ZKAccess Data Security Management Guide

Version: V1.2
Software Version: ZKAccess 4.0/5.0
Date: March, 2011

ZKAccess Security System is a server based (software) access control management system. After the access control settings being set, the system will automatically synchronize the settings to the device under the steady network and normal device communication. By this time, the data is synchronized between the device and the server. Therefore, only by taking measure to protect the data security of the system, can we ensure the normal and stable operation of the system mostly.

✧ Database Security

1. Select the hard disk partition format for server software installation directory.

We recommend using NTFS hard disk partition as the software installation directory (Which has the better performance and higher security). According to our test, NTFS system is stronger than FAT32 in accidental power failure situation. For example, if the MySQL database is under FAT32 system, the datasheet is apt to be damaged in power failure situation, which will result in data loss. While the NTFS file system is better to protect the security of the database.

2. Prevent accidental power failure.

After the server starting, the access control management system will start the data management server, and process the event and data continually. The user should try to avoid the unexpected server shut down, especially accidental power failure and

etc. To minimize the database damage and data loss due to these kinds of situation, besides using NTFS hard disk partition, we recommend connecting UPS to the server.

3. Backup the database regularly.

Generally, after software installation, the user will add new device, personnel, set access control levels and etc. to make sure the system being used normally. We recommend backing up the database manually after all of these settings. In addition, we suggest copying the backup file (SQL file) to another computer. So that, even in the extremely serious situation which causes the entire server (especially the software installation directory) damage, the user can also restore the server and keep the device in normal working condition, and don't need to configure the device and other parameters.

4. Software installation directory and database store directory.

Due to the special security requirements of the access control system, we recommend user to install the software under the non-system hard disk to avoid the software unable to be recovered or data loss cause by the system reinstallation. If you install the default database, the database file will be saved under the software installation directory. Otherwise, we recommend setting the database saving directory under the non-system hard disk.

5. Select the database backup directory.

Similar to the situation 4, we recommend that the database backup directory should be set under the non-system hard disk. And copy the backup file to another computer periodically.

✧ **Device Data Security**

1. Add new device.

In device adding operation, the server (version before ZKAccess4.0.18, excluded) will clear all data in the device. Include user information (card, fingerprint, password, and etc.), access control levels, and time zones, holidays and event entries. The server of Access4.0.18 and above version has added an option [**Clear Data in the Device when Adding**] , if ticked , it will clear the data except the event entries in the device. If you add the device just for demonstration or testing of the system, don't tick it.

Generally, only if the user use a new device or reuse an old device, need to add the device to the system.

2. When the users need to delete the device from the system?

Only if the user don't need to use the device any more, namely, the device IP, user information, access control levels, event entries of the device are all unusable, that the device needs to be deleted from the system. If you change the server, or move the device without modifying the IP address, user information, access control levels, you don't need to delete the device from the system.

Before device deletion, it is recommended to get all events entries, and export the report for user searching purpose.

3. Can we change the server without device moving?

Under normal using situation of the access control system, if the user needs to change a server, just backup the database and restore this backup file to the new server. The system will connect all of the devices automatically. In this situation, please don't delete the device and add them to the new server again, which will increase the workload of the administrator (need to add all personnel and set the levels).

4. Synchronize all data with caution.

Synchronize all data is mainly used to synchronize the data between the server and

the device. Generally, it is only used in the situation of data asynchronous between the server and device which cause by some objective factors (such as network abnormal or other situation). This operation will delete all of the data in the device, and synchronize the server data to the device. The deletion process will mostly affect the device offline operation. So it is recommended to select a better opportunity in using this operation, to minimize the impact to the device.

5. Get the event entries.

There are two type of getting event entries, get all entries and get new entries. The server version before ZKAccess4.0.18, there is only get entries operation. It is get all event entries by default. The options of get all entries and get new entries being added in ZKAccess4.0.18 and above version.

In addition, the system downloads the new entries at 00:00 everyday by default. The device can store up to 100000 entries. When the record reach to this value, the device will delete the oldest 10000 entries, ensure no latest record being lost. User need not to delete the record manually.

Although the device can store 100000 entries, please ensure the server work normally to avoid the data loss, or get event manually if necessary.

6. Don’t install the server repeatedly.

ZKAccess is a B/S structure access control management system. For the same type device, the user needs not to install multi server to manage devices, one is enough. But the user can access the server by from other computers. You need to delete the installed software in debugging process except the formal server, especially in the Ethernet network environment. Otherwise, they will effect the communication of the formal server and the device.

7. The necessary of setting communication password.

As introduced in situation 1, in new device adding process, it will clear all or some

of the data. Except avoid to add or delete device, the communication setting is necessary too. It can ensure the device communication security better.

8. The importance of network wiring.

If you use RS485 network: Please always follow the requirement of wiring in Installation Guide, to avoid the impact of the communication quality and the accordingly loss.
If you use Ethernet network: For the especially requirements of the security system, it is recommended to build the network separately, or put the system network into independent VLAN, in order to reduce the interference outside and make sure the system running normally.

9. Disable unused device temporarily.

As mentioned above, if a device is temporarily unused (include offline device), please disable it to ensure the communication quality. If there is too many devices disconnecting, please check the network connection first, otherwise, it will result in failures when the devices were operated remotely (no effect to the offline operation).