

USER MANUAL

ZKBioPack 2.0

Version: 1.0

Date: March, 2017

Copyrights

©Copyright 1998-2017 ZKTECO CO.,LTD All rights reserved.

All rights reserved. Except as specifically permitted herein, no portion of the information in this document may be reproduced in any form or by any means without the prior written permission from **ZKTECO**. The software described in this manual may include copyrighted software of **ZKTECO** and possible licensors. Customers shall not reproduce, distribute, modify, decompile, disassemble, decrypt, extract, reverse engineer, lease, assign, or sublicense the said software in any manner, unless such restrictions are prohibited by applicable laws or such actions are approved by respective copyright holders under license.

Disclaimer

Please read documents carefully when using the software. We apologize for any inconvenience caused by the preceding reasons.

Thank you.

Table of Contents

1. Overview	1
2. Requirements.....	1
3. Installation Package.....	1
4. Concept.....	2
5. How It Works-Flowchart	3
6. Installing ZKBioPack 2.0.....	5
7. Installing ZKBioPack 2.0 Plug-In	11
8. ZKBioPack Service Controller	20
9. Adding Device	21
10. Create User/Enroll Fingerprint	26
11. Sync to Device.....	28
12. Device Menus.....	29
❖ Edit	30
❖ Delete.....	31
❖ Export	31
❖ Upgrade Firmware.....	32
❖ Reboot Device.....	32
❖ Get Device Option	33
❖ Get Personnel Information	33
❖ Synchronize Time	34
❖ Set the Registration Device	34
❖ Set Daylight Saving Time.....	35
❖ Modify IP Address	35
❖ Modify Communication Password.....	36
❖ Modify RS485 Address.....	36
❖ Modify the Fingerprint Identification Threshold.....	36
❖ View Device Capacity	37
❖ Clear Device Manager.....	38
❖ Restore	38
❖ Door Module	39
❖ Device Monitoring	41
❖ Real-time Monitoring	43

13.	Personnel Menus	47
❖	Export	47
❖	Editing Personnel(s)	48
❖	Parameters	51
14.	System Menus.....	52
❖	Exporting the Operation Logs.....	52
❖	Database Management	53
❖	Area Setting	54
❖	Email Management.....	55
❖	Data Clearing	56
❖	Authority Management.....	56
❖	Role.....	57
❖	Role Group	58
❖	Communication	59

1. Overview

The purpose of ZKBioPack is to add **biometric readers** to **Customer's access control software**. Customers can launch the ZKBioPack software application from within their software interface when ZKAccess IP-based biometric readers are added.

After launching ZKBioPack from within the software, administrators can enroll Personnel's biometric credentials (fingerprints and/or faces) by using a ZKAccess USB fingerprint enrollment device attached to the computer running the software.

After enrollment is complete, ZKBioPack synchronizes the biometric templates with all the ZKAccess biometric readers on the network.

Fingerprint template synchronization is performed in the background, making the ZKBioPack security system entirely transparent to the software users.

2. Requirements

PC Requirements:

CPU	Dual-core processor with speed of 2.4GHZ or above.
RAM	4 GB or above
Storage	30 GB Free Space (NTFS Recommended)
Operating System	Windows 7/8/10/Server 2008 (32/64 bit)

Database Requirements:

ZKBioPack Default Database	PostgreSQL
ZKBioPack Optional Database	SQL Server and Oracle
Customer Database	MSSQL
ZKBioPack Plug-in Database	MSSQL

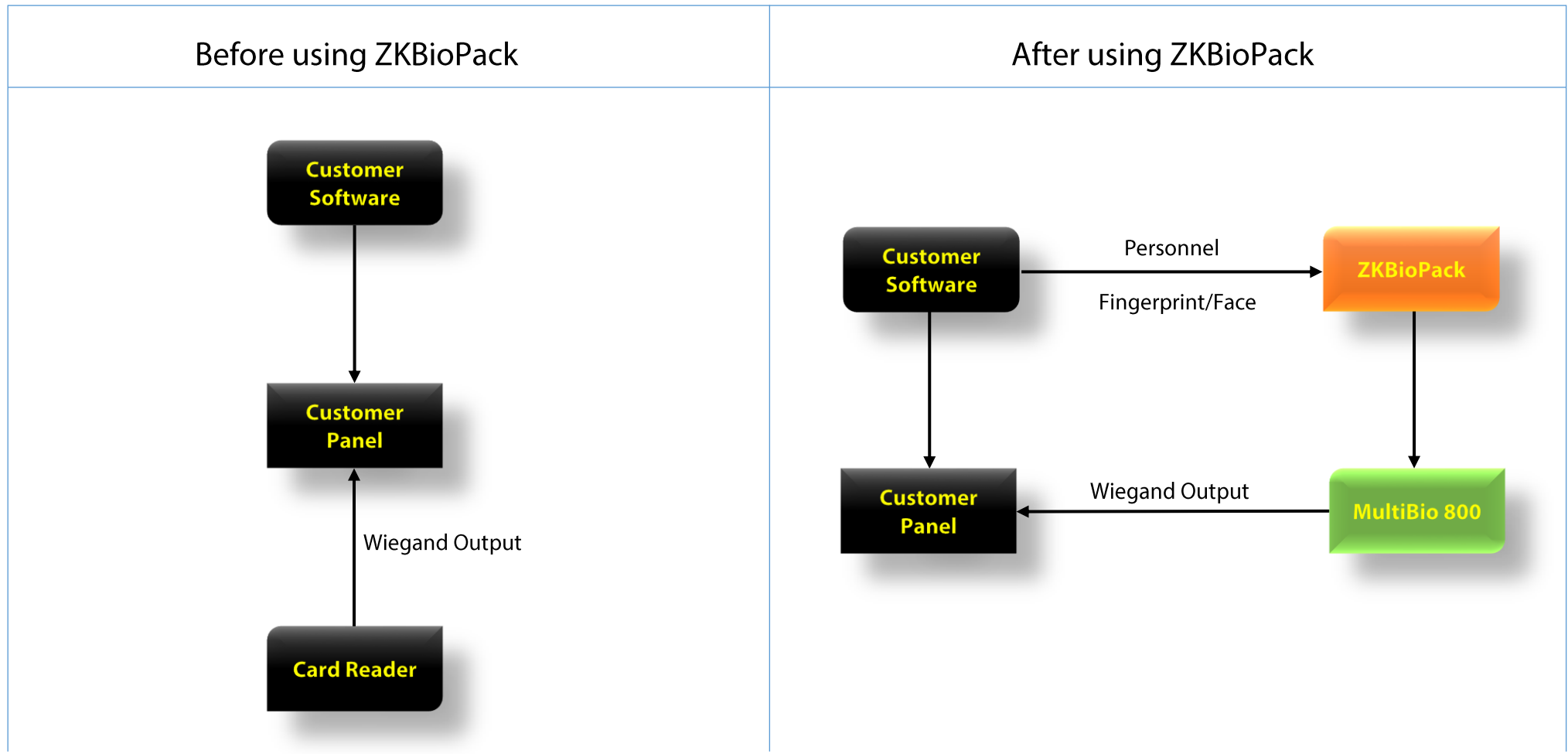
Supported models: F18, F19, Mutibio800, ProFAC, ProBio, ProCaptureT, inPulse, inPulse+.

3. Installation Package

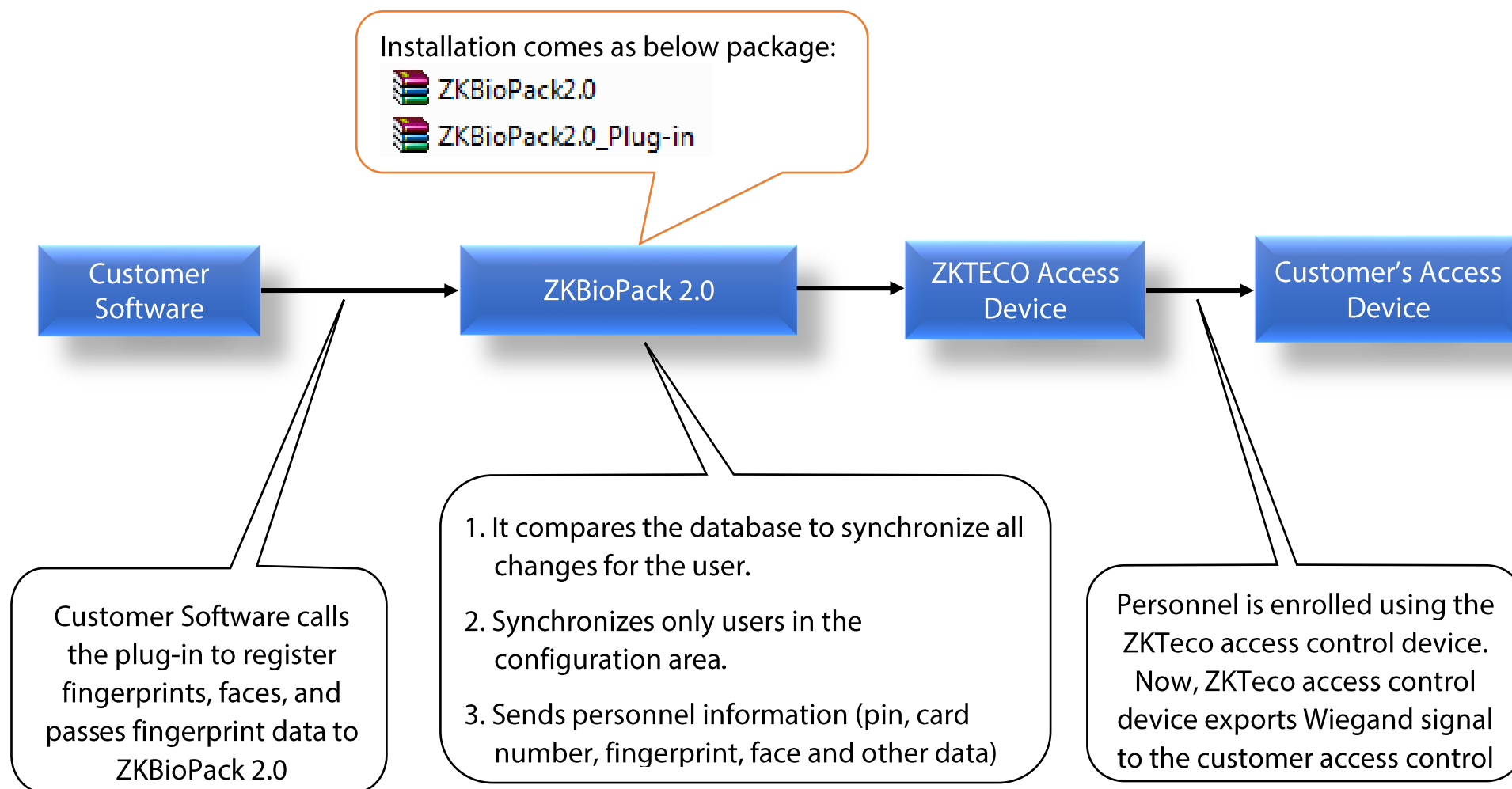
The installation comes in package of two installation package.

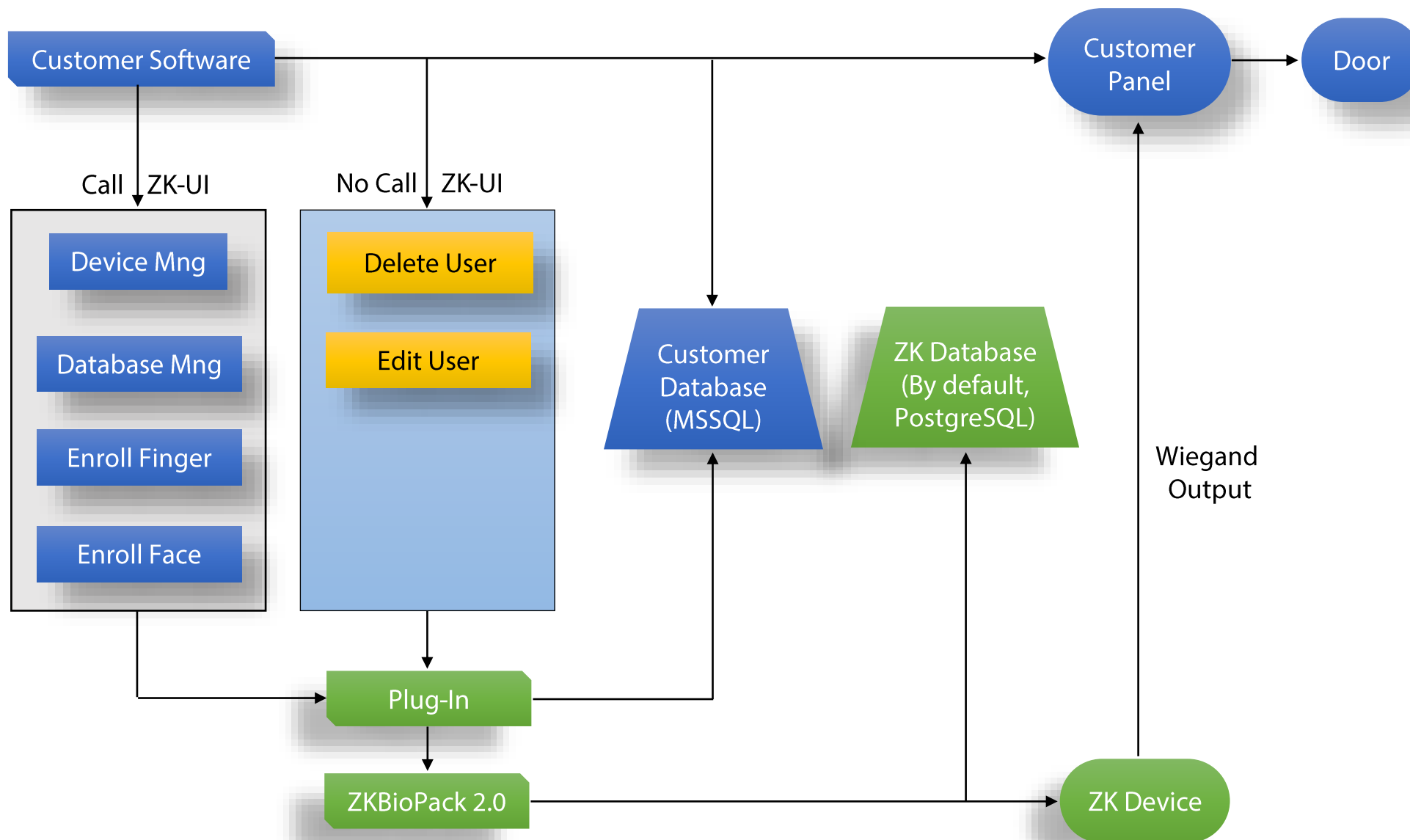


4. Concept



5. How It Works-Flowchart













6. Installing ZKBioPack 2.0

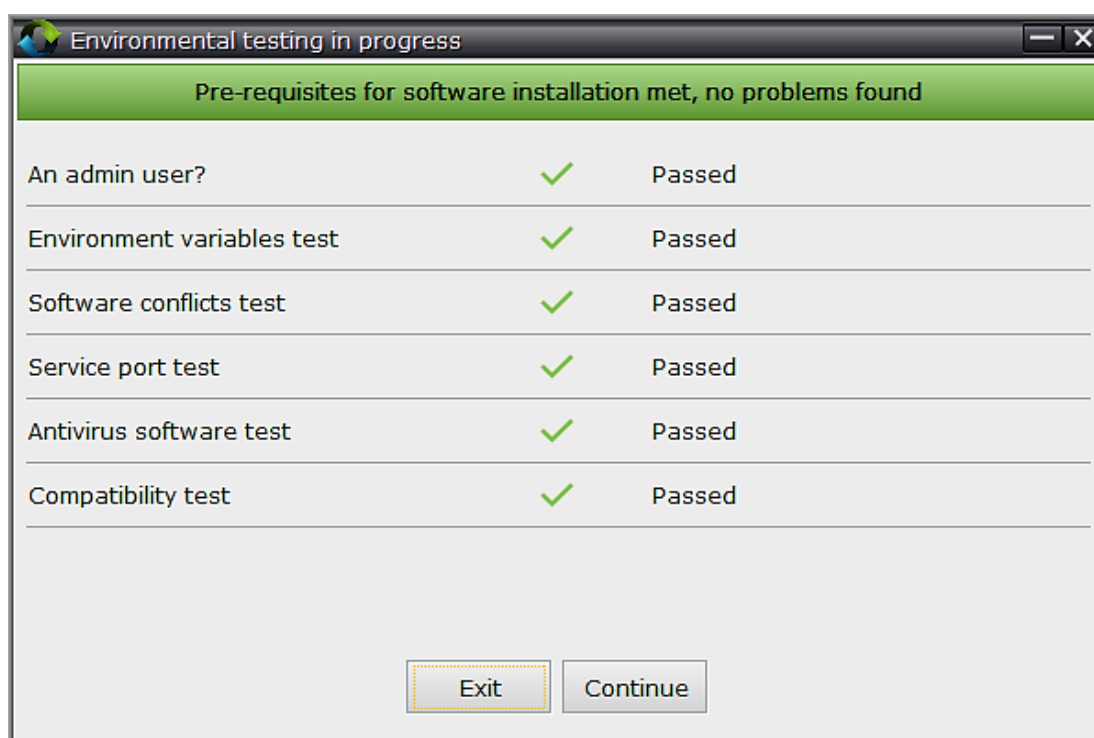
Before using the software, you need to extract and install it. Extract this  **ZKBioPack2.0** Package file.

After extracting, run the  **setup** setup file.

	Config	File folder
	DLL	File folder
	Image	File folder
	logs	File folder
	MainResource	File folder
	Pubs	File folder
	UpdatePack	File folder
	setup	Application

Once the **setup** is started, you will find below interface. This test is done to check if the PC is suitable for software installation or not. It will check all the required details to install the software.

If any discrepancy is found, then instead of green tick mark a red cross mark will be shown with a warning! Click on the warning message to know the exact reason of failure in installing the software.

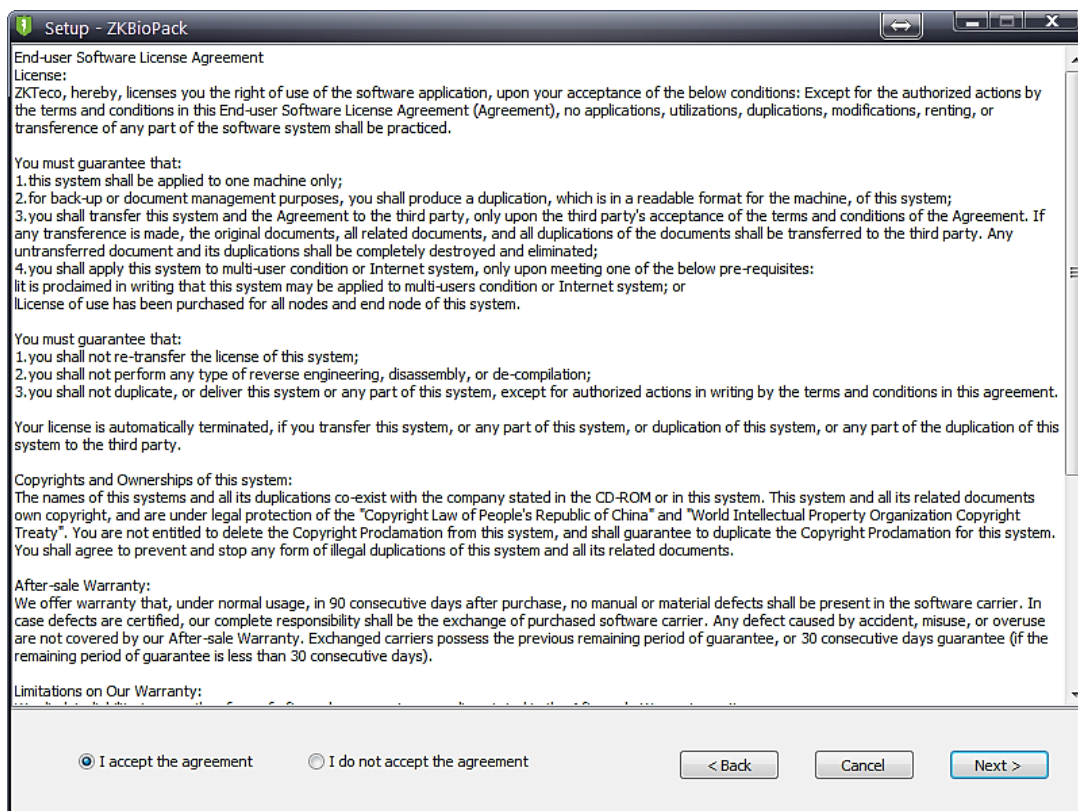


Then click on **Continue**, to start the installation.

Click on **Next** to proceed with installation.



Read the agreement and select **I Accept the agreement**. Then click **Next** to continue.



Check and confirm the correct port number. Make sure to keep the exception box ticked.



Select the drive where you want to install the software. By default, C drive will be selected.



The default database will be selected, if you have an alternative database then select as required.



Please specify the default backup folder or path.



Finally, click on **Install** to finish installation.



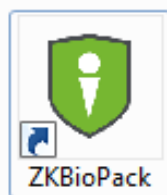
The installation may take few minutes depending upon your system hardware and software.



It is advisable to restart your PC after the installation. Make sure to save your other works before proceeding with restart.



After the installation is completed, you will find below icon at your desktop.



7. Installing ZKBioPack 2.0 Plug-In

Note 1 & 2 are only for Schneider software Continuum.

1. Before installing Plug-in, customer's software should set up the parameter for sending out personnel info.
2. Setup the path of Plug-in/BioPack.exe

biopack.exe 0.574685335 /p /e /fp lan=en

BioPack.exe is the path called

0.574685335 is the customer software ObjectID.Hi&ObjectID.Low

/p is the personnel

/e is the enroll

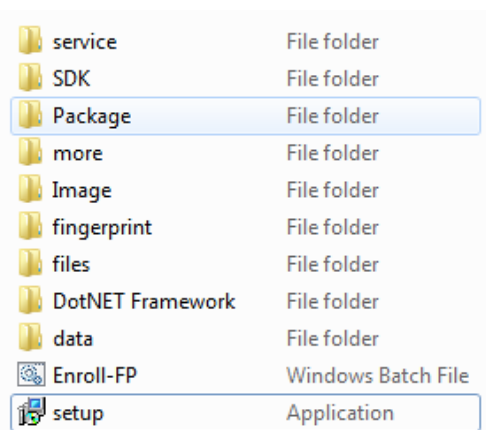
/fp is the fingerprint (optional /fa, /fv)

lan=en is the UI showing language

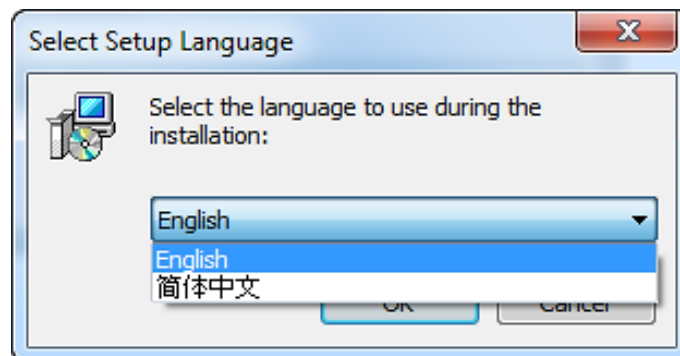
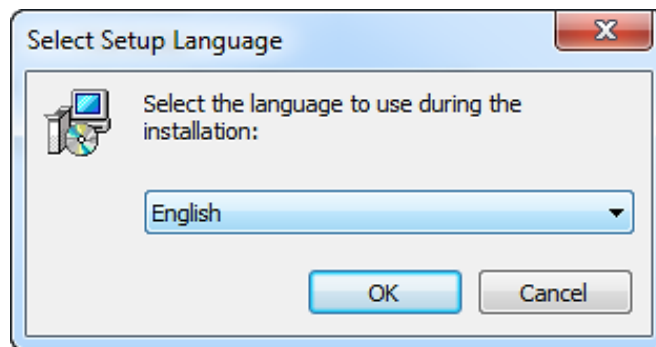
For all customer's software.

Extract this ZKBioPack2.0_Plug-in package file.

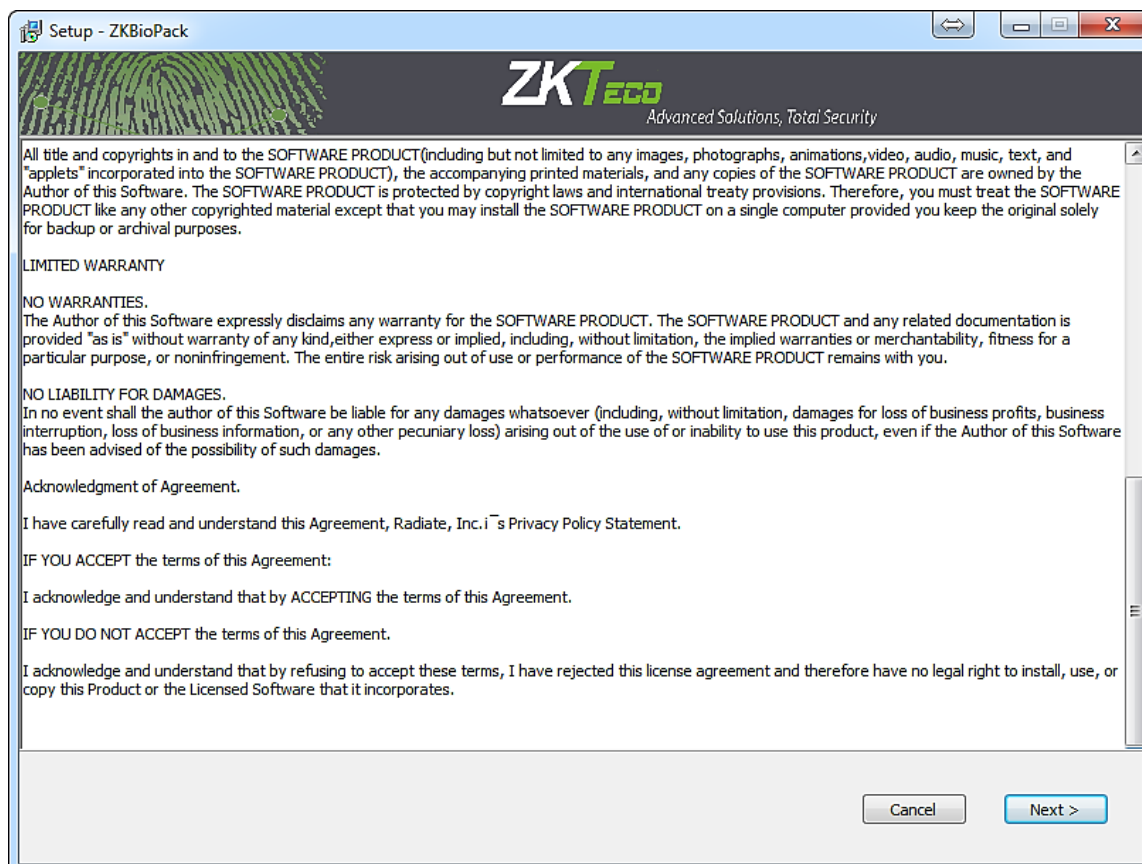
After extracting, run the setup file.



Once the **setup** is started, you will find below interface. Select your language and click OK.



Read the agreement and then click **Next** to continue.



Select the drive where you want to install the software. By default, C drive will be selected.



Select the program shortcut location.

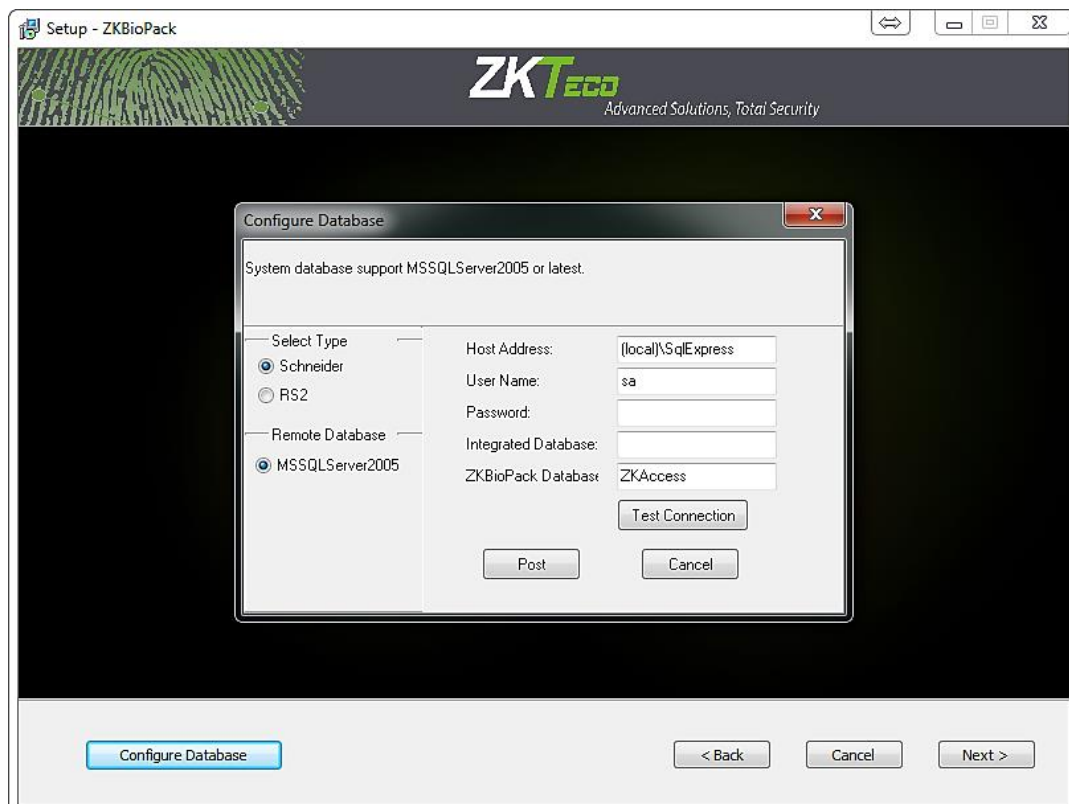


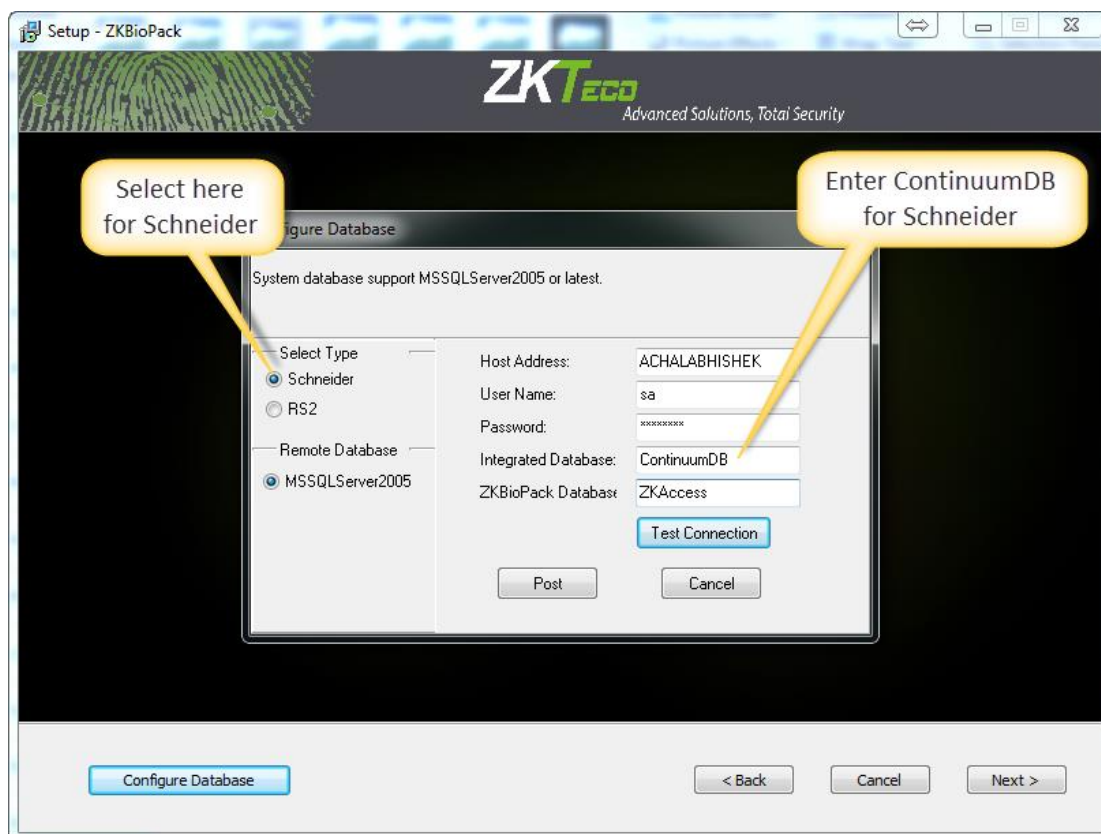
Now we need to configure the database. Click on **Configure Database**.



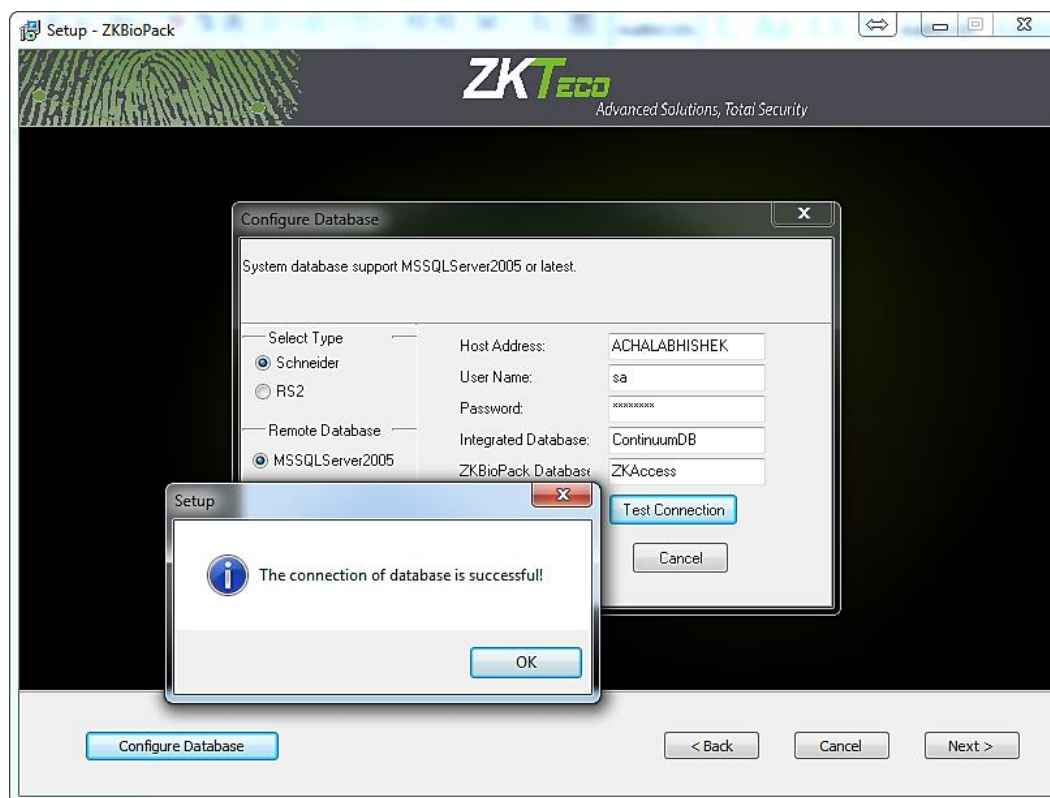
Enter the details correctly. Schneider customers please select Schneider and enter database name as ContinuumDB.

Make sure to enter the host address, username and password correctly.

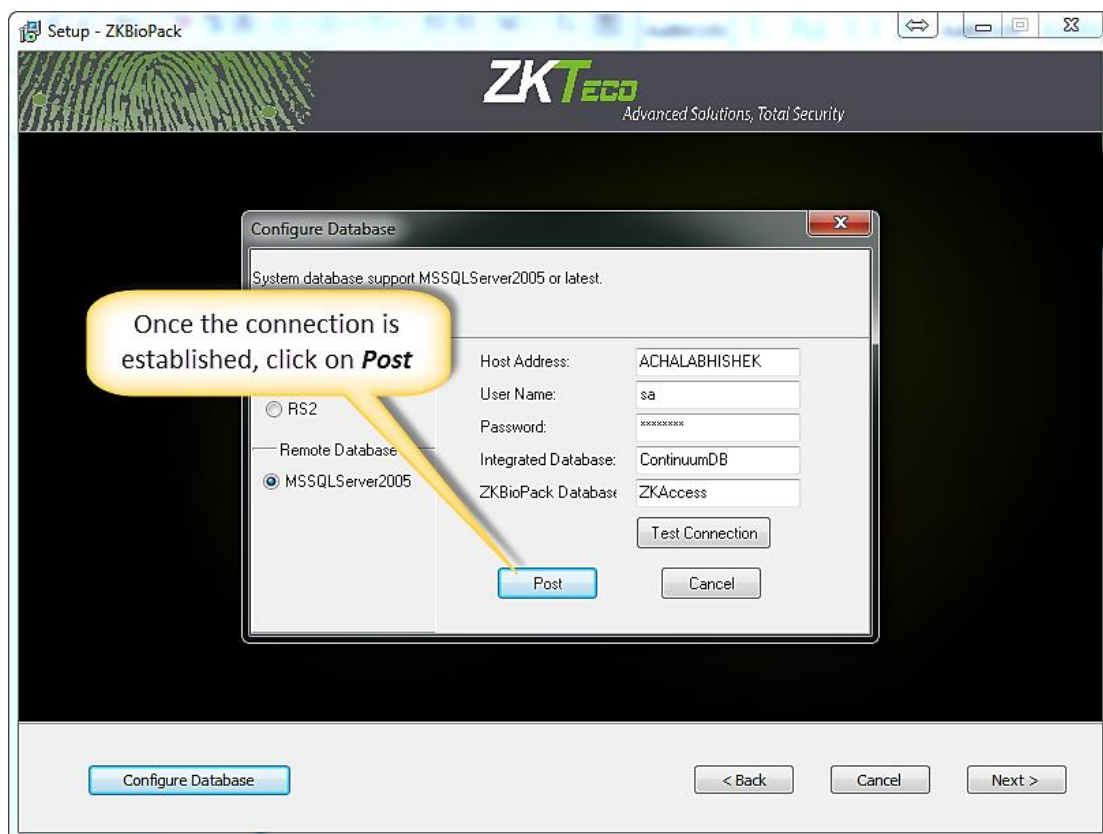




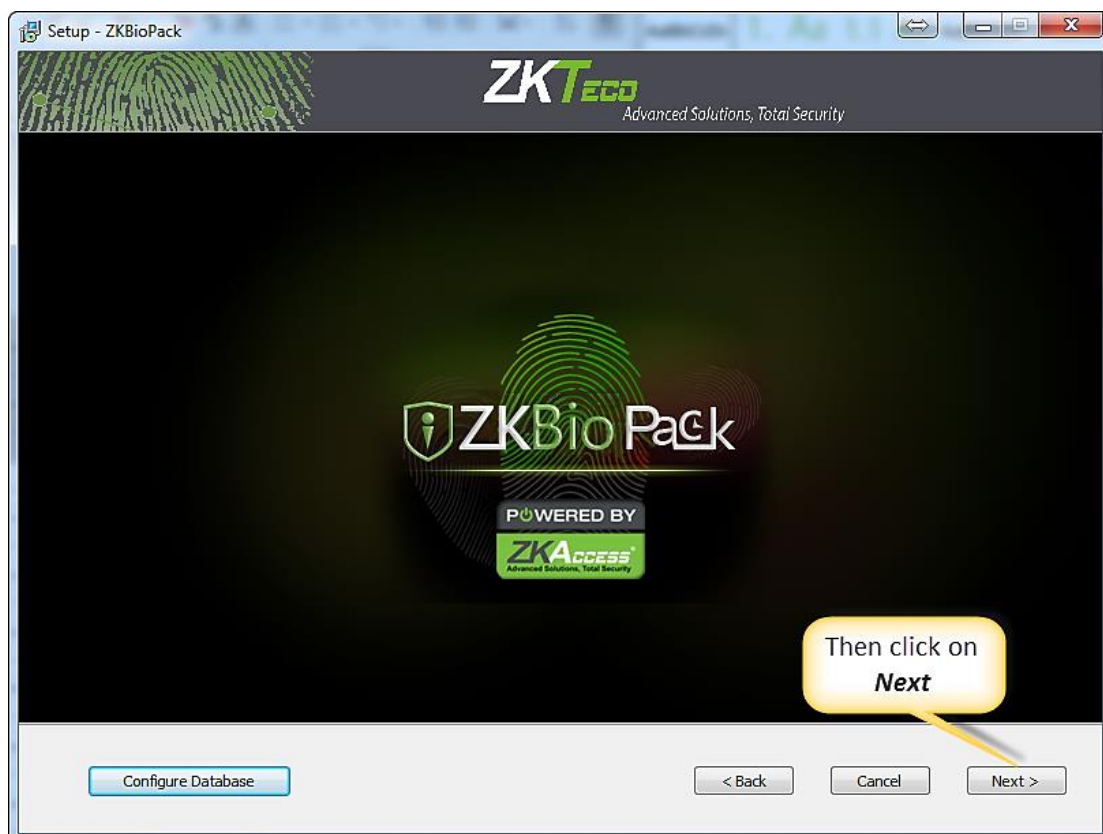
Once you have entered the details, click on **Test Connection** to check connection status.



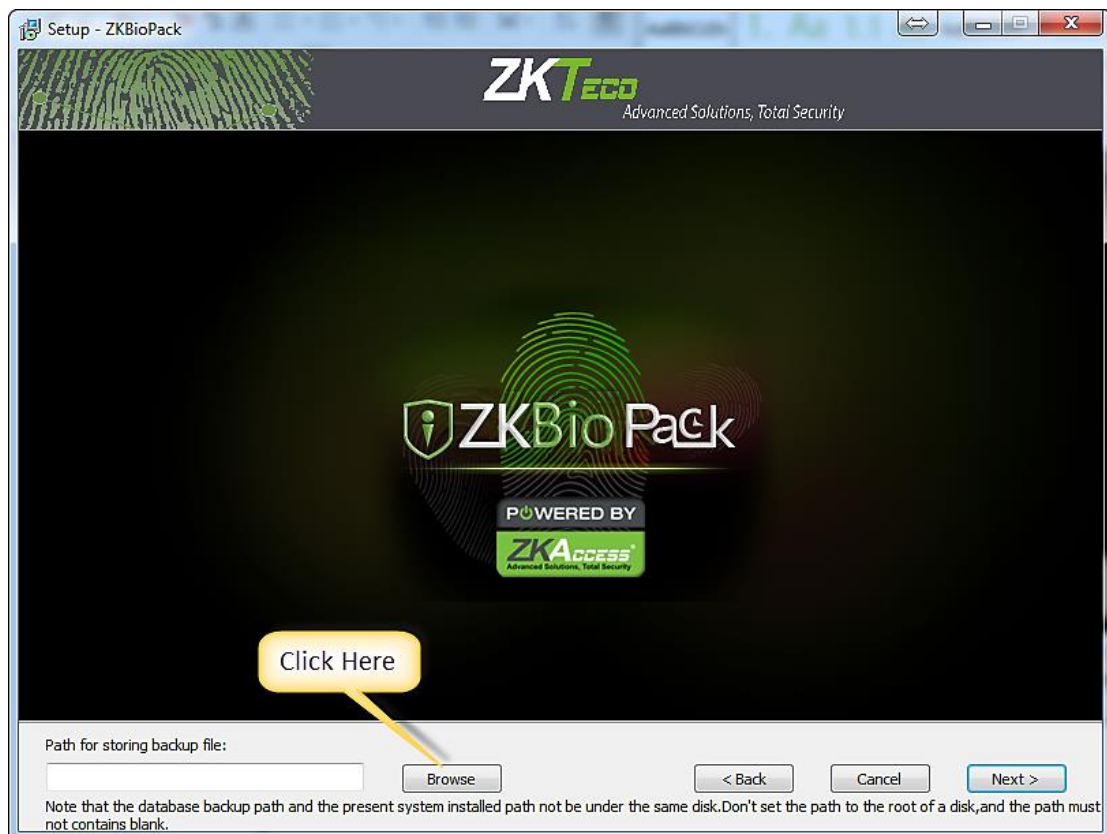
After the connection is successful, click on **Post**.



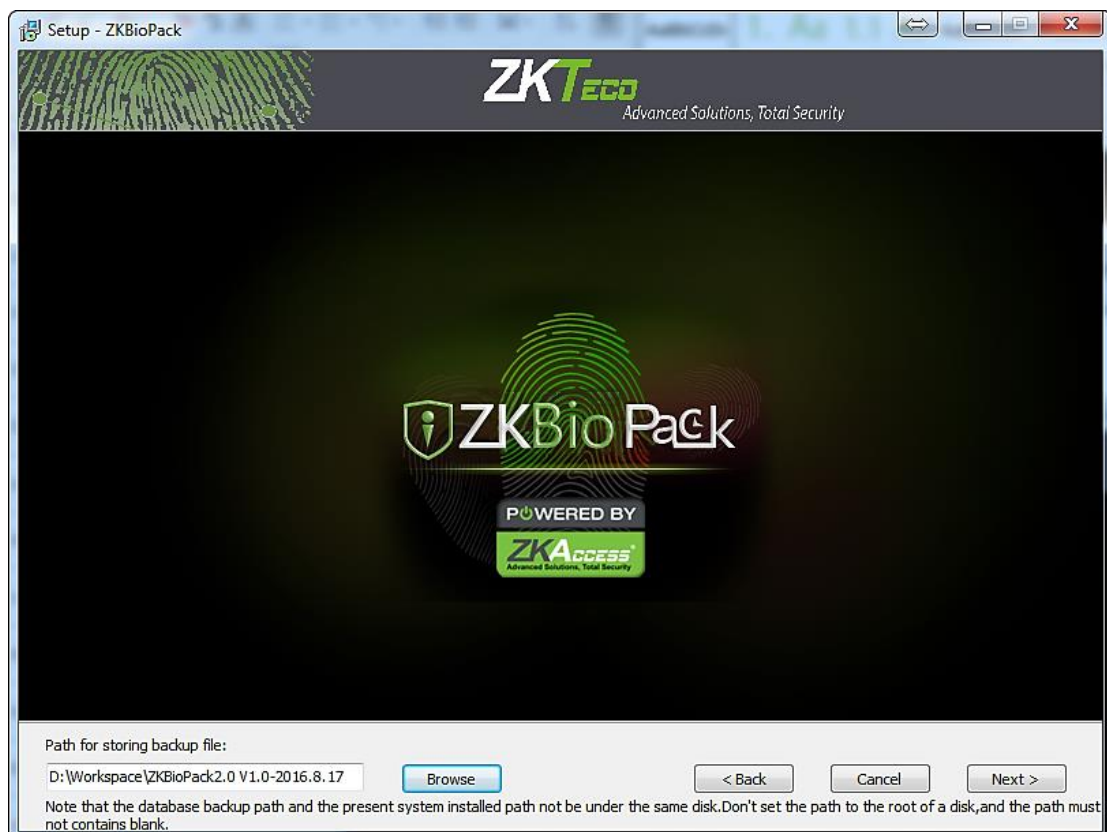
After that click on **Next** to proceed with installation.



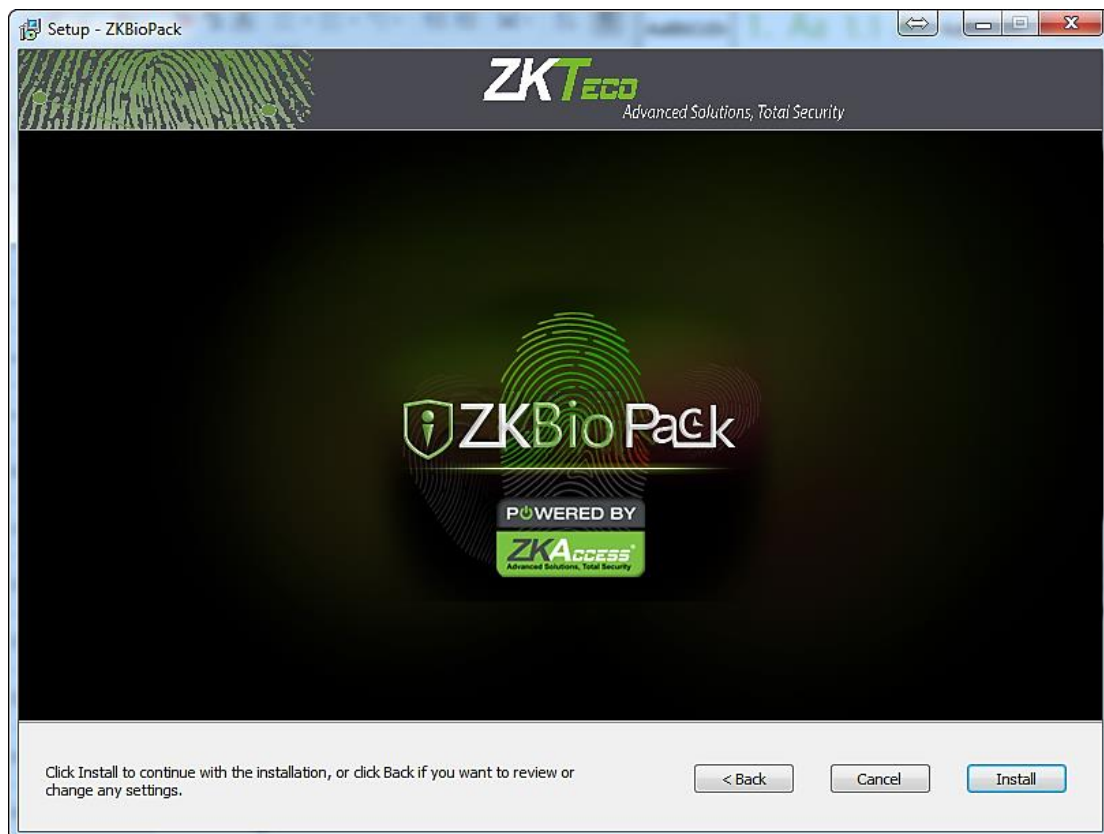
Now click on **Browse** to select the backup path or folder.



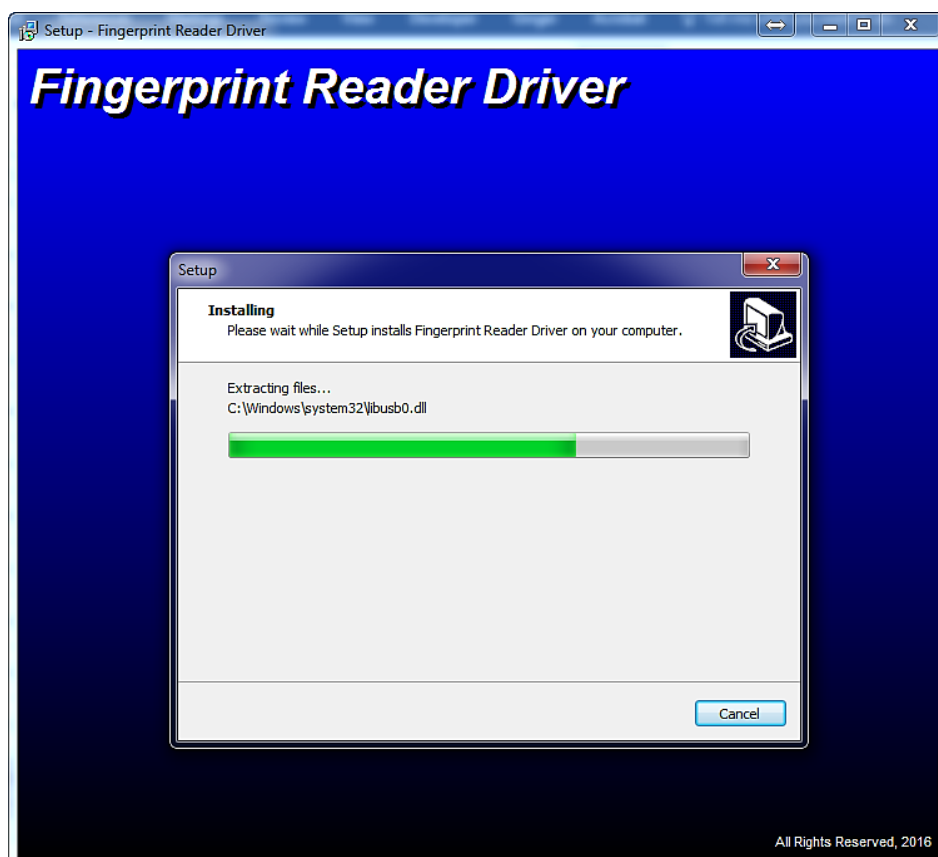
After selecting the path, click on **Next**.



Finally, click on **Install** to finish setup.



Then after, you will get below interface to install Fingerprint Reader Driver. Click on install, so that the system installs the required drivers.

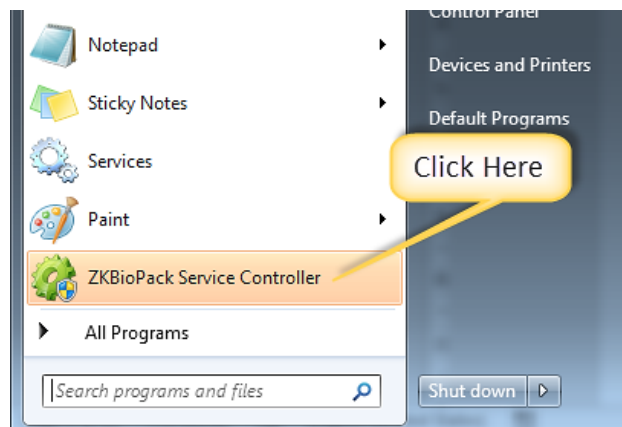


Once it is completed, click on **Finish**.



8. ZKBioPack Service Controller

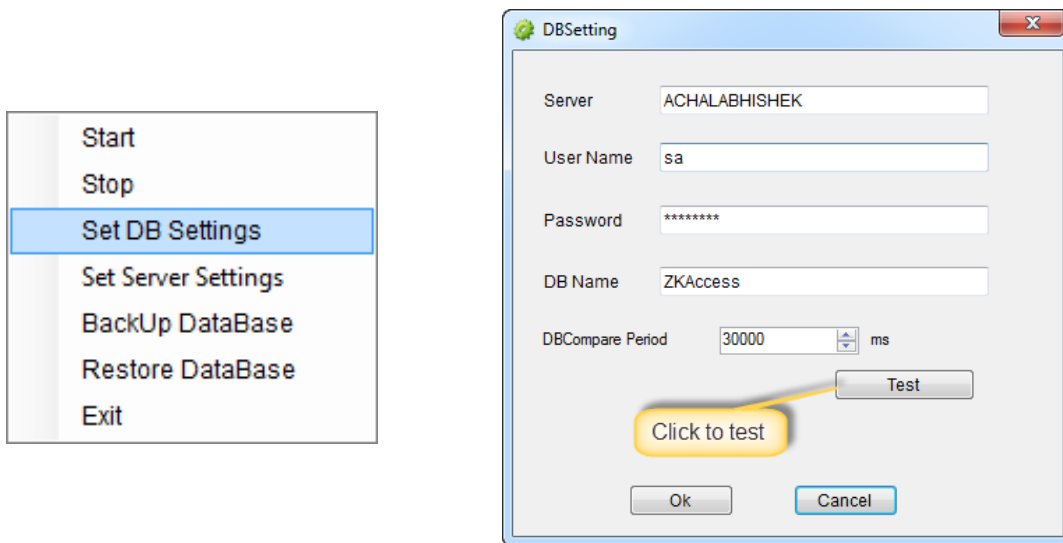
After the installation, in the start menu you will find below shown program. Click on it to open.



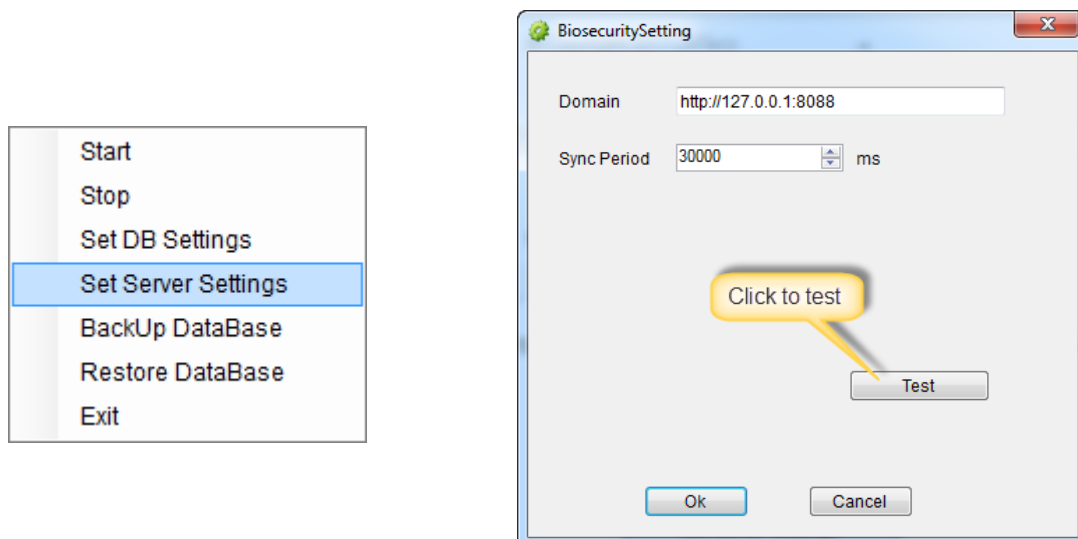
Once clicked, the program will be running in background in your taskbar as shown. Click once to open menu.



Go to **Set DB settings** in below shown menu to test the database settings.



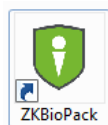
Go to **Set Server settings** in below shown menu to test the connection with ZKBioPack 2.0.



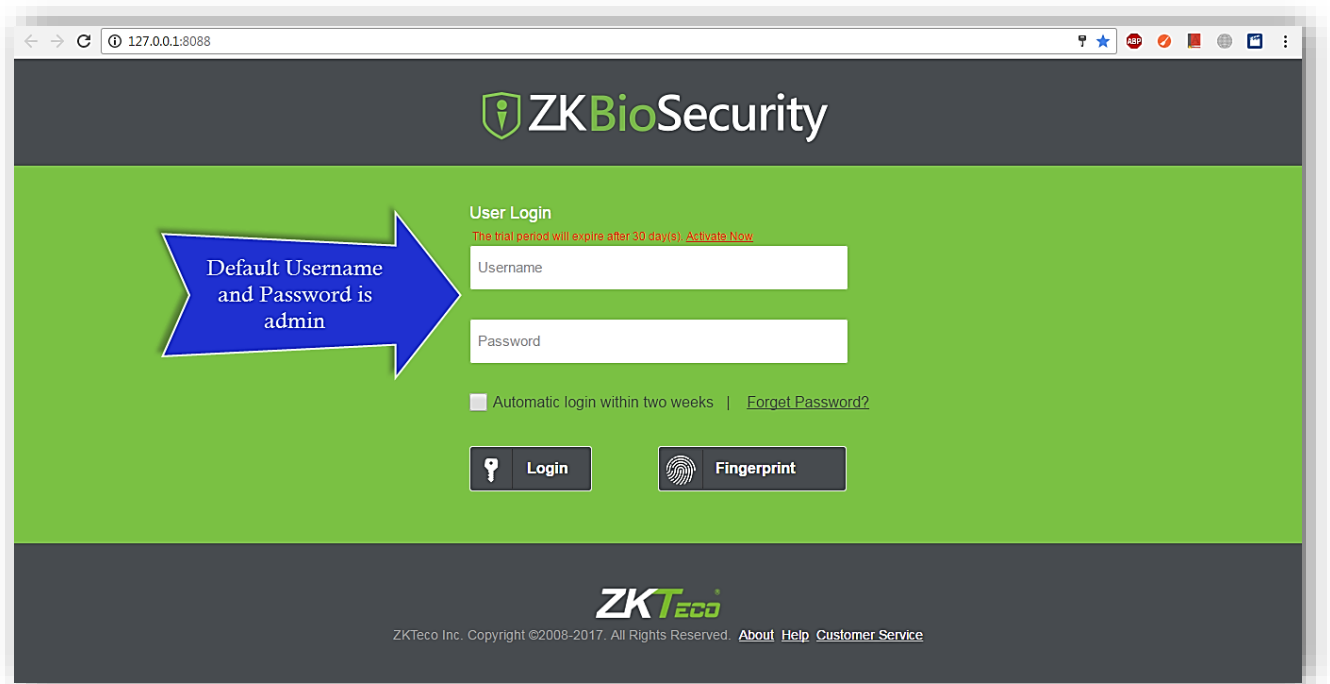
9. Adding Device

You can add device automatically by searching. Once added, you can view the information of connected devices, and perform remote monitoring, uploading and downloading etc.

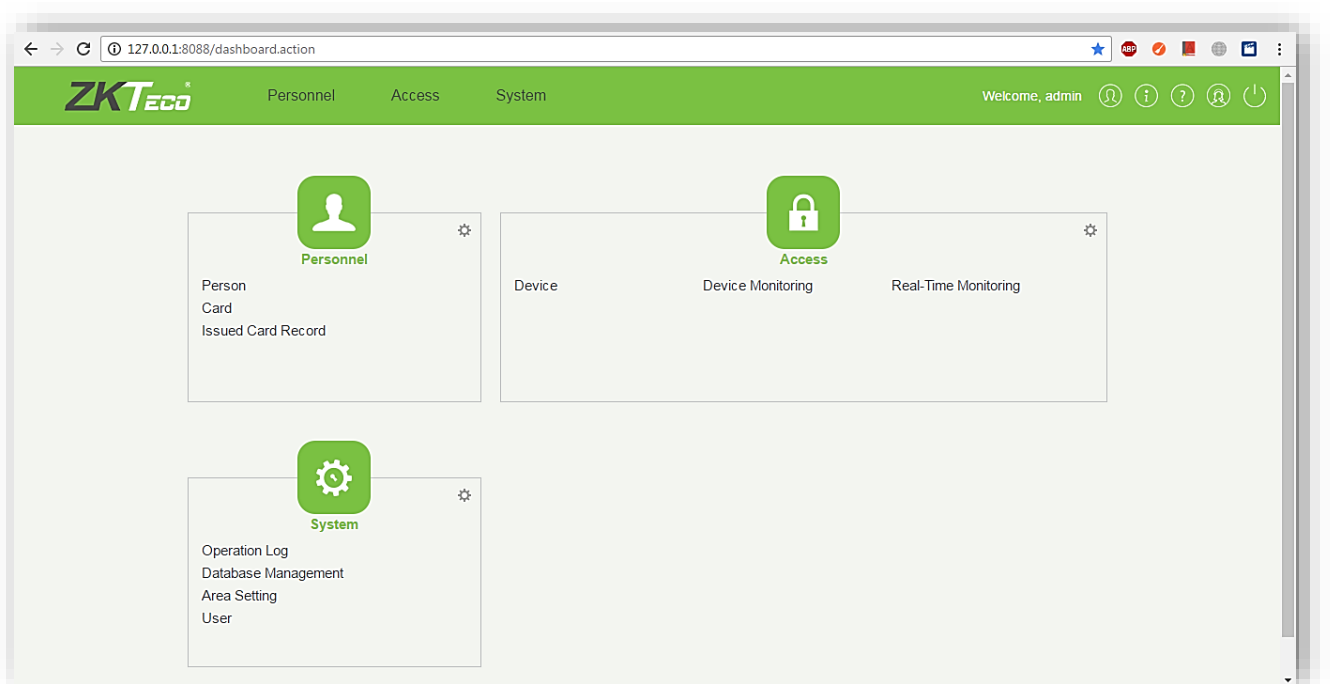
Please find below icon at your desktop and open it.



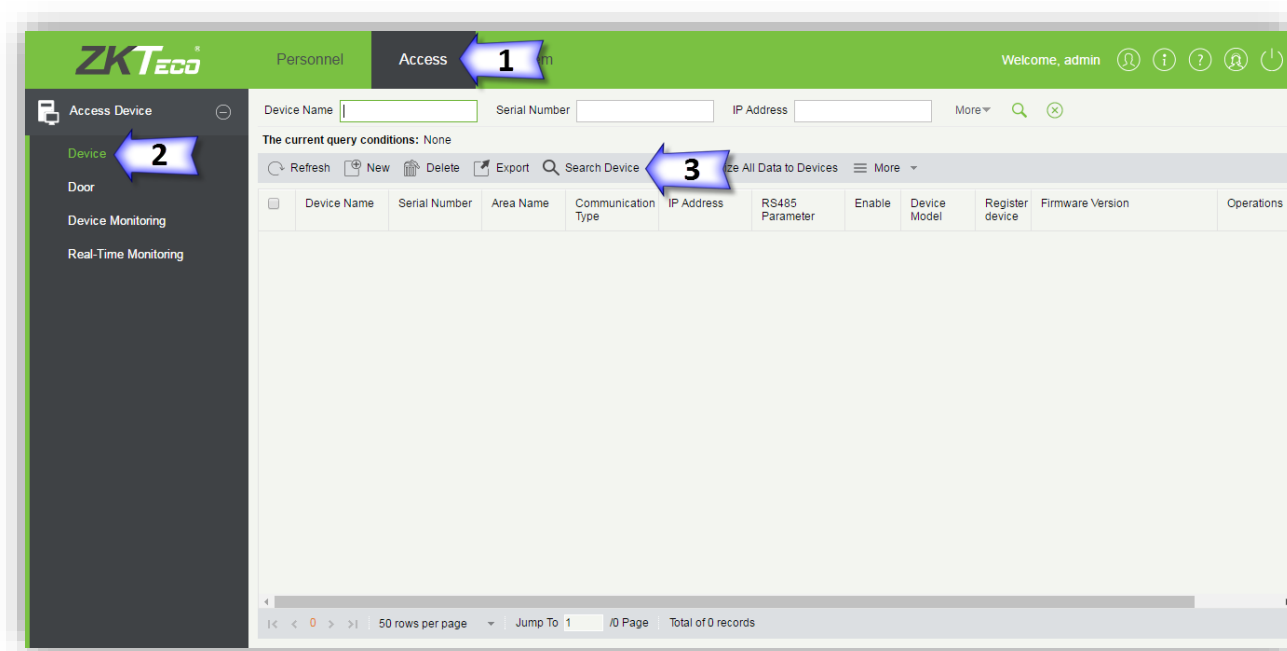
Login using **admin** as username and password.



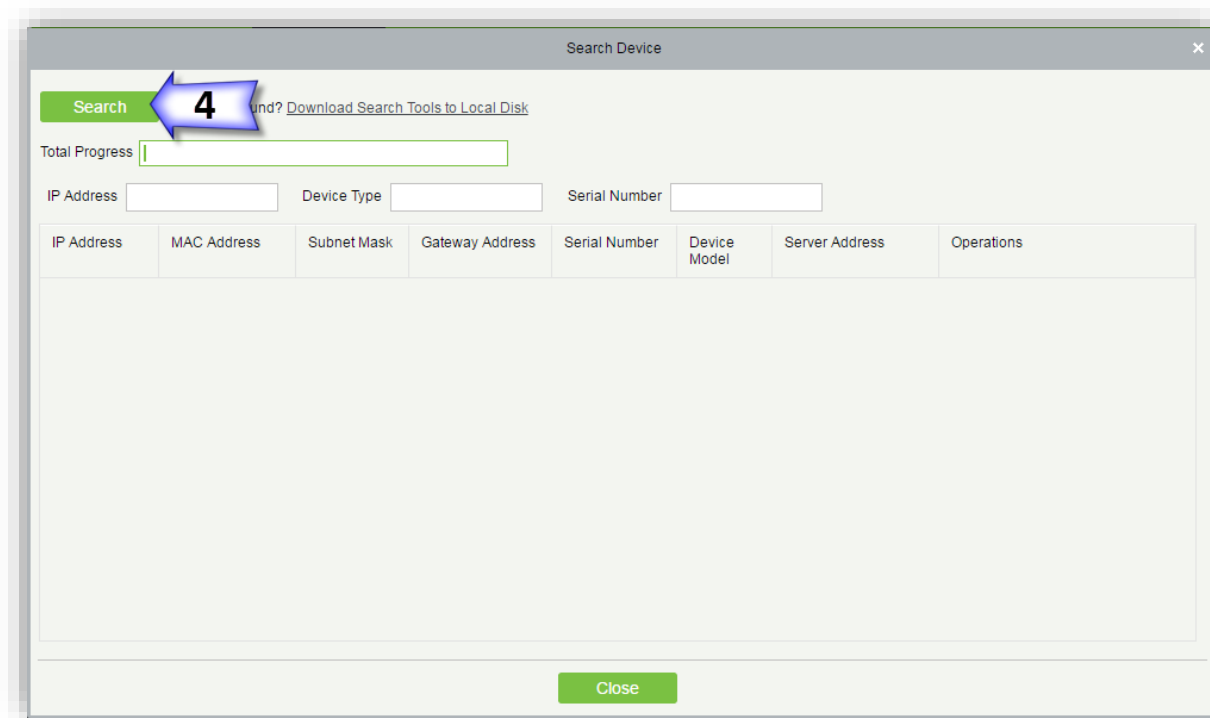
Below is the initial interface of ZKBioPack 2.0.



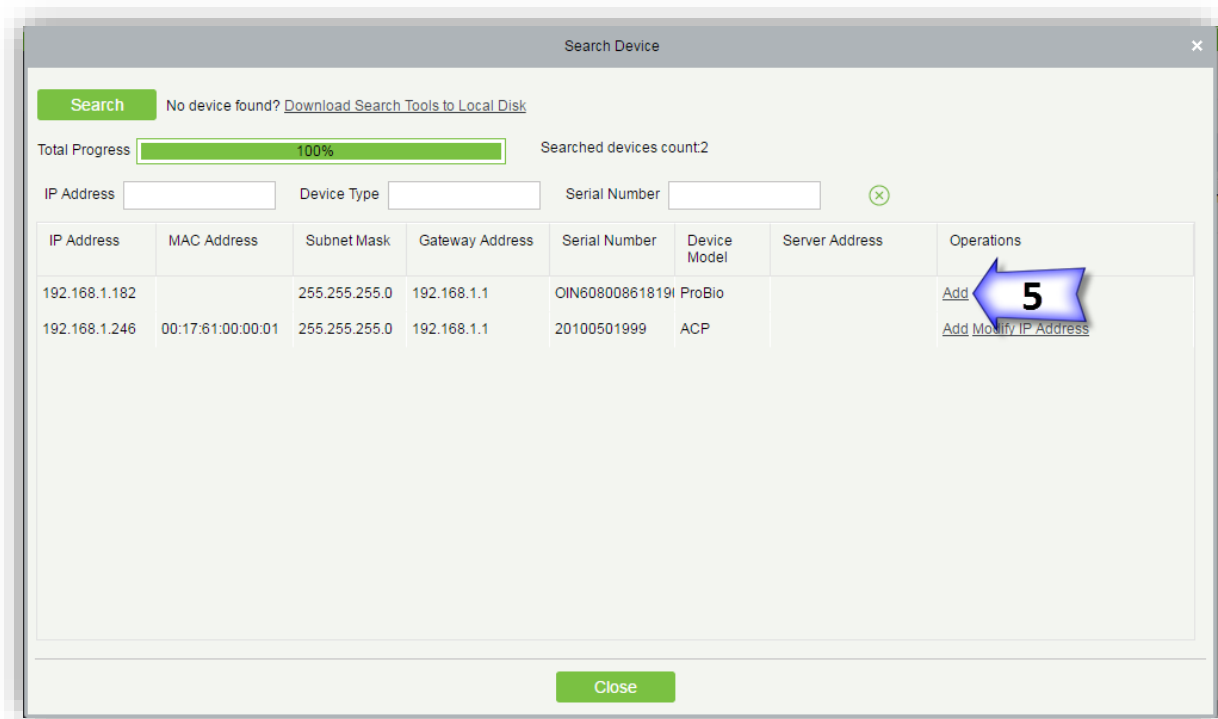
Go to Access→Device→Search Device



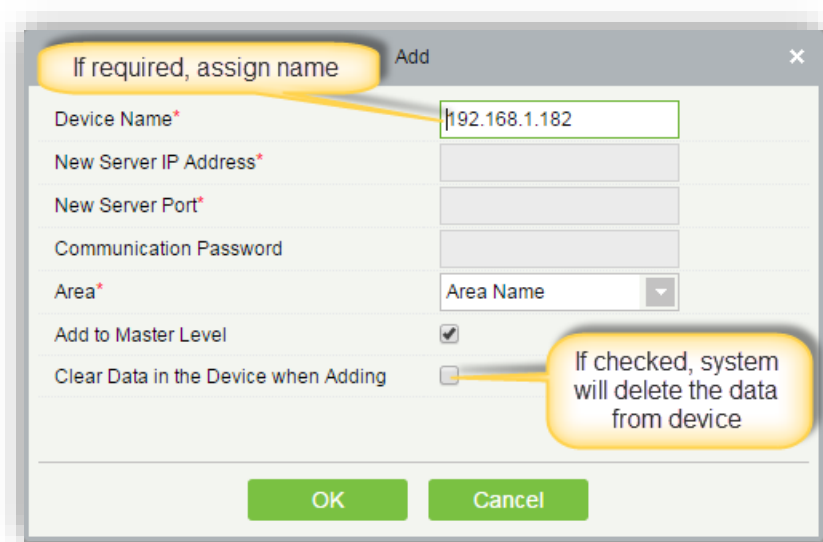
Click on **Search** to search the device.



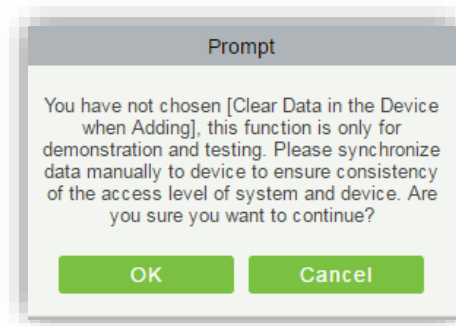
Find the required device in the list and click on **Add**.



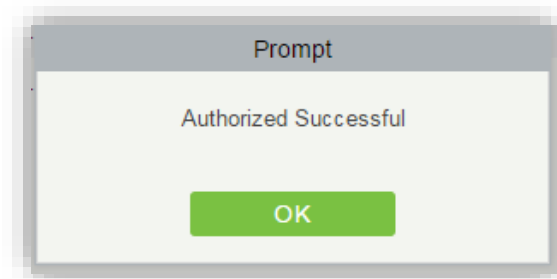
If you want to give a name to identify the device easily, then please enter required name. If you want to clear the data in the device while adding, then check the box below. After entering the details, please click on **OK** to continue.



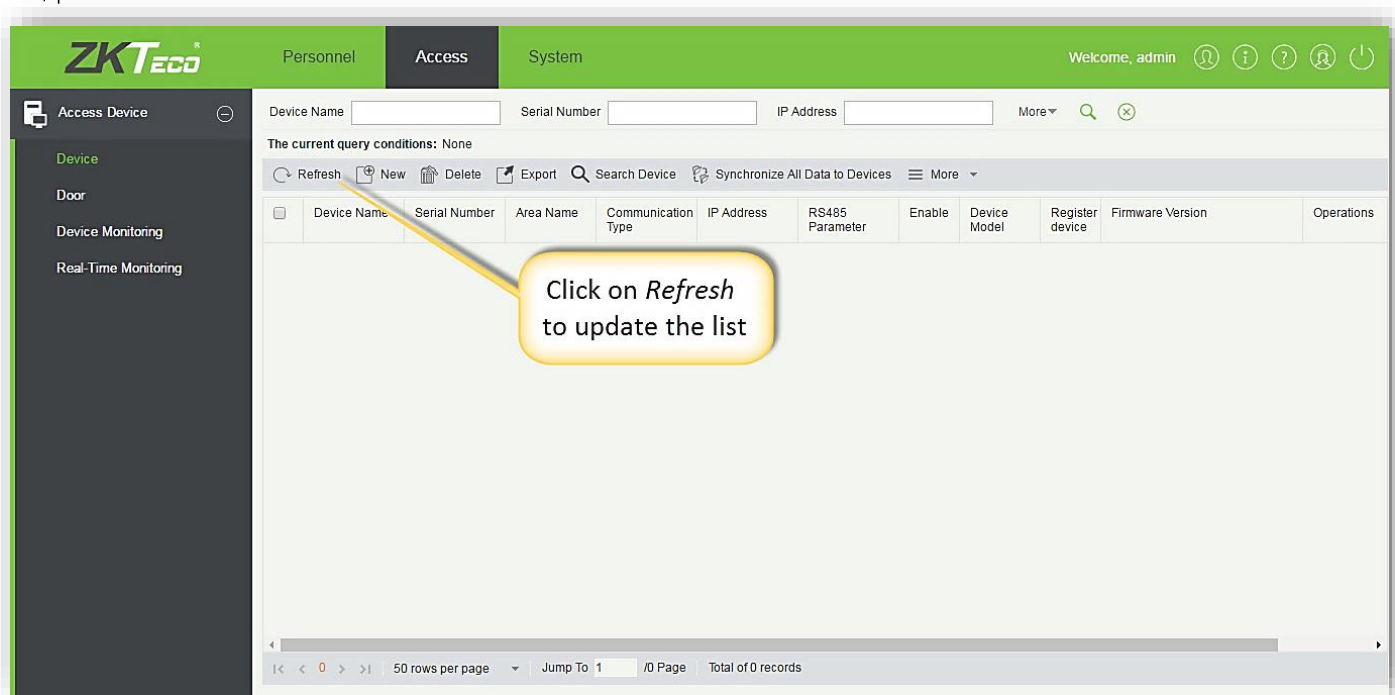
If you have not chosen to clear data while adding, then system will prompt message as shown in the picture below. Please click on **OK** to save.



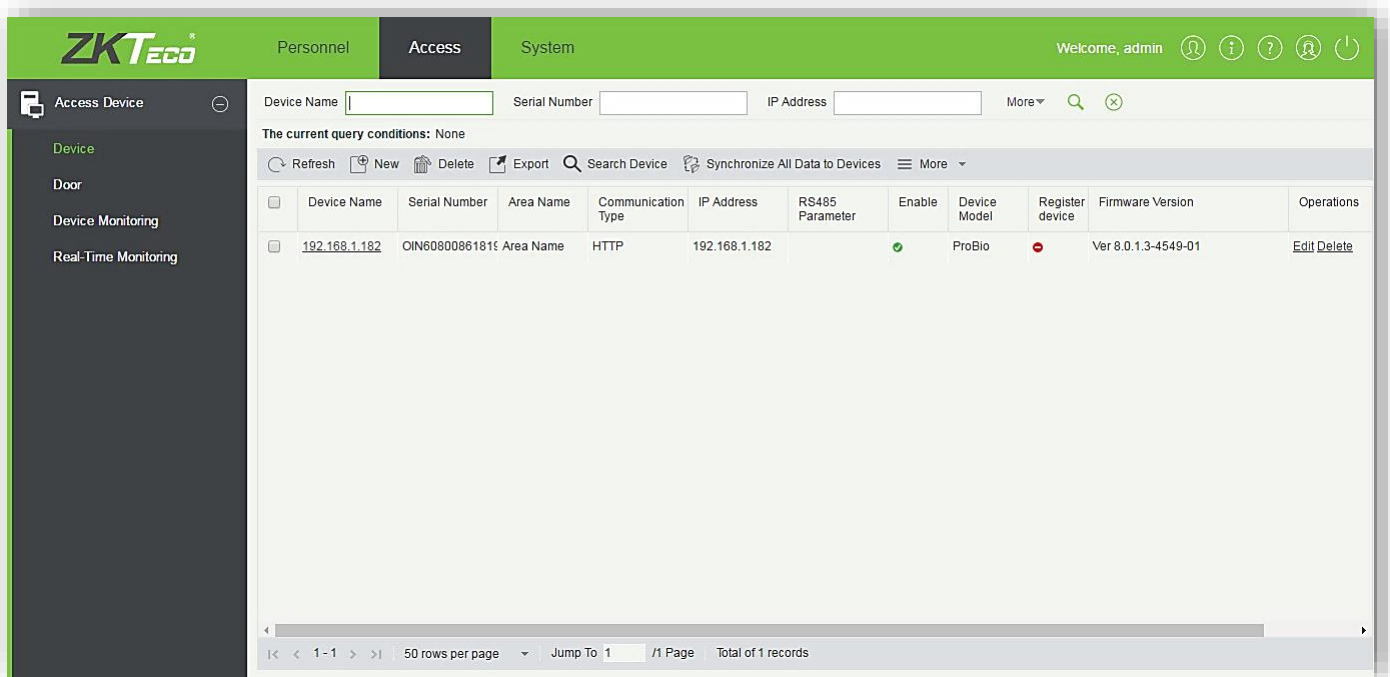
Click **OK** to finish adding the device.



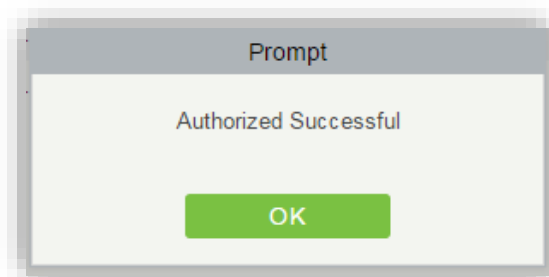
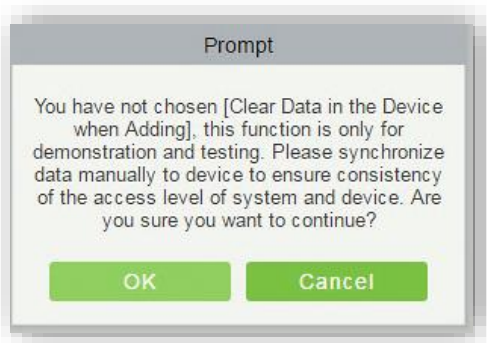
Generally, the device list get refreshed after some few seconds. To see the added device instantly in the list, please click **Refresh** as shown below.



As you can see below, the added device is added in the device list.

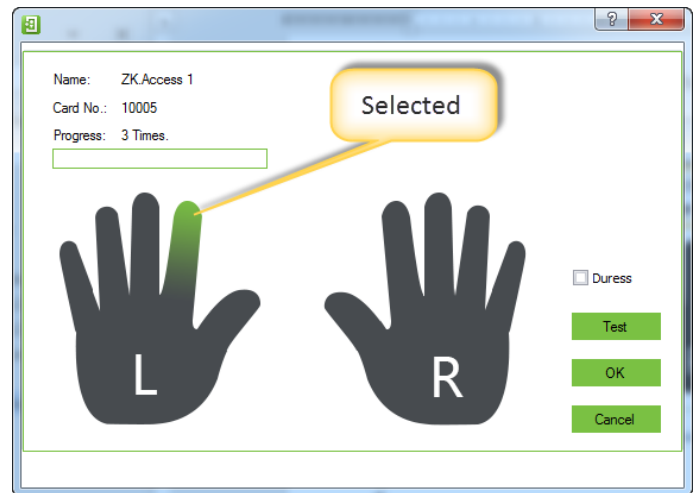
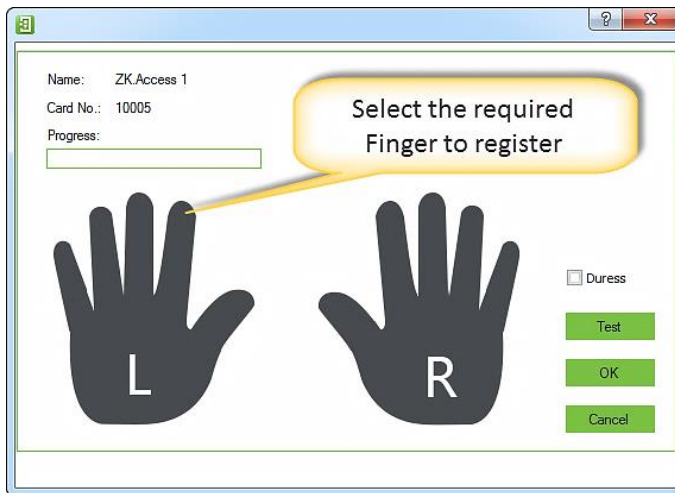


If you have not selected to **Clear Data in Device when Adding** above, then below interface will appear. Click OK to add the device.

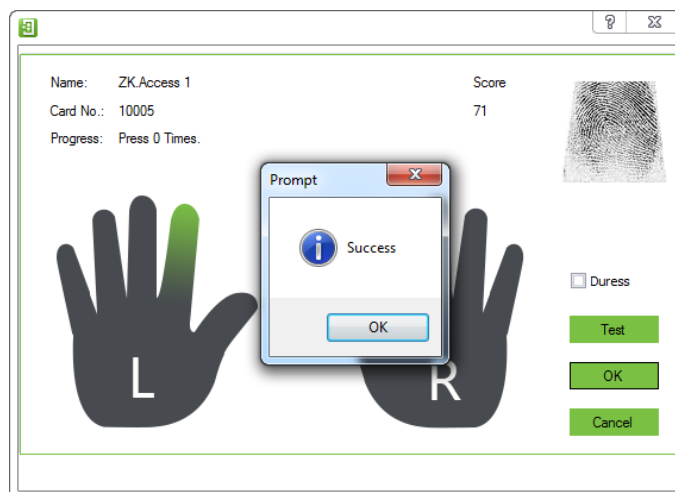


10. Create User/Enroll Fingerprint

For enrolling personnel, use your software to register.

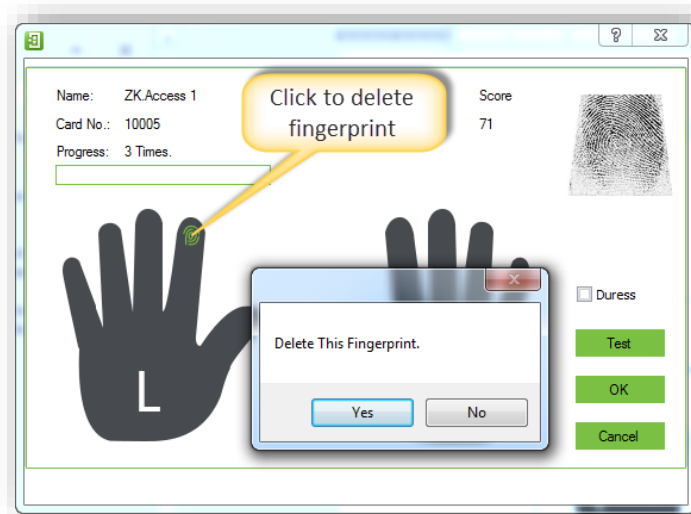


Now press the finger 3 times as prompted.

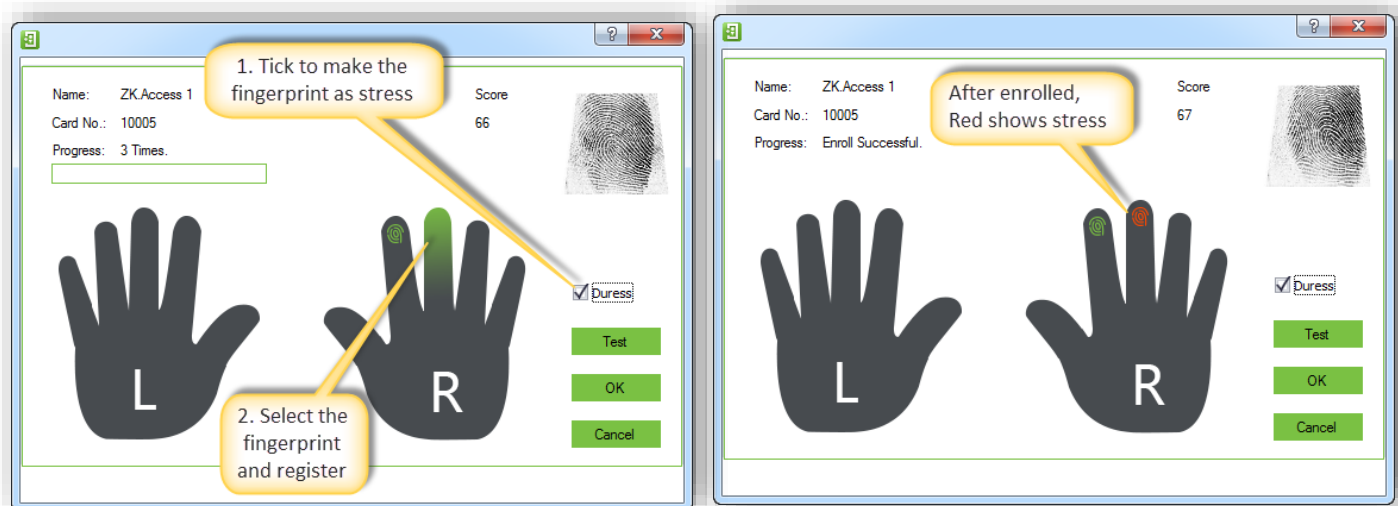


Follow this same process for another finger(s).

If you want to delete fingerprint, then follow below shown method.



If you want to make a fingerprint as a stress fingerprint, then first tick the **Duress** checkbox, then select the fingerprint and register.

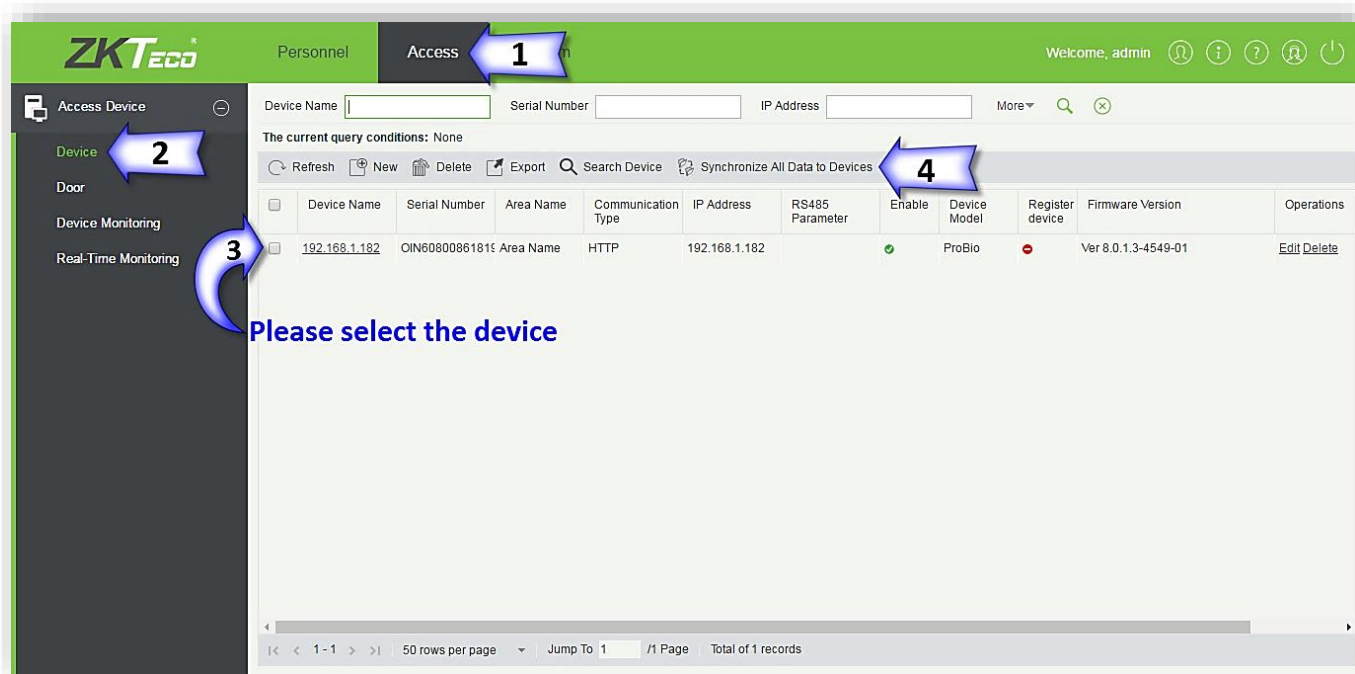


11. Sync to Device

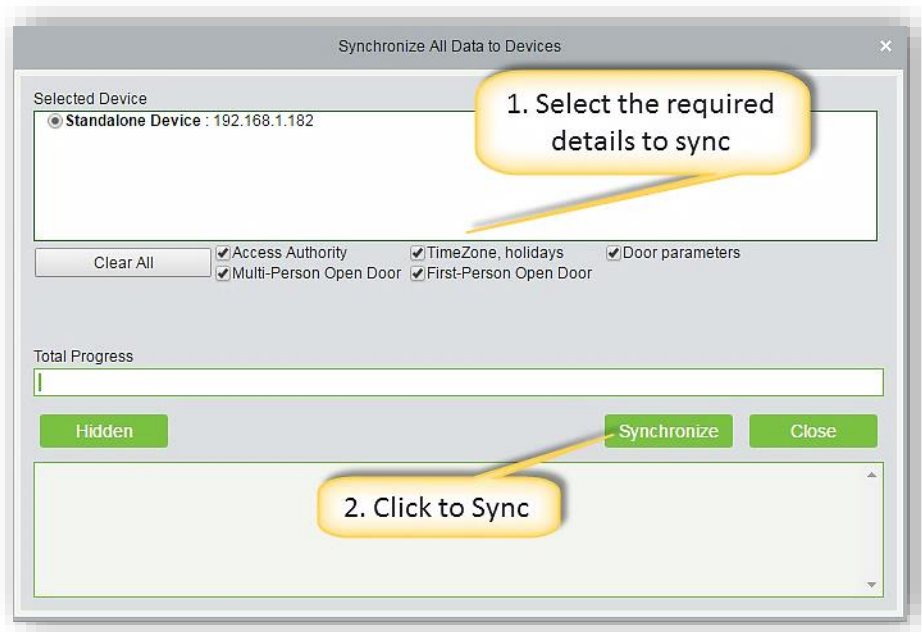
Once the Personnel is enrolled, you can go to ZKBioPack software and synchronize with the device.

You can perform the **Synchronize All Data to Devices** operation on the device list to re-synchronize data in the software to the device.

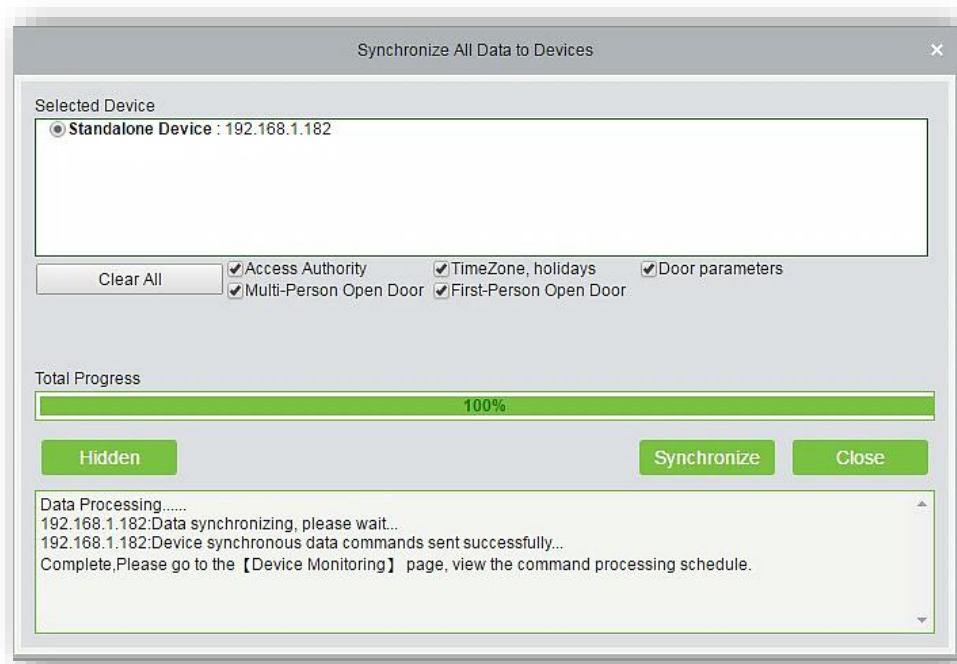
Go to **Access**→**Device**, then select the required device and click **Synchronize All Data to Devices**.



Select the details which you want to sync.

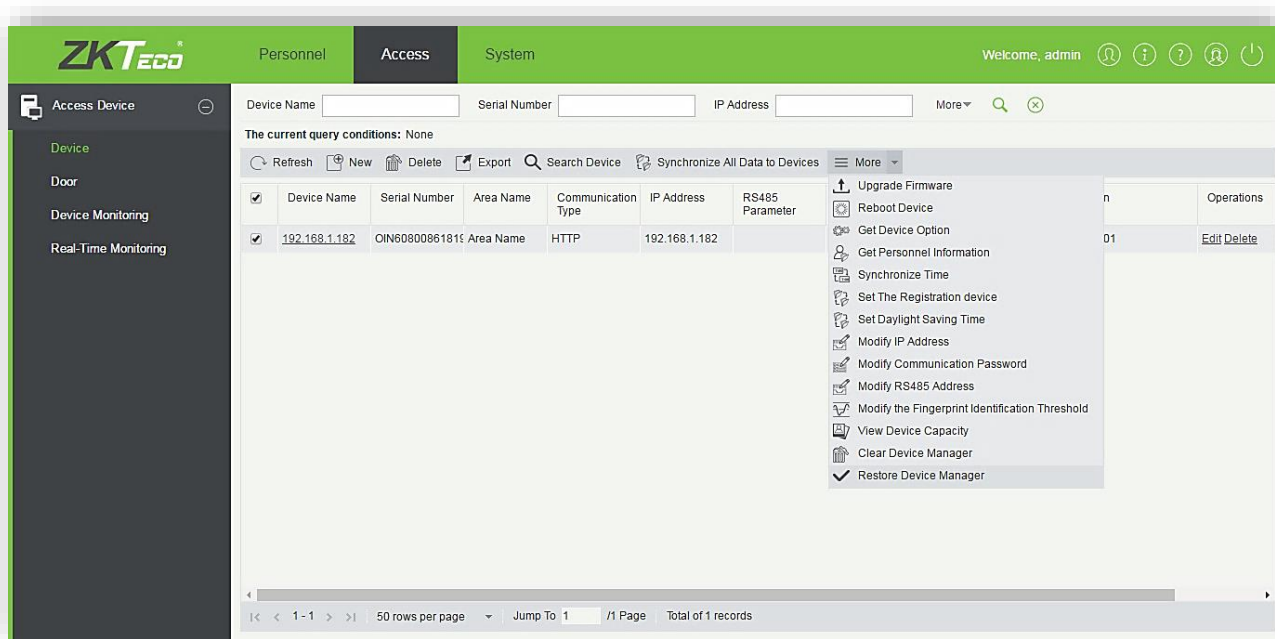


Note: **Synchronize All Data to Devices** is an internal process between device and software, so please keep the net connection stable and avoid power shut down situations, etc.



12. Device Menus

You can add or modify device information through several device menus shown below.



❖ Edit

Click on the Device Name, or select the device and click **Edit** in the Operations to open the edit interface.



Edit

Device Name*

192.168.1.182

Communication Type*

☐ TCP/IP
 ☐ RS485
 ☒ HTTP

Serial Number*

OIN6080086181900001

IP Address*

192.168.1.182

Communication port*

8088

Control Panel Type

Standalone Device

Area*

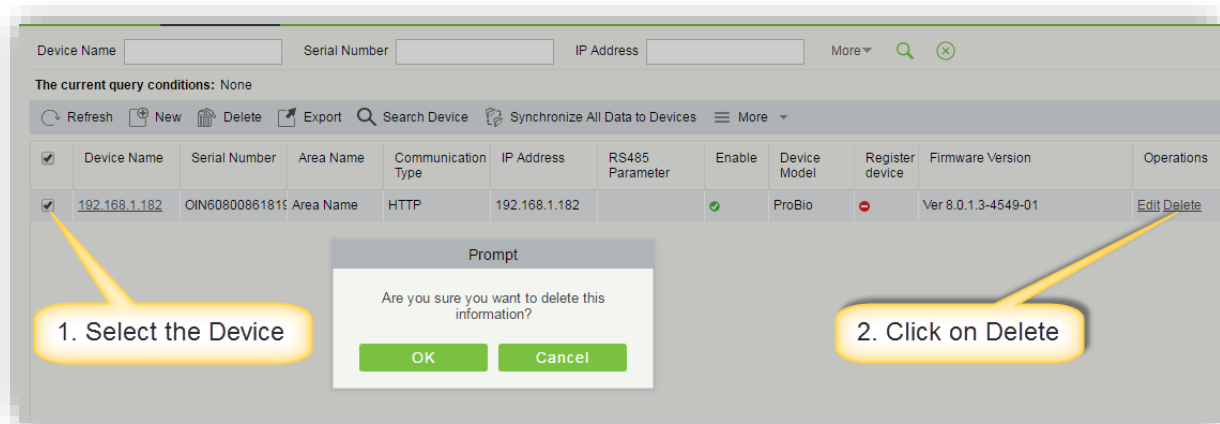
Area Name

OK

Cancel

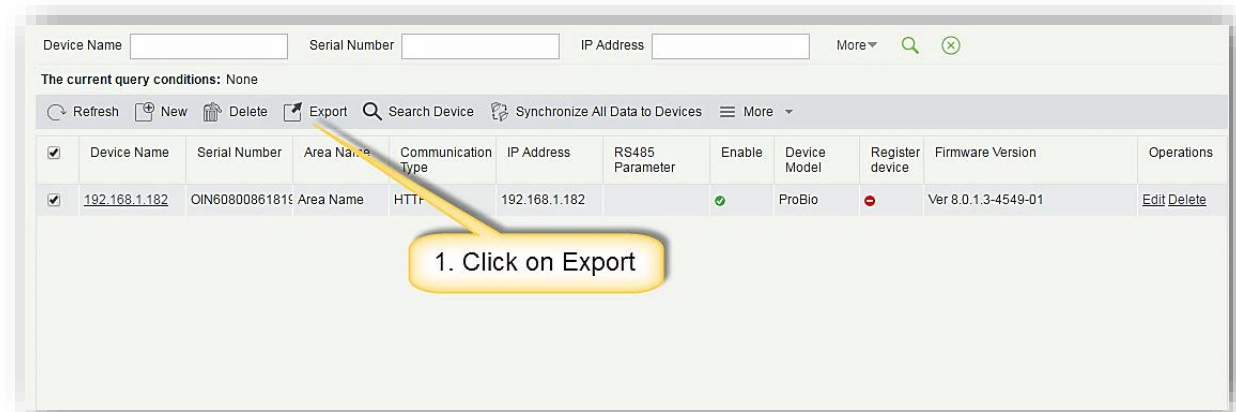
❖ Delete

Click on the Device Name, or select the device and click **Delete** in the Operations to open the edit interface.

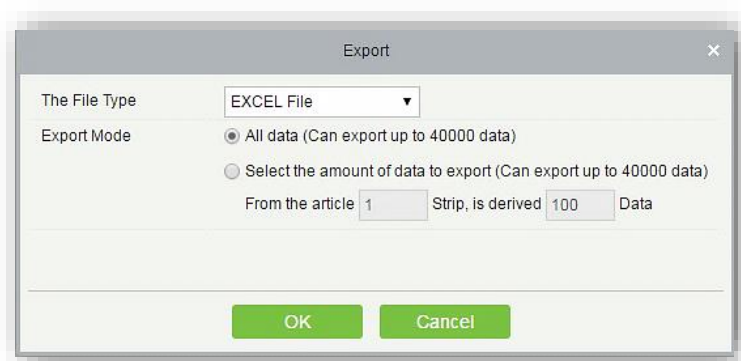


❖ Export

1. Click on Export.

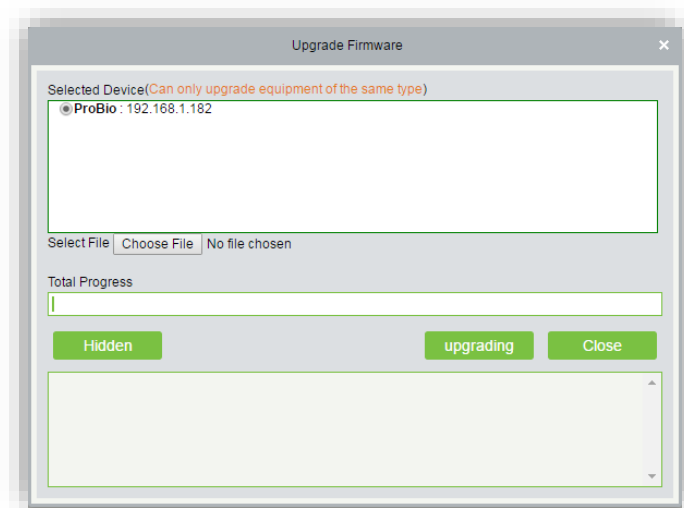
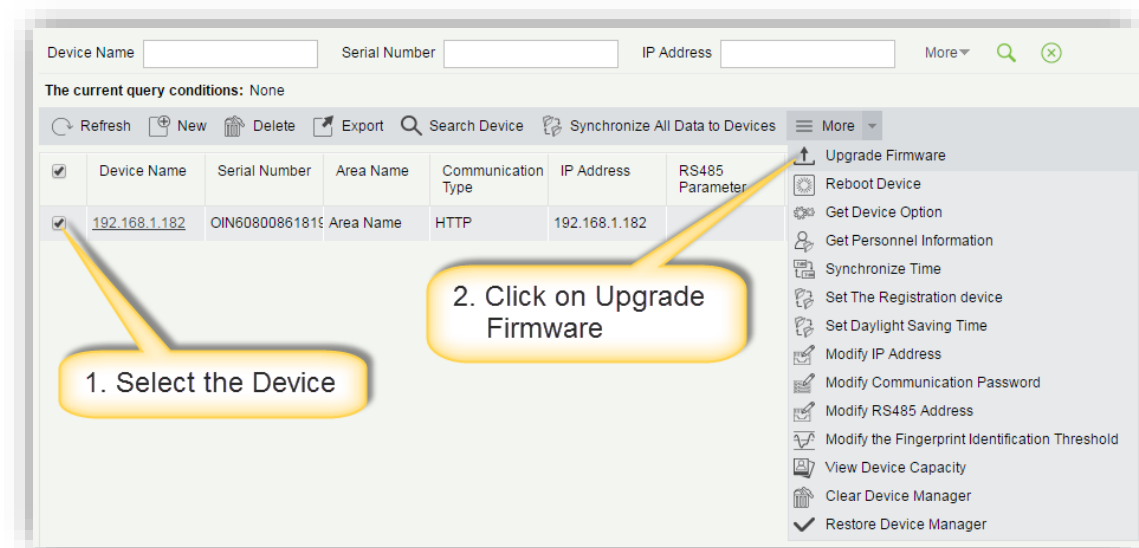


2. Select the file format and export mode to be exported. Click **OK**.
3. You can view the file in your local drive.



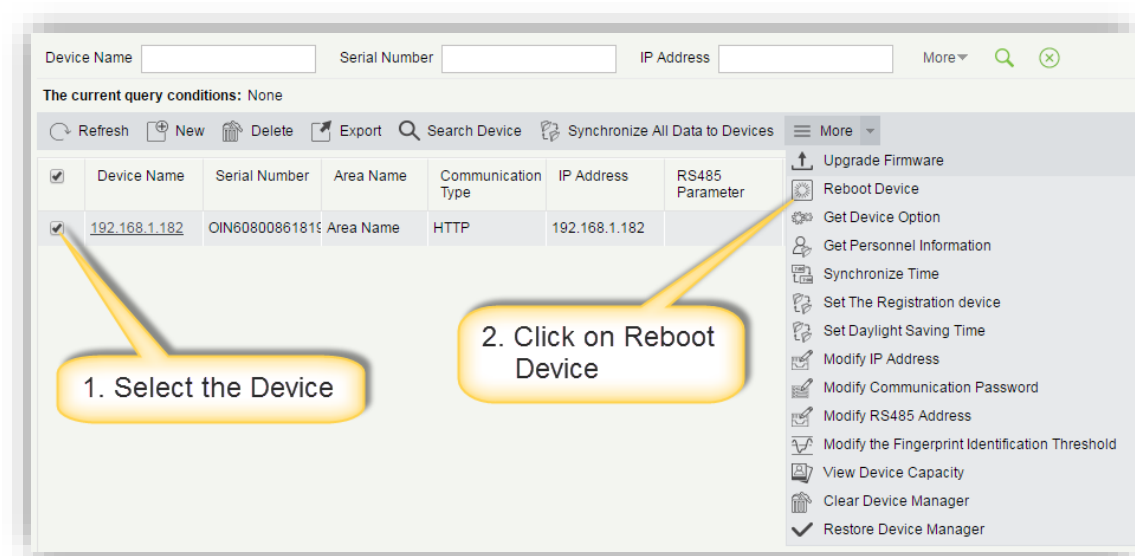
❖ Upgrade Firmware

Select the device that needs to upgrade firmware, then click **Upgrade firmware** to enter edit interface, then click **Browse** to select firmware upgrade file (named emfw.cfg) provided, and click **OK** to start upgrading.



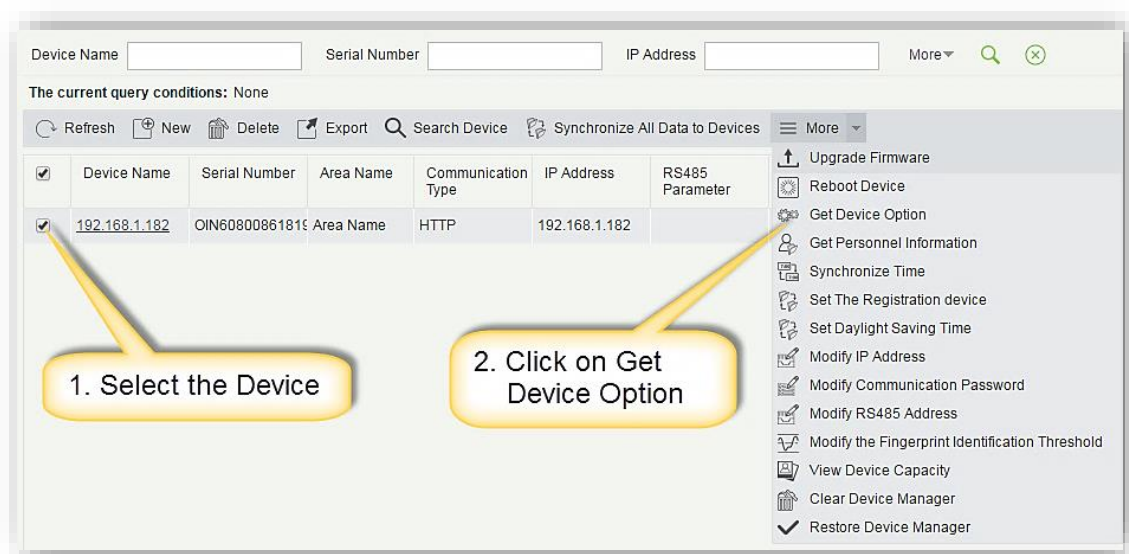
❖ Reboot Device

To reboot the selected device.



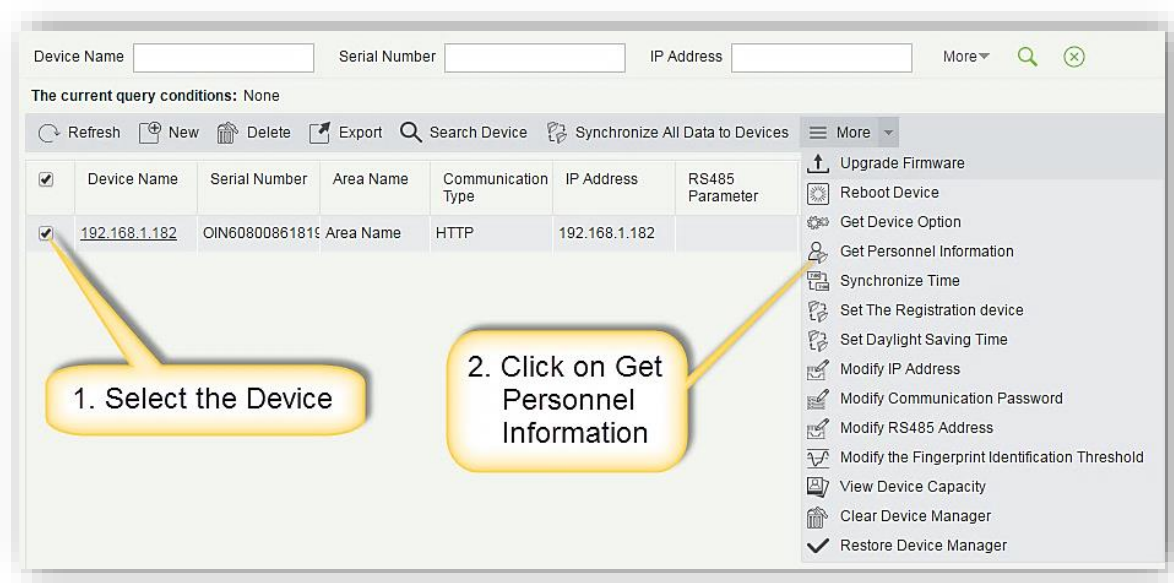
❖ Get Device Option

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



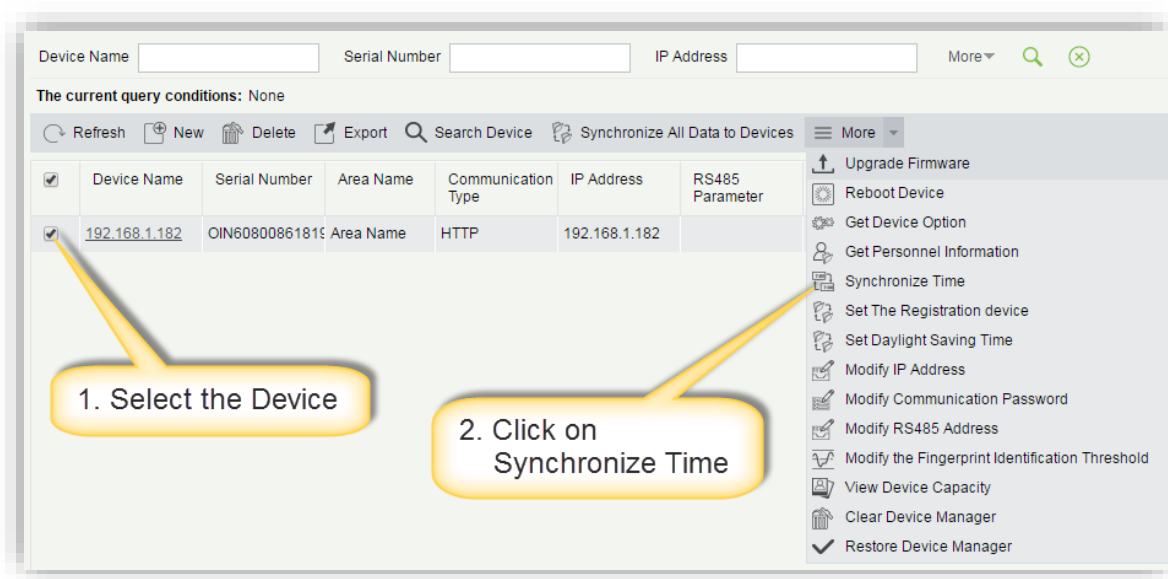
❖ Get Personnel Information

To get personnel information of fingerprint, finger vein, face or get the number of the corresponding data.



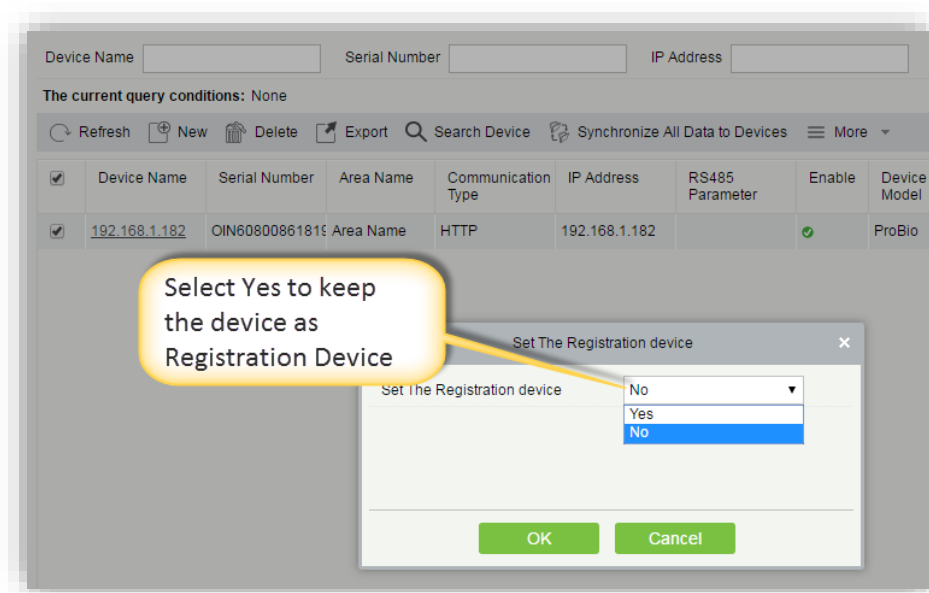
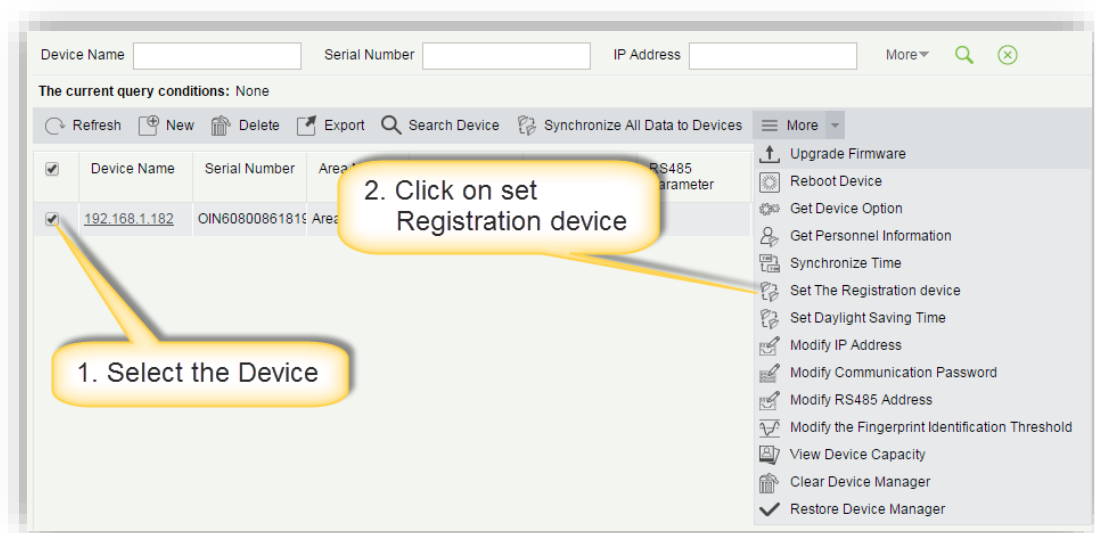
❖ Synchronize Time

Synchronize device time with current server time.



❖ Set the Registration Device

The data from standalone device can be uploaded to the system automatically.

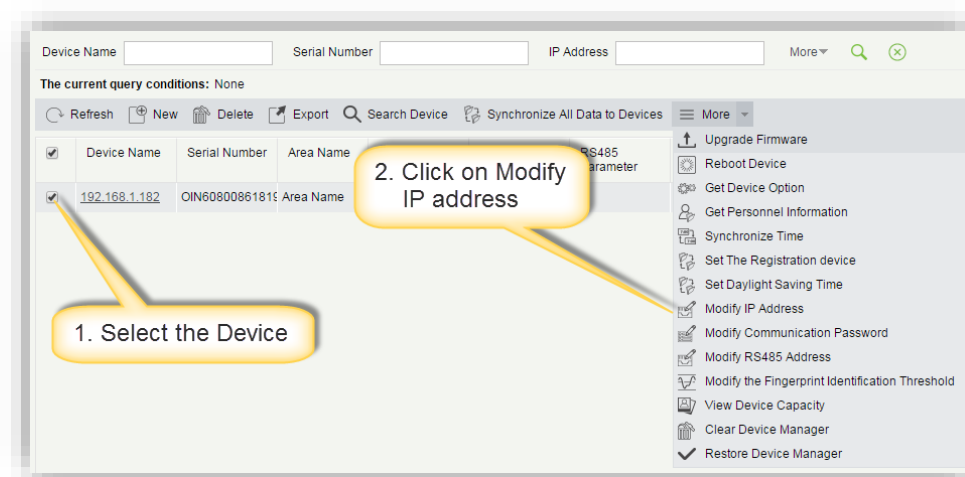


❖ Set Daylight Saving Time

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

❖ Modify IP Address

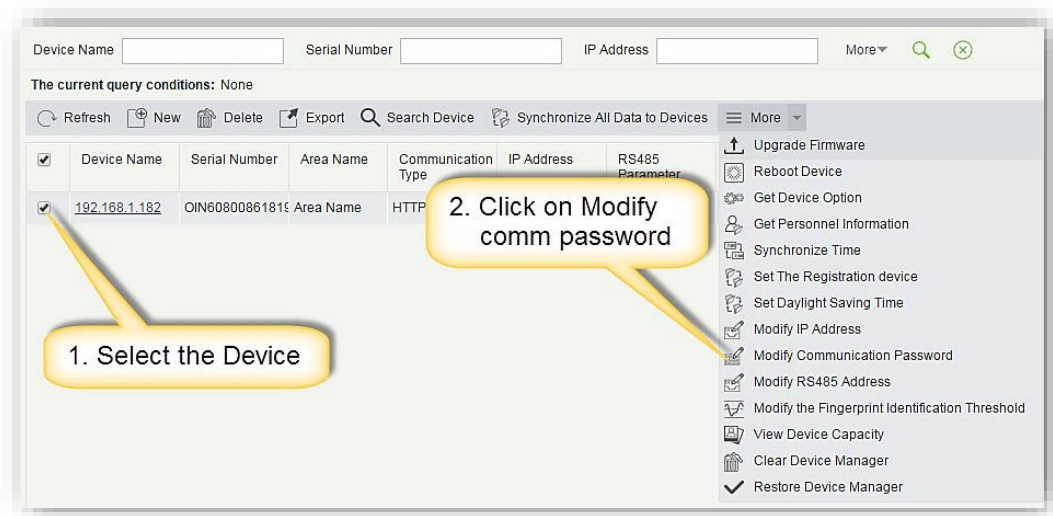
Select device and click **Modify IP address** to open the modification interface. It will obtain real-time network gateway and subnet mask from the device (If obtaining fails, IP address cannot be modified). Enter new IP address, gateway, and subnet mask. Click **OK** to save settings and exit.



❖ Modify Communication Password

Enter the old communication password before modification. After verification, input the same new password twice, and click **OK** to modify the communication password.

Note: Communication password cannot contain space; it can only be integer. Communication password setting can improve the device security. It is recommended to set communication password for each device.

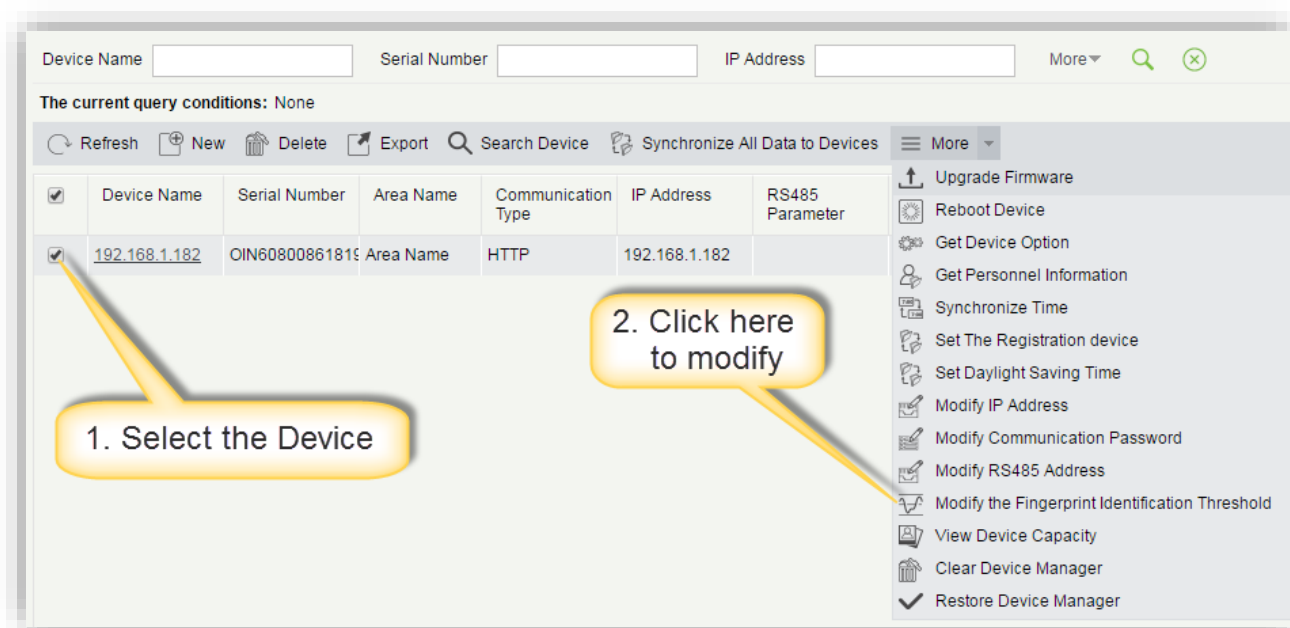


❖ Modify RS485 Address

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

❖ Modify the Fingerprint Identification Threshold

User can modify the fingerprint identification threshold in the device; scale is 35-70 and 35 by default. When adding a device, the system will read the threshold from the device. User can view the threshold in the devices list.

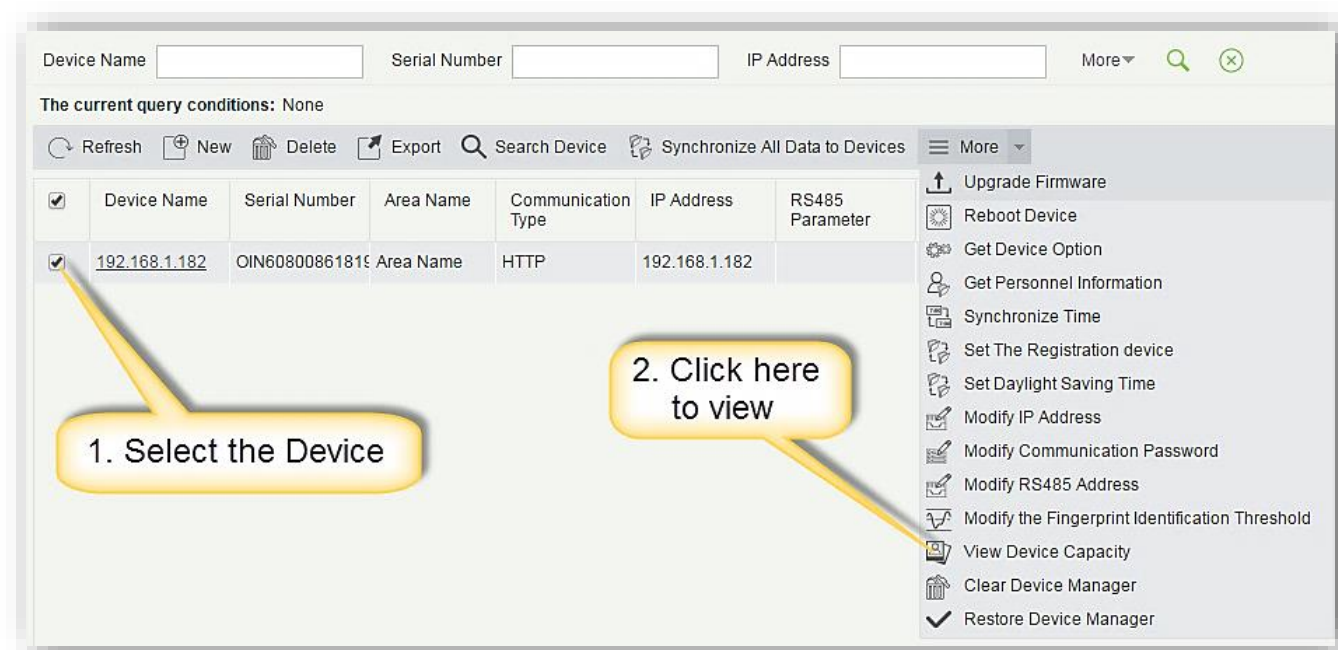


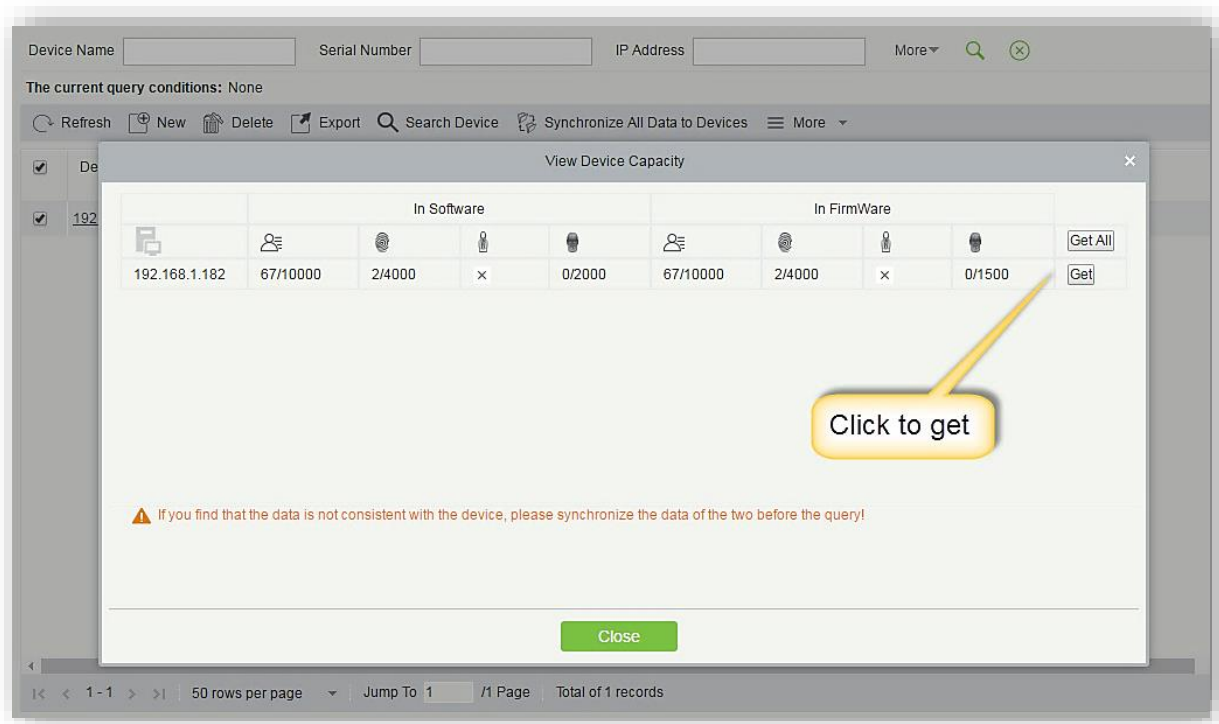
❖ View Device Capacity

Check the capacity of personnel's fingerprint/face/finger vein in the device.

From the statistical software information; the user can confirm the adequacy of equipment capacity (personnel, fingerprints, etc.).

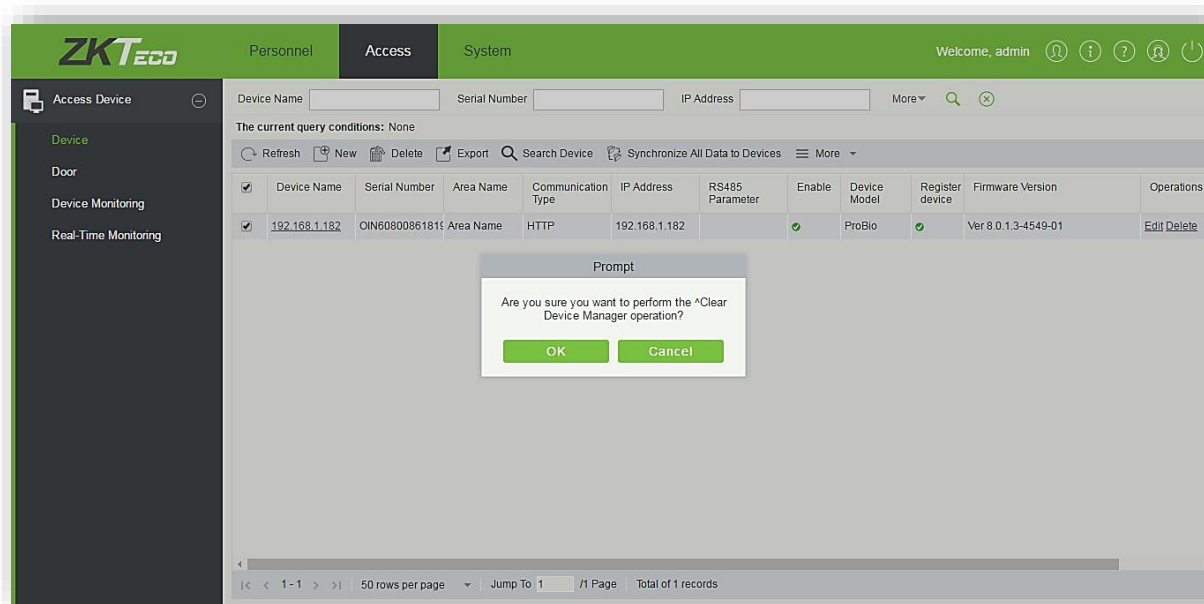
If data found from the software and information obtained from the device is inconsistent, you can manually sync data.





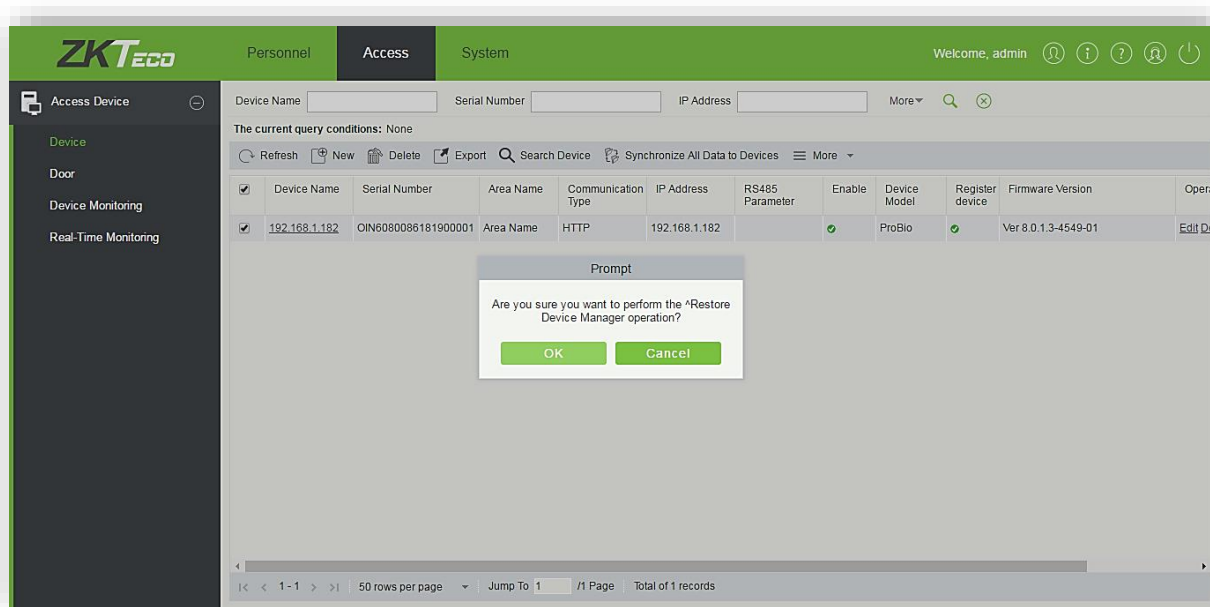
❖ Clear Device Manager

This function is used to clear all the administrator's (Super user) privileges and allow any normal user to access the device.



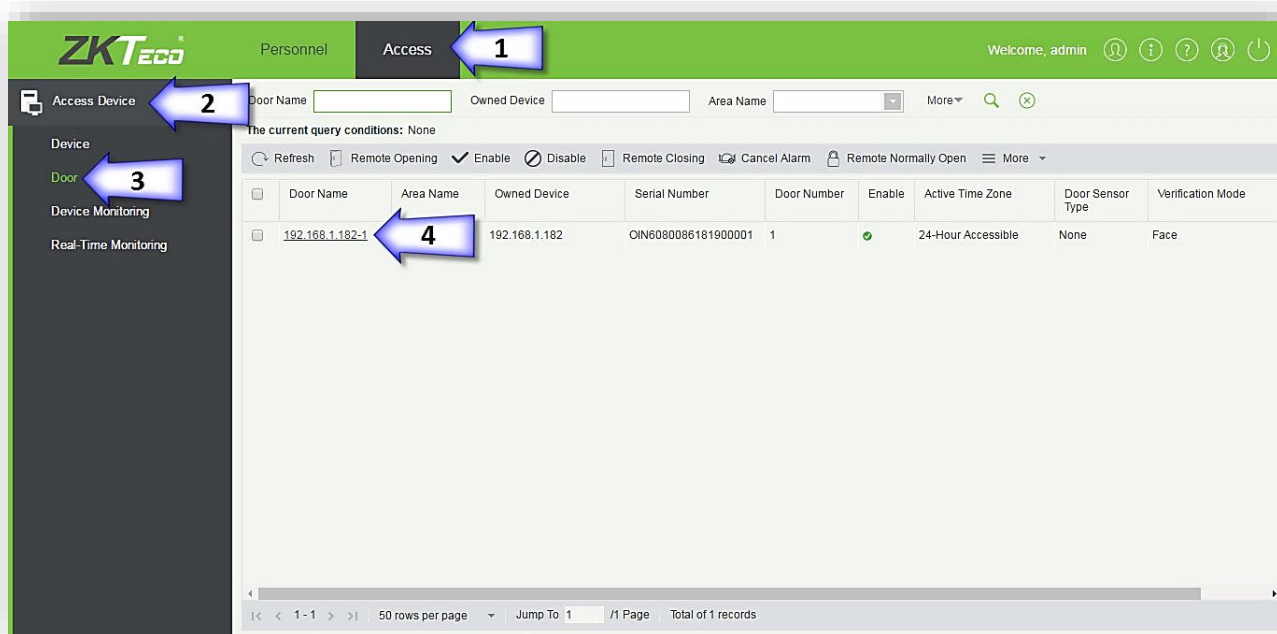
❖ Restore

This function is used to restore all the administrator's (Super user) privileges.



❖ Door Module

Click **Access** → **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).



A. Once you click on the device name, you will get below interface.

Edit	
Device Name*	192.168.1.182
Door Name*	192.168.1.182-1
Verification Mode*	Face
Operate Interval*	0 second(0-254)
Anti-passback Duration of Entrance	0 minute(0-120)
Duress Password	(Maximum 6 Bit Integer)
Emergency Password	(8 Bit Integer)
Disable Alarm	<input type="checkbox"/>
Door Number*	1
Active Time Zone*	24-Hour Accessible
Lock Open Duration*	5 second(1-254)
Door Sensor Type*	None
Door Sensor Delay	second(1-254)
Passage Mode Time Zone	-----
The above settings are copied to -----	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Device Name: It is not editable.

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

Note: By default, the number following the underline in the Door Name is consistent with the Door Number.

Door Name: The default is "device name -door number." The field allows user to modify as required. Up to 30 characters can be entered.

Active Time Zone: By default, it will be 24-Hour accessible.

Verification Mode: Identification modes include all the combination of Fingerprint, Card, Face and Password. Recommended is Automatic Identification. The default is Face. When Card plus Password mode is selected, make sure the device supports card verification.

Lock Open Duration: Used to control the delay for unlocking after punching. The unit is second (controller range: 0 to 254 seconds, one machine range: 1 to 254), and the default is 5 seconds.

Door Sensor Type: None (Door sensor not detected), Normal Open, Normal Close. The default is NO. When door sensor type is set as Normal Open or Normal Close, the default door sensor delay is 15 seconds, and enables close and reverse state.

Duress Password, Emergency Password: Upon duress, use the Duress Password (used with legal card) to open the door, when opening with Duress Password, it will alarm. 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 legal card): Password is 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. Finally, punch legal card. The door opens and triggers the alarm. When Card + Password verification mode is used, please punch legal card first, then press the password plus **OK** button (same to normal opening in card plus password verification mode), the door open and trigger 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 a 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 the two passwords should not be the same.

Passage Mode Time Zone: By default, it will be none. Passage Mode Time Zone must be set within the Active Time Zone.

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

The above settings are copied to: Includes below option.

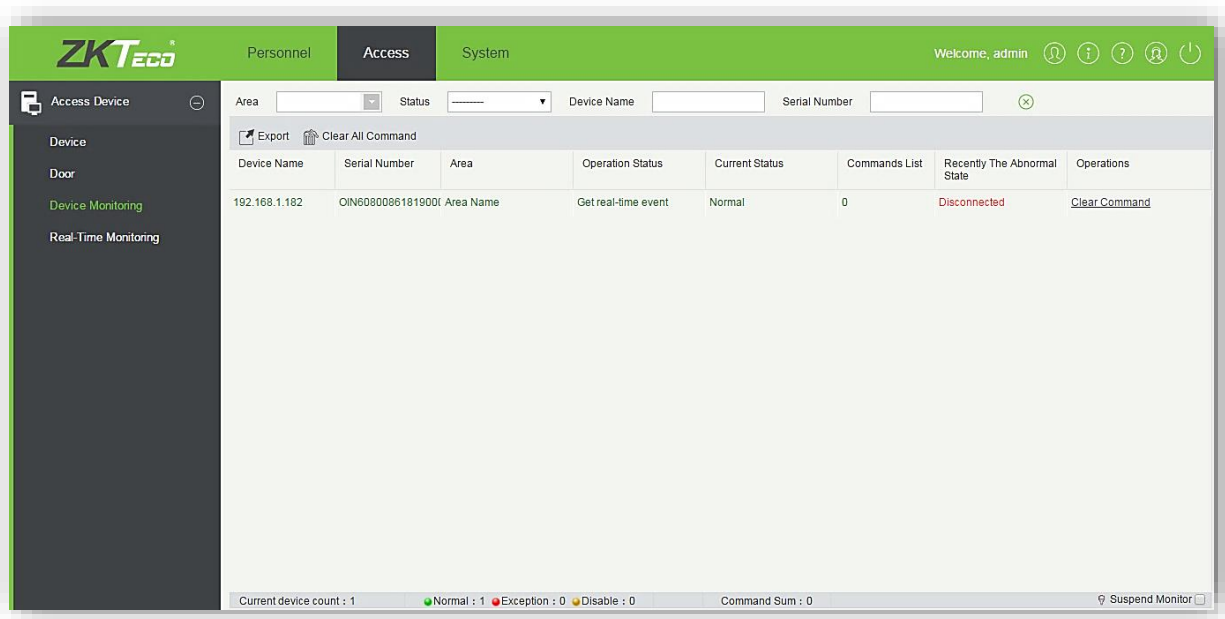
- All doors of all Standalone devices: Click to apply to all doors of all devices within the current user's level.

B. After parameter editing, click **OK** to save and exit.

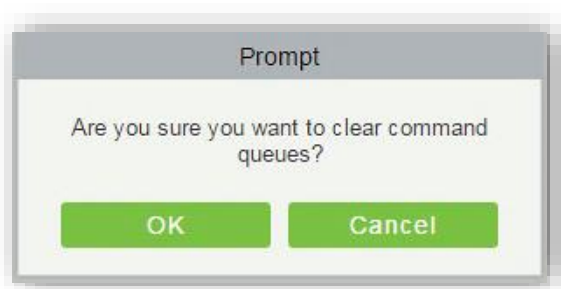
❖ Device Monitoring

By default, it monitors all devices within the current user's level.

Click **Access Device → Device Monitoring**, and it lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, Recently the Abnormal state, and Related Operation.



You may clear command as required. Click **Clear Command** behind the corresponding device:



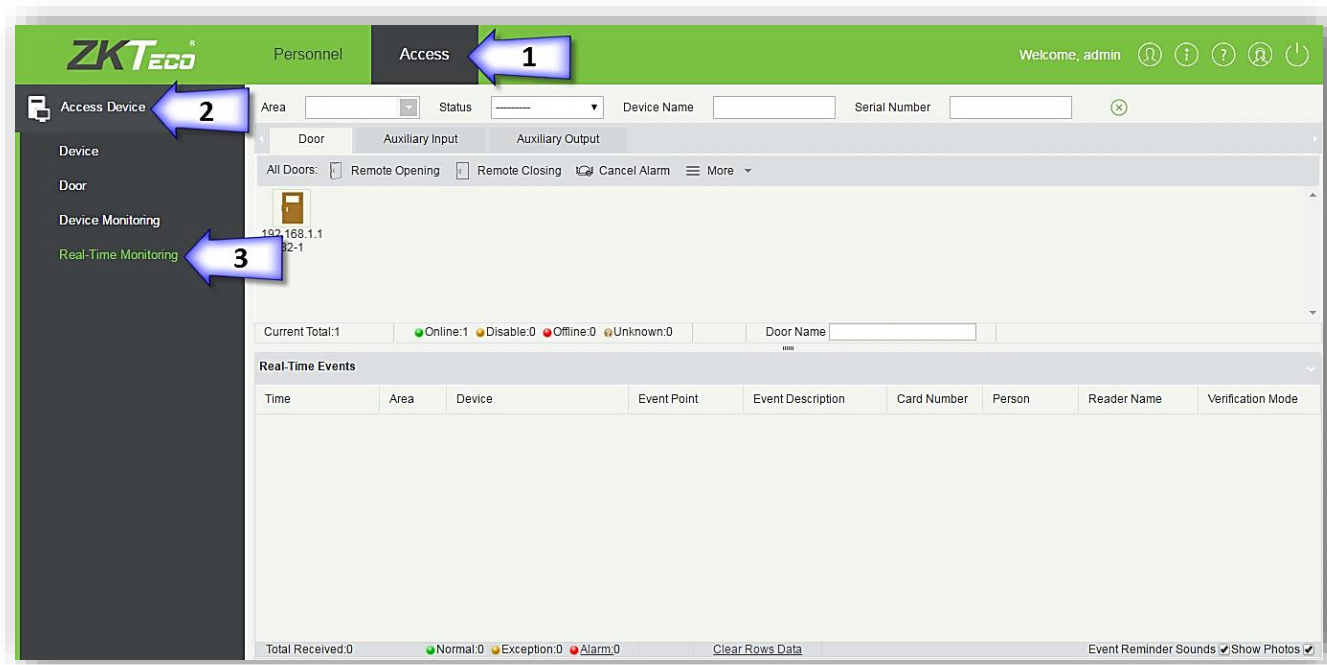
Click **OK** to clear.

Note:

- a) After the Clear Command is executed, you can perform the Synchronize All Data to Device operation on the device list to re-synchronize data in the software to the device, but this operation cannot be performed when the user capacity and fingerprint capacity are fully consumed on the device. Once the capacity is insufficient, you may replace the current device with a large-capacity one, or delete the right of some personnel to access this device, and then perform the Synchronize All Data to Device operation.
- b) Operate State is the content of communications equipment of the current device, mainly used for debugging.
- c) In the command list, the number of commands to be performed is greater than 0, indicating that data is not synchronized to the device, so just wait.

❖ Real-time Monitoring

Click **Access** → **Access Device** → **Real-Time Monitoring** to monitor the status and real-time events of devices under the access control panels in the system in real-time, including normal events and abnormal events (including alarm events). Real-Time Monitoring interface is shown as follows:



Different icons represent status as follows:

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

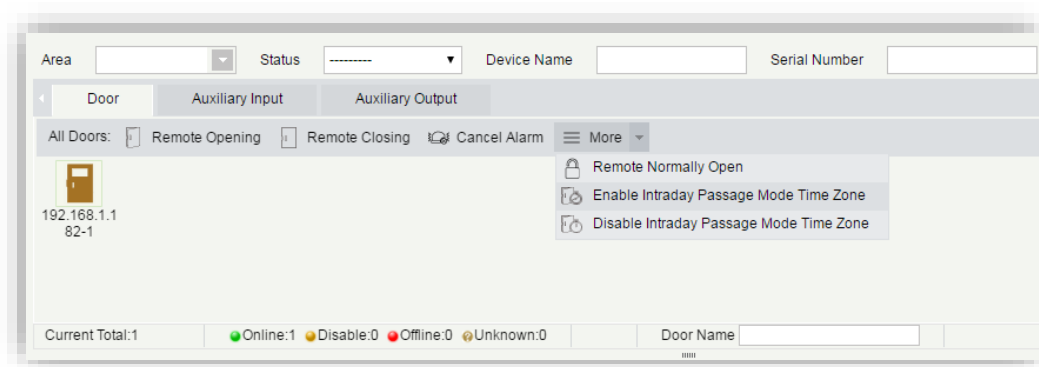
	Door opening timeout, Relay closed/ Door Sensor Closed		Door opening timeout, Relay opened/ Door Sensor Closed
	Door closed alarming, Relay closed/Without relay status		Door closed alarming, Relay opened/Without relay status
	Door sensor unset, Door alarming, Relay closed		Door sensor unset, Door alarming, Relay opened

Note: Without relay status, indicates that the current firmware does not support detect relay status function.

An example of Real-Time Event is shown below. When a registered person punches then below pop-up message will come at the bottom right corner.

Remote Opening/Closing: Controls one door or all doors. To control a single door, right click mouse, 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 duration of a door being open (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 is not limited by any time zones (open for 24 hours).



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

Note: If **Remote Opening /Closing** always fails, check whether many devices are disconnected. If any, check the network.

Cancel Alarm: Once an alarming door is displayed on the interface, the alarm sound will ring. Alarm cancellation is involved in control on single door and all doors. To control a single door, put the mouse over the door icon, to pop out a menu, and then click **Remote Opening/ Closing**. To control all doors, directly click **Remote Opening/ Closing** behind Current All.

Note: If **Cancel the alarm** fails, check whether many devices are disconnected. If any, check the network.

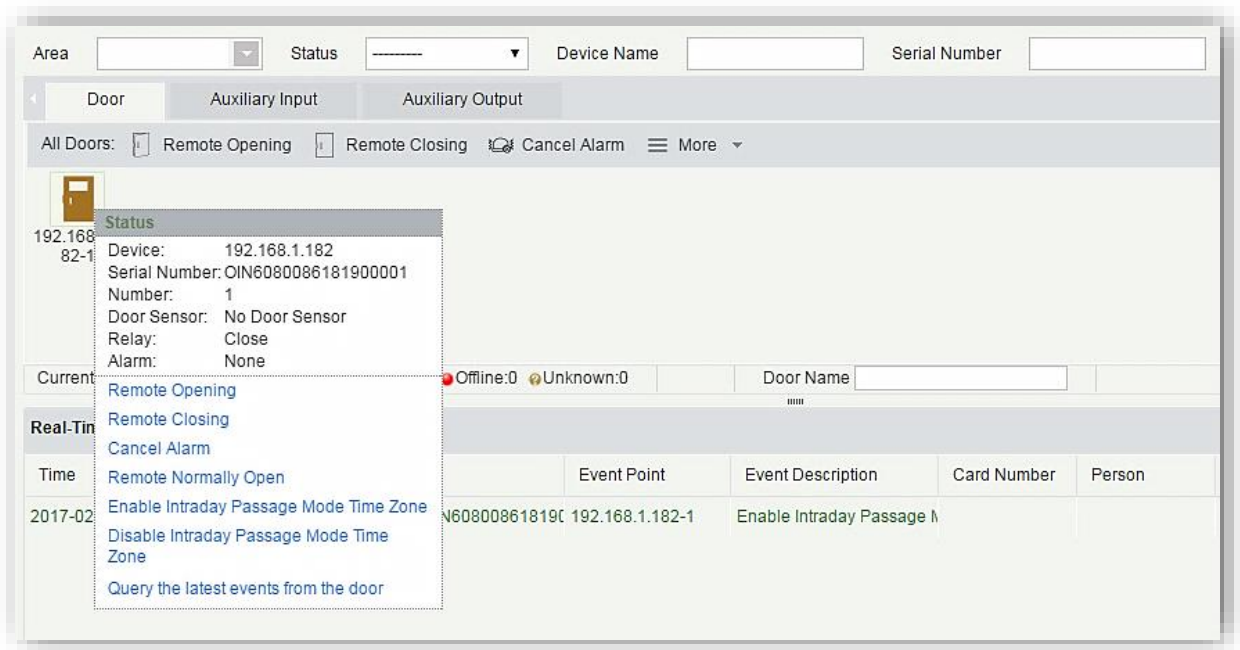
Remote Normally Open: Set the device as normal open by remote.

Show Photos: At the bottom right corner, you can see the Check box. If Real-Time Monitoring is involved in a person, the monitor displays the personal photo (if no photo is registered, display default photo). The event name, time and name are displayed.

Event Reminder Sounds: After checking this option, it plays a sound once an alarming event occurs of the current page.

● Quick Management of Doors

Move the cursor to a door's icon; you can also do the above operations. In addition, you can query the latest events from the door.



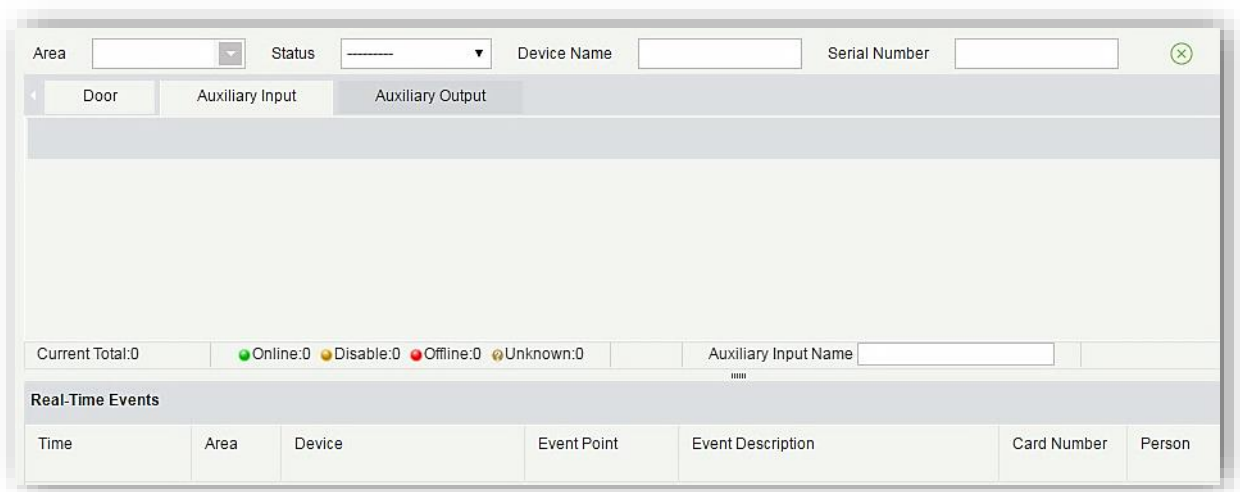
Query the latest events from the door: Click to quickly view latest events happened on 5 doors.
 Issue card to person: If you swap an unregistered card, in real-time monitoring interface, will turn up a record with a card number. Right click that card number will show you a menu, click "Issue card to person," you can assign that card to one person.

● Event monitoring

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

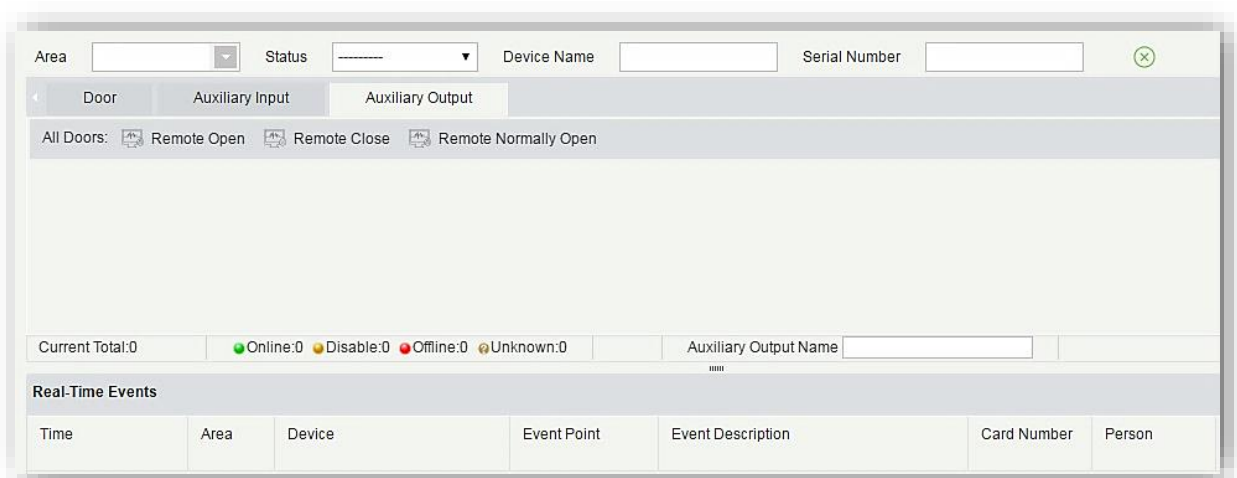
A. Auxiliary Input

Real-Time monitor the current auxiliary input events.



B. Auxiliary Output

You can perform Remote open, Remote Close, Remote Normally Open.



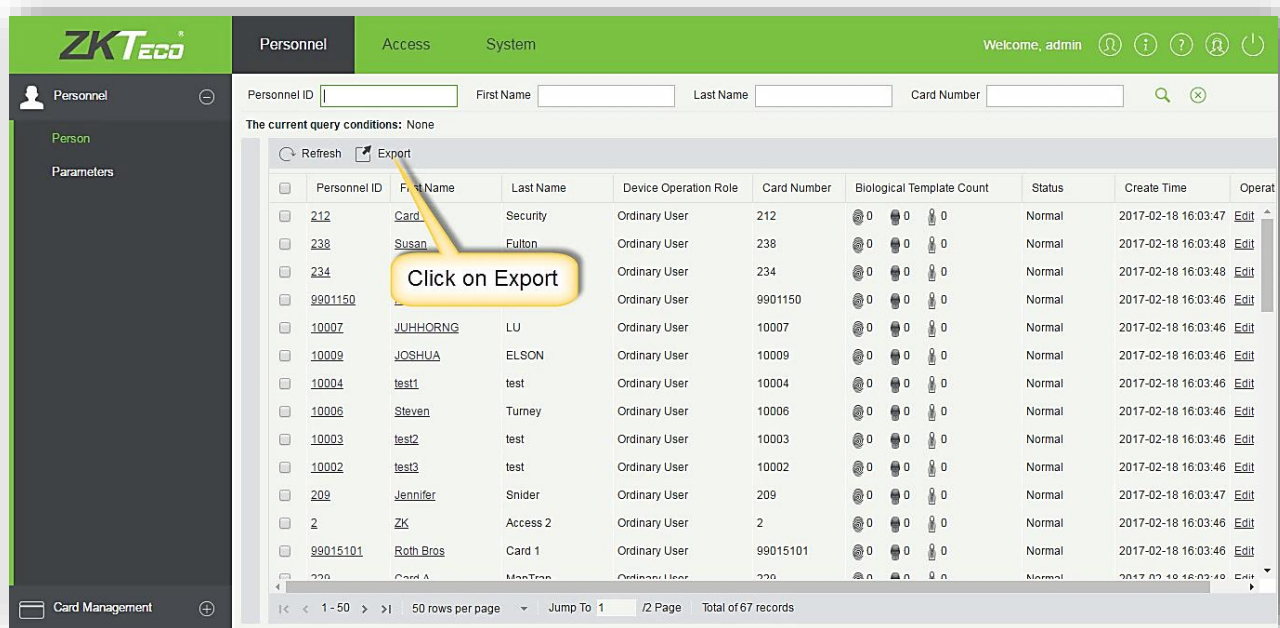
13. Personnel Menus

Personnel menus includes viewing/editing Personnel, exporting Personnel, edit passwords, registering fingerprint and card number.

Note: Data in this module can only be viewed or modified but cannot be deleted.

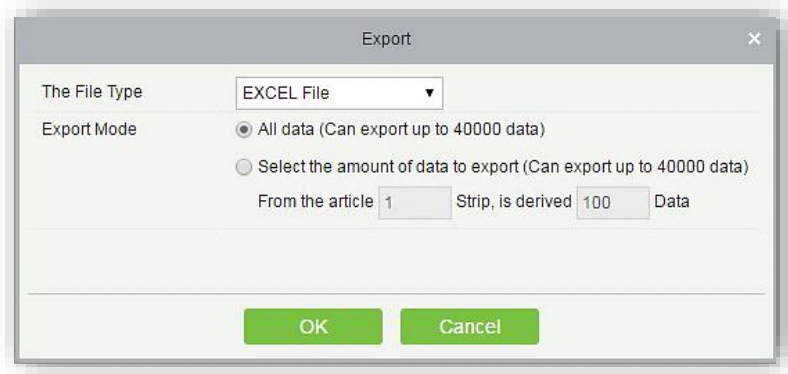
❖ Export

1. Click on Export.



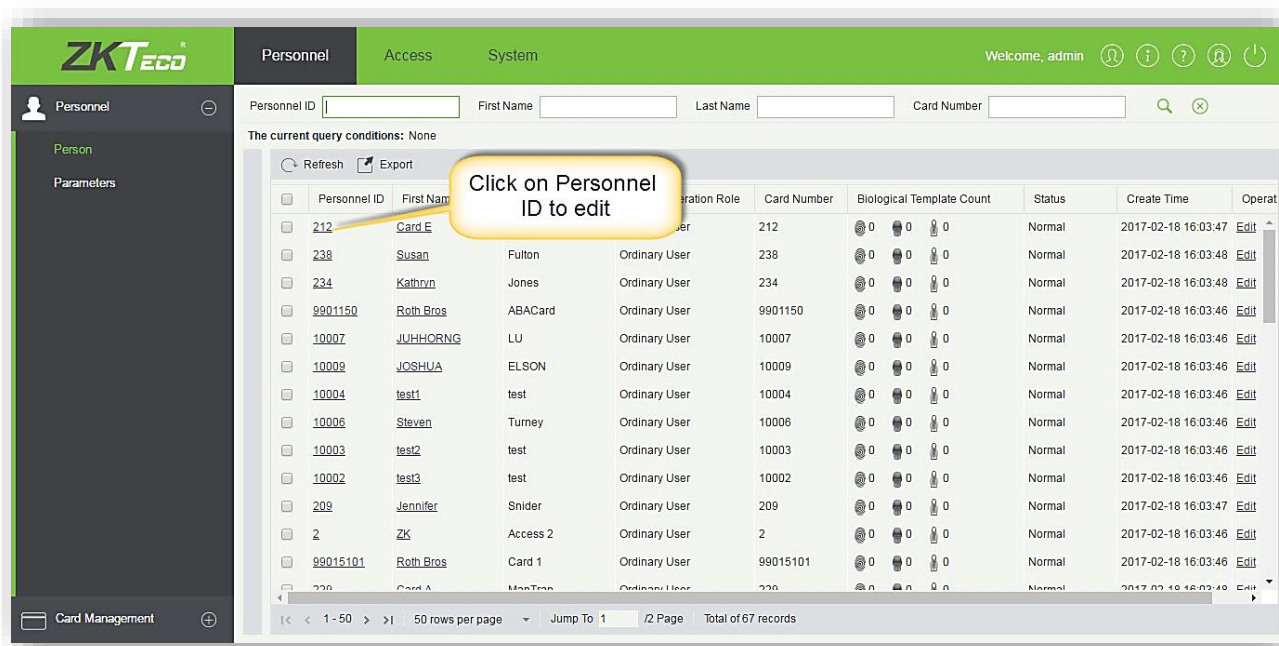
2. Select the file format and export mode to be exported. Click OK.

- You can view the file in your local drive.



❖ Editing Personnel(s)

Through this function, you can edit the name, password and Device role. You can also add fingerprint, issue card, upload picture of the personnel.



Personnel ID* 212

First Name Card E Last Name Security

Password Device Operation Role Ordinary User

Fingerprint Register 0

Card Number Type Without Site Code Site Code Card Number 212

1. You can register fingerprint from here

2. You can issue card from here

OK Cancel

1. Registering fingerprint

You can register fingerprint as shown below.

Fingerprint

Make sure you have connected a USB fingerprint reader to your PC

No fingerprint readers detected.

Click on the finger which you want to register and let the personnel punch

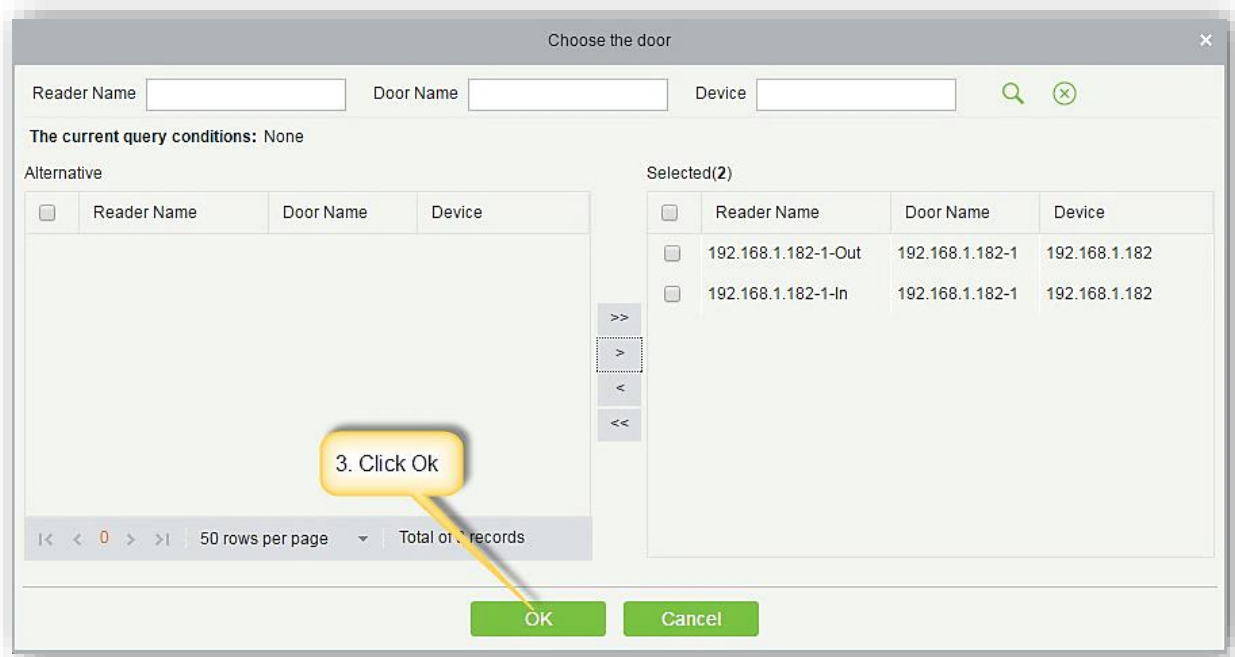
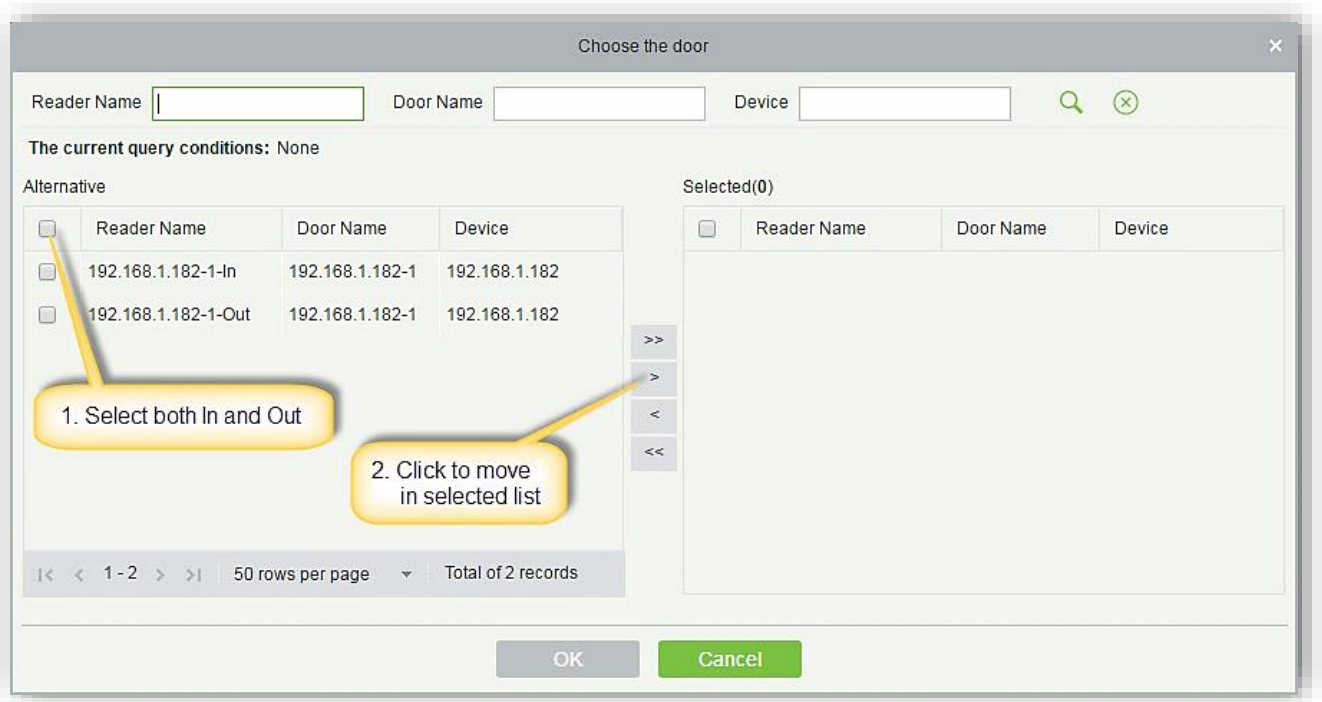
☐ Duress Fingerprint

OK Cancel

2. Issuing Card

Click **Start to read**, the system will read the card number automatically, and issue it to the user.

Note: During issuing Card, System will check whether the card number is “issued card” or not, if card has been issued before, the system will prompt “The Card Number has already been issued.”



Click **OK** to complete card issue and return.

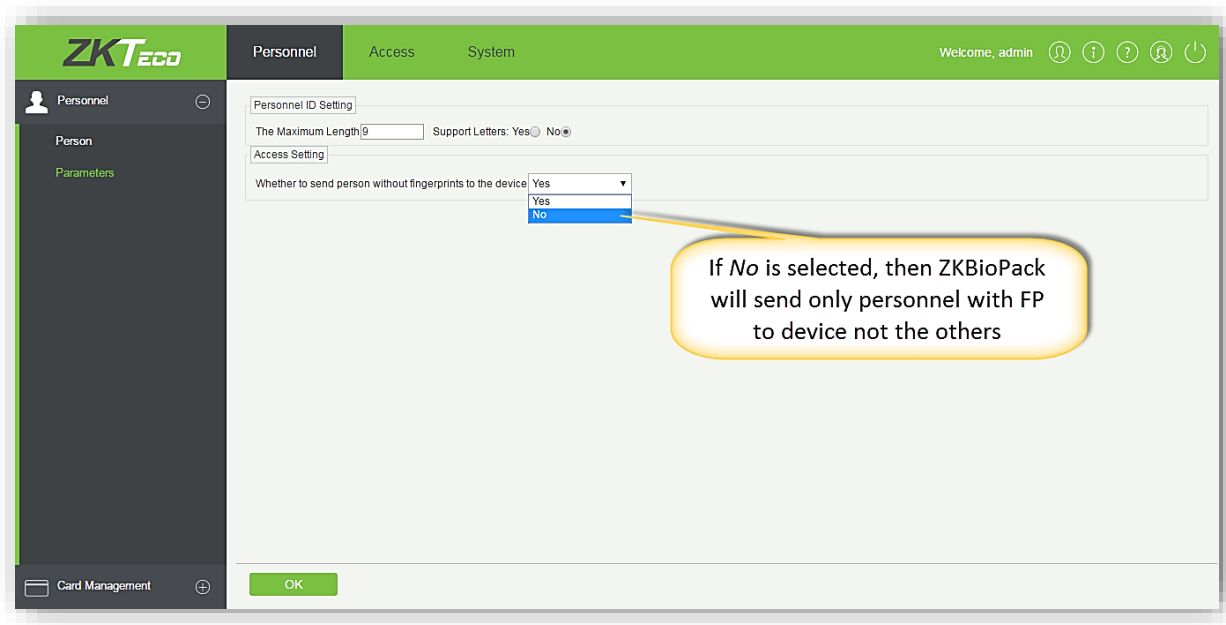
❖ Parameters

Personnel ID setting:

You can set here Personnel ID character. If you want ID as alphanumeric, then select **Yes** or else **No**.

Access Setting:

Through this option, you can set if ZKBioPack should send Personnel without FP or not to device.



The screenshot shows the ZKTeco web interface with the 'Personnel' tab selected. The 'Access Setting' dropdown menu is open, showing 'Yes' and 'No' options. A callout box explains that selecting 'No' means only personnel with fingerprints will be sent to the device.

Personnel ID Setting

The Maximum Length: Support Letters: Yes ☐ No ☒

Access Setting

Whether to send person without fingerprints to the device: Yes ☐ No ☒

If No is selected, then ZKBioPack will send only personnel with FP to device not the others

OK

14. System Menus

System settings primarily include Operation logs, Database Management, Area creation, Email Management, Data Cleaning, Authority Management and Communication settings.

Click System → Basic Management → Operation Log

The screenshot shows the ZKTeco System menu with the 'Operation Log' tab selected. The table displays the following data:

Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result
admin	2017-02-24 15:39:18	127.0.0.1	Access	Device	View Device Capacity	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 15:32:39	127.0.0.1	Access	Device	View Device Capacity	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 15:31:16	127.0.0.1	Access	Device	View Device Capacity	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 15:26:09	127.0.0.1	Access	Device	Modify Communication Password	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 15:10:38	127.0.0.1	System	User	Login	Login	✓
admin	2017-02-24 13:25:33	127.0.0.1	System	User	Login	Login	✓
admin	2017-02-24 12:12:58	127.0.0.1	Access	Device	Get Device Option	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 12:08:38	127.0.0.1	Access	Device	Export	Export	✓
admin	2017-02-24 12:08:19	127.0.0.1	System	User	Login	Login	✓
admin	2017-02-24 10:46:12	127.0.0.1	Access	Device	Get Personnel Information	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 10:43:16	127.0.0.1	Access	Device	View Device Capacity	192.168.1.182/JOIN6080086181900001	✓
admin	2017-02-24 10:33:28	127.0.0.1	Access	Device	Search Device	Search Device	✓
admin	2017-02-24 10:29:16	127.0.0.1	Access	Device	Delete	192.168.1.182/JOIN6080086181900001	✓

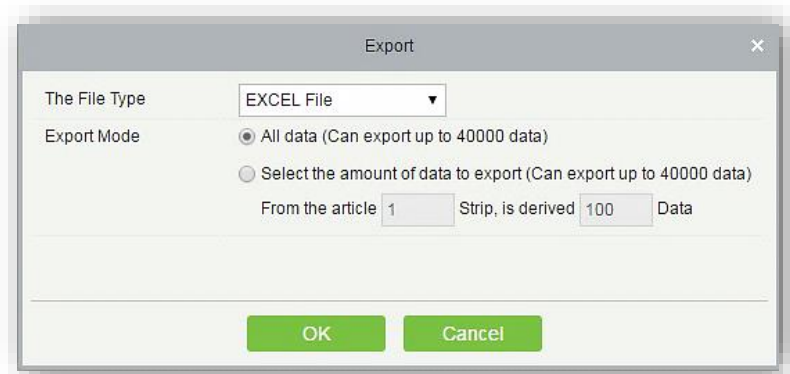
❖ Exporting the Operation Logs

All operation logs are displayed in this page. You can query specific logs by conditions.

1. Click on Export.

The screenshot shows the ZKTeco System menu with the 'Operation Log' tab selected. The table displays the same data as the previous screenshot. An arrow points to the 'Export' button in the top left corner of the table area.

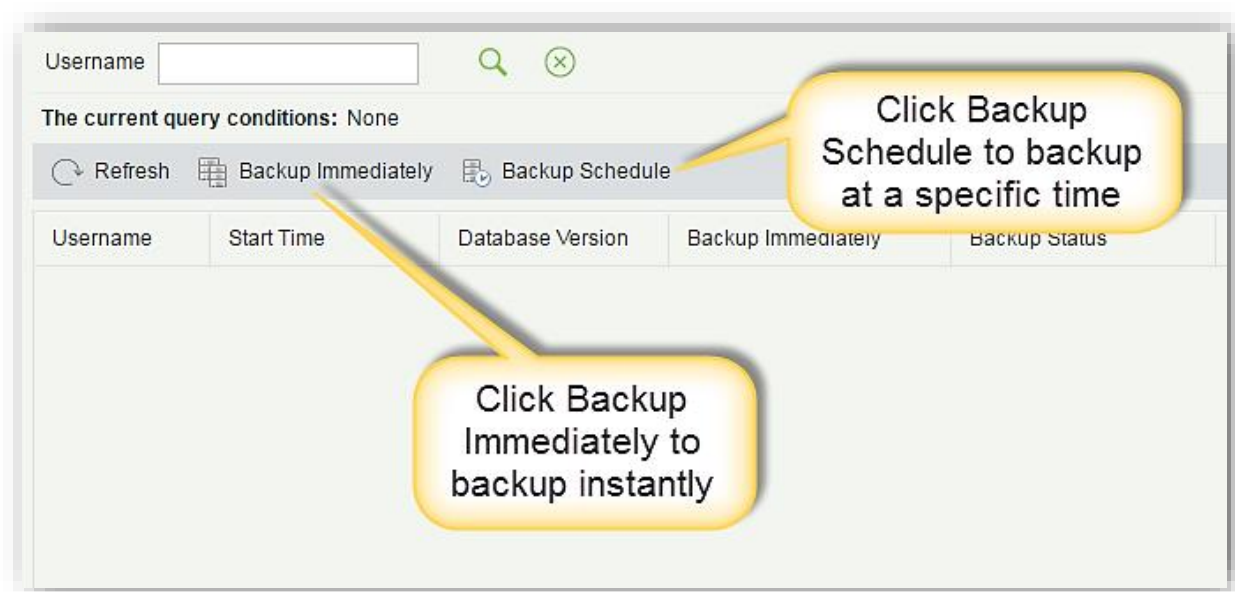
2. Select the file format and export mode to be exported. Click **OK**.
3. You can view the file in your local drive.



❖ Database Management

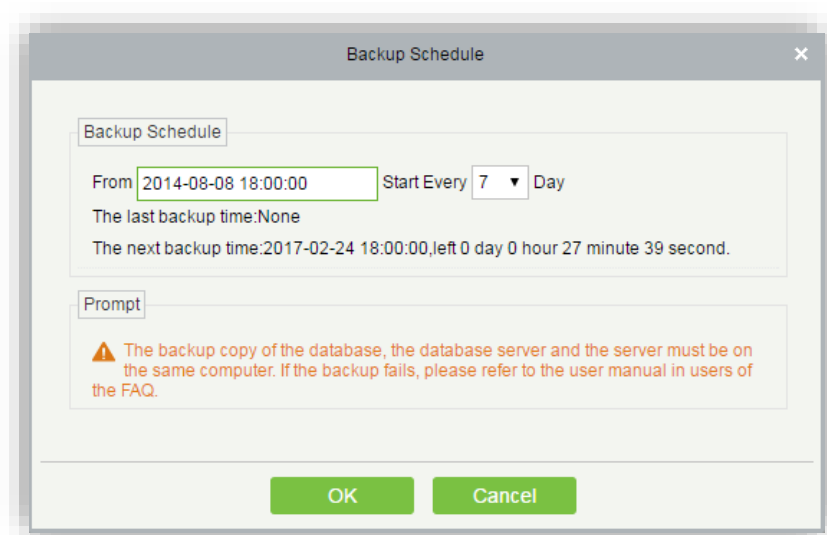
Click System → Basic Management → Database Management.

All history operation logs about database backup are displayed in this page. You can delete, backup and schedule backup database as required

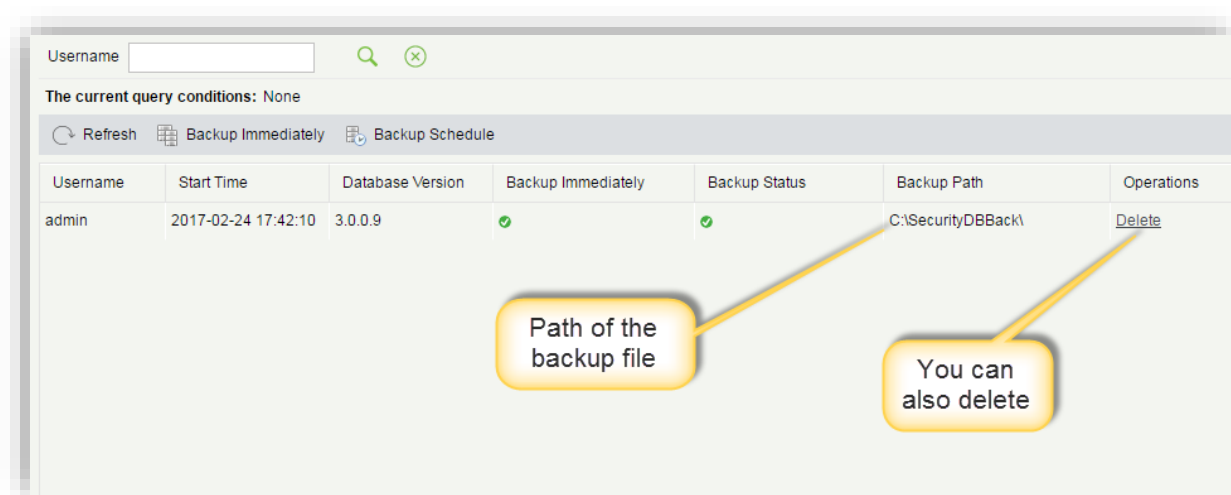


A. Backup Schedule

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



B. Backup Immediately



❖ Area Setting

Area enables the user to manage devices in a specific area. After area setting, devices can be filtered by area for ease of viewing in real-time monitoring.

The system, by default, has an area named **Area Name** and numbered **1**.

Click **System → Basic Management → Area Setting → New**

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

Remark

Save and New **OK** **Cancel**

- Area Number:** It must be unique.
- Area Name:** Any characters with a length less than 30.
- Parent Area:** Determines the area structure of system.

Click **OK** to finish adding.

❖ Email Management

You can set your email to get Real time event details.

Sender Receiver 🔍 ✕

The current query conditions: None

🔄 Refresh 🗑️ Delete 📝 Email Parameter Settings 📄 Export

<input type="checkbox"/>	Sender	Receiver	Subject	Content

Click here to set email

Email Parameter Settings

Email Sending Server* (smtp.xxx.xxx)

Port* ☒ SSL

Email Account* (xxx@xxx.xxx)

Password*

Sender Name

Prompt

⚠️ 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.

Test Connection

After entering the details, click here to test

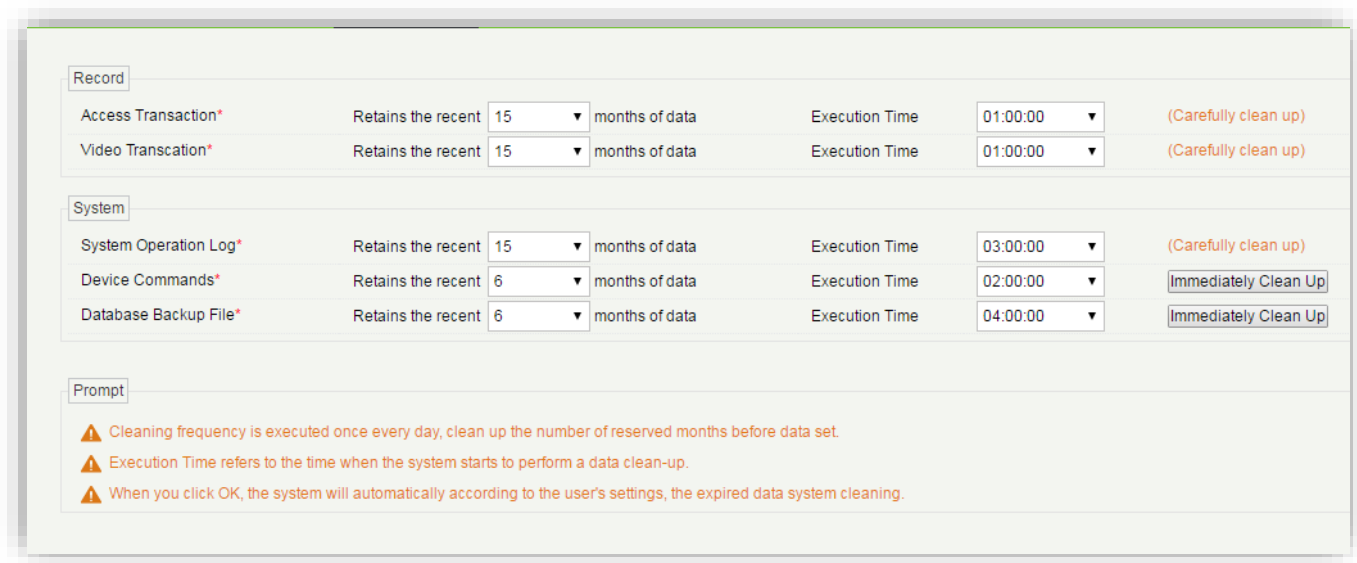
OK **Cancel**

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

❖ Data Clearing

The data clearing time settings are available to set. The data volume will increase with the use of the system. To save the storage space on the disks, you need to periodically clear expired data generated by the system.

Click **System** → **Basic Management** → **Data Cleaning**.



Record				
Access Transaction*	Retains the recent	15	months of data	Execution Time 01:00:00 (Carefully clean up)
Video Transcation*	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.

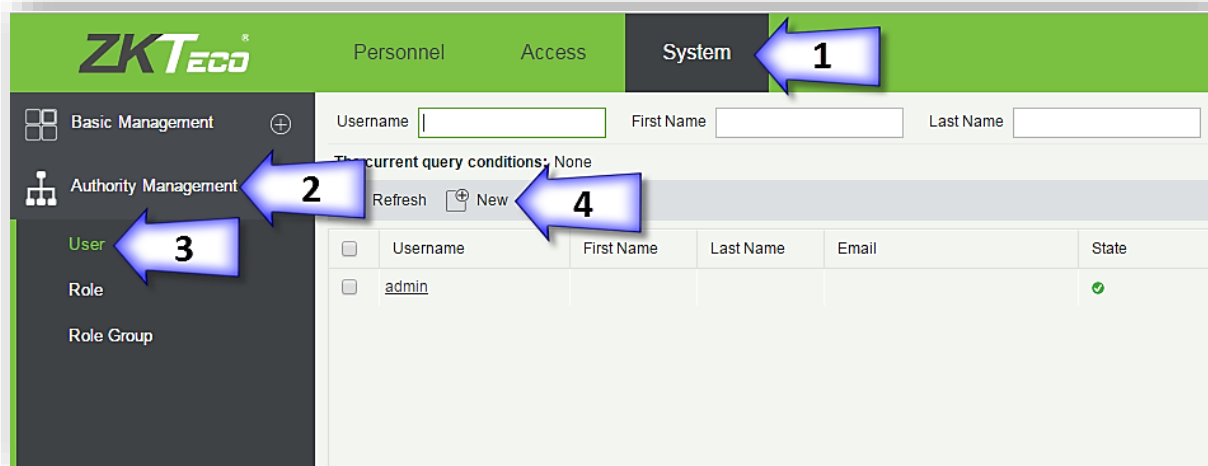
The system executes Immediately Clean Up operation after it is clicked and **OK** is clicked. Without clicking **OK**, the system will not clean data.

Note: In order to reduce the load of the system and not to affect the normal running, the cleaning time should be set as 1 am.

❖ Authority Management

Add new user other than default admin and register fingerprint for the user in the system.

Click **System** → **Authority Management** → **User** → **New**



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.

Email: Enter the email of the person.

First Name/Last Name: Enter as required.

Fingerprint: Enroll the user fingerprint or duress fingerprint. The user can login the system by pressing the enrolled fingerprint. If the user presses the duress fingerprint, it will trigger the alarm and send the signal to the system.

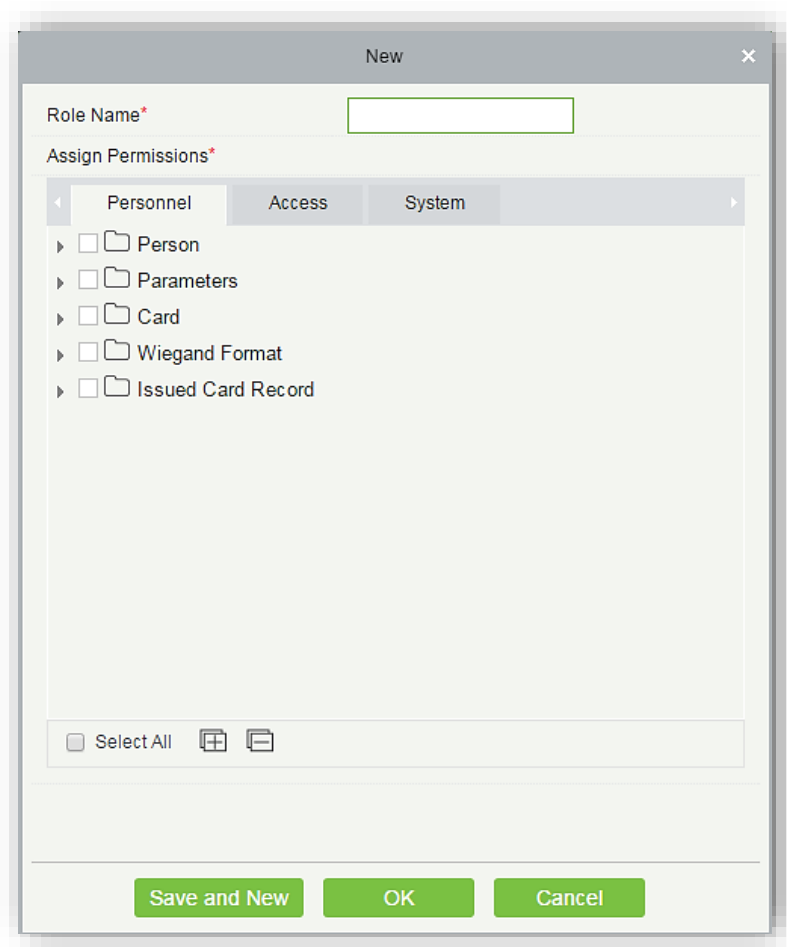
2. After editing, click **OK** to complete user adding, and the user will be shown in the list.

Click **Edit** or **Delete** as required.

❖ 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 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 authorization according to requirements.

A. Click **System Management** → **Authority Management** → **Role** → **New**.



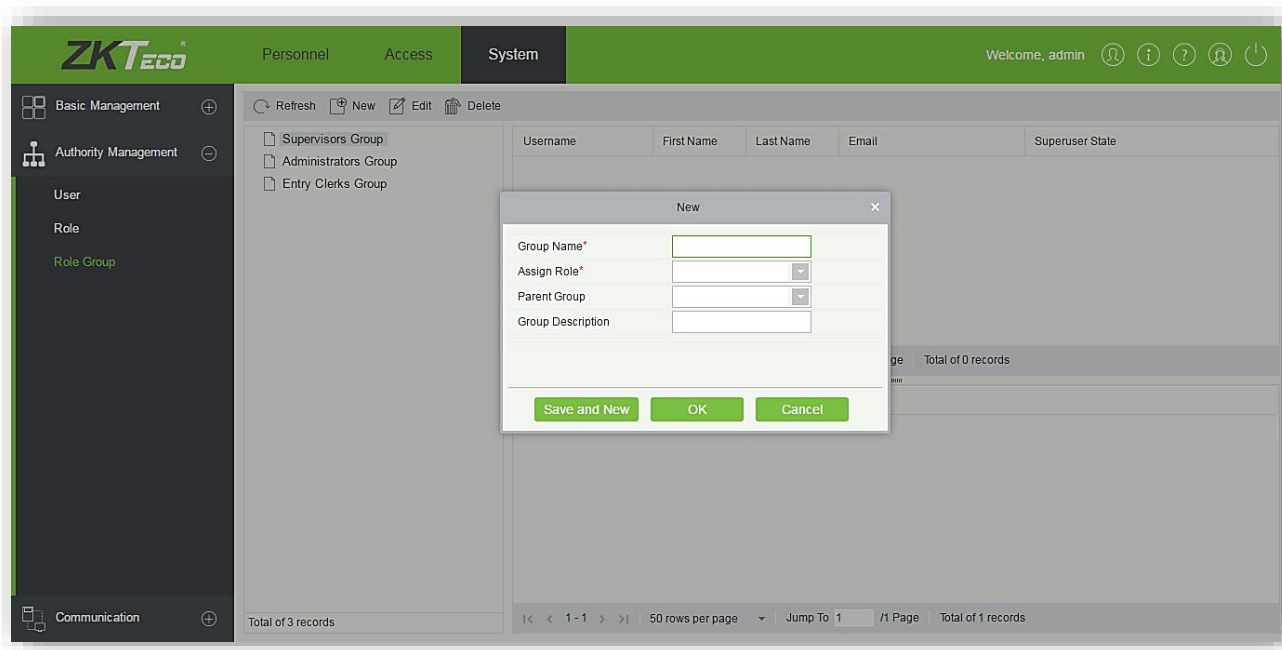
B. Set the Role name, assign permissions for the role.

C. Click **OK** to save.

❖ Role Group

You can add role groups to the system. A role group has all the authority assigned to roles within the group. An appropriate role group can be directly assigned to a newly-added user. Include all the authorization for using all the service modules of the system and the system setup module. The default super user of the system has all the authorization, and can assign rights to new users and set corresponding role groups according to the requirements.

A. Click **System Management**→ **Authority Management**→ **Role Group**→ **New**

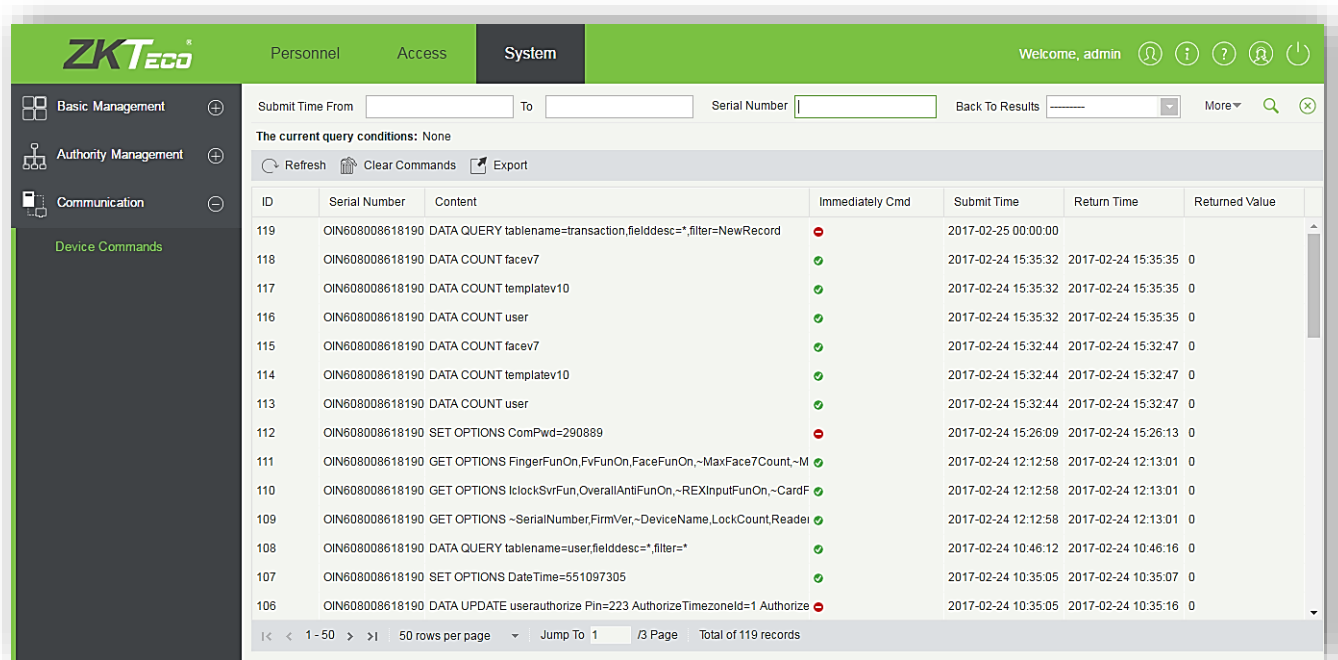


B. Set the name and parent group, assign role for the group.

C. Click **OK** to save.

❖ Communication

Click **System Management** → **Communication** → **Device Commands**, the commands lists will be displayed.



If the returned value is **more than** or equal to **0**, the command is successfully issued. If the returned value is less than 0, the command is failed to be issued.