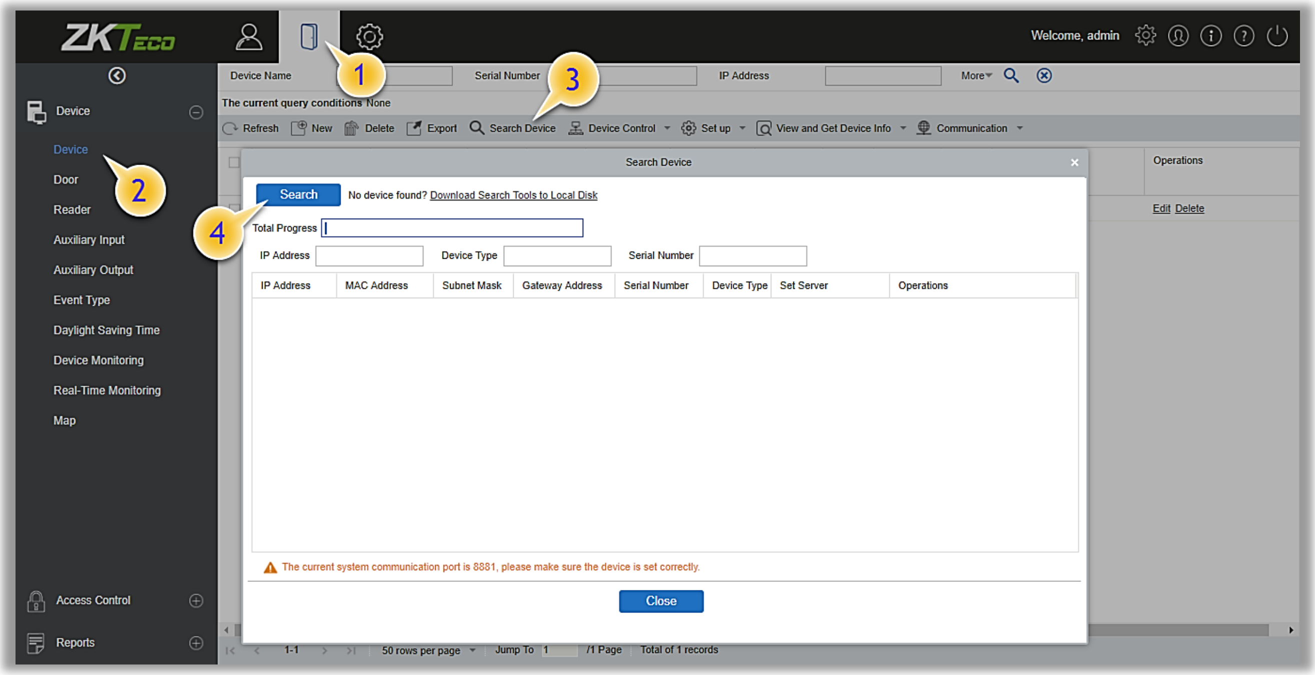
B. After editing, click [OK], and the system will try to connect the current device.

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

✍**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).

2. Add Device by Searching Access Controllers.

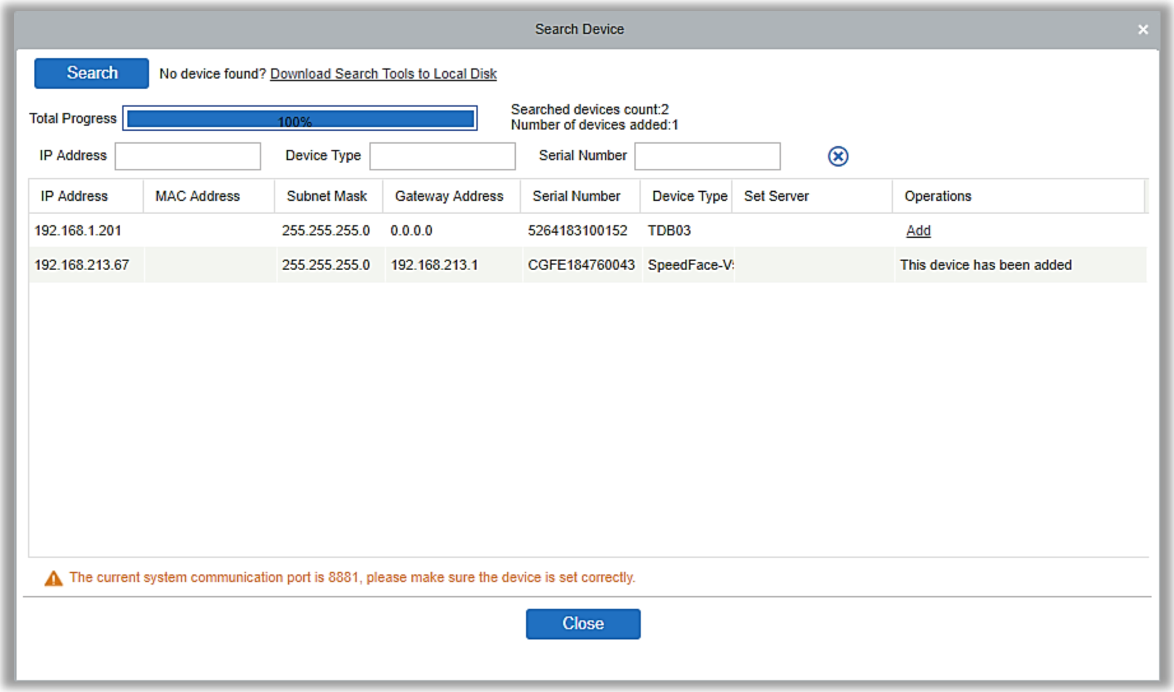
Search the access controllers in the Ethernet.



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

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

(3) After the search is complete, the list and total number of access controllers will be displayed.



No device found? Download Search Tools to Local Disk

Searched devices count:2
Number of devices added:1

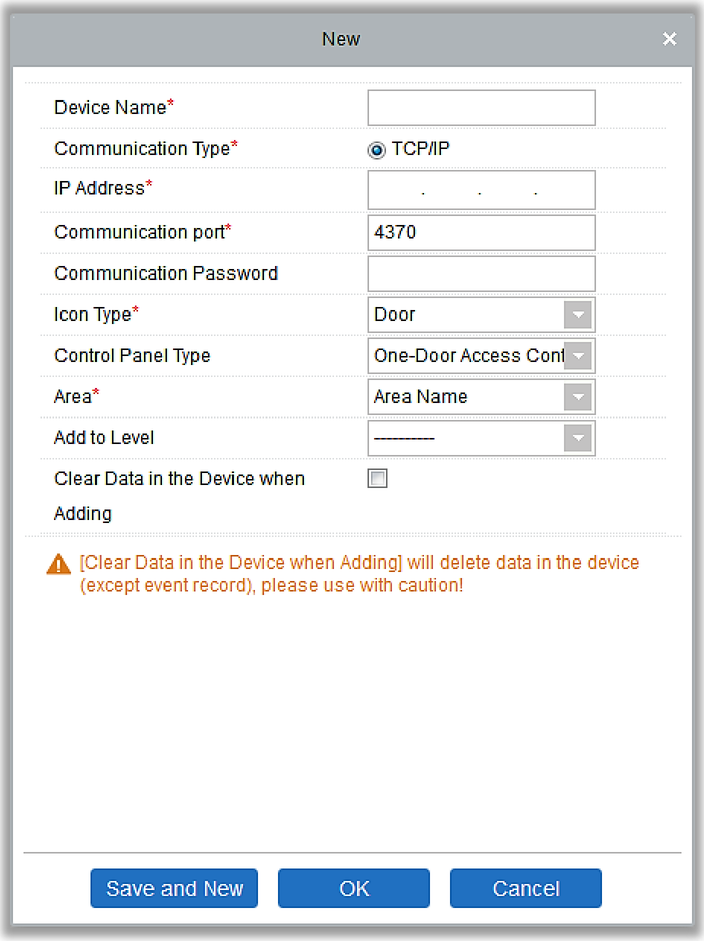
| IP Address | MAC Address | Subnet Mask | Gateway Address | Serial Number | Device Type | Set Server | Operations |
|---|---|---|---|---|---|---|---|
| 192.168.1.201 | | 255.255.255.0 | 0.0.0.0 | 5264183100152 | TDB03 | | Add |
| 192.168.213.67 | | 255.255.255.0 | 192.168.213.1 | CGFE184760043 | SpeedFace-V: | | This device has been added |

The current system communication port is 8881, please make sure the device is set correctly.

✍**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.



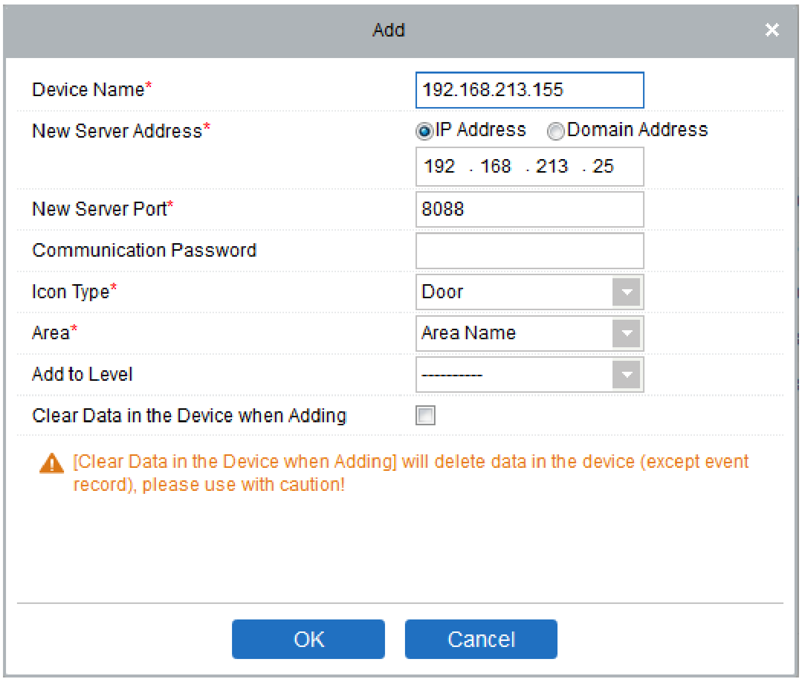
New

| | |
|---|---|
| Device Name* | |
| Communication Type* | ● TCP/IP |
| IP Address* | . . . |
| Communication port* | 4370 |
| Communication Password | |
| Icon Type* | Door |
| Control Panel Type | One-Door Access Cont |
| Area* | Area Name |
| Add to Level | ---------- |
| Clear Data in the Device when Adding | □ |

⚠ [Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

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

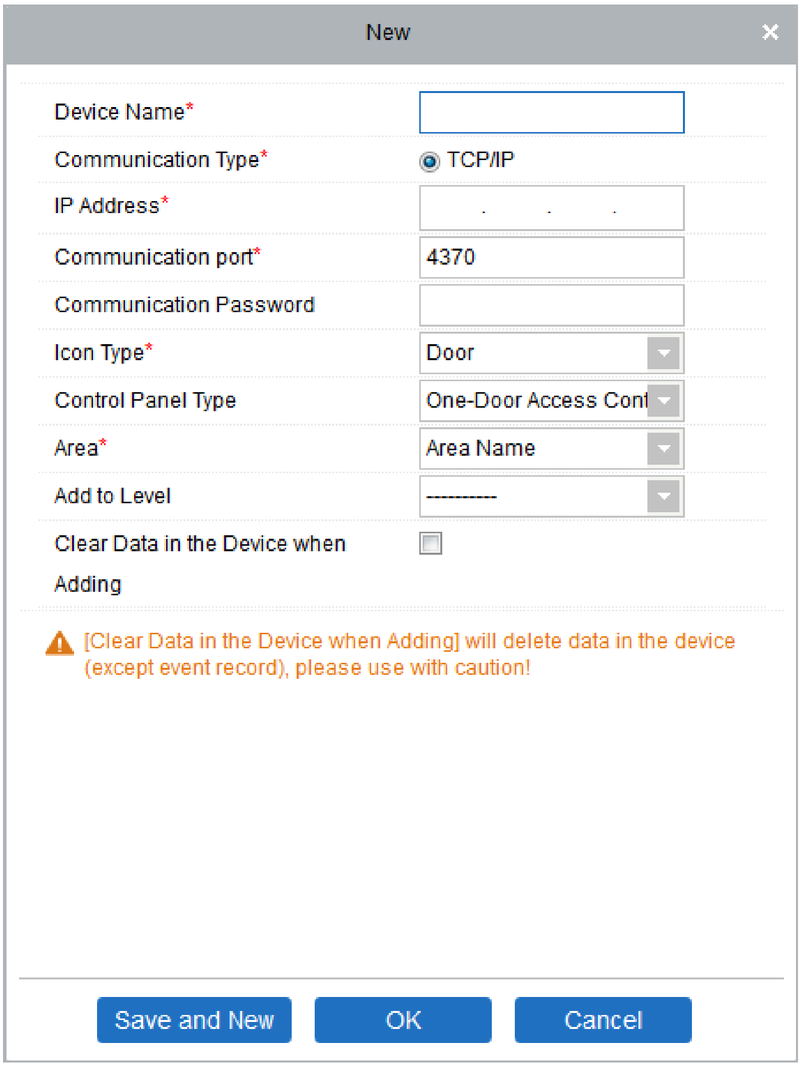
If the device is a push firmware device, the following windows will pop-up after clicking [Add]. If IP Address in [New Server Address] is selected, then configure IP address and port number. If Domain Address in [New Server Address] option is selected, then configure domain address, port number and DNS.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



Add

| | |
|---|---|
| Device Name* | 192.168.213.155 |
| New Server Address* | ● IP Address ○ Domain Address<br>192 . 168 . 213 . 25 |
| New Server Port* | 8088 |
| Communication Password | |
| Icon Type* | Door |
| Area* | Area Name |
| Add to Level | ---------- |
| Clear Data in the Device when Adding | □ |

[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!



New

| | |
|---|---|
| Device Name* | |
| Communication Type* | ● TCP/IP |
| IP Address* | . . . |
| Communication port* | 4370 |
| Communication Password | |
| Icon Type* | Door |
| Control Panel Type | One-Door Access Cont |
| Area* | Area Name |
| Add to Level | ---------- |
| Clear Data in the Device when Adding | □ |

[Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

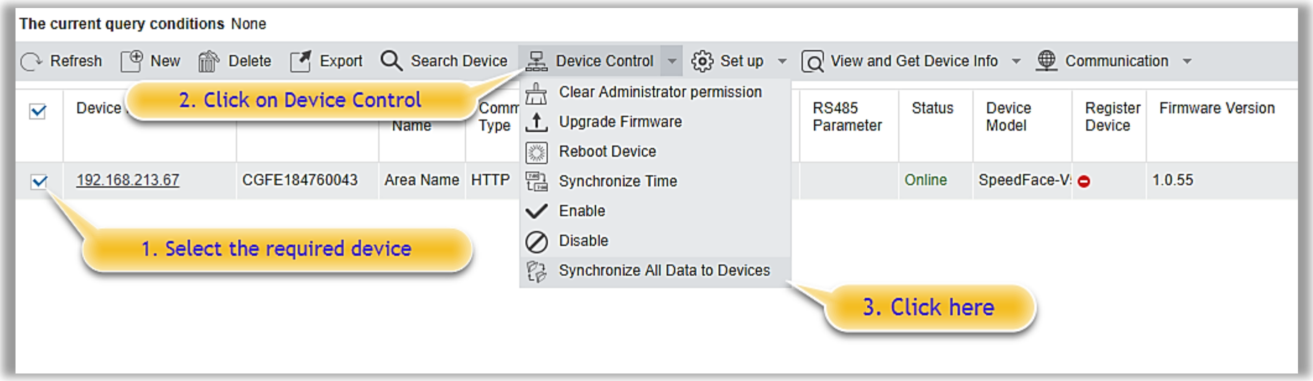
New Server Address: To add a device by IP Address or Domain Address, devices can be added to the software by entering the domain address.

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 select 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.



The current query conditions None

| ☑ | Device | | Name | Comm Type | RS485 Parameter | Status | Device Model | Register Device | Firmware Version |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 192.168.213.67 | CGFE184760043 | Area Name | HTTP | | Online | SpeedFace-V: | ⊖ | 1.0.55 |

1. Select the required device

2. Click on Device Control

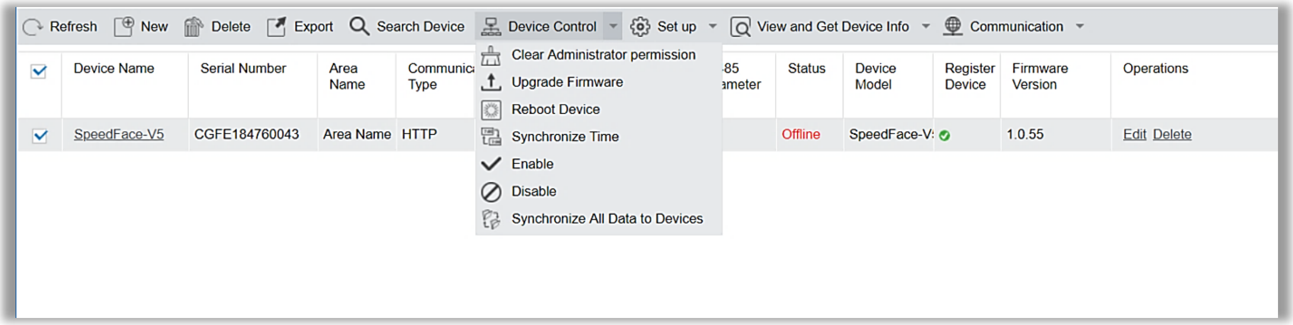
3. Click here

(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).

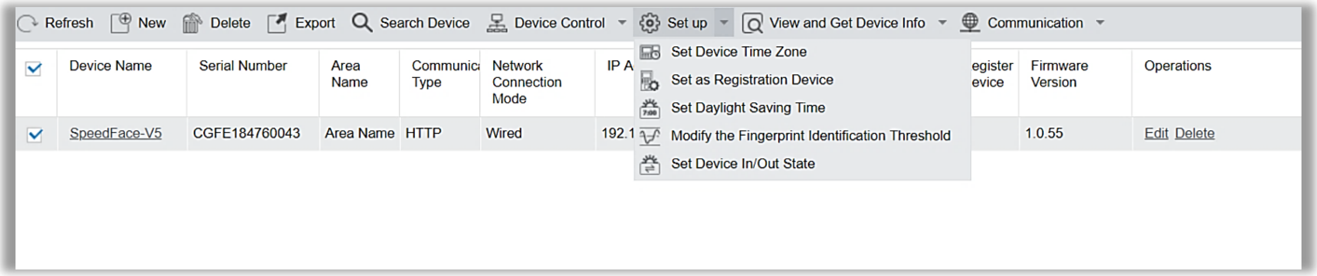
✍**Note:** Some PUSH devices support SSL. To use this function, select the HTTPS port during software installation and ensure that the device firmware supports SSL.

## 4.1.2 Device Operation

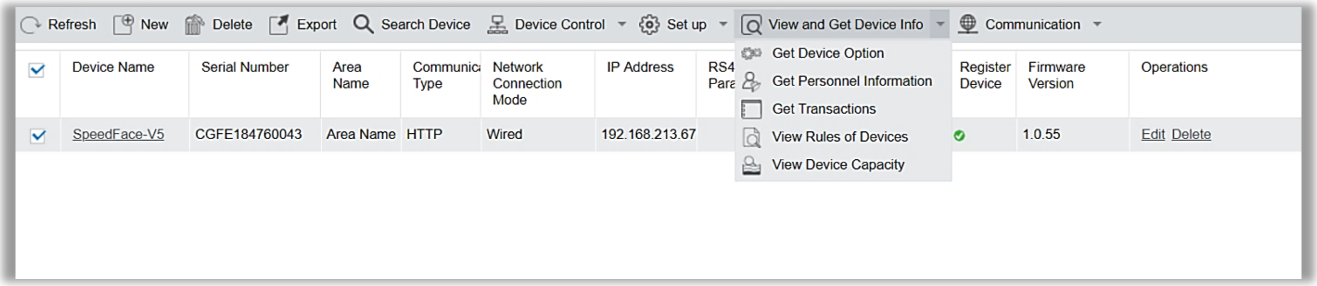
For the communication between the system and device; data uploading, configuration downloading, device and system parameters shall be set. Users can edit access controllers within relevant levels in the current system; users can only add or delete devices in Device Management if needed.



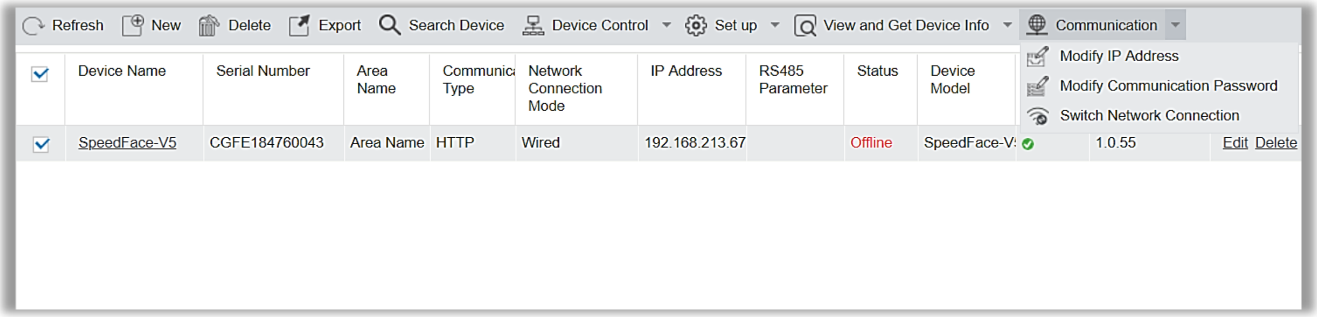
| ☑ | Device Name | Serial Number | Area Name | Communic Type | 85 ameter | Status | Device Model | Register Device | Firmware Version | Operations |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | SpeedFace-V5 | CGFE184760043 | Area Name | HTTP | | Offline | SpeedFace-V: | ✓ | 1.0.55 | Edit Delete |



| ☑ | Device Name | Serial Number | Area Name | Communica Type | Network Connection Mode | IP A | egister evice | Firmware Version | Operations |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | SpeedFace-V5 | CGFE184760043 | Area Name | HTTP | Wired | 192.1 |  | 1.0.55 | Edit Delete |



| ☑ | Device Name | Serial Number | Area Name | Communica Type | Network Connection Mode | IP Address | RS4 Para | Register Device | Firmware Version | Operations |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | SpeedFace-V5 | CGFE184760043 | Area Name | HTTP | Wired | 192.168.213.67 |  | ✓ | 1.0.55 | Edit Delete |

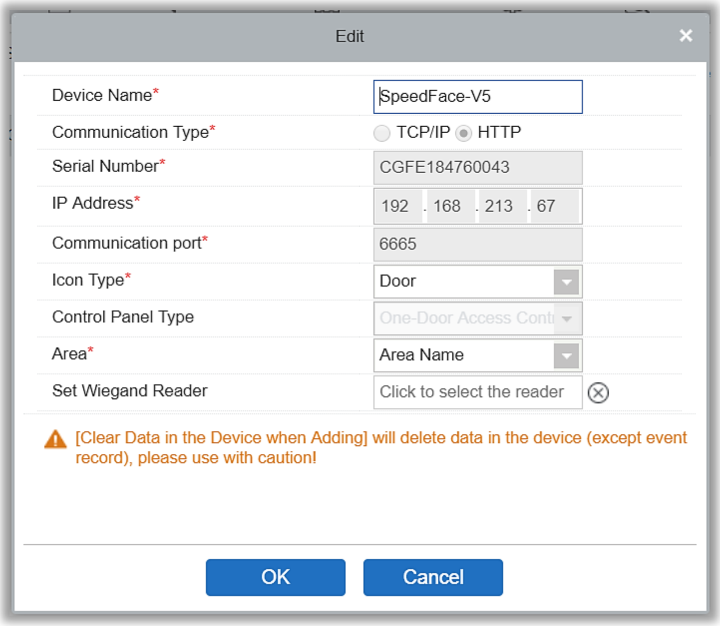


| ☑ | Device Name | Serial Number | Area Name | Communica Type | Network Connection Mode | IP Address | RS485 Parameter | Status | Device Model |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | SpeedFace-V5 | CGFE184760043 | Area Name | HTTP | Wired | 192.168.213.67 |  | Offline | SpeedFace-V: | ✓ | 1.0.55 | Edit Delete |

## ➢ 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.



| | |
|---|---|
| Device Name* | SpeedFace-V5 |
| Communication Type* | ○ TCP/IP ● HTTP |
| Serial Number* | CGFE184760043 |
| IP Address* | 192 . 168 . 213 . 67 |
| Communication port* | 6665 |
| Icon Type* | Door |
| Control Panel Type | One-Door Access Contr |
| Area* | Area Name |
| Set Wiegand Reader | Click to select the reader |

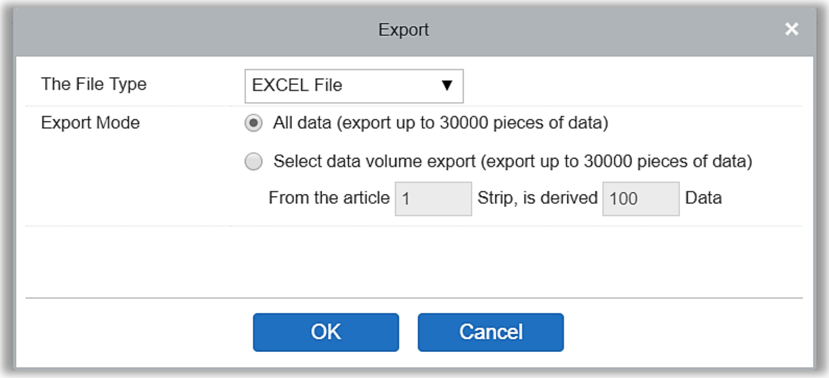
⚠ [Clear Data in the Device when Adding] will delete data in the device (except event record), please use with caution!

For the details and settings of the above parameters, see Device. Some details cannot be edited. The device Name should be unique and must not be identical to another device.

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.

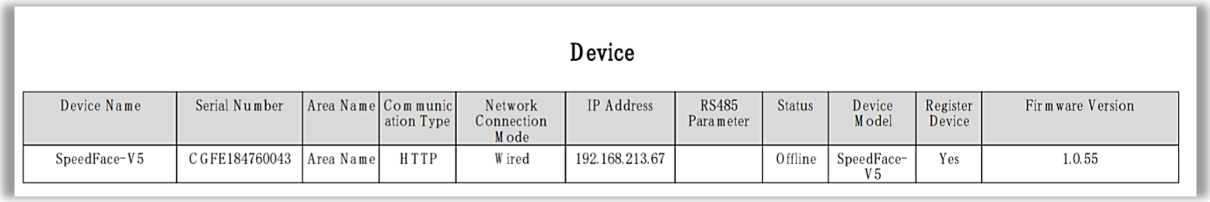


Export ×

The File Type: EXCEL File ▼

Export Mode:
● All data (export up to 30000 pieces of data)
○ Select data volume export (export up to 30000 pieces of data)
From the article 1 Strip, is derived 100 Data

OK Cancel

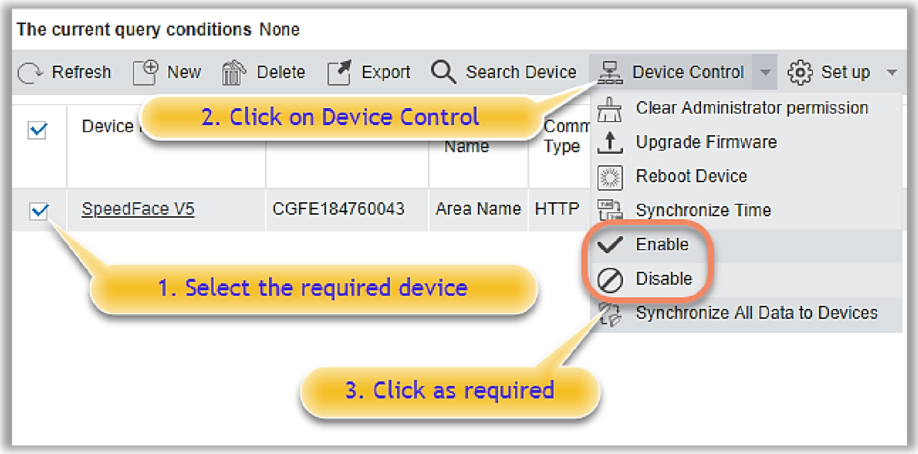


Device

| Device Name | Serial Number | Area Name | Communication Type | Network Connection Mode | IP Address | RS485 Parameter | Status | Device Model | Register Device | Firmware Version |
|---|---|---|---|---|---|---|---|---|---|---|
| SpeedFace-V5 | CGFE184760043 | Area Name | HTTP | Wired | 192.168.213.67 |  | Offline | SpeedFace-V5 | Yes | 1.0.55 |

## ➢ 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.



The current query conditions None

☑ SpeedFace V5 CGFE184760043 Area Name HTTP

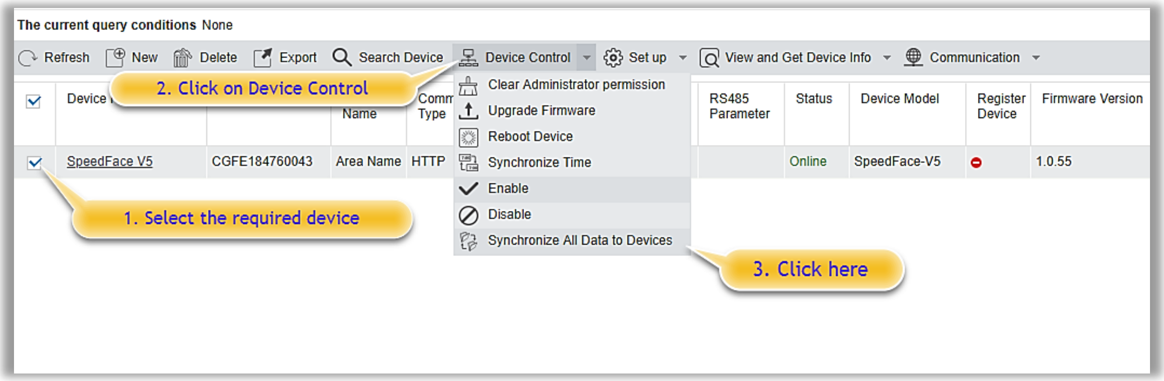
1. Select the required device

2. Click on Device Control

3. Click as required

## ➢ Synchronize All Data to Devices

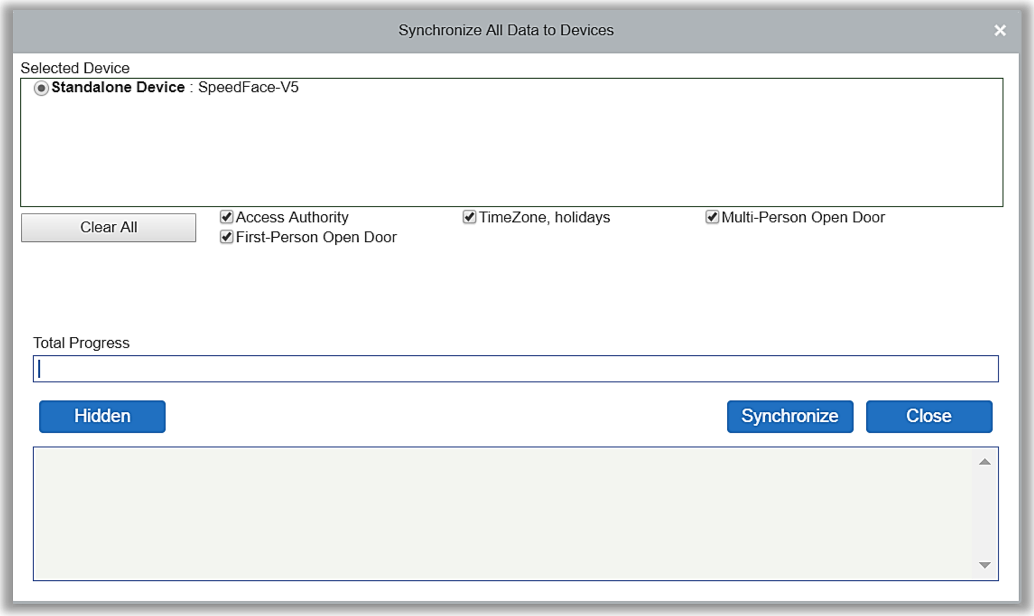
Synchronize data of the system to the device. Select device, click [Synchronize All Data to Devices] and click [OK] to complete synchronization.



1. Select the required device

2. Click on Device Control

3. Click here



Selected Device

● **Standalone Device** : SpeedFace-V5

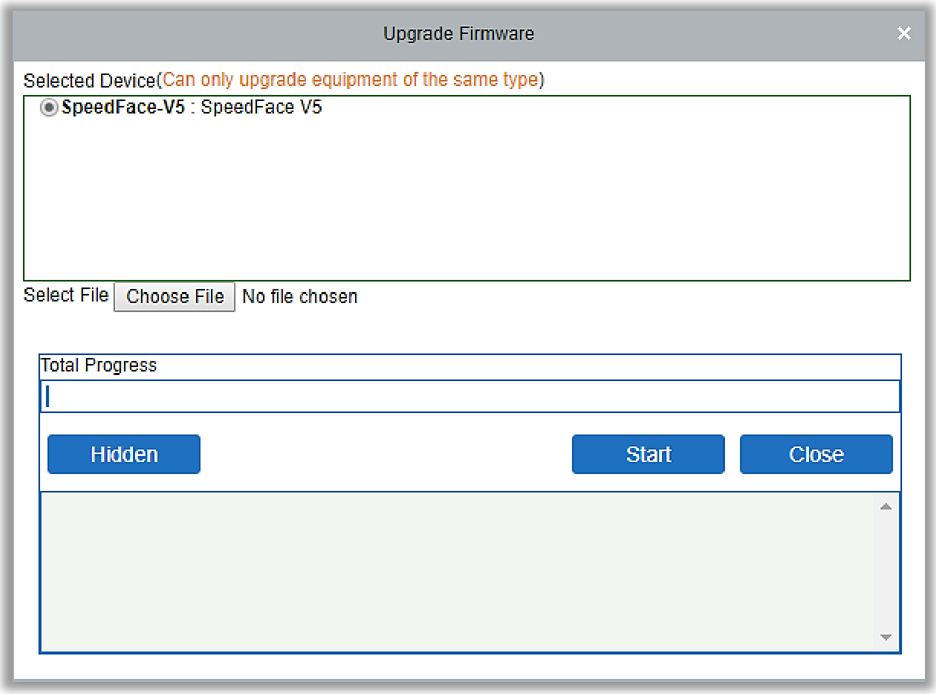
☑ Access Authority ☑ TimeZone, holidays ☑ Multi-Person Open Door

☑ First-Person Open Door

✍**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

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



Upgrade Firmware

Selected Device(Can only upgrade equipment of the same type)

● SpeedFace-V5 : SpeedFace V5

Select File Choose File No file chosen

Total Progress

✍**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.

### ➢ Synchronize Time

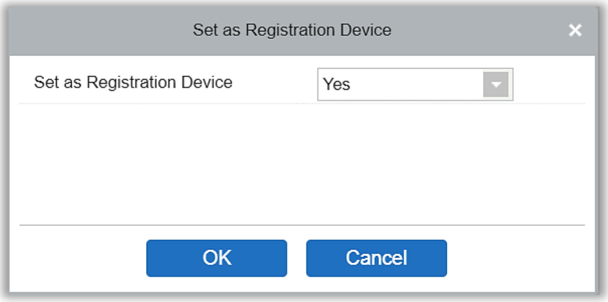
It will synchronize device time with server's current time.

### ➢ 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 as Registration device

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



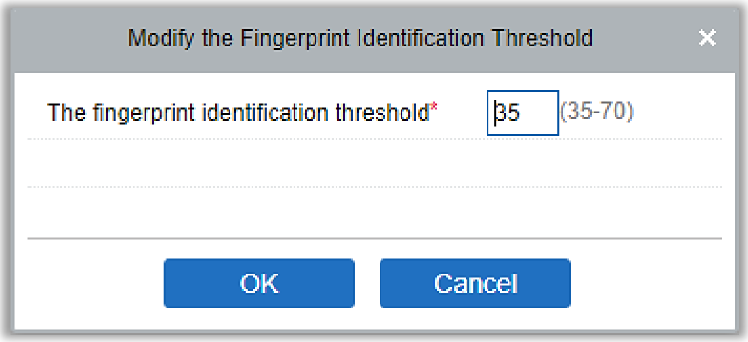
Set as Registration Device

Set as Registration Device: Yes

- ### Set Daylight Saving Time

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

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

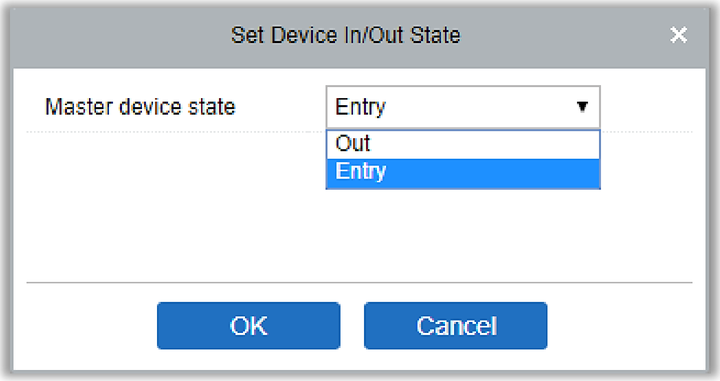


Modify the Fingerprint Identification Threshold

The fingerprint identification threshold* 35 (35-70)

- ### Set Device In/Out state

It will define the condition of the master device as Entry or Exit.



Set Device In/Out State

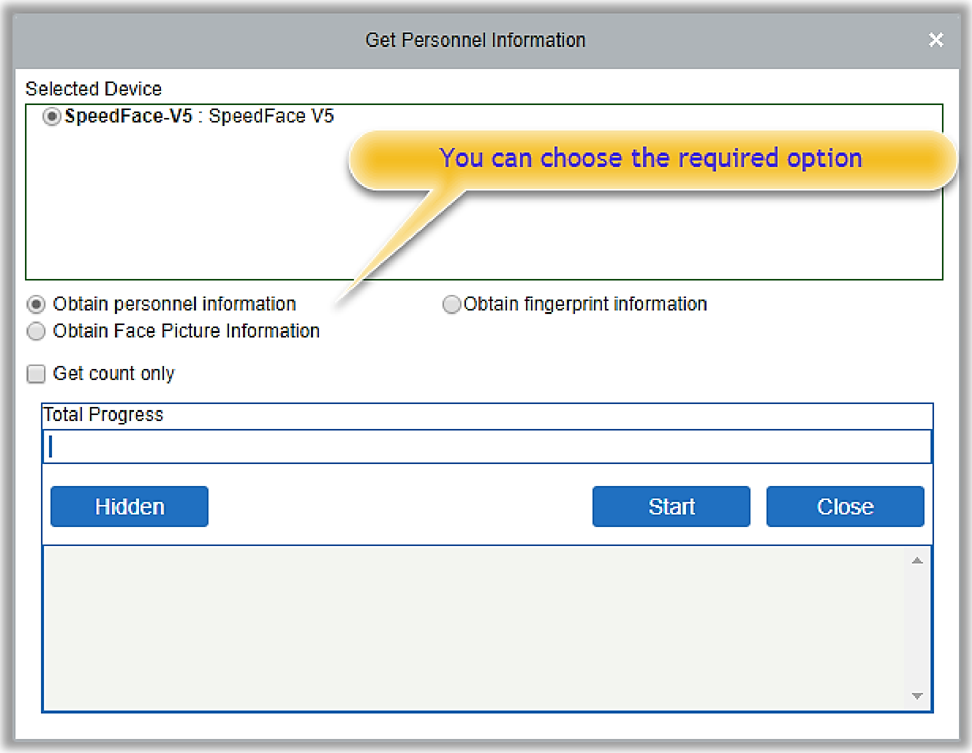
Master device state: Entry

- ### 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.



Selected Device

● **SpeedFace-V5** : SpeedFace V5

You can choose the required option

● Obtain personnel information ○ Obtain fingerprint information

○ Obtain Face Picture Information

□ Get count only

Total Progress

### ➢ 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.

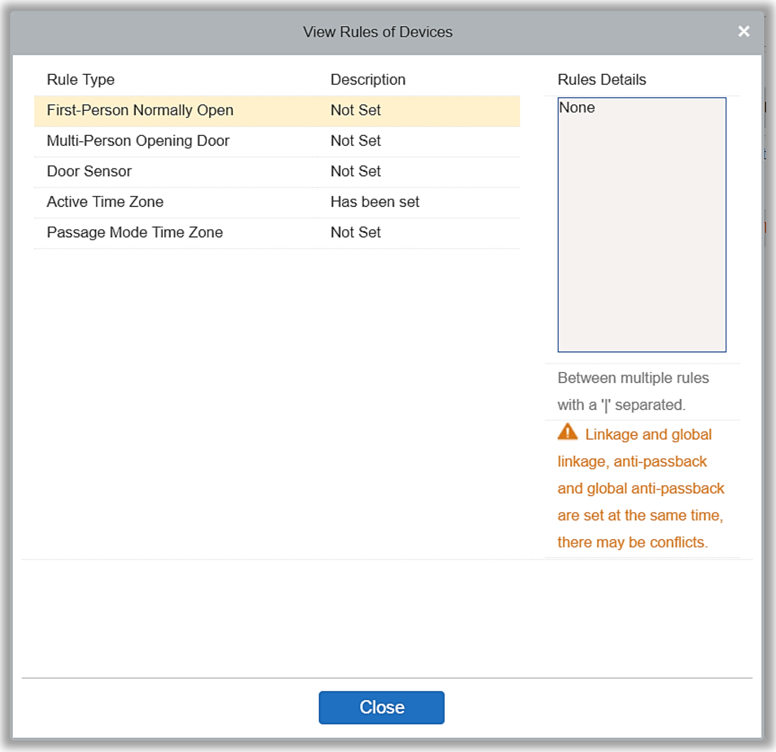
Get All Transactions: The system will get transactions again. Repeated entries will not be shown twice.

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).

### ➢ View Rules of Devices

Shows the Access rules in the device.



View Rules of Devices

| Rule Type | Description |
|---|---|
| First-Person Normally Open | Not Set |
| Multi-Person Opening Door | Not Set |
| Door Sensor | Not Set |
| Active Time Zone | Has been set |
| Passage Mode Time Zone | Not Set |

Rules Details

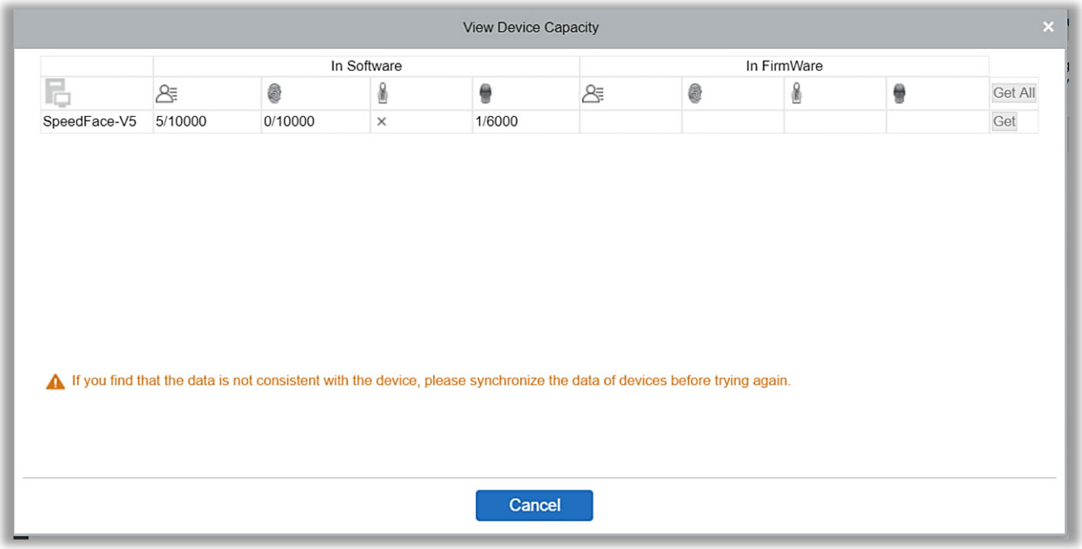
None

Between multiple rules with a '|' separated.

⚠ Linkage and global linkage, anti-passback and global anti-passback are set at the same time, there may be conflicts.

## ➢ View Device Capacity

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



View Device Capacity

|  | In Software |  |  |  | In FirmWare |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  | Get All |
| SpeedFace-V5 | 5/10000 | 0/10000 | × | 1/6000 |  |  |  |  | Get |

⚠ If you find that the data is not consistent with the device, please synchronize the data of devices before trying again.

## ➢ 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

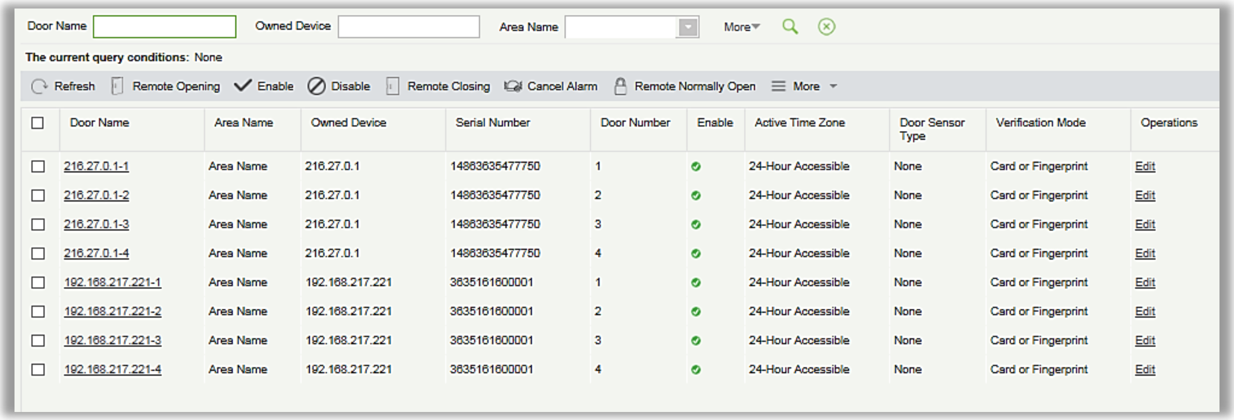
The system will ask for the old communication password before modifying it. After verification, input the new password twice, and click [OK] to modify the communication password.

✍**Note:** A Password should be a combination of number and letters of 6 digits.

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.

## 4.1.3 Doors

1. Click [Access] > [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).

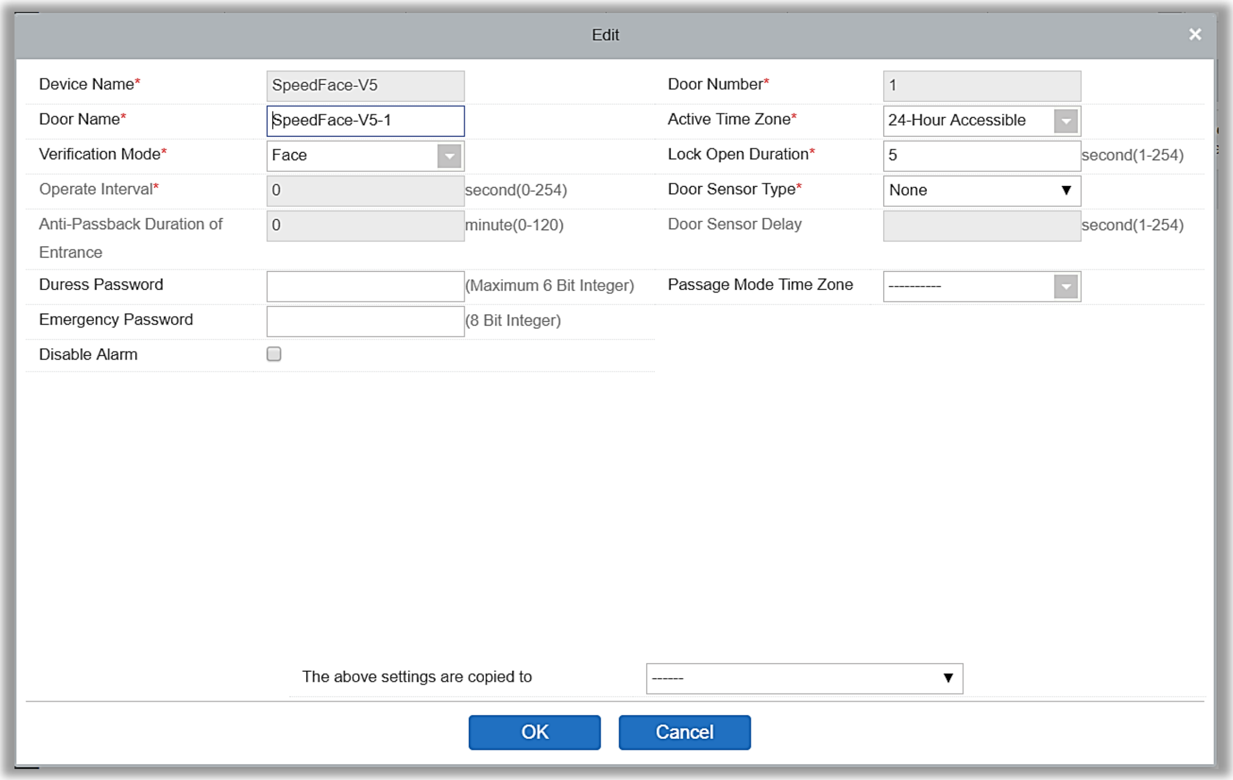


The current query conditions: None

| □ | Door Name | Area Name | Owned Device | Serial Number | Door Number | Enable | Active Time Zone | Door Sensor Type | Verification Mode | Operations |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | 216.27.0.1-1 | Area Name | 216.27.0.1 | 14863635477750 | 1 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 216.27.0.1-2 | Area Name | 216.27.0.1 | 14863635477750 | 2 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 216.27.0.1-3 | Area Name | 216.27.0.1 | 14863635477750 | 3 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 216.27.0.1-4 | Area Name | 216.27.0.1 | 14863635477750 | 4 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 192.168.217.221-1 | Area Name | 192.168.217.221 | 3635161600001 | 1 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 192.168.217.221-2 | Area Name | 192.168.217.221 | 3635161600001 | 2 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 192.168.217.221-3 | Area Name | 192.168.217.221 | 3635161600001 | 3 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |
| □ | 192.168.217.221-4 | Area Name | 192.168.217.221 | 3635161600001 | 4 | ✓ | 24-Hour Accessible | None | Card or Fingerprint | Edit |

### ➢ Modify Door Parameter:

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



| | | | | |
|---|---|---|---|---|
| Device Name* | SpeedFace-V5 | | Door Number* | 1 |
| Door Name* | SpeedFace-V5-1 | | Active Time Zone* | 24-Hour Accessible |
| Verification Mode* | Face | | Lock Open Duration* | 5 second(1-254) |
| Operate Interval* | 0 | second(0-254) | Door Sensor Type* | None |
| Anti-Passback Duration of Entrance | 0 | minute(0-120) | Door Sensor Delay | second(1-254) |
| Duress Password | | (Maximum 6 Bit Integer) | Passage Mode Time Zone | ---------- |
| Emergency Password | | (8 Bit Integer) | | |
| Disable Alarm | □ | | | |

The above settings are copied to ------

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 name can be modified as required. Numbers, letters or a combination of both is allowed up to 30 characters.

Active Time Zone: Active Time Zone must be selected, so that the door can be opened and closed normally. A Passage Mode Time Zone must be set within the Active Time Zone.

✍**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 during 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.

Verification Mode: Identification modes include Automatic Identification, Only fingerprint, Only Pin, Only Password, Pin and Fingerprint, Fingerprint and Password, Pin and Password and Fingerprint, Face, Face and finger, Face and Finger and Password. 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.

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

Operate Interval: It is the time-interval between two verifications. The unit is Seconds (range: 0~254 seconds), and the default value is 0 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), Normally Open, Normally Close. If you have selected as Normally Open or Normally 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 Normally Open or Normally Close, the default door sensor delay is 15 seconds, and the close and reverse state is enabled.

Door Sensor Delay: It is the delayed duration for the 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.

Duress Password, Emergency Password: Duress means any threats, violence, constraints, or other action used to force 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 swipe 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: Select the Disable Alarm check box to disable the alarm voice in real-time monitoring page.

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

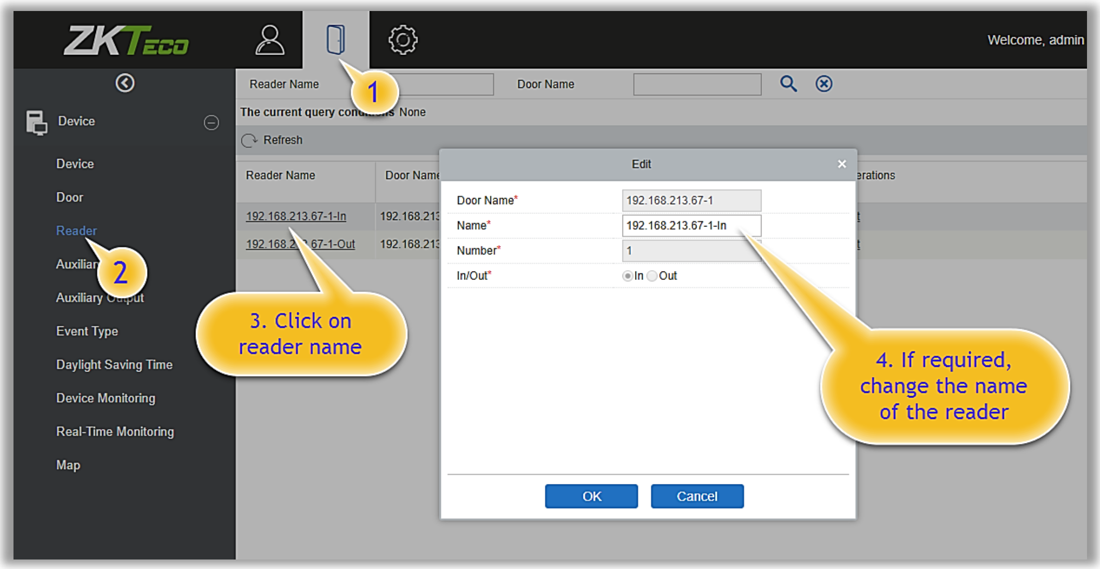
- All doors in current device: Click to apply the above settings to all doors of the current access device.

- All doors in All Control 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 [Device] → [Reader] on the Menu, then click on reader name or [Edit]:



Door Name* 192.168.213.67-1

Name* 192.168.213.67-1-In

Number* 1

In/Out* ● In ○ Out

3. Click on reader name

4. If required, change the name of the reader

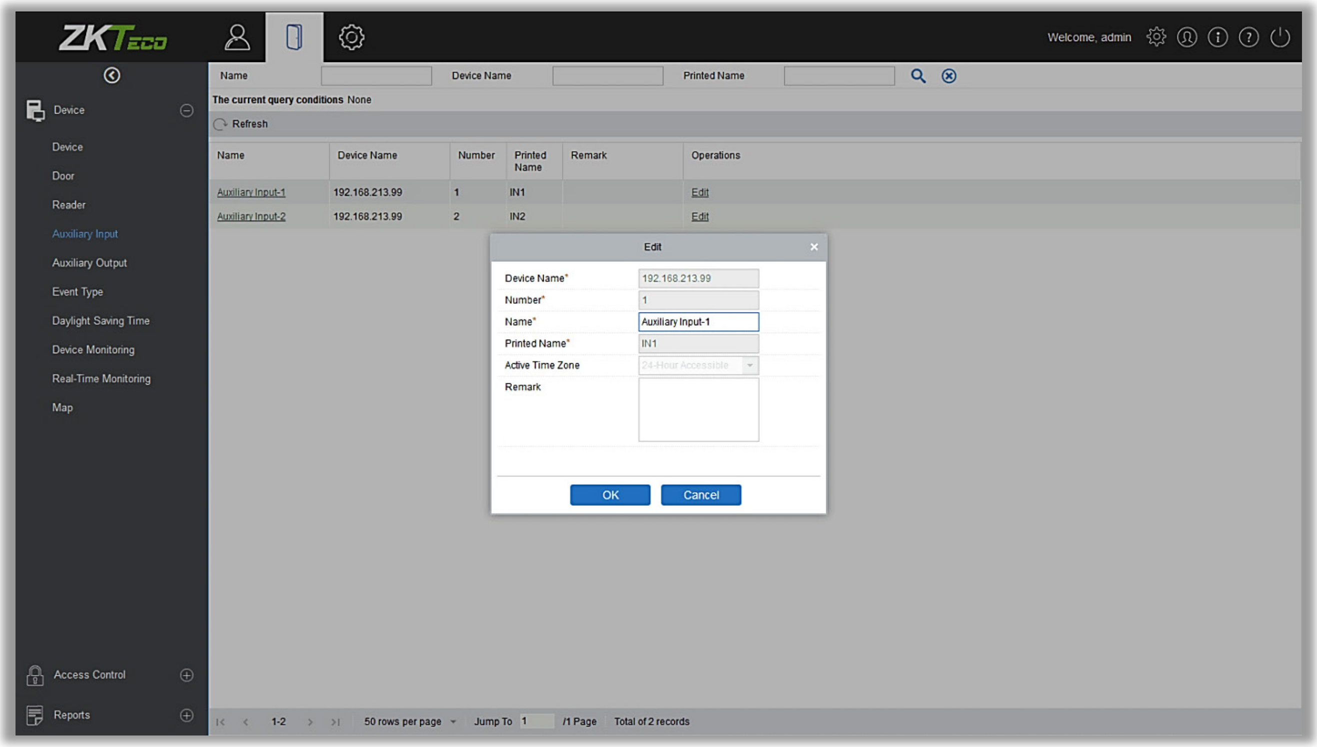
Name: Set the name of the reader displayed on the list page.

### 4.1.5 Auxiliary Input

It is mainly used to connect devices like infrared sensors, smog sensors, smoke detector, etc.

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:



Name | Device Name | Printed Name

The current query conditions None

| Name | Device Name | Number | Printed Name | Remark | Operations |
|---|---|---|---|---|---|
| Auxiliary Input-1 | 192.168.213.99 | 1 | IN1 | | Edit |
| Auxiliary Input-2 | 192.168.213.99 | 2 | IN2 | | Edit |

Edit

| | |
|---|---|
| Device Name* | 192.168.213.99 |
| Number* | 1 |
| Name* | Auxiliary Input-1 |
| Printed Name* | IN1 |
| Active Time Zone | 24-Hour Accessible |
| Remark | |

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 will be available only in the specified time segment.

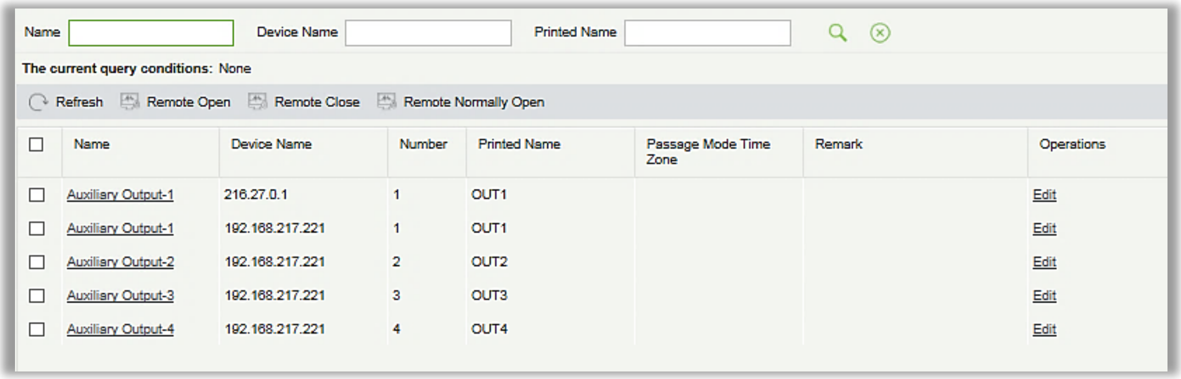
✍Note: Only Name can be modified.

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

## 4.1.6 Auxiliary Output

It is mainly used for alarm output and with active linkage function.

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

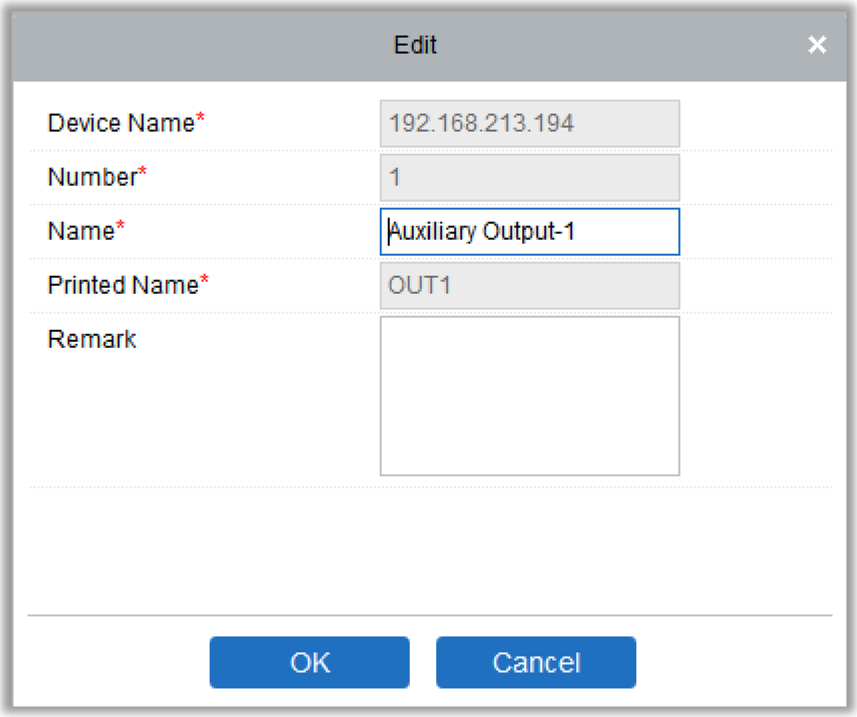


Name | Device Name | Printed Name

The current query conditions: None

| □ | Name | Device Name | Number | Printed Name | Passage Mode Time Zone | Remark | Operations |
|---|---|---|---|---|---|---|---|
| □ | Auxiliary Output-1 | 216.27.0.1 | 1 | OUT1 | | | Edit |
| □ | Auxiliary Output-1 | 192.168.217.221 | 1 | OUT1 | | | Edit |
| □ | Auxiliary Output-2 | 192.168.217.221 | 2 | OUT2 | | | Edit |
| □ | Auxiliary Output-3 | 192.168.217.221 | 3 | OUT3 | | | Edit |
| □ | Auxiliary Output-4 | 192.168.217.221 | 4 | OUT4 | | | Edit |

2. Click [Edit] to modify the parameters:



| | |
|---|---|
| Device Name* | 192.168.213.194 |
| Number* | 1 |
| Name* | Auxiliary Output-1 |
| Printed Name* | OUT1 |
| Remark | |

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.

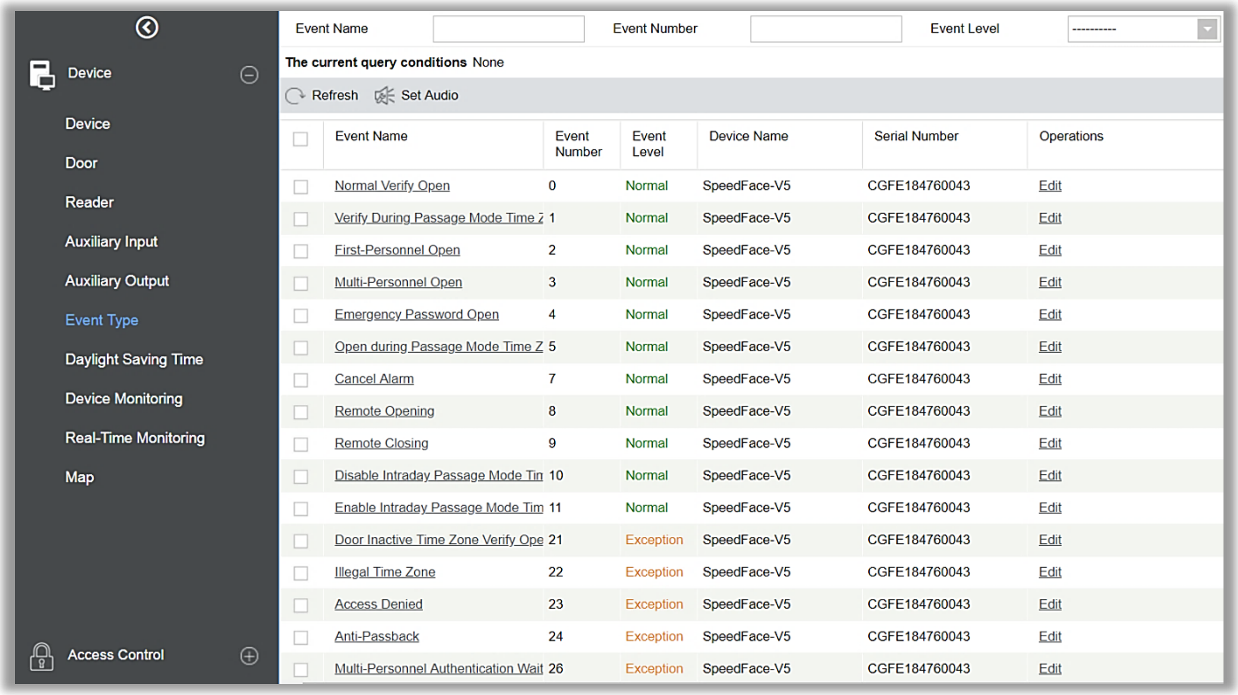
✍**Note:** Only Name, Passage Mode Time Zone and Remarks can be modified.

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 [Device] > [Event] to access the following page:

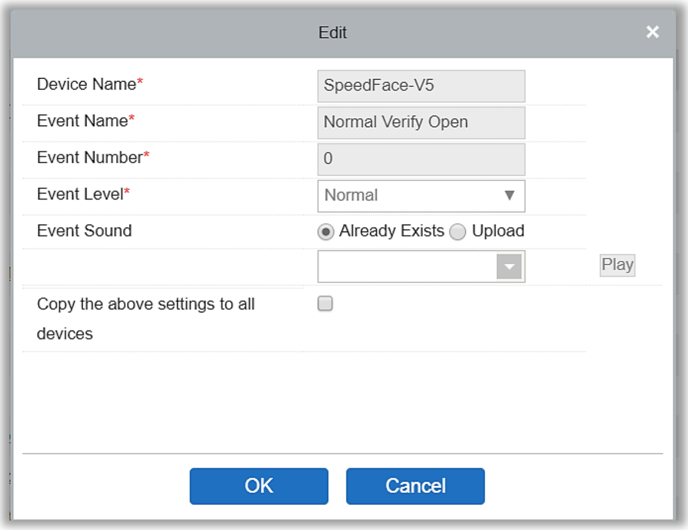


Event Name | Event Number | Event Level ----------

**The current query conditions** None

| □ | Event Name | Event Number | Event Level | Device Name | Serial Number | Operations |
|---|---|---|---|---|---|---|
| □ | Normal Verify Open | 0 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Verify During Passage Mode Time Z | 1 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | First-Personnel Open | 2 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Multi-Personnel Open | 3 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Emergency Password Open | 4 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Open during Passage Mode Time Z | 5 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Cancel Alarm | 7 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Remote Opening | 8 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Remote Closing | 9 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Disable Intraday Passage Mode Tin | 10 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Enable Intraday Passage Mode Tim | 11 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Door Inactive Time Zone Verify Ope | 21 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Illegal Time Zone | 22 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Access Denied | 23 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Anti-Passback | 24 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Multi-Personnel Authentication Wait | 26 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |

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



| | |
|---|---|
| Device Name* | SpeedFace-V5 |
| Event Name* | Normal Verify Open |
| Event Number* | 0 |
| Event Level* | Normal ▼ |
| Event Sound | ● Already Exists ○ Upload |
| Copy the above settings to all devices | □ |

## Fields are as follows:

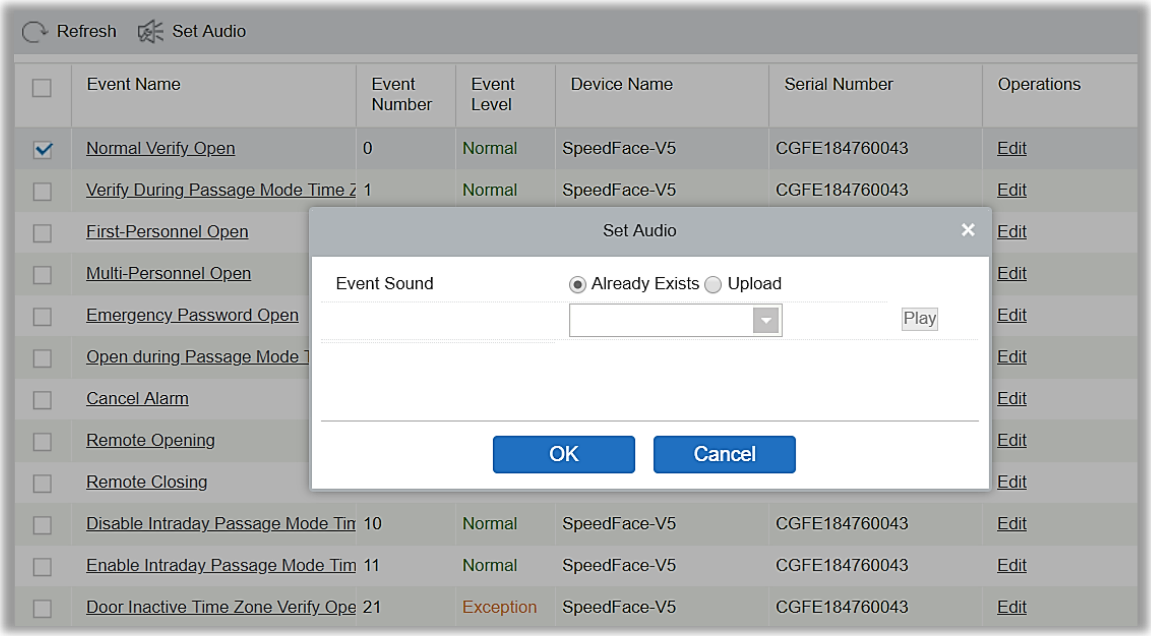
Event Level: Normal, Exception, and Alarm are available.

Event Name: It cannot 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]:



| □ | Event Name | Event Number | Event Level | Device Name | Serial Number | Operations |
|---|---|---|---|---|---|---|
| ☑ | Normal Verify Open | 0 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Verify During Passage Mode Time Z | 1 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | First-Personnel Open | | | | | Edit |
| □ | Multi-Personnel Open | | | | | Edit |
| □ | Emergency Password Open | | | | | Edit |
| □ | Open during Passage Mode T | | | | | Edit |
| □ | Cancel Alarm | | | | | Edit |
| □ | Remote Opening | | | | | Edit |
| □ | Remote Closing | | | | | Edit |
| □ | Disable Intraday Passage Mode Tin | 10 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Enable Intraday Passage Mode Tim | 11 | Normal | SpeedFace-V5 | CGFE184760043 | Edit |
| □ | Door Inactive Time Zone Verify Ope | 21 | Exception | SpeedFace-V5 | CGFE184760043 | Edit |

Set Audio ×

Event Sound ● Already Exists ○ Upload

Play

OK Cancel

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.

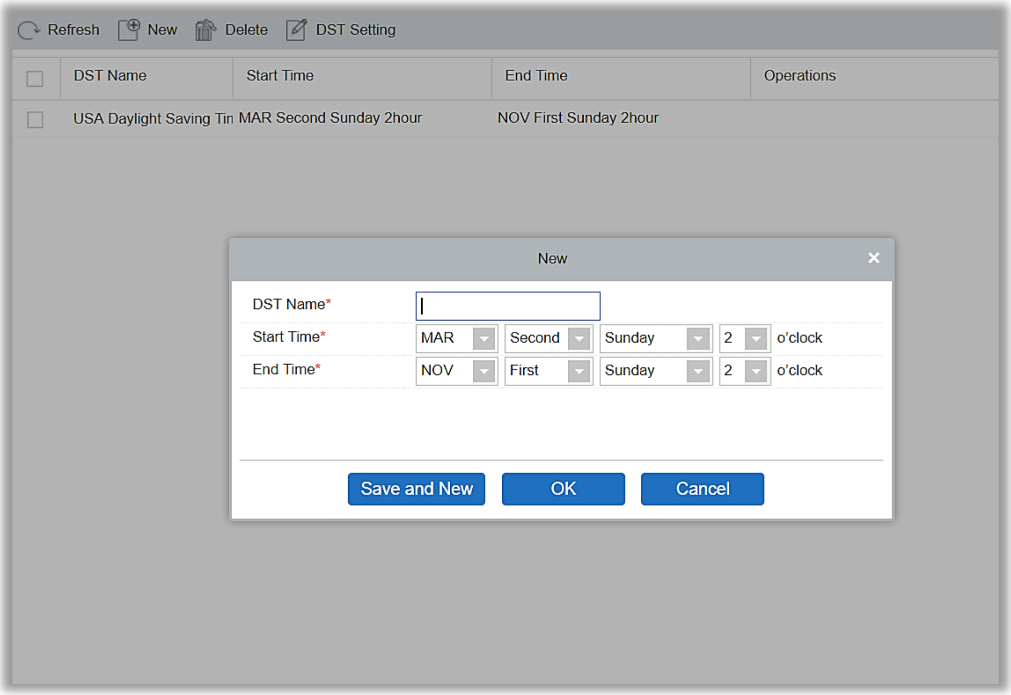
### 4.1.8 Daylight Saving Time

The Daylight-Saving Time is a function to adjust the official prescribe local time to save energy. The unified time adopted during the implementation is known as the "DST". Typically, regions that use daylight saving time adjust clocks forward one hour to standard time close to the start of spring in the summer to make people sleep early. It can also help to save energy. In autumn, adjust clocks are adjusted backwards to get up early. 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 ahead at (hour) (day) (month) and one hour backward at (hour) (day) (month) if necessary.

- Add DST

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



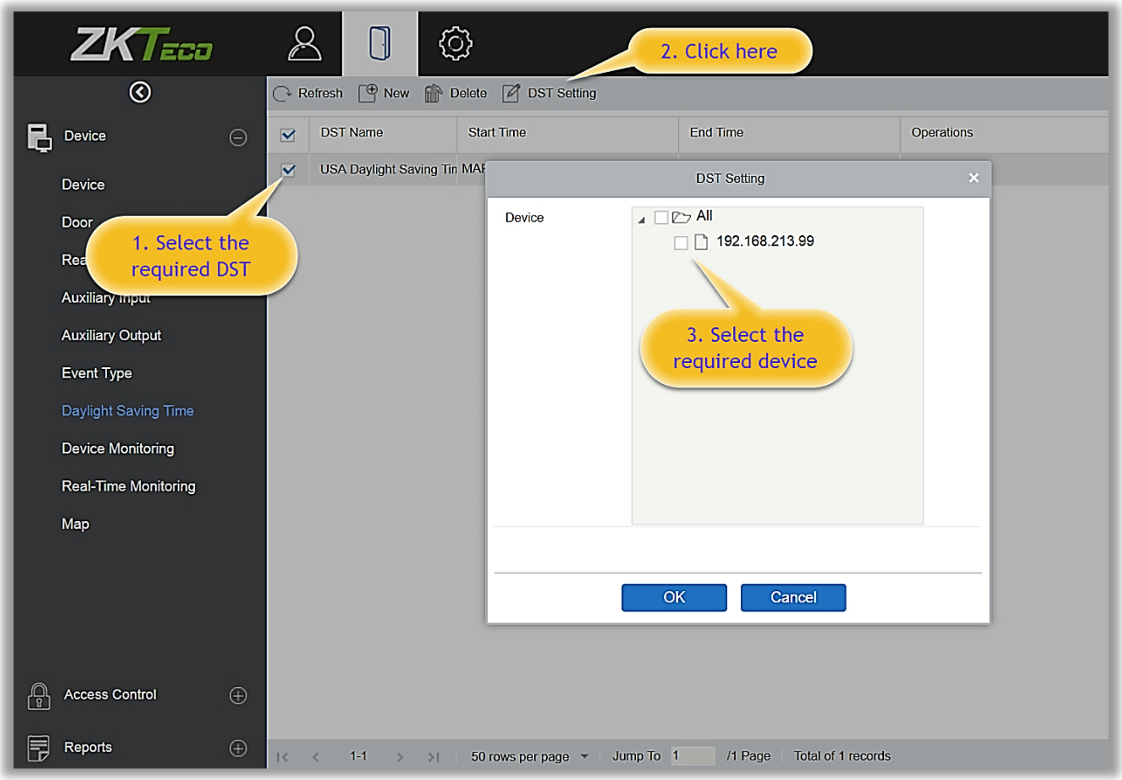
| ☐ | DST Name | Start Time | End Time | Operations |
|---|---|---|---|---|
| ☐ | USA Daylight Saving Tin | MAR Second Sunday 2hour | NOV First Sunday 2hour | |

New

| | | | | | |
|---|---|---|---|---|---|
| DST Name* | | | | | |
| Start Time* | MAR | Second | Sunday | 2 | o'clock |
| End Time* | NOV | First | Sunday | 2 | o'clock |

The row fields are as; "Month – Week – Day - Hour" format. For example, if the start time is set as "March – Second – Sunday – 2 o'clock" it means the DST will start from the second Sunday of March at 2 AM. 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



2. Click here

1. Select the required DST

3. Select the required device

| ☑ | DST Name | Start Time | End Time | Operations |
|---|---|---|---|---|
| ☑ | USA Daylight Saving Tin | MAR | | |

DST Setting

Device: ☐ All
☐ 192.168.213.99

1-1 | 50 rows per page | Jump To 1 /1 Page | Total of 1 records

The user can enable the DST setting on a device: In the DST interface, select desired DST, and click

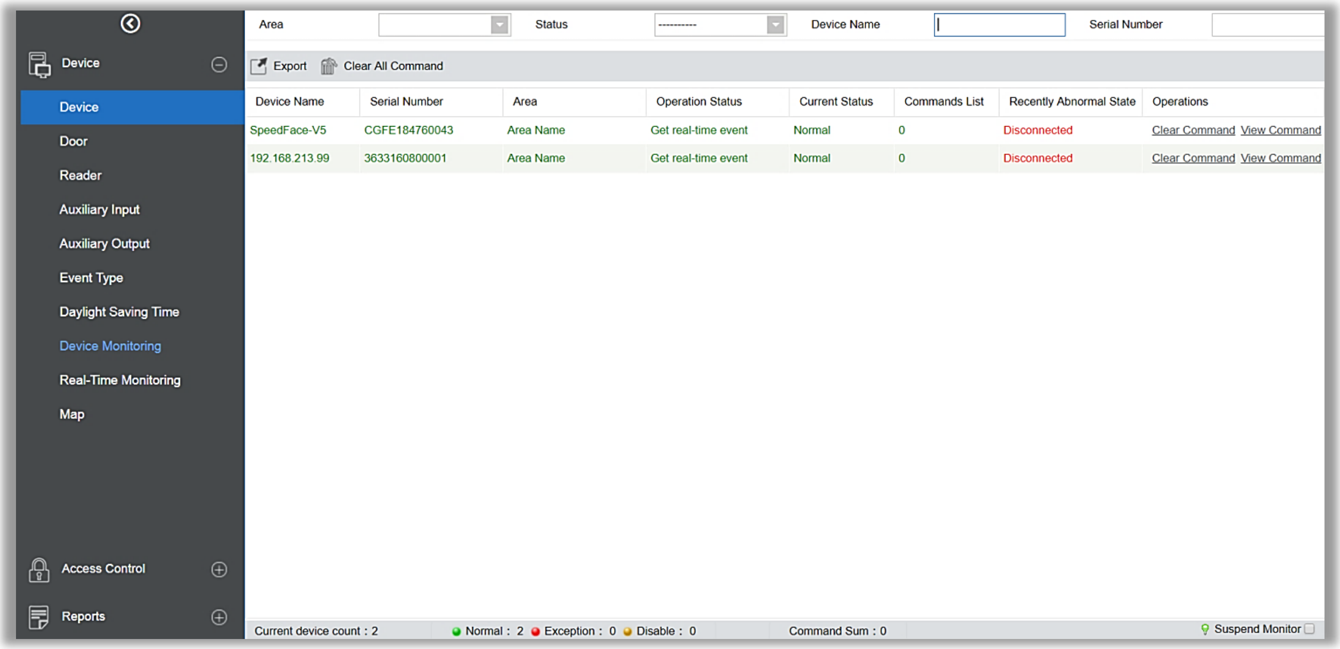
[DST Setting], select the device to apply the DST setting to and click [OK] to confirm.

✍**Notes:**

- If a DST setting is in use, it cannot be deleted. Deselect DST setting and then delete.
- 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.



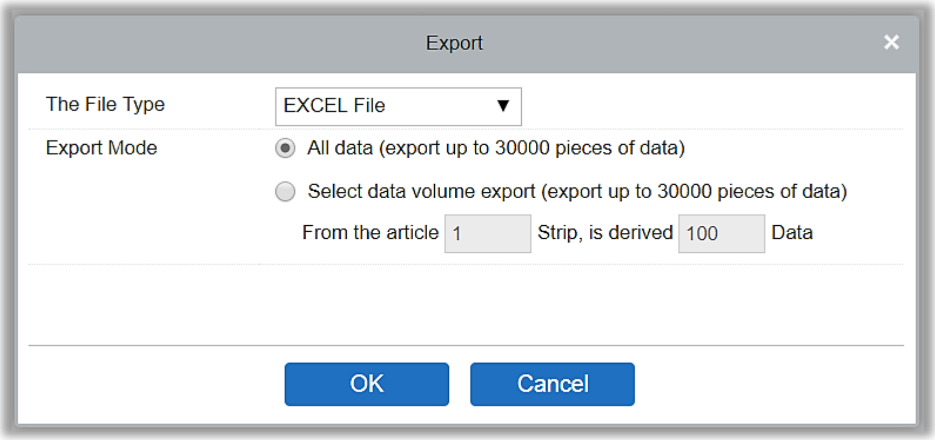
Area | Status ---------- | Device Name | Serial Number

| Device Name | Serial Number | Area | Operation Status | Current Status | Commands List | Recently Abnormal State | Operations |
|---|---|---|---|---|---|---|---|
| SpeedFace-V5 | CGFE184760043 | Area Name | Get real-time event | Normal | 0 | Disconnected | Clear Command View Command |
| 192.168.213.99 | 3633160800001 | Area Name | Get real-time event | Normal | 0 | Disconnected | Clear Command View Command |

Current device count : 2 ● Normal : 2 ● Exception : 0 ● Disable : 0 Command Sum : 0

### Export

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

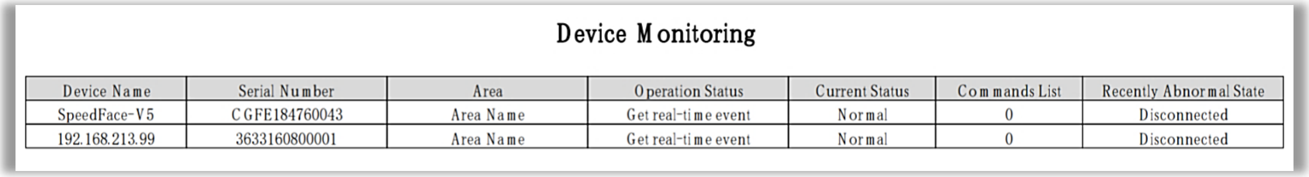


The File Type: EXCEL File ▼

Export Mode: ● All data (export up to 30000 pieces of data)

○ Select data volume export (export up to 30000 pieces of data)

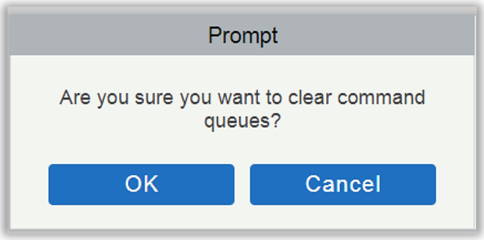
From the article 1 Strip, is derived 100 Data



Device Monitoring

| Device Name | Serial Number | Area | Operation Status | Current Status | Commands List | Recently Abnormal State |
|---|---|---|---|---|---|---|
| SpeedFace-V5 | CGFE184760043 | Area Name | Get real-time event | Normal | 0 | Disconnected |
| 192.168.213.99 | 3633160800001 | Area Name | Get real-time event | Normal | 0 | Disconnected |

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



Are you sure you want to clear command queues?

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 maximum capacity is reached, 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.
- Operation Status shows the state of the current device, mainly used for debugging.
- If the number of commands to be performed is greater than 0, then it indicates that the data is not yet synchronized to the device, so wait for the synchronization to complete.

### 4.1.10 Real-Time Monitoring

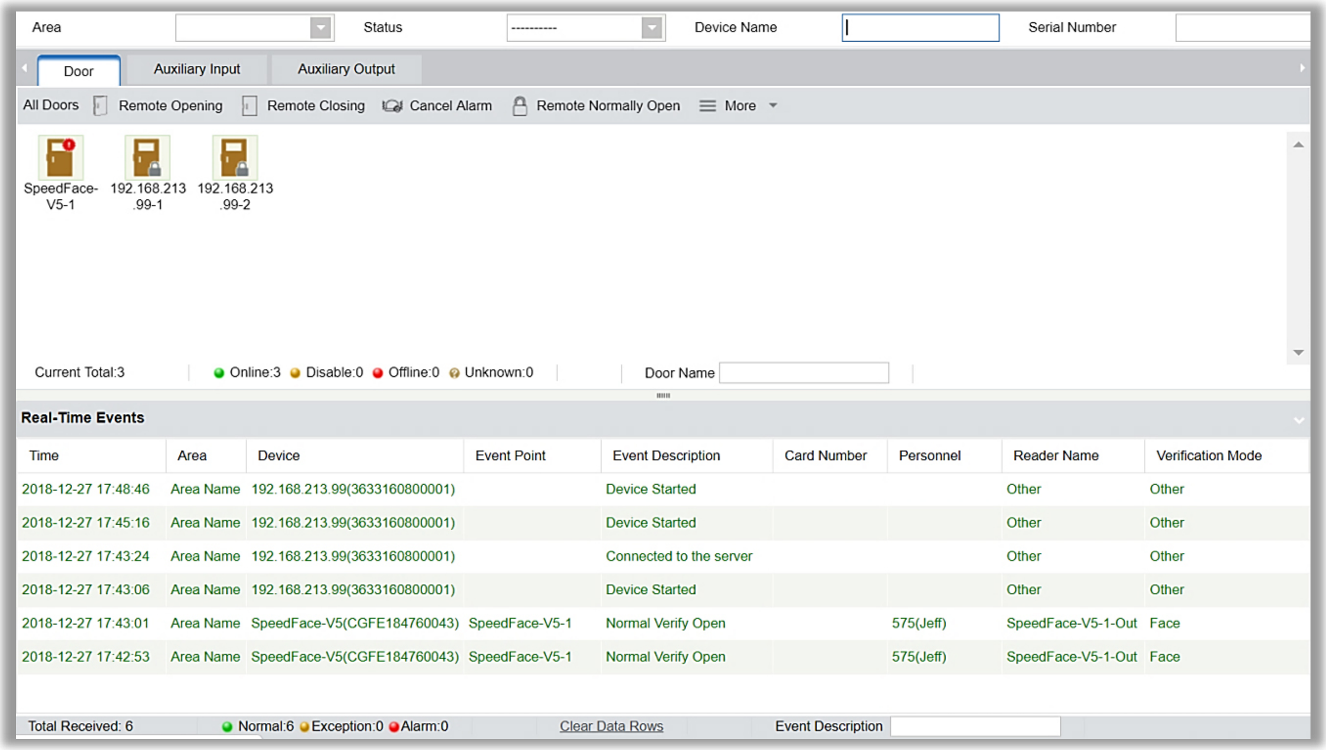
Click [Access Device] > [Real-Time Monitoring].

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:

| Icons | Status | Icons | Status |
|---|---|---|---|
| 🚪 | Device blocked | 🚪 | Door Offline |
| 🚪 | Door sensor not set, relay closed | 🚪 | Door sensor not set, relay opened |
| 🚪 | Door sensor not set, and the present firmware does not support current action on the device | | |
| 🚪 | Online status Door closed, Relay closed | 🚪 | Online status Door closed, Relay opened |
| 🚪 | Online status Door closed, and the present firmware does not support current action on the device | | |
| 🚪 | Online status Door opened, Relay closed | 🚪 | Online status Door opened, Relay opened |
| 🚪 | Online status Door opened, and the present firmware does not support current action on the device | | |
| 🚪 | Door opened alarming, Relay closed | 🚪 | Door opened alarming, Relay opened |
| 🚪 | Door opening timeout, Relay closed | 🚪 | Door opening timeout, Relay opened |
| 🚪 | Door opening timeout, and the present firmware does not support current action on the device | | |
| 🚪 | Door opening timeout, Relay closed/Door Sensor Closed | 🚪 | Door opening timeout, Relay opened/ Door Sensor Closed |
| 🚪 | Door closed alarming, Relay closed | 🚪 | Door closed alarming, Relay opened |
| 🚪 | Door closed alarming, Indicates that the present firmware does not support current action on the device | | |

|  |  |  |  |
|---|---|---|---|
| 🚪 | Door sensor not set, Door alarming, Relay closed | 🚪 | Door sensor unset, Door alarming, Relay opened |
| 🚪 | Door opening timeout, Without relay status/Door Sensor Closed | 🔒 | Door locking |
| **Without relay status, indicates that the current firmware does not support action on the device.** |  |  |  |



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

Door | Auxiliary Input | Auxiliary Output

All Doors | Remote Opening | Remote Closing | Cancel Alarm | Remote Normally Open | More

SpeedFace-V5-1 | 192.168.213.99-1 | 192.168.213.99-2

Current Total:3 | Online:3 Disable:0 Offline:0 Unknown:0 | Door Name

Real-Time Events

| Time | Area | Device | Event Point | Event Description | Card Number | Personnel | Reader Name | Verification Mode |
|---|---|---|---|---|---|---|---|---|
| 2018-12-27 17:48:46 | Area Name | 192.168.213.99(3633160800001) |  | Device Started |  |  | Other | Other |
| 2018-12-27 17:45:16 | Area Name | 192.168.213.99(3633160800001) |  | Device Started |  |  | Other | Other |
| 2018-12-27 17:43:24 | Area Name | 192.168.213.99(3633160800001) |  | Connected to the server |  |  | Other | Other |
| 2018-12-27 17:43:06 | Area Name | 192.168.213.99(3633160800001) |  | Device Started |  |  | Other | Other |
| 2018-12-27 17:43:01 | Area Name | SpeedFace-V5(CGFE184760043) | SpeedFace-V5-1 | Normal Verify Open |  | 575(Jeff) | SpeedFace-V5-1-Out | Face |
| 2018-12-27 17:42:53 | Area Name | SpeedFace-V5(CGFE184760043) | SpeedFace-V5-1 | Normal Verify Open |  | 575(Jeff) | SpeedFace-V5-1-Out | Face |

Total Received: 6 | Normal:6 Exception:0 Alarm:0 | Clear Data Rows | Event Description

Different icons represent status as followed:

1. 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 (can be opened at any time).

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.

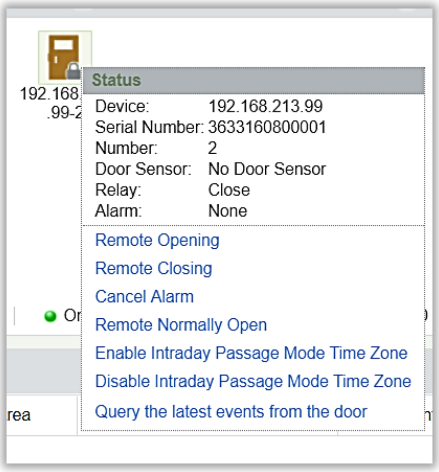
Cancel the alarm: Once an alarming door pops-up over the interface, the alarm sound will be played. Alarm cancellation can be done for single door and all doors. To control a single door, move the cursor over the door icon, a menu will pop-up, then click [Remote Opening/ Closing] in the menu. To control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

- Quick Management of Doors

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



Status

Device: 192.168.213.99
Serial Number: 3633160800001
Number: 2
Door Sensor: No Door Sensor
Relay: Close
Alarm: None

192.168
.99-2
On
rea
Remote Opening
Remote Closing
Cancel Alarm
Remote Normally Open
Enable Intraday Passage Mode Time Zone
Disable Intraday Passage Mode Time Zone
Query the latest events from the door

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

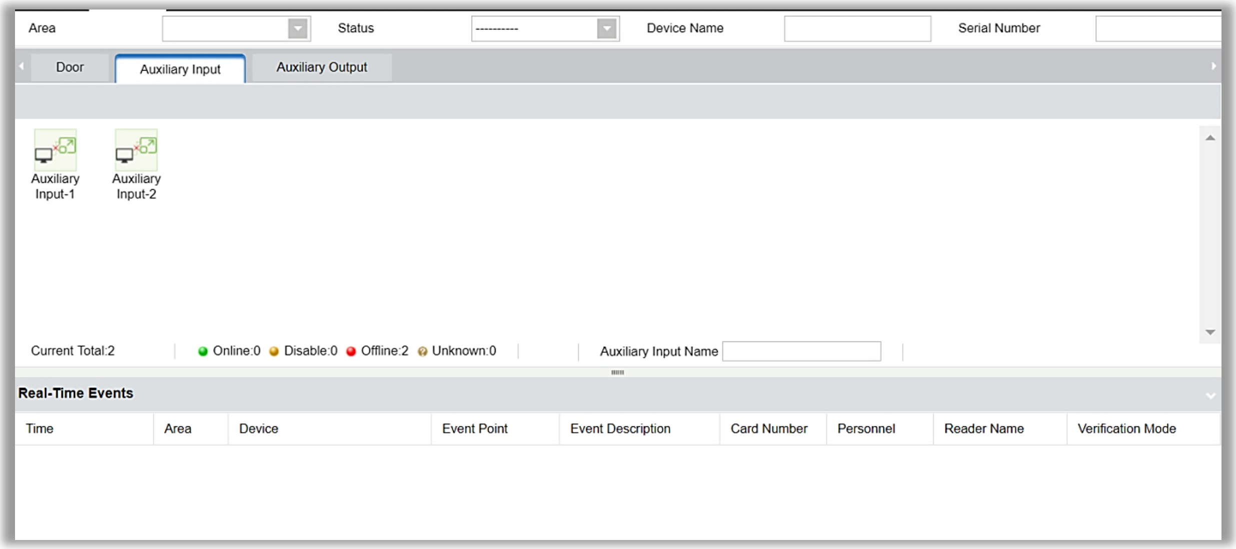
Issue card to person: If you swap an unregistered card, a record with a card number will pop-up in real-time monitoring interface. Right click that card number, and a menu will pop-out. Click "Issue card to person", to assign that card to one person.

- 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.

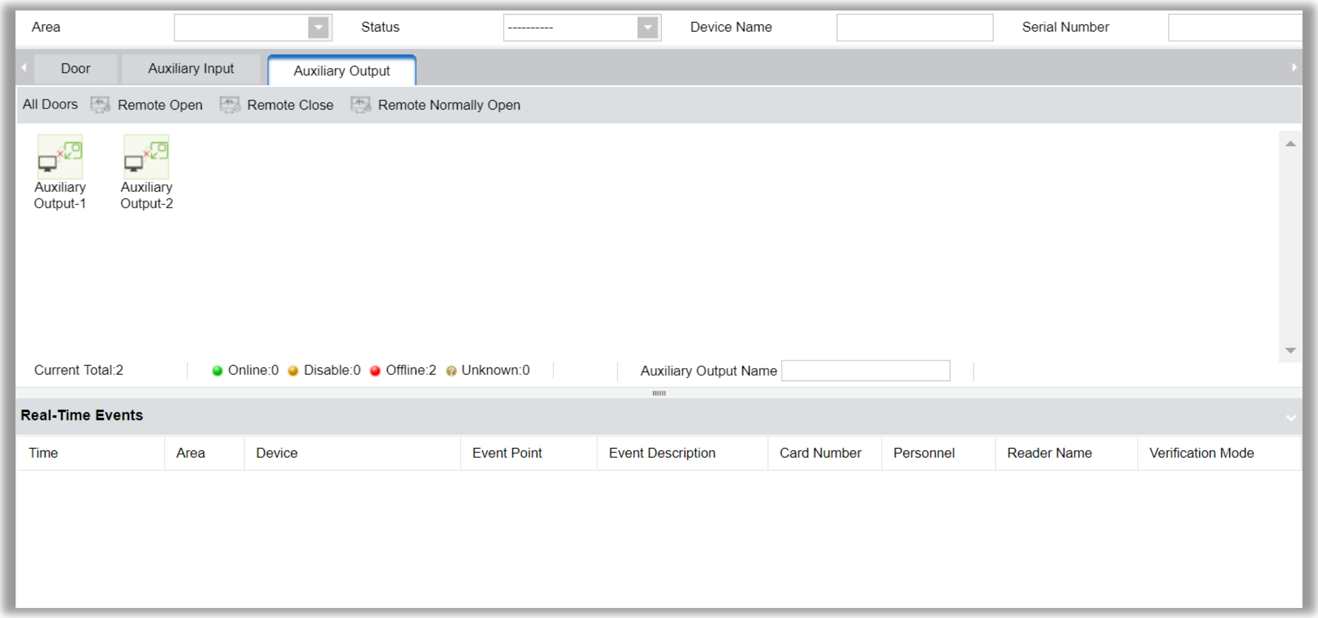
### 2. Auxiliary Input

It monitors current auxiliary input events in real-time.



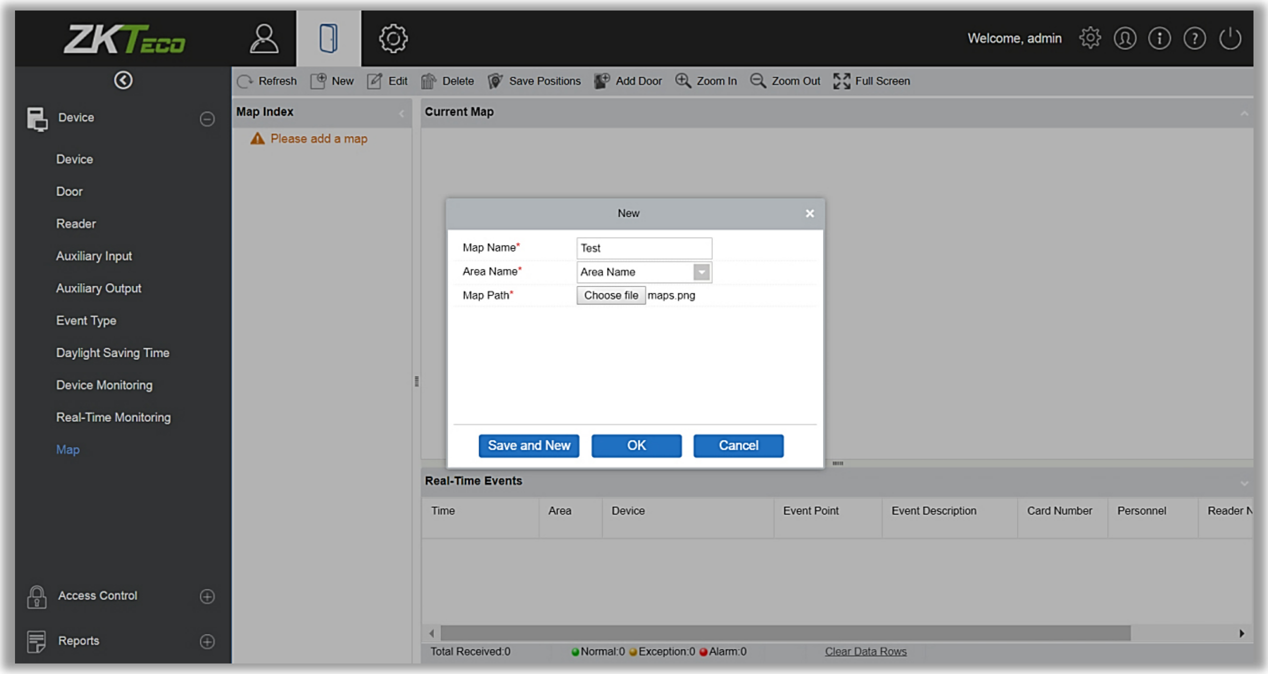
## 3. Auxiliary Output

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



## 4.1.11 Map

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

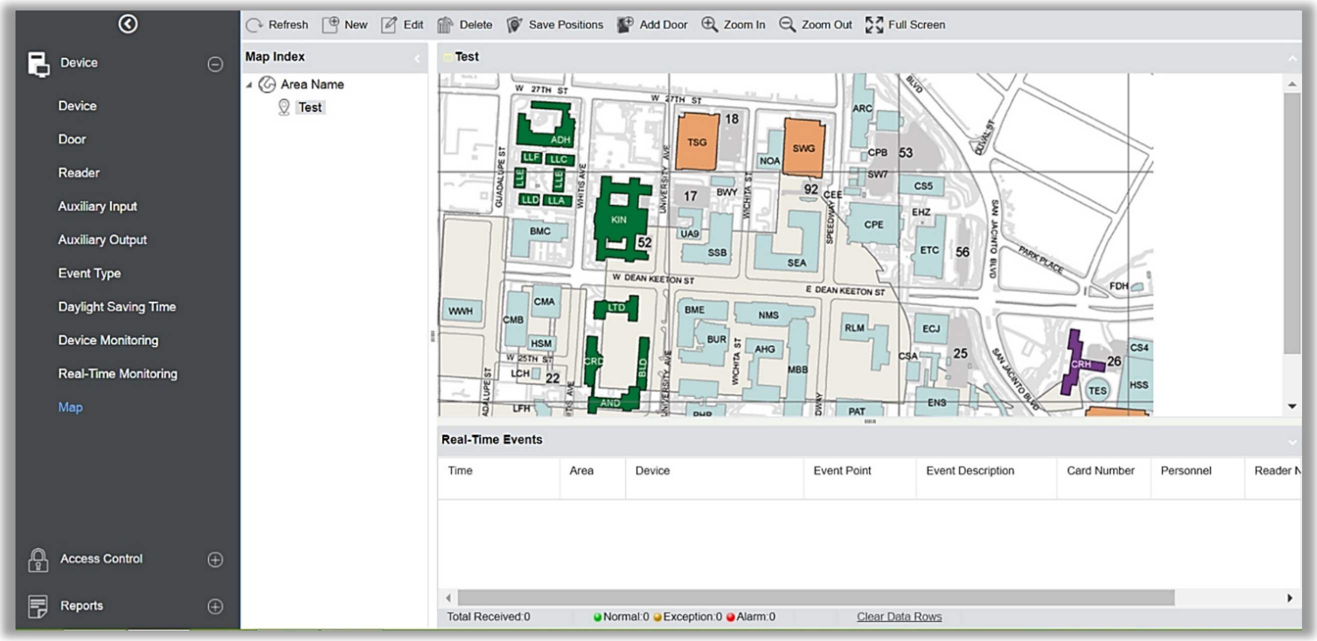


Map Name* Test

Area Name* Area Name

Map Path* Choose file maps.png

After adding, users can add door on the map, perform zoom-in, zoom-out, etc. If users relocated some sections or modified the map, click [Save Positions] to save. The user can view the new setting after re-opening Map interface.



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 over a door icon, 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:**

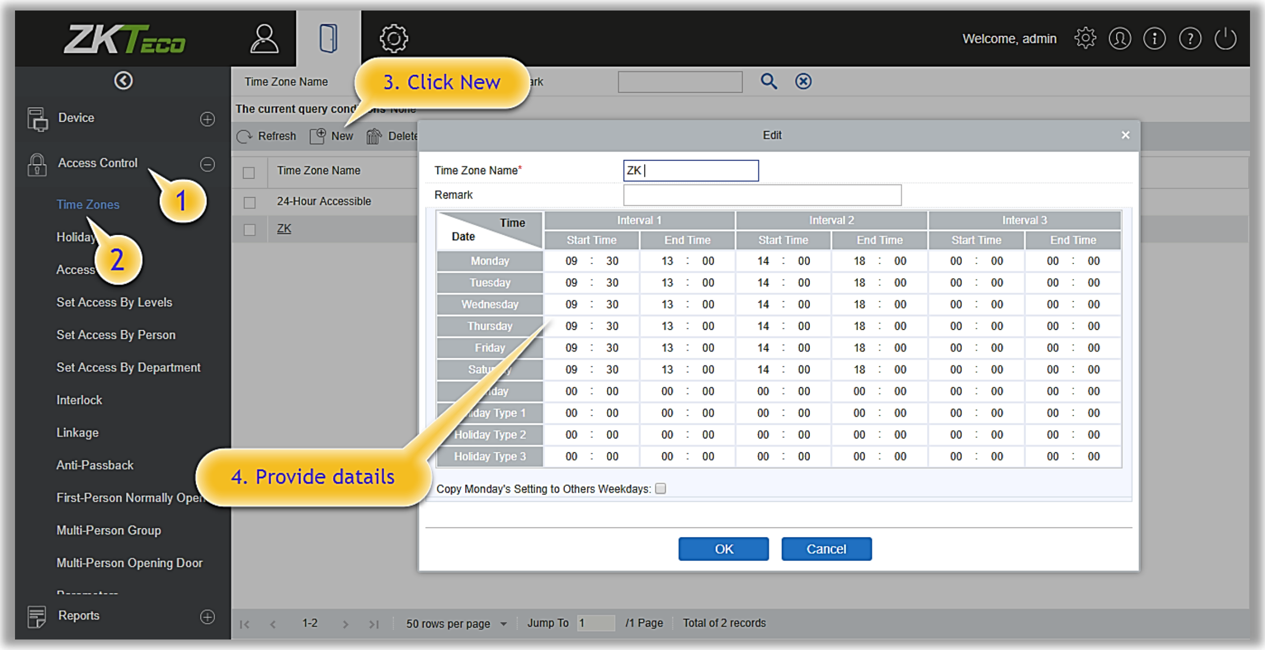
- In map modification, users can choose to modify the map name but not the path. Users only need to check the box to activate the modification option.
- The system supports adding multi doors at the same time. After adding the doors, users need to set the door position on the map and click [Save].
- 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 can only be used only during a valid time periods of certain doors. 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 Time Zones as required.



Edit

Time Zone Name*: ZK|

Remark:

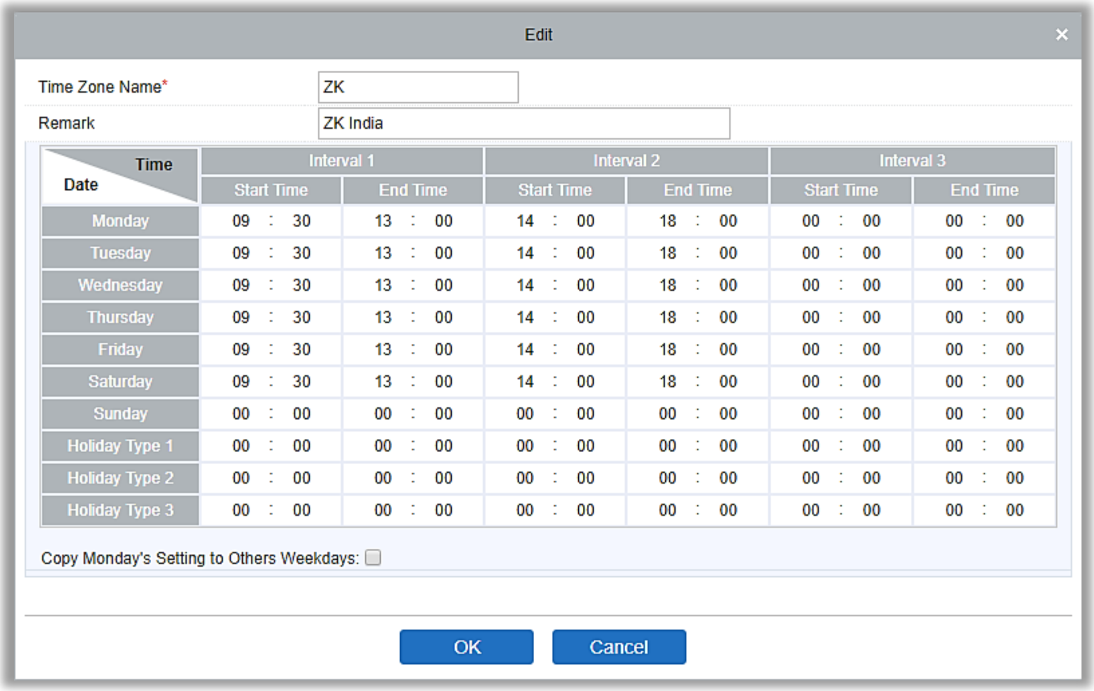
| Time / Date | Interval 1 |  | Interval 2 |  | Interval 3 |  |
|---|---|---|---|---|---|---|
|  | Start Time | End Time | Start Time | End Time | Start Time | End Time |
| Monday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Tuesday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Wednesday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Thursday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Friday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Saturday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Sunday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 1 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 2 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 3 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |

Copy Monday's Setting to Others Weekdays: □

OK Cancel

## 1. Add Access Control Time Zone

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



Edit

Time Zone Name*: ZK

Remark: ZK India

| Time / Date | Interval 1 |  | Interval 2 |  | Interval 3 |  |
|---|---|---|---|---|---|---|
|  | Start Time | End Time | Start Time | End Time | Start Time | End Time |
| Monday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Tuesday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Wednesday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Thursday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Friday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Saturday | 09 : 30 | 13 : 00 | 14 : 00 | 18 : 00 | 00 : 00 | 00 : 00 |
| Sunday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 1 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 2 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Holiday Type 3 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |

Copy Monday's Setting to Others Weekdays: □

OK Cancel

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: Select the check box to copy the settings of Monday to other weekdays.

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

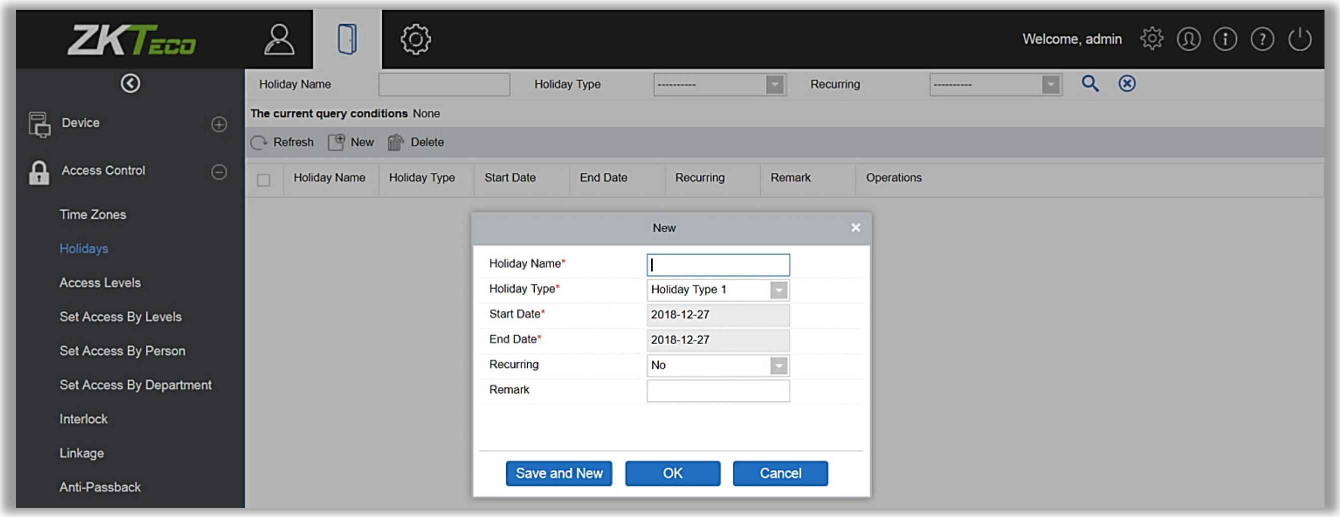
### 2. Modify Access Control Time Zones

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 select the check boxes one or more time zones in the list, and click the [Delete] button over the list, then click [OK] to delete, or click [Cancel] 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.

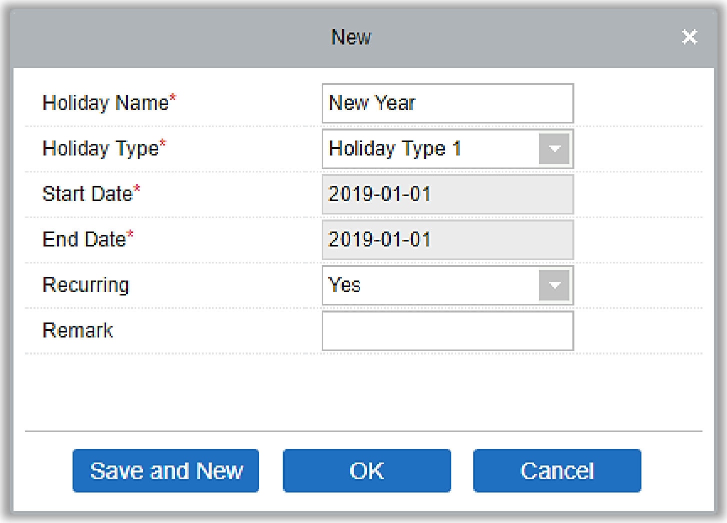


The current query conditions None

| | |
|---|---|
| Holiday Name* | |
| Holiday Type* | Holiday Type 1 |
| Start Date* | 2018-12-27 |
| End Date* | 2018-12-27 |
| Recurring | No |
| Remark | |

- Add

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



| | |
|---|---|
| Holiday Name* | New Year |
| Holiday Type* | Holiday Type 1 |
| Start Date* | 2019-01-01 |
| End Date* | 2019-01-01 |
| Recurring | Yes |
| Remark | |

Fields are as follows:

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

Holiday Type: Holiday Type 1/2/3, as explained in Holiday. 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 is 2019-01-01. 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 is used when the holiday repeats on same date every year. The default is No. For example, the Near Year's Day is on January 1 each year, and can be set as Yes. Some festival date changes every year, so it cannot be set a repeated and should be set as No.

For example, the date of Near Year's Day is set as January 1, 2019, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of Tuesday, 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.

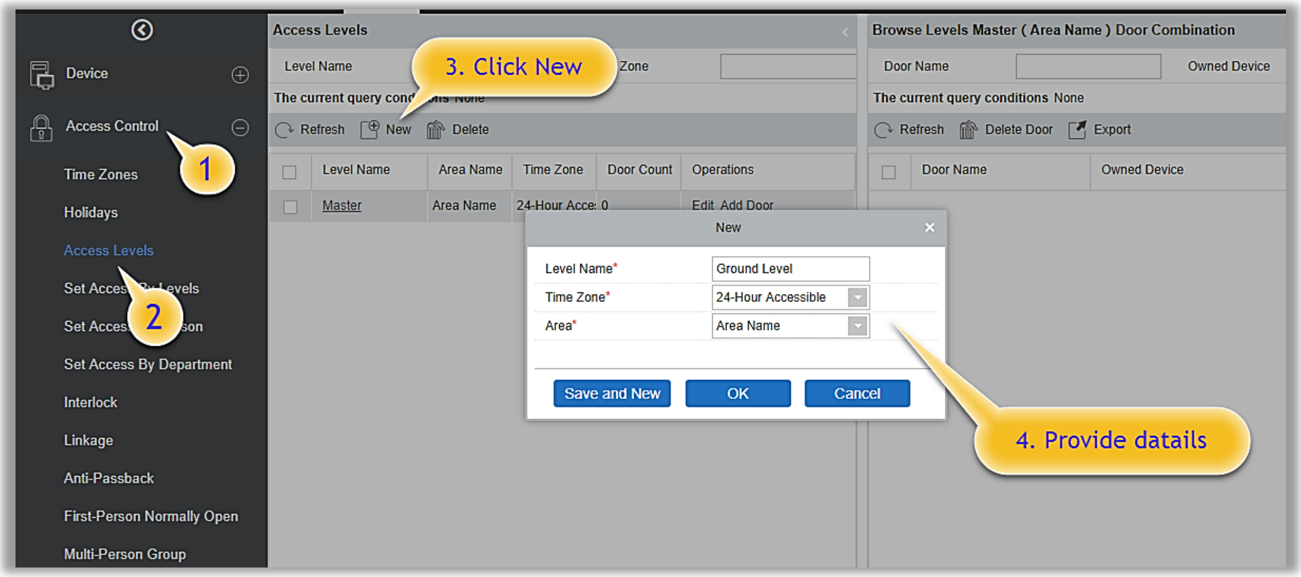
- Delete

In the access control holiday list, click [Delete] button under Operations. Click [OK] to delete, or 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.



Level Name* Ground Level

Time Zone* 24-Hour Accessible

Area* Area Name

1

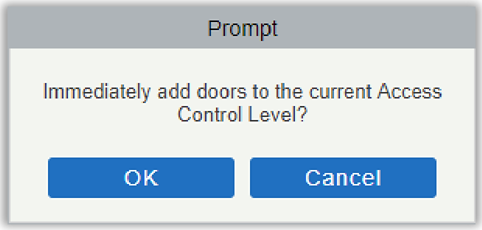
2

3. Click New

4. Provide datails

- Add

1. Click [Access Control] > [Access Levels] > [New] to enter the Add Levels editing interface:
2. Set each parameter: Level Name (must not be same as other level names), Time Zone.
3. Click [OK] and then the system prompts “Immediately add doors to the current Access Control Level”, click [OK] to add doors, or you can click [Cancel] to return the access levels list. The added access level will be displayed in the list.

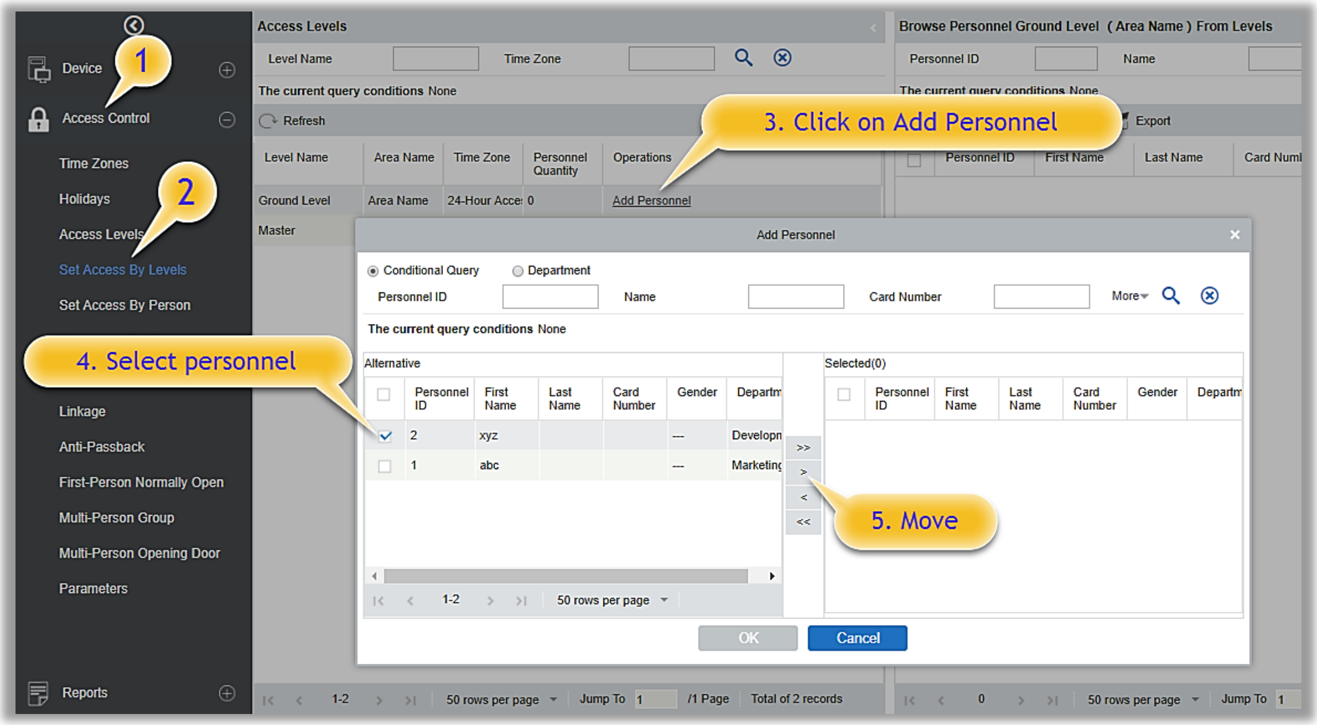


Immediately add doors to the current Access Control Level?

✍**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:



The current query conditions None

| Level Name | Area Name | Time Zone | Personnel Quantity | Operations |
|---|---|---|---|---|
| Ground Level | Area Name | 24-Hour Acce: | 0 | Add Personnel |
| Master | | | | |

| □ | Personnel ID | First Name | Last Name | Card Number | Gender | Departm |
|---|---|---|---|---|---|---|
| ☑ | 2 | xyz | | | --- | Developn |
| □ | 1 | abc | | | --- | Marketing |

(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:

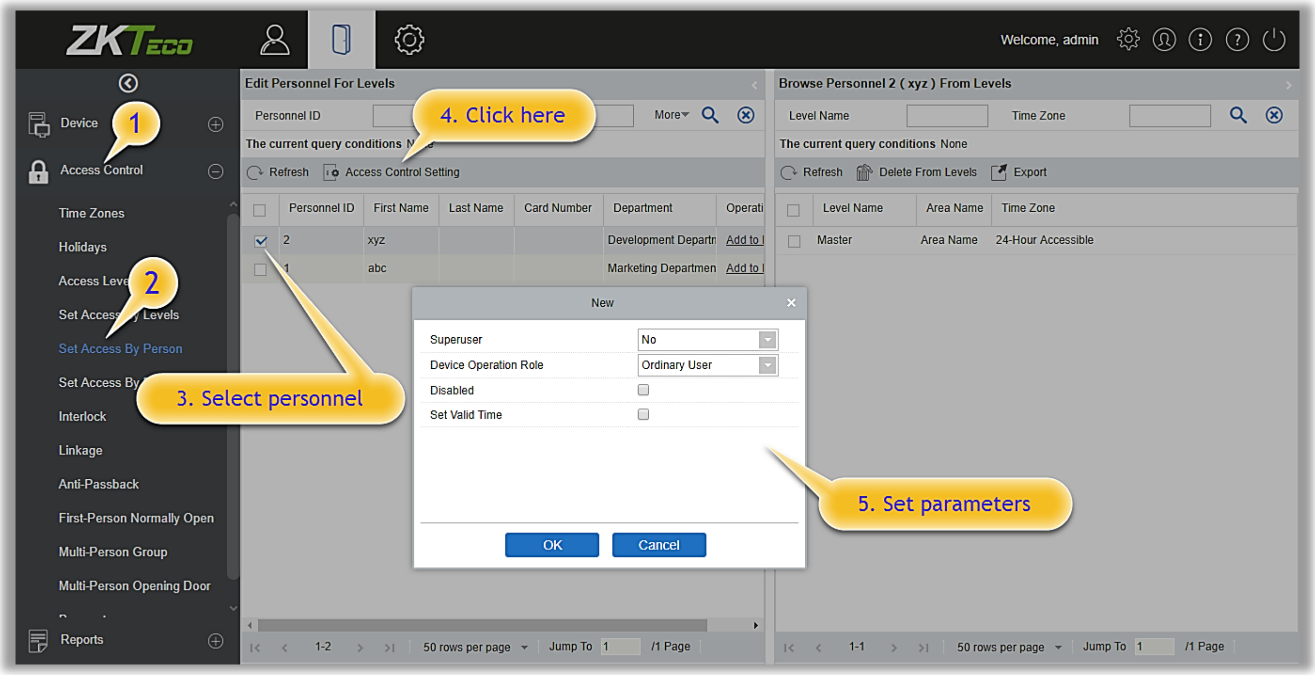
(1) Click [Access Control] > [Access Levels] > [Set Access By Person], click Employee to view the levels in the list on the right.

(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].



1

2

3. Select personnel

4. Click here

5. Set parameters

The current query conditions None

| ☐ | Personnel ID | First Name | Last Name | Card Number | Department | Operati |
|---|---|---|---|---|---|---|
| ☑ | 2 | xyz | | | Development Departn | Add to l |
| ☐ | 1 | abc | | | Marketing Departmen | Add to l |

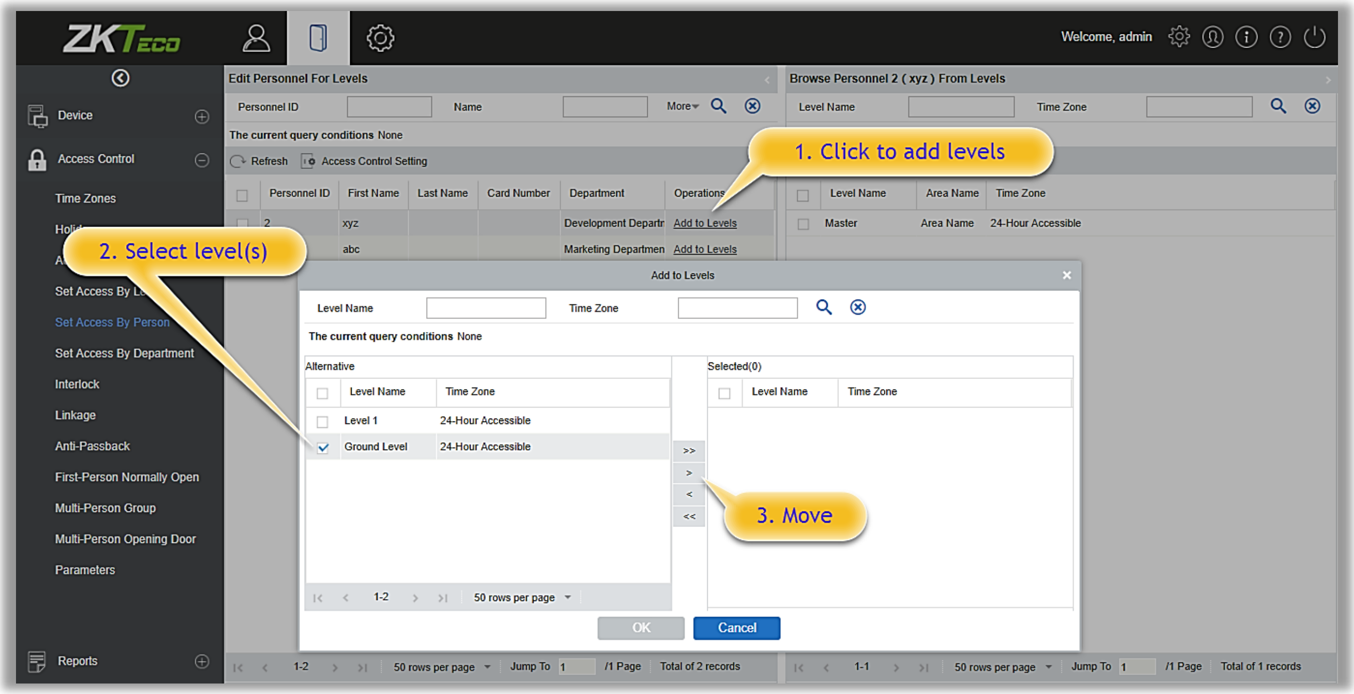
The current query conditions None

| ☐ | Level Name | Area Name | Time Zone |
|---|---|---|---|
| ☐ | Master | Area Name | 24-Hour Accessible |

| | |
|---|---|
| Superuser | No |
| Device Operation Role | Ordinary User |
| Disabled | ☐ |
| Set Valid Time | ☐ |

B. If required, set access control parameters and then click [OK] to save the settings.

C. Now you need to add levels to the personnel.



1. Click to add levels

2. Select level(s)

3. Move

The current query conditions None

| ☐ | Personnel ID | First Name | Last Name | Card Number | Department | Operations |
|---|---|---|---|---|---|---|
| ☐ | 2 | xyz | | | Development Departn | Add to Levels |
| ☐ | 1 | abc | | | Marketing Departmen | Add to Levels |

The current query conditions None

| ☐ | Level Name | Area Name | Time Zone |
|---|---|---|---|
| ☐ | Master | Area Name | 24-Hour Accessible |

Add to Levels

The current query conditions None

Alternative

| ☐ | Level Name | Time Zone |
|---|---|---|
| ☐ | Level 1 | 24-Hour Accessible |
| ☑ | Ground Level | 24-Hour Accessible |

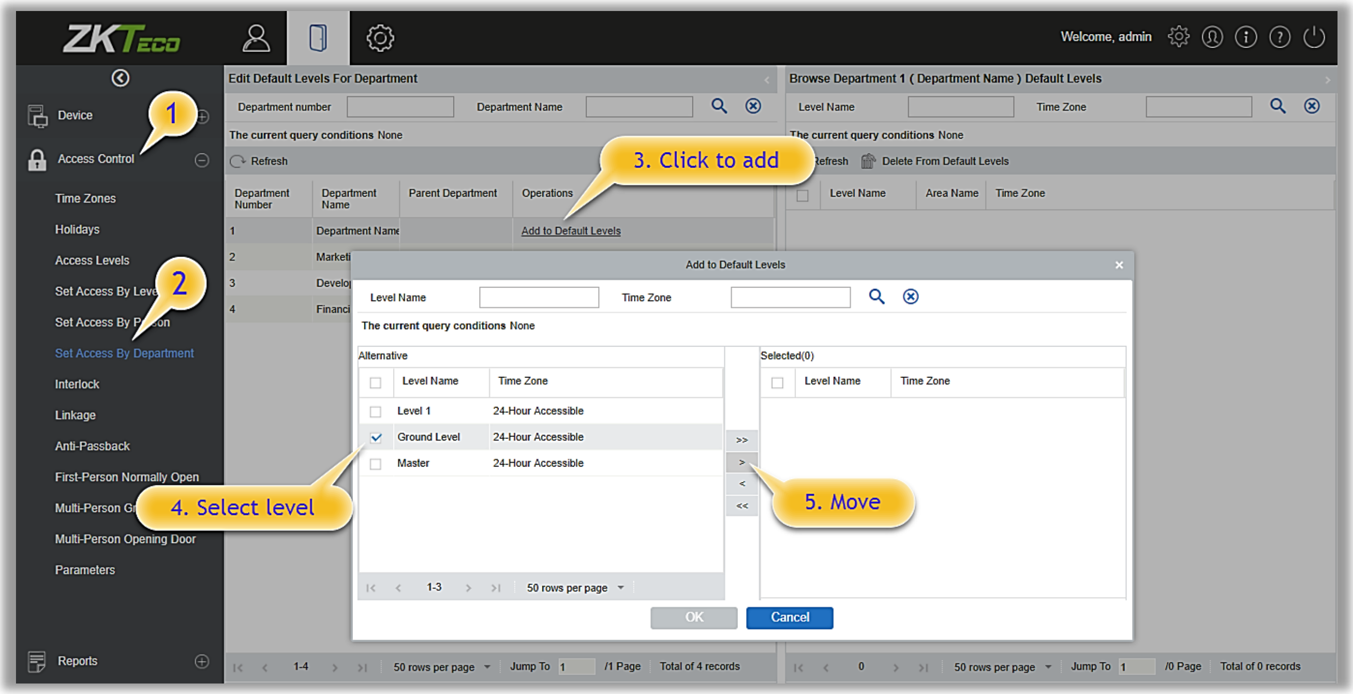
Selected(0)

| ☐ | Level Name | Time Zone |
|---|---|---|

D. After selecting the required level(s), click OK to save and exit.

### 4.2.6 Set Access By Department

You can add the selected department to the selected access levels or delete the selected department from the access levels. The access of the personnel in the department will be changed.



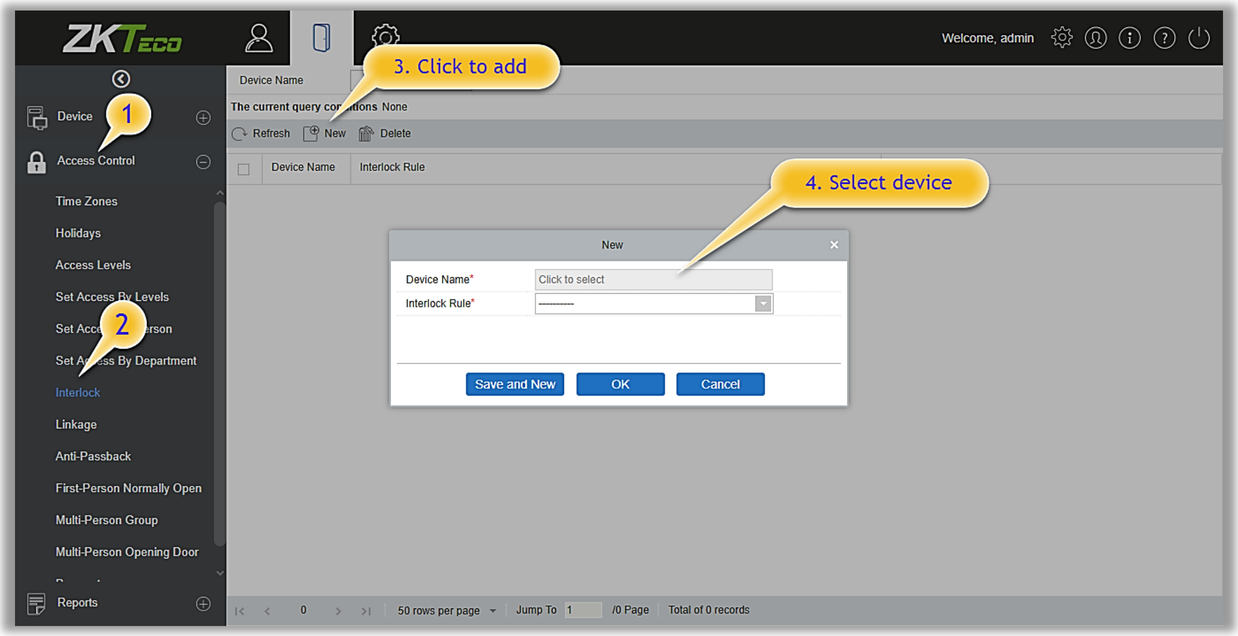
## 4.2.7 Interlock

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 connects 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 the required Device. 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.

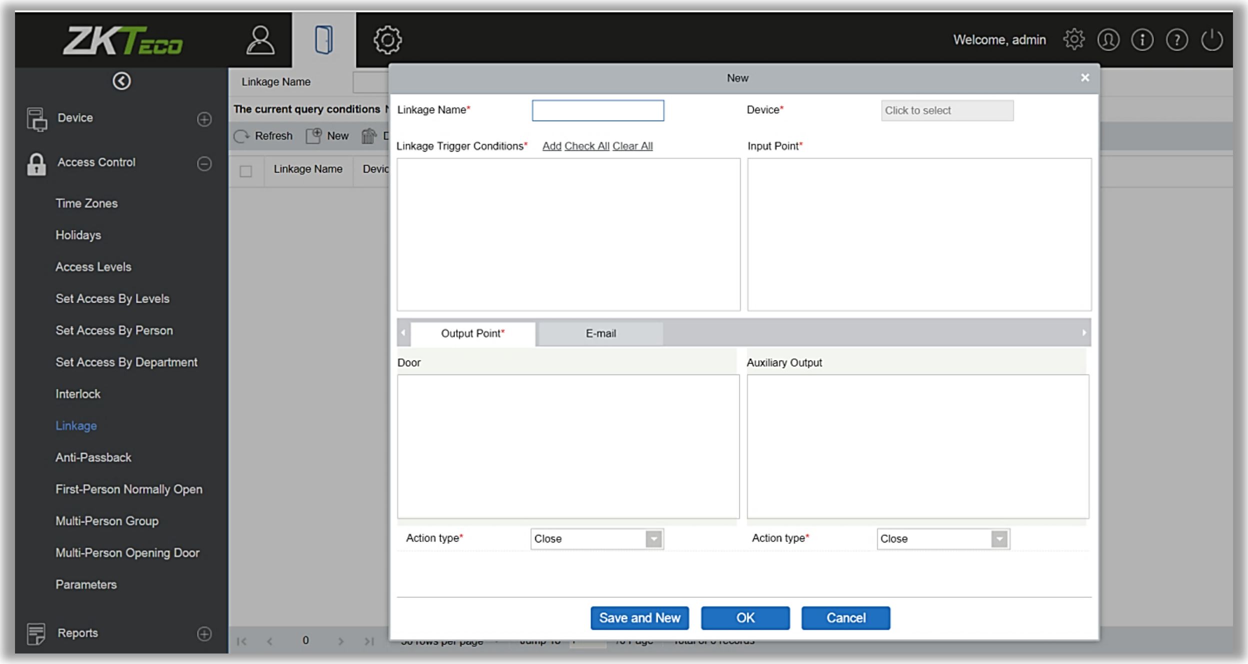
3. Select Interlock Rule, select an item, then click [OK] to complete. The new added interlock settings will be shown in the list.

✍**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:

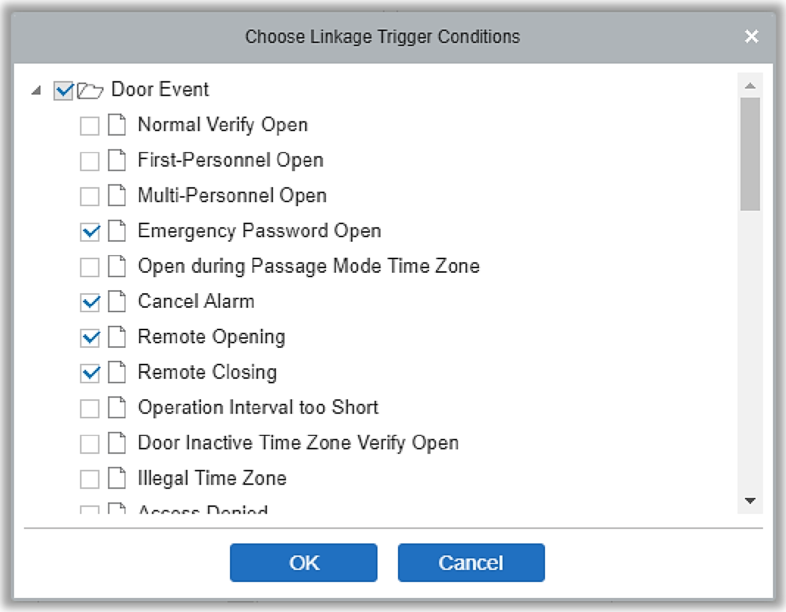


Action type* Close

Action type* Close

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.

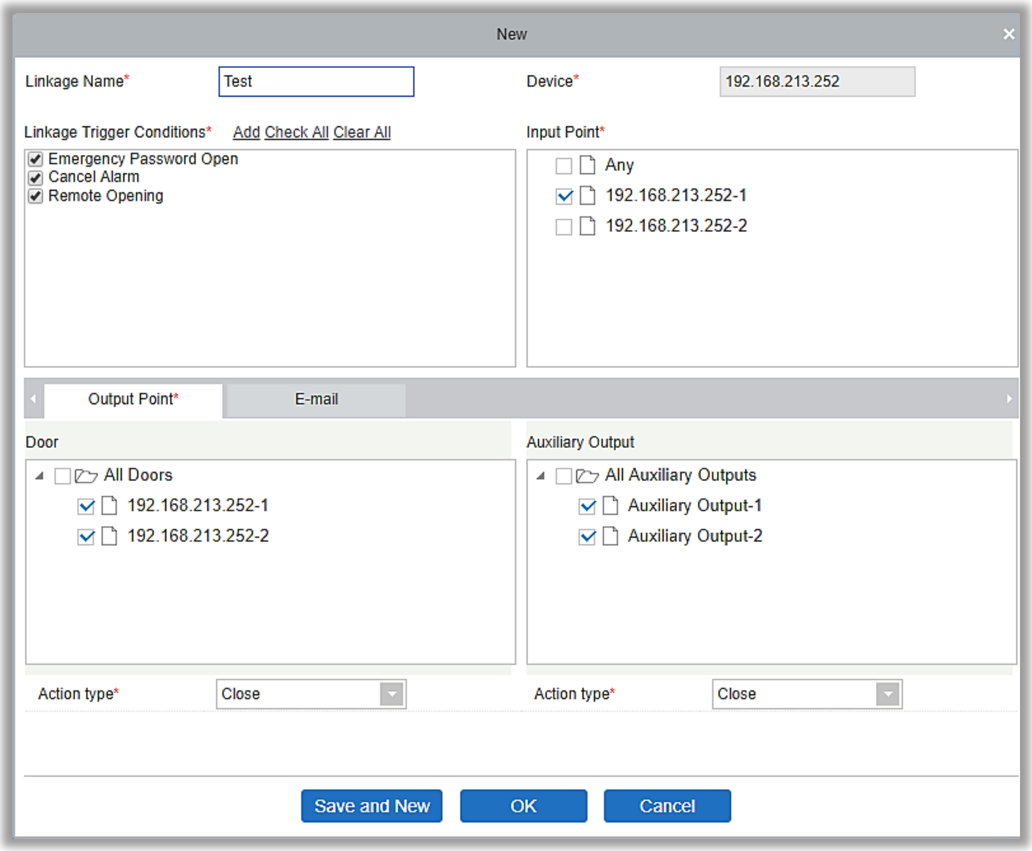
3. After selecting devices, corresponding linkage settings will be displayed. The System will first judge whether the device is successfully connected and reads extended parameters. If there are no available extended parameters, the system cannot set any linkage. If there is an available extended parameter(s), the system will show linkage settings according to the door quantity, auxiliary input and output quantity of currently selected device:



Choose Linkage Trigger Conditions

☑ Door Event
- □ Normal Verify Open
- □ First-Personnel Open
- □ Multi-Personnel Open
- ☑ Emergency Password Open
- □ Open during Passage Mode Time Zone
- ☑ Cancel Alarm
- ☑ Remote Opening
- ☑ Remote Closing
- □ Operation Interval too Short
- □ Door Inactive Time Zone Verify Open
- □ Illegal Time Zone
- □ Access Denied

✍**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.



New

Linkage Name*: Test

Device*: 192.168.213.252

Linkage Trigger Conditions* Add Check All Clear All
- ☑ Emergency Password Open
- ☑ Cancel Alarm
- ☑ Remote Opening

Input Point*
- □ Any
- ☑ 192.168.213.252-1
- □ 192.168.213.252-2

Door

□ All Doors
- ☑ 192.168.213.252-1
- ☑ 192.168.213.252-2

Auxiliary Output

□ All Auxiliary Outputs
- ☑ Auxiliary Output-1
- ☑ Auxiliary Output-2

Action type*: Close

Action type*: Close

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

The fields are as follows:

Linkage Name: Set a linkage name.

Linkage Trigger Condition: It contains trigger conditions for Door and Auxiliary input. These conditions trigger the event type of selected device. All events could be trigger condition.

Input Point: Select appropriate triggering input point (the specific input point please refers to specific device parameters).

Output Point: Select required output point (the specific output point please refers to specific device parameters).

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

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, and 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.

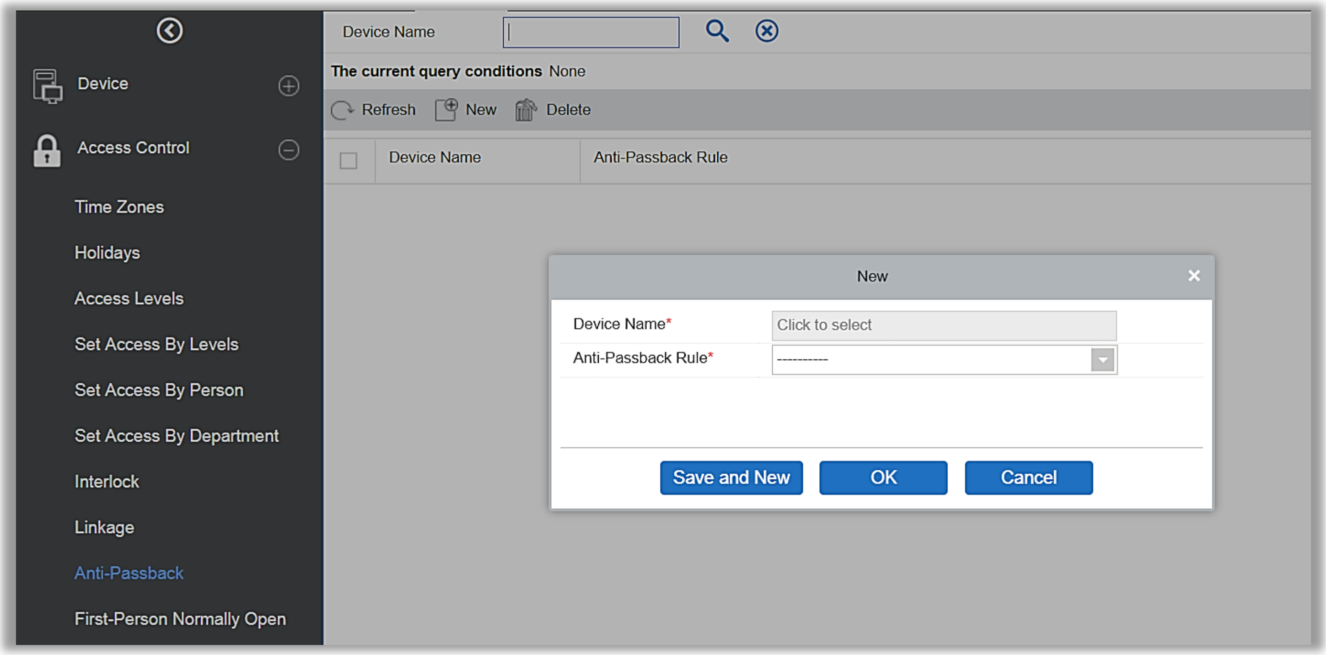
In addition, same linkage setting at input point and output point is not allowed. The same device permits consecutive logical linkage settings. The system allows to set several trigger conditions for a linkage setting at a time.

### 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 door 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:



Device Name* Click to select

Anti-Passback Rule* ----------

2. Select the required device(s). When 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 **connects** 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 select 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

This function helps to keep the door open for a specific time interval after the first verification by a assigned personnel.

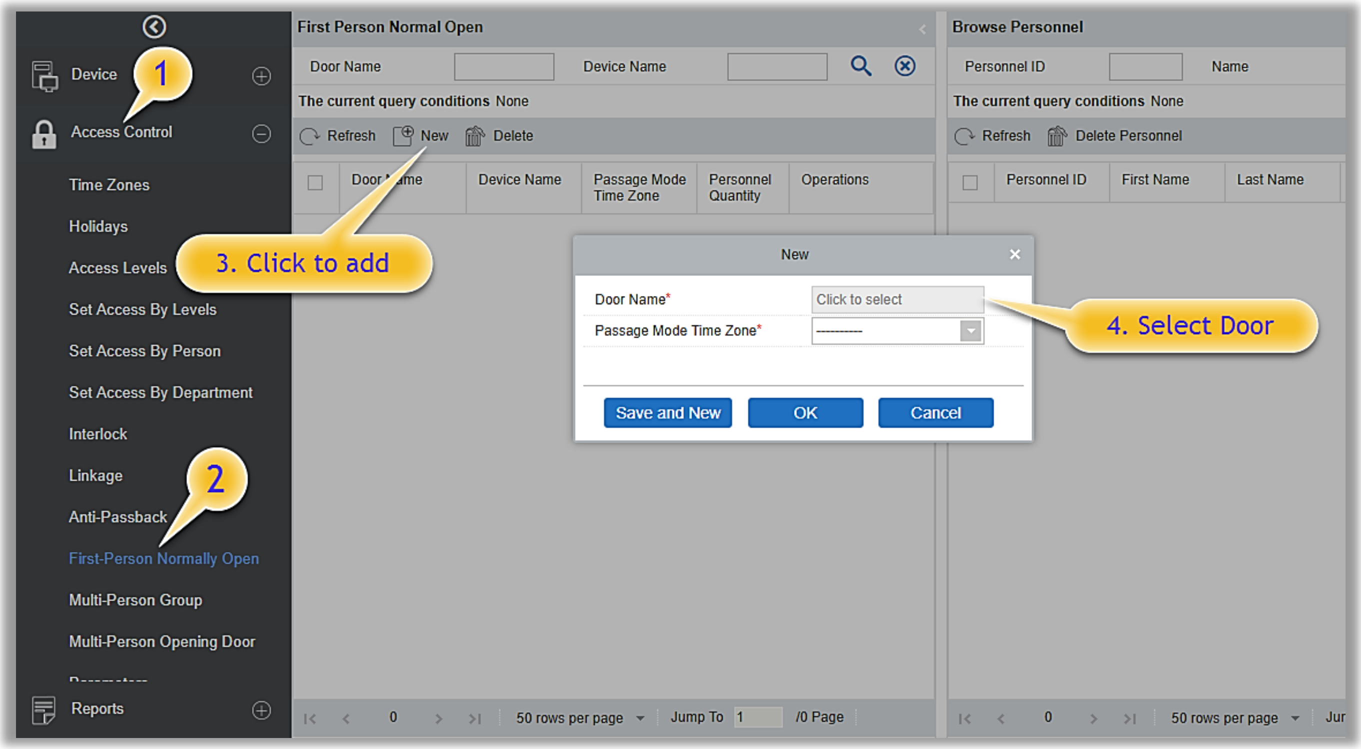
During a specified interval, If the first verification is by a person having First-Person Normally Open level access, then the door will be Normal Open, and will automatically restore closing after the valid interval has expired.

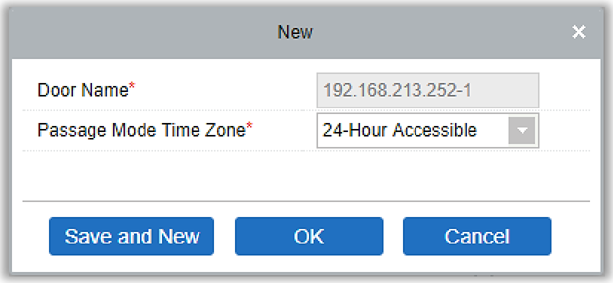
Users can set First-Person Normally Open for a specific door (the settings include door, door opening time zone and personnel with First-Person Normally Open level). A door can set First-Person Normally Open for multiple time zones. The interface of each door will show the number of existing First-Person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

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



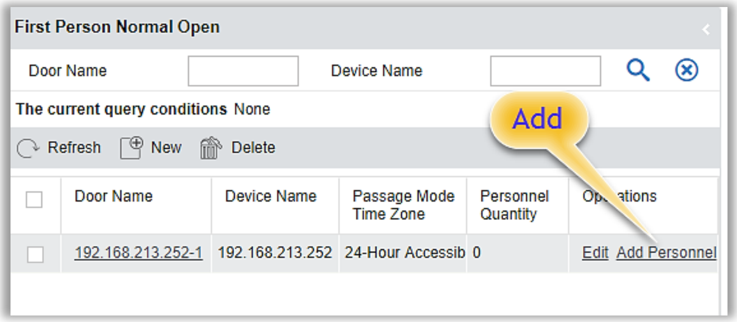


New

Door Name* 192.168.213.252-1

Passage Mode Time Zone* 24-Hour Accessible

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.



First Person Normal Open

Door Name | Device Name

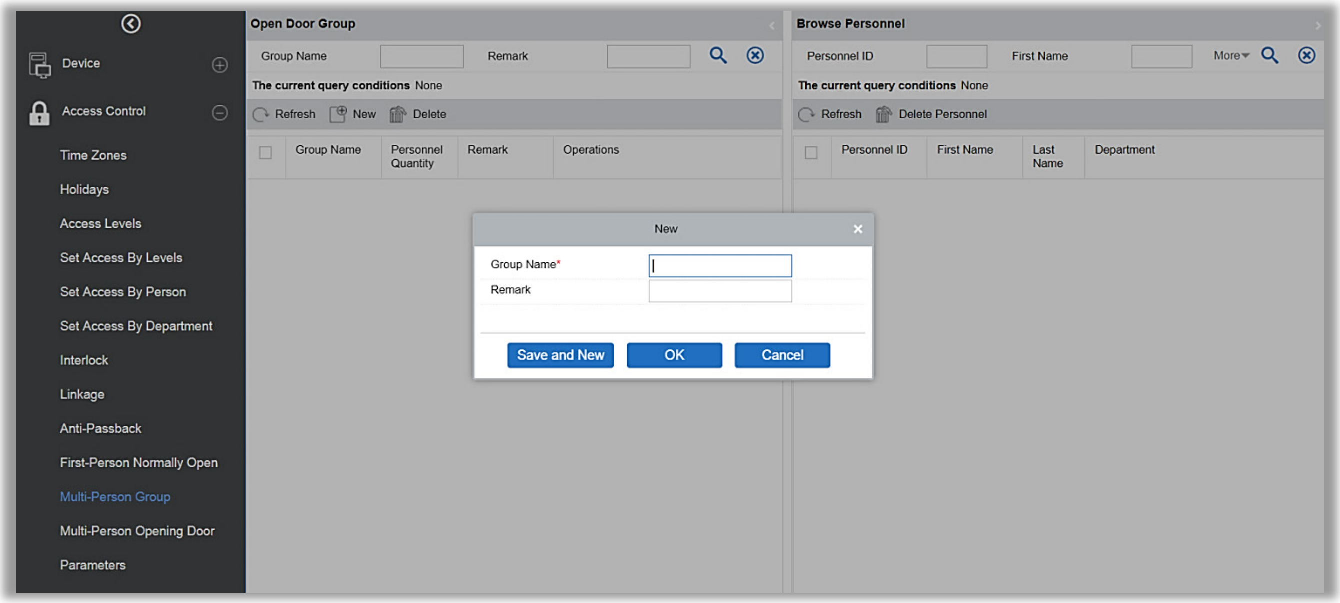
The current query conditions None

| □ | Door Name | Device Name | Passage Mode Time Zone | Personnel Quantity | Operations |
|---|---|---|---|---|---|
| □ | 192.168.213.252-1 | 192.168.213.252 | 24-Hour Accessib | 0 | Edit Add Personnel |

## 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 any other valid combination) will interrupt the procedure and you need to wait for 10 seconds to restart verification. The door cannot be opened by verifying using just one of the combinations.

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



Open Door Group

Group Name | Remark

The current query conditions None

| □ | Group Name | Personnel Quantity | Remark | Operations |
|---|---|---|---|---|

Browse Personnel

Personnel ID | First Name | More

The current query conditions None

| □ | Personnel ID | First Name | Last Name | Department |
|---|---|---|---|---|

New

Group Name*

Remark

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 a part of only one group.

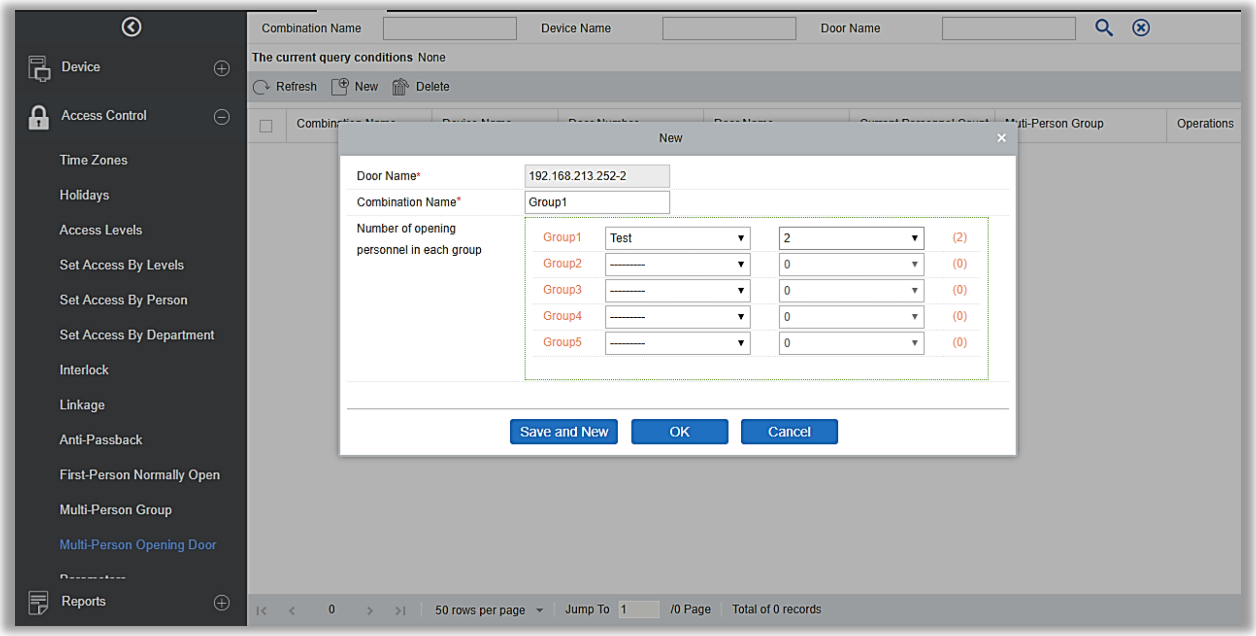
## 4.2.12 Multi-Person Opening Door

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]:



The current query conditions None

New

Door Name* 192.168.213.252-2

Combination Name* Group1

Number of opening personnel in each group

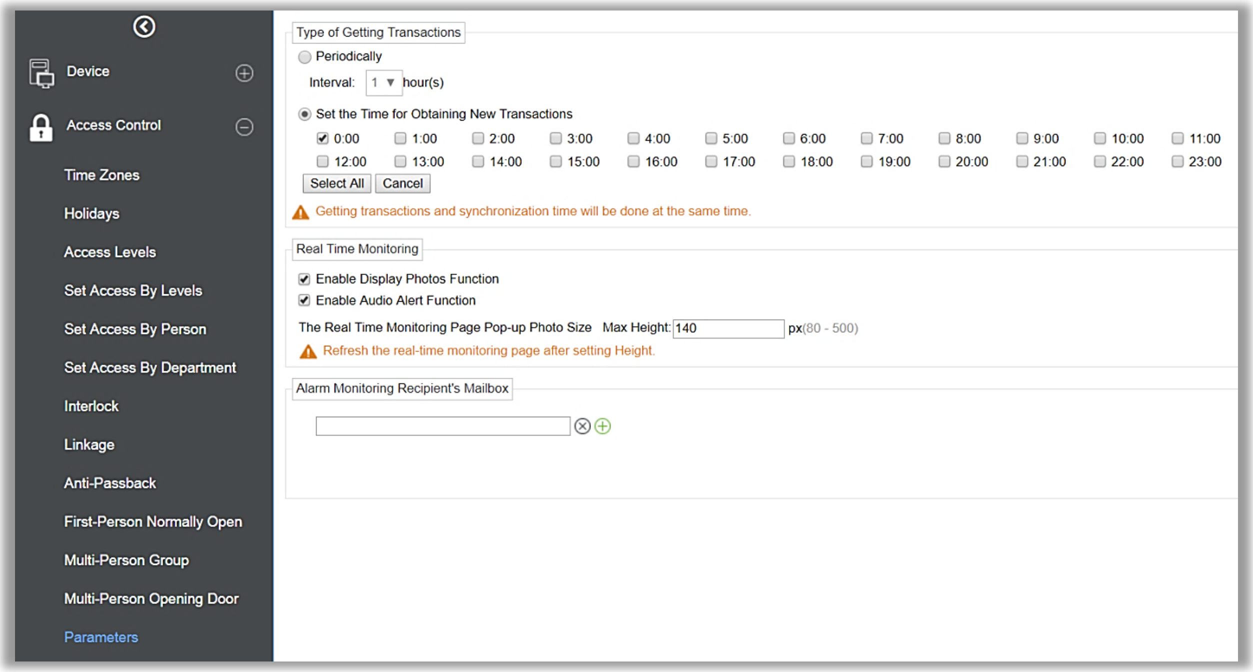
| | | | |
|---|---|---|---|
| Group1 | Test | 2 | (2) |
| Group2 | --------- | 0 | (0) |
| Group3 | --------- | 0 | (0) |
| Group4 | --------- | 0 | (0) |
| Group5 | --------- | 0 | (0) |

(2) The maximum number of Multi-Person Opening Door people for combined door opening is 5. Numbers in the brackets shows 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 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 Parameters

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



Type of Getting Transactions

○ Periodically

Interval: 1 ▼ hour(s)

● Set the Time for Obtaining New Transactions

☑ 0:00 □ 1:00 □ 2:00 □ 3:00 □ 4:00 □ 5:00 □ 6:00 □ 7:00 □ 8:00 □ 9:00 □ 10:00 □ 11:00

□ 12:00 □ 13:00 □ 14:00 □ 15:00 □ 16:00 □ 17:00 □ 18:00 □ 19:00 □ 20:00 □ 21:00 □ 22:00 □ 23:00

⚠ Getting transactions and synchronization time will be done at the same time.

Real Time Monitoring

☑ Enable Display Photos Function

☑ Enable Audio Alert Function

The Real Time Monitoring Page Pop-up Photo Size Max Height: 140 px(80 - 500)

⚠ Refresh the real-time monitoring page after setting Height.

Alarm Monitoring Recipient's Mailbox

- Type of Getting Transactions

- Periodically

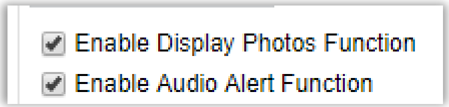
The system will download new transactions at the selected time interval.

- Set the Time for Obtaining New Transactions

The system will download new transactions automatically at the selected time instances.

- The Real Time Monitoring

You can select the checkbox accordingly.



☑ Enable Display Photos Function

☑ Enable Audio Alert Function

If the display photo is selected, the real-time monitoring page will display the personnel photo during an access control event. You can set the quality of image as required, the more px value will give more clearer photo.

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

## 4.3 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.

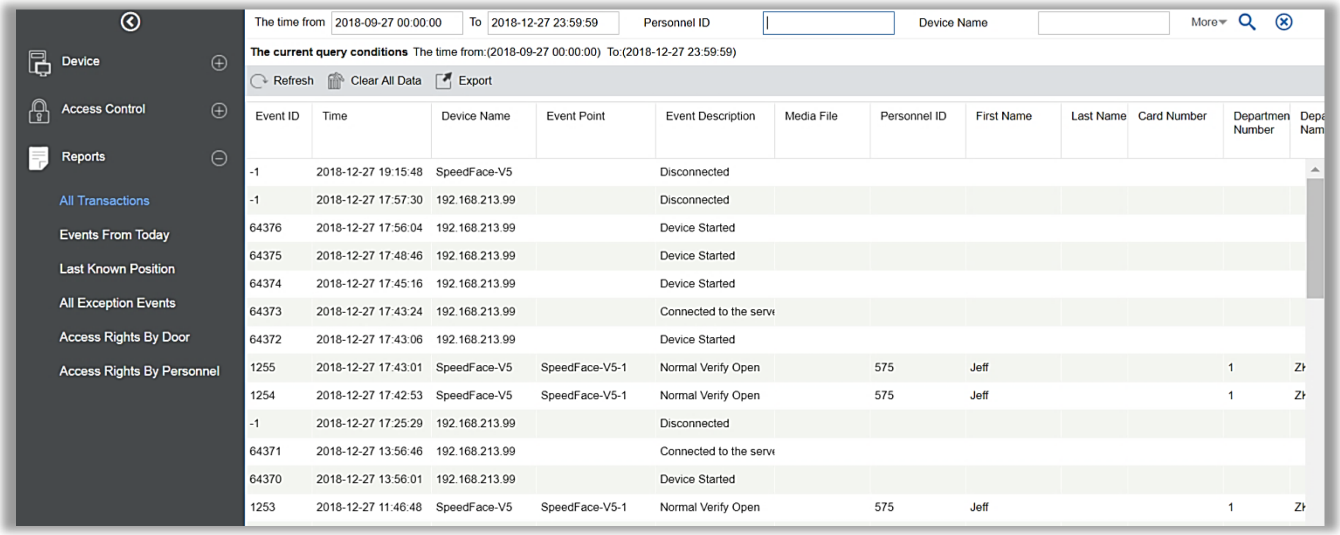
About the Normal and abnormal event please refer to Real-Time Monitoring for details.

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.

### 4.3.1 All Transactions

Because the data quantity of access control event records is more, 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:



The time from 2018-09-27 00:00:00 To 2018-12-27 23:59:59 Personnel ID Device Name

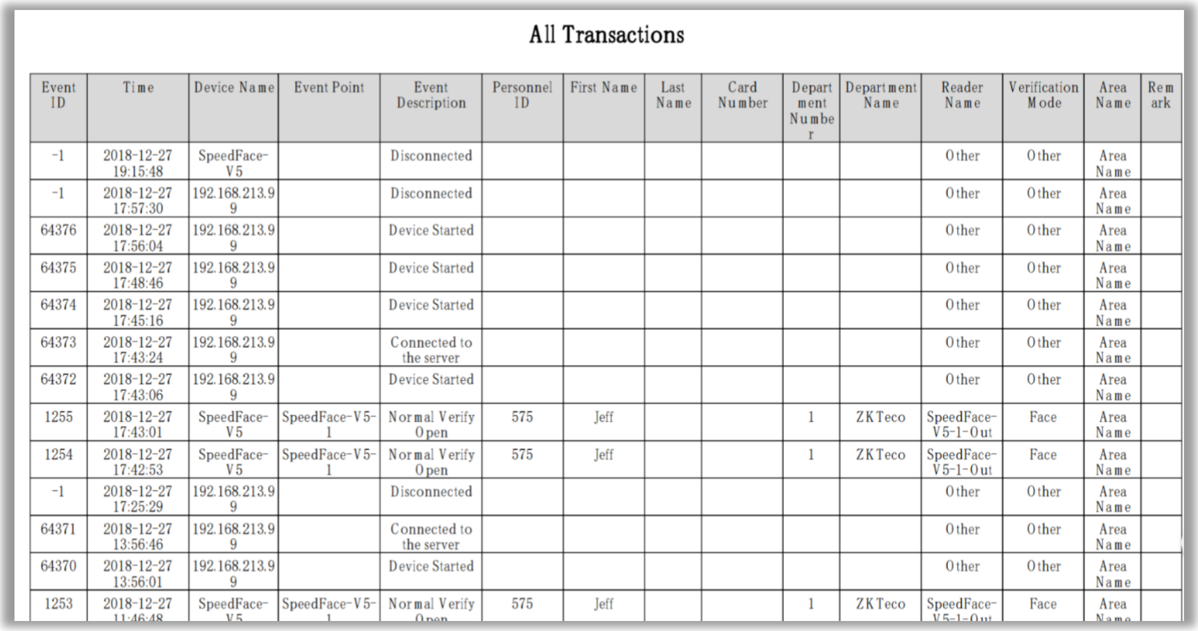
**The current query conditions** The time from:(2018-09-27 00:00:00) To:(2018-12-27 23:59:59)

| Event ID | Time | Device Name | Event Point | Event Description | Media File | Personnel ID | First Name | Last Name | Card Number | Departmen Number | Depa Nam |
|---|---|---|---|---|---|---|---|---|---|---|---|
| -1 | 2018-12-27 19:15:48 | SpeedFace-V5 | | Disconnected | | | | | | | |
| -1 | 2018-12-27 17:57:30 | 192.168.213.99 | | Disconnected | | | | | | | |
| 64376 | 2018-12-27 17:56:04 | 192.168.213.99 | | Device Started | | | | | | | |
| 64375 | 2018-12-27 17:48:46 | 192.168.213.99 | | Device Started | | | | | | | |
| 64374 | 2018-12-27 17:45:16 | 192.168.213.99 | | Device Started | | | | | | | |
| 64373 | 2018-12-27 17:43:24 | 192.168.213.99 | | Connected to the serve | | | | | | | |
| 64372 | 2018-12-27 17:43:06 | 192.168.213.99 | | Device Started | | | | | | | |
| 1255 | 2018-12-27 17:43:01 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | | 575 | Jeff | | | 1 | Zh |
| 1254 | 2018-12-27 17:42:53 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | | 575 | Jeff | | | 1 | Zh |
| -1 | 2018-12-27 17:25:29 | 192.168.213.99 | | Disconnected | | | | | | | |
| 64371 | 2018-12-27 13:56:46 | 192.168.213.99 | | Connected to the serve | | | | | | | |
| 64370 | 2018-12-27 13:56:01 | 192.168.213.99 | | Device Started | | | | | | | |
| 1253 | 2018-12-27 11:46:48 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | | 575 | Jeff | | | 1 | Zh |

Media File: You can view or download the photos and videos.

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.



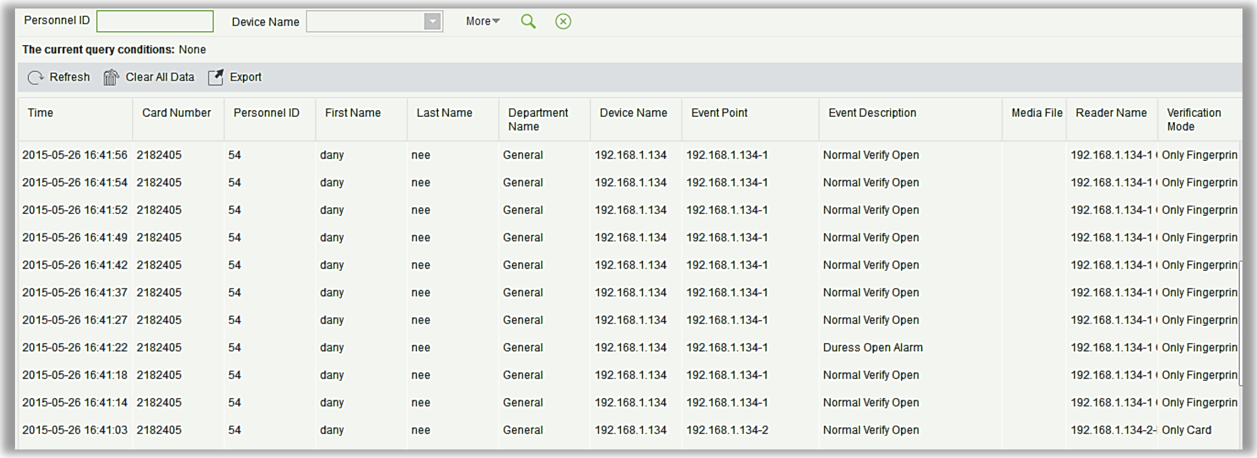
All Transactions

| Event ID | Time | Device Name | Event Point | Event Description | Personnel ID | First Name | Last Name | Card Number | Department Number | Department Name | Reader Name | Verification Mode | Area Name | Remark |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -1 | 2018-12-27 19:15:48 | SpeedFace-V5 | | Disconnected | | | | | | | Other | Other | Area Name | |
| -1 | 2018-12-27 17:57:30 | 192.168.213.99 | | Disconnected | | | | | | | Other | Other | Area Name | |
| 64376 | 2018-12-27 17:56:04 | 192.168.213.99 | | Device Started | | | | | | | Other | Other | Area Name | |
| 64375 | 2018-12-27 17:48:46 | 192.168.213.99 | | Device Started | | | | | | | Other | Other | Area Name | |
| 64374 | 2018-12-27 17:45:16 | 192.168.213.99 | | Device Started | | | | | | | Other | Other | Area Name | |
| 64373 | 2018-12-27 17:43:24 | 192.168.213.99 | | Connected to the server | | | | | | | Other | Other | Area Name | |
| 64372 | 2018-12-27 17:43:06 | 192.168.213.99 | | Device Started | | | | | | | Other | Other | Area Name | |
| 1255 | 2018-12-27 17:43:01 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | 575 | Jeff | | | 1 | ZKTeco | SpeedFace-V5-1-Out | Face | Area Name | |
| 1254 | 2018-12-27 17:42:53 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | 575 | Jeff | | | 1 | ZKTeco | SpeedFace-V5-1-Out | Face | Area Name | |
| -1 | 2018-12-27 17:25:29 | 192.168.213.99 | | Disconnected | | | | | | | Other | Other | Area Name | |
| 64371 | 2018-12-27 13:56:46 | 192.168.213.99 | | Connected to the server | | | | | | | Other | Other | Area Name | |
| 64370 | 2018-12-27 13:56:01 | 192.168.213.99 | | Device Started | | | | | | | Other | Other | Area Name | |
| 1253 | 2018-12-27 11:46:48 | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | 575 | Jeff | | | 1 | ZKTeco | SpeedFace-V5-1-Out | Face | Area Name | |

## 4.3.2 Events from Today

Check out the system record today.

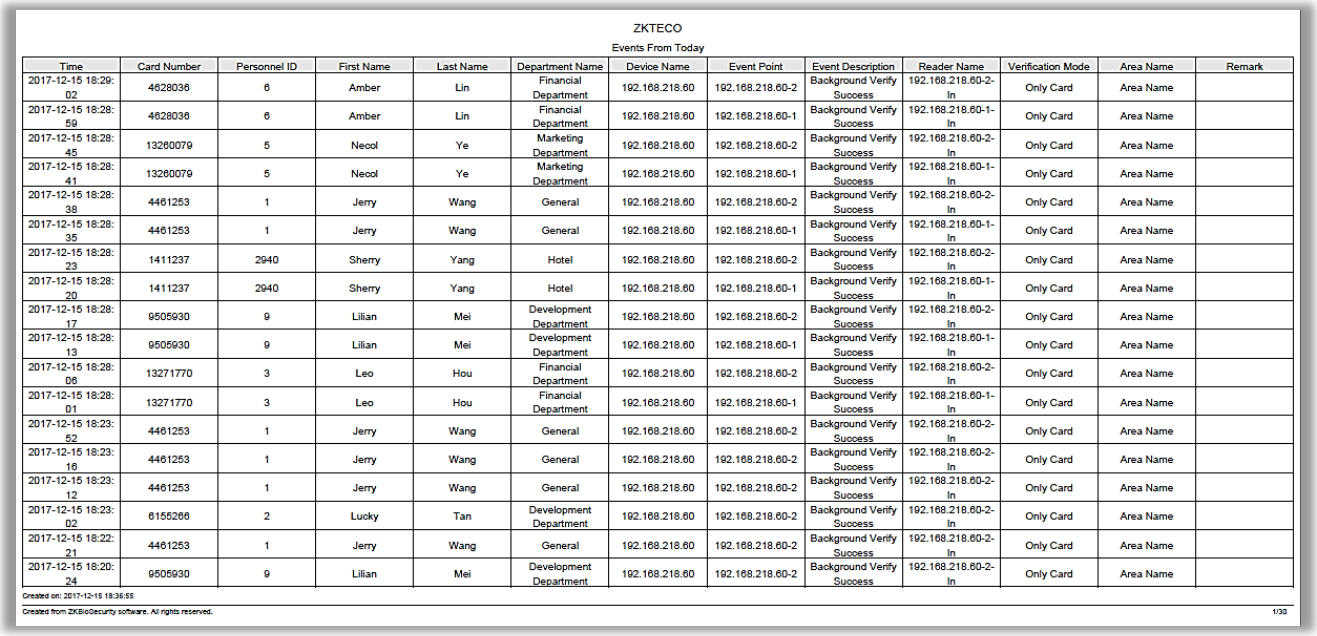
Click [Reports] > [Events from Today] to view today's records.



**The current query conditions:** None

| 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

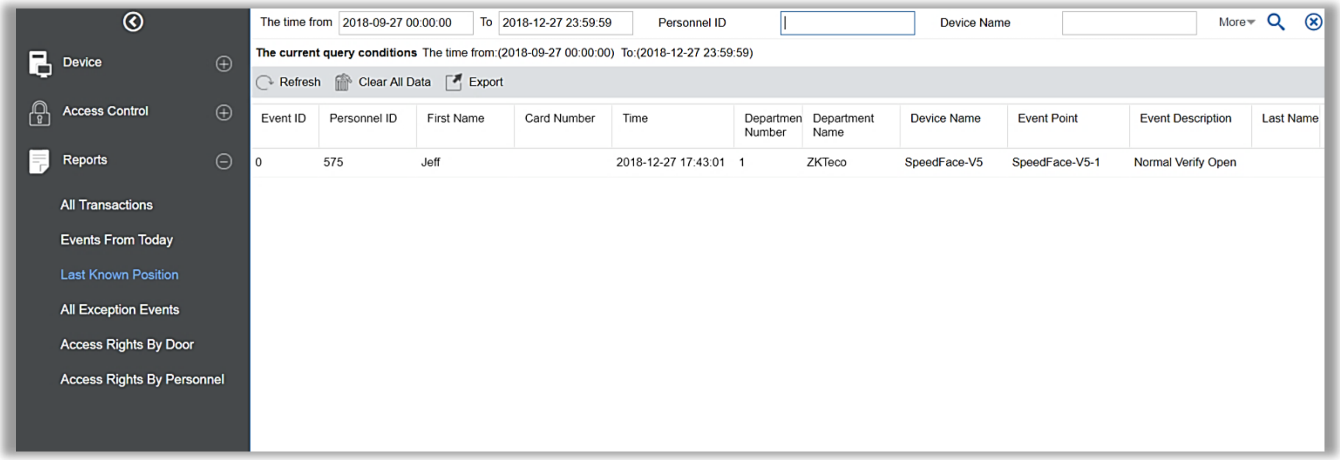
Created from ZKBioSecurity software. All rights reserved.

1/30

## 4.3.3 Last Known Position

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

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



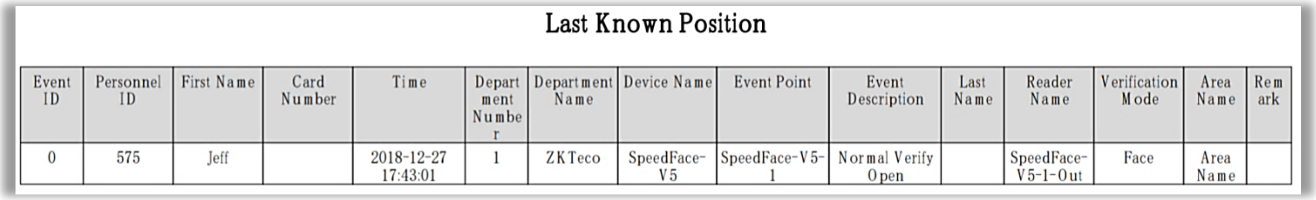
The time from 2018-09-27 00:00:00 To 2018-12-27 23:59:59 Personnel ID Device Name

**The current query conditions** The time from:(2018-09-27 00:00:00) To:(2018-12-27 23:59:59)

| Event ID | Personnel ID | First Name | Card Number | Time | Departmen Number | Department Name | Device Name | Event Point | Event Description | Last Name |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 575 | Jeff | | 2018-12-27 17:43:01 | 1 | ZKTeco | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | |

**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.

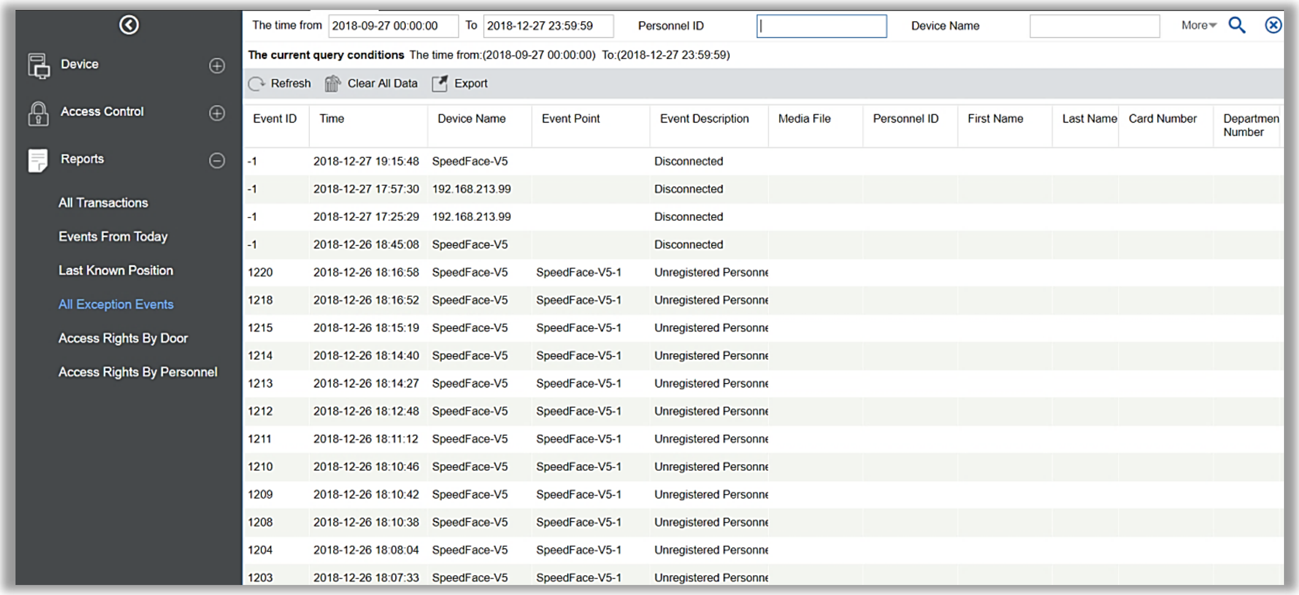


Last Known Position

| Event ID | Personnel ID | First Name | Card Number | Time | Department Number | Department Name | Device Name | Event Point | Event Description | Last Name | Reader Name | Verification Mode | Area Name | Remark |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 575 | Jeff | | 2018-12-27 17:43:01 | 1 | ZKTeco | SpeedFace-V5 | SpeedFace-V5-1 | Normal Verify Open | | SpeedFace-V5-1-Out | Face | Area Name | |

## 4.3.4 All Exception Events

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



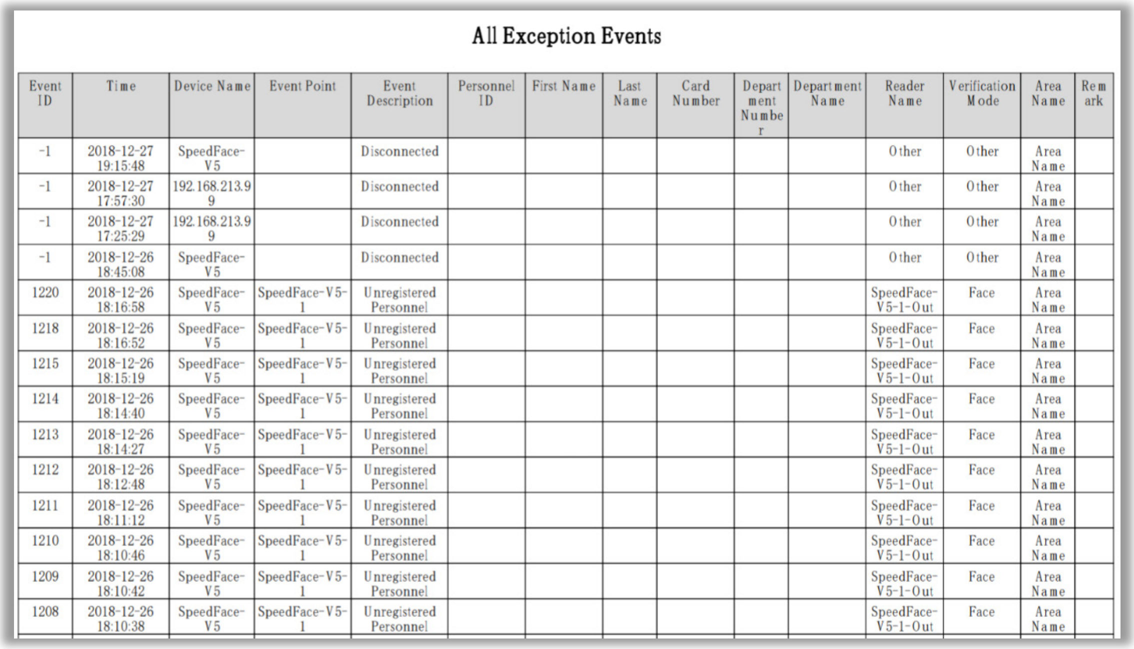
The time from 2018-09-27 00:00:00 To 2018-12-27 23:59:59 Personnel ID Device Name

**The current query conditions** The time from:(2018-09-27 00:00:00) To:(2018-12-27 23:59:59)

| Event ID | Time | Device Name | Event Point | Event Description | Media File | Personnel ID | First Name | Last Name | Card Number | Department Number |
|---|---|---|---|---|---|---|---|---|---|---|
| -1 | 2018-12-27 19:15:48 | SpeedFace-V5 | | Disconnected | | | | | | |
| -1 | 2018-12-27 17:57:30 | 192.168.213.99 | | Disconnected | | | | | | |
| -1 | 2018-12-27 17:25:29 | 192.168.213.99 | | Disconnected | | | | | | |
| -1 | 2018-12-26 18:45:08 | SpeedFace-V5 | | Disconnected | | | | | | |
| 1220 | 2018-12-26 18:16:58 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1218 | 2018-12-26 18:16:52 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1215 | 2018-12-26 18:15:19 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1214 | 2018-12-26 18:14:40 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1213 | 2018-12-26 18:14:27 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1212 | 2018-12-26 18:12:48 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1211 | 2018-12-26 18:11:12 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1210 | 2018-12-26 18:10:46 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1209 | 2018-12-26 18:10:42 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1208 | 2018-12-26 18:10:38 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1204 | 2018-12-26 18:08:04 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |
| 1203 | 2018-12-26 18:07:33 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personne | | | | | | |

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.

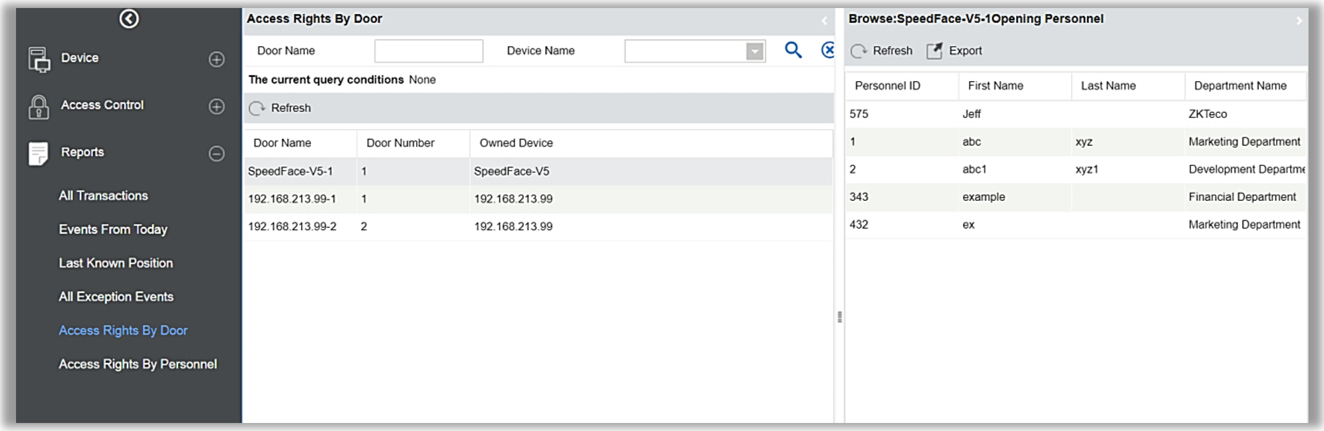


All Exception Events

| Event ID | Time | Device Name | Event Point | Event Description | Personnel ID | First Name | Last Name | Card Number | Department Number | Department Name | Reader Name | Verification Mode | Area Name | Remark |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -1 | 2018-12-27 19:15:48 | SpeedFace-V5 | | Disconnected | | | | | | | Other | Other | Area Name | |
| -1 | 2018-12-27 17:57:30 | 192.168.213.99 | | Disconnected | | | | | | | Other | Other | Area Name | |
| -1 | 2018-12-27 17:25:29 | 192.168.213.99 | | Disconnected | | | | | | | Other | Other | Area Name | |
| -1 | 2018-12-26 18:45:08 | SpeedFace-V5 | | Disconnected | | | | | | | Other | Other | Area Name | |
| 1220 | 2018-12-26 18:16:58 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1218 | 2018-12-26 18:16:52 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1215 | 2018-12-26 18:15:19 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1214 | 2018-12-26 18:14:40 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1213 | 2018-12-26 18:14:27 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1212 | 2018-12-26 18:12:48 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1211 | 2018-12-26 18:11:12 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1210 | 2018-12-26 18:10:46 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1209 | 2018-12-26 18:10:42 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |
| 1208 | 2018-12-26 18:10:38 | SpeedFace-V5 | SpeedFace-V5-1 | Unregistered Personnel | | | | | | | SpeedFace-V5-1-Out | Face | Area Name | |

## 4.3.5 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.



Access Rights By Door

Door Name  Device Name

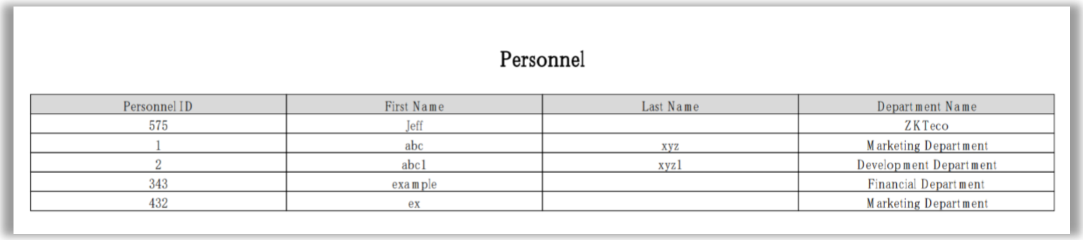
The current query conditions None

| Door Name | Door Number | Owned Device |
|---|---|---|
| SpeedFace-V5-1 | 1 | SpeedFace-V5 |
| 192.168.213.99-1 | 1 | 192.168.213.99 |
| 192.168.213.99-2 | 2 | 192.168.213.99 |

Browse:SpeedFace-V5-1Opening Personnel

| Personnel ID | First Name | Last Name | Department Name |
|---|---|---|---|
| 575 | Jeff | | ZKTeco |
| 1 | abc | xyz | Marketing Department |
| 2 | abc1 | xyz1 | Development Departme |
| 343 | example | | Financial Department |
| 432 | ex | | Marketing Department |

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



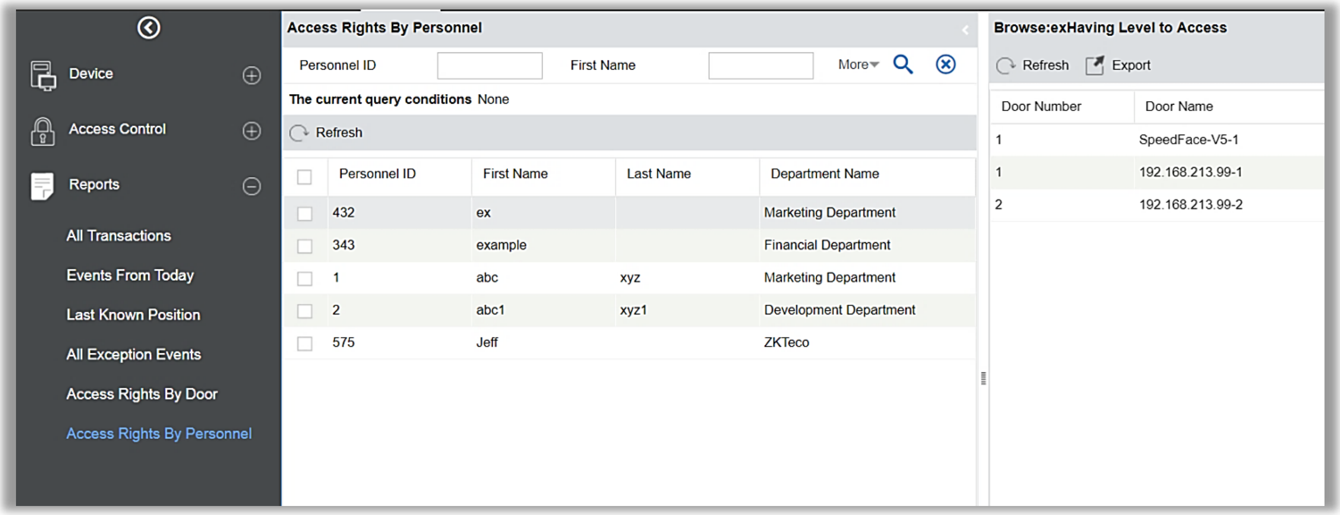
Personnel

| Personnel ID | First Name | Last Name | Department Name |
|---|---|---|---|
| 575 | Jeff | | ZKTeco |
| 1 | abc | xyz | Marketing Department |
| 2 | abc1 | xyz1 | Development Department |
| 343 | example | | Financial Department |
| 432 | ex | | Marketing Department |

## 4.3.6 Access Rights By Personnel

View related access levels 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.

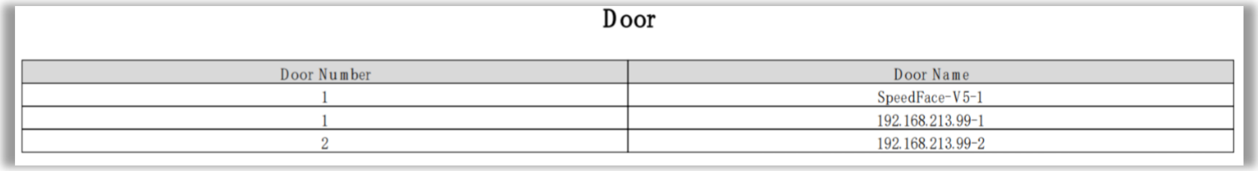


The current query conditions None

| □ | Personnel ID | First Name | Last Name | Department Name |
|---|---|---|---|---|
| □ | 432 | ex | | Marketing Department |
| □ | 343 | example | | Financial Department |
| □ | 1 | abc | xyz | Marketing Department |
| □ | 2 | abc1 | xyz1 | Development Department |
| □ | 575 | Jeff | | ZKTeco |

| Door Number | Door Name |
|---|---|
| 1 | SpeedFace-V5-1 |
| 1 | 192.168.213.99-1 |
| 2 | 192.168.213.99-2 |

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



Door

| Door Number | Door Name |
|---|---|
| 1 | SpeedFace-V5-1 |
| 1 | 192.168.213.99-1 |
| 2 | 192.168.213.99-2 |

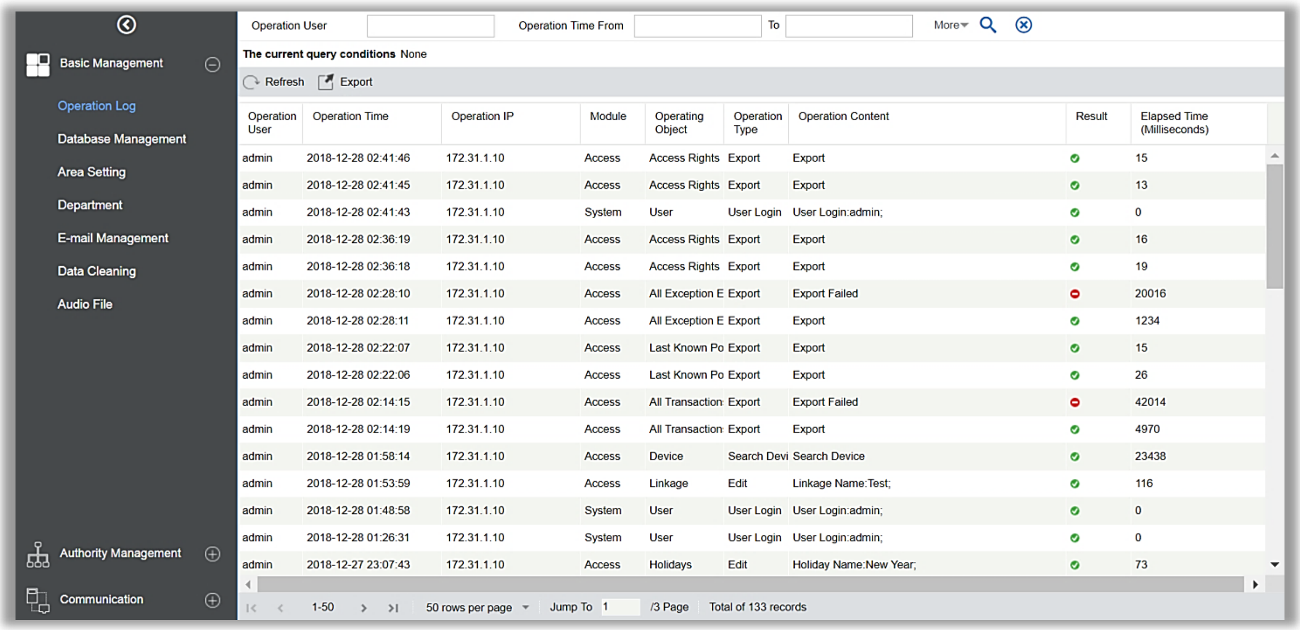
# 5. System Management

System settings primarily include assigning system users (such as company management user, administrator, access control administrator) and configuring the roles of corresponding modules, managing database, setting system parameters and view operation logs, etc.

## 5.1 Basic Management

### 5.1.1 Operation Logs

Click [System] > [Basic Management] > [Operation Log]:



Operation User | Operation Time From | To

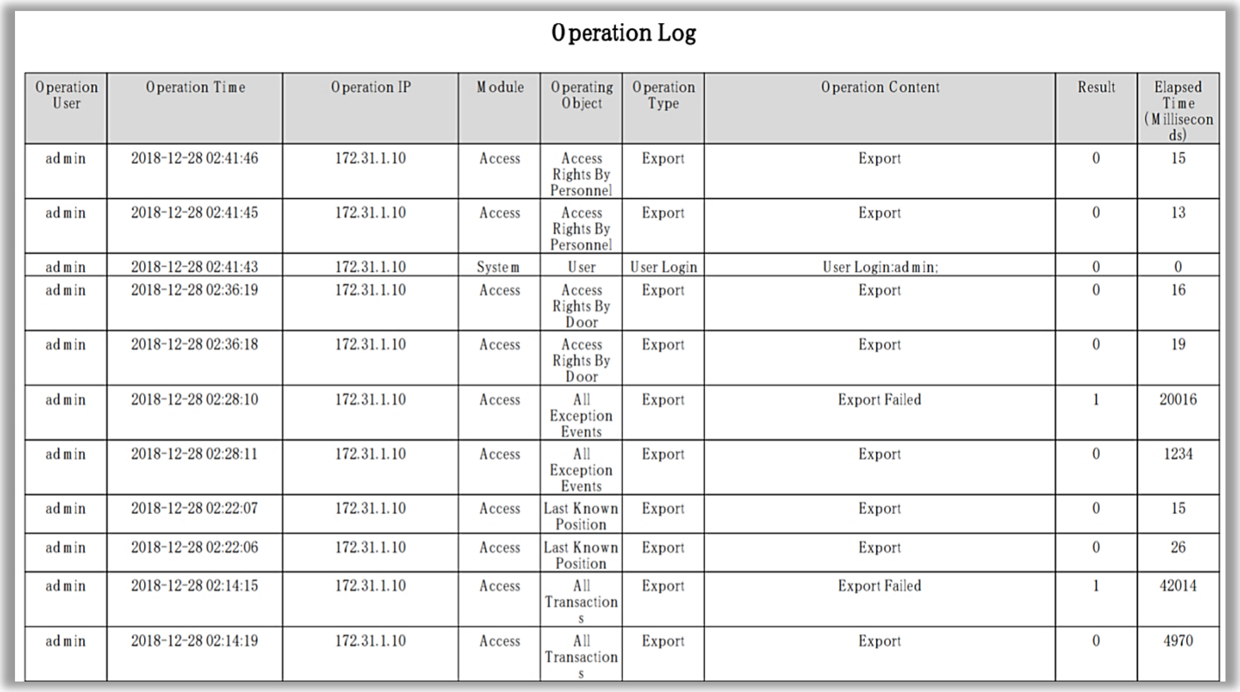
The current query conditions None

| Operation User | Operation Time | Operation IP | Module | Operating Object | Operation Type | Operation Content | Result | Elapsed Time (Milliseconds) |
|---|---|---|---|---|---|---|---|---|
| admin | 2018-12-28 02:41:46 | 172.31.1.10 | Access | Access Rights | Export | Export | ✓ | 15 |
| admin | 2018-12-28 02:41:45 | 172.31.1.10 | Access | Access Rights | Export | Export | ✓ | 13 |
| admin | 2018-12-28 02:41:43 | 172.31.1.10 | System | User | User Login | User Login:admin; | ✓ | 0 |
| admin | 2018-12-28 02:36:19 | 172.31.1.10 | Access | Access Rights | Export | Export | ✓ | 16 |
| admin | 2018-12-28 02:36:18 | 172.31.1.10 | Access | Access Rights | Export | Export | ✓ | 19 |
| admin | 2018-12-28 02:28:10 | 172.31.1.10 | Access | All Exception E | Export | Export Failed | ⛔ | 20016 |
| admin | 2018-12-28 02:28:11 | 172.31.1.10 | Access | All Exception E | Export | Export | ✓ | 1234 |
| admin | 2018-12-28 02:22:07 | 172.31.1.10 | Access | Last Known Po | Export | Export | ✓ | 15 |
| admin | 2018-12-28 02:22:06 | 172.31.1.10 | Access | Last Known Po | Export | Export | ✓ | 26 |
| admin | 2018-12-28 02:14:15 | 172.31.1.10 | Access | All Transaction | Export | Export Failed | ⛔ | 42014 |
| admin | 2018-12-28 02:14:19 | 172.31.1.10 | Access | All Transaction | Export | Export | ✓ | 4970 |
| admin | 2018-12-28 01:58:14 | 172.31.1.10 | Access | Device | Search Devi | Search Device | ✓ | 23438 |
| admin | 2018-12-28 01:53:59 | 172.31.1.10 | Access | Linkage | Edit | Linkage Name:Test; | ✓ | 116 |
| admin | 2018-12-28 01:48:58 | 172.31.1.10 | System | User | User Login | User Login:admin; | ✓ | 0 |
| admin | 2018-12-28 01:26:31 | 172.31.1.10 | System | User | User Login | User Login:admin; | ✓ | 0 |
| admin | 2018-12-27 23:07:43 | 172.31.1.10 | Access | Holidays | Edit | Holiday Name:New Year; | ✓ | 73 |

1-50 | 50 rows per page | Jump To 1 /3 Page | Total of 133 records

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.

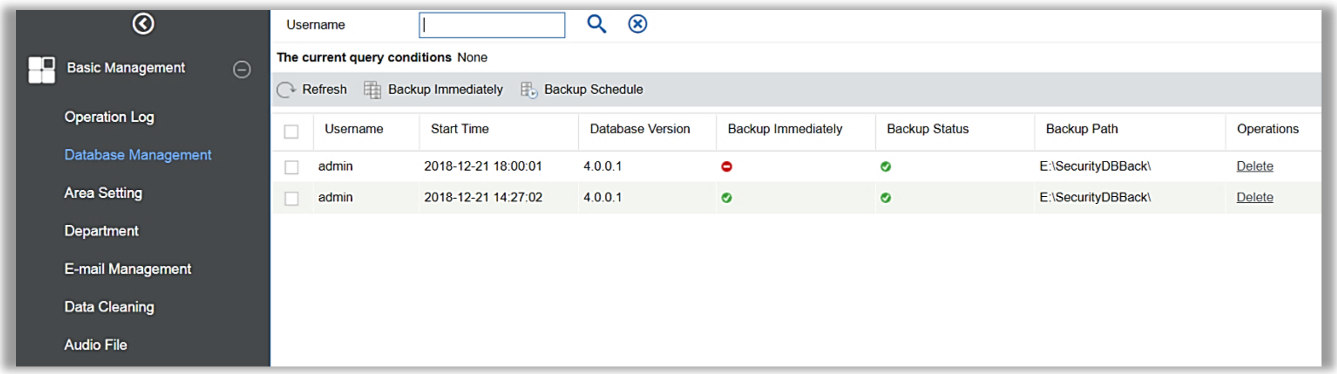


Operation Log

| Operation User | Operation Time | Operation IP | Module | Operating Object | Operation Type | Operation Content | Result | Elapsed Time (Milliseconds) |
|---|---|---|---|---|---|---|---|---|
| admin | 2018-12-28 02:41:46 | 172.31.1.10 | Access | Access Rights By Personnel | Export | Export | 0 | 15 |
| admin | 2018-12-28 02:41:45 | 172.31.1.10 | Access | Access Rights By Personnel | Export | Export | 0 | 13 |
| admin | 2018-12-28 02:41:43 | 172.31.1.10 | System | User | User Login | User Login:admin; | 0 | 0 |
| admin | 2018-12-28 02:36:19 | 172.31.1.10 | Access | Access Rights By Door | Export | Export | 0 | 16 |
| admin | 2018-12-28 02:36:18 | 172.31.1.10 | Access | Access Rights By Door | Export | Export | 0 | 19 |
| admin | 2018-12-28 02:28:10 | 172.31.1.10 | Access | All Exception Events | Export | Export Failed | 1 | 20016 |
| admin | 2018-12-28 02:28:11 | 172.31.1.10 | Access | All Exception Events | Export | Export | 0 | 1234 |
| admin | 2018-12-28 02:22:07 | 172.31.1.10 | Access | Last Known Position | Export | Export | 0 | 15 |
| admin | 2018-12-28 02:22:06 | 172.31.1.10 | Access | Last Known Position | Export | Export | 0 | 26 |
| admin | 2018-12-28 02:14:15 | 172.31.1.10 | Access | All Transactions | Export | Export Failed | 1 | 42014 |
| admin | 2018-12-28 02:14:19 | 172.31.1.10 | Access | All Transactions | Export | Export | 0 | 4970 |

## 5.1.2 Database Management

Click [System] > [Basic Management] > [Database Management]:



The current query conditions None

| □ | Username | Start Time | Database Version | Backup Immediately | Backup Status | Backup Path | Operations |
|---|---|---|---|---|---|---|---|
| □ | admin | 2018-12-21 18:00:01 | 4.0.0.1 | ⛔ | ✓ | E:\SecurityDBBack\ | Delete |
| □ | admin | 2018-12-21 14:27:02 | 4.0.0.1 | ✓ | ✓ | E:\SecurityDBBack\ | Delete |

History of database backup operation logs are displayed in this page. You can refresh, backup and schedule backup database as required.

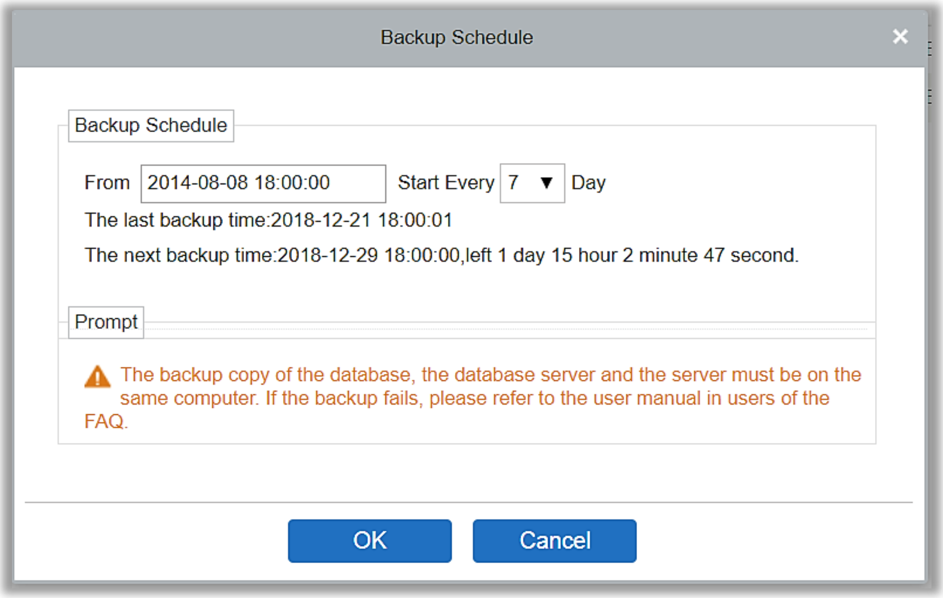
- **Backup Immediately**

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 ZKBioAccess Installation Guide.

- Backup Schedule

Click [Backup Schedule]:



Backup Schedule

Backup Schedule

From 2014-08-08 18:00:00 Start Every 7 Day

The last backup time:2018-12-21 18:00:01

The next backup time:2018-12-29 18:00:00,left 1 day 15 hour 2 minute 47 second.

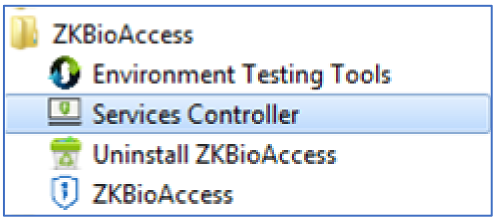
Prompt

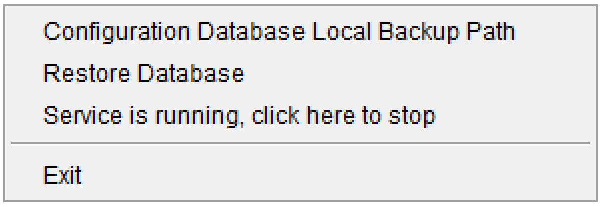
⚠ The backup copy of the database, the database server and the server must be on the same computer. If the backup fails, please refer to the user manual in users of the FAQ.

Set the start time, set interval between two automatic backups, click [OK].

- Restore Database

1. Click the start menu of the PC → [All Programs] → [ZKBioAccess] → 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".

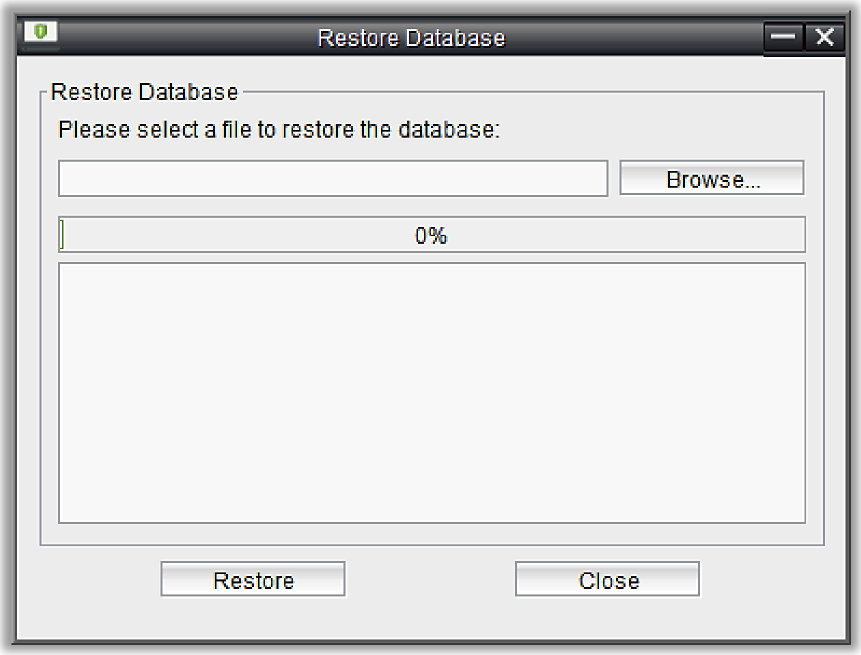




Configuration Database Local Backup Path
Restore Database
Service is running, click here to stop
Exit

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.



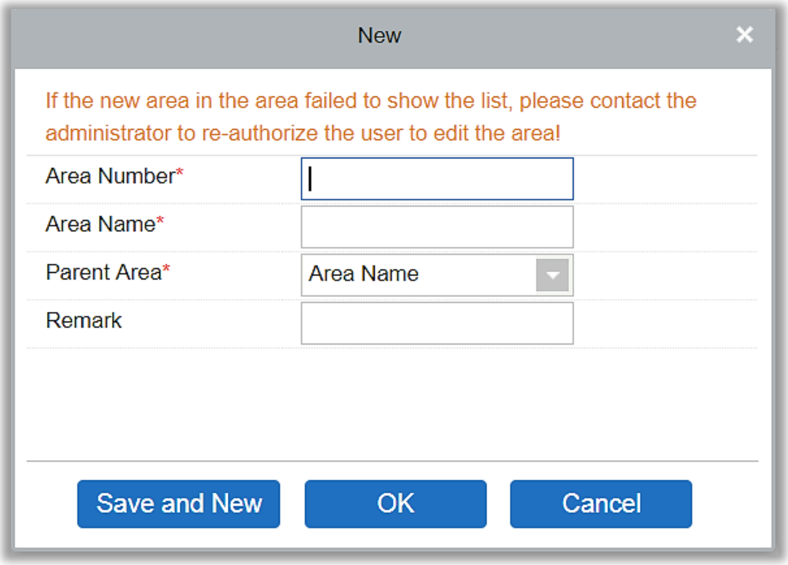
## 5.1.3 Area Setting

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 [Area Name] and numbered [1].

- Add an Area

Click [System] > [Area Setting] > [Area] > [New]:



If the new area in the area failed to show the list, please contact the administrator to re-authorize the user to edit the area!

|  |  |
|---|---|
| Area Number* |  |
| Area Name* |  |
| Parent Area* | Area Name |
| Remark |  |

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.

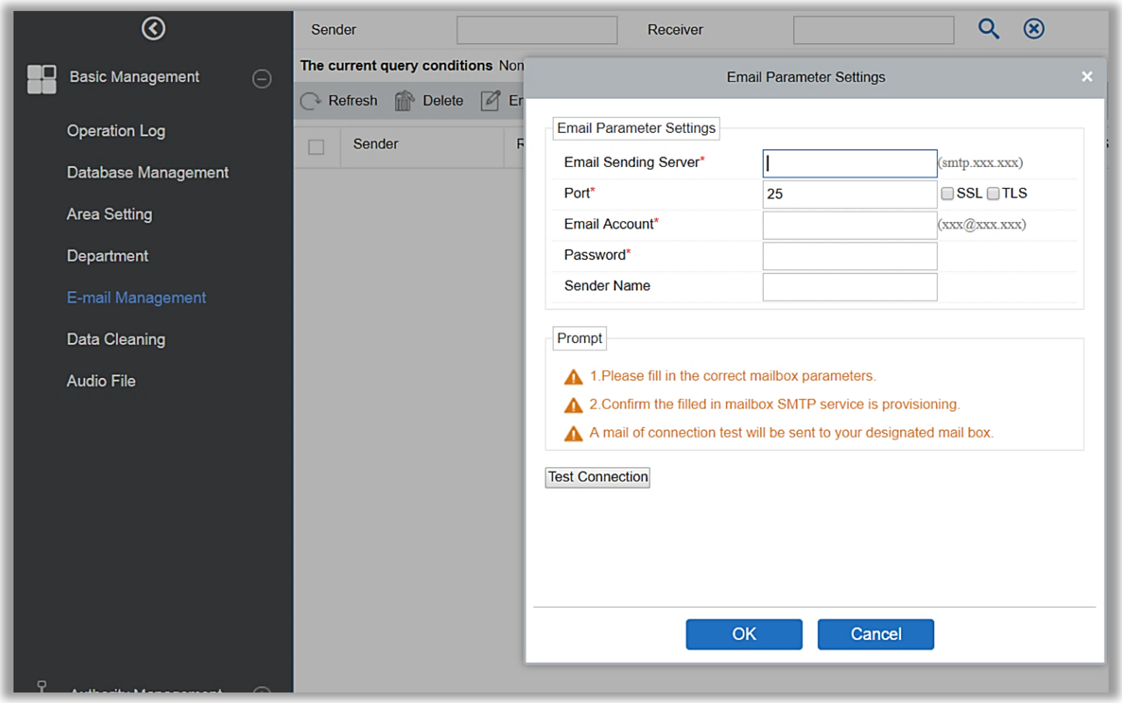
- Edit/Delete an Area

Click [Edit] or [Delete] as required.

### 5.1.4 E-mail Management

Set the email sending server information. The recipient Email should be set in Linkage Setting.

Click [Basic Management] > [Email Management] > [Email Parameter Settings]:



Email Sending Server* (smtp.xxx.xxx)

Port* 25 □SSL □TLS

Email Account* (xxx@xxx.xxx)

Password*

Sender Name

1.Please fill in the correct mailbox parameters.

2.Confirm the filled in mailbox SMTP service is provisioning.

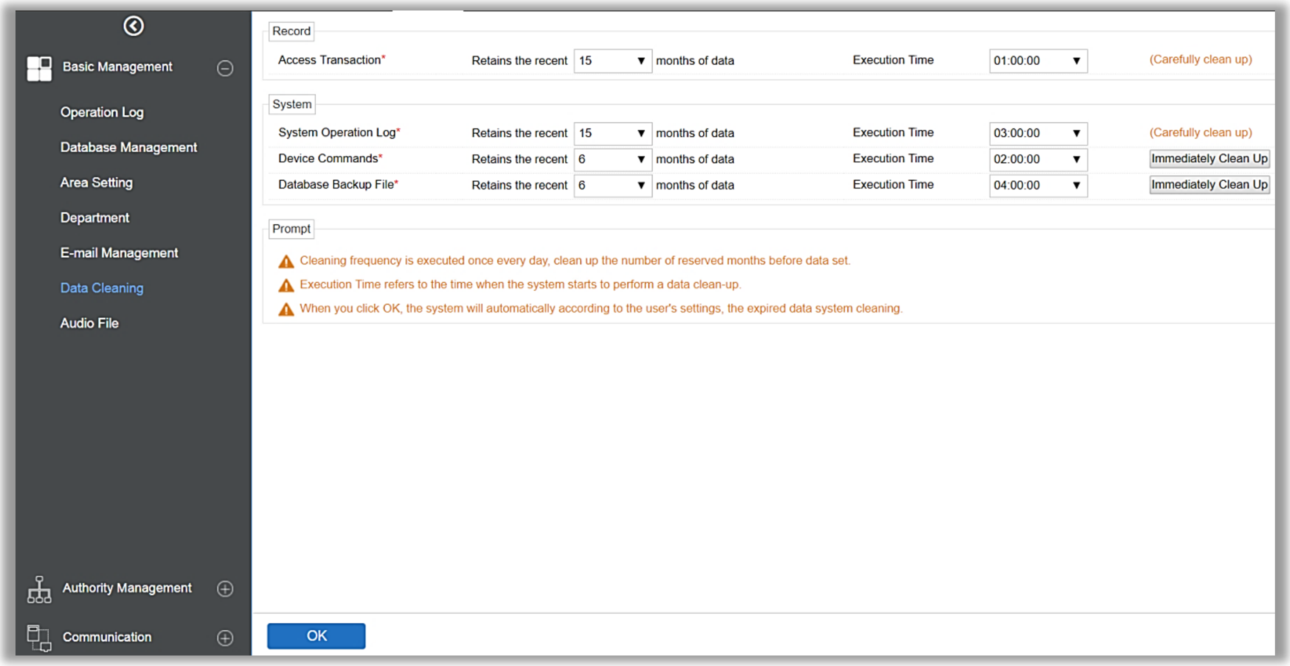
A mail of connection test will be sent to your designated mail box.

✍**Note:** The domain name of E-mail address and E-mail sending sever must be identical. For example, if the Email address is: test@gmail.com, then the E-mail sending sever must be: smtp.gmail.com.

### 5.1.5 Data Cleaning

The data cleaning time settings are available to set. The data volume increases with the use of the system. To save the storage space on the disks, you need to periodically clean old data generated by the system.

Click [Basic Management] > [Data Cleaning]:



Record

| | | | | | | |
|---|---|---|---|---|---|---|
| Access Transaction* | Retains the recent | 15 | months of data | Execution Time | 01:00:00 | (Carefully clean up) |

System

| | | | | | | |
|---|---|---|---|---|---|---|
| System Operation Log* | Retains the recent | 15 | months of data | Execution Time | 03:00:00 | (Carefully clean up) |
| Device Commands* | Retains the recent | 6 | months of data | Execution Time | 02:00:00 | Immediately Clean Up |
| Database Backup File* | Retains the recent | 6 | months of data | Execution Time | 04:00:00 | Immediately Clean Up |

Prompt

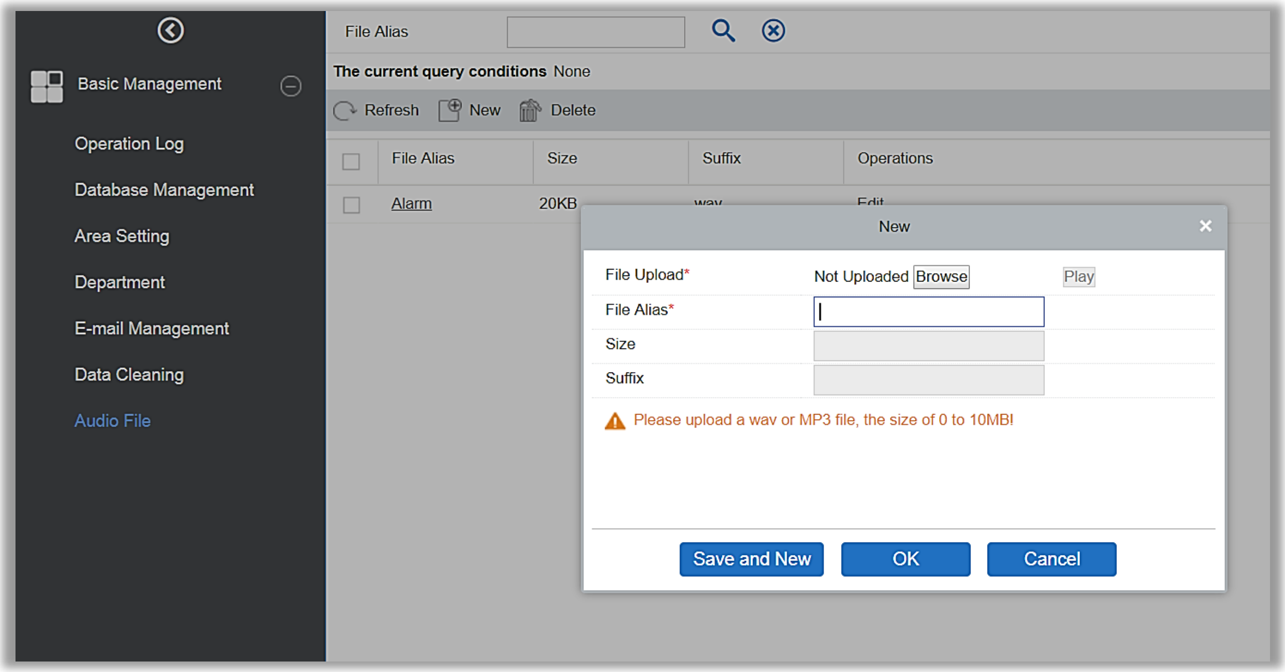
- Cleaning frequency is executed once every day, clean up the number of reserved months before data set.
- Execution Time refers to the time when the system starts to perform a data clean-up.
- When you click OK, the system will automatically according to the user's settings, the expired data system cleaning.

The system executes [Immediately Clean Up] operation after it is clicked and [OK] is clicked. Without clicking [OK], the system will not clean data.

✍**Note:** In order to reduce the load of the system and not to affect the normal running, the cleaning time should be set in the 1 o'clock am.

## 5.1.6 Audio File

Click [Basic Management] > [Audio File] > [New]:



File Alias

The current query conditions None

| File Alias | Size | Suffix | Operations |
|---|---|---|---|
| Alarm | 20KB | wav | Edit |

New

| | |
|---|---|
| File Upload* | Not Uploaded |
| File Alias* | |
| Size | |
| Suffix | |

Please upload a wav or MP3 file, the size of 0 to 10MB!

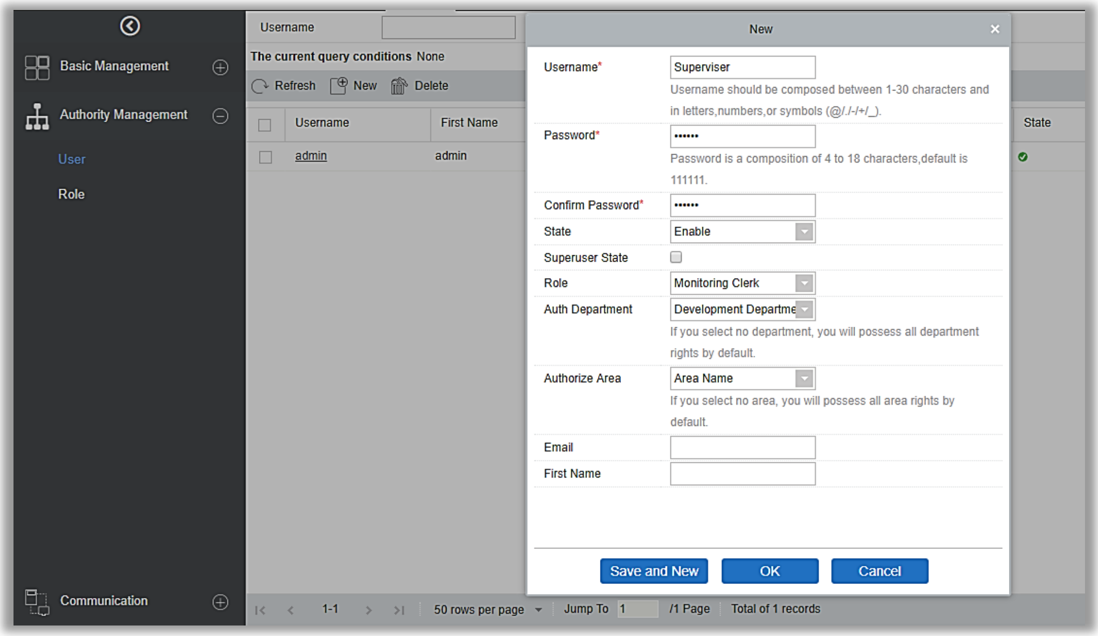
You can upload a sound from the local. The file must be in wav or mp3 format, and it must not exceed 10MB.

## 5.2 Authority Management

### 5.2.1 User

**Add new user and implement levels for the user in the system.**

1. Click [System Management] > [Authority Management] > [User] > [New]:



Username

The current query conditions None

| | Username | First Name | State |
|---|---|---|---|
| □ | admin | admin | ✓ |

1-1 | 50 rows per page | Jump To 1 /1 Page | Total of 1 records

New

Username*: Supervisor
Username should be composed between 1-30 characters and in letters,numbers,or symbols (@/.-/+/_).

Password*: ••••••
Password is a composition of 4 to 18 characters,default is 111111.

Confirm Password*: ••••••

State: Enable

Superuser State: □

Role: Monitoring Clerk

Auth Department: Development Departme
If you select no department, you will possess all department rights by default.

Authorize Area: Area Name
If you select no area, you will possess all area rights by default.

Email:

First Name:

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.

Super User State: Enable or disable the user to have the super user's levels.

Role: You need to define role as explained in Role.

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: Type your initials.

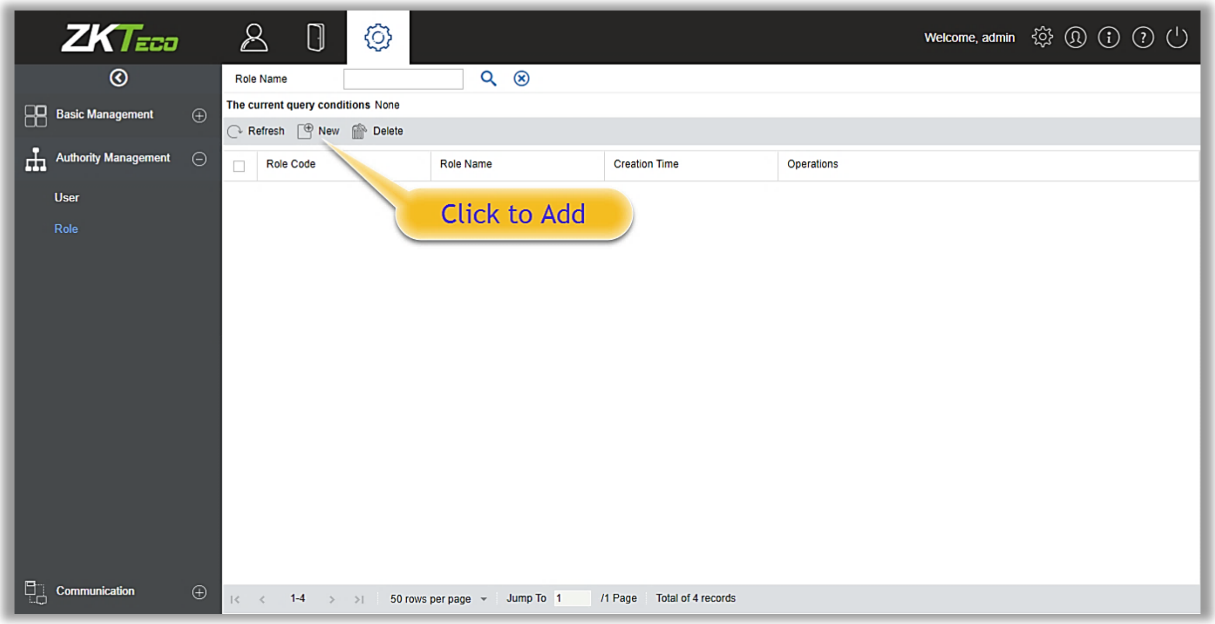
2. After editing, click [OK] to complete user adding, and the user will be shown in the list.

Click [Edit] or [Delete] as required.

### 5.2.2 Role

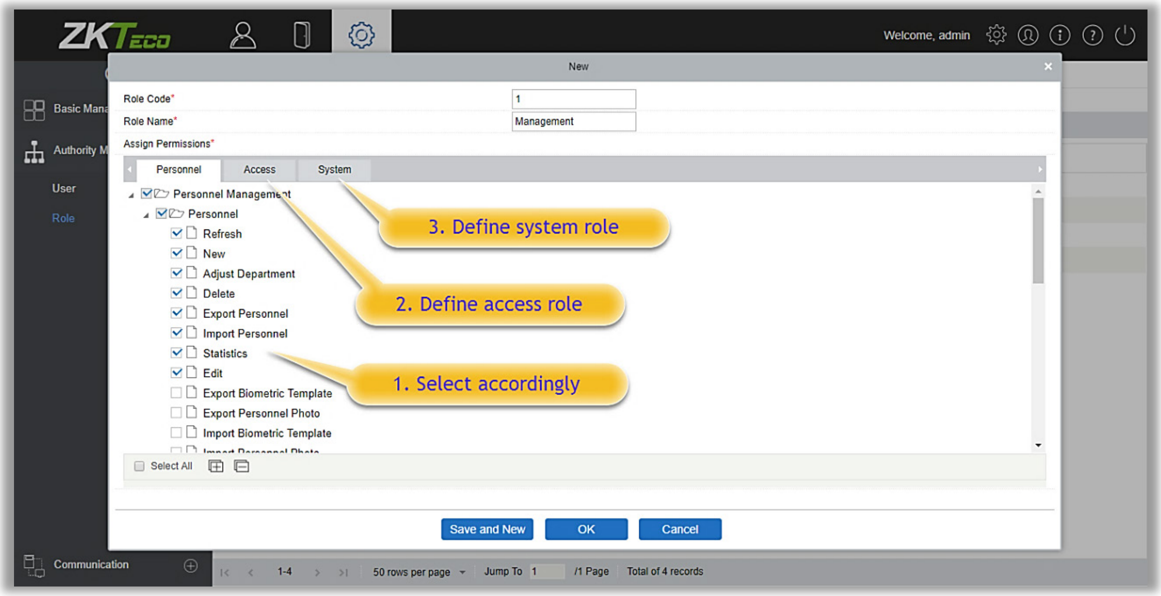
When using the system, the super user needs to assign different levels to new users. To avoid setting users one by one, you can set roles with specific levels in role management and assign appropriate roles to users when adding users. A super user has all the levels, can assign rights to new users and set corresponding roles (levels) according to requirements.

1. Click [System] > [Authority Management] > [Role] > [New]:



Click to Add

2. Set the name and assign permissions for the role.



Role Code* 1

Role Name* Management

Assign Permissions*

- ☑ Personnel Management
  - ☑ Personnel
    - ☑ Refresh
    - ☑ New
    - ☑ Adjust Department
    - ☑ Delete
    - ☑ Export Personnel
    - ☑ Import Personnel
    - ☑ Statistics
    - ☑ Edit
    - □ Export Biometric Template
    - □ Export Personnel Photo
    - □ Import Biometric Template
    - □ Import Personnel Photo

3. Define system role

2. Define access role

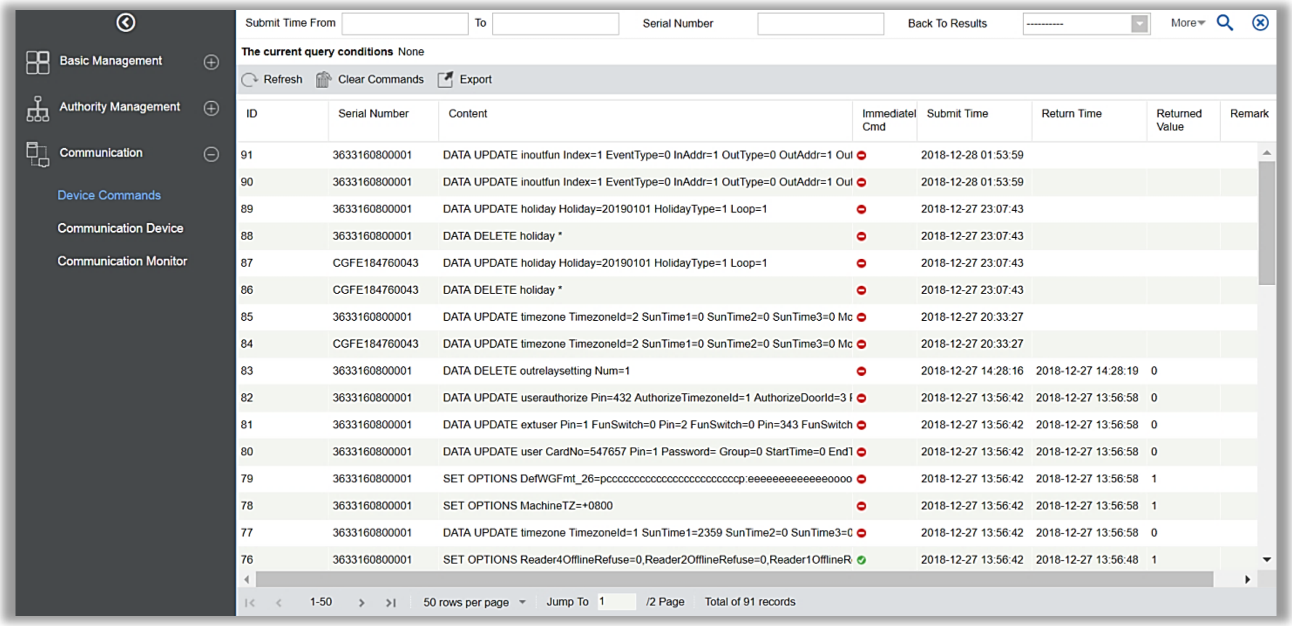
1. Select accordingly

3. Click [OK] to save.

## 5.3 Communication

### 5.3.1 Device Commands

Click [System] > [Communication] > [Device commands], the commands lists will be displayed.



The current query conditions None

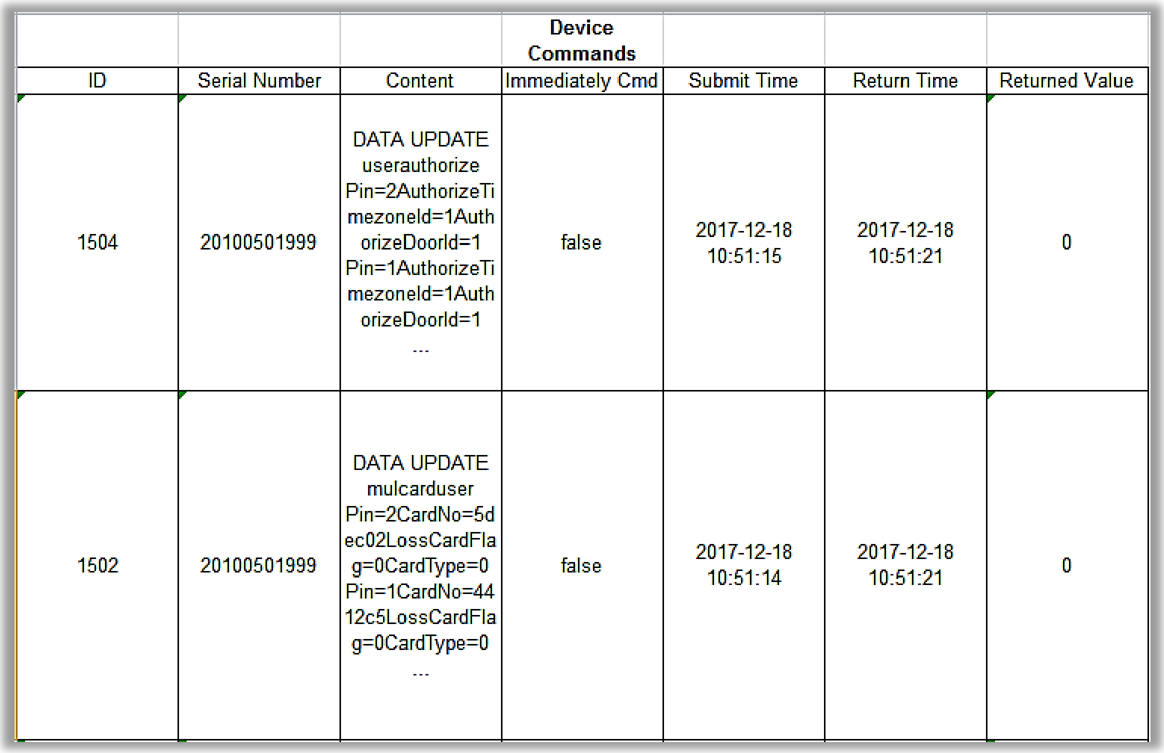
| ID | Serial Number | Content | Immediatel Cmd | Submit Time | Return Time | Returned Value | Remark |
|---|---|---|---|---|---|---|---|
| 91 | 3633160800001 | DATA UPDATE inoutfun Index=1 EventType=0 InAddr=1 OutType=0 OutAddr=1 Out | ⊖ | 2018-12-28 01:53:59 | | | |
| 90 | 3633160800001 | DATA UPDATE inoutfun Index=1 EventType=0 InAddr=1 OutType=0 OutAddr=1 Out | ⊖ | 2018-12-28 01:53:59 | | | |
| 89 | 3633160800001 | DATA UPDATE holiday Holiday=20190101 HolidayType=1 Loop=1 | ⊖ | 2018-12-27 23:07:43 | | | |
| 88 | 3633160800001 | DATA DELETE holiday * | ⊖ | 2018-12-27 23:07:43 | | | |
| 87 | CGFE184760043 | DATA UPDATE holiday Holiday=20190101 HolidayType=1 Loop=1 | ⊖ | 2018-12-27 23:07:43 | | | |
| 86 | CGFE184760043 | DATA DELETE holiday * | ⊖ | 2018-12-27 23:07:43 | | | |
| 85 | 3633160800001 | DATA UPDATE timezone TimezoneId=2 SunTime1=0 SunTime2=0 SunTime3=0 Mo | ⊖ | 2018-12-27 20:33:27 | | | |
| 84 | CGFE184760043 | DATA UPDATE timezone TimezoneId=2 SunTime1=0 SunTime2=0 SunTime3=0 Mo | ⊖ | 2018-12-27 20:33:27 | | | |
| 83 | 3633160800001 | DATA DELETE outrelaysetting Num=1 | ⊖ | 2018-12-27 14:28:16 | 2018-12-27 14:28:19 | 0 | |
| 82 | 3633160800001 | DATA UPDATE userauthorize Pin=432 AuthorizeTimezoneId=1 AuthorizeDoorId=3 I | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 0 | |
| 81 | 3633160800001 | DATA UPDATE extuser Pin=1 FunSwitch=0 Pin=2 FunSwitch=0 Pin=343 FunSwitch | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 0 | |
| 80 | 3633160800001 | DATA UPDATE user CardNo=547657 Pin=1 Password= Group=0 StartTime=0 EndT | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 0 | |
| 79 | 3633160800001 | SET OPTIONS DefWGFmt_26=pccccccccccccccccccccccccp:eeeeeeeeeeeeeoooo | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 1 | |
| 78 | 3633160800001 | SET OPTIONS MachineTZ=+0800 | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 1 | |
| 77 | 3633160800001 | DATA UPDATE timezone TimezoneId=1 SunTime1=2359 SunTime2=0 SunTime3=0 | ⊖ | 2018-12-27 13:56:42 | 2018-12-27 13:56:58 | 0 | |
| 76 | 3633160800001 | SET OPTIONS Reader4OfflineRefuse=0,Reader2OfflineRefuse=0,Reader1OfflineR | ✓ | 2018-12-27 13:56:42 | 2018-12-27 13:56:48 | 1 | |

1-50 | 50 rows per page | Jump To 1 /2 Page | Total of 91 records

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 failed.

Clear Commands: Clear the command lists.

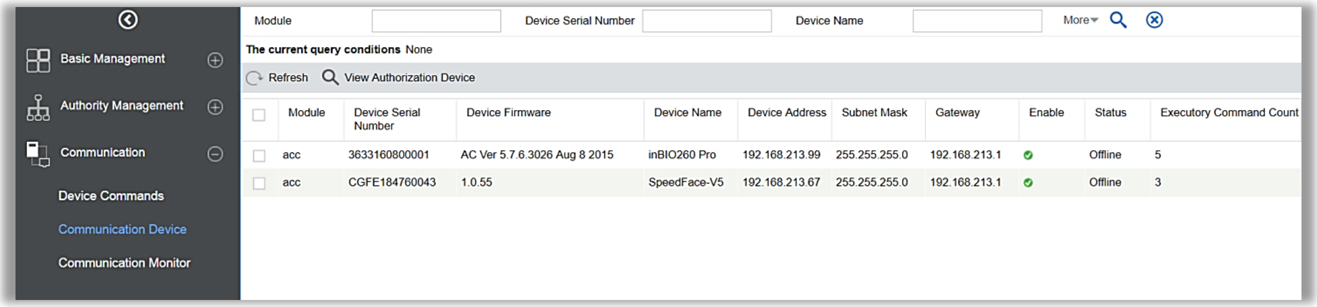
Export: Export the command lists to local host. You can export to an Excel file. See the following figure.



|  |  |  | 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<br>… | 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<br>… | false | 2017-12-18 10:51:14 | 2017-12-18 10:51:21 | 0 |

## 5.3.2 Communication Device

Click [System] > [Communication] > [Communication Device], the device list will be displayed:

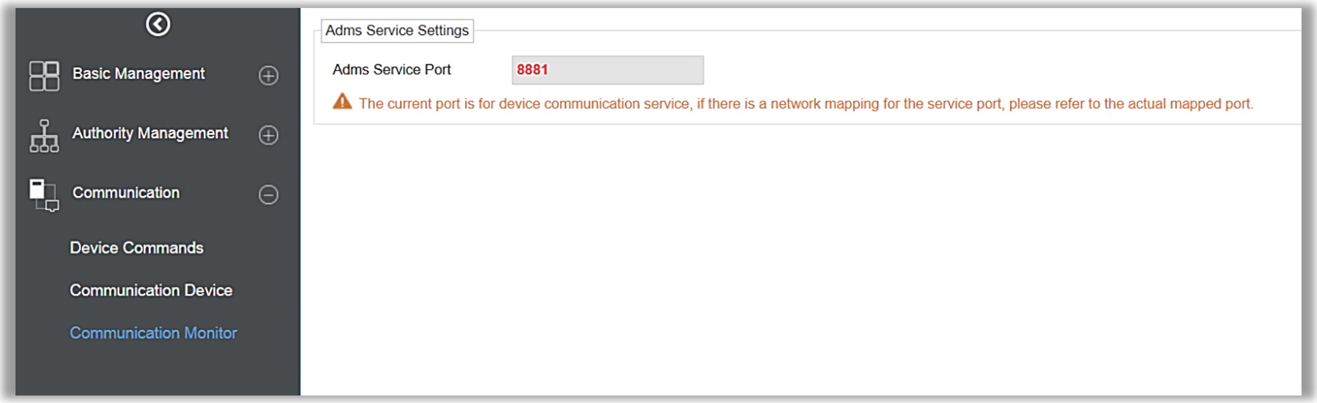


The current query conditions None

| □ | Module | Device Serial Number | Device Firmware | Device Name | Device Address | Subnet Mask | Gateway | Enable | Status | Executory Command Count |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | acc | 3633160800001 | AC Ver 5.7.6.3026 Aug 8 2015 | inBIO260 Pro | 192.168.213.99 | 255.255.255.0 | 192.168.213.1 | ✓ | Offline | 5 |
| □ | acc | CGFE184760043 | 1.0.55 | SpeedFace-V5 | 192.168.213.67 | 255.255.255.0 | 192.168.213.1 | ✓ | Offline | 3 |

## 5.3.3 Communication Monitor

Click [System] > [Communication] > [Communication Monitor], the device service port and its details will be displayed:



Adms Service Settings

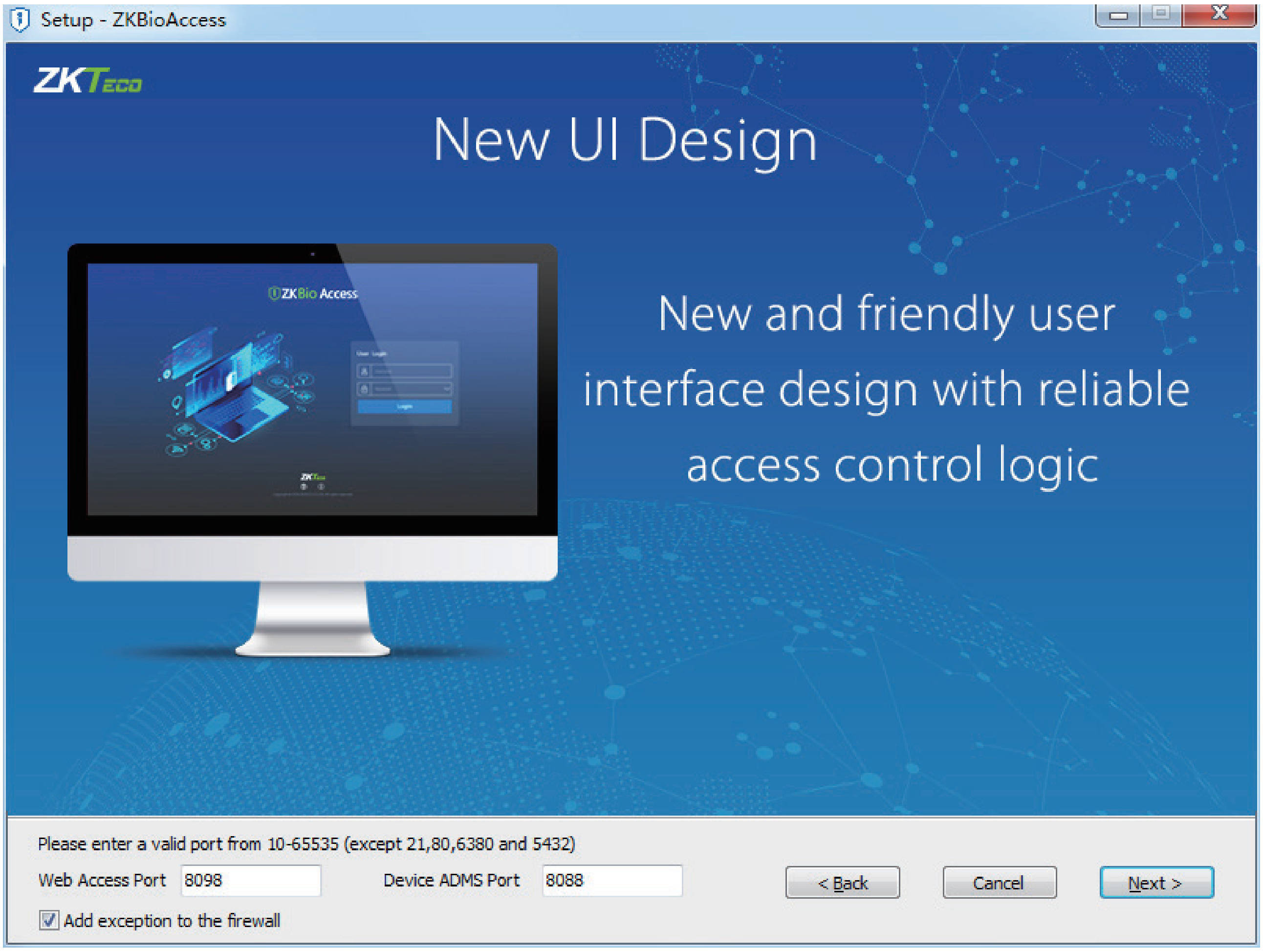
Adms Service Port: 8881

⚠ The current port is for device communication service, if there is a network mapping for the service port, please refer to the actual mapped port.

**Note:** While installing ZKBioAccess, you need to input port number properly.

**Web Access Port** is used to access the website

**Device ADMS Port** is used to connect to the device


Setup - ZKBioAccess
ZKTeco
New UI Design
ZKBio Access
New and friendly user interface design with reliable access control logic
< Back
Cancel
Next >

Please enter a valid port from 10-65535 (except 21,80,6380 and 5432)

Web Access Port: 8098

Device ADMS Port: 8088

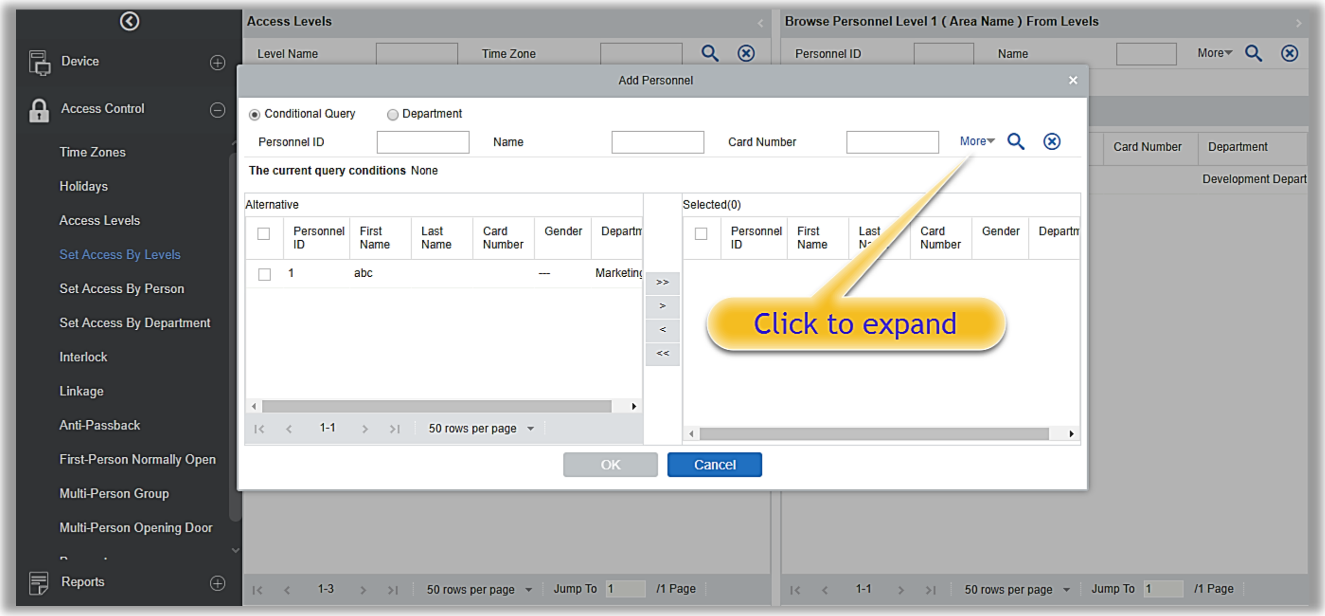
☑ Add exception to the firewall

# 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.

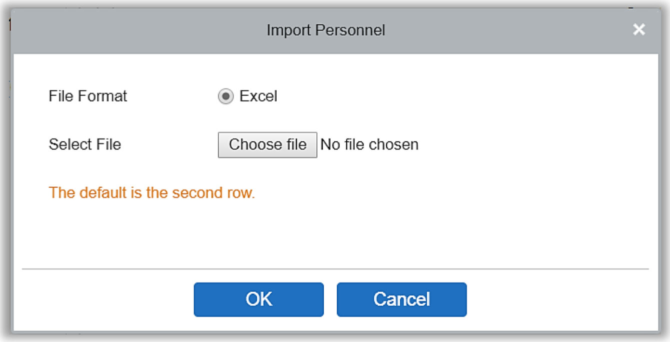
Click > to move the selected personnel in to the selected lists. If you want to cancel the movement, click < .

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]:


Import Personnel

File Format ● Excel

Select File Choose file No file chosen

The default is the second row.

Fields are as follows:

Destination File: Choose file to be imported.

2. Click [OK]:

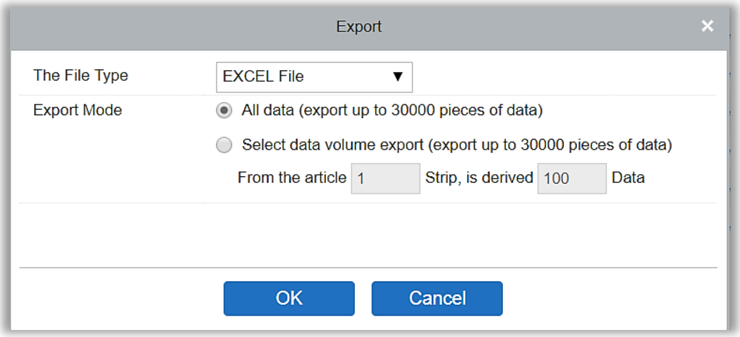
The data is imported successfully.

✍**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]:


Export

The File Type: EXCEL File ▼

Export Mode:
● All data (export up to 30000 pieces of data)
○ Select data volume export (export up to 30000 pieces of data)
From the article 1 Strip, is derived 100 Data

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 is not closed within the specified delay time after opening, then the sensor detects and triggers this abnormal event.

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.

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).

# 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. 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, clear the checkbox. 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\ZKBioAccess\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

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com