User Manual

ProRF

Version: 1.0

Date: April 2021

Green Label

Important Statement

Thank you for choosing our product. Before using this product, please read this user manual carefully to avoid risks of danger to the users of this product or those nearby and damaging the device. Follow these instructions to ensure that your product functions properly and completes verifications in a timely manner.

Unless authorized by our company, no group or individual shall take excerpts of or copy all or part of these instructions nor transmit the contents of these instructions by any means.

The products described in this manual may include software that is copyrighted by our company and its possible licensors. No one may copy, publish, edit, take excerpts of, decompile, decode, reverse-engineer, rent, transfer, sublicense, or otherwise infringe upon the software's copyright unless authorized by the copyright holder(s). This is subject to relevant laws prohibiting such restrictions.

As this product is regularly updated, we cannot guarantee exact consistency between the actual product and the written information in this manual. Our company claims no responsibility for any disputes that arise due to differences between the actual technical parameters and the descriptions in this document. The manual is subject to change without prior notice.

Contents

1. Must Know

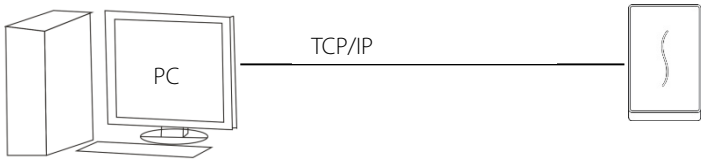
1.1 Product Profile

ProRF released by our company is the World's first access controller and reader based on TCP/IP, professional access control machine with ID card but no screen and no press-key. These access control product series added with ID card provide a more product choices for system access control solutions. It can be used as a separate control lock, also can be used as an access controller connecting ID cards, to realize master-slave machine or anti-passback function. The device can connect with Ethernet over TCP/IP. It can be embedded with Webserver to visit query records and so on via Internet.

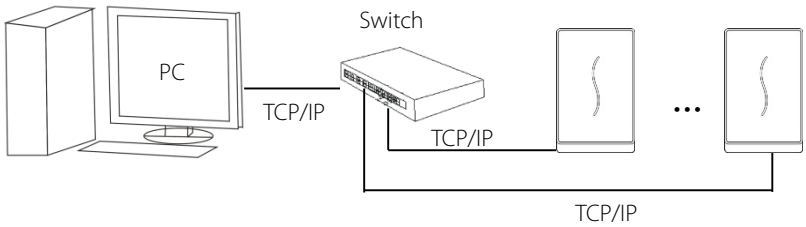
1.2 Communication Connections

The background PC software can communicate with the device, upload and download data and perform remote management of the terminal over TCP/IP. The device can connect with Ethernet in the following two ways:

1. The device directly connects to the computer.



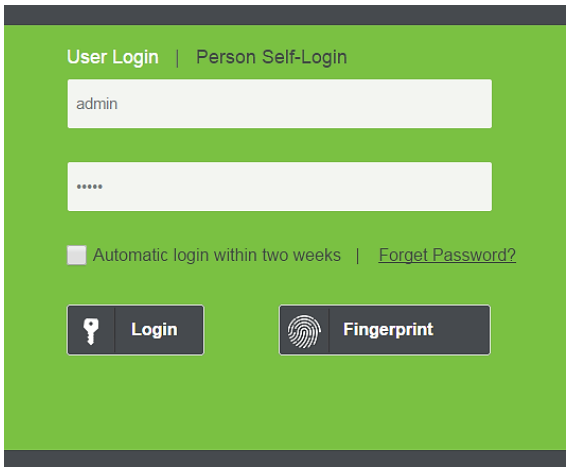
2. The device connects to the computer over an Ethernet through a switch.



The default IP address is 192.168.1.201. IP addresses of the server (PC) and the device must be in the same network segment.

2. Access Control Software

Suppose the device has connected with PC well and the access control software has been installed already.

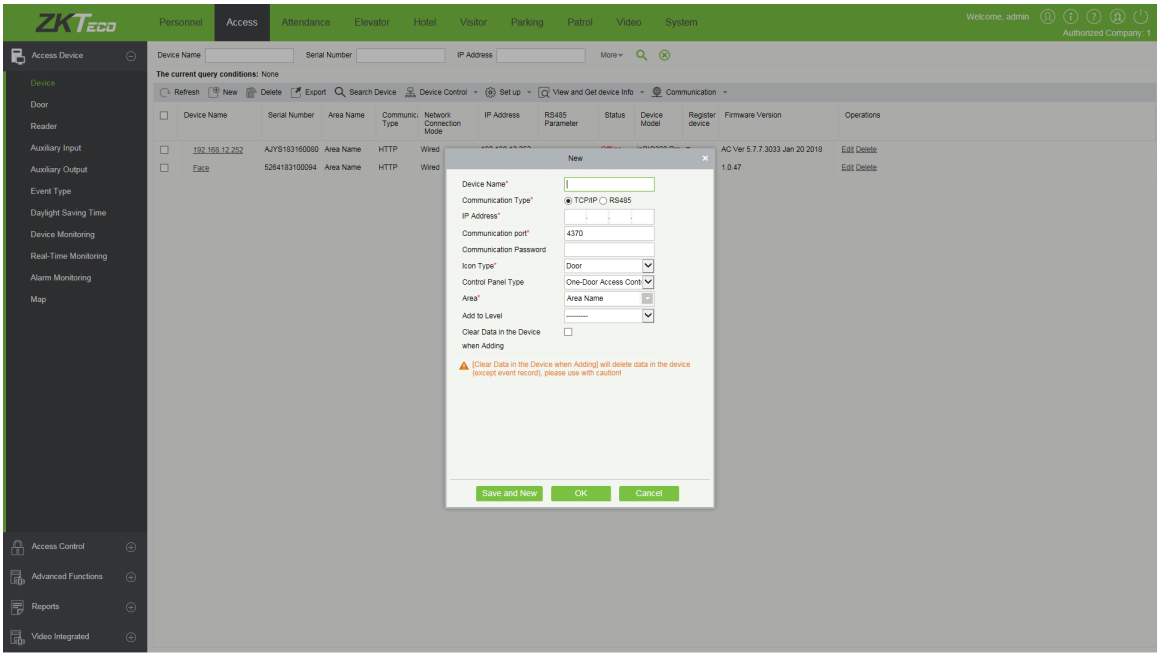


On the desktop, double-click the ZKBiosecurity icon to enter the system. The user name of the super user is [admin], and the password is [admin], then click [login]. After the first login to the system, please reset the password in [Personnel Information].

2.1 Adding a device

✧ Add Device by manually

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



Device Name: Any character, up to a combination of 50 characters.

Communication type: TCP/IP.

IP Address: Please enter the IP Address of the device, the default IP address is 192.168.1.201.

Communication port: The default value is 4370.

Communication Password: Any character, up to a combination of 8 characters (No blank). You need to input this field only when you add a new device with the communication password. It cannot be modified when you edit the device information except in [Modify communication password] operation.

✍**Note**:

You do not need to input this field if the device has no communication password, such as when it is a new factory device or just after the initialization.

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

Control Panel Type: Standalone Device.

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area 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 being ticked, after adding device, the system will clear all data in the device, except the event logs. If you add the device just for demonstration or testing of the system, there is no need to tick it.

2) After editing, click [OK], and the system will try connecting the current device:

✍**Note**:

When you add a new device to the system, the system will clear all user information, time zones, holidays, and access control levels settings (including access control group, anti-passback, interlock settings, linkage settings, etc.) from the device, except the events record in the device. Unless the information in the device is unusable, we recommend you not to delete the device in used, to avoid the loss of information.

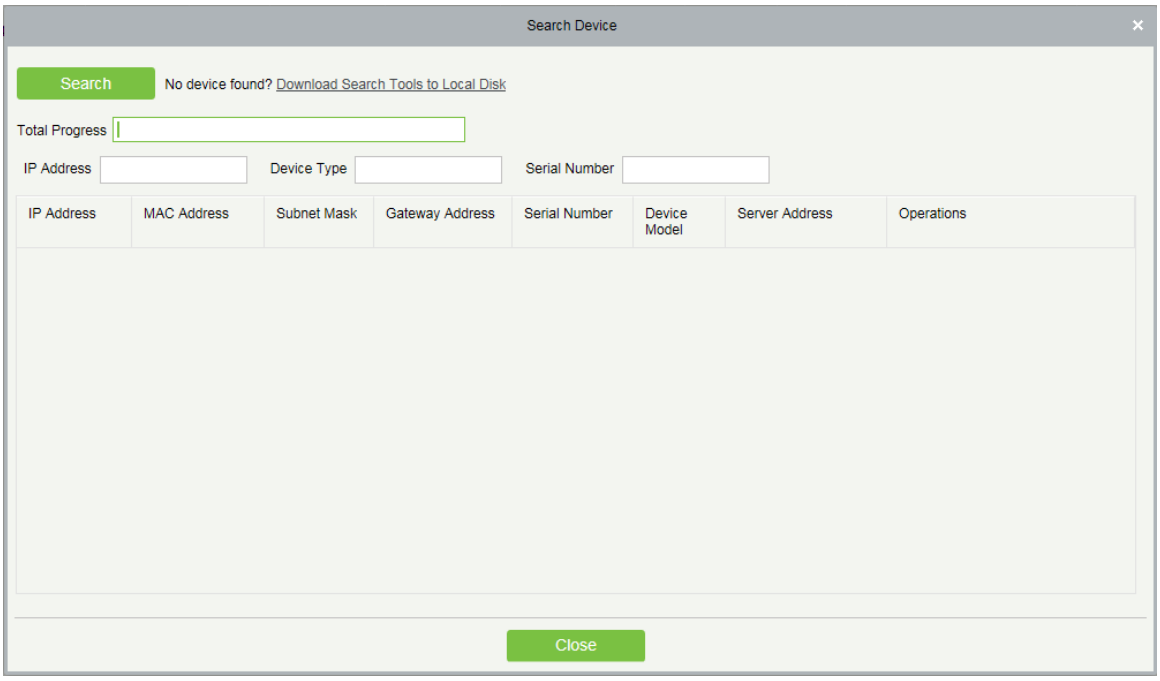
---

3) One PC can connect with multiple devices, and the access control software in PC can manage multiple devices at the same time. If you want to add devices, please click [New]. If you want to delete devices, select devices and click [Delete]. For details, please refer to "ZKBiosecurity User Manual".

✧ Add Device by Searching Access Controllers

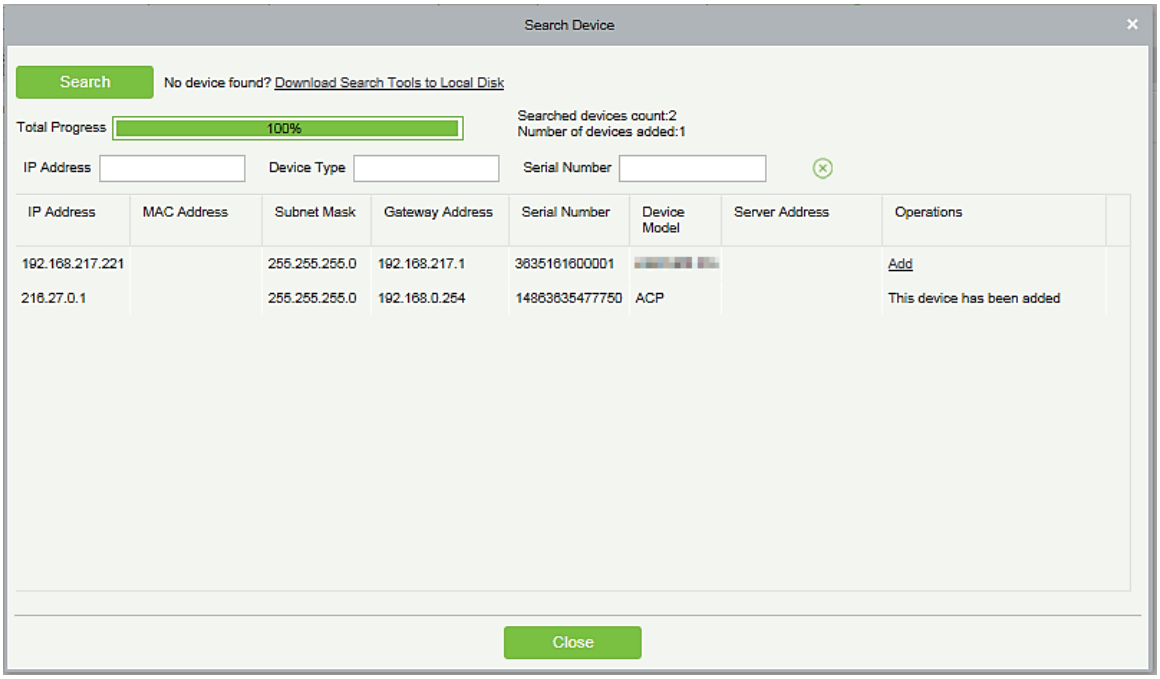
Search the device in the Ethernet.

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



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

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



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

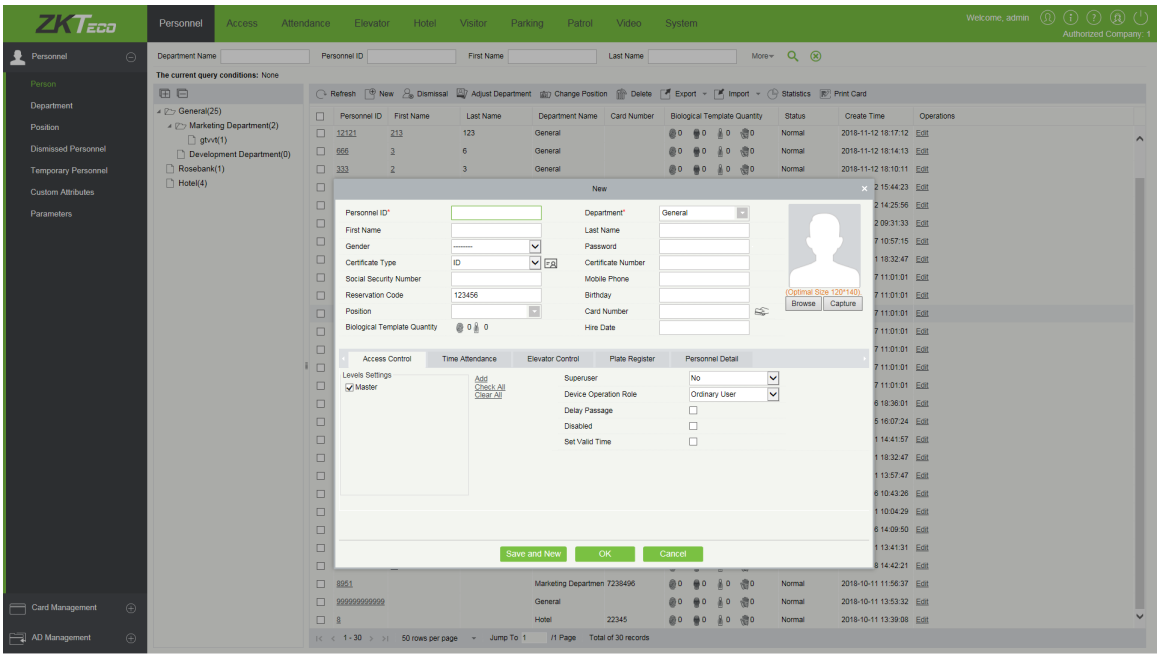
2.1.1 Device Settings

Includes that Modify IP Address, Close Auxiliary Output, Disable, Enable, Modify Communication Password, Synchronize Time, Upgrade Firmware, Get Logs From SD Card, Import Data From USB disk and so on.

For more details, please refer to "ZKBiosecurity User Manual".

2.2 Adding a user and a card

1) Click [Personnel] > [Person] > [New]:



The fields are as follows:

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

Notes:

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

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

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

Card number: Assign a card number to the person for access control use. The max length is 10, and it should not

be repeated. This can be done manually or by using card issuer.

2.3 Access Control Settings

The access control system can set the opening levels of registered users, namely, allowing some personnel to open some doors by verification during a time period. Access Control System Management primarily includes Access Control Time Zones, Access Control Holiday, Door Settings, Access Levels, Personnel Access Levels, Real-Time Monitoring, and Reports, etc.

Access control system parameters

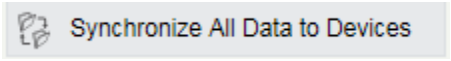
- 255 time zones.
- Unlimited access levels.
- Three holiday types and 96 holidays total.
- Anti-passback function.
- Wiegand format.
- Interlock function.
- Linkage function.
- First-Card Normal Open function.
- Multi-Card Opening function.
- Remote door opening and closing.
- Real-time monitoring.

For more details, please refer to "ZKBiosecurity User Manual".

2.4 Upload and download

For a PC corresponding to multiple devices, the user information in PC can be uploaded to multiple devices, and user information in multiple devices can be downloaded to this PC also.

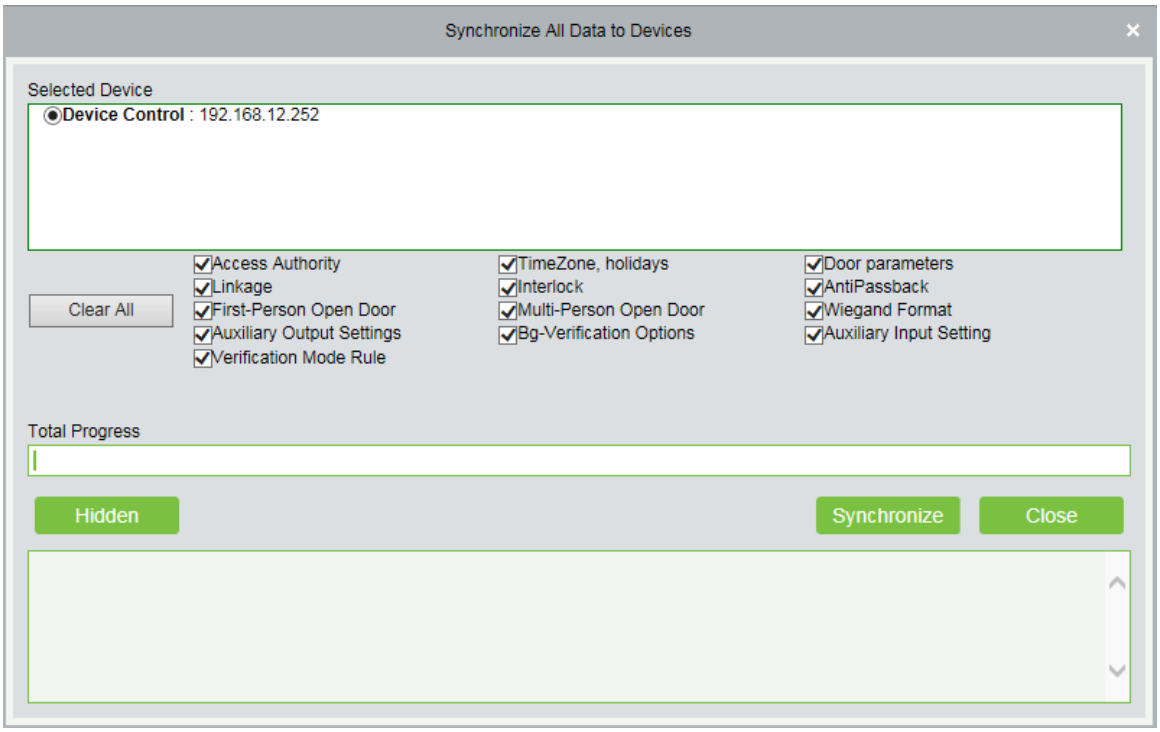
For the first time to use, after user information and ID cards are registered, user information can be uploaded from

PC to device through 

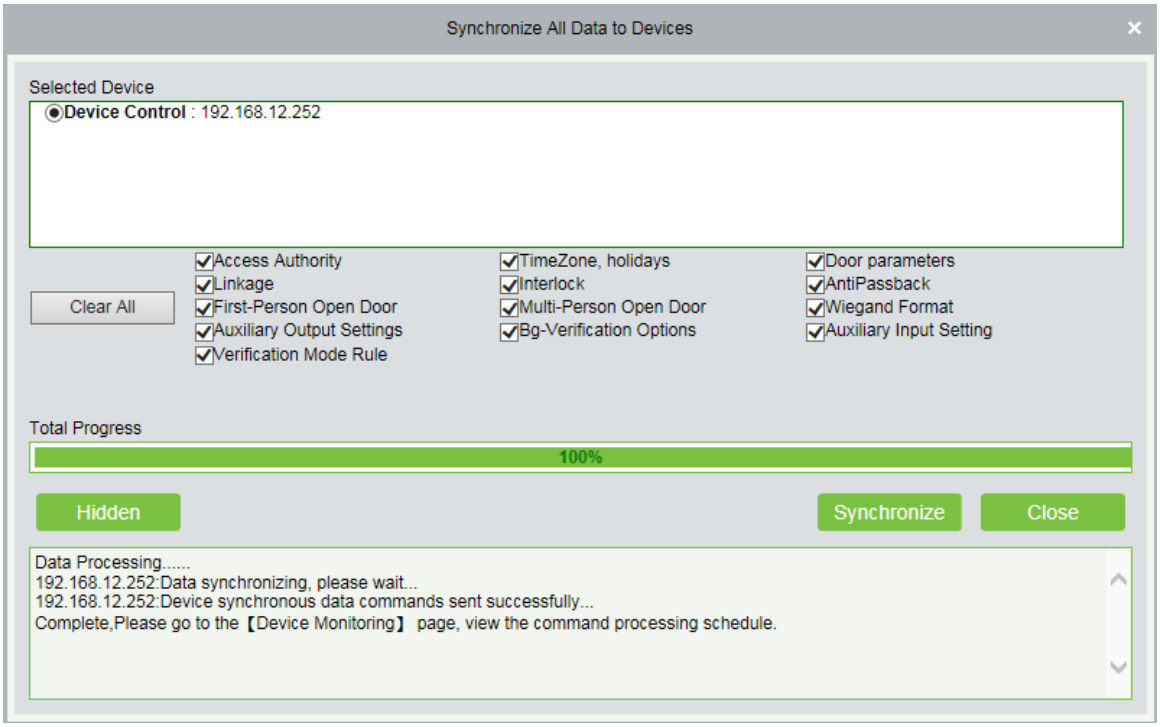
. After the registered ID cards are punched on device successfully, attendance records will be generated in device. These attendance records can be downloaded from device to PC through [Reports].

2.4.1 Sync All Data to Device

1) Click [Device Control] > [Synchronize All Data To Devices] in the Device page.



2) Click [Synchronize], the following interface will be shown.



✍**Note:**

The operation of Synchronize All Data is mainly to delete all data in the device first (except event record). Download all settings again, please keep the net connection stable and avoid power down situations, etc. If the device is working normally, please use this function with caution. Execute it in rare user situations to avoid impacting on normal use of the device.

2.4.2 Get Event Entries

Click [Device Control] > [View and Get device Info] > [Get Transactions] to get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.

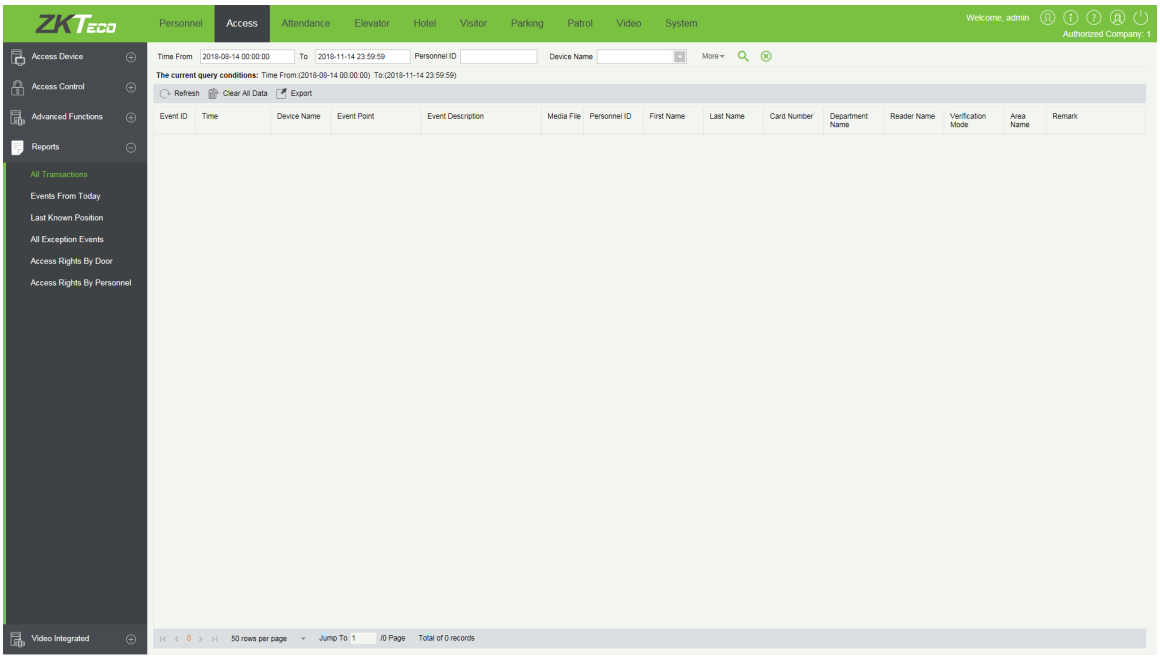
Get New Transactions: The system only gets new transactions since the last collected and recorded transaction. Repeated transactions will not be rewritten.

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.

You can view the statistics of relevant device data in [Report], including card verification information, door operation information, and normal punching information, etc.

By default, the system displays latest three months transactions. Click [Reports] > [All Transactions] to view all transactions:



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.

✍**Note**:

The device can restore up to 1 million of event entries. When the entries exceed this number, the device will automatically delete the oldest restored entries.

2.4.3 Get Personnel Data From Device

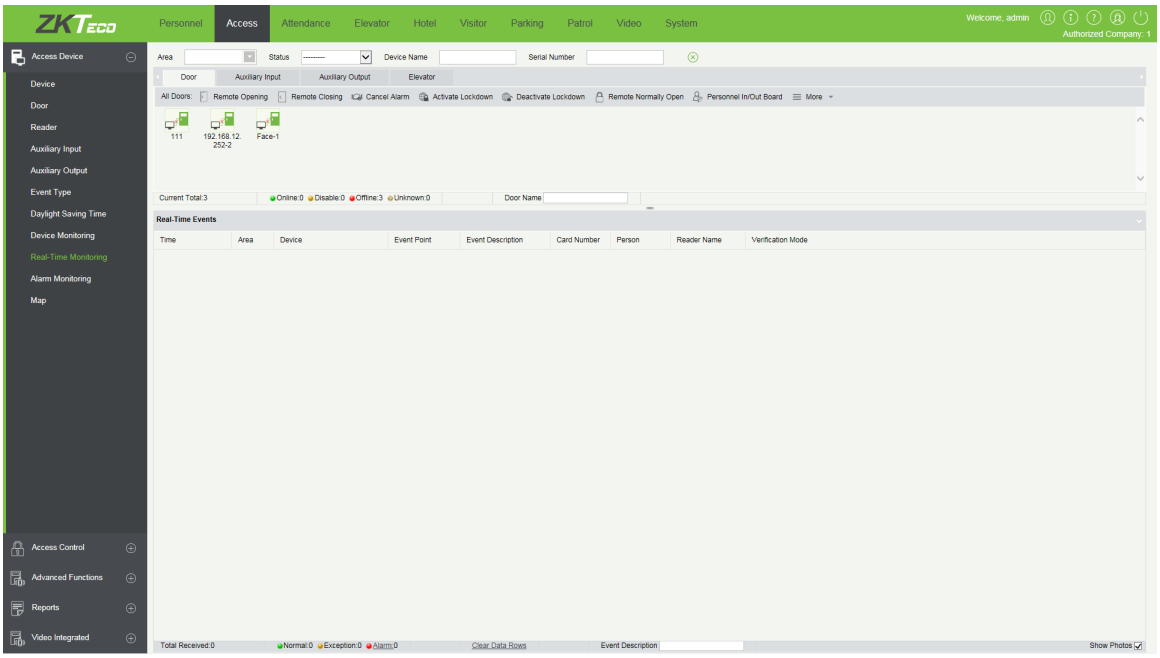
Click [Device Control] > [View and Get device Info] > [Get Personnel Information] in the Device page. Renew the current information in the device. The final value will be displayed in the device list.

2.5 Monitor in real time

Suppose a user with an ID card has been uploaded to device, when this card is punched on the device, the device will pass the verification (LED indicator light will turn green and be constant on for 2 seconds) and then generate an attendance record.

In ZKBiosecurity Software, click [Access] > [Access Device] > [Real-Time Monitoring] to monitor the statuses, real-time events of doors and punching on device in real time. If you want to stop monitoring, please click [Stop

Monitoring].


ZKTeco
Personnel
Access
Attendance
Elevator
Hotel
Visitor
Parking
Patrol
Video
System
Welcome, admin
Authorized Company: 1
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
Video Integrated
Area
Status
Device Name
Serial Number
Door
Auxiliary Input
Auxiliary Output
Elevator
All Doors:
Remote Opening
Remote Closing
Cancel Alarm
Activate Lockdown
Deactivate Lockdown
Remote Normally Open
Personnel In/Out Board
More
111
192.168.12.252-2
Face-1
Current Total:3
Online:0
Disable:0
Offline:3
Unknown:0
Door Name
Real-Time Events
Time
Area
Device
Event Point
Event Description
Card Number
Person
Reader Name
Verification Mode
Total Received:0
Normal:0
Exception:0
Alarm:0
Clear Data Rows
Event Description
Show Photos

CE Note

Manufacturer: ZKTECO CO., LTD.

Address: No.26, Pingshan 188 Industry zone, Tangxia Town, Dongguan City, Guangdong Province, China 523728

Hereby, ZKTECO CO., LTD. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

Importers: ZKTECO EUROPE SL

Address: Carretera de Fuencarral, 44 Edificio 1, Planta 2, 28108 Alcobendas, Madrid- Spain

A copy of the declaration of conformity can be obtained with this user manual; this product is not restricted in the EU.

The wireless operation frequency

RFID: 13.56MHz; Max H-Field Strength: -15.78dBuA/m at 10m

Or 125kHz; Max H-Field Strength: 20.13 dBuA/m at 10m

The device has been evaluated to meet CE general RF exposure requirement. The device can be used without restriction.

FCC Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the separation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure Statement

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.

Green Label

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone: +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com