

ZKBioSecurity3.0 Data Security and Software Usage Instructions

Version: 1.1

Date: May, 2016

Software Version: ZKBioSecurity3.0.1.0 or Above

Change Log

Version	Date	Author	Description	Remark
V1.0	2016.3.28	Darcy	Created the draft.	Adapted from the <i>Instructions on Data Security Management of ZKTeco ZKAccess System</i> prepared in 2011.
V1.1	2016.5.5	Wonder	Supplemented content.	

Contents

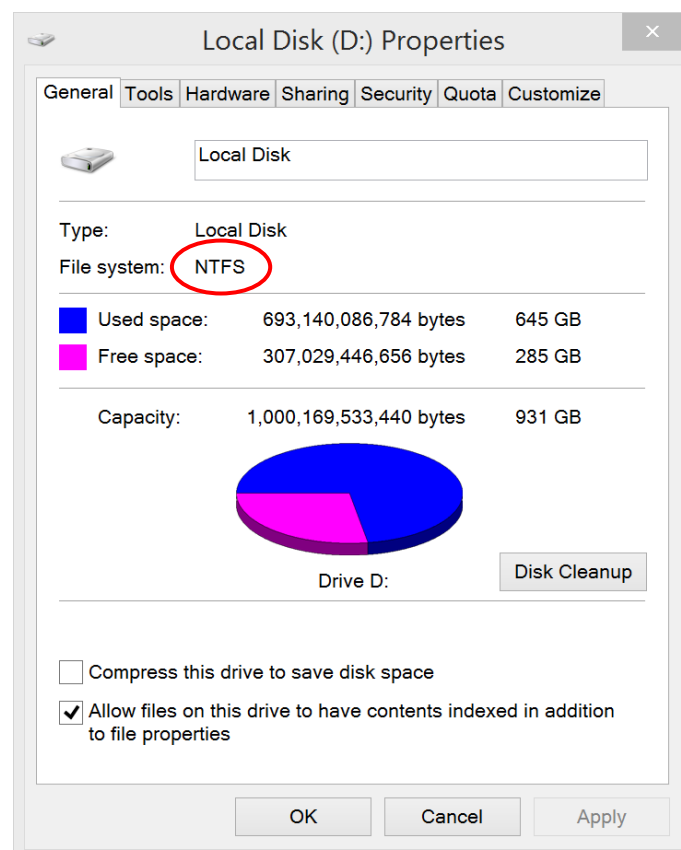
1. Security of the Server and Database.....	1
1.1 Selection of the File System Format for the Installation Directory of the Server Software.....	1
1.2 Prevention of Unexpected Power Failures on the Server.....	2
1.3 Timely Backup of the Database	2
1.4 Software Installation Directory and Database Storage Directory	3
1.5 Server Breakdown Prevention.....	4
2. Device Data Security.....	5
2.1 Adding Devices	5
2.2 Deleting Devices from the System	5
2.3 Replacing the Server without Changing Devices.....	6
2.4 Synchronizing All Data with Caution	7
2.5 Getting Transaction Records.....	7
2.6 Preventing Server Re-installation.....	7
2.7 Setting Communication Passwords for Devices.....	8
2.8 Laying Out Network Cables.....	8
2.9 Disabling Devices That Are Not Used Temporarily.....	9
2.10 Using Clear All Command with Caution.....	9
2.11 Maintaining Transaction Records Periodically.....	10
3. Software Usage Instructions	11
3.1 Security Control of Permissions Granted During Visitor Registration.....	11
3.2 Real-time Capability of Access Control Video Linkage	11

The ZKBioSecurity3.0 is a server (software)-centered security management system that implements data synchronization and exchange between the server and devices as well as between the server and clients to ensure data security of the server and network stability. It provides the best user experience and safeguards the normal and stable running of the system to the maximum extent. Carefully read the following instructions.

1. Security of the Server and Database

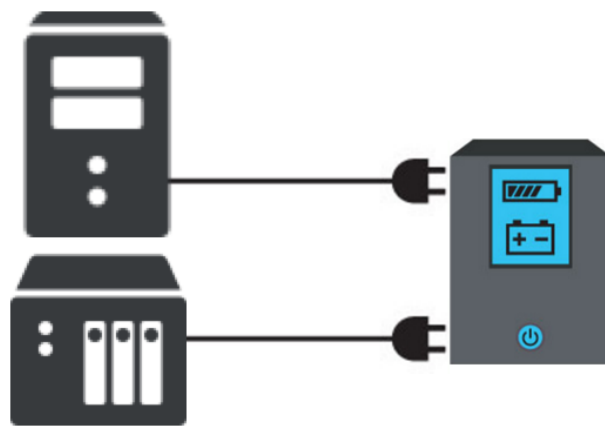
1.1 Selection of the File System Format for the Installation Directory of the Server Software

It is recommended that the New Technology File System (NTFS)-based hard disk partitions be used as the software installation directory (NTFS hard disk partitions are capable of providing better performance and higher security). A test shows that the NTFS file system is more robust than the FAT32 file system and can better protect database security in the case of an unexpected power failure.



1.2 Prevention of Unexpected Power Failures on the Server

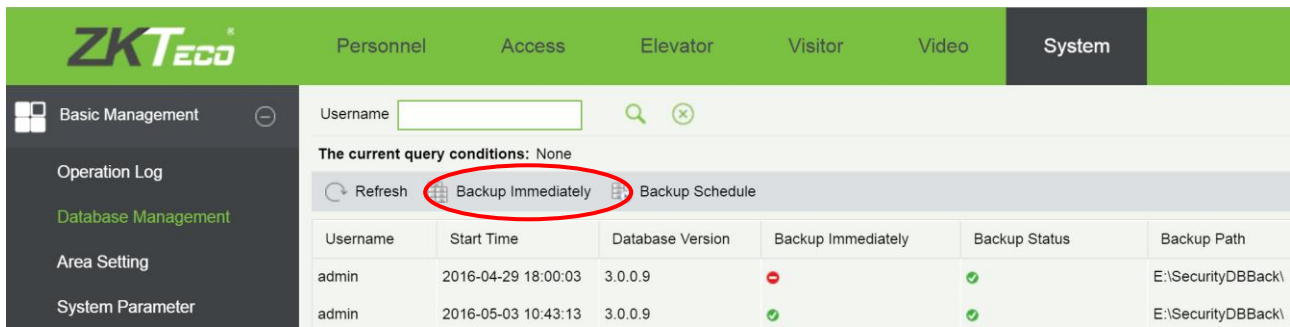
After the server is started, the ZKBioSecurity3.0 starts the data management service to process transactions and data persistently. Therefore, avoid shutting down the server unexpectedly, especially avoid unexpected power failures. Apart from using the NTFS-based hard disk as the software installation directory, it is recommended that the Uninterrupted Power Supply (UPS) be configured for the server as a standby power supply, to minimize database damage and data loss caused by unexpected power failures.



1.3 Timely Backup of the Database

After the software installation is complete, administrators usually add devices and users, and set permissions till the system can be used normally. It is recommended that administrators manually back up the database in a timely manner after adding devices and users, and setting permissions. By default, automatic backup of the ZKBioSecurity3.0 is enabled for contingencies.

In addition, it is recommended that database backup files be copied to other computers periodically. In this way, the ZKBioSecurity3.0 can be restored easily even if the server breaks down due to extreme objective factors, especially when the hardware where the software is installed is damaged; it is unnecessary to register users, add devices, and set permissions again.

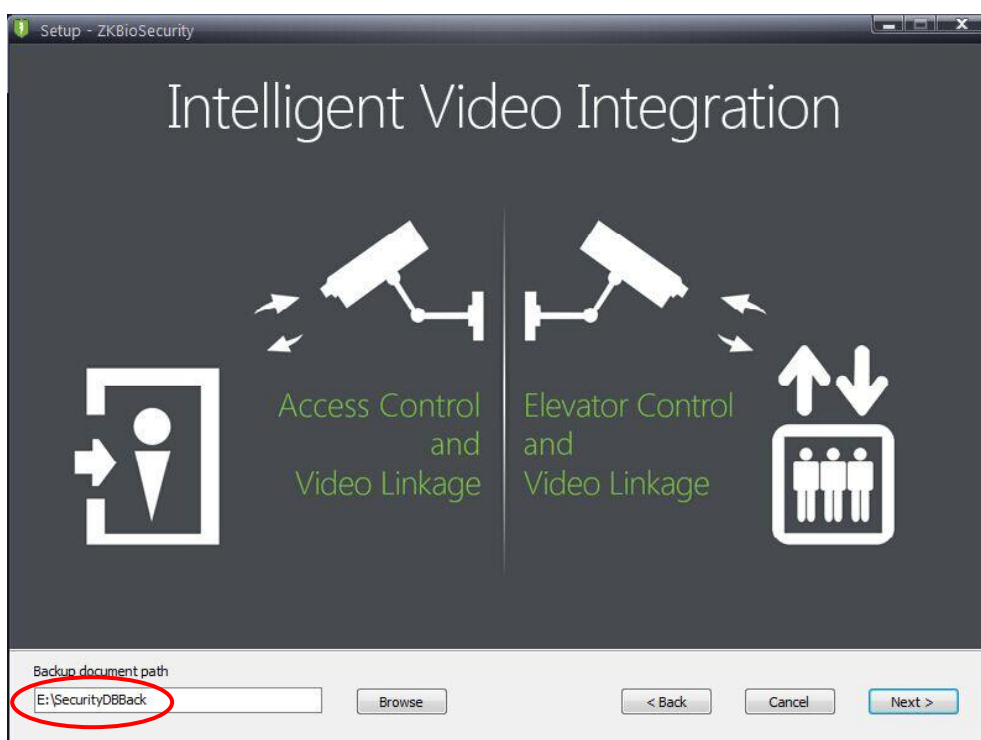


1.4 Software Installation Directory and Database Storage Directory

The security management system has special requirements for security. Therefore, the software should be installed in a non-system disk, so as to prevent data loss and even thorough breakdown of the ZKBioSecurity3.0 caused by system exceptions or system reinstallation. If the default database (PostgreSQL database) is used, the database is stored in the software installation directory. If a non-default database (SQL Server or Oracle database) is used, it is recommended that the database be stored in a non-system disk or the database server be deployed separately.

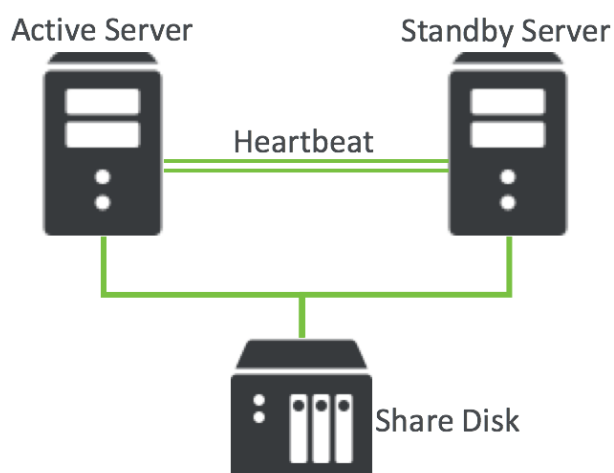


A prompt requesting user to select the backup path for the database will be displayed during software installation. It is recommended that a non-system directory be selected and database backup files be periodically copied to other computers.



1.5 Server Breakdown Prevention

In scenarios with high requirements for real-time capability such as visitor registration and global pass-back, severe consequences such as people crowding and security degrading will be incurred if the server runs abnormally or crashes. For such scenarios, it is recommended that the two-node cluster hot backup solution be deployed based on the actual budgets to ensure that when a server crashes, the other server runs immediately so as not affect users.

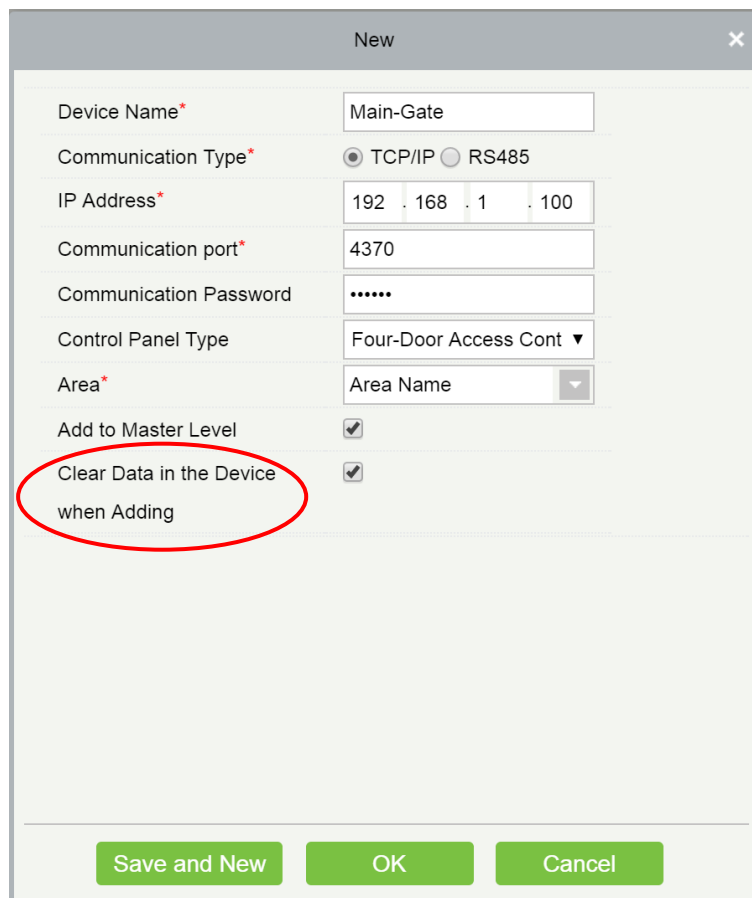


2. Device Data Security

2.1 Adding Devices

The **Clear Data in the Device When Adding** item is added to the **New** dialog box for adding a device on the ZKBioSecurity3.0. If this item is selected, data other than transaction records will be deleted from the device. Deselect this item if the system is used for demonstration or testing.

In general, only new devices or old devices to be reused need to be added to the system.



The screenshot shows a 'New' dialog box with the following fields and options:

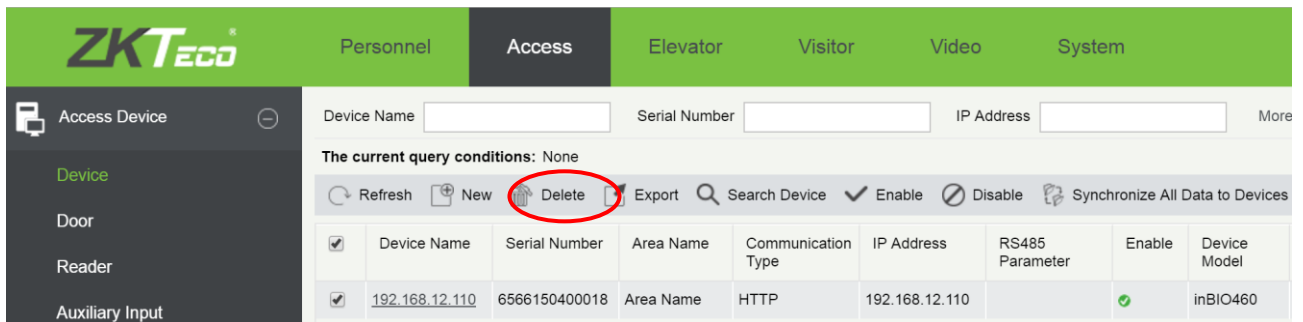
- Device Name*: Main-Gate
- Communication Type*: ☒ TCP/IP ☐ RS485
- IP Address*: 192 . 168 . 1 . 100
- Communication port*: 4370
- Communication Password:
- Control Panel Type: Four-Door Access Cont ▼
- Area*: Area Name ▼
- Add to Master Level: ☒
- Clear Data in the Device when Adding: ☒ (This checkbox is circled in red)

At the bottom of the dialog box are three buttons: Save and New, OK, and Cancel.

2.2 Deleting Devices from the System

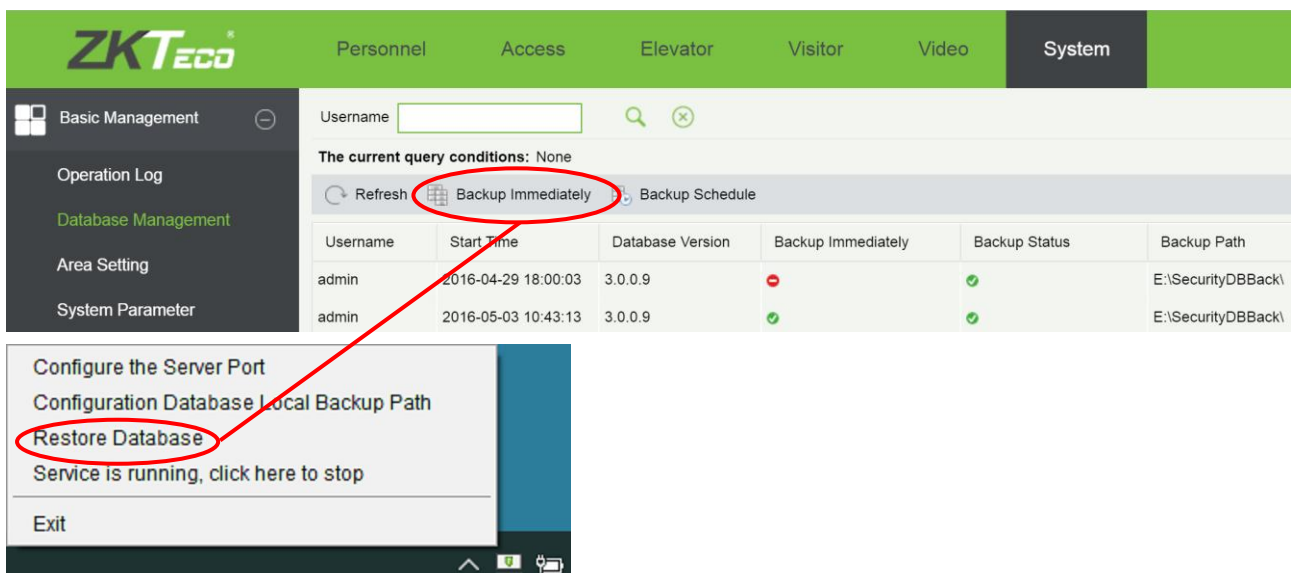
A device can be deleted from the system only when the device IP address, personnel information, permissions, and transaction records in the device are not required any more. When the server is replaced or a device is relocated but the device IP address, personnel information, and permissions do not need to be changed, the device does not need to be deleted from the system.

It is recommended that all transaction records in a device be exported to a worksheet for future search if the device needs to be deleted.



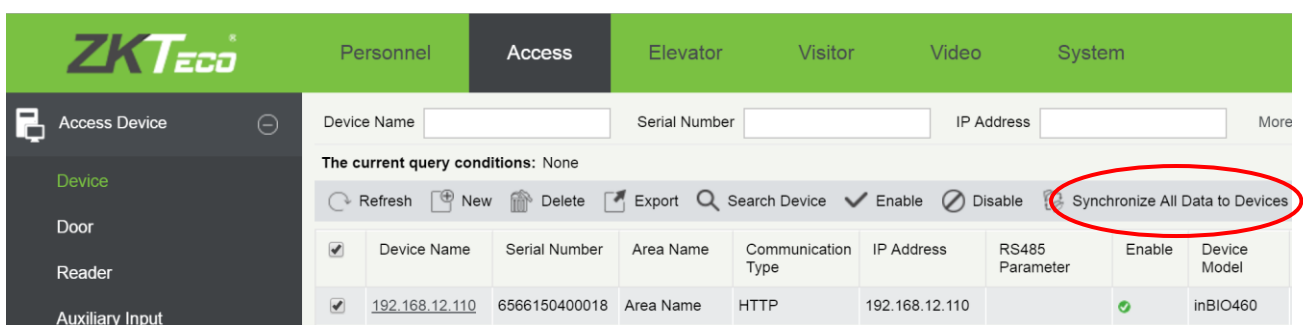
2.3 Replacing the Server without Changing Devices

If the server needs to be replaced after the security management system is put into normal use, only the database needs to be backed up. Then, the database can be restored to the new server and the system automatically connects to original devices. Devices do not need to be deleted from the original server and then added to the new server, thereby reducing the workload for administrators (administrators need to add users and set permissions again if devices are deleted from the original server).



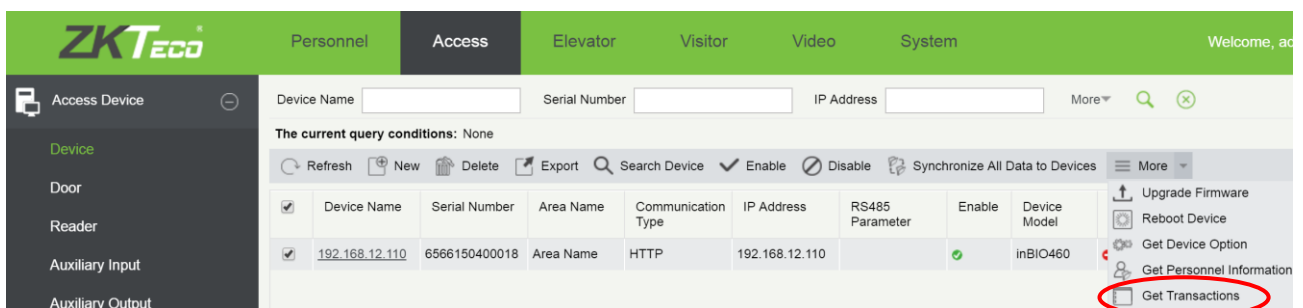
2.4 Synchronizing All Data with Caution

Synchronizing all data is synchronizing data in the server to devices. In general, this operation is required only data in devices is inconsistent with data in the server due to objective factors such as network exceptions. When this operation is performed, existing data in devices is first deleted and data in the server is synchronized to the devices. The devices may go offline during data deletion. Therefore, it is recommended that this operation be performed in idle periods so as not to affect normal use of the devices.



2.5 Getting Transaction Records

The system allows getting all transaction records or getting new transaction records. In ZKBioSecurity3.0.1.0, the options of getting all transaction records and getting new transaction records are deleted for supported green label integrated devices. The function of getting transaction records enables the software to automatically get missing records from devices.



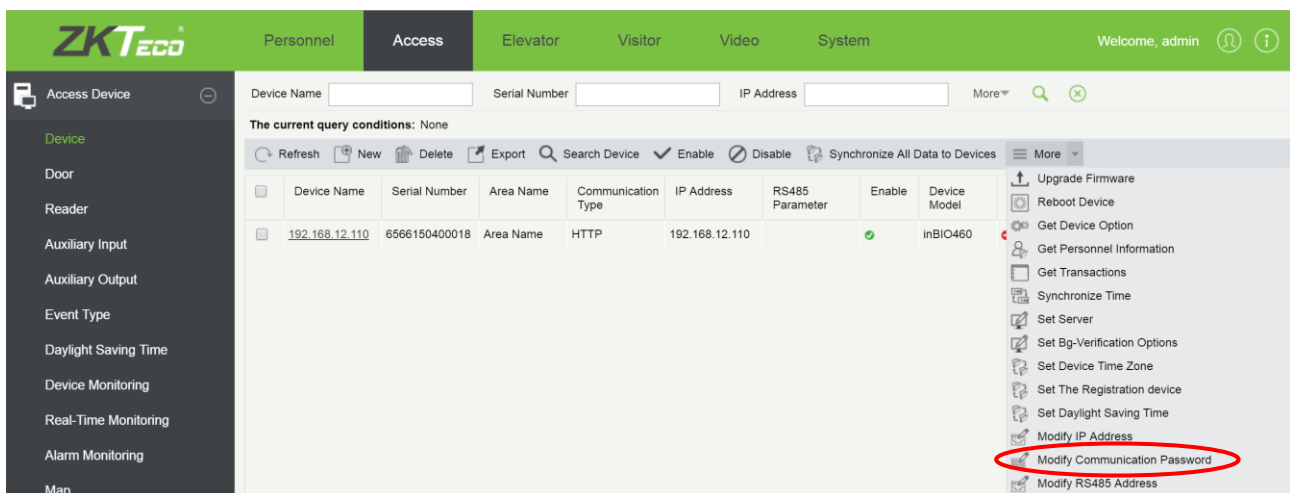
2.6 Preventing Server Re-installation

The ZKBioSecurity3.0 adopts the browser/server architecture. It is unnecessary to install multiple servers to manage the same devices and only one server is required. Users can access the server

from browser clients in other computers. Software installed during debugging must be uninstalled except the formal server, especially in the Ethernet networking environment. Otherwise, the communication between the formal server and devices will be affected.

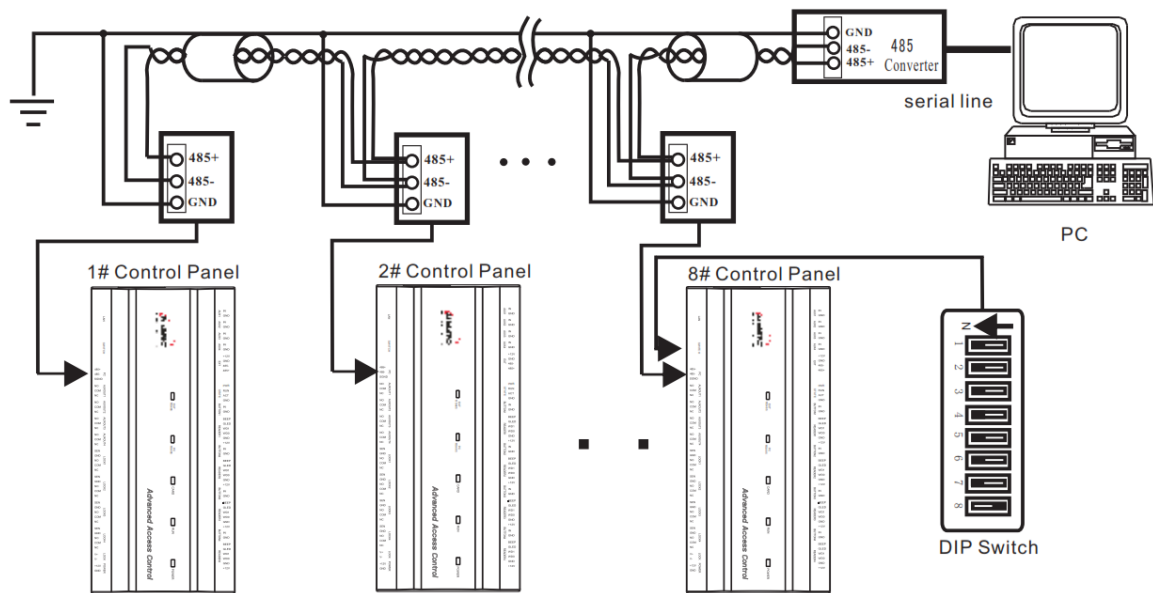
2.7 Setting Communication Passwords for Devices

All or some data will be cleared in devices when a device is added, as described in 2.1 Adding Devices". In addition to unnecessary addition and deletion of devices, it is necessary to set communication passwords for the devices. Communication passwords better safeguard communication security of devices in the current network environment.



2.8 Laying Out Network Cables

If the RS-485 networking mode is adopted, lay out cables according to relevant requirements (see the *Installation Guide*) so as not affect the communication quality and prevent unnecessary data loss. If the Ethernet networking mode is adopted, in consideration of special security requirements posed by the security management system, it is recommended that the access control system and the security system be deployed in separated networks, or the access control system be configured as a separate subnet through the Virtual Local Area Network (VLAN). In this way, external interference can be reduced and the normal and stable running of the access control system can be ensured.



2.9 Disabling Devices That Are Not Used Temporarily

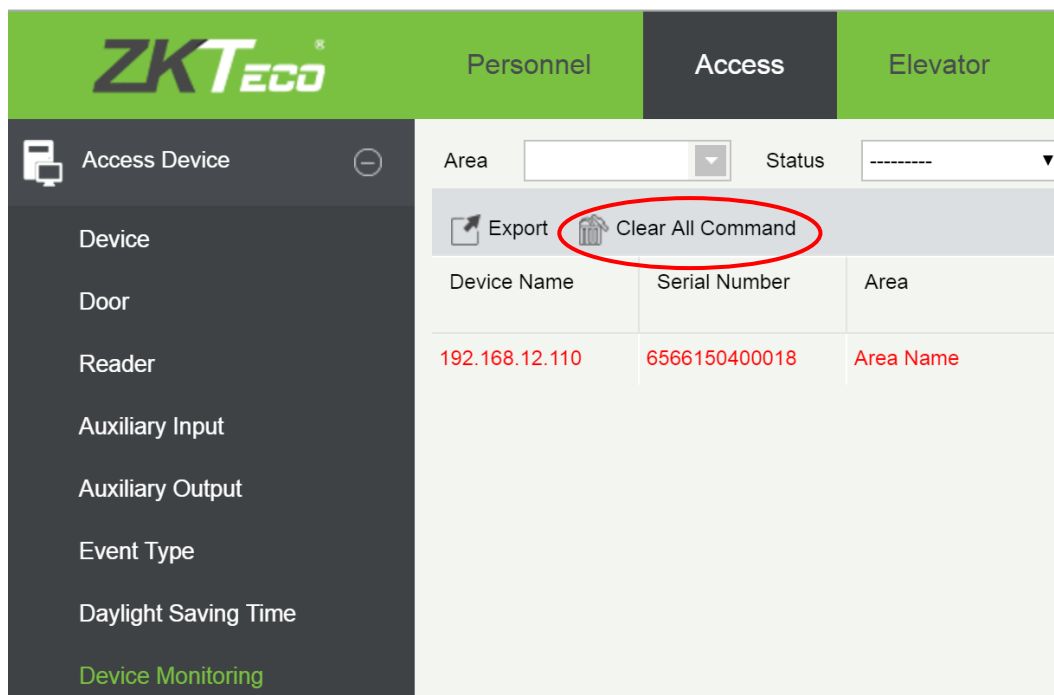
Disable devices that are not used temporarily (including devices that work in offline mode) so as not affect normal communication of other devices. If excess devices fail to connect to the server due to a network failure, check the network. If excess devices fail to communicate with the server, some devices may fail to be controlled to open or close doors (devices running in offline mode will not be affected).

The screenshot shows the ZKTeco software interface with the 'Access' tab selected. The 'Access Device' sidebar is visible on the left. The main area displays a table of devices with columns: Device Name, Serial Number, Area Name, Communication Type, IP Address, RS485 Parameter, Enable, and Device Model. The 'Disable' button in the top toolbar is circled in red.

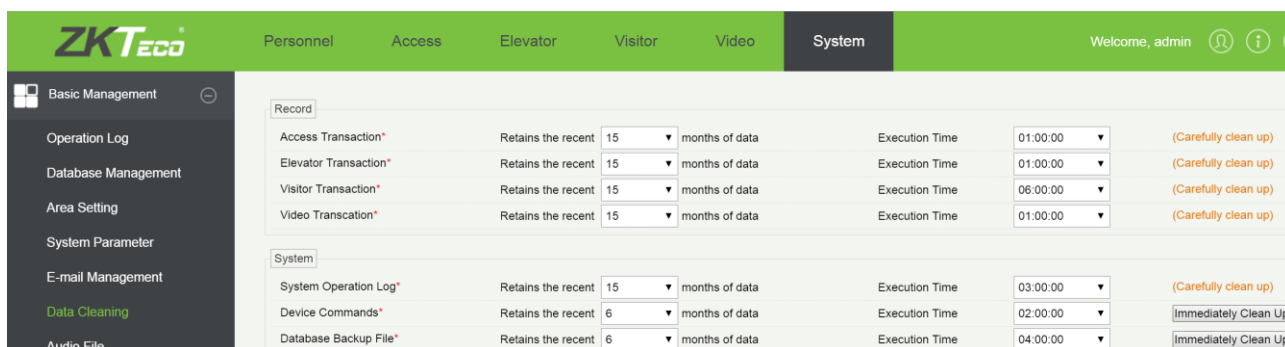
Device Name	Serial Number	Area Name	Communication Type	IP Address	RS485 Parameter	Enable	Device Model
192.168.12.110	6566150400018	Area Name	HTTP	192.168.12.110		✓	inBIO460

2.10 Using Clear All Command with Caution

Clearing all commands is mainly used during debugging, that is, during project implementation or after-sale service. This operation is unnecessary when the software functions properly. If you click **Clear All Command** by accident for a device, you must synchronize all data of the device after the operation is complete, to prevent exceptions caused by inconsistency between data in the software and data in the device.



2.11 Maintaining Transaction Records Periodically

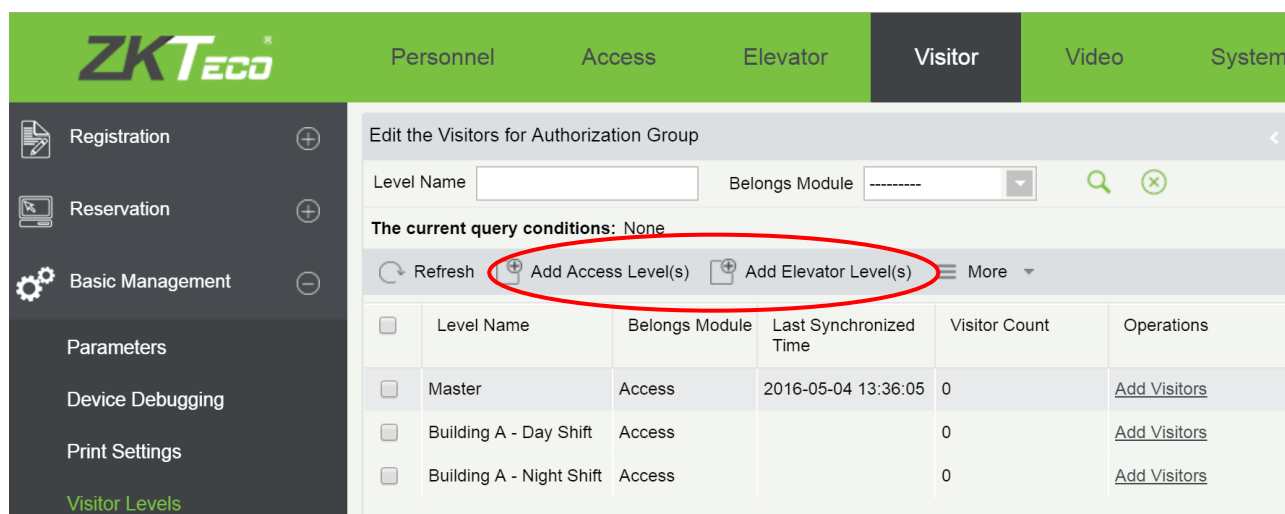


3. Software Usage Instructions

3.1 Security Control of Permissions Granted During Visitor

Registration

Registration managerial personnel (for example, security personnel or clerks) can be granted proper visitor permissions in **Visitor > Basic Management** so that they grant permissions to visitors during visitor registration. The purpose is to avoid granting unnecessary access permissions, prevent unnecessary personal risks or property loss, and improve security of an enterprise or a building. The visitor permissions include the access control level and elevator control level.



3.2 Real-time Capability of Access Control Video Linkage

As far as small videos recorded by means of video linkage are concerned, the real-time capability is out of question because of the existence of the prerecording duration. There are 2~5 seconds of delay in the linked photographing. Therefore, the application scenarios of linked photographing are limited. For example, it is not applicable to scenarios with fast passing speed. It is mostly applied in scenarios with high security requirements, for example, in a prison, a door can be opened only after a photo taken by means of linked photographing is manually compared with the photo on the credential and the result is matched.

Personnel
Access
Elevator
Visitor
Video
System

Welcome, admin

Access Device

Device
Door
Reader
Auxiliary Input
Auxiliary Output
Event Type
Daylight Saving Time
Device Monitoring
Real-Time Monitoring
Alarm Monitoring
Map

Access Control

Advanced Functions

Reports

Area

Status

Device Name

Serial Number

Door

Auxiliary Input

Auxiliary Output

Elevator

All Doors

Remote Opening

Remote Closing

Cancel Alarm

More

192.168.1.2 33-1

192.168.1.2 33-2

192.168.1.2 33-3

192.168.1.2 33-4

Current Total 4

Online 4

Disable 0

Offline 0

Unknown 0

Door Name

Real-Time Events

Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2016-05-05 10:31:23	Area Name	192.168.1.233(6688143600002)	192.168.1.233-1-In	Linkage Event Triggered(Li	9505930	52553	192.168.1.233-1-In	Only Card
2016-05-05 10:31:23	Area Name	192.168.1.233(6688143600002)	192.168.1.233-1	Normal Verify Open	9505930	52553	192.168.1.233-1-In	Only Card

Video Linkage

192.168.1.91-1

Normal Verify

Total Received 2

Normal 2

Exception 0

Alarm 0

Clear Rows Data

New Message 1

Event Reminder Sounds

Show Photos

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

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com

