

User Manual

ZKBio CVSecurity

Version: 1.0.0 Date: November 2022 Software Version: ZKBio CVSecurity_5.2.0 and above English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

ĸ

For further details, please visit our Company's website www.zkteco.com.

Copyright © 2022 ZKTECO CO., LTD. All rights reserved.

Without the prior written consent of ZKTeco, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ZKTeco and its subsidiaries (hereinafter the "Company" or "ZKTeco").

Trademark

ZKTECD is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or

typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on <u>http://www.zkteco.com</u>.

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit <u>www.zkteco.com</u>.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/Floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader door locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **ZKBioCVSecurity**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

	For Software		
Convention	Convention Description Bold font Used to identify software interface names e.g. OK, Confirm, Cancel.		
Bold font			
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.		
	For Device		
Convention	Description		
<>	Button or key names for devices. For example, press <ok>. Window names, menu items, data table, and field names are inside square brackets. For example, pop up the New User window.</ok>		
/	Multi-level menus are separated by forwarding slashes. For example, File/Create/Folder.		

Symbols

Convention	Description
	This represents a note that needs to pay more attention to.
ę	The general information which helps in performing the operations faster.
*	The information which is significant.
۲	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

TABLE OF CONTENTS

1	INST	ALLATIO	N AND LOGIN	
	1.1	Ор	PERATING ENVIRONMENT REQUIREMENTS	
	1.2	SYS	STEM INSTALLATION	
2	Pers	SONNEL.		21
	2.1	Pei	rsonnel Management	21
		2.1.1	Person	
		2.1.2	DEPARTMENT	
		2.1.3	Position	
		2.1.4	DISMISSED PERSONNEL	42
		2.1.5	Pending Review	43
		2.1.6	CUSTOM ATTRIBUTES	
		2.1.7	LIST LIBRARY	<mark>4</mark> 5
		2.1.8	Parameters	<mark>4</mark> 6
	2.2	CA	RD MANAGEMENT	
		2.2.1	Card	
		2.2.2	Weigand Format	
		2.2.3	Issue Card Record	54
3	Acc	ESS CON	TROL	
	3.1	Op	PERATION SCENARIO	55
	3.2	Ор	eration Process	
	3.3	Ac	cess Device	
		3.3.1	DEVICE	
		3.3.2	Door	65
		3.3.3	Reader	
		3.3.4	Auxiliary Input	
		3.3.5	Auxiliary Output	70
		3.3.6	EVENT TYPE	71
		3.3.7	DAYLIGHT SAVING TIME	73
		3.3.8	Device Monitoring	74
		3.3.9	Real-Time Monitoring	76
		3.3.10	Alarm Monitoring	
		3.3.11	Мар	
	3.4	Ac	cess Rule	
		3.4.1	TIMEZONE	
		3.4.2	HOLIDAY	
		3.4.3	Access Level	
		3.4.4	Set Access Level Allocation	

	3.4.5	SET ACCESS LEVEL GROUPS BY PERSON	93
	3.4.6	SET ACCESS LEVEL GROUPS BY DEPARTMENT	95
	3.4.7	INTERLOCK	
	3.4.8	Linkage	
	3.4.9	Anti-Passback	100
	3.4.10	THE FIRST-PERSON NORMALLY OPEN	101
	3.4.11	Multi-Person Group	
	3.4.12	Multi-People Open The Door	105
	3.4.13	Verification Mode	107
	3.4.14	Parameters	108
3.5	AD	VANCED FUNCTION	110
	3.5.1	ENTRANCE GUARD AREA(ZONE)	110
	3.5.2	Reader Definition	<mark>1</mark> 12
	3.5.3	WHO IS INSIDE	<mark>1</mark> 14
	3.5.4	GLOBAL ANTI-PASSBACK	115
	3.5.5	GLOBAL LINKAGE	
	3.5.6	THE GLOBAL INTERLOCK GROUP	
	3.5.7	THE GLOBAL INTERLOCK	121
	3.5.8	Personnel Availability	122
	3.5.9	OCCUPANCY CONTROL	124
	3.5.10	Muster Point	
	3.5.11	Muster Point Setting	129
3.6	Ac	CESS CONTROL REPORTS	131
	3.6.1	ALL TRANSACTIONS	
	3.6.2	Events from Today	
	3.6.3	ALL EXCEPTION EVENTS	134
	3.6.4	Access Rights by Door	
	3.6.5	Access Rights by Personnel	
	3.6.6	First In and Last Out	
Vide	EO MANA	\GEMENT	138
4.1	VIC	DEO VIEW	138
	4.1.1	VIDEO PREVIEW	138
	4.1.2	VIDEO PLAYBACK	
4.2	De	VICE MANAGEMENT	
	4.2.1	Device (Add Device)	
	4.2.2	CAMERA	145
	4.2.3	GROUP MANAGEMENT	157
4.3	De	CODING ON THE WALL	157
	4.3.1	Decoder	158

4

	4.3.2	TV WALL	
	4.3.3	LARGE SCREEN CONTROL	
4.4	Se	ARCH	
	4.4.1	Face Search	
	4.4.2	Vehicle Retrieval (AS1700)	
	4.4.3	TARGET COMPARISION (AS1700)	
	4.4.4	Search for Pictures with Pictures	
	4.4.5	Personnel Frequency Retrieval (NVR800)	
4.5	IN	TELLIGENT	
	4.5.1	Algorithm Model (AS1700 Supported)	
	4.5.2	TARGET INTELLIGENCE	
	4.5.3	BEHAVIOR ANALYSIS (AS1700 SUPPORTED)	170
	4.5.4	Crowd Situation	<mark>1</mark> 81
	4.5.5	GENERAL INTELLIGENCE (AS1700/ZKNVR SUPPORTED)	<mark>1</mark> 86
	4.5.6	VEHICLE INTELLIGENCE (AS1700 SUPPORTED)	<mark></mark>
	4.5.7	INTELLIGENT APPLICATION	
4.6	St	ATISTICS	
	4.6.1	FACE ANALYSIS	
	4.6.2	FACE REPORT	
	4.6.3	CROSS-LINE STATISTICS	
	4.6.4	Неат Мар	
	4.6.5	OBJECT STATISTICS	
	4.6.6	ALARM REPORT	
	4.6.7	PATROL REPORT	
	4.6.8	PATROL ALARM	
4.7	VI	DEO PATROL	
	4.7.1	Patrol Group	
	4.7.2	Patrol Plan	
	4.7.3	REAL-TIME PATROL	
4.8	М	AINTENANCE CONFIGURATION (AS1700 SUPPORTED)	207
	4.8.1	Developer Log	
	4.8.2	Client Request Log	
	4.8.3	CU REQUEST	
	4.8.4	PARAMETERS	210
4.9	VI	DEO INTERCOM	
	4.9.1	VIDEO INTERCOM EQUIPMENT	211
	4.9.2	CALL RECORDS	214
INTE	LLIGENT	ANALYSITS	
5.1	Sc	ENE APPLICATION	

5

5.1.1 TARGET SEARCH 5.1.2 PERSONNEL CONTROL 5.1.3 TAILING DETECTION 5.1.4 PERIMETER PROTECTION 5.1.5 ATTANDANCE CHECKING DETECTION 5.1.6 PEOPLE COUNTING 5.1.7 LIVE ALARM 5.1.8 MY DASHBOARD 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 10) 5.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2	
5.1.3 TAILING DETECTION 5.1.4 PERIMETER PROTECTION 5.1.5 ATTANDANCE CHECKING DETECTION 5.1.6 PEOPLE COUNTING 5.1.7 LIVE ALARM 5.1.8 MY DASHBOARD 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 S.2.1 TIMEZONE 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 5.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENA	
5.1.4 PERIMETER PROTECTION 5.1.5 ATTANDANCE CHECKING DETECTION 5.1.6 PEOPLE COUNTING 5.1.7 LIVE ALARM 5.1.8 MY DASHBOARD 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 / S.3 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION SCENARIO 6.3 ATTENDANCE MANAGEMENT	
5.1.5 ATTANDANCE CHECKING DETECTION	
5.1.6 PEOPLE COUNTING 5.1.7 LIVE ALARM 5.1.8 MY DASHBOARD 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 1) 5.3.3 SERVICE CONFIGURATION 5.3.4 TIMEZONE 5.3.5 CUSTOM ICON 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.1.7 LIVE ALARM 5.1.8 MY DASHBOARD 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 1 5.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION SCENARIO 6.3 ATTENDANCE MANAGEMENT	
5.1.8 My Dashboard 5.2 DEVICE MANAGEMENT 5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 1) 5.3.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
 5.2 DEVICE MANAGEMENT	
5.2.1 IPC CONNECTION (CURRENTLY, ONLY SUPPORT HWSDK CAMERA CON HARDWARE SUGGESTION LIST) 5.2.2 SERVICE CONFIGURATION 5.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.1 ALIVE ALARM QUERY 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 5.4.5 G ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION SCENARIO 6.3 ATTENDANCE MANAGEMENT	NECTION, PLEASE CHECK THE 231 CONNECTION) (SMART BOX) 233
HARDWARE SUGGESTION LIST) 5.2.2 ZKIVA-EDGE CONNECTION (CURRENTLY, ONLY SUPPORT ZKIVA-EDGE T1 1 5.3 SERVICE CONFIGURATION 5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.3 Service Configuration 5.3.1 TIMEZONE 5.3.2 Application Configuration 5.3.3 Regional Occupancy Control Configuration 5.3.4 Live Alarm Configuration 5.3.5 Custom Icon 5.3.6 Dashboard Configuration 5.3.7 Parameters 5.4 Reports 5.4.1 All Records 5.4.2 Entry & Exit Records 5.4.3 Trend Reports 5.4.4 Live Alarm Query 5.4.5 Dismissal Report 6 Attendance Management 6.1 Operation Scenario 6.2 Operation Flow 6.3 Attendance Management	
5.3.1 TIMEZONE 5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.3.2 APPLICATION CONFIGURATION 5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION 5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.3.3 REGIONAL OCCUPANCY CONTROL CONFIGURATION	
5.3.4 LIVE ALARM CONFIGURATION 5.3.5 CUSTOM ICON 5.3.6 DASHBOARD CONFIGURATION 5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.3.5 CUSTOM ICON	<mark></mark>
5.3.6 DASHBOARD CONFIGURATION 5.3.7 PARAMETERS 5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.3.7 PARAMETERS 5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
5.4 REPORTS 5.4.1 ALL RECORDS 5.4.2 ENTRY & EXIT RECORDS 5.4.3 TREND REPORTS 5.4.4 LIVE ALARM QUERY 5.4.5 DISMISSAL REPORT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
 5.4.1 ALL RECORDS	244
 5.4.2 ENTRY & EXIT RECORDS	
 5.4.3 TREND REPORTS	
5.4.4 Live Alarm Query	
5.4.5 DISMISSAL REPORT 6 ATTENDANCE MANAGEMENT 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT	
 6 ATTENDANCE MANAGEMENT	
 6.1 OPERATION SCENARIO 6.2 OPERATION FLOW 6.3 ATTENDANCE MANAGEMENT 	247
6.2 OPERATION FLOW6.3 ATTENDANCE MANAGEMENT	248
6.3 Attendance Management	
6.3.1 By Area	
6.3.2 Attendance Device Description (Attendance Device)	
6.3.3 Attendance Point	
6.3.4 Roll Call	
6.3.5 Command from Server	
6.3.6 Device Operation Log	
6.4 Attendance Setting	
6.4.1 Attendance Rule Setting	
6.4.2 Holidays	

	6.4.3	LEAVE TYPE	
	6.4.4	Automatic Report	
	6.4.5	Process Settings	
6.5	Re	gular Shift Setting Schedule	
	6.5.1	Тіметавle	
	6.5.2	Personnel Schedule	
	6.5.3	GROUP SCHEDULE	271
	6.5.4	Schedule Details	
6.6	Ex	CEPTION	
	6.6.1	Appended Log	
	6.6.2	Ask For Leave	
	6.6.3	Overtime	
	6.6.4	Adjust Rest	<mark>2</mark> 78
	6.6.5	Shift Adjustment	
6.7	Ат	TENDANCE DETAIL REPORT	
	6.7.1	Manual Calculation	
	6.7.2	Attendance Transaction Transaction	
	6.7.3	Daily Attendance	
	6.7.4	DAILY REPORT	
	6.7.5	MONTHLY DETAIL REPORT	
	6.7.6	Appended Log Details	
	6.7.7	LEAVE DETAILS	
	6.7.8	EXCEPTION REPORT	
	6.7.9	Work Time Report	
	6.7.10	ANNUAL LEAVE BALANCE SHEET	
6.8	CA	ALCULATE REPORT	
	6.8.1	LEAVE SUMMARY	
	6.8.2	Monthly Staff Report	
	6.8.3	MONTHLY DEPARTMENTAL	
	6.8.4	ROLL CALL REPORT	
CON	ISUMPTIC	DN	
7.1	Co	DNSUMPTION BASIC INFORMATION	
	7.1.1	Piecewise Fixed Value	
	7.1.2	CONSUMPTION TIME ZONE	
	7.1.3	Restaurant Information	
	7.1.4	MEAL INFORMATION	
	7.1.5	COMMODITY INFORMATION	
	7.1.6	Key Value Information	
	7.1.7	CARD INFORMATION	

7

7.2	Co	DNSUMPTION DEVICE	
	7.2.1	CONSUMPTION DEVICE	
	7.2.2	CONSUMPTION PARAMETER	
7.3	Co	DNSUMPTION CARD MANAGEMENT	
	7.3.1	Card Service	
	7.3.2	CARD MANAGEMENT	
	7.3.3	INCOME AND EXPENSES	
7.4	Co	DNSUMPTION DETAIL	
	7.4.1	CONSUMPTION DETAIL REPORT	
	7.4.2	CONSUMPTION EXCEPTION REPORT	
7.5	M	ANUAL SUPPLEMENT	
	7.5.1	MANUAL SUPPLEMENT	
7.6	Su	BSIDY	
	7.6.1	SUBSIDY REGISTRATION	<mark>3</mark> 12
	7.6.2	ONE- CLICK REVIEW	
	7.6.3	Review	
	7.6.4	Reissue the Command	
	7.6.5	DELETE	
	7.6.6	IMPORT	
	7.6.7	More	
	7.6.8	Export	
	7.6.9	DOWNLOAD TEMPLATE	
7.7	Co	DNSUMPTION REPORT	
	7.7.1	Issue Card Report	
	7.7.2	TOP UP REPORT	
	7.7.3	REFUND REPORT	
	7.7.4	Subsidy Report	
	7.7.5	Report of Return Card	
	7.7.6	CARD COST REPORT	
	7.7.7	CARD BALANCE REPORT	
	7.7.8	Non-Card Return Card Report	
	7.7.9	Report of Resume the Card	
7.8	Co	DNSUMPTION STATISTICS	
	7.8.1	Personal Consumption Report	
	7.8.2	Department Summary	
	7.8.3	Restaurant Summary	
	7.8.4	Device Summary	
	7.8.5	Income and Expenses Report	
	7.8.6	Meal Summary	

8	ELE1	ATOR C	ONTROL MANAGEMENT	
	8.1	Op	PERATION SCENARIO	
	8.2	Op	PERATION FLOW	
	8.3	ELE	EVATOR DEVICE	
		8.3.1	MANUALLY ADD ELEVATOR CONTROL DEVICE (DEVICE)	
		8.3.2	Expanding Board	
		8.3.3	Reader	
		8.3.4	FLOOR FLOOR SETTING	
		8.3.5	Auxilary Input	
		8.3.6	Event Type	
		8.3.7	Device Monitoring	
		8.3.8	Real Time Monitoring	
	8.4	EL	evator Control Rules	
		8.4.1	TIME PERIOD SETTINGTIME ZONES	
		8.4.2	Holiday Setting	
		8.4.3	ELEVATOR LEVELS	
		8.4.4	SET ACCESS BY LEVELS	
		8.4.5	SET ACCESS BY PERSON	
		8.4.6	SET ACCESS BY DEPARTMENT	
		8.4.7	DIRECT SELECTION SET	
		8.4.8	LINKAGE SETTING GLOBAL LINKAGE	
		8.4.9	PARAMETERS	
	8.5	ELE	EVATOR CONTROL REPORTS	
		8.5.1	ALL TRANSACTION	
		8.5.2	ALL EXCEPTION EVENTS	
		8.5.3	Access Rights by Floor	
		8.5.4	ACCESS RIGHTS BY PERSONNEL	
		8.5.5	First In and Last Out	
9	Par	KING MA	ANAGEMENT	
	9.1	Ор	PERATION SCENARIO	
	9.2	Ор	Peration Flow	
	9.3	BA	sic Parking Setting	
		9.3.1	Parking Settings	
		9.3.2	Device	
		9.3.3	Parking Area	
		9.3.4	ENTRANCE AND EXIT AREA	
		9.3.5	Guard Booth	
		9.3.6	CHANNEL	
		9.3.7		

		9.3.8	SHIFT SETTINGS	358
		9.3.9	Manual Release Reason	359
	9.4	Сн	arge Management	
		9.4.1	Fixed Cars Are Charging Rules	
		9.4.2	TEMPORARY CAR CHARGING RULES	
		9.4.3	Overtime Charging Rules	
		9.4.4	DISCOUNT STRATEGY	
		9.4.5	BUSINESS MANAGEMENT	
		9.4.6	FINANCIAL RECONCILIATION	
	9.5	VE	CHICLE MANAGEMENT	
		9.5.1	LICENSE PLATE REGISTERATION	
		9.5.2	VEHICLE AUTHORIZATION	
		9.5.3	Fixed Vechicle Extension	<mark>3</mark> 71
		9.5.4	BLOCK&ALLOW LIST MANAGEMENT	<u>37</u> 2
	9.6	Ref	PORT MANAGEMENT	
		9.6.1	VECHICLE INSIDE	
		9.6.2	ENTRY RECORD	
		9.6.3	Exit Record	
		9.6.4	Charge Record	
		9.6.5	Expired Vehicle	
		9.6.6	Fixed Vehicle Authorization Record	
		9.6.7	DEVICE OPREATION RECORD	
		9.6.8	HANDOVER STATISTICS	
		9.6.9	DAILY INCOME STATISTICS	
		9.6.10	MONTHLY INCOME STATISTICS	
	9.7	Re/	AL-TIME MONITORING	
		9.7.1	SENTRY BOOTH MONITORING	
		9.7.2	Monitor Room	
10		VISITOR	MANAGEMENT	
	10.1	Op	ERATION SCENARIO	
	10.2	Op	ERATION FLOW	
	10.3	Vis	ITOR REGISTRATION	
		10.3.1	ENTRY REGISTRATION	
		10.3.2	Visitor	
	10.4	Vis	ITOR RESERVATION	
		10.4.1	VISITOR RESERVATION	
		10.4.2	Reservation Audit	
		10.4.3	Invite	
		10.4.4	Respondent Self-Approval	

	10.5 BA	SIC MANAGEMENT	403
	10.5.1	Parameters	403
	10.5.2	DEVICE DEBUGGING	406
	10.5.3	Print Settings	407
	10.5.4	VISITOR LEVELS	409
	10.5.5	VISITOR COMMON PERMISSION GROUP	413
	10.5.6	Host Level	416
	10.5.7	SET UP PERMISSION GROUPS BY VISITED DEPARTMENT (VISITED DEPARTMENT LEVEL)	419
	10.5.8	ENTRY PLACE	421
	10.5.9	VISIT REASON	425
	10.5.10	CUSTOM ATTRIBUTES	426
	10.6 Ac	DVANCED	427
	10.6.1	CATEGORY	
	10.6.2	WATCHLIST	
	10.6.3	WATCH LIST THUMBNAILS	
	10.6.4	ALERT TEMPLATE	432
	10.6.5	LINKAGE	433
	10.7 Vis	sitor Reports	435
	10.7.1		435
	10.7.2	VISITOR HISTORY RECORD	
11		MANAGEMENT	
11	Patroi		438
11	PATROI 11.1 OF	MANAGEMENT	438 438
11	PATROI 11.1 OF 11.2 OF	PERATION SCENARIO	438 438 438
11	PATROI 11.1 OF 11.2 OF 11.3 PA	PERATION SCENARIO	438 438 438 438
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1	PERATION SCENARIO	438 438 438 438 438 438
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA	PERATION SCENARIO	438 438 438 438 438 438 438 439
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA	PERATION SCENARIO	438 438 438 438 438 438 439 439
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1	PERATION SCENARIO	438 438 438 438 438 438 439 439 439 440
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3	PERATION SCENARIO	438 438 438 438 438 438 439 439 439 440 441
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3	PERATION SCENARIO	438 438 438 438 438 438 439 439 439 440 441 441
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA	PERATION SCENARIO	438 438 438 438 438 438 439 439 439 440 441 442 442 442
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2	PERATION SCENARIO	438 438 438 438 438 439 439 439 439 440 441 442 442 442 442
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2 11.5.3	PERATION SCENARIO	438 438 438 438 438 439 439 439 439 440 441 442 442 442 443 444
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2 11.5.3	PERATION SCENARIO	438 438 438 438 438 438 439 439 439 439 440 441 442 442 442 442 442 443 444
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2 11.5.3 11.6 RE	MANAGEMENT PERATION SCENARIO	438 438 438 438 438 438 439 439 440 442 442 442 442 442 444 444 446
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2 11.5.3 11.6 RE 11.6.1	PERATION SCENARIO	438 438 438 438 438 438 439 439 440 442 442 442 443 444 444 446 448
11	PATROI 11.1 OF 11.2 OF 11.3 PA 11.3.1 11.4 BA 11.4.1 11.4.2 11.4.3 11.5 PA 11.5.1 11.5.2 11.5.3 11.6 RE 11.6.1 11.6.2 11.6.3	MANAGEMENT	438 438 438 438 438 438 439 439 440 442 442 442 444 444 446 448 449

12.1	Op	eration Scenario	451
12.2	Ор	ERATION FLOW	451
12.3	Сн	ANNEL DEVICE	452
	12.3.1	Passage	452
	12.3.2	Device	453
	12.3.3	GATE	460
	12.3.4	Reader	461
	12.3.5	Auxiliary Input	462
	12.3.6	Event Type	462
	12.3.7	DAYLIGHT SAVING TIME	
	12.3.8	DEVICE MONITORING	465
	12.3.9	Real-Time monitoring	
12.4	En	TRANCE CONTROL	<mark>4</mark> 67
	12.4.1	Barrier Gate Permission Group	<mark>4</mark> 67
	12.4.2	SET ACCESS BY LEVELS	<mark></mark>
	12.4.3	ANTI-PASSBACK	471
	12.4.4	LINKAGE SETTING	
	12.4.5	Parameters	
12.5	PA	SSAGE SETTINGS	
	12.5.1	BARRIER GATE PASSING RULES	475
	12.5.2	FLAP BARRIER	
	12.5.3	Swing Barrier	
12.6	Сн	ANNEL REPORTS	
	12.6.1	ALL TRANSACTIONS	
	12.6.2	TODAY'S ACCESS RECORD	
	12.6.3	Personnel Last Access Location	
	12.6.4	ALL EXCEPTION EVENTS	
	TEMPER	ATURE DETECTION	484
13.1	Op	eration Scenario	
13.2	Op	ERATION FLOW	
13.3	Set	TING OF EPIDEMIC PREVENTION PARAMETERS	
13.4	TEN	MPERATURE MANAGEMENT	
	13.4.1	Real-Time Monitoring	
	13.4.2	STATISTIC PANEL	
	13.4.3	Temperature Raw Record	
	13.4.4	Individual Temperature Record	
	13.4.5	Abnormal Temperature Record	
	13.4.6	DEPARTMENT DAILY STATISTICS	
	13.4.7	Monthly Statistics	
	12.2 12.3 12.4 12.5 12.6 12.6 13.1 13.2 13.3	12.2 OP 12.3 CH 12.3.112.3.212.3.312.3.412.3.512.3.612.3.712.3.812.3.912.412.4.112.4.212.4.312.4.312.4.312.4.312.5.112.5.212.5.312.512.512.512.612.6.112.6.212.6.312.6.412.6.312.6.412.6.312.6.112.6.312.6.312.6.413.413.413.4.113.4.313.4.113.4.313.4.6	12.2 OPERATION FLOW

	13.4.8	AUTOMATIC REPORT	
	13.4.9	Parameters	
14	SERVIC	E CENTER	
	14.1 Di	EVICE CENTER	
	14.1.1	Device	
	14.2 Ev	/ENT CENTER	
	14.2.1	The Event Type	
	14.2.2	The Event Record	
	14.3 No	OTIFICATION CENTER	
	14.4 TH	HE MAP CENTER	500
	14.4.1	Real-Time Monitoring	
	14.4.2	MAP CONFIGURATION	
	14.5 Pu	JSH CENTER	<u>5</u> 08
	14.5.1	Push Configuration	
	14.5.2	PUSH EXCEPTION RECORD	<u>50</u> 9
15	System	I MANAGEMENT	510
	15.1 Sy	STEM MANAGEMENT	
	15.1.1	OPERATION LOG	
	15.1.2	DATABASE MANAGEMENT	
	15.1.3	AREA SETTINGS	513
	15.1.4	E-MAIL MANAGEMENT	
	15.1.5	DICTIONARY MANAGEMENT	
	15.1.6	DATA CLEANING	
	15.1.7	Audio File	
	15.1.8	CERTIFICATE TYPE	
	15.1.9	PRINT TEMPALATE	
	15.1.1	0 System Monitoring	
	15.1.1	1 Parameters	
	15.2 Au	JTHORITY MANAGEMENT	
	15.2.1	User	
	15.2.2	ROLE	
	15.2.3	API AUTHORIZATION	
	15.2.4	CLIENT REGISTER	
	15.2.5	Security Parameters	530
	15.3 Co	OMMUNICATION MANAGEMENT	
	15.3.1	Device Commands	
	15.3.2	COMMUNICATION DEVICE	
	15.3.3	Product	534
	15.3.4	Authorized Device	

	15.3.5	COMMUNICATION MONITOR	536
	15.4 TH	IIRD PARTY INTEGRATION	537
	15.4.1	LED DEVICE	537
	15.4.2	DIGIFORT CAMERA	
	15.4.3	LINE NOTIFICATION	
	15.4.4	AD MANAGEMENT	545
	15.4.5	SMS MANAGEMENT	
16	FACEKI	OSK	
	16.1 FA	cekiosk Device	548
	16.1.1	Device	548
	16.1.2	Set Attendance by Area	
	16.1.3	Set Attendance by Person	550
	16.2 M	edia Advertisement Resources	<u>5</u> 51
	16.2.1	Advertisement Resources	
	16.2.2	Advertisement Settings	
		CEKIOSK REPORTS	
		VERIFICATION RECORD	
17	HOTEL	System	
	17.1 De	EVICE MANAGEMENT	
	17.1.1	DEVICE	553
	17.2 Rc		555
	17.2.1	ROOM MONITOR	
	17.2.2	RESERVATION	555
	17.2.3	RESERVATION LIST	556
	17.3 CA	ARD MANAGEMENT	559
	17.3.1	READ CARD	559
	17.3.2	CANCEL CARD	
	17.3.3	Setting Card	
	17.4 Ho	DTEL MANAGEMENT	
	17.4.1	HOTEL SETTINGS	
	17.4.2	ROOM Түрез	564
	17.4.3	Rоом	
	17.4.4	HOTEL FACILITY	566
	17.4.5	Booking Methods	
	17.5 RE	PORT MANAGEMENT	
	17.5.1	GUEST CHECK-IN REPORT	
	17.5.2	ROOM OCCUPANCY REPORT	
	17.5.3	Room Charges Report	
	17.5.4	Issue Card Report	

	17.5	.5	Write Card Record Remotly	
	17.5	.6	UNLOCK LOG REPORT	572
	17.5	.7	Device Command List	572
	17.5	.8	Lost Card List	573
18	INTR	USI	ON	574
	18.1	Int	RUSION DEVICE	574
	18.1	.1	Device	
	18.1	.2	Partition	577
	18.1	.3	Zone	579
	18.1	.4	Device User	
	18.2	Re/	al-Time Monitoring	582
	18.3	Ιντ	RUSION RECORD	583
19	Loci	(ER		<mark>5</mark> 85
	19.1	Lo		
	19.1	.1	Device	<u>58</u> 5
	19.1	.2	Parameters	
	19.1	.3	VISUAL PANEL	
	19.2	Lo	CKER REPORT	590
	19.2	.1	ALL TRANSACTION	590

1 Installation And Login

1.1 Operating Environment Requirements

Category	Minimum Configuration Requirements				
CPU	At least Intel quad-core (above intel core i5-6600)				
RAM	Not less than 8GB				
Hard Disk Not less than 500GB (the remaining space of the system disk is more to 15GB)					
OS Support 64-bit Windows 7 Professional Edition, 64-bit Windows 10 O					
Graphics Card	Intel integrated graphics, video memory greater than 2.0G (Intel [®] HD Graphics 530 and above recommended)				
Network Card	At least one network card, the recommended network speed is not less than 1000Mbit/s				
Monitor	At least 21.5 inches, and the best resolution of the monitor is recommended: 1920 * 1080. It is recommended to set the display resolution to 1920 * 1080. Using other resolutions may cause the interface to be abnormal.				
Browser Support Chrome33+ (recommended)/Firefox27+/Explorer11+					

Table 1-1

Instruction:

The number of live channels supported under the minimum configuration requirements:

Resolution	Configuration a (H.264 format)	Configuration a (H.265 format)
CIF (512K)	38	38
4CIF/D1(2M)	22	22
720P(2M 25fps)	10	10
1080P(4M 25fps)	6	6
	Table 1-2	

Table 1-2

In the video preview window, you can view the system CPU or memory usage in real time. If the CPU reaches 80%, it is not recommended to increase the video preview window, which will cause the video stream to freeze; if the CPU has reached 80% and the video window does not meet the actual application, the system configuration needs to be improved.

1.2 System Installation

Step 1: Obtain the installation package.

Instruction:

Before installing the software, it is recommended to close the anti-virus software in the system to avoid failing the environment detection. If the antivirus software detects abnormality, you can also choose to ignore it.

After running the application, there will be a few seconds of detection process, please be patient.

Step 2: Right-click the installation package installer, choose to run as an administrator, and the environment detection tool will automatically perform system environment detection. If an abnormality is detected during the installation process, the interface will give a prompt. The user can refer to the prompt information to repair, and re-test after repairing until all the test items are passed before proceeding to the next Step.

Step 3: If the detection is normal, click **Continue**.

Step 4: Select "I agree to this agreement (A)" and click Next.

Step 5: After configuring the server port and other parameters, click Next.

Instruction:

The default port is 8098, and the Adms service port defaults to 8088.

If the port is occupied, please modify the port number manually. When modifying, try to avoid the occupied ports in the system, and can not overlap with the database port 5442, redis port 6390, and 21 and 80 ports.

Check "Add firewall exception to this port" to prevent Windows Firewall from blocking the program from running.

The https protocol is used by default.

Step 6: After setting the installation directory, click Next.

Instruction:

The default installation path is C:\Program Files\ZKBioCVSecurity. You can also click **Browse** to customize the installation path. Please follow the interface prompts to ensure that the selected installation path has enough disk space.

Step 7: After setting the backup file storage path, click **Next**.

Instruction:

The system scans the entire disk by default, locates the drive letter with the largest free space, and creates a new SecurityDBBack folder. You can also click **Browse** to customize the storage path of the backup file.

Step 8: Click "Install" to start installing the software.

Step 9: After the installation is complete, you will be prompted whether to restart the computer immediately (the default is "Yes"). Click **Finish** to restart the computer to complete the software installation.

Instruction:

After the software installation is complete, it will take a long time (about 2 minutes) for the service to start up. Please wait patiently for the service to start and then complete the operation.

Step 10: Enter the login page as shown in Figure 1-2, log in to the system.

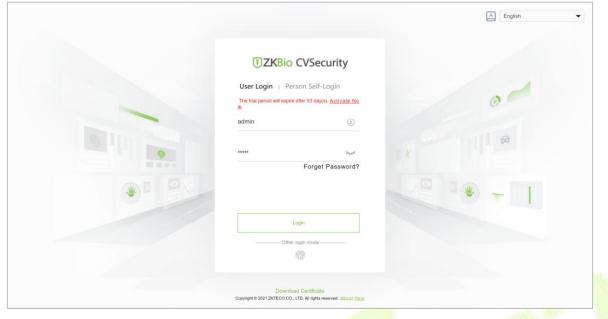


Figure 1-1

2 Personnel

Before using the other functions, please configure the personnel system: Personnel and Card Management.

TKBio CVSecurity									
🛔 Personnel 🗸 🗸	Personnel / Personnel / Person								
Person	Department Name	Personnel ID	Na	ame	More *	Q 🖉			
Department									
Position	к ^л л ⁴	C Refresh ∓ New	Es Personnel Adju	istments - 🖻	Delete * 1 Export	* ± Import *	··· More 👻		
Dismissed Personnel	 ⑦ Department Name(14) ⑦ Development(5) ⑧ hr(1) ▲ best9(0) ▶ test8(0) 	Personnel ID	First Name L	ast Name	Department Name	Card Number	Verification Mode	Create Time	Operations
Pending Review		1	tang O	DP1	Department Name	123123232	8 0%	2022-07-22 08:38:21	2 🗇
Custom Attributes		9527			Department Name	1139274691	8	2022-07-26 02:38:20	∠ â
List Library	▶ □ test7(0)	<u> </u>	tsf		Department Name			2022-07-26 02:38:20	_ ₪
Parameters		<u>666</u>	chen		Department Name			2022-07-26 02:38:20	2 1
		9999	K-TEST		Department Name		d 8	2022-07-21 00:23:45	<u>/</u> 🖻

Figure 2-1 Personnel

2.1 Personnel Management

Personnel Management includes these modules: **Person, Department, Position, Dismissed Personnel, Pending review, Custom Attributes, List Library,** and **Parameters.**

Operating Procedures:

This operation process is suitable for guiding users how to configure and manage the basic personnel organization after the system is installed.

The flow of personnel organization configuration is shown in Figure 2-2.

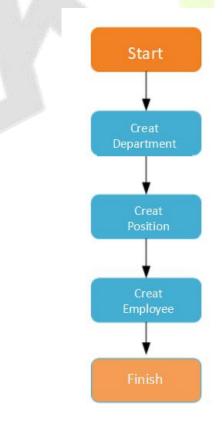


Figure 2-2 Flowchart of Personnel Configuration

2.1.1 Person

When using this management program, the user shall register personnel in the system, or import personnel information from other software or documents into this system.

Main functions of Person include Refresh, Add (New), Personnel Adjustments, Delete, Export, Import, and more.

2.1.1.1 Add Personnel (New)

Click **Personnel** > **Personnel** > **New**.

			New			×
Personnel ID* First Name Gender Certificate Type Birthday Hire Date Device Verification Passwo Biometrics Type	10000		Department* Last Name Mobile Phone Certificate Number Email Position Name Card Number	Department Name		Browse Capture Personnel Detail >
Levels Settings			Superuser Device Opera Extend Passa Disabled Set Valid Time	ge	•	
Add	Select All Uns	elect All				
		Save and New	ОК	Cancel		

Figure 2-3 Add Personnel New

Fields are as follows:

∠Notes:(Personnel ID)

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**.

Parameter	Description
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.
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	The max length is 20, and this is an optional field.
Certificate Type	There are four types of certificates: ID, Passport, Driver License and Others. Select one to upload.
Certificate Number	Enter certificate number
Birthday	Input employee's actual birthday.
Email	Set the available email address of the personnel. The max length is 30. Punctuations, namely, the "-", "_" and "." are supported. If the Event Notification is checked, the Email is required.
Hire Date	It is the date on which the personnel are appointed. Click to select the date.
Position Name	Set a suitable name for the position. Any character, maximum combination of 100 characters. Position names should not be repeated.
Device Verification Password	Set password for personnel accounts. It can only contain up to 6-digits. If a password exceeds the specified length, the system will truncate it automatically. It cannot be the same with others password and the duress password.
Card Number	The max length is 10, and it should not be repeated.

Table 2- 1 Personnel ID

Biometrics Type:

This paper introduces the Steps of personnel biometric registration in ZKBioCVSecurity. The registered biometric data can be used for verification and identification of **Access Control**, attendance, and other equipment.

Biometric registration includes **fingerprint**, **finger vein**, and **palm registration**. Since the interfaces of fingerprint registration and finger vein registration are similar, fingerprint registration and palm print registration are used as examples to illustrate the operation process.

Description:

The server side of the box does not support external "palmprint meter, finger vein meter" to collect biometrictemplates, and the fingerprint reader is only supported by the "Live20R" model.

Preconditions:

On the computer terminal where the administrator registers the personnel information, connect the fingerprint reader device through the USB port.

Steps:

Step 1: In the **Personnel** module, choose **Personnel Management > Person**.

Step 2: Click Add with the mouse, and the interface for adding personnel will pop up.

Step 3: On the interface for adding personnel, click the "^{Solon}" button.

Step 4: (Optional) If the driver is not installed, click the icon to pop up the registration and driver download box, download the driver, and complete the installation.

Step 5: After the driver is installed, fingerprint registration can be performed, as shown in Figure 2-4.

	Registe	er	×
Fingerprint	Finger Vein	Palm registration	•
	~	Please select a finger.	
nnn		Duress Finger	print
\bigcirc	0	Ок Cancel	
	Device Driver is pr		

Figure 2-4 Biometric Type

Step 6: Select the fingers respectively, press the fingerprint on the connected fingerprint reader three times in a row, and the system prompts the fingerprint to be registered successfully.

Step 7: Click OK to save and close the fingerprint registration interface.

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 local photo to upload.

Capture: Taking photo by camera is allowed when the server is connected with a camera.

Access Control:

Click Access Control parameter for the personnel.

Access Control Levels Settings General	Time Attendance	Elevator Control	Plate Register Pass Superuser Device Operation Role Extend Passage Disabled Set Valid Time	No Ordinary User	FaceKiosk	Personnel Detail •
		Save and New	OK Cancel			

Figure 2-5 Access Control

Fields are as follows:

Parameter	Description
Level settings	Click Add , then set passage rules of special positions in different time zones.
Superuser	In access controller operation, a super user is not restricted by the regulations on time zones, anti-passback and interlock and has extremely high door- opening priority.
Device Operation Role	Select administrator to get its levels.
Extend Passage	Extend the waiting time for the personnel through the access points. Suitable for physically challenged or people with other disabilities.
Disabled	Temporarily disable the personnel's access level.
Set Valid Time	Set Temporary access level. Doors can be set to open only within certain time periods. If it is not checked, the time to open the door is always active.



		Add to Levels	×
Level Name	Time Zone	Q &	
Alternative		Selected(0)	
Level Nam	ne Time Zone	Level Name Time Zone	
K-Test	24-Hour Accessible		
multibio	multibio	>>	
☐ test	24-Hour Accessible	< No data	
ic c 1-3	> >∣ 50 rows per page 👻	o NO data	
	an a	OK Cancel	

Figure 2-6 Level Settings

∕≤Note:

- 1. The system will automatically search for the relevant numbers in the departure library during verification.
- 2. 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.
- 3. 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. If the user needs to use this function, please upgrade the device.
- 4. Not all the devices support the "Set Valid Time" function of setting the hour, minute, and second. 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. If the user needs to use this function, please upgrade the device.

Time Attendance:

Set the **Time Attendance** parameter for the personnel.

•	Access Control	Time Attendance	Elevator Control	Plate Register	Pass	age Setting	FaceKiosk	Personnel Detail 🕨
	idance Area			Attendance M	ode	Normal Attenda	ance 🔻	
4	Area Name			Device Opera	tion Role	Employee	5	
	🗌 🗊 XM 🗌 🗊 T Campus			Verification M	ode		•	
			Save and New	ОК	Cancel			

Figure 2-7 Time Attendance

Fields are as follows:

Parameter	Description
Attendance Mode	You can set the staff attendance area as Normal Attendance and No Punch Required.
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, Employee , Enroller , Administrator , and Superuser
Verification Mode	You can set verification mode as following options: Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.

Table 2-3 Time Attendance

Elevator Control:

Click Elevator Control, set the Elevator Control parameter for the personnel.

•	Access Control	Time Attenda	ance Elevator Control	Plate Register	Passage Setting	FaceKiosk	Personnel Detail 🕨
	Please add a elevato	or control level!		Superuser Set Valid Time	No). *	
	Add	Select All	Unselect All				
			Save and New	ок	Cancel		

Figure 2-8 Elevator Control

Fields are as follows:

NIDerlicer	In elevator controller operation, a super user is not restricted by the regulations on time zones, holidays and has extremely high door-opening priority.
Sof Valid Limoc	Set Temporary elevator level. Floor buttons can be set to be pressed only within the time periods. If it is not checked, the time to press the floor button is always active.

Table 2- 3 Elevator Control

Solution Note: The Elevator level must be set in advance.

Plate Register:

Click **Plate Register**, set the plate control parameter for the personnel.

Access Control	Time Attendance	Elevator Control	Plate Register	Passage Setting	FaceKiosk	Personnel Detail 🕨
License Plate		Pa	king Space Number			\otimes \oplus
		Save and New	ок	Cancel		
		35 113	217 - 228			

Figure 2-9 Plate Register

Fields are as follows:

Parameter	Description
License Plate	The user needs to register the licese plate.
Parking Space Number	Parking space number corresponding to the vehicle.
10 CT	Table 2. 4 Plate Persister

Table 2- 4 Plate Register

Note: Each personnel may register a maximum of 6 license plates.

Passage Setting:

Click **Passage Setting**, set the Passage Setting parameter for the personnel.

•	Access Control	Time Attenda	ance Elevator Contro	I Plate Register P	assa	age Setting	FaceKiosk	Personnel Detail 🕨
	els Settings			Superuser		No	•	
~	General			Device Operation R	ole	Ordinary User	•	
	Add	Select All	Unselect All					



Fields are as follows:

Parameter	Description
Superuser	Set Superuser as Yes or No according to requirement.
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, Ordinary User, Administrator , and Enroller.
	Table 2- 5 Passage Setting

Facekiosk:

Click **Facekiosk**, set the Facekiosk parameter for the personnel.

•	Access Control	Time Attendance	Elevator Control	Plate Register F	assage Setting	FaceKiosk	Personnel Detail 🕨
1999	eKiosk Area			Device Operation R	ole Employee	•	
4	Area Name			Personnel Type	Common	-	
	🗌 🗊 XM 🗌 🗊 T Campus						
	Campus						
-							
			Save and New	OK Can	1		

Figure 2-11 Facekiosk

Fields are as follows:

Parameter	Description
Device Operation Role	It will set the authority for operating the device and send it to the corresponding device such as, employee and Superuser.
Personnel Type	Select type of personnel such as Common, VIP, and Blocklist.

Table 2- 6 Facekiosk

Personnel Details:

Click **Personnel Details**, to set the Personnel detail parameter for the personnel.

Employee Type Hire Type Job Title Street		
Home Phone Home Address Office Phone Office Address Any exposure to suspected ca ses Yes No Any symptoms in the last 14 d None Cough Fever ays City visited in past 14 days Remarks on health		

Figure 2-12 Personnel Details

After entering the information, click **OK** to save and exit, the person details will be displayed in the added list.

2.1.1.2 Personnel Adjustments

Click Personnel > Person > Personnel Adjustment.

Adjust Department:

Click **Personnel** > **Person** > **Personnel Adjustment**, then select **Adjust Department**.

Department Name	Personnel ID	Name	More * Q 🖉				
^ر א ^ע	C Refresh ∓ Nev	v Es Personnel Adjustments	💼 Delete 🍷 🛧 Export 🍷 👱 Impor	* … More *			
Department Name(11)	Personnel ID	First Name Last Name	Department Name Card Numbe	r Verification Mode	Create Time	Oper	ration
Development(5) Image: Provide the second	1	ju	Department Name	•	2022-07-22 08:38:21	2	۵ ۱
✓ ➡ test9(0) → ➡ test8(0)	9999	K-TEST	Adjust Department ×	ೆ ೫	2022-07-21 00:23:45	₫	ŵ
 testo(0) test7(0) 	<u>12135</u>	Selected Person*	1		2022-07-12 09:23:52	0	ŵ
	<u>12134</u>	name1			2022-07-12 06:02:20	0	创
	□ <u>1114</u>	Md. Jala New Department* Transfer Reason		8	2022-05-10 08:10:52	0	Û
1	<u>1119</u>	multibio		ď	2022-06-18 09:43:14	2	۵,
		>1 50	17 r	ecords			Þ

Figure 2-13 Adjust Department

Fields are as follows:

Parameter	Description
New Department	Select new department from list.
Transfer Reason	Mention the reason for transfer.
	Table 2- 7 Adjust Department

Change Position:

Click **Personnel > Person > Personnel Adjustment**, then select **Change Position**.

Selected Person*	1	
New Position*		
Transfer Reason		

Figure 2-14 Change Position

Parameter	Description
New Position	Select new Position from list.
Transfer Reason	Mention the reason for transfer.
	Table 2-8 Change Position

Dismissal:

Click **Personnel > Person > Personnel Adjustment**, then select **Dismissal**.

Dismissal Date*	2022-07-25
Dismissal Type*	
Dismissal Reason	
Disable	

Figure 2- 15 Dismissal

Fields are as follows:

Parameter	Description
Dismissal Date	Select date.
Dismissal Type	Select the type of dismissal from follows, Voluntary Redundancy, Transfer, Dismissed, Resignation.
Dismissal Reason	Mention the reason for Dismissal.

Table 2-9 Dismissal

2.1.1.3 Delete

Click **Personnel > Person**, then select **Delete**.

Delete Personnel:

Click **Personnel > Person > Delete**, then select **Delete Personnel**.

Delete Biometric Data:

Click **Personnel > Person > Delete**, then select **Delete Biometric Data**.

2.1.1.4 Export

Click **Personnel > Person**, then select **Export**.

Export Personnel:

Click **Personnel > Person > Export**, then select **Export Personnel**.

Personnel's basic information is all checked (selected), check custom attributes as required.

		Export Personnel			
Basic Information	Personnel ID	First Name	🔄 Last Name	Department	
	Department	Gender	Birthday	Mobile Phone	
	🛃 Card Number	License Plate	🗹 Email	Certificate Type	
	Z Certificate Nu	Position Num	Position Name		
Custom Attributes	Office Phone	Office Address	City visited i	Remarks on	
	Employee Ty	Hire Type	Job Title	Any exposur	
	Street	Any sympto	Birthplace	Country	
	Home Phone	Home Address			
Encrypt or not	🚫 Yes 💿 No				
File Format	EXCEL	•			
Data to Export	All (max 10000)	0 records)			
	O Selected (max	100000 records)			
	Start Position	1			
	Total Records	100			
	Total Records	100			
		ок Са	ncel		

Figure 2-16 Export Personnel

Autos	ave 💽 🗄 🖓	=	20220725124611 - Prot		arch (Alt+Q)			Pooja A N 🤒	<i>ä</i> = -	
le	Home Insert	Page Layout Formu	ilas Data Rev	riew View Help						🖻 Sha
PR	DTECTED VIEW Be c	areful—files from the Internet o	an contain viruses. Unl	ess you need to edit, it's safer to	o stay in Protected View.	Enable Editing				
	• : ×	√ <i>f</i> _x Person								
	A	В	С	D	E	F	G	Н	1	
								Person		
	Personnel ID	First Name	Last Name	Department Number	Department Name	Gender	Birthday	Mobile Phone	Card Number	L
	1	ju	111111	1	Department Name					
	9999	K-TEST		1	Department Name					
	12135			1	Department Name					
	12134	name1		3	hr	Male				
	1114	Md. Jalal		2	Development	Male			123456	
	1119	multibio		1	Department Name					
	5	уууу		1	Department Name					
	2222	ygv		1	Department Name					
	555	fc		1	Department Name					
	4	W9		1	Department Name					
	3			1	Department Name					
	1118			1	Department Name					
	1116			1	Department Name					
	1115	Zorro		2	Development					
	1113	Abdulla		2	Development	Male			654321	
	1111	Esha Test		2	Development	Female			145632	
	1112	Anwar Hossain Abid		2	Development	Male			654987	
	Person	÷				: 4				

Figure 2-17 Export Personnel

Export Biometric Template:

Click **Personnel > Person > Export**, then select **Export** Biometric Template.

	Export Biometric Template	
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	OK Cancel	

Figure 2-18 Export Biometric Template

1							Personnel	Biometric Template			
2	Personnel ID	First Name	Last Name	Biometric Template Validity	Biometric Template Type Number	Biometric Template Type	Biometric Template Version	Biometric Template	Biometric Template No.	Biometric Template Index	Duress
3	1	tang	OP1	Effective	8	Palm Vein	12	apotecoartry UIA2WAA2Wq&AT*UIUXUBXX8VICEHIJWTIJ2EULWTI3 CEWFnTqHe7vKH9fTUMamv&Cfr7RHHHcCbmp+IdQYHMEUJjgzIItoC EBTrohzngjSwteDn84USKfqIZA/EKngSorsJSpidVyfY3MTY3JhW392 tbTfoDRUJD8onqIQ4/CY4PS0SP5J3qLtpJ2YfWJbbwHiNN92EdAJBmZ n9KD2o0INNONISXJz+Lnv+hASS0gbC35/UII6TU2BmS2eVqLRQYWRJ In8KyyZ2XEBIV2Q6Cocm0aKJPC3KV8CPreq3a6vCH+LPDRCKIS0YL 7BLKnOMApWH9IRMbHUERVQtvrRg/IULITI4A7Xsq9UX7TXN7fdG4 bu0BTSLr6errWIBI/AVWTbX8fb3zJTGMv0JzTpDBwIDKMo6AQZXOChL Kq4PPN8u0QttNaQffhobyIF3EyShRIJgHSYnS0VDp6jH1gXx21z/fbL0 CH+HSCQJ4/yMrSiExb1Fj+OEpLXMbdwBj0XE/SJFZXwNfD1YSiyFNKEG JJ/eV/6iqX+mdgHG5vK7JSG5d7vp0+Xp7SVDJ7HhC05iBY4HGRQAJ9 B80a/EXTARBH59YW73a76fFmv02QHVWLtraqmrcSh12gXT3 7a3IPaG/LuFJRH5sLD6AvqmcdB6fzL+S7PnR+TTcFT73iqrtrbtB03Q+Ut 0SXDgubnYDJaW0XXPqQGnvLzfG5GBPHIaPMoKP7/lvq3MAybkAuMc AoL44xXINLPRAQBRYXixeDnN7JJRISWSJJJv1A0ARsaYgrS4voylodf 9mv5L5no6P+V/rD9Vbp3Gu/pdblD7Lrg9e+1WyqanoTKIGFsYfRkzrK zryIdh6iILZłxb6/m1ZrcIbZUjEsrcIv9NXbBIJxdzrtbKs8dJfb4lzdDb6 ELJV/gfyV8K4UTw5e7Vbwxw8d31stFr7bxR93DeeKZ52QYHmu4H bAuQrarTMB11nLEB7k0F7b84fMk4BRCL2BYCVDiorEMVGTJpMYSz EJY32PV1JzxR8agckJD1Y32wGF0356kSPWTTAmX1ZcqNlpBRdF1A026J YqLd6fqeDJgbyIZ3xq42D491jnTc+gaKJNcykBJXgb36js6jNR01u MqnxrRmbg7UgzNN+44K3MbH217TLNxNF3DeeKZ52QYHmu4H bAuQrarTMB11nLEB7k0b7b9B4fMk4BRCL2BYCVDiorEMVGTJpMYSz EJY32PV1JzxR8agckJD1Y32wGF0356kSPWYTTamX1ZcqNlpBRd5fL01u MqnxrRmbg7UgzNN+44K3MbH217TLNxNF3DeeKZ52QYHmu4H bAuQrarTMB17JLgZNN+44K3MbH217TLNxNF3DeeKZ52QYHmu4H bAuQrarTMB17JLgZNN+44K3MbH217TLNxNF3DeeKZ52QYHmu4H bAuQrarTMB17JLgZNN+44K3MbH27TLNxNF3DeeKZ52QYHmu4H bAuQrarTMB17JLZXAb2QP6JJACF43SW5JA65JAV7S5GTdKbIUS YqL6fqE0JBgV1ZXAq52QP6JJACF43SW5JA65JAV71TamX1ZcqNlpBRd5fL01U MqnxrRmbg7JLgZNN+44K3MbH27TLNxNF3DeeKZ52QYTMa4H bAUQrarTMB17JLZZAq52QP6JJACF43SW5JA657DeeKAKX5YMWpdCDUV xb7t7u0+20fN4FBszurrtXJPKN5+Gwaixb3SXdfYrV1qEm0hgIDjda11 nF1EVM+Yg4PmTK5BAwP450Zh0b8JA57DaeKAKX5YMWpdCDUV		1	No



Export Personnel Photo:

Click **Personnel > Person > Export**, then select **Export Personnel Photo**.

Encrypt or not	🔿 Yes 💿 No	
File Format	ZIP 🔹	
	OK Cancel	

rigure 2-20 Export reisonner in

2.1.1.5 Import

Introduce the configuration Steps of manually importing personnel in batches in ZKBioCVSecurity.

It is suitable for scenarios where a large number of personnel information is added. Compared with the manual registration method of individual personnel, the batch import and addition method is faster.

Before adding departments in batches, you need to fill in the template file as required. After filling out the template file, you can import and add departments in batches in the "Department" interface.

Instruction:

- 1. The import and addition of personnel includes importing personnel information, personnel biometrictemplate data (optional), and personnel photos (optional), which need to be imported separately.
- 2. Importing is to pay attention to the uniqueness of the personnel number. When the personnel number is repeated, the result of import and addition will fail.

• Import Personnel Information

Before adding people in batches, you need to obtain or fill in a template file as required. After filling in

the template file, you can import and add people in batches on the Personnel Management > Personnel interface.

Steps:

Step 1: In the Personnel module, choose "Personnel Management > Personnel".

Step 2: On the personnel interface, select and click the "**Import** > **Download Personnel Import Template**" button, select the parameters to be filled in, and download the template "personnel information template.xls" locally. The parameter selection is shown in Figure 2-21.

partment Name	Personnel ID	Name	More -	Q @		
۲ ^μ	O Refresh ⊒∓ New 18 Per	onnel Adjustments 👻	ੰ Delete - ↑ Export	* 坐 Import 🔹 … More 👻		
Department Name(0)	Personnel ID First Na	me Last Name	Department Name	c ± Import Personnel	Create Time	Operations
Soluction(1)	. 1		Soluction	보 Import Biometric Template 보 Import Personnel Photo 보 Import Dismissions	2021-12-10 09:24:25	_ û
			(8 Download Personnel Import Template		
				Download Dismission Import Template		

Figure 2-21 Import Personnel Information Template

Step 3: Open the exported template file "Personnel Information Template.xls" for adding personnel information.

Step 4: In the personnel interface, select and click the "**Import** > **Import** Personnel Information" button; in the **Import Personnel** Interface, click the **Browse** button to import the batch import template into the system, as shown in Figure 2-22.

File Format	Excel	
Select File	Browse Not Uploaded	
The first line of the d	the firmers in factor where the second first is the	
	ata format is table name, the second line is he	ader, the third
	ata format is table name, the second line is ne a, please check the file and then import.	ader, the third
		ader, the third

Figure 2-22 Import Personnel

Step 5: Click **OK**, and the interface displays the result of personnel import and addition.

Step 6: Click Close to complete the import and addition of personnel information.

• Import Biometric Template

Preconditions:

- 1. The system needs to have the basic information files of the personnel in order to support the import of biometric template data.
- 2. The biometric template data of the current system personnel has been obtained.

Steps:

Step 1: In the Personnel module, choose "Personnel Management > Personnel".

Step 2: On the personnel interface, select and click the "**Import** > **Import Biometric Template Data**" button; in the pop-up import personnel biometric template data interface, click the **Browse** button to import personnel biometric template data into the system in batches, as shown in Figure 2-23 is shown.

	Import Personnel	
File Format	• Excel	
Select File	Browse Not Uploaded	
The first line of the o	lata format is table name, the second line is header, the	e third
line is the import dat	a, please check the file and then import.	

Figure 2-23 Importing Personnel Biometric Template Data

Step 3: Click OK, the interface displays the import and addition results.

Step 4: Click Close to complete the import of personnel biometrictemplate data.

Import Personnel Photos

Preconditions:

- 1. The system needs to have the basic information files of the personnel in order to support the import of personnel photos.
- 2. The personnel photos of the current system personnel have been obtained and correctly named according to the personnel number.
- 3. The photo requirements for personnel are as follows:

Image Format: support .jpg, .png format.

Image Size: The recommended image size is 35KB~200KB, and the maximum size of a single image is 5MB.

Image Quality: Faces in images are clear and not blurred by lens defocus or face motion. The minimum image depth is an 8-bit grayscale image.

Pixels: The recommended value of face pixels is 80*80~200*200, and the distance between the eyes should be greater than or equal to 60 pixels, preferably greater than or equal to 90 pixels.

Brightness and Contrast: The ambient illumination is not less than 300Lux, the image brightness is uniform, the contrast is moderate, and the face has no invisible, no backlight, no reflection, no overexposure, no underexposure and no yin and yang faces.

Attitude: The portrait is upright, looking straight ahead, the horizontal rotation angle of the face should be within $\pm 10^{\circ}$, the elevation angle should be within $\pm 10^{\circ}$, and the tilt angle should be within $\pm 10^{\circ}$.

Blocking: Eyebrows, eyes, mouth, nose and facial contours should not be blocked by bangs, masks, accessories, glasses, etc. The lenses of glasses should be colorless and non-reflective, and the frames of glasses should not be too thick to block human eyes.

Face Area: The face is complete, the outline and facial features are clear, and there is no heavy makeup. The face area of the image should not be processed by PS.

Expression: Natural expression, neutral or smiling (no missing teeth), eyes open naturally, mouth closed naturally, no obvious expressions such as laughter or frown.

Steps:

Step 1: In the Personnel module, choose "Personnel Management > Personnel".

Step 2: On the Personnel interface, select and click the "Import > Import Personnel Photo" button, as shown in Figure 2-24.



Figure 2-24 Import Personnel Photos

Step 3: Optional: upload photos and compressed packages.

Step 4: After selecting the photo method, click **OK** to enter the interface for importing personnel photos, select the photo and click **Start Uploading**.

Import Personnel Photo	×	
Please Select Photo Press Ctrl to make multiple selections		
Total: 0 (Please do not delete photo while uploading)		
A Please name the photo with personnel ID. The correct format is JPG/GIF/BMP/PNG.Make sure the photo name does not contain special characters. Do not choose more than 3000 pictures in a single import!		
Start Upload Add More Close		

Figure 2-25 Photos - Importing Personnel Photos

Step 5: After selecting the compression package method, click **OK** to enter the interface of importing personnel photos, click **Browse** to select the file and then click "**Start Uploading**".

Import Personnel Photo
Select File Browse Not Uploaded
Operation log
Start Upload Close

Figure 2- 26 Compressed Package - Importing Personnel Photos

Step 6: After the upload is complete, the interface displays the results of the imported personnel photos.

Step 7: Click **Close** to complete the import and addition of personnel photos.

```
2.1.1.6 More
```

• Statistics

Click **Personnel > Person > More**, then select **Statistics**.

	Statist	ics	×
Statistical Type		Current Total	
Male		4	
Female		1	
Person		22	
Fingerprint		0	
Near Infrared Fac	e .	0	
Finger Vein		0	
Palm Vein	V12.0	1	
Visible Face	V58.12	1	
Card		6	
Face Picture		3	

Figure 2-27 Statistics

View the number of Person, Male, Female, and the number of Fingerprints, Near Infrared Face, Finger

Vein, Palm Vein, Visible Face, Card, and Face Picture.

• Reset Self Login Password

Click **Personnel** > **Person** > **More**, then select **Reset Self Login Password.**

Pr	ompt
Are you want to perfo Password	rm the Reset Self Login d operation?

Figure 2-28 Statistics

2.1.2 Department

Click Personnel, then select 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 (New), Delete, Export and Import Department.

2.1.2.1 Add a Department (New)

Introduce the configuration Steps for manually adding a single department in ZKBioCVSecurity.

It is suitable for scenarios where a small number of departmental organizations are added. After most departmental organizations have been created, individual departments can be added individually.

Steps:

Step 1: In the Personnel module, choose "Personnel Management > Department".

Step 2: Click Add with the mouse, and the interface for adding a department will pop up.

Step 3: In the interface of adding a department, fill in the corresponding parameters according to the adding requirements, as shown in Figure2-29. Please refer to Table 2-10 for the description of parameter filling.

	New	
f the new department does n he administrator to re-author		
Department Number*	l	
Department Name*		
Sort*	99999	
Parent Department		•

Figure 2-29 Add Department (New)

Instructions	
Customize the department number, support letters and numbers.	
Customize the department name.	
Fill in the number of the superior department.	
The department name corresponding to the superior department number.	

Table 2- 10 Add Department

2.1.2.2 Delete

Click **Personnel > Department**, then select **Delete**.

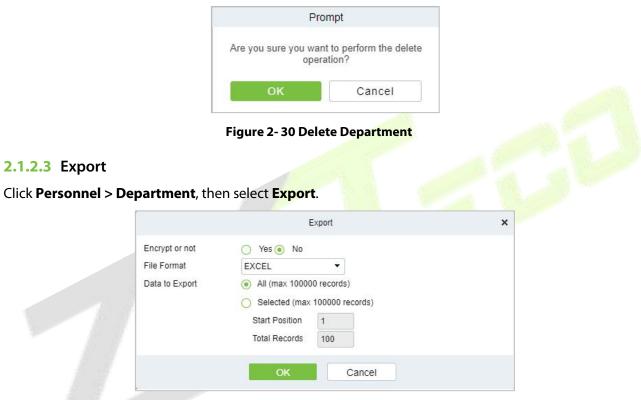


Figure 2-31 Export Department

2.1.2.4 Import

Import:

Click **Pesonnel > Department > Import**, then select **Import**.

File Format	Excel	
Select File	Browse Not Uploaded	
	data format is table name, the second line is header, the third	
The first line of the	data format is table name, the second line is header, the third ta, please check the file and then import.	

Figure 2-32 Import Department.

Download Import Template Department:

Click **Personnel > Department > Import**, then select **Download Import Template Department**.

	Download Department Import Te	implate >
File Format	EXCEL	

Figure 2-33 Download Import Template Department

2.1.3 Position

Introduces the configuration Steps of manually adding a job in ZKBioCVSecurity, and adding a job is used to define the job information of a person.

Click **Personnel**, then select **Position**.

2.1.3.1 Add Position

Steps:

Step 1: In the Personnel >Personnel Management > Position.

Step 2: Click New (Add Position), and the new job interface will pop up.

Step 3: On the new job interface, fill in the corresponding parameters according to the adding requirements, as shown in Figure 2-34; please refer to Table 2-11 for parameter filling instructions.

	New	
Position Number*		
Position Name*		
Sort*	99999	
Parent Position		•

Figure 2-34 Add Position (New)

Parameter	Instructions
Job number	Customize the job number for easy memory.
Job Title	Customize job title.
Sort	Sort job listings, only numbers are supported.
Parent position	Select the corresponding parent position from the drop-down radio box. If you need to cancel, click Selected again.

Table 2-11 Adding New Position

2.1.3.2 Delete

Click **Personnel > Position**, then click **Delete**.

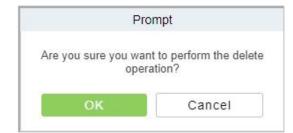


Figure 2-35 Delete Position

2.1.3.3 Export

Step 1: Click Personnel > Position, then select Export.

Encrypt or not	🚫 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	

Figure 2-36 Export Position

Step 2: Click OK to save to exit.

2.1.3.4 Import

Step 1: Click Personnel > Position > Import, then select Import.

	Import	
File Format	Excel	
Select File	Browse Not Uploaded	
	data format is table name, the second line is hea	ider, the third
	data format is table name, the second line is hea ata, please check the file and then import.	ider, the third
		ider, the third

Figure 2-37 Import Position.

Step 2: Click OK to save and exit.

2.1.4 Dismissed Personnel

This parameter will display the personnel who are not working in company anymore. Once the person is dismissed, it will be listed.

Click **Personnel**, then select **Dismissed Personnel**.

2.1.4.1 Delete

Step 1: Click Personnel > Dismissed Personnel, then select Delete.

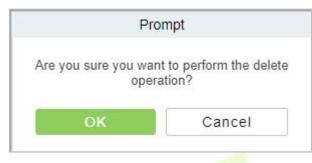


Figure 2-38 Delete

Step 2: Click OK to save and exit.

2.1.4.2 Export

Step 1: Click Personnel > Dismissed Personnel, then select Export.

		Export	×
	Encrypt or not	🔿 Yes 💿 No	
	File Format	EXCEL 🔻	
	Data to Export	 All (max 100000 records) 	
		O Selected (max 100000 records)	
		Start Position 1	
		Total Records 100	
1			
		OK Cancel	

Figure 2-39 Export

Step 2: Click OK to save and exit.

2.1.5 Pending Review

2.1.5.1 Delete

Step 1: Click Personnel > Pending Review, then select Delete.

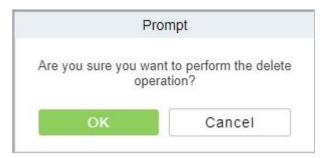


Figure 2-40 Delete Pending Review

Step 2: Click OK to save and exit.

2.1.6 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.

Click Personnel, then select Custom Attributes.

2.1.6.1 Add Custom Attributes (New)

Step 1: Click Personnel > Custom Attributes, then select New (Custom Attributes).

Display Name*		
Input Type*	Pull-down List 🔹	
Attribute Value *		
Using a '; ' delimiter.		
Row*	10	
Column*	1	
Display in Person List	○ Yes No	
	0	

Figure 2-41 Add Customer Attribute (New)

User Manual

Fields are as follows:

Parameter	Description	
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/Column	The column and row of a field are used together to control the display position of the field. Numerals are supported. The column number cannot exceed 99, and the row number can only be 1 or 2. 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.	

Table 2-12 Add Customer Attribute (New)

Step 2: Click OK to save and exit.

2.1.6.2 Delete

Step 1: Click Personnel > Custom Attributes, then select Delete.

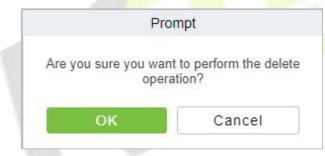


Figure 2-42 Delete Custom attributes

Step 2: Click OK to save and exit.

2.1.7 List Library

2.1.7.1 Add a List Library (New)

Step 1: Click Personnel > List Library, then select New (List Library).

List Library Name*	1		
List Library Type*		•	
Description	-		

Figure 2- 43 Add List Library (New)

Parameter	Description
List Library Name	Give a name for list library.
List Library Type	Select type of list library.
Description	Fill Decription as required.

Table 2-13 Add List Library

Step 2: Click OK to save and exit.

2.1.7.2 Delete

Step 1: Click Personnel > List Library, then select Delete.

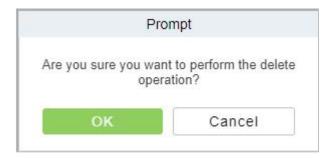


Figure 2-44 Delete List Library

Step 2: Click OK to save and exit.

2.1.8 Parameters

In Parameters you can do few settings for options like **Personnel ID Setting, Card setting, Pending Personnel Selling, Self-Service registration, and Registration Client.**

Click Personnel > Personnel Management, then select Parameters.

Personnel /	Personnel / Parameters		
	Personnel ID Setti	ng	Personnel ID Setting Card Setting
		The Maximum Length: 12 Support Letters: Yes No	Pending personnel settings Self-service Registration Registration Client
		Personnel ID Auto-Increment:	
	Card Setting		
«		The Maximum Length:	
4		32 Bits(Binary)	
		Card Format Display: O Decimal O Hexadecimal	
		Multiple Cards per Person:	
		○ Yes ● No	
		Card Reading Mode: Read By Controller	
	Pending personne	I settings	1
		Enable Auto-audit:	
		Yes O No No	
«	Self-service Regis	tration	
		Enable Self Registration:	
		Yes O No No	
		Enable the declaration of health information:	
		QR Code URL:	
		http://Server address-Port	
	Registration Clien	t	
		Device Driver	
		Certificate Recognition Driver Installation Status: Detected Certificate Recognition Driver is not installed	
*		Card Printer Driver Installation Status: Detected Card Printer Driver is not installed	
		Certificate Recognition	
		OCR OIDReader Registration Code*	
		Register	
		O Download OCR V1.0 Driver Download OCR V2.0 Driver	
		Certificate No. Automatic Backfill Type Document No. Personal No.	
		Card Printing	
		Registration Code"	
		Register Download Driver	
		ОК	

Figure 2-45 Parameters

2.1.8.1 Personnel ID Setting

The maximum length of ID should be of 12.

Support Letters: yes/No.

Personnel ID Auto-increment: Yes/No.

Personnel I	ID Setting	
	The Maximum Length:	
	12	
	Support Letters:	
	🚫 Yes 💿 No	
	Personnel ID Auto-increment:	
	Yes O No	



2.1.8.2 Card Setting

The maximum Length is of 32 characters.

Set Card Format display to Decimal or Hexadecimal.

Multiple Cards per Person: Yes/No.

Set Card Reading Mode as Read by controller.

Card Setting		
	The Maximum Length:	
	32	Bits(Binary
	Card Format Display:	
	Decimal	
	Multiple Cards per Person:	
	🔿 Yes 💿 No	
	Card Reading Mode:	
	Read By Controller	

Figure 2-47 Card Setting

2.1.8.3 Pending Personnel Selling

Enable Auto-audit option to Yes or No.

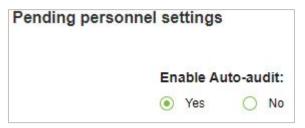


Figure 2-48 Pending Personnel Selling

2.1.8.4 Self Service Registration

Change option as Yes or No for Enable Self Registration and Enable the Declaration of health information.

Self-service	Registration	
	Enable Self Registration:	
	Yes O No	
	Enable the declaration of health information:	
	Yes O No	
	QR Code URL:	
	http://Server address:Port	

Figure 2-49 Self Service Registration

2.1.8.5 Registration Client

Fields	are as	foll	ows:
---------------	--------	------	------

Registration Clier	n la
	Device Driver
	Certificate Recognition Driver Installation Status: Detected Certificate Recognition Driver is not installed
	Card Printer Driver Installation Status: Detected Card Printer Driver is not installed
	Certificate Recognition
	OCR OIDReader
	Registration Code*
	Register
	O Download OCR V1.0 Driver
	Certificate No. Automatic Backfill Type
	Document No. Personal No.
	Card Printing
	Registration Code*
	· · · · · · · · · · · · · · · · · · ·
	Register
	Download Driver

Figure 2-50 Registration Client

Click **Ok** to save and exit.

∕≤Note:

- 1. 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 one by one, the ID in field automatically updates to the next new number.
- 2. Set the maximum length (binary number) of the card number that the current system will support.
- 3. Set whether the personnel ID for the demission employee can be kept.

- 4. Set whether the temporary personnel uploaded and registered by scanning the QR code of the big-screen facial recognition time and attendance device need to review.
- 5. Set the card format currently used in the system. The card format cannot be switched once it is set up.
- 6. Set whether "Multiple Cards per Person" will be allowed or not.
- 7. Used the QR code to Self-Registration.
- 8. Registration Client.
- 9. If no driver has been installed, the Download Driver link is displayed. Click the link to download and install the driver.

2.2 Card Management

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

🥃 Card Management 🗸 🗸	Card Number	Personnel ID	Department Nam	e	More - Q 🖉	
Card	🔾 Refresh 🛛 🖓 Bati	ch Issue Card 🗔 Reported I	Lost Card 🛛 🛱 Reactivate Lost Card	↑ Export		
Wiegand Format	Card Number	Personnel ID First Name	Last Name Department Number	Department Name	Issue Card Date	Card State
Issued Card Record	1139274691	9527	1	Department Name	2022-07-26 02:38:20	Effective
	123123232	1 tang	OP1 1	Department Name	2022-07-26 02:38:20	Effective
	145632	1111 Esha Test	2	Development	2022-05-10 08:27:37	Effective
	123456	1114 Md. Jalai	2	Development	2022-05-10 08:10:52	Effective

Figure 2-51 Card Management

2.2.1 Card

2.2.1.1 Batch Issue Card

Click **Personnel > Card Management > Card**, then click **Batch Isuue Card**.

				Batch Iss	ue Card				
Department Name			Start Personnel ID		End Pers	sonnel ID	C	2	
Card Enrollment N	lethod USB Reader	r 🔹	Input Card Number		Issue Car	<u>d</u>			
nissued person				<	Current issue per	son			;
Personnel ID	First Name	Last Name	Depa	rtment N	Personnel ID	First Name	Last Name	Department N	Ca
10002	raj	h	hr	-					
10001			Depa	rtment N					
666	chen		Depa	rtment N					
2	tsf		Depa	rtment N					
9999	K-TEST		Depa	rtment N			No data		
12135			Depa	rtment N 🖕					
<				•					
< < 1-16	> > 50) rows per pag	e 👻 Total of 16	records	4				Þ

Figure 2-52 Batch Issue card

Fill the fields for Department Name, Start Personnel ID, End Personnel ID, Card Enrollment Method, and Input Card Number.

Enter Start and End Personnel No. and click **Generate List** to generate personnel list and show all personnel without cards within this number series.

Note: The Start and End Personnel No. only support numbers.

Select Card Enrollment Method: Register with a USB Reader or device.

If you want to enroll a card with a USB Reader, you may place the card over the "issue machine" directly. The System will get the card number and issue it to the user in the list on the left.

For the use of device, you need to select the position of punching, click Start to read, the system will read the card number automatically, and issue it to the user in the list on the left one by one. After that, click Stop to read.

Note: During the "Batch Issue Card", system will check whether the card issuer issues 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 exit.

2.2.1.2 Reported Lost Card:

Click Personnel > Card Management > Card, then select Reported Lost Card.

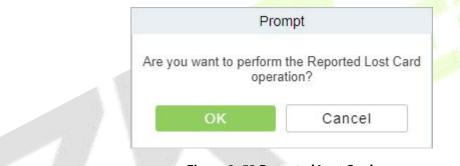


Figure 2-53 Reported Lost Card

Note: Report Lost Card is applicable to all functional modules, not to the offline elevator module. After the report of loss, the status of the card becomes invalid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **Write management card** (**Elevator Device** > **Card** > **Write management card**).

2.2.1.3 Reactive Lost Card

Click Personnel > Card Management > Card, then select Reactive Lost Card.

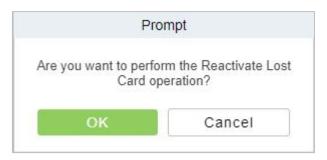


Figure 2-54 Reactive Lost Card

Note: Reactivate Lost Card is applicable to all functional modules, not to the offline elevator module. After reactivating lost card, the status of the card becomes valid but not written into the management card. Need to write management card in the appropriate module, such as offline elevator control module **Write management card** (**Elevator Device** > **Card** > **Write management card**).

2.2.1.4 Export

Step 1: Click Personnel > Personnel Management > Card Management > Card, then select Export.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
	OK Cancel	
	Figure 2- 55 Export	

Step 2: Click OK to save and exit.

2.2.2 Weigand 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.

Click **Personnel > Personnel Management > Card Management**, then select **Weigand Format**.

2.2.2.1 Add weigand Format (New)

Click **Personnel** > **Personnel Management** > **Card Management** > **Weigand format**, then select **New** (Add Weigand format).

					New				
Name*	ſ	l.							
Total Bit*	(
Site Code		0							
Auto									
Mode (Dne								
First Parity	Check(p)								
Second Par	rity Check(p)								
Odd F	Parity Check(o)	Even I	Parity Check(e)		CID(c)	S	ite Code(s)	Manufa	acturer 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
) Mode 1	Гwo								
Card Che	ck Format*								
Parity Che	eck Format [*]								
			Save and N	lew	ОК	Cancel			
						2			

Figure 2- 56 Add Weigand format (New)

Fields are as follows:

Parameter	Instructions
Name	Enter the Name.
Total Bit	Enter the total bit.
Site Code	Enter the Site code.
Auto	Click if Auto is required.
Mode One	In Mode One Odd Parity Check, Even Parity Check, CID, Site Code, and Manufacturer Code should be set as Start Bit and The Maximum Length.
Mode Two	In Mode Two Card Check format and Parity check Format must be entered.

Table 2-14 Weigand Format

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

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.

2.2.2.2 Delete

Click **Personnel > Personnel Management > Card Management > Weigand Format**, then select **Delete.**

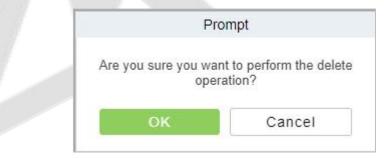


Figure 2-57 Delete Weigand Format

2.2.2.3 Card Formats Testing

Click **Personnel > Personnel Management > Card Management > Weigand Format**, then select **Card format Testing**.

			Card Formats Testing	×
Device * Clie	ck to select	Read Card	Clear Card Information	
 Card 1 Card 2 Card 3 	Site Code	Card Number*	Original Card Number	
-	ended Card F s	ead a new card, please manual format Auto calculate s	Ily switch to the next card. ite code while the site code is left blank	
<			OK Cancel	•

Figure 2-58 Card Formats Testing

When the card number does not match with the one which is displayed on the system, the user can use the **Card Formats Testing function** to calibrate the Wiegand format. The page is explained as follows:

Select the device that supports the card format test function, and fill the card number and the site code (optional):

Steps:

Click **Read Card** and swipe the card on the reader. The original card number will be displayed on the **Original Card Number** text box.

Click **Recommended Card Format** and the recommended Wiegand card format will be displayed below.

Click **Auto calculate site code while the site code is left bank** and the software will calculate the site code according to the card format and card number.

Click **OK** and the page will jump to the Wiegand format page to save the new Wiegand format.

Note: The card format testing function is only supported by few devices.

2.2.3 Issue Card Record

Click **Personnel > Personnel Management > Card Management,** then select **Issue Card Record.**

2.2.3.1 Export

Step 1: Click Personnel > Personnel Management > Card Management > Issue Card Record, then select Export.

	Ex	port	×
Encrypt or not	🚫 Yes 💿 No		
File Format	EXCEL		
Data to Export	All (max 100000)	records)	
	O Selected (max 1	00000 records)	
	Start Position	1	
	Total Records	100	
			1
	OK	Cancel	
	132 - 57		

Figure 2- 59 Issue Card Record

Step 2: Click OK to save and exit.

3 Access Control

3.1 Operation Scenario

The **Access Control** module is used as the entry and exit management of pedestrians. Through the configuration of access control equipment and permission groups, unified management of entry and exit of people is realized. The most fundamental problem to solve is to control who uses what media to enter and exit which door at what time.

3.2 Operation Process

This section describes the configuration process of the **Access Control** module service.

The Access Control module service configuration process is shown in Figure 3-1.

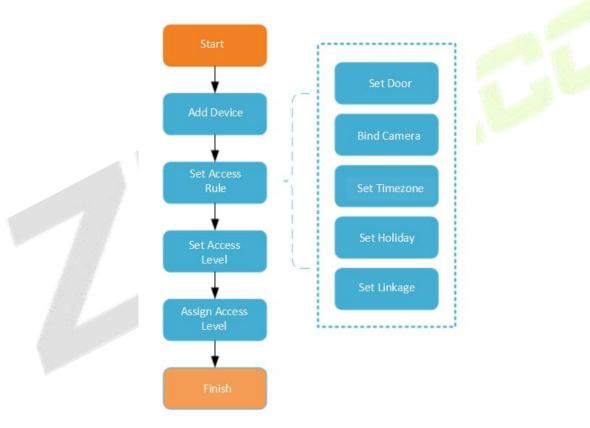


Figure 3-1 Access Control Configuration Process

3.3 Access Device

3.3.1 Device

Introduce the configuration Steps of searching and adding access control devices in ZKBioCVSecurity.

Through the search method, the access control devices that have been set to point to the server can be found, and the access control devices that have been searched can be added directly, which is convenient to operate.

Preconditions:

- 1. Before adding the Access Control device, perform IP allocation settings.
- 2. The device needs to set the server address in advance before searching and adding. The configuration Steps for the server are as follows:

a. In the access control device that has been connected to the power supply and the network, set it directly on the device screen.

b. Select and click "Main Menu > Communication Equipment > Network Management Platform or Cloud Server Settings"

c. Set the IP address and port of the current server, that is, the IP address and port of the current ZKBioCVSecurity server and complete the configuration to the server.

3.3.1.1 Add devices (New)

Steps:

Step 1: In the Access Control module, select "Device > Access Control Device".

Step 2: On the device interface, click the "search" button to pop up a search box.

Step 3: Click "start **Search**" in the search box to display the **access control devices** that can be added, as shown in Figure 3-2.

		Search		×
Search No de	vice found? Download Search Tools to	Local Disk		
Total Progress	100%	Searched devices count:1 Number of devices added:1		
IP Address	Device Type	Serial Number	\otimes	
IP Address	MAC Address Subnet Mask	Gateway Add Serial Number	Device Type Set Server	Operations
192.168.134.168	255.255.255.0	192.168.134.254 CN3M212460001	TDB08M-TI/M	This device has bee
A The current system of	communication port is 8088, please make s	ure the device is set correctly.		
		Close		

Figure 3- 2 Device Search and Add Interface

Step 4: Optional: Modify the IP address of the **Access Control** device, click "**Modify IP Address**", the device will be restarted after modifying the IP address, and the IP address modification will be completed after the restart.

Step 5: For the searched access control devices, click the **Add** button in the operation bar to add the device; the device addition settings are shown in Figure 3-3, and the parameter settings are described in Table 3-3.

	New	×
Device Name*		
Communication Type*	• TCP/IP O RS485	
IP Address*		
Communication port*	4370	
Communication Password		
Icon Type*	Door •	
Control Panel Type	One-Door Access C 🔻	
Area*	Area Name 🔹	
Add to Level		
Clear Data in the Device when		
Adding		
[Clear Data in the Device v (except event record), plea	when Adding] will delete data in thase use with caution!	ne device
(
ок	Cancel	

Figure 3-3 Device Add Interface

Parameter	How to set
Device Name	Customize the name of the device.
New Server Address/Port	Set the IP address and communication port of the system to be used (the default communication port is 8088).
Communication Password	Fill in the communication password of the device. If there is no password, you do not need to fill in it. You can add it only after the verification is successful. For new factory equipment and initialized equipment, the communication password is empty. In order to ensure that the device is not used by others, users can enter the device IP address through the web page to enter the background to customize the device verification password.
lcon Type	Select the icon display type of the real-time monitoring interface: door, channel.
Area	Divide the device into regions and select the region to which the device belongs.
Add To Permission Group	The device is automatically added to the selected permission group.
Delete Data From Device When Adding	Set whether the original Access Control data in the device will be automatically cleared after the device is added.

Table 3-1 Parameter setting

Step 6: Click OK to complete the operation of adding access control devices. After the operation is

completed, the device will restart, and the device will be added after the restart is complete.

Step 7: Click Close to close the device search and add interface.

3.3.1.2 Delete

Select device, click **Delete**, and click **OK** to delete the device.

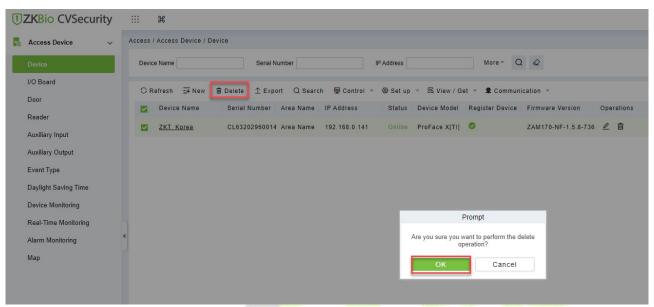


Figure 3-4 Device Add Interface

3.3.1.3 Export

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

The File Type	EXCEL File	~			
Export Mode	All data (Can expo All data (Can expo	ort up to	o 40000 data)		
	O Select the amount	of data	a to export (Can ex	xport up	to 40000 dat
	From the article 1		Strip, is derived	100	Data

Figure 3-5 Export

					ZKTECO					
					Device					
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.303 Jun 16 2017

Figure 3-6 Export

3.3.1.4 Control

Clear Administration Permission

Administration has permission to clear the administration permission from device.

• Upgrade Firmware

Tick the device that needs to be upgraded, click Upgrade firmware to enter edit interface, then click

Browse to select firmware upgrade file (named emfw.cfg) provided by Access software, and click **OK** to start upgrading.

✓ 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.

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.

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.

	Sync	hronize All Data to Devices		×
Selected Device Standalone Dev	rice : ZKT_Korea			
Unselect All Total Progress	 Access Authority AntiPassback Linkage Verification Mode Rule 	 TimeZone, holidays First-Person Open Door Bg-Verification Options 	 Door Parameters Multi-Person Open Doo Auxiliary Input Setting 	r
Hidden Info			Synchronize	Close
				*

Figure 3-7 Synchronize All Data to Devices

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.

3.3.1.5 Set Up

• Set Background Verification Parameters:

Select the required online device; click **More** > **Set Bg verification parameters**.

ected Device The devices which have disable	d background verification : ZKT_Korea	
	a background vernication . 2KT_Kolea	
Set Bg-Verification Options		
	(Second and Second	
Background Verification	Disable	
If the device is offline	Standard Access Level 💌	
tal Progress		
an rogicoo		
Hidden Info	Start	Close
		-

Figure 3-8 Set Bg-Verification Parameters

Background verification: Enable or Disable Background verification function.

If the device is offline: If the controller is offline, the device has levels of Standard Access Level or Access Denied.

After setting parameters, click **Start** button to issue command to the device setting.

Solution Note: If you need advanced access control functions, please enable Background verification, and issue the background verification parameters to the device.

• Set the Registration device

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



Figure 3-9 Set the Registration device

• 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.

• **Modify the Fingerprint Identification Threshold** (Ensure that the access controller supports fingerprint function)

Modify the Hingerpr	int Identification Threshold	
The fingerprint identification	55 (35-70)	
threshold"		
OK	Cancel	

Figure 3-10 Modify the Fingerprint Identification Threshold

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.

Set Device In/Out Status: We can set the status of device In/Out

Set Extended Parameters: We can set the extended parameters of device like temperature detection and mask detection

Set Video Intercom Server: We can set the video intercom server of device

3.3.1.6 View/ Get

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.

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.

Solution 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	Rules Details	
nterlock	Not Set	None	
inkage	Not Set		
Anti-Passback	Not Set		
irst-Person Normally Open	Not Set		
/lulti-Person Opening Door	Not Set		
Door Sensor	Not Set		
Active Time Zone	Has been set		
assage Mode Time Zone	Not Set		
Background Verification	Not opened	Between multiple rules with	
Blobal Anti-Passback	Not opened	a 'l' separated.	
Blobal Interlock	Not opened	▲ Linkage and global	
Blobal Linkage	Not opened	linkage, anti-passback and	
Person Availability	Not opened	global anti-passback are set	
Occupancy Control	Not opened	at the same time, there may	
		be conflicts.	

Figure 3-11 View rules of device

View Device Capacity

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

				View D	Device Capacity			×
ß	<i>P</i> at	×	<i>\$</i>	盘	⊕	*	[c]	Get All
ZKT_Korea								Get
🛕 If you find	that the data	is not consister	it with the device, pl	ease synchronize the data of	devices before trying agai	in.		
				1	Close			

Figure 3-12 View device capacity

3.3.1.7 Communication

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: Communication password shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password setting can improve the device's 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.

Switch Network Connection

Search WIFI
Wireless SSID* TP-LINK_6D9C_xinxiao
Wireless Key*

Figure 3-13 Switch network connection

This function is applicable to InBio5 series access control panels, which is used to switch among different network connection modes of the control panel.

3.3.1.8 Device Replacement

Introduce the configuration Steps for replacing access control devices in ZKBioCVSecurity.

When a device is unavailable, we can quickly add a new device and synchronize all configurations from faulty device to the new device by simply entering the serial number of the replaced device.

Step 1: Go to the Access > Access Device, select the unavailable device.



Figure 3-14 Select the Unavailable Device

Step2: Click Set up > Replace Device.

ZKBio CVSecurity	··· 8	\rm e admin 👻
Access Device 🗸 🗸	Access / Access Device / Device	
Device	Device Name IP Address More * Q 🖉	
I/O Board Door	C Refresh ∓ New @ Delete ↑ Export Q Search ♥ Control ▼	
Reader		
Auxiliary Input	<u>10.8.14.206</u> COKC220266004 Area 1 10.8.14.206 Co Set Device Time Zone ZAM180-NF550VA-Ver3 2 10 Co Set Device Time Zone ZAM180-NF550VA-Ver3 2 10 Co Set Device Time Zone ZAM180-NF550VA-Ver3 2 10	
Auxiliary Output	₩ Modify the Fingerprint Identification Threshold	
Event Type	I Set Device In/Out Status	
Daylight Saving Time	Set Extended Parameters	
Device Monitoring	I Set Video Intercom Server	
Real-Time Monitoring	B Replace Device	
Alarm Monitoring		
Мар		
Access Rule		
) Advanced Functions >		
Access Control Reports	< < 1-1 > > 50 rows per page ▼ Jump To 1 /1 Page Total of 1 records	

Figure 3-15 Replace Device

Step 3: Enter the serial number of the new device, then click OK.

Replace Device	×	
Serial Number*]	
 Please make sure the replacement device model i After the replacement, please perform the "sync a operation; 		
OK Cancel		

Figure 3-16 Input the Serial Number

Step 4: Select the new device, then click **Control > Enable**.

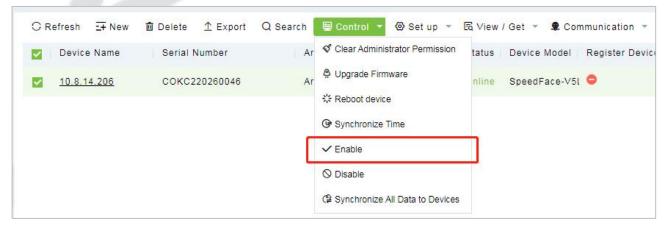


Figure 3-17 Enable Device

Step 5: Select the new device, then click **Control** > **Synchronize All Data to Device**.

	Sync	hronize All Data to Devices		
Selected Device Standalone Devi	ce : 10.8.14.206			
Unselect All	 Access Authority AntiPassback Linkage Verification Mode Rule 	 TimeZone, holidays First-Person Open Door Bg-Verification Options 	 Door Parameters Multi-Person Open Doo Auxiliary Input Setting 	or
Total Progress				
Hidden Info			Synchronize	Close

Figure 3-18 Synchronize Device Data

∕≤Note:

- 1. Before replacement, the device needs to configure the server address and IP allocation.
- 2. Make sure that the replacement device model is the same.
- 3. After the replacement, please perform the "sync all data" operation.

3.3.2 Door

The setting of door parameters affects the logic judgment of access control verification. The door parameters support different parameter settings according to the different firmware of the device. The following describes the configuration Steps of the door parameters with one of the devices.

Operation Step:

Step 1: In the Access Control module, select "Devices > Door".

Step 2: In the management interface of the door, click the **Edit** button in the door operation bar to pop up the door parameter setting box.

Step 3: In the door parameter setting interface, fill in the corresponding parameters according to the addition requirements, as shown in Figure 3-4, please refer to Table 3-2 for parameter filling instructions.

		Ed	it		
Device Name*	ZKT_Korea		Door Number*	1	
Door Name*	ZKT_Korea-1]	Active Time Zone*	24-Hour Accessible	-
Verification Mode*	Automatic Identification 👻]	Lock Open Duration*	5	second(1-
				254)	
Operate Interval*	0	second(0-254)	Door Sensor Type*	None	•
Anti-Passback Duration of	0	minute(0-120)	Door Sensor Delay		second(1-
Entrance				254)	
Duress Password		(Maximum 6 Bit	Passage Mode Time Zone		s. - .
	Integer)				
Emergency Password		(8 Bit Integer)	Multi-Person Operation	10	second(5-60)
Disable Alarm Sounds			Interval*		
	The above settings a	e copied to		•	
		OK	Cancel		

Figure 3-19 Setting Door Parameters

Instructions:

The firmware of different access control devices supports different door parameters. Set the parameters based on the actual door parameter page. Table 3-4 describes the parameter set for different devices.

Parameter	Setup Instructions
Device Name/Door Number	The basic information about the door is displayed. Reset is not supported.
Name of the Door	Customize the name of the door for easy memory.
Gate Validity Period	Select a period when the gate is valid. Not within the validity period of this door, even if the person has the permission of this door, can not open the door inside.
Verify The Way	Set this parameter to the authentication mode supported by the device.
Lock Drive Duration	Set the time range for unlocking a lock after authentication. For example, if the value is set to 5 seconds, the door can be opened within 5 seconds after the verification. If the door is not opened after 5 seconds, the door will be automatically locked, and the door can be opened only after the verification.
Weiganka Format	Select a Weigand card format that can be recognized by the door's Weigand reader. The card format and Settings are different, will not open the door. There are 9 built-in formats in the software, the default is automatic matching wiegand card format, automatic matching can identify a variety of built-in wiegand card format.
Exit Button State	Set the status of the door exit button, locked, not locked. Lock: the door lock does not open after pressing the exit button. Not locked: the door lock is opened after pressing the exit button.
The Exit Button Is	When the exit button is set to lock, set the delay time of the exit button, that is,

Parameter	Setup Instructions
Delayed	the delay time of the inspection door alarm after the exit button is locked.
Operation Interval	Set the interval for Access Control Operation.
Effective Time of Exit Button	Select the time period for setting the exit button.
Magnetic Door Type	Option No, normally open, normally closed, default none.
Behind Closed Doors to Lock	Set whether to lock back after the door is closed.
Magnetic Door Delay	Set the delay for checking the door status sensor after the door is opened. When the door is not "normally open", if it is open, it will start timing, alarm will start after the door magnetic delay time, and alarm will be cancelled when the door is closed.
Duration Of Anti- Passback Entry	Set a limit on how long an intelligent entry can take.
Stress The Password	Set up the user to open the door when the threat password. An alarm will be generated when the coerced code opens the door.
Emergency Code	Set a password for the user to use in an emergency. The password is used by the administrator and is valid in any period and authentication mode.
The Door Is Normally Open	Select the time when this door is normally open.
Extended Time of Passage	Set on the basis of the original <mark>open</mark> ing tim <mark>e, additio</mark> nal limit time. Common terms for participants, inconvenie <mark>nt per</mark> sonnel to extend the passage time.
Open Time Delay	Set the time for waiting for the del <mark>ayed</mark> door opening after authentication.
Disable Alarm Reminder	If alarm event occurs on this door, whether there will be alarm sound reminder on the real-time monitoring interface.
Allow Superuser Access When the Door Is Locked	Set whether the super user can verify access when the door is locked.
The Above Settings Are Copied To	To set the door parameters above, the options are all doors of the current device, all doors of all devices.

Table 3-2 Door Parameters

Step 4: Click OK to complete the setting of the door parameters

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 (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**.

EXNOTE: 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 is displayed on 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.

Solution 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.

Activate Lockdown: It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

Deactivate Lockdown: It will unlock a locked door. This function is supported only by certain devices.

3.3.3 Reader

This section describes the Step configuration of the Reader binding camera in ZKBio CVSecurity.

Operation Scenario:

After the camera is bound, if related Settings are set during linkage, the Reader will perform video linkage (capture) once corresponding events occur. The Reader bind cameras in the same way. This section uses the Reader as an example to describe how to bind cameras.

The Premise Conditions:

A video camera has been added in the **Video Management** module.

Operation Step:

Step 1: In the access Control module, choose "Device > Reader".

Step 2: In the Operation column of the corresponding Reader, click Bind/Unbind camera. The bind/unbind camera page is displayed.

Step 3: On the Select Reader screen, set the Reader as required, as shown in Figure.

Binding/unb	inding the camera	>
Channel Name Serial Number	Q &	
Alternative	Selected(0)	
Channel Name Owned Device Serial Number	Channel Name Owned Device Serial Number	
☐ 192.168.134.59 AS1700 21024127099SL8	>> <	
< < 1-1 > > 50 rows per page ▼ OK	No data	

Figure 3- 20 Binding A Camera

Step 4: Click **OK** to bind the camera.

Parameter	How to set
Device Name	Customize the name of the device.
Reader Name	Display the reader's name of the device
Communication Type	Wiegand/RS485, Wiegand, RS485, and Disabled are available. When a communication type is selected, the reader interface on the device will receive data (including card and fingerprint data) for the specified type only
In/Out	Display the in/out of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.

Table 3- 3 Reader Parameters

3.3.4 Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

Operation Step:

Step 1: Click Access Device > Auxiliary Input on the Action Menu, to access below shown interface.

TKBio CVSecurity	::: ж			
🔚 Access Device 🗸 🗸	Access / Access Device / Auxiliary Input			
Device	Name Device	Name Printed Name	Q @	
I/O Board Door	O Refresh			
Reader Auxiliary Input	Name Device Name Auxiliary Input-1 ZKT_Korea	Number Printed Name Bound camera	Owning Board Remarks	Operations
Auxiliary Output		Edit ×		
Event Type Daylight Saving Time	Device Name* Number*	ZKT_Korea		
Device Monitoring	Name* Printed Name*	Auxiliary Input-1		
Real-Time Monitoring Alarm Monitoring	Active Time Zone Remarks	24-Hour Accessible		
Мар				
	ОК	Cancel		

Figure 3-21 Auxiliary input

Step 3: Click OK to save the name and remark and exit.

Bind/Unbind Camera:

Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos or screenshots) once there is a corresponding event occurs. For this, the interaction setting in Linkage or in Global Linkage should be done before. For details, please refer to Reader: Bind/Unbind Camera.

SNote: An auxiliary input point can bind more than one channel.

Parameter	How to set
Device Name	Customize the name of the device.
Name	Display the name of the device
Number	Customize the name of the device
Printed Name	Display the input number of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.
	Table 3- 4 Auxiliary Input Parameters

3.3.5 Auxiliary Output

It is mainly related to alarm and is used when linkage is working.

Operation Step:

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

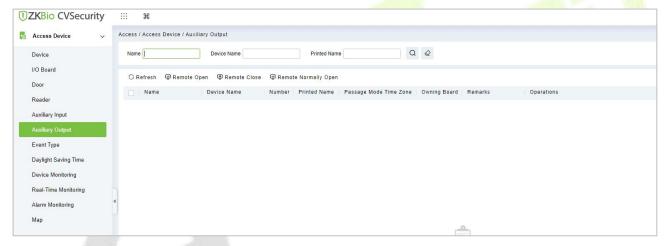


Figure 3-22 Auxiliary Output

Step 2: Click Edit to modify the parameters.

Device Name*	192.168.12.155	
Number*	1	
Name*	Auxiliary Output-1	
Printed Name*	OUT1	
나군 Passage Mode Time Zone		•
Remark		

Figure 3-23 Auxiliary Output Edit

Step 3: Click OK to save the name and remark and exit.

3.3.5.1 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.

3.3.5.2 Remote Normally Open

It will set the device as normal open by remote.

Parameter	How to set
Device Name	Customize the name of the device.
Name	Display the name of the device
Number	Customize the name of the device
Printed Name	Display the input number of the device.
Bound Camera	connecting the camera with the reader.
Owning Camera	The device is automatically added to the selected permission group.
	Table 3- 5 Remote Normally Open Parameter

3.3.6 Event Type

It will display the event types of the access devices.

Operation Step:

Step 1: Click **Access Device** > **Event** to access the following page:

Access Device 🗸 🗸	Access	/ Access Device / Event Type					
Device	Event	Name 🔹	Event Number		Event Level	▼ More ▼	Q @
I/O Board	OR	efresh 🕼 Set Audio					
Door		Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Reader		Normal Verify Open	0	Normal	ZKT_Korea	CL63202960014	<u>@</u>
Auxiliary Input Auxiliary Output		<u>Verify During Passage Mode T</u>	1	Normal	ZKT_Korea	CL63202960014	2
Event Type		First-Personnel Open	2	Normal	ZKT_Korea	CL63202960014	<u></u>
Daylight Saving Time		<u>Multi-Personnel Open</u>	3	Normal	ZKT_Korea	CL63202960014	2
Device Monitoring		Emergency Password Open	4	Normal	ZKT_Korea	CL63202960014	0
Real-Time Monitoring		<u>Open during Passage Mode Ti</u>	5	Normal	ZKT_Korea	CL63202960014	2
Alarm Monitoring	«	Linkage Event Triggered	6	Normal	ZKT_Korea	CL63202960014	0
Мар		Cancel Alarm	7	Normal	ZKT Korea	CL63202960014	0

Figure 3-24 Event Type

Step 2: Click Edit or click the event type name to edit.

Device Name*	192.168.12.145 🔻	
Event Number*	1	
Event Level*	Normal 🔻	
Event Name*	Verify During Passage Mod	
Event Sound	Already Exists Oupload	
		Play
Copy the above settings to all devices		

Figure 3-25 Event Type Edit

3.3.6.1 Set Audio

Same as the event sound. Click Set Audio:

JZKBio CVSecurity	/ ::: ¥					
Access Device	, Access / Access Device / Ever	t Type				
Device	Event Name	Event Number		Event Level	▼ More ▼	Q @
I/O Board Door	🔾 Refresh 🗖 Set Audio]				
Reader	Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Auxiliary Input	Verify During Passar	0 Ne Mode T. 1	Normal	ZKT_Korea	CL63202960014 CL63202960014	<u>_</u>
Auxiliary Output		Set Audio		Korea	CL63202960014	2
Event Type Daylight Saving Time	Event Sound	 Already Exists O Upload 	Play	_Korea	CL63202960014	_
Device Monitoring				_Korea	CL63202960014	2
Real-Time Monitoring	he	OK Cancel		_Korea	CL63202960014	2
Alarm Monitoring			Hormon	Korea	CL63202960014	2
Мар	Cancel Alarm	7	Normal	ZKT Korea	CL63202960014	0

Figure 3-26 Event Type Set Audio

You can upload an audio from your local PC. The file must be in wav or mp3 format, and it must not exceed 10MB.

Parameter	How to Set
Event Level	Normal, Exception, and Alarm are available
Event Name	Display the name of the device and it can't be modified.
Device Name:	Display the name of the device
Event Number	Display the event number of the device.
Serial Number	Display the serial number of the device
<u></u>	Table 3- 6 Event Parameters

3.3.7 Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. 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 forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

3.3.7.1 Add DST (New)

ZKBio CVSecurity	::: ¥		
Access Device 🗸 🗸	Access / Access Device / Day	light Saving Time	
Device	⊖ Refresh 🔤 New 🛍	Delete	
I/O Board	DST Name	Start Time End Time	TimeZone Operations
Door	🗌 Alaska	MAR Second Sunday 20'clock NOV First Sunday 20'clock	k UTC-09
Reader	Amsterdam, Berlin,	E MAR Fifth Sunday 20'clock OCT Fifth Sunday 30'clock	k UTC+01
Auxiliary Input	🗌 Belgrade, Bratislava	a, MAR Fifth Sunday 20'clock OCT Fifth Sunday 30'clock	k UTC+01
Auxiliary Output		New	x JTC+01
Event Type	DST Name*	146W	JTC+01
Daylight Saving Time	TimeZone*		JTC+01
Device Monitoring	Start Time*	MAR	
Real-Time Monitoring	End Time*	NOV First Sunday O'clock	JTC-07
Alarm Monitoring	« 🗌		JTC-07
Мар	S	Save and New OK Cancel	JTC+12

Step 1: Click Access Device > Daylight Saving Time > New.

Figure 3-27 Daylight Saving Mode

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as "second Monday in March, 02:00". The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Parameter	How to set
DST Name	Display the DST name
Start Time	Display the start time of the device
End Time	Display the end time of the device
Time Zone	Display the timezone of the device.

Table 3-7 Daylight Saving Mode Parameters

3.3.7.2 Delete

Select device, click **Delete**, and click **OK** to delete the device.

Access Device v	Access / Access Device / Dayl	ight Saving Time		
Device	🔾 Refresh 🛛 🖅 New 💼	Delete		
I/O Board	DST Name	Start Time	End Time	TimeZone Operations
Door	🗹 Alaska	MAR Second Sunday 20'clock	NOV First Sunday 20'cloc	ck UTC-09
Reader	🗌 Amsterdam, Berlin, E	MAR Fifth Sunday 20'clock	OCT Fifth Sunday 3o'cloc	k UTC+01
Auxiliary Input	🗌 Belgrade, Bratislava	MAR Fifth Sunday 20'clock	OCT Fifth Sunday 30'cloc	k UTC+01
Auxiliary Output	Brussels, Copenhage	MAR Fifth Sunday 20'clock	OCT Fifth Sunday 3o'cloc	:k UTC+01
Event Type	Casablanca	MAY Third Sunday 2o'clock	APR Second Sunday 3o'c	lock UTC+01
Daylight Saving Time	Sarajevo, Skopje, W	MAR Fifth Sunday 20'clock	OCT Fifth Sunday 3o'cloc	k UTC+01
Device Monitoring	Mountain time (USA	MAR Second Sunday 20'clock	NOV First Sunday 20'c	Prompt
Real-Time Monitoring Alarm Monitoring	« 🗌 Chihuahua, La Paz,	APR First Sunday 20'clock	OCT Fifth Sunday 20'c	Are you sure you want to perform the delete
Map	Petropavlovsk Kamc	MAR Fifth Sunday 20'clock	OCT Fifth Sunday 3o'c	operation?
	Norfolk Island	OCT First Sunday 20'clock	APR First Sunday 3o'c	OK Cancel

Figure 3- 28 Daylight Saving Mode Delete

3.3.8 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.

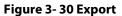
JZKBio CVSecurity	
🖷 Access Device 🗸 🗸	Access / Access Device / Device Monitoring
Device	Area 🔻 Status Vervice Name Serial Number
I/O Board	⊥ Export 💼 Clear All Command
Door	Device Name Serial Number Area Operation Status Current Status Commands List Recently Abnormal State Operation
Reader	
Auxiliary Input	
Auxiliary Output	
Event Type	
Daylight Saving Time	
Real-Time Monitoring	
Alarm Monitoring	۹.
Map	

Figure 3-29 Device monitoring

3.3.8.1 Export

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

The File Type	EXCEL File	~			
Export Mode	 All data (Can export up to 40000 data) 				
	O Select the amou	nt of data	to export (Can ex	port up	to 40000 data)
	From the article	1	Strip, is derived	100	Data



			ZKTECO			
			Device Monitoring			
Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State
192.168.218.60	20100501999	Area Name	Get real-time event	Normal	0	None

Figure 3- 31 Device monitoring Export

3.3.8.2 Clear All Command

You may clear the command as needed. Click **Clear Command** in operations column.

Pro	ompt
Are you sure to clea	ar command queues?
ок	Cancel

Figure 3-32 Device monitoring Clear command

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 capacity is insufficient, 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.

Operate State is the content of communications equipment of current device, mainly used for debugging.

The number of commands to be performed is greater than 0, indicating that the data is not yet synchronized to the device, so wait for the synchronization to complete.

3.3.9 Real-Time Monitoring

On the real-time management screen, the status of the added device is displayed and the device can be opened or closed. At the same time, the dynamic of real-time events is monitored. If the door opening can be verified and corresponding access control events can be generated, the access control management service configuration is complete.

Operation Step:

Step 1: Check whether the device is online.

In the Access Control module, choose "Access Control Device > Real-time Monitoring".

Check whether the icon status of the added device is online. For details about the icon status, see Table 3-8.

lcon	State	lcon	State					
	The device is disabled.	_ *	Door offline status					
۲, ۲	No door status sensor, relay off/no relay status		Door status sensor not set, relay open/no relay state					
, 2	The door is closed and the relay is off/no relay is in online state	2,8	The door is closed and the relay is on/no relay					
	On line door open, relay closed/no relay	. , .	On line door open, relay open/no relay state					
	Door opens alarm, relay closes		The door opens to alarm and the relay opens					
.	Door opening timeout alarm, relay closed/no relay, door magnetic open	· 🚅	Door opening timeout alarm, relay open/no relay, door magnetic open					
	Door opening timeout alarm, relay closed/door magnetic closed		Door opening timeout alarm, relay open/door magnetic close					
;	Door close alarm, relay off/no relay status	;	Door close alarm, relay open/no relay status					
	No door magnetic setting, door alarm, relay closed		No door magnetic setting, door alarm, relay open					
.	Door opening timeout alarm, no relay/door magnetic		The door was locked					
Note: If there is	Note: If there is no relay status, the current firmware does not support the "Check relay Status"							

Note: If there is no relay status, the current firmware does not support the "Check relay Status" function.

Table 3-8 Description of Door Types

Step 2: Remote opening/closing verification, taking remote opening as an example

Select the online door device, click "**Remote door opening**", enter the user password in the pop-up security verification, and click **OK**.

On the remote door opening screen, enter the time to open the door and tap **OK**, as shown in Figure 3-33.

If "Operation succeeded" is displayed, the remote door opening Operation is complete.

KBio CVSecurity III #	\varTheta admin ~
Access / Access Device / Real-Time Monitoring	-
Area Status Device Name More - Q	
Door Auxiliary Input Auxiliary Output	
Remote Opening Remote Closing Cancel Alarm Activate Lockdown More * Profesex1 1 Security Verification x User Password* 2 Current Totat 1 Online 1 Disable 0 Other 0	×
Real-Time Events	
Time Area Device Event Point Event Description Card Number Person Reader Name Verification Mode	
Sounds Reminder	and a start of the

Figure 3-33 Remote Door Opening

Step 3: Permission to verify

Verify personnel permissions on added devices.

In the real-time monitoring window, judge whether the personnel permissions are correctly configured according to the event status; If the user has been granted access rights, the real-time access event is a normal verification event, as shown in Figure 3-38, indicating that the access level service is configured

al-Time Events								
Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2021-12-16 11:15:26	Area Name	ProfaceX(CN3M212460001)	ProfaceX-1	Remote Opening			Other	Other



3.3.9.1 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 (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**.

Solution 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 is displayed on 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.

Solution 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.

Activate Lockdown

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices. Super User Swipe to Initiate Lockdown after 3 swipes

Deactivate Lockdown

It will unlock a locked door. This function is supported only by certain devices. Super User Swipe to Initiate disable after 3 swipes

• Quick Management of Doors

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

• Do	or Auxiliary Input Auxiliary	Outpu
	emote Opening 🛛 Remote Closing	D× (
TKT K	Status	Ĩ
ZKT_Ke -1	Device: ZKT_Korea Serial Number: CL63202960014 Number: 1 Door Sensor: Loading Relay: Loading Alarm: Loading	
	Remote Opening	
	Remote Closing	
	Activate Lockdown	
	Deactivate Lockdown	
	Cancel Alarm	
	Remote Normally Open	
	Enable Intraday Passage Mode Time Zone	
	Disable Intraday Passage Mode Time Zone	
Curren	Query the latest events from the door	ible:0

Figure 3-35 Quick management of doors

Personnel Photo Display

If a Real-Time Monitoring event contains personnel activity, the monitor will display the person photo (if no photo is registered, the monitor will display default photo). The event name, time and date are

displayed.

• Play Audio

If this option is selected, it plays an audio after an alarming event occurs.

• Query the Latest Events from The Door

Click to quickly view the latest events happened 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.

The Superuser can initiate lockdown after 3 swipes and deactivate the same after 3 swipes.

3.3.9.2 Auxiliary Input

It monitors current auxiliary input events in real-time.

ZKBio CVSecurity	::: ¥
Access Device 🗸	Access / Access Device / Real-Time Monitoring
Device	Area
I/O Board	Door Auxiliary Input Auxiliary Output
Door	
Reader	
Auxiliary Input	Auxillary Input-1
Auxiliary Output	inpu-1
Event Type	
Daylight Saving Time	
Device Monitoring	
Real-Time Monitoring	
Alarm Monitoring	e
Мар	Current Total:1 Online:0 Olisable:0 Offline:0 Unknown.0 Auxiliary Input Name
	Real-Time Events
	Time Area Device Event Point Event Description Card Number Person Reader Name Verification Mode

Figure 3- 36 Real Time Monitoring Auxiliary Input

3.3.9.3 Auxiliary Output

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

	Access / Access Device / Real-Time Monitoring
Access Device 🗸	Access / Access Device / Rear-Time Molinitoring
Device	Area 🔹 Status Device Name More + 🖉
I/O Board	Door Auxiliary Input Auxiliary Output
Door	
Reader	All Doors 🥥 Remote Open 🖤 Remote Close 👽 Remote Normally Open
Auxiliary Input	
Auxiliary Output	
Event Type	
Daylight Saving Time	
Device Monitoring	
Real-Time Monitoring	
Alarm Monitoring	< c
Мар	
	Current Total 0 Online: 0 Oliable: 0 Ol
	Real-Time Events
	Time Area Device Event Point Event Description Card Number Person Reader Name Verification Mode

Figure 3-37 Real Time Monitoring Auxiliary Output

Monitoring All

By default, the home page displays all doors of the panels within the user's level. User may monitor door(s) by setting the Area, Access Control or Door.

3.3.10 Alarm 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

ZKBio CVSecurity	::: ¥						
🔚 Access Device 🗸 🗸	Access / Access Devi	ce / Alarm Monitoring					
Device	설 Acknowledge						
I/O Board	Time	Device	Event Point	Event Description	Person	Reader Name	
Door							
Reader							
Auxiliary Input							
Auxiliary Output							
Event Type							
Daylight Saving Time							
Device Monitoring							
Real-Time Monitoring							
Alarm Monitoring	«						
Мар							

Figure 3-38 Alarm Monitoring

3.3.11 Map

Click **Access Device** > **Map** > **New** to add a map.

TKBio CVSecurity	::: ¥							
📕 Access Device 🗸 🗸	Access / Access Device	/ Map						
Device	⊖ Refresh = Nev	v 🖉 Edit 🗴 🖻 Delete	🕒 Save Positions	C Add Door	⊕ Zoom In	Q Zoom Out	23 Full Screen	
I/O Board	Map Index	< Current Map						
Door	A Please add a map							
Reader								
Auxiliary Input								
Auxiliary Output								
Event Type			New	×				
Daylight Saving Time	Ma	p Name*						
Device Monitoring		ea Name* p Path* Browse I	▼					
Real-Time Monitoring	Ma	p Path Browse	vol Opioaded					
Alarm Monitoring	*							
Мар								uuu
		ОК	Cancel			Event Poi	nt Event Descript	ion Card Numb

Figure 3-39 Map

After adding, users can add door on the map, perform zoom-in, zoom-out, etc. If users relocated or modified the map, click **Save Positions** to save. The user can view the new setting at next visit.

Access Device	~	Access / Access	Device / N	Map				
Device		O Refresh	Ξ + New	<u>⊿</u> E	dit <u> D</u> elete	🕒 Save Positions	🗗 Add Door	€ Zoom I
I/O Board		Map Index		<	BLR			
Door		🖌 🕒 T Campus	1		The first start of the		RT.	
Reader		BLR					5 8 8	
Auxiliary Input								
Auxiliary Output								
Event Type						E F		
Daylight Saving Time					LE MARKEN PARTY		5	
Device Monitoring					Real-Time Even	ts		
Real-Time Monitoring		«			Time	Area	Device	
Alarm Monitoring								
Мар								
	_							

Figure 3-40 Map Position

3.3.11.1 Add/Delete Map

Users can add or delete a map as needed.

3.3.11.2 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**).

• Add Doors & Cameras

After adding the map, click on "Add doors" and "Add cams" in the toolbar on the right to select devices to add to the map.

• Door Operation

If you move the cursor to a door, 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

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.

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.

Note:

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.

3.4 Access Rule

Access control rules are the core logic control part of access control, including time period settings, linkage settings, etc.

3.4.1 Timezone

In **Access Control** Module, time period is a very important basic concept, which is used to set the use time of the door and specify that **Access Control** is available in the valid time period.

This section describes how to configure Step to manually add a time range in ZKBio CVSecurity.

3.4.1.1 Add (New)

Operation Step:

Step 1: In the access Control module, choose "Access Rule > Time zone".

Step 2: Click **New**, the interface for adding time segments is displayed.

Step 3: The time segment page is added. Set the content based on the new requirements, as shown in Figure 3-41. For parameter Settings, see Table 3-9.

marks							
Time	Inter	rval 1	Inter	rval 2	Inter	val 3	
Date	Start Time	End Time	Start Time	End Time	Start Time	End Time	
	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
Tuesday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
Wednesday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
Thursday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
Friday	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
Saturday	00 : 00	00 : 00	00 : 00	00 : 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	13
Holiday Type 3	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	
py Monday's Settin	g to Others Weekda	ays:					1

Figure 3- 41 Adding A Time Range

Parameter	How to set up
Schedule Name	You can set a time range name for easy memory.
Note	Remarks Description of user-defined Settings.
Time interval	Set the start time and end time for each time range. The time period includes one week and three holiday-type time periods.
Copy Monday's time to other weekdays	You can quickly copy your Monday Settings to other weekdays.

Table 3-9 Parameters to Be Added in The Time Range

Step 4: Click OK to finish adding the time range.

3.4.1.2 Delete

Select time zone name, click **Delete**, and click **OK** to delete the time zone.

TZKBio CVSecurity	::: ¥						
Access Device >	Access / Access Rule / Time Zones						
🖡 Access Rule 🗸 🗸	Time Zone Name Remarks	Q @					
Time Zones	◯ Refresh 🎞 New 🔟 Delete						
Holidays	Time Zone Name	Remarks	Operations				
Access Levels	24-Hour Accessible	24-Hour Accessible					
Set Access By Levels	Multibio multibio		<u>∠</u> <u>ū</u>				
Set Access By Person							
Set Access By Department							
Interlock		Promp	t				
Linkage	«	Are you sure you want to					
Anti-Passback		operatio	n?				
First-Person Normally Open		ок	Cancel				
Multi-Person Group							
Figure 3- 42 Time Zone Delete							

3.4.2 Holiday

The access control time on holidays may be different from that on weekdays. To facilitate Operation, the system supports separate access control time on holidays.

This section describes how to manually add a holiday Step in ZKBio CVSecurity.

3.4.2.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Access Rule > Holidays".

Step 2: Click New, the page for adding holidays is displayed.

Step 3: When a page is added during holidays, set the content as required, as shown in Figure 3-43. For parameter Settings, see Table 3-10.

Holiday Name*		
Holiday Type*	Holiday Type 1 🔹	
Start Date*	2021-12-16	
End Date*	2021-12-16	
Recurring	No 🔻	
Remarks		

Figure 3-43 Adding Holidays

Parameter	How to set up			
Holiday Name	You can set holiday names for easy memory.			
Type of Holidays The holiday type can be: Holiday type 1, Holiday type 2, holiday type holiday type to time Range.				
Start time/End time	Set the holiday time range.			
According to the annual circulation	Set whether this holiday cycle by year: yes, no. For example, if New Year's Day is January 1, set this parameter to Yes.Mother's Day falls on the second Sunday in May. If the date is uncertain, set it to No.			
Note	Custom Settings description.			
Table 3- 10 Parameters for Adding Holidays				

Step 4: Click **OK** to finish adding the holiday.

3.4.2.2 Delete

Select holiday, click **Delete**, and click **OK** to delete the holiday. **TKBio CVSecurity** Ħ Access / Access Rule / Holidays Access Device Holiday Name Recurring -----• Q @ Access Rule Holiday Type -----Time Zones ⊖ Refresh ☲ New 💼 Delete 🛃 Holiday Name Holiday Type Start Date End Date Recurring Remarks Operations Access Levels spring festival Holiday Type 1 2022-07-19 2022-07-23 No _ ₫ Set Access By Levels Set Access By Person Set Access By Department Interlock Prompt Linkage Are you sure you want to perform the delete Anti-Passback Cancel First-Person Normally Open Multi-Person Group Multi-Person Opening Door

Figure 3-44 Holiday Delete

3.4.3 Access Level

Access level groups define groups and categories of internal doors to facilitate subsequent permission assignment operations.

Setting operations include creating access level groups and adding doors to access level groups.

3.4.3.1 Add (New)

This section describes how to create Step for Access Control groups in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Access Rule > Access Level".

Step 2: Click New in the left column, and the page for adding access level groups is displayed.

Step 3: On the page for adding access level groups, set parameters based on the new requirements, as shown in Figure 3-45. For parameter Settings, see Table 3-11.

		×
Level Name*		
Time Zone*	•	
Area*	•	
_		

Figure 3-45 Adding Access Level Groups

Parameter	How to set up		
Permission Group Name	You can customize the name of the access level group for easy query.		
Access Control Period	Select the configured access time range to define the valid access time range for this permission group.		
Area Select the configured area from System > System Management Settings and define the area to which the Access Control group be			
Table 3- 11 Description of Access Control Right Groups			

Step 4: Click **OK** to finish configuring the access control right group.

3.4.3.2 Add Door

This topic describes how to add Operation Step to the door of the created access level group in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Access Rule > Access level>Add Door".

Step 2: Click **"Add Door"**, and the page for selecting a door is displayed. add a door as required, as shown in Figure 3-46.

TKBio CVSecurity	
Access Device >	Access / Access Rule / Access Levels
👢 Access Rule 🗸 🗸	Access Levels Ceneral (Area Name) Door Combination
Time Zones Holidays	Level Name Time Zone Q & Door Name Owned Device
Access Levels Set Access By Levels	○ Refresh ∓ New ill Delete I Door Control - ○ Refresh ill Delete Door 1 Export □ Level Name Area Name □ Level Name Area Name
Set Access By Person Set Access By Department	General Area Name 24-Hour Acci 2 2 3 test Area Name 24-Hour Acci 0 7 Add Door Add Door ×
Interlock Linkage	
Anti-Passback	Alternative Selected(0)
First-Person Normally Open	Door Name Owned Device Serial Number Area Name Owned Device Serial Number Area Name
Multi-Person Group	192.168.1.28-1 192.168.1.28 CL9M203460071 Area Name
Multi-Person Opening Door	ZKT_Korea-1 ZKT_Korea CL63202960014 Area Name
Verification Mode	>>> >>
Verification Mode Group	< <
Parameters	<< No data
비 Advanced Functions >	I< < 1-2 > > 50 rows per page ▼ Total of 2 records
II. Access Control Reports >	OK Cancel

Figure 3-46 Adding Access Level Groups Add Doors

Step 3: Click OK to finish configuring the door for the access control right group.

3.4.3.3 Door Control

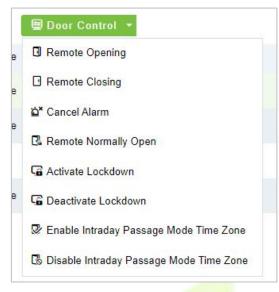


Figure 3-47 Door Control

• 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 (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** fails, check whether the devices are disconnected or not. If disconnected, check the network.

• Cancel the Alarm

Once an alarming door is displayed on 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.

Solution 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.

• Activate Lockdown

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices. Super User Swipe to Initiate Lockdown after 3 swipes

Deactivate Lockdown

It will unlock a locked door. This function is supported only by certain devices. Super User Swipe to Initiate disable after 3 swipes.

3.4.3.4 Import or Export Access Level

Step 1: Export and fill in Access Level Template:

In the Access Module, click Access Rule > Access Levels > Export > Export Access Level, then fill in the Access levels information.

TKBio CVSecurity		\rm e admin ~
Access Device >	Access / Access Rule / Access Levels	
🖡 Access Rule 🗸 🗸	Access Levels General (Area 1) Door Combination	>
Time Zones	Level Name Time Zone Q 🖉 Door Name Ovined Device	Q 🖉
Holidays	C Refresh ∓ New 18 Delete ፼ Door Control ▼	
Access Levels	Level Name Area Name Time Zone Doo 2 Export Access Level Door Name Owned Device	
Set Access By Levels	General Area 1 24-Hour Acct 1	
Set Access By Person		

Figure 3- 48 Export Access Level Template

Access Levels				
Level Name	Area Name	Time Zone		
Level 1	Area 1	Time Zone 1		
Level 2	Area 2	Time Zone 1		
Level 3	Area 3	Time Zone 1		
Level 4	Area 4	Time Zone 1		
Level 5	Area 5	Time Zone 1		

Figure 3- 49 Fill in Access Level Template

Note: The Level name can be customized. The Area Name can be set from **System** > **System** Management > **Area Settings**, the Time Zone can be set from **Access** > **Access Rule** > **Time Zones**.

Step 2: Export the Doors of Access Level Template:

In the Access Module, click Access Rule > Access Levels > Export > Export Doors of Access Level, then You can export doors of access level in Excel file format.

Enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export, and Click **OK**.

ZKBio CVSecurity	,	::: ¥			
Access Device >		Access / Access Rule	e / Access Levels		
Access Rule 🗸		Access Levels			
Time Zones	^	Level Name		Time Zone	Q &
Holidays		O Refresh Ξ∓	New 💼 Delete	🗐 Door Control	
Access Levels		Level Nam	e 🔰 Area Name	Time Zone Door	
Set Access By Levels		General	CMO group	24-Hour Acce 1	${f \pm}$ Export Doors of Access Level
Set Access By Person		KR	Korea	24-Hour Acce 1	∠ C.
Set Access By Department	«	CITall	พื้นที่CIT	24-Hour Acce 3	<u> </u> C+
Interlock				21.1100.4000.0	

Figure 3-50 Export the Access Level Template 1

	OR	efresh ∓ New	💼 Delete 🛛 🖳 Door Control	★ Export ★ Import ★	
		Level Name	Area Name Time Zone Do	Export Doors of Access Level	
		<u>General</u>	CMO groi Encrypt or not	○ Yes ● No	
1		KR	Korea File Format	EXCEL All (max 100000 records)	
«		<u>CITall</u>	Data to Export พื้นที่CIT		
		<u>BM</u>	BM		
		Jap A	CMO grou		
		<u>3</u>	CMO grou	OK Cancel	
		<u>visitor level</u>	CMO group 24-Hour Acce 1	_ □	

Figure 3- 51 Export the Access Level Template 2

Step 3: Import the Access Level Template:

In the Access module, click Access Rule > Access Levels > Import > Import Access Level, and click Browser to upload the Access Level Template.

ZKBio CVSecurity	III ¥ 0	admin ~
Access Device >	Access / Access Rule / Access Levels	
👢 Access Rule 🗸 🗸	Access Levels General (Area Name) Door Combination	>
Time Zones	Level Name Time Zone Q Q Door Name Owned Device Q	\oslash
Holidays	⊖ Refresh 🍜 New 🗰 Delete 🗐 Door Control 👻 🛨 Export 👻 Import 🔫 🗘 Refresh 💼 Delete Door	
Access Levels	🗌 Level Name Area Name Time Zone Door Count Oper 🔽 Import Access Level 😽 or Name Owned Device	
Set Access By Levels	General Area Name 24-Hour Acct 1 ℓ Import Doors of Access Level dcor fds 10.8.14.206	
Set Access By Person		

Figure 3- 52 Import the Access Level Template 1

TKBio CVSecurity	::: ¥		e	admin 👻
Access Device >	Access / Access Rule / Access Levels			
📕 Access Rule 🗸 🗸	Access Levels	< Browse Level	is General (Area Name) Door Combination	>
Time Zones	Level Name Time Zone	Q & Door Name	Owned Device C	2 @
Holidays	CRefresh ∓New of Delete ■ Door Contr	ol → ⊥ Export → ⊥ Import → ○ Refrest	n m∰ Delete Door	
Access Levels	Level Name Area Na	Import Access Level	× e Owned Device	
Set Access By Levels	General Area Na File Format	• Excel	10.8.14.206	
Set Access By Person	Select File Update Existing	Browse Plot Uploaded		
Set Access By Department		data format is table name, the second line is header, the third ata, please check the file and then import.		
Interlock		and brance ender me us and mathem.		
Linkage				
Anti-Passback		OK Cancel		

Figure 3-53 Import the Access Level Template 2

nulluays	C Refresh ∓ New	💼 Delete 🖳 Door Control → 🛧 Export → 🔟 Import →	🔿 Refresh 🛛 🖻 Delete Door
Access Levels	Level Name	Import	× Owned Device
Set Access By Levels	General	Total Progress	10.8.14.206
Set Access By Person		100%	
Set Access By Department	Level 1	Data processing, please wait Upload successful, starting to parse data, please wait	*
Interlock	Level 5	Diplate adjustion, starting to parse duate, prease wat The data has been parsed, starting database updates. Data processing, please wait Succeed 5. Failed 0.	
Linkage	Level 4	Operation finished	
Anti-Passback	Level 2		Close
First-Person Normally Open	Level 3	Area 3 Time Zone 1 0 🖉 📭	



Step 4: After the upload is successful, we can view the uploaded level as the following figure.

ZKBio CVSecurity	::: ¥					e admin
Access Device >	Access / Access Rule /	Access Levels				
Access Rule 🗸 🗸	Access Levels		۲	Browse Levels General (Are	a 1) Door Combination	
Time Zones	Level Name	Time Zone	Q &	Door Name	Owned Device	Q &
Holidays	🔾 Refresh 🛛 🖅 Ne	w 💼 Delete 😐 Door Control 👻	∱ Export - ↓ Import -	⊖ Refresh 🏛 Delete D	100	
Access Levels	Level Name	Area Name Time Zone Door	Count Operations	Door Name	Owned Device	
Set Access By Levels	General	Area 1 24-Hour Acce 1		abdcor fds	10.8.14.206	
Set Access By Person	-	Area 1 Time Zone 1 0	2 0			
Set Access By Department	«	Area 1 Time Zone 1 U				
Interlock	Level 5	Area 2 Time Zone 1 0	∠ ⊡			
Linkage	Level 4	Area 3 Time Zone 1 0	_ ⊡			
Anti-Passback	Level 2	Area 2 Time Zone 1 0	∠ ⊡			
First-Person Normally Open	Level 3	Area 3 Time Zone 1 0	_ ₽			

Figure 3-55 Import the Access Level Template 4

Step 5: Import the Doors of Access Level Template:

visitor level CMO group 24-Hour Acce 1

In the Access module, click Access Rule > Access Levels > Import > Import Doors of Access Level, and click **Browser** to upload the Access Level Template.

1	ZKBio CVSecu	ty III #
	Access Device	> Access / Access Rule / Access Levels
Į.	Access Rule	Access Levels
	Time Zones	Level Name Time Zone Q
	Holidays	C Refresh ∓ New @ Delete 및 Door Control ▼ 1 Export ▼ 🔽 Import ▼
	Access Levels	Level Name Area Name Time Zone Door Count Oper 4 Import Access Level
	Set Access By Levels	General CMO group 24-Hour Accc 1
	Set Access By Person	
		Figure 3- 56 Import the Doors of Access Level Template 1
) r	efresh ∓ New	on Delete
	Level Name	Area Name Time Zone Door Count Operations
	<u>General</u>	CMO group
	KR	File Format Excel
		Select File Browse Not Uploaded
	<u>CITall</u>	นที่CIT The first line of the data format is table name, the second line is header, the third line is the import data, please check the file and then import.
	<u>BM</u>	3M
	Jap A	MO group
1		OK Cancel
	<u>3</u>	CMO group

2 C+ Figure 3- 57 Import the Doors of Access Level Template 2

Step 6: After the upload is successful, we can view the uploaded level as the following figure.

ZKBio CVSecurity		¥							e admin
Access Device >	Aco	cess / Access Rule / Ac	ccess Levels						
Access Rule 🗸 🗸 🗸	Ac	cess Levels			۲	Bro	owse Levels General (Area	1) Door Combination	
Time Zones		Level Name		Time Zone	Q &	C	Door Name	Owned Device	Q &
Holidays		◯ Refresh =+ New	💼 Delete	🗐 Door Control 👻 🛧	Export 👻 Import 👻		🔾 Refresh 🗴 Delete Do	10	
Access Levels		Level Name	Area Name	Time Zone Door Co	unt Operations		Door Name	Owned Device	
Set Access By Levels		General	Area 1	24-Hour Acce 1	∠ ₽		abdcor fds	10.8.14.206	
Set Access By Person		Level 1	Area 1	Time Zone 1 0	2 B				
Set Access By Department	«	Level	Alea I	Time Zone 1 0					
Interlock	9	Level 5	Area 2	Time Zone 1 0	_ ₽				
Linkage		Level 4	Area 3	Time Zone 1 0	_ ₽				
Anti-Passback		Level 2	Area 2	Time Zone 1 0	_ □				
First-Person Normally Open		Level 3	Area 3	Time Zone 1 0	2 B				



3.4.4 Set Access Level Allocation

Permission assignment Manages the access level of personnel. After permission assignment, personnel can verify the door opening Operation.

You can assign user rights by user group or assign user rights by user group.

3.4.4.1 Assign Personnel Rights by Permission Group

Assigning personnel permissions by permission group is used to define a set of open-door personnel for a permission group.

Describes Operation Step that assigns staff permissions by permission group in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Access Rule>Set Access by Levels".

Step 2: In the Operation column of the corresponding permission group, tap "**Add Personnel**". The Add personnel page is displayed. Select personnel as required, as shown in Figure 3-48.

Holidays	⊖ Refresh		🔾 Refresh 🛛 🗴 Delete Personne
Access Levels	Level Name Area Name Time Zone	Operations	Personnel ID First Name
Set Access By Levels	K-Test Area Name 24-Hour Acces	ssi 🐣	9999 K-TEST
Set Access By Person	multibio XM multibio	8+ 2+	
Set Access By Department		Add Personnel	×
Interlock	Query Oppartment		
« Linkage	Personnel ID Name	Department Name	Q @
Anti-Passback			
First-Person Normally Open	Alternative	Selected(0)	
Multi-Person Group	Personne First Name Last Name	Depart Personne First Name L	ast Name Department
•	🗆 1 ju	Departmei	
Multi-Person Opening Door	12135	Departmen >	
Verification Mode	12133	<	
Verification Mode Group	12134 name1	hr <<	
Parameters	🔲 1119 multibio	Departmer No data	
	IC 2000 IC < 1-16 → >I 50 rows per page	n	
Advanced Functions >		OK Cancel	

Figure 3- 59 Assigning Rights to Users by Rights Group

Step 3: Click OK to complete the assignment of personnel permissions.

3.4.4.2 Delete Personnel

Select personnel ID, click **Delete**, and click **OK** to delete the personnel ID.

ZKBio CVSecurity		e admin
Access Device >	Access / Access Rule / Set Access By Levels	
🖡 Access Rule 🗸 🗸	Access Levels < Browse Personne	el K-Test (Area Name) From Levels
Time Zones	Level Name Time Zone Q Q Personnel ID	Name More * Q Ø
Holidays	O Refresh O Refresh	in Delete Personnel
Access Levels	Level Name Area Name Time Zone Operations	nel ID First Name Depart
Set Access By Levels	K-Test Area Name 24-Hour Accessi 🐣 👿 9999	K-TEST Departme
Set Access By Person	multibio XM multibio 2*	
Set Access By Department	test Area Name 24-Hour Accessi 🏝 Prompt	
Interlock Linkage	c General Area Name 24-Hour Accessi 🏖 Are you sure you want to perform the delete operation?	
Anti-Passback	Concel	
First Parson Normally Open		

Figure 3- 60 Delete Personnel

3.4.4.3 Export

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

		E	xport				×
The File	Г <mark>ур</mark> е	EXCEL File	~]			and the second
Export M	ode	All data (Can ex	c <mark>port up</mark> t	o <mark>400</mark> 00 data)			
		O Select the amo	unt of dat	a to export (Can e	kport up	to 40000 data)	
		From the article	1	Strip, is derived	100	Data	
		ОК		Cancel			
	X						
		Figure	3- 61 E	xport			
			ZKTECO)			

					Device					
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Figure 3- 62 Set Access level Allocation Export

3.4.5 Set Access Level Groups by Person

Assigning access level groups by person A permission set is used to define the access level set of a person.

This section describes Operation Step that assigns access control group permissions by person in ZKBio CVSecurity.

3.4.5.1 Access Control Setting

Operation Step:

Step 1: In the Access Control module, choose "Access Control > Settings by Personnel".

Step 2: In the Operation column of the Access Control group, click **"Add Access Control Group**". The page for adding access control groups is displayed. Select the Access Control group as required.

ZKBio CVSecurity	::: ¥		
Access Device >	Access / Access Rule / Set Access By Person		
🖡 Access Rule 🗸 🗸	Edit Personnel For Levels		<
Time Zones	Personnel ID Name	More* Q Q	
Holidays	○ Refresh	ort 🏟 Synchronize Level	
Access Levels	Personne First Name Last Name	Department Device Ope Operations	
Set Access By Levels	🗹 1 ju	Department Name Ordinary User 🖗	
Set Access By Person	9999 K-TEST	Department Name Ordinary User 🖗	
Set Access By Department	New	×	
Interlock	12135 Superuser N	v User ∦Ar	
Linkage	Device Operation Role	Ordinary User 🦂	
Anti-Passback	1119 Extend Passage Disabled	User Pr	
First-Person Normally Open	555 Set Valid Time		
Multi-Person Group	2222	vUser ∲k	
Multi-Person Opening Door	5	User Ph	
Verification Mode	3 OK	Cancel User 🕅	
Verification Mode Group	4 W9	Department Name Ordinary User 🖗	
Parameters			

Figure 3-63 Assigning Rights Groups by User

Step 3: Click OK to complete the assignment of personnel permissions.

3.4.5.2 Add Level

Permission assignment Manages the access level of personnel. After permission assignment, personnel can verify the door opening Operation.

You can assign user rights by user group or assign user rights by user group.

• Assign Personnel Rights by Permission Level

Assigning personnel permissions by permission group is used to define a set of open-door personnel for a permission group.

Describes Operation Step that assigns staff permissions by permission group in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Access Rule>Set Access by Levels "

Step 2: In the Operation column of the corresponding permission group, tap "**Add Levels**". The Add level page is displayed. Select personnel as required.

ZKBio CVSecurity

Access Device >	Access / Access Rule / Set	t Access By Person						
Access Rule 🗸 🗸 🗸	Edit Personnel For Levels						Browse Personnel 12135 From Leve	ls
Time Zones	Personnel ID	Name	More *	Q &			Level Name	Time Zone Q d
Holidays	O Refresh 🕞 Acces	ss Control Setting 🔶 Exp	ort 🏾 🚯 Synchronize Leve	đ			🔾 Refresh 🖀 Delete From Le	rvels
Access Levels	Personne Fi	rst Name Last Name	Department Devi	ce Ope Operations			Level Name Area Nar	me Time Zone
Set Access By Levels	🗹 t ju		Department Name Ordi	nary User 🗛			🔄 General 🛛 Area Nar	me 24-Hour Accessible
Set Access By Person	0 9999 K-	TEST	Department Name Ordi	nary User				
Set Access By Department	12135		Department Name Ord			Add to Levels		×
nterlock								
inkage	12134 na	ame1	hr Ord	Level Name	Time Zone	Q @		
Anti-Passback	🗌 1119 mi	ultibio	Department Name Ord	Alternative		Selected(0)		
First-Person Normally Open	🖸 555 fo		Department Name Ord	Level Name	Time Zone	Lev	el Name 🔰 Time Zone	
Multi-Person Group	2222 yg	2V	Department Name Ord	K-Test	24-Hour Accessible			
Multi-Person Opening Door	ј 5 уу	ryy	Department Name Ord	multibio	multiblo	>>		
verification Mode	D 3		Department Name Ord	test	24-Hour Accessible	> <		
/erification Mode Group	0 4 W	ro.	Department Name Ord		24-riddi Accessiole	~ ~		
Parameters	1118		Department Name Ord				No data	
	1118		Department Name Ord	< < 1-3 >	>) 50 rows per page *			
	🗌 1115 Zo	prro	Development Ord			OK Cancel		
	1114 M	d, Jalal	Development Ordi	hary User 🔒				

Figure 3- 64 Assigning Rights to Users by Rights Group

Step 3: Click **OK** to complete the assignment of level permissions.

3.4.5.3 Delete from Level

Select level name, click **Delete**, and click **OK** to delete the level name.

TKBio CVSecurity	::: %									Θ	
Access Device >	Access / Access Rule / Set	t Access By Person									
📱 Access Rule 🗸 🗸	Edit Personnel For Levels				٢	¢ Browse Personnel 2222 From Levels					
Time Zones	Personnel ID	Name	More *	Q @		Level Nam	e [ime Zone Q Q		
Holidays	O Refresh 🕞 Acces	ss Control Setting 🔶 Exp	ort 🛯 🕅 Synchronize Level			O Refre	sh 🛱 Del-	ete From Levels			
Access Levels	Personne Fin	rst Name Last Name	Department Device	Ope Operations		Le	vel Name	Area Name	Time Zone		
Set Access By Levels	🖸 1 ju		Department Name Ordinar	ry User 🔗		🖬 к-	Test	Area Name	24-Hour Accessible		
	🗆 9999 K-	TEST	Department Name Ordinar	ryUser 🖗			ltibio	ХМ	multible		
Set Access By Department Interlock	12135		Department Name Ordinar	ryUser 🖗		🗆 ter	st	Area Name	24-Hour Accessible		
Linkage	🗌 12134 na	ame 1	hr Ordinar	ryUser 🖗		Ge	neral	Area Name	24-Hour Accessible		
Anti-Passback	🗆 1110 m.	ultiblo	Department Name Ordinar	ry User 🖗							
First-Person Normally Open	🗖 555 fo		Department Name Ordinar	ry User 🖗							
Multi-Person Group	2222 yg	py	Department Name Ordinar	ry User Ph	Prompt						
Multi-Person Opening Door	б 5 уу	ууу	Department Name Ordinar	ry User 🗚	Are you sure you want to perform the dele operation?						
Verification Mode	3		Department Name Ordinat	ry User 🔗	OK Cancel						
Verification Mode Group	🗆 4 🛛 W	Ŷ	Department Name Ordinar	ryUser Pa							
Parameters	1118		Department Name Ordinar	ry User 🖗							

Figure 3-65 Access Level Group by Person Delete

3.4.5.4 Export

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

The File Type	EXCEL File	\sim		
Exp <mark>ort Mo</mark> de	All data (Can expo All data (Can expo	ort up to 40000 data)		
	O Select the amount	of data to export (C	an export up	to 40000 data
	From the article 1	Strip, is der	ived 100	Data

Figure 3-66 Export

					ZKTECO					
					Device					
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	нттр	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Figure 3- 67 Access Level Group by person Export

3.4.5.5 Synchronize Level

Select the level to be synchronized and send the corresponding device area data in the software to the device.

ZKBio CVSecurity	::: ¥		
Access Device >	Access / Access Rule / Set Access By Perso	n	
Access Rule 🗸 🗸 🗸	Edit Personnel For Levels		K Browse Personnel 2222 From Level
Time Zones	Personnel ID Na	me More* Q Q	Level Name
Holidays	C Refresh 🕞 Access Control Setting		🔿 Refresh 🛛 💼 Delete From Le
Access Levels	Personne First Name Las	t Name Department Device Ope Operations	Level Name Area Na
Set Access By Levels	🛃 1 ju	Department Name Ordinary User 🤌	K-Test Area Na
Set Access By Person Set Access By Department	0000 K-TEST	Dep Prompt	multibio XM
Interlock	12135	Dep Are you want to perform the Synchronize Level operation?	🗌 test 🛛 Area Na
Linkage	12134 name1	hr OK Cancel	General Area Na
Anti-Passback	1119 multibio	Dep	
First-Person Normally Open	555 fc	Department Name Ordinary User	

Figure 3-68 Synchronize Level

3.4.6 Set Access Level Groups by Department

The access level group assigned by department defines the set of access levels for the personnel in the department.

This section describes Operation Step that assigns Access Control group permissions by person in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Access Control > Set by department".

Step 2: In the Operation column of the Access Control group, click **"Add Access Control Group"**. The page for adding Access Control groups is displayed. Select the Access Control group as required.

Add to	o Default Levels	×
Level Name	Q &	
Alternative	Selected(0)	
Level Name Time Zone	Level Name Time Zone	
General 24-Hour Accessible		
	>> < << No data	
I< < 1-1 >>I 50 rows per page ▼		
ОК	Cancel	

Figure 3- 69 Assigning Rights Groups by Department

Step 3: Click OK to complete the assignment of department permissions.

3.4.6.1 Add Default Level

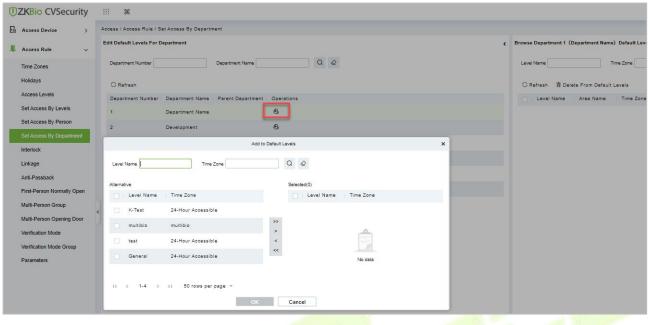


Figure 3-70 Add Default Level Groups by Department

3.4.6.2 Delete Default Level

Select delete default level name, click **Delete**, and click **OK** to delete the default level name.

ZKBio CVSecurity			
Access Device >	Access / Access Rule / Set Access By Person		
📕 Access Rule 🗸 🗸	Edit Personnel For Levels ¢	Browse Personnel 2222 From Levels	
Time Zones	Personnel D Name More * Q Q	Level Name Time Zone	
Holidays	⊖ Refresh 🔞 Access Control Setting 🖈 Export 🖓 Synchronize Level	🔿 Refresh 📋 Delete From Levels	
Access Levels	Personne First Name Last Name Department Device Ope Operations	Level Name Area Name Time Zone	
Set Access By Levels	🖸 1 ju Department Name Ordinary User 🐴 Prompt	K-Test Area Name 24-Hour Acces	
Set Access By Person Set Access By Department	9000 K-TEST Department Name Ordinary User 🖗 Are you sure you want to perform the delet	ete multibio XM multibio	
Interlock	12135 Department Name Ordinary User Pk	test Area Name 24-Hour Acces	
Linkage	12134 name1 hr Ordinary User 🕅 Cancel	General Area Name 24-Hour Acces	
Anti-Passback	🗌 1119 multibio Department Name Ordinary User 🍂		

Figure 3-71 Delete Rights Groups by Department

3.4.7 Interlock

Set interlock control between two or more doors on the access controller device: To verify the opening of a door, ensure that all other doors interlocked with the door are closed; otherwise, the door cannot be opened.

This section describes the Step of adding interlock effect in ZKBio CVSecurity.

The Premise Conditions:

- The door opening/closing state monitoring is realized by detecting the door magnetic state. Therefore, interlock function requirements:
- 1. The door status sensor at the device end must be correctly installed
- 2. In door setting on the software side, the status of the door status sensor must be set to normally open or normally closed (based on the actual installation).

3.4.7.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Access Control > Interlock" and click New.

Step 2: Select the specified device.

Instructions:

When you add a device for which interlock has been configured, the device cannot be found in the drop-down list. After the configured interlock information is deleted, the device is returned to the drop-down list.

Interlock Settings vary with the number of doors controlled by the device:

Single-door controller: no interlock setting

Dual door controller: 1-2 two door interlock Settings

Four-door controller: 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, 1-2-3-4 four-door interlock, 1-2 and 3-4 door interlock

Step 3: Select the interlock rule, and click **OK** to complete the settings, as shown in Figure 3-52. The new interlock Settings are displayed in the list.

	New	×
Device Name*	Click to select	
Interlock Rule*		
(3)	and New OK Cancel	

Figure 3-72 Adding Interlock Configuration

Parameter	How to set up
Device Name	You can customize the name of the Device
Interlock Rule	Select the configured interlock rule.
	Table 3- 12 Description of interlock

3.4.7.2 Delete

Select interlock, click **Delete**, and click **OK** to delete the interlock.

3.4.8 Linkage

The use method and scenario of linkage are flexible. After a specific event is triggered by an input point in the **Access Control** system, a linkage action will be generated at the specified output point to control events such as verification opening, alarm and abnormality in the system.

This section describes how to add Step to the linkage effect in ZKBio CVSecurity.

• Add (New)

The Premise Conditions:

Before adding a linkage configuration, perform the following operations:

Step 1: Add Settings for binding cameras to access control devices, input points, output points, and

read heads.

Step 2: Optional: In the **System Management** module, choose **"System Management > Mail Management**" to set the sender server. The Step of setting the sender server is as follows:

In the System Management module, choose 'system Management > Mail Management".

Click "Sender Server Settings" to pop up the sender server Settings interface.

On the Sender server Settings screen, set parameters as required, as shown in Figure 3-73. For parameter Settings, see Table 3-13.

After setting, click "**Test connection**" to receive the email, indicating that the test has passed.

Step 3: Click **OK** to finish setting email parameters.

1	Outgoing Mail Server Settings Email Sending Server* Port* Email Account*	25	(smtp.xxx.xxx)	
	Password*		(xxx@xxx.xxx)	1
	Sender Name Test Connection Please complete the email ve	erification.		
	OK	Cancel		

Figure 3-73 Mailbox Parameters

Parameter	How to set up
Email server address/port	You can customize the email server address and port. The email products that provide the SMTP server can be used, such as NetEase 163 email, Tencent QQ email, and Foxmail email. The specific address and port configurations must be obtained from the corresponding provider.
Email username and password	Enter the user's name and password for the mailbox.
Name of sender	Sets the name of the sender on the received message.

Table 3-13 Mailbox Management Parameters

Operation Step:

Step 1: In the Access Control module, choose "Access Control > Linkage".

Step 2: On the linkage setting screen, click **Add**, as shown in Figure 3-69. Table 3-14 and Table 3-15 refer to the linkage parameters.

		New		×
Linkage Name*		Device*	Click to select	
Linkage Trigger Conditions*	Add	Input Point*		
Output Point*				•
Output Point*	Video Linkage	E-mail S	Send SMS	,
7001				
Action type*	Close •	Action type*	Close •	
	Save and New	ОКС	ancel	

Figure 3-74 New Linkage Configuration

Parameter	How to set up
Linkage Name	You can customize the l <mark>inkag</mark> e name for easy query.
Equipment	Custom Select an added access control device.
Linkage Departure Condition	Select the condition triggered by the linkage Operation, that is, the event type generated by the selected device.
Input Point	Select the input point to set device input.
Dots	Select the output point to set device output.
Linkage Action Setting	You can set the linkage action, including Operation, video linkage, and email. Table 3-3 describes the configurations of the three modes.
	Table 3- 14 New Linkage Parameters

Parameter	How to set up
The Output Point of Operation	Set the output action type: close, open, normally open. Sets the delay time if the output action is on.
Video Linkage	Pop-up video and display duration: Select pop-up video on the real-time monitoring screen and set the pop-up duration. Video recording and Video Duration: Select Video recording to set the video duration. Capture: Set linkage action whether to take a photo: If a photo is taken, you also need to set whether to pop up on the real-time monitoring interface and the display duration.
Mail	Set the email address that receives the linkage content when a linkage event occurs.

Table 3-15 Setting Linkage Actions

Step 3: Click **OK** to complete the linkage configuration.

3.4.8.1 Delete

Select linkage, click **Delete**, and click **OK** to delete the linkage.

JZKBio CVSecurity	::: ¥			
Access Device >	Access / Access Rule / Linkage			
Access Rule 🗸 🗸	Linkage Name De	evice Name Q Q		
Time Zones	⊖ Refresh ∓ New 📋 Delete			
Holidays	🕎 Linkage Name Device Name	Linkage Trigger Conditions	Operations	
Access Levels	Sdsd 10.10.20.144	Normal Verify Open	L 🖬	
Set Access By Levels				
Set Access By Person				
Set Access By Department		Prompt		
Interlock		Are you sure you want to perform the delete		
Linkage		operation?		
Anti-Passback		OK		
First-Person Normally Open				

Figure 3-75 Adding Interlock Configuration

3.4.9 Anti-Passback

Some occasions require the personnel that brush card to verify, brush card to come in from a door must brush card to go out from another door, brush card record must enter a strict correspondence. This function can be used when users enable it in the settings. It is generally used in special units, scientific research, bank vaults and other occasions.

This section describes the Step of adding the Anti-Passback effect in ZKBio CVSecurity.

3.4.9.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Access Control > Anti-Passback" and click New.

Step 2: Select the specified device.

Instructions:

When you add an Anti-Passback device, the configured Anti-Passback device is not displayed in the device list. After the antisubmarine information is deleted, the device returns to the device list.

The Anti-Passback setting varies with the number of gates controlled by the equipment:

Anti-Passback setting of single door controller: Anti-Passback between readers

Two controllers: door 1 Anti-Passback between readers, door 2 Anti-Passback between readers, door 1 and door 2 Anti-Passback

Four door controllers: door 1 and door 2 Anti-Passback, door 3 and door 4 Anti-Passback, door 1/ door 2 and door 3/ door 4 Anti-Passback, door 1 and door 2/ door 3/ door 4 Anti-Passback, door 1 and door 2/ door 3/ door 4 Anti-Passback, door 1/ door 2/ door 3/ door 4 Anti-Passback reader

Step 3: Select the Anti-Passback rule and click **OK** to complete the settings. The new Anti-Passback Settings are displayed in the list.

	New	×
Device Name*	Click to select	
Anti-Passback Rule*	•	
Save and	New OK Cancel	

Figure 3-76 Adding the Anti-Passback Configuration

3.4.9.2 Delete

Select device, click **Delete**, and click **OK** to delete the device.

TZKBio CVSecurity		
Access Device >	Access / Access Rule / Anti-Passback	
🖡 Access Rule 🗸 🗸	Device Name Q Q	
Time Zones	⊖ Refresh ∓ New 💼 Delete	
Holidays	Device Name Anti-Passback Rule	Operations
Access Levels	192.188.1.28 Anti-Passback between readers of door 192.188.1.28-1	2 1
Set Access By Levels		
Set Access By Person		
Set Access By Department		
Interlock		
Linkage		
Anti-Passback		
First-Person Normally Open		
Multi-Person Group		Prompt
Multi-Person Opening Door	Ĵ.	Are you sure you want to perform the delete operation?
Verification Mode		OK Cancel
Verification Mode Group		Cancer
Parameters		

Figure 3-77 Anti-Passback Delete

3.4.10 The First-Person Normally Open

In the specified period, after the verification of the first person with normally open permission, the door normally open, the end of the valid period of the door automatically closed.

This section describes how to add Step in ZKBio CVSecurity.

The Premise Conditions:

The time range has been set for the Access Control module.

3.4.10.1 Add (New)

Operation Step:

Step 1: In the **Access Control** module, choose "**Access Control** > **First person normally Open**" and click **New**.

Step 2: Select the specified device, add Settings for the specified door, and select the normally open time period, and click **OK**, as shown in Figure 3-58.

1	New	×
Door Name*	Click to select	
Passage Mode Time Zone*]
ОК		

Figure 3-78 Configuring the First Person to Open the Door

Step 3: Click "**Add People**" on the interface of "**Opening of the first person**". After adding people, click **OK** to complete the setting of "opening of the first person".

	Add P	Personnel	×
Query Department			
Personnel ID Name		Department Name	
Alternative		Selected(0)	
	epartment	Personne First Name Last Name Department	
Personne First Name Last Name De	epartment	reisonne Frischame Laschame Department	
□ 1 So	oluction		
		>>	
		<	
		<< No data	
		No data	
I< < 1-1 > >I 50 rows per page ▼			
1	OK	Cancel	
	OK	Calloci	

Figure 3-79 Adding A First Person Normally Open Person Configuration

3.4.10.2 Delete

Select personnel ID, click **Delete**, and click **OK** to delete the personnel ID.

TZKBio CVSecurity	111 %				
Access Device >	Access / Access Rule / First-Person Normally Open				
🖡 Access Rule 🗸 🗸	First Person Normal Open C	Browse	e Personnel		
Time Zones	Door Name Q Q	Pers	onnel ID		Name
Holidays	O Refresh 🖙 New 🝵 Delete	01	Refresh 💼 De	lete Personnel	1
Access Levels	Door Name Device Name Passage Mode Time Zone Operations		Personnel ID	First Name	Last Name
Set Access By Levels	□ <u>192.163.1.28-1</u> 192.168.1.28 24-Hour Accessible 🖉 💁		1	ju	
Set Access By Person			0000	K-TEST	
Set Access By Department			12135		
Interlock			12134	name1	
Linkage				multibio	
Anti-Passback					
First-Person Normally Open	Prompt	1 g	555	fc	
Multi-Person Group			2222	YQV	
Multi-Person Opening Door	Please select the objects you want to opera	al: 🔲	5	уууу	
Verification Mode			3		
Verification Mode Group		- 5	4	We	

Figure 3-80 Delete Person Normally Open Person Configuration

3.4.11 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 other valid combination) will interrupt the procedure and you need to wait 10 seconds to restart verification. It will not open by verification by only one of the combinations.

3.4.11.1 Add (New)

Step 1: Click Access Rule > Multi-Person Group > New to access the following edit interface:

TZKBio CVSecurity		
Access Device >	Access / Access Rule / Multi-Person Group	
🖡 Access Rule 🗸 🗸	Open Door Group (Browse Personnel
Time Zones	Group Name Remarks Q	Personnel ID
Holidays	O Refres → New B Delete	🔿 Refresh 🛛 🗃 Delete Personnel
Access Levels	Group Name Personn Remarks Operations	Personnel ID First Name
Set Access By Levels	□ <u>1</u> 2 Group 1 <u>ℓ</u> <u>2</u> *	1116
Set Access By Person		1115 Zorro
Set Access By Department		
Interlock		
Linkage	New X	
Anti-Passback	Group Name*	
First-Person Normally Open	Remarks	
Multi-Person Group		
Multi-Person Opening Door	OK Cancel	
Verification Mode		

Figure 3-81 Adding A Multi-Person Group

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.

Step 2: Click Add personnel under Related Operations to add personnel to the group.

Step 3: After selecting and adding personnel, click OK to save and return.

Note: A person can only be grouped into one group.

3.4.11.2 Edit

Click **Access Rule** > **Multi-Person Group** > **Edit** after selecting the required section in the interface.

Access Device >	Access / Access Rule / Multi-Person Group	
Access Rule 🗸 🗸	Open Door Group	¢ Browse Personnel
Time Zones	Group Name Remarks Q	Personnel ID
Holidays	⊖ Refresh 🔄 New 💼 Delete	🔾 Refresh 🛛 💼 Delete Personn
Access Levels	Group Name Personn Remarks Operations	Personnel ID First Name
Set Access By Levels	□ <u>1</u> 2 Group 1 🖉 <mark>8</mark> *	1116
Set Access By Person		1115 Zorro
Set Access By Department	Edit X	
Interlock	Group Name"	
Linkage	Remarks Group 1	
Anti-Passback		
First-Person Normally Open	OK Cancel	

Figure 3-82 Edit Multi-Person Group

3.4.11.3 Add Personnel

Click **Access Rule** > **Multi-Person Group** > **Add Personnel** after selecting the required section in the interface.

TKBio CVSecurity	···· · · · · · · · · · · · · · · · · ·	
Access Device >	Access / Access Rule / Multi-Person Group	
🖡 Access Rule 🗸 🗸	Open Door Group	< Browse Personne
Time Zones Holidays Access Levels Set Access By Levels Set Access By Person	Group Name Remarks Q. Q. ○ Refresh → New Belete □ Group Name Personn 1 2 Group 1	Personnel ID O Refresh Personr 1116
Set Access By Department		1115
Linkage Anti-Passback First-Person Normally Open Multi-Person Group	Add Personnel X • Query • Department Department Name • Q • Q • Atternative Alternative Selected(0)	
Multi-Person Opening Door Verification Mode Verification Mode Group Parameters	Personne First Name Last Name Depart 1 ju Departme 0000 K-TEST Departme 12135 Departme 12134 name1 hr No data	

Figure 3-83 Adding A personnel fo<mark>r Mul</mark>ti-Person Group

3.4.11.4 Delete

Click **Access Rule** > **Multi-person group** > **Delete** after selecting the required section in the interface.

TZKBio CVSecurity	*	
Access Device > Acce	sss / Access Rule / Multi-Person Group	
Access Rule V	en Door Group 🤇	Browse
G G	Sroup Name Q Q	Persor
Holidays	O Refresh ∓ New a Delete	O Re
Access Levels	Group Name Personn Remarks Operations	
Set Access By Levels	2 1 2 Group 1	
Set Access By Person		
Set Access By Department		
Interlock	Prompt	
Linkage	Are you sure you want to perform the delete operation?	
Anti-Passback		
First-Person Normally Open	Cancel	
Multi-Person Group		
Multi-Person Opening Door		
Verification Mode		
Verification Mode Group		
Parameters		

Figure 3-84 Delete A Multi-Person Group

3.4.12 Multi-People Open The Door

In a specific scenario, it is necessary for more than one person to be present at the same time to verify their identity before they can open the door through permission verification.

Instructions:

- 1. In an application scenario where, multiple users are required to verify their identities before opening the door, the authentication process is limited to N (no more than 5) by grouping people into groups.
- 2. In practice, if all the personnel to be verified are of the same type or level, it can be verified by multiple people in a single group. If there are different categories or levels of personnel, you can set a certain number of personnel in each group to achieve verification.
- 3. Before the multi-party door verification rule is reached, if the verification fails during the process, wait 10 seconds for the verification again.

3.4.12.1 Add (New)

Step 1: In the **Access Control** module, choose "**Access Rule** > **Multiple Door Opening Personnel Group**" and click **New**. After filling in the corresponding parameters, click **OK** to save the settings.

Step 2: Click "**Add Personnel**" on the right of the list of created multi-person door opening personnel, select the personnel to be added to the group in the pop-up function, and click **OK** to save the settings.

Add Personnel										
Query Department										
Personnel ID Name	Department Name									
Alternative	Selected(0)									
Personne First Name Last Name Department	Personne First Name Last Name Department									
☐ 1 Soluction	>> < << No data									
ОК	Cancel									

Figure 3-85 Adding Multiple Door Openers

Step 3: In the multi-person door opening interface, click **Add**, set permissions for multi-person door opening personnel group.

Step 4: On the page for adding multiple door users, select the specified door, group information for multiple door users, and the number of verification personnel for each group, and click **OK** to save the settings.

			New			
Door Name*	Click to sele	ect				
Combination Name* Number of opening	Group1		•	0	¥	(0)
personnel in each group	Group2		•	0	*	(0)
	Group3		•	0	-	(0)
	Group4		-	0		(0)
	Group5		•	0	-	(0)

Figure 3-86 Adding Multiple Door Openers

Step 5: In the **Access Control** module, choose "**Access Rule** > **Authentication Mode Rule**" and click **Add** to set the access control authentication rule for the corresponding period.

le Name*											Time	Zones*				-		•				
Time					Interval 1							Interval 2							Interval 3			
Date	Star	t Time	End	Time	Door Verific	ation	Personnel Verification	Sta	art Time	En	d Time	Door Verification	on P	Personnel Verification	Start T	ime	End	Time	Door Verifi	cation	Personnel Ve	rificati
Monday	00	: 00	00	: 00		•		00	: 00	00	: 00		•	••••••••••	00 :	00	00	: 00		•		•
Tuesday	00	: 00	00	: 00		•		00	: 00	00	: 00	•	•	······ •	00 :	00	00	: 00		•		•
	00	: 00	00	: 00		•		00	: 00	00	: 00		•		00 :	00	00	: 00				•
	00	: 00	00	: 00		•	······ •	00	: 00	00	: 00		•	••••••	00 :	00	00	: 00		•		•
	00	: 00	00	: 00		•	(00	: 00	00	: 00		•	······	00 :	00	00	: 00		•		•
Saturday	00	: 00	00	: 00		•		00	: 00	00	: 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	1	•	•••••••	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		•		•
ppy Monday's Settin RS485 reader ca	The second second		enerteno	fication	mode, does no	t suppr	ort the personnel verif		mode. Id New		ОК	Canc										

Figure 3-87 Delete A Multi-Person Group

Step 6: Click **Add Door** on the right of the created authentication mode rule, select a door, and set the authentication mode rule for the door.

Ac	id Door ×
Door Name Serial Number	Q &
Alternative	Selected(0)
Door Name Owned Device Serial Number	Door Name Owned Device Serial Number
ProfaceX-1 ProfaceX CN3M2124600	>> < << No data
4 F	
< < 1-1 >> 50 rows per page ▼ OK	Cancel

Figure 3-88 Verification Rule Configuration for Adding Multiple Door Openers

Step 7: click OK to save the settings.

3.4.12.2 Delete

Click **Access Rule** > **Multi-person opening door** > **Delete** after selecting the required section in the interface.

IZKBio CVSecurity	::: ¥					
Access Device >	Access / Access Rule / Multi-F	Person Opening Door				
Access Rule >	Combination Name	Device Name	Door Name	Q Ø		
] ¹ Advanced Functions ~	O Refresh 🖙 New 📑	Î Delete				
Zone	Combination Name	Device Name Door N	umber Door Name	Current Personnel Count Muti-Person Gro	qu	Operations
Reader Define		ZKT_Korea 1	ZKT_Korea-1	2 1(2)		۷ 🗊
Who Is Inside	Zorro	192.188.134.105 1	192.168.134.105-1	2 1(2)		ℓ û
Global Anti-Passback				Prompt		
Global Linkage						
Global Interlock Group				Are you sure you want to perform the delet operation?		
Global Interlock				OK Cancel		
Person Availability						

Figure 3-89 Delete A Multi-Person Group

3.4.13 Verification Mode

Verification Mode:

You can set verification modes for doors and personnel separately in a specified time segment.

3.4.13.1 New

Step 1: Click Access Rule > Verification Mode > New to go to the page for adding a verification mode rule.

	Verification Mode																		De	or 10						
Access Rule 🗸 🗸																										
Time Zones	Rule Name		Q	0																Door Nan	•			Ovre	C Device	
Holdays																										
	ORation St New	奇 Dele	-																	ORetre	187	B Datata	Door			
Access Levels	Rus Name	107	ine Zo	944 (d	Operatio	018														0	par Na	***		Owned	Device	
Set Access By Levels																										
Set Access By Person			_				_					Ne	w.;		_		_				_				×	1
Set Access By Department	Rule Name*			5				1					Time Zi	nes"				General			3					
Interlock	Time				115	1		-		Discourse				and I				Concession in which the		- 200	1	11.2.5			-	
Linkape	Date	- 241	100	Crief Te		Spen all and	- 11	Personal P		10.044	100	Ins		Dente Marine		A COLUMN ST	-	Start T		First 1		Barry Street		6-1	1.00	
	Director	00	00		00 -		•			00	00	00	00	_	•	-	•	00	00	00	00		•		•	
Anti-Passback	Vindenday	00	00		00 -		-		-	00	00	00	00	_	-		-	00	00	00	00	-	-			
First-Person Normally Open	Thenday	00	00		00 -		-	-		00	00	00	00	_		-		00	00	00	00		-	-		
Multi-Person Group	f states	00	00		00 -	_		-		00	00	00	00	-		_			00	00	00					
Multi-Person Opening Door	Salaring	00	00	00	00 -	_		-		00	00	00	00	_	•	_		00	00	00	00	-				
Vertication Made	Sarahay	00	00	00	00 -					00	00	00	00		•		•	00	00	00	00					
Verification Mode Group	Hubbary Types 1	00	00	00 :	00 -		٠	-		00	00	00	00		•		٠	00 -	00	00 :	00					
	Halking Type 2	00	00	00	00 -		•			00	00	.00	00	-		_	•		00	00	00		•		•	
Parameters	Haldoy Type 3	00	00	00	00 -					00	00	00	- 00			_	•	00	00	00	00		٠			
	Copy Monday's Setting	to Other	s Visei	days 🗌																						
	A RS455 reader star	ony ful	er Part	tor writes	iun mod	k dies no	A REPORT	of the period	Vel verili	nation me	ode -															

Figure 3-90 Add Verification mode

Step 2: Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.

Step 3: Click OK to finish the setting.

On the list page, you can add or delete doors in the verification mode rule.

3.4.13.2 Verification Mode Group

You can set verification modes for doors and personnel separately in a specified time segment.

Steps:

Step 1: Click **Access Rule** > **Verification Mode** > **New** to go to the page for adding a verification mode rule.

ule name*																Zones*				-			۲				
Time						Interval 1										iterval 2								nterval 3			
Date	Sta	d ffe	10	En	d Time	Door V	crificatio	n Perso	nnel Verificati	on S	tart	Time		nd Ti	me	Door Ventic	ation	Personnel Veri	fication	Star	Time	End	Time	Door Verific	ation	ersonnel Veni	2
	00	: 1	00	00	: 00		10.0		Y	00	1	00	00		00		۲		۲	00	: 00	00	: 00		۲		
	00		00	00	: 00		28 - 8 1	-	T	00	1	00	00		00		۲			00	: 00	00	: 00				
	00	: 1	00	00	: 00		- 1		T	00) :	00	00		00		۳		۳	00	: 00	00	: 00		T		
Thursday	00	2.1	00	00	: 00		.			00	1.1	00	00		00		۲		۲	00	: 00	00	: 00				
Friday	00		00	00	: 00		- 1	·	T	00	1.1	00	00		00		۲		۲	00	: 00	00	: 00		۳		
Saturday	00		00	00	: 00		- 1		¥	00	6.3	00	00		00		۲		۲	00	: 00	00	: 00		۲		
Sunday	00	: ()	00	00	: 00				T	00	1	00	00		00		۳		۳	00	: 00	00	: 00		•		
Holiday Type 1	00		00	00	: 00			·	¥	00	0.3	00	00		00		۲		۳	00	: 00	00	: 00		۲		
Holiday Type 2	00		00	00	: 00		17 11	- 1		00	1.1	00	00		00		•		۲	00	: 00	00	: 00		۲		
Holiday Type 3	00	2.1	00	00	: 00		2 10		¥	00	1	00	00		00		۳		۲	00	: 00	00	: 00				
opy Monday's Settin	g to Oth	ers V	Veekda	iys: 🗌																							

Figure 3-91 Add Verification mode Group

Step 2: Set the following parameters: Select a rule name (not repeatable), the time segment, and verification mode for a door or person in each time segment.

Step 3: Click OK to finish the setting.

On the list page, you can add or delete doors in the verification mode rule.

Note: If a rule includes the verification mode for personnel, you cannot select doors with the RS485 readers when adding doors. You can modify only the configuration on the reader setting page before adding doors.

Verification Mode Group:

Set appropriate personnel for configured verification mode rule.

3.4.14 Parameters

Click **Access Rule** > **Parameters** to enter the parameter setting interface:

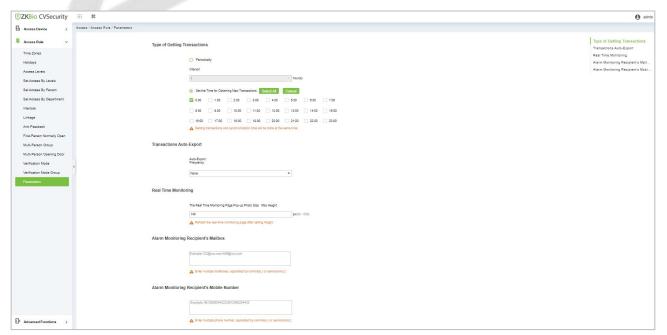


Figure 3-92 Add Parameters

Type of Getting Transactions:

• Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

• Set the Time for Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

• Transaction Auto-Export

The user can choose the export frequency and the data to be exported each time. If the export frequency is selected as **"By day"**, you must set the time to export the data. You must also select the mode of export. It can be daily transactions or all the system data (30000 data units can be sent at a time. We can customize the data that we need to export from custom report 1 and custom report 2.

If the export frequency is selected as **"By Month"**, you must select the day to export the data. It can be the first day of the month or you can specify any particular date. Then select the export frequency as Daily Data or all System data. Finally, add the recipient's mail address to send the transaction data.

Transactions Auto-	Export		
	Auto-Export Frequency		
	None		

Figure 3-93 Transaction Auto Export

The Real Time Monitoring Page Pop-up Staff Photo Size

When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

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

Figure 3-94 Real Time Monitoring

Alarm Monitoring Recipient Mailbox

The system will send email to alarm monitoring recipient's mailbox if there is any event.

Example:123@xxxx.com;456@xxxx.com	

Figure 3-95 Alarm Monitoring Recipient Mailbox

• Alarm Monitoring Recipient Mobile Number

The system will send alarm monitoring recipients to mobile, if there is any event.

Example: 8813606044222;8612585254433	

Figure 3-96 Alarm Monitoring Recipient Mobile Number

3.5 Advanced Function

Advanced access control is optional. You must obtain permission to activate the advanced access control.

In addition to the global linkage function, enable the background authentication function first.

The access control area must be defined when advanced functions such as global Anti-Passback are used.

3.5.1 Entrance Guard Area(Zone)

Divide areas and define access control areas. The access control area is reserved for advanced access control but not for system management.

This section describes Step in ZKBio CVSecurity to add an access control area.

3.5.1.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Advanced function > zone" and click New.

Step 2: On the page that is displayed, set related parameters, and click OK.

	Ν	lew	×
Zone Code* Name*			
Remarks			
	OK	Cancel	

Figure 3-97 Page for Adding Access Control Areas

3.5.1.2 Delete

Click **Advanced function** > **Zone** > **Delete** after selecting the required section in the interface.

TZKBio CVSecurity	::: %			
Access Device >	Access / Advanced Functions / Zone			
Access Rule >	Zone Code	Name Q Q		
Advanced Functions 🗸	C Refresh 🖅 New 📋 Delete	What Rules Apply Inside		
Zone	Zone Code Name	Remarks Operation	ns	
Reader Define	1 Outside	Outside 💼		
Who Is Inside	🔲 <u>2</u> empty	2 0		
Global Anti-Passback	🖬 🧕 4th floor	2 🖬		
Global Linkage	🔲 🛓 5th floor	2 🖬		
Global Interlock Group				
Global Interlock				
Person Availability				
Occupancy Control				
	0			Prompt
				Are you sure you want to perform the delete operation?
				OK Cancel
				Cancer

Figure 3-98 Delete Access Control Areas

3.5.1.3 What rules Apply Inside

Click **What rules inside** after selecting the required section in the interface we can check the rules are applied for the particular zone.

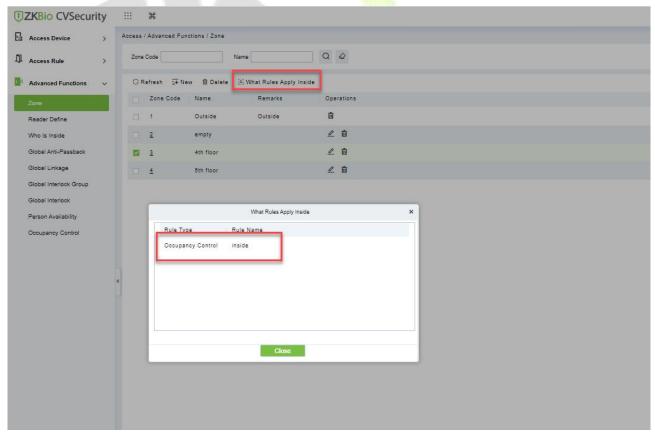


Figure 3-99 What Rules Apply Inside

3.5.2 Reader Definition

This function is configured based on the access control area. To use the global Anti-Passback function, you must define the read head.

This section describes the Step of adding a Reader definition in ZKBio CVSecurity.

3.5.2.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose " Advanced function > Reader Define" and click New

Step 2: On the page that is displayed, set related parameters and click **OK**.

	New	×
Reader Name* Goes From* Goes To*		
	OK Cancel	

Figure 3- 100 Page for Adding a Reader

3.5.2.2 Batch New

Step 1: Click **Advanced Functions** > **Reader Define** > **Batch New** to enter the batch add interface:

TZKBio CVSecurity	
Access Device >	Access / Advanced Functions / Reader Define
Access Rule	Reader Name Q Q
🚺 Advanced Functions 🗸 🗸	O Refresh ∓ New ∓ Batch New 1 Delete
Zone	Reader Name Goes From Goes To Operations
Reader Define	
Who Is Inside	
Global Anti-Passback	Batch New X
Global Linkage	
Global Interlock Group	Select Reader* Add Select All Unselect All Please add reader
Global Interlock	
Person Availability	
Occupancy Control	
	e Goes From*
	Goes To*
	Cancel

Figure 3-101 Batch New

Step 2: Click Add, select Reader(s) and move towards right and click OK.

ame		Owned Devi	се			Se	rial Number		$\mathbf{Q} \otimes$
ne cu erna	irrent query condition	1s: None			:	Selecte	ed(1)		
	Name	Owned Device	Serial Number				Name	Owned Device	Serial Number
	192.168.12.155-2-In 192.168.12.155-3-In 192.168.12.155-3-Ou 192.168.12.155-4-In 192.168.12.155-4-Ou 192.168.214.74-1-In 192.168.214.74-1-Ou	192.168.12.155 192.168.12.155 192.168.12.155 192.168.12.155 192.168.214.74	AK1F173460006 AK1F173460006 AK1F173460006 AK1F173460006 AK1F173460006 3763161600001 3763161600001		>		192.168.12.155-1-Ou	192.168.12.155	AK1F173460006
5 4	: 1-9 > > 50	rows per page 👻	Total of 9 record	S	i i	Can	cel		

Figure 3- 102 Add Reader Define

Step 3: Set Goes from and Goes to as required and press OK.

3.5.2.3 Delete

In the Access > Advanced Functions > Reader Define, click Delete button under Operations. Click OK to delete.

TZKBio CVSecurity	HH %
Access Device >	Access / Advanced Functions / Reader Define
Access Rule >	Reader Name Q Q
Advanced Functions 🗸 🗸	O Refresh ∓ New ∓ Batch New B Delete
Zone	Reader Name Coes From Goes To Operations
Reader Define	ZKT Korez-1-In 4th floor 5th floor 🖉 🔒
Who Is Inside	
Global Anti-Passback	
Global Linkage	
Global Interlock Group	
Global Interlock	
Person Availability	
Occupancy Control	
Muster Point	
Muster Point Report	Prompt
	Are you sure you want to perform the delete operation?

Figure 3-103 Delete Reader Define

3.5.3 Who is inside

After entering the access control area, users can use this function to view the personnel in the access control area. You can choose the access control area tree to view the personnel in the corresponding access control area.

This section describes how to view the Steps of people in a region in ZKBio CVSecurity.

Operation Step:

Step 1: In the Access Control module, choose "Advanced Function > View Personnel in the Area"

Step 2: On the page for viewing personnel in a region, you can select the area on the left to view and delete personnel in the area, as shown in Figure 3-84.

ŪΖ	KBio CVSecurity III	*	😫 admin 👻
G	Access / Advanced Functions / Who I	s Inside	
Ţ1	Personnel ID	Name Department Q	
•	Zone	O Refresh 🗑 Delete Personnel ⊥ Export	
ı.	▲ 🖻 All 🔋 2(0)	Personnel ID First Name Last Name Department Last Access Time Last Access Reader	
ĸ			

Figure 3- 104 View Area Personnel Page

3.5.3.1 Delete personnel

Select personnel ID, click **Delete**, and click **OK** to delete the level name.

TKBio CVSecurity	::: ¥	
Access Device >	Access / Advanced Functions / Who Is	s Inside
Access Rule >	Personnel ID	Name Department Q
Advanced Functions V	Zone	○ Refresh 🕅 Delete Personnel 1 Export
Zone	* 🗗 All	Personnel ID First Name Last Name Department Last Access Time Last Access Reader
Reader Define	empty(0) 4th floor(0)	
Who Is Inside	5th floor(0)	
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability		
Occupancy Control		

Figure 3-105 Delete Who Is Inside

3.5.3.2 Export

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

The File Type	EXCEL File	~			
Export Mode	All data (Can explanation)	port up to	40000 data)		
	◯ Select the amou	nt of data	a to export (Can ex	c <mark>port u</mark> p	to 40000 data)
	From the article	1	Strip, is derived	100	Data
			-12		

Figure 3- 106 Export

					ZKTECO					
					Device					
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.303 Jun 16 2017

Figure 3- 107 Export Who is Inside

3.5.4 Global Anti-Passback

Global Anti-Passback Settings can be carried out across devices, and only push devices support global Anti-Passback functions. This function supports logical Anti-Passback, timed Anti-Passback and timed logical Anti-Passback, and can be configured for specific personnel.

This section describes the Step configuration of global Anti-Passback in ZKBio CVSecurity.

The Premise Condition:

- 1. Background authentication has been enabled on the device.
- 2. Set the access control area and read head definition.

3.5.4.1 Add (New)

Operation Step:

Step 1: In the **Access Control** module, choose "**Advanced Access Control** > **Global Anti-Passback**" and Click **New.**

UZKBio CVSecurity		θ
Access Device >	Access / Advanced Functions / Global Anti-Passback	
Access Rule >	Otobal Anti-Passback	¢ Person
Advanced Functions 🗸	Rule Name Zone More * Q Q	Personal D Name More * Q Q
Zone	O Refresh 🐨 New 🖞 Delete	O Refresh 🖹 Delete Personnel
Reader Define	Rule Name Zone Anti-Pasab. Perso. Operations	Personnel ID First Name Last Name Department
Who is inside	🔲 aaaa Sin floor Timed Anti-Pai All Person 🖉	
Global Anti-Passiback		
Global Linkage		
Global Interlock Group		
Global Interlock		Nev X
Person Availability	Rule Name*	
Occupancy Control	Zone" The following doors control	
Muster Point	access in and out of the	
Muster Point Report	Zone Anti-Pessback Type"	Logial Anti-Pantiaski *
	 Lockout Duration 	minute(1-600)
	Reset Anti-Pasaback Status Anti-Pasaback Time Reset	anna a krósok
		Al Pesonel
		No data
		NO DATA
		Cancel

Figure 3- 108 Add Global Anti-Passback

Step 2: On the page for adding global Anti-Passback Settings, set related parameters and click **OK**, as shown in Figure 3-102. For parameter description, see Table 3-16.

Parameter	Description
Rule Name	The value can contain a maximum of 30 characters.
Entrance Guard Area	Select an option from the access control area drop-down list box.
The Door List Controls Access to The Access Control Area	The corresponding door information is displayed. The same gate shall not be used to control two independent Anti-Passback boundaries.
Anti-Passback Type	It contains three types of Anti-Passback: logic Anti-Passback, timing Anti- Passback and timing logic Anti-Passback. instructions Logical Anti-Passback: strictly follow the "one in, one out" rule in the Anti- Passback area, otherwise the verification will not open Timed Anti-Passback: A user can enter the Anti-Passback area only once within a specified period of time. After the specified period expires, the user's status will be cleared and the user can enter the Anti-Passback area again Timed logical Anti-Passback: the user can open the door normally only after following the exit and entry rules of logical Anti-Passback.Timing logic antisubmarine is only used in abnormal situations. For example: if the logical Anti-Passback time is set and the personnel follows others out, the personnel cannot swipe the card machine within the set locking time. The Anti-Passback state will be reset after the set locking time, and the traffic can continue.
The Locking Time	You can set the locking period only when you select timing Anti-Passback or logic Anti-Passback type.
Reset Global Anti-Passback Status	Clear the Anti-Passback status of personnel in the system and restore the initialization status.
Reset Anti-Passback Time	The reset time can be selected only when reset global Anti-Passback status is selected. When it is time to reset Anti-Passback, the system will automatically clear the Anti-Passback status of all personnel in the access control area.
Applied	All personnel, selected personnel, except selected personnel three types: instructions All personnel: This type can only be edited. Personnel selection is not supported Selected Personnel: If you select this type, you can add personnel. This Anti-Passback type takes effect only for these personnel. Personnel other than selected: Select this type, add personnel, this Anti- Passback type will only take effect for personnel other than selected. Table 3- 16 Global Anti-Passback Settings

Table 3-16 Global Anti-Passback Settings

3.5.4.2 Delete

In the Access > Advanced Functions > Global Anti-Pass, click Delete button under Operations. Click OK to delete.

TZKBio CVSecurity		
Access Device >	Access / Advanced Functions / Global Anti-Passback	
Access Rule >	Global Anti-Passback	< Person
Advanced Functions 🗸 🗸	Rule Name Zone More * Q 2	Personnel ID Name
Zone	⊖ Refresh IF New 🔒 Delete	🔿 Refresh 🛛 📋 Delete Personnel
Reader Define	🜌 Rule Name Zone Anti-Passb Perso Operations	Personnel ID First Name Last Name
Who Is Inside	📴 aaaa 5th floor Timed Anti-Pas All Person 🖉	
Global Linkage		
Global Interlock Group	Prompt	
Global Interlock	Are you sure you want to perform the delete	
Person Availability	operation?	
Occupancy Control	OK Cancel	

Figure 3- 109 Delete Global Anti-Passback

3.5.5 Global Linkage

The global linkage function can be set across devices. Only the push device supports the global linkage function

This section describes how to configure Step for global linkage in ZKBio CVSecurity.

3.5.5.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Advanced Function! > Global Linkage" and Click New.

UZKBio CVSecurity				
Access Device >	Access / Advanced Functions / Global Linkage			
I Access Rule >	Giobal Linkage	٠	Browse Personnel	
Advanced Functions	Linkage Name Q		Personnel ID Name	Nore* Q Q
Zone	⊙Refresh 🕞 New 🗄 Delete 🗸 Enable © Disable		O Refresh 🕆 🕆 Delete Personnel	
Reader Define	Linkag. Linkage Trigger Co., Enable Perso., Operations		Personnel ID First Name Last Name Department	t
Who is inside	🗆 1831 Normal Verify Open 🔍 Any 🖉 🗟			
Olobal Anti-Passback	🗌 🔠 Any 🖉 🗃	New	×	
Global Linkage		Linkage Name" Apply to all personnel		
Global Interlock Group		Linkage Trigger Conditions" Add Input Point" Add		
Olobal Interlock				
Person Availability				
Occupancy Control Muster Point				
Muster Point Report				
aluster moint report	1			
			E-mail Linkage Voice Prompts	
		Door Add Auxiliary Output Add		
				, <u>A</u> ,
				Ê
				No data
		Action type" Close Action type"	Close •	
		4	•	
		Sinve and New OK Car	roel	

Figure 3-110 Add Global Linkage

Step 2: On the page for adding global linkage, set related parameters and tap **OK**, as shown in Figure 3-104. Table 3-17 describes the parameter description to complete global linkage Settings.

Parameter	Operation Instructions
Linkage Name	You can customize the linkage name for easy query
It Works for Everyone	After this parameter is selected, the linkage Settings take effect on all personnel

Parameter	Operation Instructions
Linkage Trigger Condition	Select the condition triggered by the linkage Operation, that is, the event type generated by the selected device
Input Point	Select the input point to set device input
Dots	Select the output point to set device output Set the output action type: close, open, normally open. Sets the delay time if the output action is on.
Video Linkage	Pop-up video and display duration: Select pop-up video on the real-time monitoring screen and set the pop-up duration. Video recording and Video Duration: Select Video recording to set the video duration. Capture: Set linkage action whether to take a photo: If a photo is taken, you also need to set whether to pop up on the real-time monitoring interface and the display duration.
Valid Time	The reset time can be selected only when reset global Anti-Passback status is selected When it is time to reset Anti-Passback, the system will automatically clear the Anti-Passback status of all personnel in the access control area.
Mail	Set the email address that receives the linkage content when a linkage event occurs

Table 3-17 Global Linkage Parameters

Apply to all personnel: If this option is selected, this linkage setting is effective for all personnel.

Active Time: Set the active time of the linkage setting.

Step 3: Choose Global Linkage trigger conditions, the input point (System will filter devices according to the choice in first step) and the output point, Set up linkage action. For more details about these parameters, please refer to Linkage Setting.

Solution Select multiple Door Events, but "Fail to connect server", "Recover connection" and "Device connection off" will be filtered automatically from Door Event.

Step 4: Click OK to save and quit. The added Global Linkage will display in the list.

3.5.5.2 Delete

In the **Access > Advanced Functions > Global Linkage**, click **Delete** button under Operations. Click **OK** to delete.

TKBio CVSecurity	111 H
Access Device >	Access / Advanced Functions / Global Linkage
♫ Access Rule >	Global Linkage
Advanced Functions 🗸	Linkage Name
Zone	© Refresh 🐼 New 👔 Delete 🗸 Enable 🛇 Disable
Reader Define	Linkag Linkage Trigger Co Enable Perso Operations
Who is inside	🔯 🗚 Normal Verify Open 🔍 Any 🖉 🗃
Global Anti-Passback	
Global Linkage	
Global Interlock Group	Prompt
Global Interlock	Are you sure you want to perform the delete
Person Availability	operation?
Occupancy Control	OK Cancel

Figure 3-111 Delete Global Linkage

3.5.5.3 Enable

After the device is enabled, the upload and download of data are enabled normally. (When the device is enabled, users can choose whether it is a registration device or not).

TZKBio CVSecurity		
Access Device >	Access / Advanced Functions / Global Linkage	
D Access Rule >	Global Linkage	Browse Personnel
Advanced Functions V	Linkage Name	Personnel ID N
Zone	⊖ Refresh 🖅 New 🖹 Delete 🗸 Enable S Disable	C Refresh 🖀 Delete Personnel
Reader Define	Linkag Linkage Trigger Co Enable Perso Operations	Personnel ID First Name L
Who Is Inside	🜌 🗚 Normal Verify Open 🖉 Any 🖉 🛱	
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability		
Occupancy Control		
	Prompt	
	e. Are you want to perform the Enable oper	tion?
	Cancel	

Figure 3- 112 Enable Global Linkage

3.5.5.4 Disable

After the device is disabled, the device is not allowed to upload and send data.

TZKBio CVSecurity	···· *	
Access Device >	Access / Advanced Functions / Global Linkage	
D Access Rule >	Global Linkage c	Browse Personnel
Advanced Functions 🗸 🗸	Liniage Name Q Ø	Personnel ID Name
Zone	⊖Refresh ∓New 🛱 Delete 🗸 Enable 🛇 Disable	C Refresh 👔 Delete Personnel
Reader Define	Z Linkag Linkage Trigger Co Enable Perso Operations	Personnel ID First Name Last Name
Who Is Inside	📴 🗛 Normal Verify Open 🔍 Any 🖉 🛍	
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability		
Occupancy Control		
	Prompt	-
	Are you want to perform the Disable operation	-
	Are you wait to perform the Disable operato	112
	Cancel	

Figure 3- 113 Disable Global Linkage

3.5.6 The Global Interlock Group

Global interlocking the global interlocking function can be set across devices. Only the push device supports global interlocking. By setting the global interlock group to group doors, you can set global interlock.

This section describes the Step configuration of global interlock in ZKBio CVSecurity.

The Premise Condition:

Background authentication has been enabled on the device.

3.5.6.1 Add (New)

Operation Step:

Step 1: In the Access Control module,	choose "Adva	anced Access Control	> Global Interlock Group"
and Click New .			

Step 2: On the page for adding a global interlock group, set related parameters and Click **OK**, as shown in Figure 3-93.

	New	×
Group Name* Remarks Group Interlock		
	OK Cancel	

Figure 3-114 Global Interlock Group Settings Screen

Parameter How to set up	
Group Name	Any combination of up to 30 characters that cannot be identical to an existing group name
Group Interlock	Select the configured interlo <mark>ck ru</mark> le.

Table 3-18 Description of Advance Global Interlock

Step 3: On the global interlock group page, tap Add Door next to the configured group name on the left, as shown in Figure 3-94.

Add I	Door ×
Door Name Serial Number	Q &
Alternative	Selected(0)
Door Name Owned Device Serial Number	Door Name Owned Device Serial Number
	>> < <> No data
I< < 1-1 > >I 50 rows per page ▼ OK	Cancel

Figure 3-115 Adding A Door to A Global Interlock Group

3.5.6.2 Delete

In the Access > Advanced Functions > Global Interlock Group, click Delete button under Operations. Click OK to delete.

TZKBio CVSecurity	····· ··· ··· ··· ··· ···· ··· ··· ···		
Access Device >	Access / Advanced Functions / Global Interlock Group		
Access Rule >	Global Interlock Group	¢ Door	
Advanced Functions 🗸	Girop Name Remarks Q Q	Door Name	Owned Device Q
Zone	⊖ Refresh III New B Delete	🔾 Refresh 🛛 📋 Delete Doo	e and a second se
Reader Define	Group Name Door Count Group Inter Remarks Operations	Door Name	Owned Device
Who Is Inside	🖾 azof 0 🗢 az 🖉 🖪		
Global Anti-Passback			
Global Linkage			
Global Interlock Group	Prompt		
Global Interlock	Are you sure you want to perform the delete operation?		
Person Availability	operation?		
Occupancy Control	OK		
			No data

Figure 3-116 Delete A Door to A Global Interlock Group

3.5.7 The Global Interlock

3.5.7.1 Add (New)

Step 1: In the Access Control module, choose "Advanced Access Control > Global Interlock" and Click New.

On the page for adding global interlock, set related parameters and Click OK, for example

Step 2: The global interlock name is set.

		New	×
/	Name*		
	Remarks		
		OK Cancel	

Figure 3-117 Global Interlock Settings Screen

Parameter	How to set up		
Name	Any combination of up to 30 characters that cannot be identical to an existing name		
Remark	Select the configured interlock rule.		
	select the compared interior rate.		

Table 3-17 Description of Access Control Right Groups

Step 3: On the global interlock screen, click **Add** Group next to the configured global interlock on the left, as shown in Figure 3-112.

	Add Group			×
Group Name Remarks		Q &		
Alternative		Selected(0)		
Group Name Remarks		Group Name	Remarks	
☐ 1	>> < <		No data	
IK K 1-1 > >I 50 rows per page ▼ OK		Cancel		

Figure 3-118 Page for Adding Global Interlock Groups

3.5.7.2 Delete

In the Access > Advanced Functions > Global Interlock, click Delete button under Operations. Click OK to delete.

TZKBio CVSecurity		
Access Device >	Access / Advanced Functions / Global Interlock	
Access Rule	Global Interlock c	Global Interlock Group
Advanced Functions 🗸	Name Remarks Q Q	Group Name Remarks
Zone	O Refresh ∓ New 🔒 Delete	C Refresh 🖀 Delete Group
Reader Define	Name Remarks Operations	Group Name Remarks
Who Is Inside	🖬 <u>assti</u> aas 🖉 😣	asdf aa
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability		
Occupancy Control		
	Prompt	
	Are you sure you want to perform the delet operation?	
	Cancel	

Figure 3-119 Page for Adding Global Interlock Groups

3.5.8 Personnel Availability

It is used to restrict the expiration date, the number of days after the first use, and the number of times the user passes the specified advanced access control area.

The Premise Condition:

- 1. Background authentication has been enabled on the device
- 2. Set the access control area and read head definition.

3.5.8.1 Add (New)

Operation Step:

Step 1: In the Access Control module, choose "Advanced Access Control >Personnel Avaliability> Set Access Control Area Properties", and Click New.

Step 2: On the Access Control Area Properties page, set related parameters and Click OK.

Access / Advanced Functions / Pe	rson Availability				
Availability Name	Q &				
⊖ Refresh ∓ New 💼 De	lete 🕼 Set Zone Prop	arties			
Availability Name	Zone	Zone property name	Use	Detail	Operations
		Availability Name" Zone" Zone Properties"	New	•	×
		Save and New	ок	Cancel	

Figure 3- 120 Page for Setting Access Area Properties

Step 3: In the properties of the **access control area** that has been set, click **Add** Personnel on the left to add the corresponding personnel, and Click **OK**.

Add	personnel ×
Query Opepartment	
Personnel ID Name	Card Number More * Q 🖉
Alternative	Selected(0)
Personnel ID First Name Last Name Card Nu	Personnel ID First Name Last Name Card Nu
	»»
	>
No data	~
	No data
<	
I< < 0 > >I 50 rows per page ▼	٠
ОК	Cancel
	Query Department Personnel ID Alternative Personnel ID First Name Last Name Card Nu No data K 50 rows per page *

Figure 3- 121 Personnel Availability Add Personnel Settings Screen

Step 4: On the personnel validity screen, tap Add, set related parameters, and tap OK.

	New		×
Availability Name* Zone* Zone Properties*		▼ ▼	
Save and New	ОК	Cancel	

Figure 3-122 Personnel Validity Setting Screen

3.5.8.2 Delete

In the Access > Advanced Functions > Personnel Availability, click Delete button under Operations. Click OK to delete.

Access Device >	Access / Advanced Functions / Person Availability		
Access Rule >	Person Availability	۲.	Browse Personnel
Advanced Functions 🗸	Availability Name Q		Personnel ID
Zone	C Refresh 🖙 New 🔒 Delete		🔾 Refresh 🛛 📋 Del
Reader Define	Availabi Zone Use Detail Operations		Personne
Who Is Inside	🕎 <u>ask</u> 4th floor Valid Date Valid Until 2022-07-25 14:22:0 🏞 🖉		
Global Anti-Passback	🗌 <u>test</u> Outside Valid Date Valid Until 2022-08-30 17/35:0 🐣 🖉		
Global Linkage			
Global Interlock Group			
Global Interlock			
Person Availability			
Occupancy Control			
		Prompt	
	•	Are you sure you want to perform the delet operation?	e
		OK Cancel	1

Figure 3- 123 Delete Personnel Validity Setting

3.5.9 Occupancy Control

Control the maximum/minimum capacity of the area in the Advanced Access Control.

This section describes the Step configuration for population control in ZKBio CVSecurity.

The Premise Condition

- 1. Background authentication has been enabled on the device.
- 2. Set the access control area and read head definition.

3.5.9.1 Add (New)

Operation Step

Step 1: In the Access Control module, choose "Advanced Function> Occupancy" and Click New.

Step 2: On the Add Person control screen, set related parameters and click OK.

	New		×
Name* Zone* Maximum Capacity			
Minimum Capacity Minimum Capacity No capacity value means no	limitation.		
Save and New	ОК	Cancel	

Figure 3-124 Configuring the People Counting Function

3.5.9.2 Delete

In the Access > Advanced Functions > Occupancy Control, click Delete button under Operations. Click OK to delete.

TZKBio CVSecurity	::: ¥					
Access Device >	Access / Advanced Fu	nctions / Occupancy Contro	oli			
Access Rule >	Name	Q &				
Advanced Functions 🗸	◯ Refresh 📴 N	lew 🔒 Delete				
Zone	Name	Zone	Maximum Capacity	Minimum Capacity	Operations	
Reader Define	TEST OCC	empty	5	Unlimited	2 1	
Who is inside	inside.	4th floor	20	1	2 1	
Global Anti-Passback						
Global Linkage						
Global Interlock Group						
Global Interlock						
Person Availability						
Occupancy Control						
						Prompt
	×					Are you sure you want to perform the delete operation?
						operation?
						OK Cancel

Figure 3- 125 Delete Configuring the People Counting Function

3.5.10 Muster Point

Designate the access control device of a certain place as the Muster Point. When an emergency event (such as a fire alarm) occurs, the linkage triggers the activation of the Muster Point to open the door, and the AC Device is used to count the escape of personnel, and quickly identify the escaped personnel and dangerous personnel.

3.5.10.1 Add (New)

Select the access control devices as the equipment of Muster Point, and assign the corresponding department. Note: The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

Operation Steps:

Step 1: Set device as Muster Point, go to "Access Control > Advanced Functions > Muster Point > New: Sign device to the point".

cess / Advanced Functions / Muster Point		
uster Point	<	Department
Name Q	New	× Name Q
⊖ Refresh 🖅 New 💼 Delete 🗸 Activate	Name* Test	🗇 Delete Department
Name Sign Point	Sign Point* Add	artment Department Name Parent Department Name
Outside1 192.168.134.23-1-Out	192.168.134.23-1-In	⊘ Department Name
	Save and New OK Ca	incel

Figure 3-126 Sign Point

Step 2: Click add department to the point.

A	dd Department 🗙
Department Name	
Alternative	Selected(0) Department Department Name Parent Department
1 Department Name	>> < <<
< < 1-1 > > 50 rows per page ₹ Total of 1 records	
ОК	Cancel

Figure 3- 127 Add Department

Step 3: Set Global Linkage: set Linkage Trigger Conditions and Input Point, Selete Muster Point as an output action.

Access / Advanced Functions / Global Linkage		New	×
Global Linkage	Linkage Name* Muster Point	Apply to all personnel	
Linkage Name Q	Linkage Trigger Conditions* <u>Add</u>	Input Point* <u>Add</u> 192.168.134.23-1	More -
🔾 Refresh 🎞 New 💼 Delete 🗸 En			
Linkag Linkage Trigger Co Er			nt
<u>test</u> Emergency Password			
ĸ	Linkage Voice Prompts Send SMS Muster Point Outside1 Test	Digifort Line	Muster Point
i< < 1-1 > >i 50 rows per pa	Save and New	OK Cancel	/0 Page

Figure 3- 128 Global Linkage

Solution Note: Before you use global linkage, you must confirm that your device has enable background authentication.

Device Name		Set Bg-Verification Options	×	
	Selected Device			
🔾 Refresh ∓ New 💼 🕻	The devices which have enable	led background verification : 192.168.134.23		*
Device Name	Serial I			ware Version
<u>192.168.134.23</u>	575820			170-NF-Ver1.8.17
	Set Bg-Verification Options			
	Background Verification	Enable		
	If the device is offline	Standard Access Level 🔻		
	Total Progress			
	Hidden Info	Start	Close	
			*	

Figure 3- 129 Enable Bg-Verification Options.

3.5.10.2 Activated

When the linkage event is triggered, the door is opened remotely and the Muster Point would be actived.

JZKBio CVSecurity	::: ¥									e admin
Access Device 🗸 🗸	Access / Access Device	/ Real-Time Mon	litoring							
Device	Area	 Status 	• Device	Name	More - 🖉					
I/O Board	Door Auxilia	ary Input A	Auxiliary Output							
Door	Remote Opening	Remote Cl	losing 🗳 Cancel Alarm 🖙 A	ctivate Lockdown	G Deactivate Lockdown	··· More ··				
Reader	E9									
Auxiliary Input	192,168,13									
Auxiliary Output	4.23-1									
Event Type										
Daylight Saving Time										
Device Monitoring	Current Total:1	Online:1	🕨 Disable:0 单 Offline:0 🤣 Unknown:I	0 Do	or Name					
Real-Time Monitoring	Real-Time Events									
	Real-Time Lyenta									
Alarm Monitoring	Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verifica	ssage Tip
Alarm Monitoring Map			Device 192.168.134.23(5758204800	ALC: NAME OF A	Event Description	Card Number	Person	Reader Name Other	Verifica Other	ssage Tip
Мар	Time	Area Name		192.168.134.23-1		Card Number	Person 1(aaaaa)		Verifica Other	ssage Tip
Мар	Time 2022-07-07 14:18:33	Area Name Area Name	192.168.134.23(5758204800	192.168.134.23-1 192.168.134.23-1	Remote Opening	Card Number		Other	Verifica Other I Only Pa	ssage Tip
Мар	Time 2022-07-07 14:18:33 2022-07-07 14:18:28	Area Name Area Name	192.168.134.23(5758204800 192.168.134.23(5758204800	192.168.134.23-1 192.168.134.23-1	Remote Opening Trigger Global Linkage	Card Number	1(aaaaa)	Other 192.168.134.23-1-Ou 192.168.134.23-1-Ou	Verifica Other I Only Pa	1(aaaa)

Figure 3- 130 Real-Time Monitoring

Access / Advanced Functions / Muster Point			
Muster Point		<	Department
Name Q			Department Name Q
◯ Refresh ∓ New 🖻 Delete 🗸 Activate 🛇 Cancel			🔾 Refresh 💼 Delete Department
Name Sign Point	Activate	Operations	Department Department Name Parent Department Name
Outside1 192.168.134.23-1-Out	0	28	1 Department Name
Test 192.168.134.23-1-In	0	28	
««			

Figure 3-131 Muster Point

3.5.10.3 Delete

In the **Access > Advanced Functions > Muster Point**, click **Delete** button under Operations. Click **OK** to delete.

TZKBio CVSecurity	HH #	
Access Device >	Access / Advanced Functions / Muster Point	
Access Rule	Muster Point ¢	Department
Advanced Functions 🗸 🗸	Name Q Q	Department Name (
Zone	© Refresh 🐺 New 🖀 Delete VActivate 🛇 Cancel	🔿 Refresh 🛛 🔒 Delete Department
Reader Define	Name Sign Point Activate Operations	Department Department Name
Who Is Inside	Test 192.168.134.101-1-in.192.168.184.101-1-Out 🗣 🖉 🖉	
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability		
Occupancy Control		
Muster Point		
Muster Point Report	Prompt	
	Are you sure you want to perform the delet	
	Are you sure you wan to perform the dele operation?	
	Cancel)

Figure 3-132 Delete Muster Point

3.5.10.4 Cancel

In the Access > Advanced Functions > Muster Point, click Cancel button under Operations. Click OK to cancel.

TZKBio CVSecurity		
Access Device >	Access / Advanced Functions / Muster Point	
Access Rule >	Muster Point <	Department
Advanced Functions 🗸	Name Q Q	Department Name Q
Zone	⊖ Refresh 🖼 New 👔 Delete 🗸 Activate 🚫 Cancel	C Refresh 📋 Delete Department
Reader Define	Name Sign Point Activate Operations	Department Department Name Parent D
Who Is Inside	Test 192 188 134 101-1-in, 192 188 134 101-1-Out	
Global Anti-Passback		
Global Linkage		
Global Interlock Group		
Global Interlock		
Person Availability Occupancy Control		
Muster Point		
Muster Point Report		
	Prompt	
	Are you want to perform the Canoel operation	n?
	OK	

Figure 3-133 Cancel Muster Point

3.5.11 Muster Point Setting

Select the access control devices as the equipment of Muster Point and assign the corresponding department. Note: The equipment selected is equipped with safe house conditions to facilitate evacuation of personnel in the department.

Operation Steps:

Step 1: Set device as Muster Pointsetting, go to "Access Control > Advanced Functions > Muster Point Setting".

ta Analysis	C Refresh	Time From 2022-04-07 0	0:00:00 To 2022-0	07-07 23:59:59	Sign Point	Мо	re- Q 🖉		
		🖾 Sign In Manually	🗏 Generate Repor	ts <u>↑</u> Export	💼 Clear All Data				
5.2	596	'ime	Personnel ID	First Name	Last Name	Department Name	Sign Point	Muster Point	Status
		022-07-01 17:29:30	0001 <mark>1</mark> 2	吴波		Department Name			danger
		022-07-01 17:29:30	66	11		Department Name			danger
94.74%		022-07-01 17:29:30	1901	11111		Department Name			danger
		022-07-01 17:29:30	1902	बन बन बन बन बन		Department Name			danger
safe dang		022-07-01 17:29:30	1903			Department Name			danger
4 72	76	022-07-01 17:29:30	60000	张彤彤		Department Name			danger
		022-07-01 17:23:44	8			Department Name	192.168.134.23-1-Out	Outside1	safe
		022-07-01 17:38:42	7			Department Name	192.168.134.23-1-Out	Outside1	safe
		022-07-01 17:29:30	6			Department Name			danger
		022-07-01 17:29:30	5	曹		Department Name			danger

Figure 3-134 Check the Report

3.5.11.1 Sign In Manually

If someone is not verified on the device, the administrator can manually sign in: Select **Sign in Manually**, see the picture below.

ita Analysis		C Refresh	2022-04-07 00:00:00 To 2022-07-07 23:5	59:59 Sign Point	More + Q Q	
		🖾 Sign In	Manually 🗏 Generate Reports 🗅	Export 🛛 💼 Clear All Data		
				Selected Person		× Sta
		Personnel ID	Name	Q &		da
			Name	4 4		da
		Alternative		Selected(1)		da
		Perso First L	ast Department	Perso First	Last Department	da
		38170482	Department Name	2170590	Department Name	
safe	danger	12350	Department Name			da
5	71	00001 Hanker F	Department Name	>		da
		152 橘橘		~		da
			Department Name			da
		1810 hh	Department Name			da
		1170149 王一博	Department Name	•		
		< < 1-50 ≯	>I 50 rows per page 🔻			da

Figure 3-135 Sign in Manually

Check the statues will change to "safe".

ta Analysis	C Refresh	Time From 2022-04-07 0	0:00:00 To 2022-07-	07 22-50-50	Sign Point	More -	QQ		
		2022-04-07 0	10 2022-07-	07 23.59.59	Sign Foint	More	2		
		🖾 Sign In Manually	🗏 Generate Reports	1 Export	💼 Clear All Data				
		Time	Personnel ID	First Name	Last Name	Department Name	Sign Point	Muster Point	Statu
	7.89%	2022-07-01 17:38:42	7			Department Name	192.168.134.23-1-Out	Outside1	safe
		2022-07-07 14:30:33	6666	111111		Department Name	manual punch	Test	safe
92.119		2022-07-01 17:23:44	8			Department Name	192.168.134.23-1-Out	Outside1	safe
52.117		2022-07-01 17:23:49	998			Department Name	192.168.134.23-1-Out	Outside1	safe
		2022-07-07 14:30:17	00001	Hanker He		Department Name	manual punch	Test	safe
safe dan		2022-07-07 14:36:14	2170590			Department Name	manual punch	Test	safe
		2022-07-01 17:29:30	1803	cc		Department Name			dang
		2022-07-01 17:29:30	1804	supper		Department Name			dang
		2022-07-01 17:29:30	12348			Department Name			dang
		2022-07-01 17:29:30	1805	dd		Department Name			dang
			0507			D			

Figure 3-136 Sign in Manually

3.5.11.2 Generate Reports

Click "Generate Reports" to check the reports.the report format: Excel/PDF/CVS/TXT that you can selete.

Sign In Manually	A Generate Reports	1 Export	1 Clear All Data				
Time	Personnel ID	First Name	Last Name	Department Name	Sign Point	Muster Point	Status
2022-07-01 17:29:30			Export		×		danger
2022-07-01 17:29:30	Encrypt or not File Format	Yes No	•				danger
2022-07-01 17:29:30	Data to Export	EXCEL	3)				danger
2022-07-01 17:29:30		PDF CSV	ecords)				danger
2022-07-01 17:29:30		TXT					danger
022-07-01 17:29:30							danger
2022-07-01 17:29:30							danger
2022-07-01 17:29:30		ОК	Cancel				danger
2022-07-01 17:29:30	12348			Department Name	_		danger

Figure 3-137 Download Report

			Muster	Point Report			
Time	Personnel ID	First Name	Last Name	Department Name	Sign Point	Muster Point	Status
2022-07-01 17:29:30	1801	aa		Department Name			danger
2022-07-01 17:29:30	12347			Department Name			danger
2022-07-01 17:29:30	12346			Department Name			danger
2022-07-01 17:29:30	1802	bb		Department Name			danger
2022-07-01 17:29:30	1701x	xa		Department Name			danger
2022-07-01 17:29:30	12349			Department Name			danger
2022-07-01 17:29:30	1803	cc		Department Name			danger
2022-07-01 17:29:30	1804	supper		Department Name			danger
2022-07-01 17:29:30	12348			Department Name			danger
2022-07-01 17:29:30	1805	dd		Department Name			danger
2022-07-01 17:29:30	9527			Department Name			danger
2022-07-01 17:29:30	156456456	啦啦啦		Department Name			danger
2022-07-01 17:29:30	1806	ee		Department Name			danger
2022-07-01 17:29:30	10002	李长艾		Department Name			danger
2022-07-01 17:29:30	12345			Department Name			danger
2022-07-01 17:29:30	1807	sup		Department Name			danger
2022-07-01 17:29:30	1010101	Anni 哈哈哈哈哈		Department Name			danger
2022-07-01 17:29:30	202201171	kk		Department Name			danger
2022-07-01 17:29:30	1010102			Department Name			danger
2022-07-01 17:29:30	666	chen		Department Name			danger
2022-07-01 17:29:30	123345			Department Name			danger
2022-07-01 17:29:30	2262	彭		Department Name			danger
2022-07-01 17:29:30	22222	000p0		Department Name			danger
2022-07-01 17:29:30	130303			Department Name			danger

Figure 3-138 Report

3.5.11.3 Clear All Data

In the Access > Advanced Functions > Muster Point Setting, click Clear All Data button under Operations. Click OK to clear all data.

TZKBio CVSecurity	::: ¥									
Access Device >	Access / Advanced P	unctions / Muster Point Re	port							
Access Rule	Data Analysis		C Refresh	Time From 2022-04-28 0	0:00:00 To 2022-07-	-28 23:59:59	Sign Point	More	- Q @	
Advanced Functions 🗸				🖾 Sign In Manually	居 Generate Reports	1 £ Export	💼 Clear All Data			
Zone Reader Define Who Is inside Global Anti-Passback Global Anti-Passback Global Linkage Global Interlock Group		0% 09		Time	Personnel ID	First Name	Last Name	Department Name	Sign Point	Muster Point
Global Interlock Person Availability Occupancy Centrol Muster Point Muster Point Report	safe O	danger 0	Total				Are you	Prompt sure to clear all records?		
			Figure 3	8- 139 Clea	r All Data				-	

3.5.11.4 Export

On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export, and click **OK**.

1	The File Type	EXCEL File	~	
1. 6	Export Mode	All data (Can export u	p to <mark>40000 data</mark>)	
6 9		O Select the amount of	data to export (Can e)	port up to 4000
1.11		From the article 1	Strip, is derived	100 Data
6 3				
1 3				

Figure 3-140 Export

					ZKTECO					
					Device					
Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Enable	Device Model	Register device	Firmware Version
192.168.218.60	20100501999	Area Name	HTTP	Wired	192.168.218.60		Enable	C3-400Pro		AC Ver 4.7.7.3033 Jun 16 2017

Figure 3- 141 Export

3.6 Access Control Reports

In the access control report, you can query all access control records, including All records, Today's Access records, All abnormal records, door query, personnel query and Personnel access records reports. You can export all records or query records.

This section describes the Step for querying and exporting reports in ZKBio CVSecurity.

3.6.1 All Transactions

Operation Step

Step 1: In the Access Control module, choose "Access Control Report > All Records".

Step 2: On the All Records interface, fill in the corresponding query information and click the "search" symbol to complete the query of all records, as shown in Figure 3-120.

ŪZ	KBio CVSecurity	/ :::	¥								e admin ~
G	Access / Access Control	Reports / All Tra	ansactions								
IJ	Time From 2021-09-16 0	00:00:00 То [2	021-12-16 23:59:59	Personnel ID		Device Name	More	Q	Q		
Dı	C Refresh 📋 Cle	ar All Data 🗅	Export ⊥ Export	photos							
16	Time	Area Name	Device Name	Event Point	Event Descripti	Media Personnel I	E First Name	Last Nam	e Card Number	Department	Reader Name
	2021-12-16 11:15:26	Area Name	ProfaceX	ProfaceX-1	Remote Opening						Other

Figure 3-142 Report Query Page

Step 3: On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export, and Click **OK**.

	Export	×
Encrypt or not File Format Data to Export	 Yes No EXCEL All (max 100000 records) Selected (max 100000 records) Start Position 1 Total Records 100 	
	OK Cancel	

Figure 3-143 Report Export Page

Step 4: You can export the file by selecting the address for storing the file.

Media File: You can view or download the photos and videos created in the video system.

Clear All Data: Click Clear All Data to pop up prompt and click OK to clear all transactions.

Access / Access Control	Reports / All Tra	ansactions				
Time From 2022-04-28 0	0:00:00 To 2	022-07-28 23:59:59	Personnel ID	Device Name More - Q 🖉		
🔾 Refresh 🗊 Clea	r All Data 1	Export 🛧 Export	photos			
Time	Area Name	Device Name	Event Point	Event Descripti Media Personnel IE First Name Last Name Card Number Dep	artment Reader Name	Verification Mod
2022-07-28 04:38:42	Area Name	192.168.134.101		Prompt	Other	Other
2022-07-28 01:03:24	Area Name	192.168.134.101	192.188.134.101	Are you sure to clear all records?	Other	Other
2022-07-28 01:03:12	Area Name	192.168.134.101	192.168.134.101	OK	Other	Other
2022-07-27 13:37:43	Area Name	192.188.134.101	192.168.134.101		Other	Other
2022-07-27 13:37:37	Area Name	192.188.134.101	192.188.134.101-1	Device call	Other	Other
2022-07-27 13:38:33	Area Name	192.168.134.101	192.168.134.101-1	Call ended	Other	Other
	Area Name	100 100 101 101	192,168,134,101-1	Device call	Other	Other



3.6.2 Events from Today

Check out the system record today.

Click **Access Control Reports** > **Events from Today** to view today's records. You can export all events from today in Excel, PDF, CSV format.

Access Device	> ^	Access / Access Control F	leports / Event	s From Today							
Access Rule	>	Personnel ID		Device Name		More * Q 🖉					
¹⁾ Advanced Functions	>	🔿 Refresh 🛛 🗴 Clear	All Data 1	Export							
Access Control Reports		Time	Area Name	Device Name	Event Point	Event Descripti	Media File	Personnel IC	First Name	Last N C	
• • • • • • • • • • • • • • • • • • • •		2022-07-25 08:32:44	Area Name	192. <mark>1</mark> 68.134.108	192.168.134.105-	1 Normal Verify Ope		4	W9		
All Transactions		2022-07-25 08:32:43	Area Name	192.168.134.105	192.168.134.105-	1 Normal Verify Ope		4	W9		
Events From Today		2022-07-25 08:32:41	Area Name	192.168.134. <mark>1</mark> 08	192.188.134.105-	1 Normal Verify Ope		4	W9		
All Exception Events		2022-07-25 06:32:18	Area Name	192.168.134.108	192.168.134.105-	1 Normal Verify Ope		4	W9		
Access Rights By Door Access Rights By Personne		2022-07-25 06:32:16	Area Name	192. <mark>1</mark> 68.134.108	192.168.134.105-	1 Normal Verify Ope		4	we		
First In And Last Out		2022-07-25 08:32:15	Area Name	192.168.134.10	192.168.134.105-	1 Normal Verify Ope		4	W9		
		2022-07-25 06:32:12	Area Name	192.168.134.108	192.168.134.105-	1 Normal Verify Ope		4	W9		
		2022-07-25 08:32:08	Area Name	192,168,134,105	192.168.134.105-	1 Normal Verify Ope		4	W9		
		2022-07-25 06:32:05						4	W9		
	- 1	2022-07-25 08:31:32						4	W9		
	«							4			
		2022-07-25 06:31:31				1 Multi-Personnel Au			W9		
		2022-07-25 06:31:29	Area Name	192.168.134.108	192.168.134.105-	1 Multi-Personnel Au		4	W9		
		2022-07-25 08:31:28	Area Name	192. <mark>1</mark> 68.134. <mark>1</mark> 08	192.168.134.105-	1 Multi-Personnel Au		4	W9		
		2022-07-25 06:31:27	Area Name	192.168.134.105	192.168.134.105-	1 Multi-Personnel Au		4	W9		
		2022-07-25 08:29:28	Area Name	192.168.134.108	192.168.134.105-	1 Multi-Personnel Op		4	W9		
		2022-07-25 06:29:27	Area Name	192.168.134. <mark>1</mark> 05	192.168.134.105-	1 Multi-Personnel O		4	W9		

Figure 3-145 Event from Today

Click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export, and Click **OK**.

						Events From Today	N			10		
Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name	Remark
017-12-15 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	
017-12-15 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-	Only Card	Area Name	
2017-12-15 18:28:	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	192.168.218.6D-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	192.168.218.6D-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	192.168.218.6D-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	192.168.218.6D-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	
017-12-15 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	
017-12-15 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	
017-12-15 18:23:	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	
017-12-15 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	
017-12-15 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	2

Created from ZKBioSecurity software. All rights reserved.

Figure 3- 146 Report Export Page

Clear All Data: Click Clear All Data to pop up prompt, and then click OK to clear all events from today.

ZKBio CVSecurity	::: ¥									
Access Device >	Access / Access Control	Reports / Event	s From Today							
Access Rule >	Personnel ID		Device Name		More - Q 🖉					
Advanced Functions >	🔾 Refrest 🗴 🗎 Clea	ir All Data 1	Export							
Access Control Reports V	Time	Area Name	Device Name	Event Point	Event Descripti Media Fi	le Personnel IC	First Name	Last N C		
	2022-07-25 08:32:44	Area Name	192.168.134.105	192.168.134.105-1	Normal Verify Ope	4	W9			
All Transactions	2022-07-25 08:32:43	Area Name	192.168.134.105	192.168.134.105-1	Normal Verify Ope	4	W9			
Events From Today	2022-07-25 08:32:41	Area Name	192.168.134.108	192.168.134.105-1	Normal Verify Ope	4	W9			
All Exception Events	2022-07-25 06:32:18	Area Name	192.168.134.106	192.188.134.105-1	Normal Verify Ope	4	W9			
Access Rights By Door	2022-07-25 08:32:18	Area Name	192,168,134,105	192,168,134,105-1	Normal Verify Ope	4	W9			
Access Rights By Personnel	2022-07-25 08:32:15					4	W9			
First In And Last Out										
	2022-07-25 06:32:12					4	W9			
	2022-07-25 08:32:08	Area Name	192.168.134.106	192.168.134.105-1	Normal Verify Ope	4	W9			
	2022-07-25 08:32:05	Area Name	192.168.134.105	192.168.134.105-1	Normal Verify Ope	4	W9			
	« 2022-07-25 08:31:32	Area Name	192.168.134.105	192.168.134.105-1	Multi-Personnel Au	4	W9	F	Prompt	
	2022-07-25 08:31:31	Area Name	192.168.134.108	192.168.134.105-1	Multi-Personnel Au	4	W9	Are you sure t	to clear all records?	
	2022-07-25 08:31:29	Area Name	192.168.134.106	192.108.134.105-1	Multi-Personnel Au	4	W9	ОК	Cancel	
	2022-07-25 08:31:28	Area Name	192.168.134.10	192.168.134.105-1	Multi-Personnel Au	4	W9			
	2022-07-25 08:31:27	Area Name	192.168.134.106	192.168.134.105-1	Multi-Personnel As	4	W9			
	2022-07-25 06:29:28	Area Name	192.168.134.10!	192.168.134.105-1	Multi-Personnel Oj	4	W9			
	2022-07-25 06:29:27	Area Name	192,168,134,106	192.188.134.105-1	Multi-Personnel Ol	4	W9			

Figure 3-147 Events Clear All Data

3.6.3 All Exception Events

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

Access Device >	Access / Access Control R	eports / All Exception Events							
Access Rule	Time From 2022-04-25 00:	00:00 To 2022-07-25 23:59:59	Personnel ID	Device Name		More + Q 🖉			
Advanced Functions	🔿 Refresh 🛛 🗎 Clear	All Data 🕂 Export							
Access Control Reports V	Time	Device Name Event Point	Event Descripti Media File	Personnel ID	First Name	Last N Card Number Dep	artment Reader Na	Verification	Area Nam
- House control reports	2022-07-25 11:47:13	192.168.134.108 192.168.134.108	5-1 Event Number Unc				Other	Other	Area Nam
All Transactions	2022-07-25 11:37:23	192.168.134.108 192.168.134.108	-1 Event Number Unc				Other	Other	Area Nam
Events From Today	2022-07-25 11:34:41	192.168.134.100 192.168.134.100	-1 Event Number Unc				Other	Other	Area Nam
All Exception Events	2022-07-25 07:11:31	Speedface M4.5	Disconnected				Other	Other	Area Nam
Access Rights By Door		terrende ander andere					0.440.04		the second second
Access Rights By Personnel	2022-07-25 08:38:30	192.168.134.10	Disconnected				Other	Other	Area Nam
First In And Last Out	2022-07-25 08:32:54	192.168.134.108 192.168.134.108	-1 Extended Open Dc				Other	Other	Area Nam
	2022-07-25 08:32:28	192.168.134.10! 192.168.134.10!	-1 Extended Open Dc				Other	Other	Area Nam
	2022-07-25 08:31:32	192.188.134.100 192.188.134.100	i-1 Multi-Personnel Ac	4	W9	Dep	artment Na 192.168.134.1	Face	Area Nam

Figure 3- 148 All Exception events

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.

		110.00				All Exception Events						
ime: 2017-09-15 (Time	00 : 00 : 00 - 2017-12-	-15 23 : 59 : 59 Event Point	Device Name	Card Number	Personnel ID	First Name	Last Name	Area Name	Department Name	Reader Name	Verification Mode	Remark
017-12-15 17:43: 03	Operation Interval too Short	192.168.218.60-1	192.168.218.60	Guid Humber	T CLOSINCT ID		East Hame	Area Name	beparaterit name	192.168.218.60-1- In	Other	
017-12-15 17:42: 41	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
27 27	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:35: 17	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:35: 06	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:34: 00	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:33: 52	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:33: 43	Operation Interval too Short	192.168.218.60 <mark>-1</mark>	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:33: 35	Operation Interval too Short	192.168.218.60-2	192.168.218.60					Area Name		192.168.218.60-2- In	Other	
017-12-15 16:33: 14	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 16:06: 54	Can not connect to server		192.168.218.60					Area Name		Other	Other	
017-12-15 13:50: 17	Disconnected		192.168.218.60					Area Name		Other	Other	
017-12-15 11:53: 45	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 11:41: 04	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 11:19: 45	Operation Interval too Short	192.168.218.60-1	192.168.218.60			2		Area Name		192.168.218.60-1- In	Other	
017-12-15 11:19: 37	Operation Interval too Short	192.168.218.60-1	192.168.218.60					Area Name		192.168.218.60-1- In	Other	
017-12-15 11:05: 50	Anti-Passback	192.168.218.60-1	192.168.218.60	9505930	80000005	Bill	Fang	Area Name	Visitor	192.168.218.60-1- In	Only Card	
017-12-15 11:05:	Anti-Passback	192.168.218.60-1	192.168.218.60	13260079	80000004	Tom	Lee	Area Name	Visitor	192.168.218.60-1-	Only Card	



3.6.4 Access Rights by Door

View related access levels by door. Click **Access Control 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.

TKBio CVSecurity	::: ¥							e admin
Access Device >	Access / Access Control Reports / Acc	cess Rights By Door						
Access Rule >	Access Rights By Door		٠	Person				
Advanced Functions	Door Name	Device Name Q Q			± Export			
				Personnel ID	First Name	Last Name	Department Name	
Access Control Reports 🗸	O Refresh			1	ju		Department Name	
Al Transactions	Door Name Door Numbe	ar Owned Device		0000	K-TEST		Department Name	
Events From Today	ZKT_Korea-1 1	ZKT_Kores		12135			Department Name	
All Exception Events	原病農成XIAMEN告記 1	系统集成XIAMEN的成式		12134	name1		hr	
Access Rights By Door	Speedface-M4-震门S 1	Speedface-M4-@[]SI		1119	multible		Department Name	
Access Rights By Personnel	192.108.1.28-1 1	192.108.1.28		2222	ygv		Department Name	
First In And Last Out	192.168.134.105-1 1	192.188.134.105		1118			Department Name	
				1110			Department Name	
				1115	Zorro		Development	

Figure 3-150 Access Right by Door

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

	ZKT	ECO	
	192.168.218.60-1(1)	Opening Personnel	
Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development
2	LUCKY	Idii	Department
3	Leo	Hou	Financial
3	Leo	Hou	Department
4	Berry	Cao	General
5	Necol	Ye	Marketing
5	Necol	re	Department
6	Amber	Lin	Financial
0	Amber	LIII	Department
7	Jacky	Xiang	General
8	Glori	Liu	Marketing
0	Giofi	LIU	Department
9	Lilian	Mei	Development
9	Linan	iviei	Department



Figure 3-151 Access Right by Door Export Page

3.6.5 Access Rights by Personnel

View related access levels by door or personnel.

Click **Access Control Reports** > **Access Rights by Personnel**, the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

ZKBio CVSecurity	36					O admin
Access Device >	Access / Access Co	ontrol Reports / Access Rights By Perso	nal			
Access Rule >	Access Rights By	Personnel		< Browse ju Having L	Level to Access	
Advanced Functions	Personnel ID	Name	More- Q Q	O Refresh 2	£ Export	
				Door Number	Door Name	
Access Control Reports ~	O Refresh Personnel ID	First Name Last Name	Department Name	1	ZKT_Korea-1	
All Transactions	Personner ID	ju	Department Name	1	展结集成XIAMEN造法-1	
Events From Today	8999	K-TEST	Department Name		Speedface-M4-要门SI-1	
All Exception Events	12135		Department Name	1	192.108.1.28-1	
Access Rights By Door Access Rights Dy Personnel	12134	name1	hr	1	192.108.134.108-1	
First in And Last Out	1114	Md. Jatal	Development			
	1110	multibio	Department Name			
		7777	Department Name			
	2222	¥24	Department Name			
		fe	Department Name			
		wa	Department Name			
	3		Department Name			
	1118		Department Name			
	1110		Department Name			
	1115	Zorro	Development			
	1173	Abdulla	Development			
	1111	Esha Test	Development			
	1112	Anwar Hossain Abic	Development			

Figure 3-152 Access Right by Personnel

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

;	ZKTECO
6(Amber) H	aving Level to Access
Door Number	Door Name
1	192.168.218.60-1
2	192.168.218.60-2
3	192.168.218.60-3
4	192.168.218.60-4

Figure 3-153 Access Right by Personnel Export Page

3.6.6 First In and Last Out

Click Access Control Reports > First in And Last Out to view the First and the Last time interval.

TZKBio CVSecurity	::: X								
Access Device >	Access / Access C	Control Reports / First In And La	st Out						
Access Rule >	Time From 2022	-04-25 00:00:00 To 2022-07-28	5 23:59:59 Personnel		More - Q 🖉				
Advanced Functions >	O Refresh	🗑 Clear All Data 1 Export							
Access Control Reports 🗸	Personnel ID	First Name Last Name	First in-Reader Name	First in Time	Last Out-Reader Name	Last Out Time	Department Name		
Access Control Reports V	4	W9	192.168.134.105-1-Out	2022-07-25 08:29:2	192.168.134.105-1-Out	2022-07-25 08:32:4	Department Name		
All Transactions	1	ju	192.168.134.105-1-In	2022-08-28 15:18:11	192.168.134.105-1-In	2022-08-28 15:18:11	Department Name		
Events From Today	1	уу	192.168.1.28-1-Out	2022-07-22 18:24:50	192.168.1.28-1-Out	2022-07-22 17:32:0	Department Name		
All Exception Events Access Rights By Door	9999	K-TEST	ZKT_Korea-1-Out	2022-07-21 00:25:1	ZKT_Korea-1-Out	2022-07-21 00:25:2	Department Name		
Access Rights By Personnel	3 1 .	уу	192.168.10.221-1-Out	2022-06-18 17:41:10	192.168.10.221-1-Out	2022-06-18 17:42:1	Department Name		
First In And Last Out									

Figure 3-154 Access Right by Door Export Page

3.6.6.1 Clear All Data

In the Access > Advanced Control Reports > First in and Last Out, click Clear All Data button under Operations. Click OK to clear all data.

cess Device >	Access / Access (Control Reports	First In And La	ast Out				
,,								
cess Rule >	Time From 2022	-04-28 00:00:00	To 2022-07-2	8 23:59:59 Personnel I	D [More - Q @		
vanced Functions >	O Refresh	🗑 Clear All Dat	a 🛨 Export					
ess Control Reports 🗸 🗸	Personnel ID	First Name	Last Name	First in-Reader Name	First in Time	Last Out-Reader Name	Last Out Time	Department Name
ess control Reports V	800000020	usuop	555	10.10.20.73-1-In	2022-07-27 09:42:1			
ransactions	10			192.168.134.101-1-Out	2022-07-27 05:57:0	192.168.134.101-1-Out	2022-07-27 05:57:01	н
nts From Today	10			192 168 134 101-1-Out	2022-07-26 16 36 1	192.168.134.101-1-Out	2022-07-26 17 35 1	
Exception Events	0999	K-TEST		ZKT_Korea-1-Out	2022-07-27 00:54:10		2022-07-27 00:54:11	
ess Rights By Door	8888					17.		
ess Rights By Personnel	4	W9		192.168.134.105-1-Out	2022-07-25 08:29:2	192.168.134.105-1-Out	2022-07-25 08:32:4-	Department Name
In And Last Out	1	ju		192.168.134.105-1-In	2022-08-28 15:16:10	l 192.168.134.105-1-In	2022-06-28 15:16:11	I Department Name
	1	уу		192.188.1.28-1-Out	2022-07-22 18:24:50	192.188.1.28-1-Out	2022-07-22 17:32:0	I Department Name
	9990	K-TEST		ZKT_Korea-1-Out	2022-07-21 00:25:1	ZKT_Korea-1-Out	2022-07-21 00:25:2	Department Name
	1	УУ		192.168.10.221-1-Out	2022-06-18 17:41:12	192.168.10.221-1-Out	2022-08-18 17:42:1	Department Name
								Prompt
								Are you sure to clear all records?
								Cancel
								Cancel

Figure 3-155 Clear All Data

3.6.6.2 Export

On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and click **OK**. Select whether to encrypt the file and the file format to export, and click **OK**,

4 Video Management

4.1 Video view

Click Video Management > Video View.

In this module you can access the videos as Video Preview and Video Playback.

4.1.1 Video Preview

Click Video Management > Video View > Video Preview.

You can review recorded videos here

4.1.1.1 Live Preview

Description:

When applying video monitoring products, please strictly comply with the applicable laws and regulations for the application and maintenance of video monitoring, recording, snapping and other services. It is forbidden for enterprises or individuals to install monitoring device in office areas, monitor employees" behaviors, or use video monitoring device to snoop on other people's privacy for illegal purposes.

Single camera live preview:

Step 1: In the Video Management module, select Video View > Video Preview.

Step 2: In Full Devices, double-click the online camera to the live playback pane to open live preview.

Description:

During live preview, please do not overlap the windows, interfaces, or dialog boxes of other programs on the window that opens live, otherwise it may cause live screen or video playback to be unsmooth.

Live preview of group camera:

Step 1: In the **Video Management** module, select "**Device Management > Grouping Management**" to group the cameras.

Step 2: Click **Add** in the grouping list, enter the grouping name, and click "Confirm" to complete the addition of camera grouping.

Step 3: Select the newly created camera group and click "Add Camera" on the right side. Double-click the camera in the new interface that pops up, and click **OK** to add it to the grouping, as shown in Figure 4-1.

Step 4: In **Intelligent** module, select "**Video View** > **Video Preview**", and in "**Grouping Devices**", double-click the online camera to the live playback pane to open the live preview.

Description:

During live preview, please do not overlap the windows, interfaces, or dialog boxes of other programs on the window that opens live, otherwise it may cause live screen or video playback to be unsmooth.

				New				>
Device Na	ame	Owne	d Device	Q	0			
Alternative					Selected(0)			
	hannel Name	Owned Device	Device Status		🗌 Channel Name	Owned Device	Device Status	
21	13.9_235_测试	11	Online					
19	91	11	Online	>>				
19	92.1 <mark>68.21</mark> 3.172	11	Online	>		Ê		
19	92.168.213.155	11	Online	<<				
<mark>1</mark> 9	92.168.213.177	11	Online			No data		
19	92.168. <mark>213.1</mark> 66	11	Online	•				
I< <	1-14 > >	50 rows per p	age 👻					
			OK	<	Cancel			
			Figure 4-	1 Camer	a Grouping			N.

.

4.1.1.2 Video Preview

Operation scenario:

Using the round patrol function, the user can switch the live pictures monitored by multiple cameras regularly. For example, there are multiple cameras in a scene, and the live situation of all cameras cannot be displayed on a live split screen interface. The administrator can automatically switch the cameras of a scene to monitor the live situation every 30 seconds by using the round patrol function and realize the live browsing of all cameras in batches and time periods.

Operating Steps:

Step 1: In the Video Management module, select Video View > Video Preview.

Step 2: Under the list of grouped devices or full devices, click " O " on the right to pop up the "Multiple Camera Operation Settings" page.

Step 3: Click "Round Tour" to open the round tour setting window and configure round tour information, as shown in Figure 4-2, and the parameter description is shown in Table 4-1.

C) Title 🧿 Cycli	
Panes	4	
Interval(s)	30	
Stream type	Secondary	~
 Widget count must be The minimum time in 	less then camera count terval for round robin inspection	is 10 secor

Figure 4-2 New Rotation Training Group

Parameter	Description
Window number	The number of round-robin windows must be less than the number of round-robin cameras.
Time interval (seconds)	Set the camera rotation picture residence time under the selected main device.
Stream type	 Main code stream: large code stream, high definition, and high bandwidth occupation. Auxiliary code stream: The code stream is small, the definition is low, and the bandwidth is small. Description: When there is bandwidth limitation, it is recommended to select secondary code stream.

Table 4-1 Parameter Description of Round Patrol Configuration

Step 4: Click OK to start the round tour.

Step 5: End the round and click the toolbar ^{IMD} below to close all screens.

Fast Target Search:

Screenshot for quick target search during preview or replay:

When security guards view real-time surveillance or playback video and find a suspicious person in the screen, they can zoom in on that person and take a screenshot to support quick "target search" to jump to target search and person track mapping.

Step 1: Go to the Video Management > Video Preview, click 🙆 to snap a screenshot.



Figure 4-3 Video Preview

Step 2: Then click Target search.



Figure 4-4 Screenshot

Step 3: Next click Retrieval.

		Co Target Search		
Time Frame 2022-10-11 10:34:08 - 2022-10-12 10:34:	Data Modules	Thresholds		
Gender Glasses Mask Unlimited V Unlimited V Unlimit	Upper Color Lower Color	0 25 50 75	100	
Sense 1 and				

Figure 4-5 Target search

Intelligent Scene / Scene Applicatio	on / Target Search								
Search Result									🗒 Generate Track Repor
Query Criteria									Time Sort 👻
	2022-02-25-22-00.44	2022-02-25 22:00.42	2022-02-25 22:00.42	2022-02-25 21:57:53	2022-02-25 21:57:51	2022-02-26 21:57:51	2022-02-25 20-29-46	2022 02 -25 20 29:44	2022-02-25-20.29-44
First Name Unknown Gender Unknown Label No. Unknown Department Unknown	2022-02-25 19:59:00	2022-02-25 18.51.26	2022-02-25 16-40-50	2022-02-25 18-46-55	2022-02-25 16-40:10	2022 02 25 18.33 24	2022-02-25 18:30.49	2022 02-25 18.29:14	2022-02-25 18.28.21
Time Frame 2022-02-08 14:3 Data Unknown Modules	2022 02:25 16:26:19	2022.02.25 18.28.19	2022 02 25 16 24 52	2022-02-25 18:24:52	2022-02-25 16:24-36	2022 02 25 1E.24.34	2022 02 25 18.24.34	2022 02:25 18:22:00	2022 02 25 18.21 58
		· · · · · · · · · · · · · · · · · · ·		Page	1 📀 total 6 pages in total	(*************************************			· · · · · ·
HoloSens SDC 11111		00	00	00	-	0 0	000	<u> </u>	0 0
Point Location3									
Point Location2									
Point Location1									
Point Location0	18:21:58 18:2 2022-02-25 2022-	4:34 18:24:5 02-25 2022-02-	2 18:28:21 -25 2022-02-25	18:30:49 2022-02-25	18:40:10 2022-02-25	18:48:58 2022-02-25 20	19:59:00 20:2 022-02-25 2022-	19:46 21:57:5 02-25 2022-02	i3 22:00:44 -25 2022-02-25

Figure 4-6 Object Lookup Retrieval Results

Step 5: In the retrieval result, you can click Generate Trend Report in the upper right corner of the interface to export the trend report in PDF format, as shown in Figure 4-7 and Figure 4-8.

Trend Report		Export T
Header Informat	tion	Target Detail
Report Name	Trend report about Stranger at 20220712	Name Unknown
Creater	admin	Gender Unknown
Report Time		Time Period Jul 11, 2022 5:34:21 PM - Jul 12, 2022 5:34:21 PM
Report Time	2022-07-12 17:37:00	Record Type Video Record, Intelligent Scene Record
Report Describe		Personnel ID Unknown
		Department Unknown
Trend Detail		
	10.8.51.130	0
	Entrance 08F	• × ×
	Entrance 10F	
	IPC_10.8.12.211	
	10.8.51.135 Point Location:IPC 10.8.12.211	
	Entrance 07F Time:2022-07-12 17:12:22	

Figure 4-7 Trend Report 1

ZKBio CVSecurity			User Manu
Record Detail			
Event Time	Region	Event Source	Image Event Name Event Gr
Jul 12, 2022 5:12:05 PM	Area Name	Entrance 10F	Stranger Abnorma
Jul 12, 2022 5:12:22 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal
Jul 12, 2022 5:13:34 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal
Jul 12, 2022 5:14:31 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal
Jul 12, 2022 5:15:15 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal
Jul 12, 2022 5:16:38 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal
Jul 12, 2022 5:17:15 PM	Мар	IPC_10.8.12.211	Face Detection Alarm Normal

Figure 4-8 Trend Report 2

4.1.2 Video Playback

Click Video Management > Video View > Video Playback.

4.2 Device Management

Step 1: Click Video Management > Device Management.

Step 2: Adding Device, Camera and Group Management are included.

4.2.1 Device (Add Device)

Scene Description:

This operation is used to instruct users how to connect NVR to the platform and cameras, so that the platform can manage the connected devices uniformly, such as viewing the live and video recordings of cameras.

4.2.1.1 Adding Devices (New)

Maximum supports 1024 video channels, support 64 channels prereview and 16 channels real-time playback simultaneously.

Operating Steps:

Step 1: Under the **Video Management** module, select **Device Management > Device**.

Step 2: Click **New** under the main device list to display the adding interface as shown in Figure 4-9, and the description of each parameter is shown in Table 4-2.

Address* 192 . 168 . 130 . 54 Port* 18531 Jser Name* A12	Type*	AS1700 -	
Port* 18531 Jser Name* A12	Name*	admin	
Jser Name* A12	Address*	192 . 168 . 130 . 54	
	Port*	18531	
	User Name*	A12	
Password* ••••	Password*	••••	

Figure 4-9 New Master Device

Description:

There are 4 types you can select (AS1700/NVR800/ZKNVR/TD NVR3000) , If the purchased device is AS1700, select "AS1700" for the type.

Parameters/Buttons	Description
Туре	Select the device type.
Name	Customize the device name.
Address	Configure the device address. The format is: xxx.xxx.xxx, for example: 192.168.6.5.
Port	Configure the device port.
Username and Password	The NVR'S user name and password. Note: For ZKNVR, the default account is (admin,12345678) For AS1700, you should to login the web page to add a new account.
Т	able 4- 2 Adding Device Parameters or Function Description

Step 3: Click OK.

4.2.1.2 Delete

Click Video Management > Device Management > Device, then select Delete.

4.2.1.3 Search

Click Video Management > Device Management > Device, then select Search.

Note: Search is not supported for AS1700/TD NVR3000.

				Auto Search			×
Search AS17	00TD NVR3000 is m	st supported yet					
Total Progress							
Address	Version	Device Model	Name	Port	User Name	Password	
				No data			
User Name	Passwo	and .		Batch Setup			
water reaction			Add D		ose		
			1.23 0				

Figure 4- 10 Auto Search

4.2.1.4 Sync Camera

Click Video Management > Device Management > Device, then select Sync Camera.

4.2.1.5 More

For AS1700: It Includes options like Edit, Target Maintenance, Maintenance management, View Information, Personnel Frequency Analysis, Face Fortify, Face list library, Vehicle Fortify, Vehicle List Library, Alarm Management, Task Manage, Storage Management, Third-Party Algorithm Configuration, Email Configuration, Subscription, Unsubscribe and Sync Time.

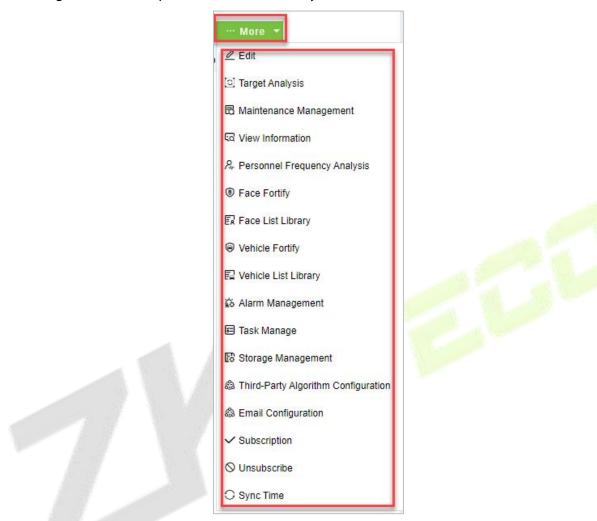


Figure 4-11 AS1700 More (Device)

For ZKNVR: It include options like Edit, Maintenance Management, Email Configuration, Subscription, Unsubscribe, and Sync Time.

···· More 💌
🖉 Edit
🗟 Maintenance Management
Lenail Configuration
✓ Subscription
S Unsubscribe
C Sync Time

Figure 4-12 ZKNVR More (Device)

Q @

4.2.1.6 Group Device

Click Video Management > Device Management > Device, then select Grouping Device.

Grouping Device						
Device Name		IP Address	Q &			
O Refresh 🗔	FNew 💼 Delete	Q Search 🔄 Adjustment Area	··· More 🔻			
Device Na	ame Channel C	ode Status Camera Type	Туре	IP Address	Area Name	Operations

Figure 4-13 Group Device

4.2.2 Camera

Cđ Video View Intelligent Video / Device Management / Camera Grouping Device Channel Device Management QQ Device Name IP Address Name Device Camera **O** Refresh C Refrest Group Management Camera Name | Status | Device Type | Camera Type | IP Address Device Name Device Area Name Status 192.168.134.101 Area Name

Figure 4-14 Camera

4.2.2.1 Search Method Add (Recommended)

Click Intelliegent Video > Device Management > Camera.

For AS1700: cameras that can be accessed to AS1700 through HWSDK and ONVIF protocol, this access method is recommended, which can complete the fast access of cameras.

Operating Steps:

Step 1: In the Video Management module, select Device Management >Device.

Step 2: Select AS1700 to add cameras under the main device list, and then click Search under the list of cameras on the right.

Step 3: Search the camera by IP address.

In the search interface, select the protocol type and the start and end IP address of the input device.

Description:

The protocol type supports the selection of ONVIF and HWSDK protocols

It is recommended to set the starting IP address and ending IP address accurately. If there are fewer cameras in a large IP address range, the search time will be longer.

If the start IP address and the end IP address are set, the system searches the cameras in unicast form, and the system can search the cameras in the IP address segment. If multiple IP address segments are set, the system can search for cameras in multiple VLANs.

If the starting IP address and ending IP address are not set, the system searches cameras in the form of broadcast. At this time, the system can only search cameras in the same network segment as the IP address of this server but can't search cameras in other IP address segments or other VLAN. Therefore, it is recommended to set IP address segment to search cameras or add cameras in batches.

Click Start Search to start searching for online cameras.

Step 4: Account verification.

For the searched camera, select a camera in the camera list, and then verify the account, as shown in Figure 4-15. Refer to Table 4-3 for parameter description.

					Auto Search			×
Sea	irch							
otal Progr	ress	100	%	No d	evice found!			
Protoco	I type ONVIF	•	IP Address					
	IP Address	Port	Type	Туре	Drive	User Name	Password	
	192.168.213.181	80			ONVIF			
	192.168.213.190	80			ONVIF			
	192.168.213.191	80			ONVIF			
	192.168.213.192	80			ONVIF			
	192.168.213.193	80			ONVIF			
	192.168.213.213	80			ONVIF			
	192.168.213.82	80			ONVIF			
Jser Nam	1e	Pas	sword		Batch Setup			
				Add	Clos			

Figure 4-15 Account Verification

Parameter	Parameter description
Port	When suggestions are added through HWSDK protocol, the default port is 6061. When recommendations are added throu <mark>gh th</mark> e ONVI <mark>F protocol, t</mark> he default port is 80.
Account/ Password	Registered username and password of the camera. If all the cameras to be added have the same registered username and password, you can also use the username and password at the bottom of the search list for batch verification. Description: For Intelligent cameras, when accessing through different protocol types, the location of the registration password in the camera Web interface is different: HWSDK Protocol: The registered password is 'sDK Password" in "Advanced Configuration > Network > Platform Docking Parameters > Password Management". ONVIF protocol: The registered password is "ONVIF password" in "Advanced Configuration > Network > Platform Docking Parameters > Password Management". GB/T 28181 Protocol: The registered password is "Password" in "Advanced Configuration > Network > Platform Docking Parameters > Second Protocol Parameters".

Table 4-3 Parameter Description

Description:

About port numbers:

If the camera is added through ONVIF protocol, the port does not need to be modified; If the camera is added through HWSDK protocol, it is recommended to configure port 6061. After the camera is connected, the message transmission will be encrypted, which improves the security of information transmission.

About camera registration username and registration password:

Usually, the registered username and password of the camera are the username and password of logging in to the Web interface. For some cameras, there may be inconsistency between the

two. Please use the registered username and password of the actual camera as the value of this parameter.

If the camera default password has been modified, please do not click "Verify" continuously. Clicking 5 times or more continuously will cause the platform to lock. After the platform is locked, you need to wait for the platform to be unlocked or restart the camera to add it again.

Step 5: Select the camera to add and click Add Camera.

The return result interface pops up to display the result of camera access.

Step 6: Close the pop-up window and complete the search and addition of cameras.

Step 7: Subsequent configurations are shown in Table 4-5.

Scene	Configuration location	Configure
Add Cameras Through ONVIF Protocol	Camera Web Interface	Configure docking parameters, see Camera Web Interface Docking Configuration-ONVIF for details.
Camera Join Grouping	Device Management > Group Management	Create groups and add cameras to facilitate the grouping management of cameras.
Adjustment Area	Device Management > Master Device > Camera Device	Under the "Camera device" list, you can check one or more cameras and click the "Adjust Area" button to adjust the area where the cameras belong.

Table 4- 4 Subsequent Config<mark>uratio</mark>n Instructions

4.2.2.2 Camera to ZKNVR Device

Search Method Added (Recommended):

This section describes the configuration steps for automatically adding cameras in batches in the ZKBio CVSecurity. For cameras th Step 4: In Intelligent module, select "**Video View** > **Video Preview**", and in "**Grouping Devices**", double-click the online camera to the live playback pane to open the live preview.

Description:

During live preview, please do not overlap the windows, interfaces, or dialog boxes of other programs on the window that opens live, otherwise it may cause live screen or video playback to be unsmooth.at can be connected to ZK NVR through ZKTeco-P, Rtsp, ZKTeco and ONVIF protocols, this access method is recommended to complete the quick access of cameras.

Steps:

Step 1: In the Video Management module, select "Device Management > Main Device".

Step 2: Select the ZKNVR whose camera is to be added under the main device list, and then click **Search** under the camera list on the right.

Step 3: Search for cameras by IP address.

In the search interface, select the protocol type, that is, the protocol type ZKTeco-P, Rtsp, ZKTeco or ONVIF (recommended to use ZKTeco) connected to the camera.

Instruction:

- 1. Protocol type supports the selection of zkteco-P, Rtsp, zkteco and ONVIF protocols. (recommended to use zkteco).
- 2. Using zkteco protocol access, all functions can be used normally.
- 3. The ONVIF protocol is used to access, and the IPC parameter configuration except "camera" and "image parameter" does not take effect.

4. Using zkteco-P, Rtsp, protocol access, PTZ control cannot be used, and IPC parameter configuration does not take effect.

Click **Start Search** to start searching for online cameras.

Step 4: Account verification.

For the searched cameras, directly check the cameras in the camera list, and then perform account verification (the account number and password are the camera's registered user name and password), as shown in Figure 4-16, and parameter descriptions are shown in Table 4-5.

a 11		Auto Search	×
Searching Ital Progress	40%	•	
I IP Address	Port Type	Type Drive User N	ame Password
		No data	
Jser Name	Password	Batch Setup	

Figure 4-16 search methods added

Parameter	Parameter Description
Port	Through zkteco-p, rtsp, zkteco, onvif protocols, the default port is 80.
Account Password	The registered username and password of the camera. If all cameras to be added have the same registered username and the same registered password, you can also use the username and password at the bottom of the search list for batch verification.

Table 4-5 Parameter Description

Step 5: Close the pop-up window to complete the search and addition of cameras.

Step 6: The subsequent configuration is shown in Table 4-6.

Scenes	Configuration Location	Configure
Camera Grouping	"Device Management > Group Management"	On the Group Management interface, click Add to create a group, click Add Camera on the right, and check the camera to complete the camera grouping.
Adjust Area	"Device Management > Main Device > Camera Device" list	Under the Camera Device tab, you can select single or multiple cameras, and then click the Adjustment Area button to adjust the area to which the cameras belong.

Table 4-6 Subsequent configuration instructions

4.2.2.3 Manual Add

This paper introduces the configuration Steps of adding cameras in platform by "adding".

Operation Steps:

For AS1700: In the Video Management module, select Device Management > Master Device.

Step 1: Select the AS1700 to which a camera is to be added in the main device list and Click **Add** under the camera list on the right. The add camera page is displayed.

Step 2: Set the corresponding content according to the new requirements, as shown in Figure 4-17. Please refer to Table 4-7 for parameter filling instructions.

	New	×	
Device Name [*]			
Drive	HWSDK 💌		
Authorize Area*	•		
Username*			
Password*			
IP Address	12 12 120		
Port	6061		
Save and New	OK Cancel		

Figure 4-17 New Camera

Parameter	Description	
Device Name	The name of the device displayed on the platform. It is recommended to enter the installation location or monitoring area of the device.	
Drive	 Protocol type of camera access. Description: When Dahua camera accesses AS1700, it needs DHSDK protocol. When accessing the camera, please ensure that the corresponding plug-in has been installed, and you need to wait for 5 minutes before accessing the device, otherwise the device cannot be accessed normally. When T3B15-ISor BioX Series cameras are accessed to AS1700, it is recommended to access them by HWSDK protocol: if the cameras are accessed to AS1700 by ONVIF protocol, the front-end video occlusion, motion detection and behavior analysis functions cannot be enabled, and can only be used when accessing by HWSDK protocol. 	
Authorized Area	Red Area Select the area where the camera belongs. If it is not specified, the current came belongs to the default area. The area is the area that has been configured in System Administration Module System Administration > Regional Settings. Users with permissions on this zone can view and operate devices under to current zone.	
Interconnect Coding	This parameter can be configured only when the Add Devicees the system through T28181 protocol. Consistent with the "Device ID" of T3B15-IS or BioX Series Camera/Consistent with the 'sIP User Authentication ID" of Haikang Camera, in which 11 ~ 13 bits are required to be 132.	

Parameter	Description
	Description: Interconnection coding is required to be a 20-bit integer, and when it is less than 20 bits, it needs to be supplemented with 0.
Enable RTSP	This parameter can be configured only when the Add Devicees the system through DHSDK protocol. After RTSP is enabled, when users browse the live picture through the platform, the live picture is directly fetched from the camera without MU processing and forwarding, which reduces the pressure of the system. Enable RTSP fetching function and require the platform and front-end device to configure the same port (default port 554).
Username/ Password	 The registered username and password used by the camera when registering with the device. For Intelligent cameras, when accessing through different protocol types, the location of the registration password in the camera Web interface is different: HWSDK Protocol: The registered password is 'sDK Password" in "Advanced Configuration > Network > Platform Docking Parameters > Password Management". ONVIF protocol: The registered password is "ONVIF password" in "Advanced Configuration > Network > Platform Docking Parameters > Password Management". GB/T 28181 Protocol: The registered password is "Password" in "Advanced Configuration > Network > Platform Docking Parameters > Second Protocol Parameters".
IP Address	Represents the IP address of the device.
Port	 Represents the access port of the device. It is recommended to keep the default value of the port. If the camera side modifies the port number, please fill it in according to the actual situation. Instructions: When the camera is registered using HWSDK protocol, it is recommended to configure port 6061. After the camera is connected, the message transmission will be encrypted, which improves the security of information transmission. After the camera is successfully accessed, if the port number is modified, the live camera will be disconnected and reconnected for about 1-5 seconds, which is related to the actual network situation.

Table 4- 7 Parameter Description for Manual Single Access

Step 3: Click **OK** to complete the addition of camera device.

Step 4: See Table 4-8 for subsequent configuration.

In the following cases, it is necessary to complete the subsequent configuration on the camera side before the camera can be used normally.

Scene	Configuration location	Configure
Adding Cameras Through T28181 Protocol	Camera Web interface	To configure docking parameters, please refer to 4.1. 2.3. 1 Camera Web Interface Docking Configuration-GB/T28181 for details
Adding Camera Via ONVIF Protocol	Camera Web interface	Configure docking parameters, see 4.1. 2.3. 2 Camera Web Interface Docking Settings- ONIVIF for details.
Camera Join Grouping	Device Management > Group	Create groups and add cameras to facilitate

Scene	Configuration location	Configure
	Management	the grouping management of cameras.
Adjustment Area	"Device Management > Master Device > Camera Device"	Under the "Camera device" list, you can check one or more cameras and click the "Adjust Area" button to adjust the area where the cameras belong.

Table 4-8 Subsequent Configuration Instructions

4.2.2.4 Camera Connect to AS1700

• Camera Web Interface Configuration-Gb/T28181

When cameras dock the platform through GB/T28181 protocol, the corresponding docking parameters need to be configured in the camera Web interface.

Precondition:

- 1. GB/T28181 protocol uses MD5 digest authentication, MD5 is a weak algorithm, there are security risks. And the signaling stream and media stream are not encrypted, please use this protocol in trusted network, otherwise there may be security risks.
- 2. When using GB/T28181 protocol to interface with AS1700, you need to obtain the parameters when adding cameras on the platform side, such as device ID.

Set System Time:

By docking with the platform through this protocol, it is necessary to make sure that the system time of the camera is calibrated by NTP.

Step 1: Enter the IP address of the camera in the browser address bar and click **Enter**.

Step 2: Enter the camera's "username" and "password" and click Login.

Step 3: In the **Camera Web** interface, select the "**Advanced Configuration** > **System Configuration** > **Time Setting**" tab to enter the "Time Setting" configuration interface.

Step 4: In the **Time Setting** interface, set NTP timing and click **Save**, as shown in Figure 4-18. Please refer to Table 4-9 for parameter description.

Time zone	(UTC+08:00) Beijing, Hong Kong (~	
Calibration mode	🔿 Manual 💿 NTP	
NTP server	ntp.ntsc.ac.cn	Q Detect NTP server
Synchronization interval (min)	60)
Device time	2021-12-20 17:36:24	
Save		

Figure 4-18 Configuring NTP Timing

Parameter	Description	
Time zone	Select the time zone where the NTP server is located.	
Timing method	Select NTP Timing.	
NTP Server	IP address of AS1700.	
Synchronization time interval	The interval at which time synchronization takes place.	
Table 4-9 Explanation of NTP Timing Parameters		

Table 4-9 Explanation of NTP Timing Parameters

• Configure Gb/T28181 Protocol Parameters

Steps:

Step 1: Log in to the camera through the Web and select "**Advanced Configuration > Network > Platform Docking Parameters**". The system displays the interface of "Platform Docking Parameters".

Step 2: Select **"Second Protocol Parameters > T28181**" and check "GB/T28181" to enable GB/T28181 protocol.

Step 3: Configure the GB/T28181 parameters, as shown in Figure 4-19, and the parameter description is shown in Table 4-10.

Enable media stream l	keep-alive			ot periodically receive keep-alive eter based on platform requireme	messages from the video surveillance platform, ents.)
eep-alive time		60	Save		
ONVIF T28181	T28181-2 GA/T 14	00 REST			
GB/T 28181					
Video stream type	Auto	~			
H.265					
Name	3402000001320000001		Registration validity (s)	86400]
Platform IP			Heartbeat interval (s)	60	
Port number	5060		Max. timeouts	3	
Device ID	3402000001320000001		Stream index	Primary stream	
Server code	340200000200000001		Lens ID	3402000001310000001	
SIP server domain	3402000000		Password		
GB35114					
GB35114 (1	Note: The GB 351 <mark>14</mark> TF card th	nat with the storage functi	on cannot function as the m	emory card after being inserted in	nto the device.)

Figure 4- 19 Gb/T28181 Parameter Interface

Parameter	How to Configure	
Media Streams Keep Alive Switch	Enable the "Media Stream Keep Alive Switch" and tick it to indicate that it is enabled. After the media stream keeping alive function is turned on, if the camera does not receive the media keeping alive packet sent by AS1700 within a certain period of time, the camera stops sending the media stream. When the platform supports keep-alive function, it is recommended to "enable".	
Keep-alive Times	The number of keep-alive connections between the camera and AS1700 media stream is an integer in the range of 2 to 24, and the single keep-alive time is 5s. For example, when the number of keep-alive times is 2, the media stream keep-alive time is 2*5s, that is, 10s. Even if the camera does not receive the media keep-alive packet within 10s, it will not stop sending the media stream, and if it does not receive the keep-alive packet for more than 10s, it will stop sending the media stream.	
Name	Customize the login name used when registering with AS1700 system.	
Platform IP	Enter the IP address of the AS1700 system.	
Port Number	Platform listens on GB/T28181 protocol port number. Port number 5080 is used when docking H" platform. If the server and camera are on different networks and NAT exists, it is configured as the mapped port of 5080.	
Device ID	Custom setting device ID, requiring 132 bits 11 to 13 and 0 bits last, and the ID of each device must be unique.	

Parameter	How to Configure
Server Code	GB/T28181 server code. Custom input 20 digits, which require the 11th to 13th digits to be 200. For cameras connected to the same AS1700 system, the server codes must be consistent.
@	Domain name, custom input 10 digits.
Password	Customize the registration password of the camera in the platform. In order to improve security, it is recommended that the password should be 8 to 20 characters in length and contain at least two letters, numbers and special characters.
Lens ID	Custom setting device lens ID number, required to be 20 digits and the 11 to 13 digits must be 131, otherwise AS1700 system cannot view the live.
Alarm Input ID	ID of the device alarm input. The platform assigns an alarm input ID to the camera according to the device ID.
Audio Output ID	ID of the device audio output. The platform assigns an audio output ID to the camera according to the device ID.
	Table 4- 10 Parameter Explanation

Step 4: Click Save.

Camera Web Interface Configuration-ONVIF

When the camera docks AS1700 through ONVIF protocol, the corresponding docking parameters should be configured in the camera Web interface.

Precondition:

ONVIF retains MD5 digest authentication. MD5 is a weak algorithm with security risks, and the media stream is not encrypted. Please use this protocol in a trusted network, otherwise there may be security risks.

- If the ONVIF protocol needs to use the H.265 encoding protocol, the ONVIF version of the camera and AS1700 need to support the H.265 encoding protocol. Intelligent cameras require V200R003C10 and later. Please contact the provider for AS1700 to confirm support. Otherwise, please modify the coding protocol of video stream (including main code stream and sub-code stream) to H.264 first, and then configure the parameters in the device. For specific operation, please log in to the camera Web interface, select "Advanced Configuration > Audio View > Video Stream Parameters", and set "Encoding Protocol" to "H.264".
- The ONVIF protocol defaults to the HTTP/HTTPS transport protocol type.
- ONVIF protocol only supports G711U audio coding format, and other audio coding formats will
 cause the functions such as accompanying voice, voice intercom and voice broadcast to be
 unavailable.
- When using ONVIF protocol to interface with AS1700, the default port number is "80".

Operating Steps:

Step 1: Log in to the camera's Web interface (https://IP address).

Step 2: Select **Advanced Configuration > Network > Platform Docking Parameters**. The system displays the interface of **Platform Docking Parameters**.

Step 3: Select **Second Protocol Parameters** > **ONVIF** to enter ONVIF Protocol Parameters Configuration Interface.Configure the ONVIF parameters, as shown in Figure 4-20, and the parameter description is shown in Table 4-11. ZKBio CVSecurity

	rs	
Enable media stream keep		ter the function is enabled, if the SDC does not periodically receive keep-alive messages from the video surveillance platform, stops sending media streams. Set this parameter based on platform requirements.)
eep-alive time 60		Save
ONVIF T28181	T28181-2 GA/T 1400 R	EST
Note: When the video encodin	g format is H.265, the ONVIF proto	col is not compatible with the old device on the live network. You need to change the video encoding format to H.264.)
Enable ONVIF		
ONVIF Supports IPv6		
ONVIF Supports IPv6 Validity period		s enabled, if the current SDC time is beyond the validity period specified on the platform, ONVIF messages become invalid. Iy when the platform supports the ONVIF validity period function.)
Validity period		
Validity period	This parameter is valid on	ly when the platform supports the ONVIF validity period function.)
	This parameter is valid on Elementary stream	ly when the platform supports the ONVIF validity period function.) (Note: Select a stream transmission type based on the requirements of the decoding device to prevent decoding failure.)

Figure 4-20 ONVIF Parameter Interface

Parameter	How to configure		
Media Streams Keep Alive Switch	Enable the "Media Stream Keep Alive Switch" and tick it to indicate that it is enable After the media stream keeping alive function is turned on, if the SDC does n receive the media keeping alive packet sent by AS1700 within a certain period time, the SDC stops sending the media stream. When the platform supports kee alive function, it is recommended to "enable".		
Lifetime	Time (s) for SDC and AS1700 media streams to keep alive, an integer in the range of 10 to 120. For example, when the keep-alive time is set to 60s, the SDC will not stop sending the media stream even if it does not receive the media keep-alive packet within 60s and will stop sending the media stream if it does not receive the keep-alive packet after 60s.		
Enable ONVIF	Enable ONVIF protocol, ticked to indicate enabled.		
ONVIF message validity period	Enable "ONVIF message validity period" and tick it to indicate that it is enabled. After the ONVIF message expiration date function is turned on, if the expiration date set by the platform is exceeded, the ONVIF message will be invalid. Description: This function is only enabled when the platform supports ONVIF message validity function, otherwise it cannot be successfully docked with AS1700, and it is only recommended to enable it when there is a security risk, and it is turned off by default.		
Onvif Metadata Flow Switch	If "ONVIF Metadata Stream Switch" is checked, the metadata stream of the camera can be obtained, otherwise, only video stream and audio stream can be obtained. "ONVIF Metadata Flow Switch" is checked by default.		
ONVIF Stream Transmission Type	 Please select the desired streaming type in the drop-down box after Streaming Type, and the default is Basic Stream. Elementary Stream: ES (Elementary Stream) packaging method is adopted. Program Stream: PS (Program Stream) packaging mode is adopted. Description: Please select the stream transmission type according to the requirements of decoding device, so as not to be unable to decode. The configuration of the ONVIF media stream is only valid when the SDC interfaces with the platform through the ONVIF protocol. 		
ONVIF Authentication	Please select the required authentication method in the drop-down box after Authentication Method.		

Parameter	How to configure
Mode	 Digest_MD5: Digest authentication for MD5 encryption. Digest_SHA256: Digest authentication for SHA256 encryption. Digest_MD5/Digest_SHA256: Both Digest_MD5 and Digest_SHA256 authentication methods are supported. Digest_MD5 (priority)/WSSE: Both Digest_MD5 and WSSE authentication modes are supported, but Digest_MD5 authentication mode is preferred. WSSE (Web Service Security): "WSSE" authentication method. None: Indicates no authentication. Description: There is a security risk using ONVIF WSSE authentication. It is recommended to enable Digest_MD5 (priority)/WSSE authentication when some platforms accessed by the camera do not support HTTP digest authentication is not support ONVIF WSSE authentication. It is recommended that WSSE authentication be enabled when HTTP digest authentication is not supported on all platforms on which the camera is accessed and only ONVIF WSSE authentication be enabled when some platforms fail to properly handle Digest messages. There are security risks in using None authentication, so it is only recommended to enable it when the platform does not support authentication. When using None authentication mode, the ONVIF protocol is used to drain and the RTSP protocol is used to request live, and authentication will not be carried out.
ONVIF Version Information	The ONVIF version supported by the camera needs to be consistent with the ONVIF version supported by the platform.
ONVIF Transport Protocol Type	 ONVIF transport uses protocol types: HTTP/HTTPS: It can be transmitted over HTTP or HTTPS protocols, respectively. HTTP: Transport using the HTTP protocol. HTTPS: Transport using the HTTPS protocol. Description: HTTP protocol is not safe protocol, there are risks, please use cautiously.
Modify The ONVIF Password	 Method 1: Select the "Password Management" tab under 'second Protocol Parameters". Select "ONVIF Password" and enter "Web User Password", "New Password" and "Confirm Password" for the ONVIF protocol. Click Save. Method 2: Select Advanced Configuration > System Configuration > Password Management. Select Protocol Password. Select "ONVIF Password" and enter "Web User Password", "New Password" and "Confirm Password" and enter "Web User Password", "New Password" and "Confirm Password" for the ONVIF protocol. Click Save. Description: To ensure the security of data information, please change the ONVIF password used by AS1700 must be consistent with this password, otherwise the docking with AS1700 cannot be successful, and the platform will be locked for 5 minutes after 20 consecutive authentication failures. After the password is modified, please record and save it in time.

Parameter	How to configure
	• The default username is "admin," and the Web user password is the same as the user currently logged on to the Web. In order to improve security, it is recommended that the password length be 8 to 20 characters, and contain at least two uppercase letters, lowercase letters, numbers and special characters.

Table 4-11 Explanation of ONVIF Parameters

4.2.2.5 Result

In the video device management interface, the added device status is displayed as "online", and the live broadcast can be seen at the same time, which means the addition is successful.

Operating Steps:

Step 1: Check to see if the device is online.

In the **Video Management** module, select Device Management > Master Device.

Select the master device list AS1700 devices, and in the camera device list on the right, check whether the added device status is "online" under the "device status" parameter.

Description:

If the camera is offline due to some reasons after the camera is successfully added for the first time, the offline reason reminder will not pop up in the interface at this time, so it is necessary to manually check the offline reason of the camera.

Step 2: Check the facts.

In the Video Management module, select Video View > Video Preview.

Select the preview window and double-click the added camera to the live window, which can play the live normally, indicating that the access is successful.



Figure 4-21 View Live

Description:

To load the video preview for the first time, you need to download the video plug-in and install it before you can successfully view the video picture.

^C If the added camera does not appear in the camera list, you can click Refresh Camera List.

Users can customize the new camera grouping. Custom camera groups can be created under Device Management > Grouping Management.

Grouping device: Show all camera groups and cameras in the group and view the live cameras individually or in the whole group.

Full device: Shows all the device of AS1700 and can view the live camera individually.

4.2.3 Group Management

Click Video Management > Device Management > Group Management.

ିର୍ବ Video View >	Intelligent Video / Device Management / Group Management	
Device Management 🗸	Group	< Camera Device
Device	Name Q	Device Name
Camera	⊖Refresh ⊒∓New @iDelete	◯ Refresh
Group Management	Name Operations	Camera Name Status Device Type Camera Type IP Address
	□ 1 ∠ 前 ♀	
	🗌 Default Group 🖉 💁	



4.2.3.1 New

Click Video Management > Device Management > Group Management, then select New.

			New		×
	Name [*]	l			
1	Save	and New	ОК	Cancel	

Figure 4-23 New (Group Management)

Click **OK** to save and exit.

4.2.3.2 Delete

Click Video Management > Device Management > Group Management, then select Delete.

4.3 Decoding On the Wall

Click Video Management > Decoding on The Wall.

G	Video View	>	Intelligent Video / Decoding On Th	e Wall / Decoder			
5	Device Management	>	Decoder Name	Q &			
1	Decoding On The Wall	~	◯ Refresh 🖅 New 🍵 De	lete			
	Decoder		Decoder Name	IP Address	Port	Туре	Operations

Figure 4-24 Decoding on the Wall

4.3.1 Decoder

Click Video Management > Decoding on the wall > Decoder.

4.3.1.1 New (Add Decoder)

Click Video Management > Decoding on The Wall, then select New.

Decoder Name*		
IP Address*		
Port*	10200	
Type*	PEMXP70 -	
UserName*		
Password		

Figure 4- 25 New (Decoding Wall)

Parameter	Description			
Decoder Name	Custom decoder <mark>name</mark> .			
IP Address	IP Address of the d <mark>ecod</mark> er			
Port	Default port 10200			
Туре	Select the device model to access the decoder Support PEMXP70 and DEC6109 decoder access			
Username	Enter the business username			
Password	Enter the business password			
3 3	Table 4- 12 New			

Table 4- 12 New

Click **OK** to save and exit, or click **Save and New** to continue.

4.3.1.2 Delete

Click Video Management > Decoding on The Wall, then select Delete.

4.3.2 TV Wall

Click Video Management > Decoding on the wall > TV Wall.

4.3.2.1 New (Create TV Wall)

Click Video Management > Decoding on the wall > TV Wall, then select New (Create TV Wall).

Step 1: In the Video Management module, select "Decoding Wall > TV Wall".

Step 2: Click Add to enter the "Add TV Wall" page, as shown in Figure 4-26.

		New		×
TV Wall Name: Matrix 4 X 4 Set up				
P	evious Step Next Ste	ep Complete	Cancel	1

Figure 4- 26 Creating Tv Wall Layout

Step 3: Enter a custom TV Wall Name.

Step 4: In the Matrix Settings box, customize the number of rows and list of input layouts, and click **Settings** to apply the layout.

Description:

Matrix Layout pane settings, supporting a minimum of 1 * 1 and a maximum of 8 * 8.

Step 5: Click next to enter the TV wall binding decoder interface, as shown in Figure 4-27.

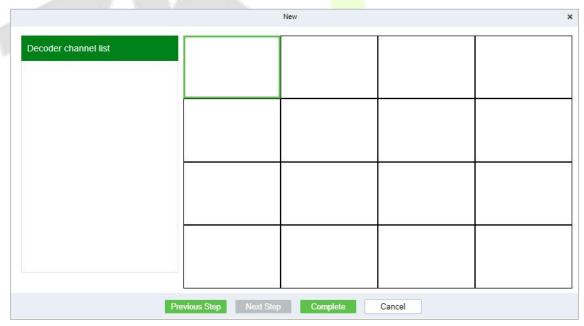


Figure 4-27 TV Wall Binding Decoder

Step 6: Select the TV wall pane to which you want to add a decoder channel, and then click **Decoder Channel** on the left to complete the binding.

Step 7: Click **Finish** to finish adding the TV wall.

4.3.2.2 TV Wall Live

Precondition:

The TV wall layout has been created and the decoder docking has been completed. See 4.4. 1 Configuring TV Wall for details.

Operating Steps:

Step 1: In **Video Management**, select "**Decoding on the Wall > Large Screen Control**", as shown in Figure 4-28.

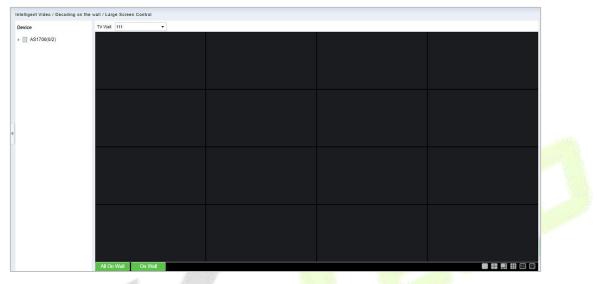


Figure 4- 28 Live Upper Wall

Step 2: Select the created TV wall layout in the TV wall drop-down box.

Step 3: Select a window bound to the decoder channel, click the camera device under the device list to realize the association between the camera and the TV wall window, and then click **Go to the wall** or **Go to the wall all** below to complete the decoder going to the wall operation, so that users can view the live situation on the TV wall screen.

Description:

"Go to the wall" is only for a single window and click "Go to the wall all" when setting split screens.

4.3.2.3 Delete

Click Video Management > Decoding on the Wall > TV Wall, then select Delete.

4.3.3 Large Screen Control

Click Video Management > Decoding on the wall > Large Screen Control.

		Device	<			
Device Management	>	Derice	,	TV Wall	•	
Decoding On The Wall	~					
Decoder						
TV Wall						

Figure 4- 29 Large Screen Control

4.4 Search

Click Video Management, then select Search.

ିର୍ଘ Video View	>	Intelligent Video /	Search / Face Search	
Device Management	>	Search Type	Face Search	∱ Export
Decoding On The Wall	>	Device*	-	
		Channel*		•
Q Search	~	Start Time*	2022-08-03 00:00:00	
Face Search		End Time*	2022-08-03 23:59:59	
Vehicle Retrieval		Gender	Unlimited	
Target Comparison		Age	Unlimited •	



4.4.1 Face Search

Step 1: Click Video Management > Search, then select Face Search.

	G	Video View	>	In	itelligent Video /	/ Search / Face Sea	rch	
1	5	Device Management	>		Search Type	Face Search		∱ Export
8	(†	Decoding On The Wall	>		Device*		•	
		Search	~		Channel* Start Time*	2022-08-03 00:00	:00	
		Face Search			End Time*	2022-08-03 23:59	:59	
		Vehicle Retrieval			Gender	Unlimited	-	
		Target Comparison			Age	Unlimited	•	
		Search For Pictures With Pictures			Mouth Mask	Unlimited	•	
		Personnel Frequency Retrieval			Glasses	Unlimited	•	
					Hat	Unlimited	*	
				«	Hair	Unlimited	•	
					List Library		•	

Figure 4-31 Face Search

Parameter	Description
Search Type	Set Search type as Face Search or Target Overall Search.
Device	Selecta device.
Channel	Select an option for channel from list and click Ok.
Start Time	Set start time.
End Time	Set end time.
Gender	Set gender as Unknown, Male, or Female.
Age	Set age as per list: under 18, 18 to 25 years old, 26 to 30 years old, 31 to 35 years old, 36 to 40 years old, 41 to 50 years old, and 51 years old and above.
Mouth Mask	Set to Unknown, Unlimited, Wear mask, and No.
Glasses	Set to Unlimited, Unknown, Have, and No.
Hat	Set to Unknown, Wear a Hat, and No.
Hair	Set to Unlimited, Unknown, long hair, and short hair.
List Library	Select an option from List and click OK.
	Table 4- 13 Face Search

Step 2: Click Search to complete.

4.4.1.1 Export

Step 1: Click Video Management > Search > Face Search, then select Export.

		Export	×
	Encrypt or not	🔿 Yes 💿 No	
	File Format	EXCEL -	
1	Data to Export	Selected (max 100 records)	
		Start Position 1	
		Total Records 50	
		OK Cancel	
		OK Cancel	

Figure 4- 32 Export

Step 2: Click OK to save and exit.

4.4.2 Vehicle Retrieval (AS1700)

Click Video Management > Search, then select Vehicle Retrieval.

Ca Video View	>	Intelligent Video / :	Search / Vehicle Retrieval	
Device Management	>	Device*	•	↑ Export
Decoding On The Wall	>	Channel*	▼ 2022 00 02 00 00 00	
Search	~	End Time*	2022-08-03 00:00:00 2022-08-03 23:59:59	
Face Search		Search UnknownPlate		
Vehicle Retrieval		Plate Number		
Target Comparison		Vehicle Brands:	Unlimited -]
Search For Pictures With Pictures		Vehicle Sub-	Unlimited -]
Personnel Frequency Retrieval		Model:		
		Year Model	Unlimited -	
	«	Car Type	Unlimited -	
		Car Color	Unlimited •	
		Special Car	Unlimited -	
		Plate Color	Unknown	
		Type Of Plate	Unlimited •	
		Plate Obscured	Unlimited •	
		Annual Logo	Uniinnited	J

Figure 4-33 Vehicle Retrieval

Parameter	Description
Device	Select Device.
Channel	Select an option from the list and slick OK.
Start/ End Time	Set Start/End Time.
Search Unknown Plate	Select Search Unknown Plate as requirement.
Plate Number	Mention Plate Number.
Vehicle Brands	Select Unlimited.
Vehicle Sub-Model	Select Unlimited.
Year Model	Set year as Unlimited, Unknown and 2013 to 2021.
Car type	Mention Car type as Unknown, Van, Car, Medium Bus, Motorcycle, SUV, Bus, Unlimited, Small truck, and Truck.
Car Color	Set Car color from list as: Unlimited, Unknown, Red, Green, Black, Purple, White, Brown, blue, Pink, Yellow, and Gray.
Special Car	Set as Unlimited, Not Special car, and School Bus.
Plate Color	Set as Unlimited, White, Yellow, Green, Blue, Black, Gradient green, Yellow and Green, Red and Gray.

Parameter	Description				
Type of Plate	Set Type of plate as: Personalized License Plate, Single Yellow Card, Single-Layer Military Card, Single Layer Blue card, Double-Decker Military Card, Double Yellow card, Single Layer Black Card, White Armed Police, White Police Sign, Unknown, and Unlimited.				
Plate Obscured	Set as Unlimited, Unobstructed License Plate, and Hide the License Plate.				
Annual Logo	Set as Unlimited, None, and Yes.				
	Table 4- 14 Vehicle retrieval				

4.4.2.1 Export

Click Video Management > Search > Vehicle Retrieval, then select Export.

4.4.3 Target Comparision (AS1700)

```
Step 1: Click Video Management > Search, then select Target Comparison.
```



Figure 4-34 Target Comparison

Step 2: Upload the personnel photos to be compared and click Compare.

4.4.4 Search for Pictures with Pictures

	Step	1:	Click	Video	Managemer	t > Se	arch, the	n select	Search	for Pict	ures with	Pictures .
--	------	----	-------	-------	-----------	--------	-----------	----------	--------	----------	-----------	-------------------

G	Video View	>	Intelligent Video	/ Search / Search For Pictures	With Pictures
5	Device Management	>			↑ Export
<u>F</u>	Decoding On The Wall	>			
Q	Search	~			
	Face Search				
	Vehicle Retrieval		Device*	-	
	Target Comparison		Channel*	•	
	Search For Pictures With Pictures		Start Time*	2022-08-03 00:00:00	
	Personnel Frequency		End Time*	2022-08-03 23:59:59	

Figure 4-35 Search for Pictures with Pictures

Step 2: Fill the parameters like Device, Channel, Start/End Time, and Similarity, click Search to finish.

4.4.4.1 Export

Click Video Management > Search > Search for Pictures with Pictures, then select Export.

4.4.5 Personnel Frequency Retrieval (NVR800)

Step 1: Click **Video Management > Search, then select Personnel Frequency Retrieval.**

G	Video View	>	Ir	ntelligent Video / S	earch / Personnel Frequenc	y Retrieval
5	Device Management	>		NVR800*	•	⊖ Refresh
<u></u>	Decoding On The Wall	>		Channel*	•	
0	Search	~		List Library		
w.		~		Start Time*	2022-08-03 00:00:00	
	Face Search			End Time*	2022-08-03 23:59:59	
	Vehicle Retrieval			Min Interval(s)	0	
	Target Comparison Search For Pictures With			Similarity Gender	85	
	Pictures Personnel Frequency			Age		
ан. Т	Retrieval		h	Mouth Mask	•	
			*	Hair Style	·	
				Glasses		
				Hat	-	
				Maximum Display Quantity	100	

Figure 4-36 Personnel Frequency Retrieval

Parameter	Description
NVR800	Select the device.
Channel	Select Channel as all or single and click OK.
List Library	Select list library from list either all or in single and click OK.
Start Time	Set start time.
End Time	Set end time.
Min Interval(s)	Set the Min Intervals(s).
Similarity	Enter or Set the Similarity.
Gender	Set gender as Unknown, Male, or Female.
Age	Set age as per list: under 18, 18 to 25 years old, 26 to 30 years old, 31 to 35 years old, 36 to 40 years old, 41 to 50 years old, and 51 years old and above.
Mouth Mask	Set to Unknown, Unlimited, Wear mask, and No.
Hair Style	Set to Unlimited, Unknown, long hair, and short hair.

Parameter	Description
Glasses	Set to Unlimited, Unknown, Have, and No.
Hat	Set to Unknown, Wear a Hat, and No.
Maximum Display Quantity	Set a Maximum Display Quantity.
	Table 4- 15 Personnel Frequency Retrieval

Step 2: Click Search to complete.

4.5 Intelligent

Click Video Management, then select Intelligent.

G	Video View	>	Intelligent Video / Intellig	ent / Algorithm Model			
5	Device Management	>	Camera Name	Algori	thm Model	• Q @	
<u></u>	Decoding On The Wall	>	🔾 Refresh 🛛 🗵 Get .	Algorithm Pattern			
	Search	>	IP Address	Camera Name	Channel Code	Algorithm Model	Operations
(B)	Intelligent	~					
	Algorithm Model						
	Target Intelligence						

Figure 4-37 Intelligent

4.5.1 Algorithm Model (AS1700 Supported)

Click Video Management> Intelligent, then select Algorithm Model.

4.5.1.1 Get Algorithm Pattern

Click Video Management> Intelligent > Algorithm Model, then select Get Algorithm Model.

4.5.2 Target Intelligence

Click Video Management> Intelligent, then select Target Intelligence.

Device Management	>	x" 7"	Target Parameters Mask Reco	gnition Target Recognition			
Device management	,		Parameter Configuration				
Decoding On The Wall	>		Target Capture	Target Properties	Detection Mode	Capture Mode	
Decoung on the num	·				Object Dete	Optimization <	
Search	>		Alarm Detection Interval (\$)	Target Detection Sensitivity	Overall Sensitivity Of Target Detection	Target Minimum Size	Maximum Target Size
			1	1	1	26	27
Intelligent	~		Advanced Parameters				
Algorithm Model			Send Target Matting	Send Target Global Matting	Send Panorama	Target Brightness Compensation	
Target Intelligence			1 - Number Of Pictures	1 - Number Of Pictures			
	- 1		Target Image Capture Quality	Image Capture Quality Of Target	Panoramic Image Capture Quality	Target Compensation Coefficient	Target Exposure Duration (minute
Behavior Analysis			1	1	1	1	1
Crowd Situation			Regional Settings				
General Intelligence			Video LineDrawing Crossed	Not Scribed			
Vehicle Intelligence							
venicle intelligence							
Intelligent Application			Schedule Settings				
			=+New @Delete All				
			Start Time	End Time	Date	Mode	Operations

Figure 4-38 Target Intelligence

4.5.2.1 Target Parameters

In this, parameters like **Parameter Configuration**, **Advanced Parameter**, **Regional Settings**, and **Schedule Settings** are included and can be operated according to requirement.

• Parameter Configuration

Target Parameters Mask Re	ecognition Target Recognition			
Parameter Configuration				
Target Capture	Target Properties	Detection Mode	Capture Mode	
		Object Dete 🔻	Optimization -	
Alarm Detection Interval (s)	Target Detection Sensitivity	Overall Sensitivity Of Target Detection	Target Minimum Size	Maximum Target Size
1	1	1	26	27

Figure 4-39 Parameter Configuration

Parameter	Description
Target Capture	Select Target capture as requirement.
Target Properties	Select Target properties as requirement.
Detection Mode	Set Detection mode to Object detection, Overall Target Detection, and Target and Overall Target detection.
Capture Mode	Set Capture Mode to Optimization, Speed, and Timing.
Alarm Detection Interval	Set a number to Alarm detection as requirement.
Target Detection Sensitivity	Set a Targ <mark>et</mark> Detecti <mark>on Se</mark> nsitivity.
Overall Sensitivity of Target Detection	Set an Overall Sensitivity of Target Detection.
Target Minimum Size	Set a range to Target Minimum Size.
Maximum Target Size	Set a range to Maximum Target Size.
	Table 4- 16 Parameter Configuration

Advanced Parameters

Send Target Matting	Send Target Global Matting	Send Panorama	Target Brightness Compensation	
1 - Number Of Pictures	1 - Number Of Pictures			
Target Image Capture Quality	Image Capture Quality Of Target	Panoramic Image Capture Quality	Target Compensation Coefficient	Target Exposure Duration (minutes)
1	1	1	1	1

Figure 4-40 Advanced Parameter

Parameter	Description			
Send Target Matting	Set Send Target Matting by selecting Number of Pictures.			
Send Target Global Matting Select Number of pictures to Send Target Global Mattir				
Send Panorama Select panorama as requirement.				
Target Brightness Compensation Select Target Brightness Compensation as requirement.				
Target Image Capture Quality	Set Target Image Capture Quality.			
Image Capture Quality of Target	Set Image Capture Quality of Target.			
Panoramic Image Capture Quality	Set Panoramic Image Capture Quality.			
Target Compensation Coefficient	Set Target Compensation Coefficient.			
Target Exposure Duration (minutes)	Set Target Exposure Duration (minutes).			
Table 4, 17 Advanced Devenses				

Table 4-17 Advanced Parameter

Regional Settings

Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4- 41 Regional Settings

In Regional Settings select Video Line Drawing as Crossed or Not Scribed.

• Schedule Setting

Schedule Settings				
EFNew Delete All				
Start Time	End Time	Date	Mode	Operations
		Every Day 👻	No Cycle 👻	Ê
		Every Day 👻	No Cycle 👻	Ê

Figure 4-42 Schedule Setting

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one click ¹ to complete delete option.

4.5.2.2 Mask Recognition

Parameter Configuration

Parameter Co	nfiguration	
Alarm Type	Close	Ŧ

Figure 4-43 Parameter Configuration

Set Alarm Type to Close, No Mask, and Have a Mask.

Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
		1

Figure 4-44 Audible Alert

Set Audible Alert in options like Audio Alarm, Audio Output, and Count.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
	Low Freque 💌	1

Figure 4- 45 Light Flashing Alarm

Parameter	Description			
Light Flashing Alarm	Set Light Flashing Alarm if require.			
Light flashing Frequency	Set Light flashing Frequency as Low Frequency, Hight Frequency, Medium Frequency, and Steady On.			

Parameter	Description	
Light flashing time	Set Light flashing time if require.	
	Figure 4- 46 Light Flashing Alarm	

• Schedule Settings

Schedule Settings				
=+New Delete All				
Start Time	End Time	Date	Mode	Operations
		Every Day 🔻	No Cycle 🔻	Ē

Figure 4-47 Schedule Settings

New

Click **New** to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

4.5.2.3 Target Recognition

• Parameter Configuration

It includes Enable Target recognition, Target Parameter Model, Target Recognition Model, and Usage Mode.

Enable Target R	
Target Recognit	
Usage Mode	Target Feature Colla

Figure 4-48 Parameter Configuration

Click **OK** to save and exit.

4.5.3 Behavior Analysis (AS1700 Supported)

4.5.3.1 IGT Alarm Config

Enable Behavioural	🔘 En	able	•	Disable
Send Metadata	🔿 En	able	•	Disable
Perimeter Enhance	O En	able	•	Disable
Alert Inhibition	🔵 En	able	•	Disable
Alar <mark>m Pic Ailnfo</mark>	🔿 En	able	•	Disable
Shadow Removal Mode	Weak	Shad	low 👻	
Detection Sensitivity	Low S	ensit	ivity 👻	
Background Update Rate	Low			
Min Target Size	5	×	5	
Max Target Size	5	×	5	1

Figure 4- 49 IGT Alarm Configuration

4.5.3.2 Intrusion Detection

• Parameter Configuration

Parameter Configuration		
Target Detect: Pedestrian Motor Vehicle	Non-motorized Vehicles	
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center -	1

Figure 4- 50 Parameter Configuration

Set Target Detect as Pedestrian, Motor vehicles, and Non-motorized Vehicles.

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

• Audible Alert

Audible Alert			
Audio Alarm		Audio Output	Count
🔿 Enable 🔾	Disable		1

Figure 4-51 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set Count for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
C Enable C Disable	Low Frequency -	1

Figure 4- 52 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings

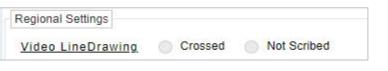


Figure 4- 53 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings				
Ξ+New DDelete All Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4- 54 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one-click ¹/₁ to complete delete option.

4.5.3.3 Perimeter Line

• Parameter Configuration

Parameter Configuration		
Target Detect: Pedestrian Motor Veh	icles Non-motorized Vehicles	
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center	1

Figure 4-55 Parameter Configuration

Set Target Detect as Pedestrian, Motor vehicles, and Non-motorized Vehicles.

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

• Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
O Enable O Disable	•	1

Figure 4- 56 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set Count for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

Figure 4-57 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings

Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4-58 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings =+New @Delete All Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4- 59 Schedule Settings

• New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁₀ to complete delete option.

4.5.3.4 Region Entrance Detection

• Parameter Configuration

Parameter Configuration		
Target Detect: Pedestrian Motor Vehicle	es Non-motorized Vehicles	
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center	1

Figure 4-60 Parameter Configuration

Set Target Detect as Pedestrian, Motor vehicles, and Non-motorized Vehicles.

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

• Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
O Enable O Disable		1
	Figure 4- 61 Audible Alert	
Set Audio Alarm to Enable or	Disable.	
Set Audio Output.		
Set Count for Audible Alert.		
• Light Flashing Alarm		
Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

Figure 4- 62 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings

Regional Settings			
Video LineDrawing	Crossed	Not Scribed	

Figure 4-63 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

ichedule Settings ⊒+New @Delete All Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4- 64 Schedule Settings

New

Click **New** to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

4.5.3.5 Region Exiting

Parameter Configuration

Parameter Configuration		
Target Detect: Pedestrian Motor Vehicle	s Non-motorized Vehicles	
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center -	1

Figure 4-65 Parameter Configuration

Set Target Detect as Pedestrian, Motor vehicles, and Non-motorized Vehicles.

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

• Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
O Enable O Disable		1

Figure 4-66 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set Count for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

Figure 4-67 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings



Figure 4-68 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings =+New @Delete All Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-69 Schedule Settings

New

Click **New** to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

4.5.3.6 Object Left

Parameter Configuration			
Alarm Detection Interval (s)	Recognize Mode	Sensitivity	Alarm Tolerance Time(second)
1	Center •	1	1
	Figure 4- 70 Paramet	er Configuration	
Set Alarm Detection Inte	erval(s).		
Set Recognize Mode as C	enter, Bottom, and Top.		
Set Sensitivity as require	ement.		
Set Alarm Tolerance Tim	e(second).		
Audible Alert			
Audible Alert			
Audio Alarm	Audio	Output	Coun
C Enable Disable		-	1

Set Audio Output.

Set **Count** for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1



Figure 4-64 Light Flashing Alarm

Set Light Flashing Alarm to **Enable** or **Disable**.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings

Regional Settings			
Video LineDrawing	Crossed	Not Scribed	

Figure 4-73 Regional Settings.

Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings				
-+New Delete All				
Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-74 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one-click ¹ to complete delete option.

4.5.3.7 Object Remove

Parameter Configuration

Recognize Mode	Sensitivity
Center	1

Figure 4-75 Parameter Configuration

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
O Enable O Disable		1

Figure 4-76 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set Count for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

Figure 4-77 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings

Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4-78 Regional Settings.

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings				
⊒+New @Delete All Start Time	End Time	Date	Mode	Operations
ок				

Figure 4-79 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click 🏛 to complete delete option.

4.5.3.8 Loitering

• Parameter Configuration

Parameter Configuration			
Target Detect: Pedestrian Motor Vehi	cles Non-motorized Vehicles		
Alarm Detection Interval (s)	Recognize Mode	Sensitivity	Alarm Tolerance Time(second)
1	Center -	1	1

Figure 4-80 Parameter Configuration

Set Target Detect as Pedestrian, Motor vehicles, and Non-motorized Vehicles.

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

Set Alarm Tolerance Time(second).

• Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
C Enable Disable		1

Figure 4-81 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set **Count** for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

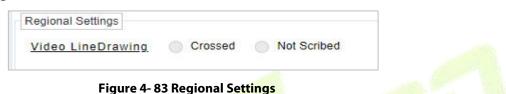
Figure 4-82 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings



Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings E+New @Delete All Start Time End Time	e Da	te Mode	e Operations
ок			

Figure 4-84 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ^{III} to complete delete option.

4.5.3.9 Fast Move

Parameter Configuration

Parameter Configuration		
Target Detect: Pedestrian Motor	Vehicles Non-motorized Vehicles	
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center	1

Figure 4-85 Fast Move

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set Sensitivity as requirement.

• Audible Alert

Audible Alert			
L'and a state of the state of the			
Audio Alarm		Audio Output	Count
O Enable	O Disable		1

Figure 4-86 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set **Count** for Audible Alert.

Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency	1

Figure 4-87 Light Flashing Alarm

Set Light Flashing Alarm to **Enable** or **Disable**.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings

12 - Alexandre III - Alexandre		100
Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4-88 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings				
<u>−</u> New D elete All				
Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-89 Schedule Settings

• New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

4.5.3.10 Electric Bike

• Parameter Configuration

Parameter Configuration		
Alarm Detection Interval (s)	Recognize Mode	Sensitivity
1	Center	1

Figure 4-90 Parameter Configuration

Set Alarm Detection Interval(s).

Set Recognize Mode as Center, Bottom, and Top.

Set **Sensitivity** as **requirement**.

• Audible Alert

Audible Alert			
Audio Alarm		Audio Output	Count
O Enable (Disable	•	1

Figure 4-91 Audible Alert

Set Audio Alarm to Enable or Disable.

Set Audio Output.

Set **Count** for Audible Alert.

• Light Flashing Alarm

Light Flashing Alarm		Light Flashing Freque	псу	Light Flashing Time
O Enable O Disable		Low Frequency	~	1
	Figure	4-92 Light Flas	hing Alarm	14
Set Light Flashing /	Alarm to Enable or Disa	ıble.		
Set Light Flashing I Dn.	requency to Low Freq	uency, Mediu	<mark>n frequency, High frequer</mark>	ncy, and Steady
Set Light Flashing	time as required.			
Regional Sett	ings			
	Regional Settings			

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Date Mode Operation	Schedule Settings				
Date Mode Operation	-+New Delete All				
	Start Time	End Time	Date	Mode	Operation
	Start Time	End Time	Date	Mode	

Figure 4-94 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

4.5.4 Crowd Situation

Ž Video View >	Intelligent Video / Intellig	ent / Crowd Situation				
Device Management >	*" 7 ^K	4 Line Crossing Statistics	Queue Length Population Density	Heat Map Off Duty Detection		
Device management /		Parameter Configuration				
Decoding On The Wall >		Enable Line Crossing Statistics		Zero Clearing Enable		Statistics Reset
						ŵ
Search >		Alarm Detection Interval (s)		Alarm Number		
		1		1		
ntelligent v		Audible Alert				
Algorithm Model		Audio Alarm				
Target Intelligence		Light Flashing Alarm				
Behavior Analysis						
Crowd Situation		Light Flashing Alarm				
General Intelligence						
		Regional Settings				
Vehicle Intelligence		Video LineDrawing C	crossed O Not Scribed			
Intelligent Application						
		Schedule Settings				
		=+New Delete All				
		Start Time	End Time	Date	Mode	Operations
		ок				



4.5.4.1 Line Crossing Status

Parameter Configuration		
Line Crossing Statistics		
Parameter Configuration		
Enable Line Crossing Statistics	Zero Clearing Enable	Statistics Reset
		血
Alarm Detection Interval (s)	Alarm Number	
1	1	

Figure 4-96 Parameter Configuration

Set Parameters like Enable Line Crossing Statistics, Zero Cleaning Enable, Statistics Reset, Alarm Detection Interval(s), and Alarm Number.

Audible Alert



Figure 4-97 Audio Alert

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency 👻	1

Figure 4-98 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings



Figure 4-99 Regional Settings.

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings				
=+New @Delete All				
Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4- 100 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one-click ¹ to complete delete option.

4.5.4.2 Queue Length

• Parameter Configuration

Parameter Configuration			
Enable Queue Length			
Alarm Detection Interval (s)	Single Processing Time	Alarm Threshold(minute)	Sensitivity
4	1	1	1

Figure 4-101 Queue Length

Set Parameters like Enable Queue Length, Alarm Detection Interval(s), Single Processing Time, Alarm Threshold(minute), and Sensitivity.

• Audible Alert



Figure 4- 102 Audio Alert

• Light Flashing Alarm

ight Flashing Frequency	Light Flashing Time
ow Frequency	1

Figure 4-103 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings

Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4-104 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings	End Time	Date	Mode	Operations
ОК				

Figure 4- 105 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ^{III} to complete delete option.

4.5.4.3 Population Density

• Parameter Configuration

Parameter Configuration		
Enable Population Density		
Alarm Detection Interval (s)	Alarm Threshold (people)	Sensitivity
1	1	1

Figure 4-106 Parameter Configuration

Set Parameters like **Enable Population Density**, **Alarm Detection Interval(s)**, **Alarm Threshold(people)**, and **Sensitivity**.

Audible Alert



Figure 4-107 Audible Alert

• Light Flashing Alarm

Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency 🔻	1

Figure 4- 108 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

• Regional Settings

Regional Settings			
Video LineDrawing	Crossed	Not Scribed	

Figure 4-109 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings				
=+New Delete All				
Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-110 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹ to complete delete option.

4.5.4.4 Heat Map

• Parameter Configuration

Parameter Configuration	
Enable Heat Map	Send Metadata

Figure 4-111 Parameter Configuration

Set Parameters Like Enable Heat Map and Send Metadata.

Regional Settings



Figure 4-112 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

4.5.4.5 Off Duty Detection

TKBio CVSecurity	::: ¥					e admin1
Ca Video View	Intelligent Video / Intelligent /	Crowd Situation				
Device Management >	² 7 ⁴	Line Crossing Statistics Parameter Configuration	tueue Length Population Density Heat Map	Off Duty Detection		
Decoding On The Wall >		Enable Off Duty Detection	Is Metadata Superimpo	ised On The Alarm Snapshot?		
Search >		Number Of Posts	Departure Time(s)		Alarm Detection Interva	al (s)
🗳 Intelligent 🗸 🗸		Audible Alert				
Algorithm Model		Audio Alarm				
Target Intelligence		Light Flashing Alarm				
Behavior Analysis Crowd Situation	«	Light Flashing Alarm				
General Intelligence		Regional Settings				
Vehicle Intelligence		Video LineDrawing Crossed	Not Scribed			
Intelligent Application						
		Schedule Settings				
		=+New Delete All				
		Start Time	End Time	Date	Mode Op	perations
C Statistics		ОК				
Video Patrol >						
@ Maintenance Configur >						
		Figure 4	- 113 Regional Settin	ngs		
Paramete	er Configurat	tion				
Parameter Configuration	1					
Enable Off Duty Detect	tion		Is Metadata Superimposed On The A	larm Snapshot?		
Number Of Posts			Departure Time(s)			Alarm Detection Interval (s)

Figure 4- 114 Parameter Configuration

1

Set Parameters like Enable Off Duty Detection, Is Metadata Superimposed on The Alarm Snapshot, Number of Posts, Departure Time, and Alarm Detection Interval(s).

Audible Alert

1

Audible Aler
Audio Alar
~

Figure 4-115 Audio Alert

• Light Flashing Alarm

Light Flashing Frequency	Light Flashing Time
Low Frequency -	1

Figure 4-116 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

1

• Regional Settings

Regional Settings		
Video LineDrawing	Crossed	Not Scribed

Figure 4-117 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

• Schedule Settings

Schedule Settings				
<u>-</u> ∓New @Delete All Start Time				
Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-118 Schedule Settings

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹ to complete delete option.

Click **OK** to save and exit.

4.5.5 General Intelligence (AS1700/ZKNVR Supported)

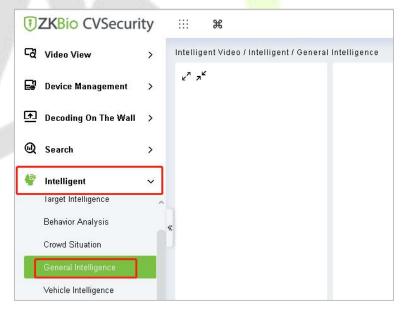


Figure 4-119 General Intelligence

• Privacy Protection Setting

Privacy Protection Settings		
Privacy Protection Settings	Enable	Disable

Figure 4-120 Privacy Protection Setting

Set Privacy Protection Setting as **Enable** or **Disable**.

• Parameter Configuration

Parameter Configuration	
Motion Detect: O Enable O Disable	
Alarm Detection Interval (s)	Sensiti
1	1

Figure 4-121 Parameter Configuration

• Audible Alert

uib	le	AI	er	t	
udi	0,	Ala	arr	n	
-					
	22512	2220202000	22112012423		udio Alarm

Figure 4-122 Audible Alert

Light Flashing Frequency	Light Flashing Time
Low Frequency -	1

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings

Crossed	Not Scribed
	Crossed

Figure 4-124 Regional Settings

Set Video Line Drawing as Crossed or Not Scribed.

Schedule Settings

Schedule Settings E+New Delete All Start Time	End Time	Date	Mode	Operations
ок				

Figure 4-125 Schedule Settings

New

Click **New** to add new schedule for Start time, End Time, Date, Mode, and Operations.

Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁₀ to complete delete option.

4.5.5.1 Lens Blocking

• Parameter Configuration

Parameter Configuration	
Lens Blocking: O Enable O Disable	
Alarm Detection Interval (s)	Sensitivity
1	1

Figure 4-126 Parameter Configuration

Set Parameters like Enable or Disable Lens Blocking, Alarm Detection Interval(s), and Sensitivity.

Audible Alert

Audible Alert		
Audio Alarm	Audio Output	Count
O Enable O Disable		1
	Figure 4- 127 Audible Alert	
Set Audio Alarm to Enable or Disab l	le.	
Set Audio Output.		
Set Count for Audible Alert.		
Light Flashing Alarm		
Light Flashing Alarm		
Light Flashing Alarm	Light Flashing Frequency	Light Flashing Time
O Enable O Disable	Low Frequency 👻	1

Figure 4- 128 Light Flashing Alarm

Set Light Flashing Alarm to Enable or Disable.

Set Light Flashing Frequency to Low Frequency, Medium frequency, High frequency, and Steady On.

Set Light Flashing time as required.

Regional Settings



Figure 4- 129 Regional Settings

• Schedule Settings

Schedule Settings ===New @Delete All Start Time	End Time	Date	Mode	Operations
ОК				

Figure 4-130 Schedule Settings

New

Click **New** to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁₀ to complete delete option.

4.5.5.2 Sound Detect

Rise Audio

Rise Audio				
Enable Rise Audio: 🔵 Enable 🔵 Disable	Enable Alarm A	udio: 🔵 Enable 🔵 Disable		
Sensitivity: 1	Audio Output:		C	punt 1
I+New Delete All				
Start Time	End Time	Date	Mode	Operations

Figure 4-131 Rise Audio

Set Rise Audio and Alarm Audio as Enable or Disable.

Set Sensitivity, Audio Output and Count.

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹ to complete delete option.

Decline Audio

Decline Audio					
Enable Decline Audio: O Enable Sensitivity:	O Disable	Enable Alarm Audio: O Enable O D Audio Output:	isable	Count 1	
<u>=</u> +New ÎDelete All Start Time	End Time	Date	Mode	Operations	
ОК					

Figure 4-132 Decline Audio

Set Decline Audio and Alarm Audio as Enable or Disable.

Set Sensitivity, Audio Output and Count.

New

Click New to add new schedule for Start time, End Time, Date, Mode, and Operations.

• Delete All

Click **Delete All** to delete all schedule, if to delete individual one Click ¹/₁ to complete delete option.

Click OK to save and exit.

4.5.6 Vehicle Intelligence (AS1700 Supported)

ZKBio CVSecurity

Video View	>	Intelligent Video / Intelligent / Vehicle Intelligence
Device Management	>	
Decoding On The Wall	>	
Search	>	
Intelligent	~	
Algorithm Model		
Target Intelligence		
Behavior Analysis		
Crowd Situation		
General Intelligence		
Vehicle Intelligence	8	
Intelligent Application		
	Device Management Decoding On The Wall Search Intelligent Algorithm Model Target Intelligence Behavior Analysis Crowd Situation General Intelligence	Device Management > Decoding On The Wall > Search > Intelligent > Algorithm Model > Target Intelligence > Behavior Analysis > General Intelligence > Vehicle Intelligence >

Figure 4-133 Vehicle Intelligence

4.5.7 Intelligent Application

It Includes Mixed Detection and Live Alarm.

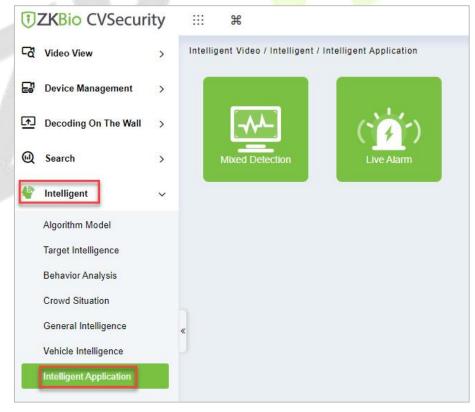


Figure 4-134 Intelligent Application

Mixed Detection

Click on Mixed Detection.

	Mixed Detection		2-08-04 14:36:10 rsday	Object(people) 0 🚊 0	Target(people)	Non Motor 0	Vehicle(set) 0	
Device List	Target Recognition	•		•				U 44 K3 W
						20		
						21-		
					Not Inst	alled Or Failed To Load.		
						isful, Please Contact Technical Support To		
				If The Installation Is Not Successful, PI	ease Contact Technical Support To Get The	Plugin.If The Plugin Has Been Installed, P	Please Try To Restart The Browser And Retry Ti	he Current Operation.
		Over	all Target/Non Motor	Vehicle Detection				
		Vehi	cle Detection					

Figure 4- 135 Mixed Detection

Device List

It will disaplays the list of devices which are connected to the software.

• Target Recognition

This function will help you to recognition of the seleted target parking vehicles.

• Live Alarm

Click **On** Live Alarm.

Device	•	Alarm Type	 Alarm Type Category	Face Recognition	Event Level Urgent,Important,
2 Full Screen	Pause Re	efresh			

Figure 4- 136 Live Alarm

Full Screen

View the video in the full screen.

• Pause Alarm.

This function will help you to pause the alarm.

4.6 Statistics

4.6.1 Face Analysis

Click Statistics > Face Analysis, then select Statistical Period as Daily, Weekly, Monthly, or Quarterly.

In this module, you can access the data for the type of personnel or person as dd, aa, VIP, or VIP, Forbidden list, pass list, and Stranger to get data to follow the options.

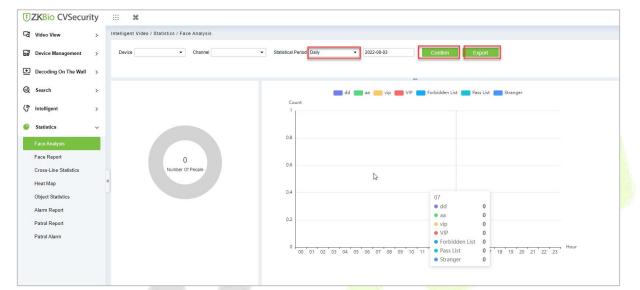


Figure 4- 137 Face Analysis

Parameters	Description
Device	Select the desired device.
Channel	Select the channel.
Statistical Period	Choose your required statistical time period.
Confirm	Click confirm to view a detailed copy of the types of people or persons.
1.39	Table 4- 18 Face Analysis

4.6.1.1 Export

Export selected personnel information in the area, you can export Excel, PDF, CSV format.

		Export	×
File Format	EXCEL		
	ОК	Cancel	

Figure 4-138 Export

4.6.2 Face Report

Click **Statistics** > **Face Report**, then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.

In this module, you can access the data for the type of personnel or person as Unknown, Juvenile (17 years old and below), Youth (18 to 35 years old), Middle Aged (36 to 59 years old), or Elderly (Over 60 years old) to get data to follow the options.

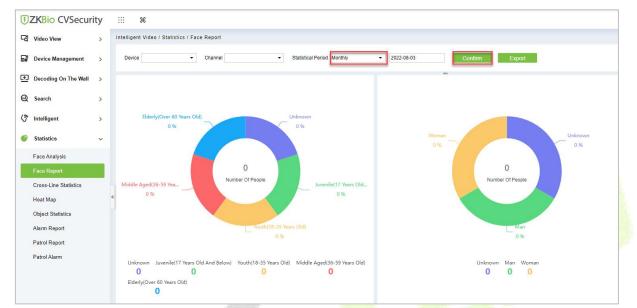


Figure 4- 139 Face Report

Description
Select the desired device.
Select the channel.
Choose your required statistical time period.
Click confirm to view a detailed copy of the types of people or persons.
Select the desired time.

Table 4-19 Face Report

4.6.2.1 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

		Export	×
File Format	EXCEL		
	ОК	Cancel	

Figure 4-140 Export

4.6.3 Cross-Line Statistics

Click **Statistics > Cross Line Statistics** then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.

In this module, you can access the data for the type of personnel or person as the number of people entering or leaving starting time to get data to follow the options.

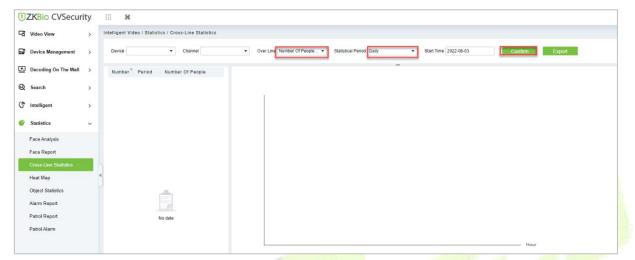


Figure 4- 141 Cross-Line Statistics

Parameters	Description
Device	Select the desired device.
Channel	Select the required channel.
Statistical Period	Choose your required statistical time period.
Confirm	Click confirm to view a detailed copy of the types of people or persons.
Over Line	Select the number of people entering or leaving.
Start Time	Select the desired time.

Table 4- 20 Cross-Line Statistics

4.6.3.1 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

		Export	×
File Format	EXCEL		
	ОК	Cancel	

Figure 4- 142 Export

4.6.4 Heat Map

Click **Statistics > Heat Map** then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.

In this module, you can access the data for the type of personnel or person as Time Heat Map and image Heat Map to follow the options.

-d Video View	>	Intelligent	Video / Statistic Personnel	s / Heat	Map ss Device	Access Rule	on Video	View			
Device Management	>	Device		•	Channel		cal Period Daily		22-08-03	Heat Map Type Time Heat Map 👻	Confirm Ex
Decoding On The Wall	>								-		
Search	>										
ntelligent 🕈	>										
Statistics	~										
Face Analysis											
Face Report											
Cross-Line Statistics		1									
Heat Map		ĸ									
Object Statistics											
Alarm Report											

Figure 4-143 Heat Map **Parameters** Description Device Select the desired device. Channel Select the required channel. **Statistical Period** Choose your required statistical time period. Confirm Click confirm to view a detailed copy of the types of Maps. Heat Map Type Select the list of Heat Map types. Start Time Select the desired time. Table 4-21 Heat Map

4.6.4.1 Export

Export selected personnel information in the area, you can export Excel, PDF, CSV format.

		Export	×
File Format	EXCEL		
	ОК	Cancel	

Figure 4-144 Export

4.6.5 Object Statistics

Click **Statistics** > **Face Report**, then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.

U	ZKDIO CVSecuri	ity	
۲ď	Video View	>	Intelligent Video / Statistics / Object Statistics
5	Device Management	>	Device Channel Channel Statistical Period Weekly 2022-08-03 Confirm Export
	Decoding On The Wall	>	
Q	Search	>	
3	Intelligent	>	
•	Statistics	~	
	Face Analysis		
	Face Report		
	Cross-Line Statistics		
	Heat Map		e de la companya de la
	Object Statistics		
	Alarm Report		
	Patrol Report		
	Patrol Alarm		
			Figure 4- 145 Object Statistics

_	
Parameters	Description
Device	Select the desired device.
Channel	Select the channel.
Statistical Period	Choose your required statistical time period.
Confirm	Click confirm to view a detailed copy of the types of people or persons.

Table 4-22 Object Statistics

4.6.5.1 Export

Export selected personnel information in the area, you can export Excel, PDF, CSV format.

		Export	;
File Format	EXCEL	×.	
	ОК	Cancel	

Figure 4- 146 Export

4.6.6 Alarm Report

Click Statistics > Alarm Report then select Alarm Type.

In this module, you can access the data for the type of personnel or person can select the start time and end time the serial number of the video channel, and different alarm types to filter the report.



4.6.6.1 Export

Export selected personnel information in the area; you can export Excel, PDF, or CSV format.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL •	
Data to Export	Selected (max 100 records)	
	Start Position 1	
	Total Records 50	
1		
	OK Cancel	

Figure 4-148 Export

4.6.7 Patrol Report

Click Statistics > Patrol Report, then select Plan Name.

In this module, you can access the data for the type of personnel or person as dd, aa, vip, or VIP, Forbidden list, pass list, and Stranger to get data to follow the options.

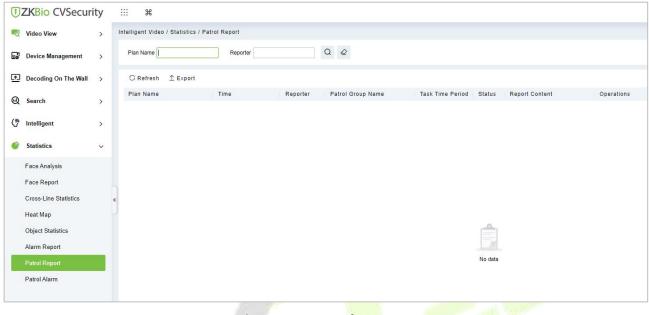


Figure 4- 149 Patrol Report

4.6.7.1 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 Selected (max 100 records) 	
	Start Position 1	
	Total Records 50	

Figure 4- 150 Export

4.6.8 Patrol Alarm

Click **Statistics > Face Analysis**, then select **Statistical Period** as Daily, Weekly, Monthly, or Quarterly.

In this module, you can access the data for the type of personnel or person as dd, aa, vip, or VIP, Forbidden list, pass list, and Stranger to get data to follow the options.

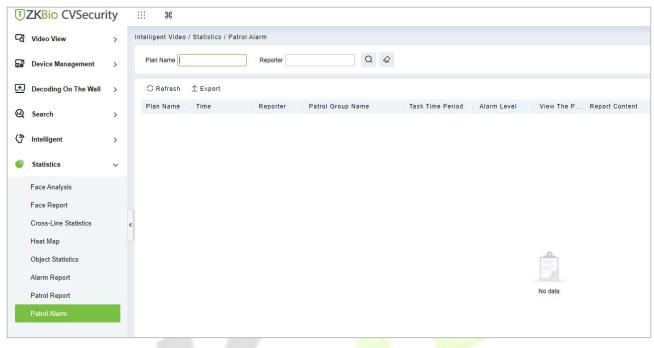


Figure 4- 151 Patrol Alarm

4.6.8.1 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL •	
Data to Export	 Selected (max 100 records) 	
	Start Position 1	
	Total Records 50	
	OK Cance	4

Figure 4-152 Export

4.7 Video Patrol

Click > Video Patrol > Patrol Group

On the preset path, you can check the punch-in by a real-time preview of the camera remotely to achieve the same patrol task as the traditional punch-in effect.

4.7.1 Patrol Group

Create a patrol group to add patrol personnel.

다. Video View	>	Intelligent Video / Video Patrol / Patrol Group
Device Mana	agement >	Patrol Group Patrol group user
Decoding on	the wall	Patrol group name Q Q
(J) Search	>	O Refresh ∓ New
(P Intelligent	>	Patrol group name Remarks Operations
		□ <u>測试</u> 测试测试测试出 <u>ℓ</u> ² *
G Statistics	>	2313 12312
🚣 Video Patrol	~	□ <u>C85</u> 2365 <u>2</u> *
Patrol Group) 	
Patrol Plan		
Real-time pat	trol	
្រាំ Maintenance	e configura >	IC < 1-3 >> J 50 rows per page + Jump To 1 /1 Page IC < 1-2 >> J 50 rows per page + Jump To 1 /1 Page

Figure 4-153 Patrol Group

4.7.1.1 New

Click Video Patrol> patrol group> New to enter the new editing interface:



Figure 4-154 New Patrol Group

Patrol Group Name: Enter the name of the patrol group for easy searching and management non-repeatable.

Remarks: Text notes of the patrol group.

4.7.1.2 Delete

Select the patrol group name and click this button to delete it.

4.7.1.3 Add Patrol Group User

In the patrol group list, click Add User to enter and select to add group members.

TZKBio CVSecurity	······································	
Cđ Video View >	Intelligent Video / Video Patrol / Patrol Group	
Device Management >	Patrol Group C Patrol Group User	
Decoding On The Wall	Patrol Group Name Q Q	
(Search >	O Refresh 🛱 Delete User	
(* Intelligent >	Patrol Group Name Remarks Operations Add User X 111 111 2 Username Q Q	
Statistics		
Video Patrol Patrol Group Patrol Plan Real-Time Patrol	If Ifford Image: Second secon	
	OK Cancel	

Figure 4- 155 Add Patrol Group User

Select the required patrol users and click the OK button to complete the addition. The added users will be displayed in the group member list on the right.

Note: Patrol users are users of the system. For adding users to the system, please refer to Adding Users.

4.7.1.4 Delete User

Select the Username and click this button to delete it.

4.7.2 Patrol Plan

Set a patrol plan for the patrol team.

d Video View	>	Intelligent Video / Video Pat	rol / Patrol Plan					
Device Management	>	Plan name	Q @					
Decoding on the wall	>	◯ Refresh 🔤 New	🖻 Delete					
Search	>	📋 📔 Plan name	Start date	End date	Patrol group name	Number of interactive cameras	Operations	
		55	2022-01-27	2022-02-03	测试	1	<u>e</u>	
Printelligent	>	22222	2022-01-27	2022-02-03	测试	1	<u>/</u> 🔟	
Statistics	>	<u> </u>	2022-01-27	2022-02-03	测试	1	_ ₪	
Video Patrol	~	33	2022-01-27	2022-02-03	测试	1	<u>/</u> 🖻	
Patrol Group		22	2022-01-25	2022-02-01	测试	2	_	
Patrol Plan		test8888	2022-01-24	2022-01-31	测试	1	<u>e</u>	
Real-time patrol		test9999	2022-01-24	2022-01-31	测试	1		
		9999	2022-01-20	2022-01-27	測试	1	_	
		<u>8</u>	2022-01-20	2022-01-27	测试	0	<u>/</u> 🖻	
		🗆 Z	2022-01-20	2022-01-27	测试	3	_ ₪	
		2	2022-01-19	2022-01-26	测试	1	<u>e</u>	

Figure 4- 156 Patrol Plan

4.7.2.1 New

Click **Video Patrol> patrol plan> New** to enter the new editing interface:

Plan name*						Patrol Group* 测试 •																			
Start d	ate*				2	022-	-02-0)7							Er	nd da	ite*				20	22-02-1	4		
0)elete			Û	Dele	te al	I																		
Mo	0	1.	2	T.	4		6	1.	8	L	10	1	12	T.	14	T.	16	1	8	20)	22	L.	24	
Tu	0		2		4		6		8		10		12		14		16	1	8	20)	22		24	
We	0	i.	2	i.	4	i.	6	i.	8	1	10	r.	12	i.	14	i.	16	ر. 10	8	20)	22	i.	24	
Th	o		2		4		6		8		10		12		14		16	, la	8	20)	22		24	
Fr	0		2		4		6		8		10		12		14		16	1	8	20)	22		24	
Sa	0		2		4		6		8	Ľ.	10		12		14		16	i. 1	8	20	j	22		24	
Su	0		2		4		6		8	ī.	10		12		14		16	1	8	20)	22		24	

Figure 4-157 New

The fields are described as follows:

Parameters	Instructions
Plan Name	Give the plan a name, make it easy to view and find, not repeatable
Patrol Group	Optional created patrol group.
Start Date	Set the start date of the patrol. The start date must not be less than the end date.
End Date	Set the end date of the patrol. The start date must not be less than the end date.
Patrol Time	Drag the time bar to select the time period that needs to be patrolled. Multiple copies are supported.

Table 4-22 New

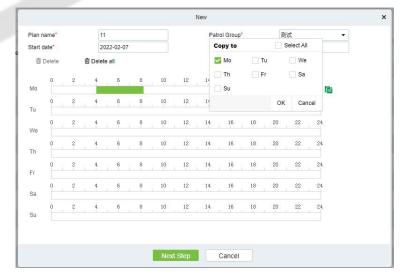


Figure 4-158 New

After editing this page, click Next to enter the camera selection interface:

				P	atrol Plan					
Number	of interactive									
Chanr	nel Name		Q &							
Alternat	tive					Selecte	d(1) 🛧 븆			
	Channel Name	Patrol	IP Address				Channel Name	Patrol	IP Address	
	10.8. <mark>1</mark> 4.109	30	10.8.14.109	^			10.8.14.107	30	10.8.14.107	
	192.168.213.166	30	192.168.213.166		_					
	测试部	30	10.8.16.120		>>					
	180	30	192.168.213.180		< <<					
	ev2001	30	10.8.14.112							
	210-kai	30	10.8.14.114							
	213.246-1 < 1-40 > >I	30 50 rows	10.8.14.110 perpage 👻	*						
			Previous Step		ОК		Cancel			

Figure 4-159 New

Number of interactive Cameras: Set the number of cameras that need to be chick-in, (like "5" means that Chick-in must be completed on 5 cameras during this patrol plan, this number must be less than or equal to the number of cameras you have chosen)

Channel Name: Search the channel

Device List: Select the equipment on the map that needs to be patrolled. The device list shows only the devices that have been added to the current map, if you want to add a device, go to Device Add

Note: You can set the length of time you need to watch each camera by clicking on the cruise time, which is 30 seconds by default

4.7.2.2 Delete

Select the Patrol Plan to be deleted and click the Delete button

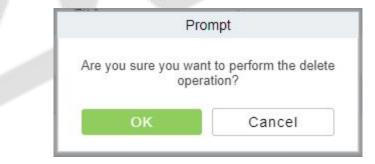


Figure 4-160 Prompt

Note: Ongoing or pause plans cannot be deleted, please complete the plan first.

4.7.3 Real-Time Patrol

Online patrols are only available if the patrolman is logged into the system.

G	Video View	>	Intelligent Video / Vid	Intelligent Video / Video Patrol / Real-time patrol							
F	Device Management	>	Video operation		Patrol Plan						
			1	0	Plan name	Start date	End date	Patrol Group	Total number of	Number of interactive cameras	Patrol plan status
	Decoding on the wall	>	Not started	In progress					videos		
Q	Search	>	0	0	¹¹ Video Device	2022-02-07	2022-02-14	测试	1	1	Not started
(7	Intelligent	>	Pause	End	10.8.14.107						
			Today's patrol task li								
G	Statistics	>	 Op Task list 	51							
4	Video Patrol	~		00-08:12(11)							
	Patrol Group		Ŭ								
	Patrol Plan								Start patrol		
	Real-time patrol										
Ō	Maintenance configura	. >									



Video Operation:

Video operation	
1 Not started	0 In progress
0	0
Pause	End

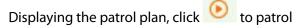
Figure 4-162 Video Operation

View different states of the Patrol plan

Today's Patrol Task List:

day's pa	atrol task list
Op	Task list
\odot	04:00-08:12(11)

Figure 4- 163 Today's Patrol Task List



Patrol Plan:

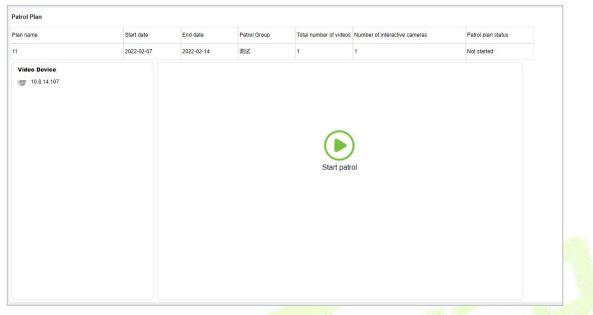


Figure 4- 164 Patrol Plan

Show patrol plan, video device, and patrol window in this area.

Patrol Window:

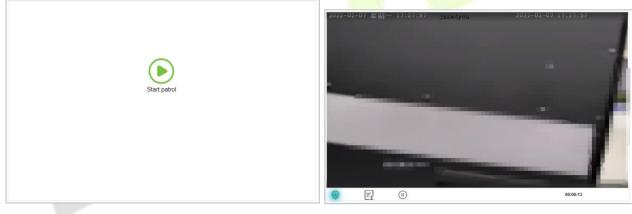


Figure 4- 165 Patrol Window

At cruising time patrolman should Check-in if required.



Figure 4- 166

Figure 4-156 Patrol Window

The check-in button blinks continuously when the check-in point is required.

Click to report the ala	ırm.			
		Alarm report	×	
	PatrolAlarm_name* Reporter* Channel Name	11 test-1 10.8.14.107		
	Alarm level* Capture a photo* Report content*			
	Figure 4	Cancel		
Click 🔟 to Pause the p	lan			
Video Device		Start patro	9	

Figure 4- 168 Video Device

After that, it automatically switches to the next camera.

When all the cameras have been cruised, a Report Window will pop up.

PatrolAlarm_name*	11	
Reporter*	test-1	ĺ
Report content*]

Figure 4- 169 Report Patrol Report

Submit the report to finish the patrol plan.

an name	Start date	End date	Patrol Group	Total number of video	s Number of in	teractive cameras	Patrol plan status
	2022-02-07	2022-02-14	测试	1	1		End
Video Device			Total number of videos	Patrol comp Number of alarms Nu		Number of missed cards	
			1	0	1	0	

4.8 Maintenance Configuration (AS1700 Supported)

4.8.1 Developer Log

Click Intelligent Video > Maintenance Configuration, then select One-Click Collection.

Users can download all system logs and system information to get Click on the **One-Click Collection** option.

TKBio CVSecurity	¥
⊂a Video View >	Intelligent Video / Maintenance Configuration / Developer Log
Device Management >	
☐ Decoding On The Wall >	
€ Search >	
Intelligent >	
C Statistics	
🛃 Video Patrol >	
🔯 Maintenance Configur 🗸	One-click Collection (Download All System Logs, System Information, Etc.)
Developer Log	
Client Request Log	
CU Request	
Parameters	

Figure 4-171 One-Click Collection

4.8.2 Client Request Log

4.8.2.1 Clear All Data

Click Clear All Data to pop up the prompt and click OK to clear all Data Operations.

IZKBio CVSecurity	::: ¥
ିର୍ପ Video View >	Intelligent Video / Maintenance Configuration / Client Request Log
Device Management >	Path Request Result IP Address Q
Decoding On The Wall >	C Refresh 💼 Clear All Data ⊥ Export
€ Search >	Creation Time Path Request Result Time Consuming IP Address
Intelligent >	
C Statistics	
🛃 Video Patrol >	
Maintenance Configur 🗸	«
Developer Log	
Client Request Log	
CU Request	
Parameters	No data

Figure 4-172 Client Request Log

4.8.2.2 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

	Export	
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 Selected (max 100 records) 	
	Start Position 1	
	Total Records 50	

Figure 4-173 Export

4.8.3 CU Request

4.8.3.1 Clear All Data

Click Intelligent Video > Clear All Data to pop up the prompt and click OK to clear all Data Operations.

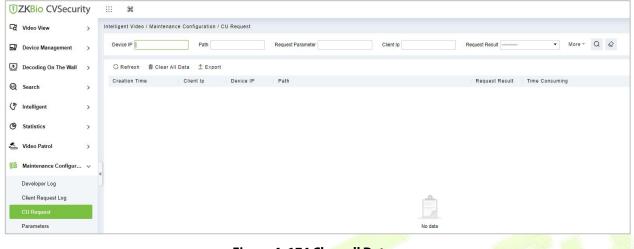


Figure 4-174 Clear all Data

4.8.3.2 Export

Export selected personnel information in the area; you can export Excel, PDF, CSV format.

	Export	ډ
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 Selected (max 100 records) 	
	Start Position 1	
	Total Records 50	
	OK Cancel	

Figure 4- 175 Export

4.8.4 Parameters

Click Intelligent Video > Parameters, then Set up all the settings, then Click OK.

UZKBio CVSecu	rity	::: ¥		e admin
Ca Video View	>	Intelligent Video / Maintenance C	Configuration / Parameters	
Device Management	>	CU Server Para	meter Settings	CU Server Parameter Settings Browser Controls
Decoding On The Wall	>		CUServer HTTP Url	Log Parameter Settings
Q Search	>		http://127.0.0.1:58098	
🖨 Intelligent	>		CUServer WS Uri ws//127.0.0.150060/websocket	
G Statistics	>		Server IP	
📥 Video Patrol	>		102.05	
Maintenance Configur	~		102.05	
Developer Log		<	WS state Connect	
Client Request Log		1		
CU Request Parameters		Browser Contro	ls	
			Current Version : Not Installed Or Failed To Load.	
			File Storage Location	
			Change Path Restore Path	
		Log Parameter	Settings	
			Debug log	
			No 👻	
			Access log	
Video intercom	>		OK	

Figure 4- 176 Parameters

4.9 Video Intercom

4.9.1 Video Intercom equipment

It mainly introduces the visual intercom application of the platform and the **Access Control** machine, mainly used for offices, and the front desk can realize the opening of the door and other applications through the visual intercom.

Operation Guide:

Step1: Add access control devices. Go to Access Control Module, Search, and add devices.

	Search No	device found? Download	d Search Tools to	Local Disk					
1	Total Progress 100%			Searched device Number of device					
	IP Address	Device 1	Гуре	Serial N	umber	(X		
	IP Address	MAC Address	Subnet Mask	Gateway Add	Serial Number	Device Type	Set Server	Operations	
	10.8.14.225	00:17:61:20:03:2D	255.255.255.0	10.8.14.1	3010163300070	ZTHCA460	http://10.8.14.12:808	Add Modify IP Address	
»	10.8.14.228	00:17:61:1 <mark>1</mark> :96:6D	255.255.255.0	10.8.14.1	4366182900001	inBIO260 Pro	https://10.8.15.99:80	This device has been added	
-	10.8.14.250	00:17:61:C2:DD:8A	255.255.255.0	10.8.14.1	3650155000020	inBIO460 Pro	http://10.8.14.15:808	Add Modify IP Address	
	10.8.1 <mark>4</mark> .31	00:17:61:10:2b:a8	255.255.254.0	10.8.14.1	CN30422170003			Add Modify IP Address	
	10.8.14.50	00:17:61:12:B2:37		10.8.14.1				Add Modify IP Address	
	10.8.14.55	00: <mark>17:61:C3:FD:18</mark>	255.255.255.0	10.8.14.1	3764164400001	C3-400Pro	https://10.8.15.99:80	This device has been added	
	192.168.134.105		255.255.255.0	192.168. <mark>1</mark> 34.1	5758204800001	xFace600		This device has been added	

Figure 4-177 Add AC Devices

Step 2: After adding, the device will automatically add to **Video Management**-Video Intercom, and you can do a Preview.

Name	9	Q &					
<mark>O r</mark>	lefresh						
	Device Name	Serial Number	Area Name	IP Address	Port	Type	Operations
	<u>10.8.14.158</u>	CKJX201460010	Area Name	10.8.14.158	80		\odot
	<u>10.8.14.207</u>	CKJX201460013	Area Name	10.8.14.207	80		⊙
	<u>192.168.161.65</u>	7299212900009	Area Name	192.168. <mark>1</mark> 61.65	80		⊙
	<u>192.168.134.105</u>	5758204800001	Area Name	192,168,134,105	80		o

Figure 4-178 Video Intercom Devices

Intelli	gen	t Video / Video inte	ercom / Video inter	com equipment					
Na	me		Q @			10	_	Preview	_
C	Re	fresh							
		Device Name	Serial Number	Area Name	IP Address	Port		1997 B	
		<u>10.8.14.158</u>	CKJX201460010	Area Name	10.8.14.158	80		-	
		10.8.14.207	CKJX201460013	Area Name	10.8.14.207		100	1000	1
		<u>192.168.161.65</u>	7299212900009	Area Name	192.168.10 ເ.ບວ	00			
		<u>192.168.134.105</u>	5758204800001	Area Name	192.168.134.105	80			0
								-	
									1000
							-		
						16			
								Close	

Figure 4- 179 Video Preview

Step 3: When someone presses the doorbell button on the device, the platform automatically pops up the call interface. You can click Sto answer.



Figure 4- 180 Incoming Call

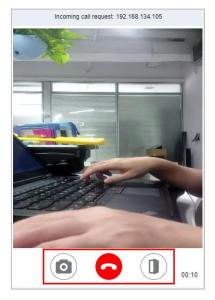
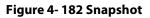


Figure 4- 181 Answering

(Capture a screenshot and will pop up the notification below.







4.9.2 Call records

Go to Video Intercom-Call records, you can view the report and see a record of all the answers, you can export the reports via excel/pdf/cvs/txt.

d Video View	>	Intelligent Video / Video	intercom / Call records				
Device Management	>	Time From 2022-04-11	00:00:00 To 2022-07-11 23:59:59 E	Device Name	Call type	More - Q 🖉	
▲ Decoding On The Wall	>	🔾 Refresh 🗴 🗊 Cle	ar All Data 1 Export				
Search	>	Call type	Call time Start Time	End Time Call duration	Area Device Name	Operator	Media File
~		Answered	2022-07-11 14:08: 2022-07-11 14:08:	2022-07-11 14:13: 249	Area Nam 192.168.134.105	admin	5
ntelligent گ	>	Cancelled	2022-07-11 14:08:	2022-07-11 14:08: 0	Area Nam 192.168.134.105		52
9 Statistics	>	No one heard	2022-07-11 14:07:	2022-07-11 14:07: 0	Area Nam 192.168.134.105		
Video Patrol	> <	Rejected	2022-07-11 14:06:	2022-07-11 14:07: 0	Area Nam 192.168.134.105	admin	53
Video intercom	~	No one heard	2022-07-11 14:06:	2022-07-11 14:06: 0	Area Nam 192.168.134.105		
	-	No one heard	2022-07-11 14:06:	2022-07-11 14:06: 0	Area Nam 192.168.134.105		5
Video intercom equipmen Call records	t	Rejected	2022-07-11 14:05:	2022-07-11 14:05: 0	Area Nam 192.168.134.105	admin	52
Call records	-	Answered	2022-07-11 13:58: 2022-07-11 13:58:	2022-07-11 14:00: 132	Area Nam 192.168.134.105	admin	1
		Cancelled	2022-07-11 13:58:	2022-07-11 13:58: 0	Area Nam 192.168.134.105		
		No one heard	2022-07-11 13:50:	2022-07-11 13:50: 0	Area Nam 192.168.134.105		1
		No one heard	2022-07-11 13:44:	2022-07-11 13:45: 0	Area Nam 192.168.134.105		
		Cancelled	2022-07-11 13:36:	2022-07-11 13:36: 0	Area Nam 192.168.134.105		5

Figure 4- 183 Call Records

Note: How to set the device?

Please Go to **Device > System > Video Intercom Parameters**, to set the intercom server address.

5 Intelligent Analysits

Scene Description:

The **Intelligent Analysits** module focuses on intelligent analysits business, and realizes design concepts such as enabling application, data analysis, process management and access control linkage based on scene application and data display through the perception and analysis ability of intelligent NVR or Intelligent cameras, providing intelligent and convenient intelligent analysits solutions for small and micro customers.

The whole module includes three menus: scenario application, business configuration and report. Scene application includes target search, People Control, Tailing Detection, Perimeter Protection, attendance checking, and people counting functions.

5.1 Scene Application

5.1.1 Target Search

Operation scenario:

Taking personnel name, ID and certificate number as retrieval conditions or uploading personnel pictures, the intelligent analysits event records of personnel within a certain time range are searched and the corresponding trend report is generated.

5.1.1.1 Personnel Information Query Intelligent Analysits Events

Operating Steps:

Step 1: In the Intelligent Scenario module, select Scenario Application > Target Search.

Step 2: In the target search interface, fill in the time period and data source, enter the name or job number of the person in the search box and click **Retrieval** to find the target.

			a Targe	et Search		
Time Frame		Data Modules		Thresholds 50		
2021-12-19 15:15:07	- 2021-12-20 15:15:07		~	0 25 50 75 100		
Gender Glass	es Mask	Upper Color	Lower Color			
Unlimited V Unlin	nited V Unlimited V	V Unlimited V	Unlimited ~			
Please enter your na	me or job number					Retrie
Trend Report						
Create Time	Report Name			Report Describe	Creater	Operate
Ground HIID	ropos tidine			Englant Broad BUD	UICald	operate

Figure 5- 1 Target Search

Step 3: After the retrieval, the retrieval results appear, as shown in Figure 5-2.

Search Res	ult									E, Generate Track Re
Query Criteria										Time Sort
		2022-02-25-22-00.44	2022 02:25 22:00.42	2022-02-25 22:00.42	2022 02 25 21:57:53	2022-02-25-21:57:51	2022-02-25-21:57:51	2022-02-25-20-29-46	2022-02-25-20-29-44	2022-02-25 20.29.44
	Unknown				1	and "				
	Unknown	2022-02-25 19:59:00	2022-02-25 18:51-26	2022-02-25 18:48:58	2022-02-25 16:46:55	2022-02-25 16:40:10	2022-02-25 18:33:24	2022-02-25 18:30.49	2022-02-25 18:29:14	2022-02-25 18:20:21
Data	2022-02-08 14;3 Unknown		-	S	N			I		2
Modules		2022-02-25 18-28-19	2022-02-25 18:28:19	2022-02-25 18:24:52	2022-02-25 18:24:52	2022-02-25 18:24:36	2022-02-25 18:24:34	2022-02-25 18:24:34	2022-02-25 18:22:00	2022-02-25 18:21-58
					Page	1 😔 total 6 pages in total				
	HoloSens SDC	0 0	0 0 0	00		0 0		0	0 0 0	0 0
	11111				00	0	00	0		
	Point Location3									
	Point Location2									
	Point Location1									
	Point Location0									

Figure 5-2 Object Lookup Retrieval Results

Step 4: In the retrieval result, you can click **Generate Trend Report** in the upper right corner of the interface to export the trend report in PDF format, as shown in Figure 5-4.

C Trend Report	tion	Target Detail
Report Name Creater Report Time Report Describe	Trend report about Stranger at 20220712 admin 2022-07-12 17:37:00	Name Unknown Gender Unknown Time Peniod Juli 11, 2022 5:34:21 PM - Juli 12, 2022 5:34:21 PM Record Type Video Record.Intelligent Scene Record Personnel ID Unknown Department Unknown
Trend Detail	10.851.130 108.水分公区 109.水分公区 109.水分公区 10.812211 7%、水分公区 10.851.135 Point Locations/PC 10.8.12.211 7%、水分公区 4%、水分公区 10.851.135 10.851.135 10.851.221 10.851.135 10.851.130 10.851.135 10.851.135 10.851.135 10.851.211 10.851.135 10.851.211 10.851.135 10.852.135	

Figure 5-3 Trend Report

Record Detail					
Event Time	Region	Event Source	Image E	vent Name	Event Grade
Jul 12, 2022 5:12:05 PM	Area Name	10楼入办公区	s	tranger	Abnormal
Jul 12, 2022 5:12:22 PM	地图	IPC_10.8.12.211	F	ace Detection Alarm	Normal
Jul 12, 2022 5:13:34 PM	地图	IPC_10.8.12.211	F	ace Detection Alarm	Normal
Jul 12, 2022 5:14:31 PM	地图	IPC_10.8.12.211	E E	ace Detection Alarm	Normal
Jul 12, 2022 5:15:15 PM	地图	IPC_10.8.12.211	F	ace Detection Alarm	Normal

Figure 5- 4 Trend Report

Intelligent Analysits detection based on video face recognition function, need to set specific function detection time period (CBL223-C01 /ZKIVA-Edge T1 supported).

5.1.2 Personnel Control

Through the construction of various types of key personnel to monitor the face database, the front-end camera is used for face capture, comparison and recognition, and an early warning is issued when the database hits.

Note: If you use Face recognition camera, such as CBL223-C01.please access the CBL223-C01 web page and make sure you have enabled the facial recognition function. Then follow the IPC Connection-Target list library to sync the list library to camera.

	ZKTECO	App Home	⊘ admin ∽
¢.		1.Parameter Settings 2.Face Library Management 3. Alert Plan 4. Linkage Policy	
		Facial recognition (first enable face detection)	
	Intelligent Analysis	Alarm interval(s) 3 Save	
×	Intelligent Alarms	(*Disabling this function may result in security risks.)	
\$	Common Intelligence	Quality filter for face images Whitelist links signal output	
Lo.	Video Quality Diagnosis	(* Enable for access control scenarios: links signal output when similarity exceeds threshold, Disable for alarm scenarios: links signal	
1	Face Detection	output when similarity is below threshold.) Fast whitelist match (configurable hit box color when enabled)	
Ľ	Facial Recognition		
	Heat Map		
		‹	

Figure 5-5 Facial Recognition Interface

5.1.2.1 Personnel List Setting

Introduces the operation of the personnel list library creation function set in the People Control pre-set.

Operating Steps:

Step 1: In the Personnel module, select Personnel Management > List Library.

Step 2: Click Add, configure the relevant parameters, and complete the new list library.

New	×
Personnal list name* Personnal list type* Description	
Save and New Ok	Cancel

Figure 5-6 Added Personnel List Library Interface

Step 3: Click the "Add Person" button on the right side of the list database information to add the personnel registered to the system to the list database, as shown in Figure 5-7.

onne	el ID		Name		Department Name Q	
ative					Selected(0)	
F	Personne	First Name	Department Name		Personne First Name Department	Name
2		1	Department Name			
1			Soluction	>>		
				>	<u>_</u>	
				<		
				<<		
					No data	
		> 50 rov	vs per page 🔻			

Figure 5-7 Add People to The List

5.1.2.2 Personnel Control

Introduce the operation Steps to realize the People Control function.

Operating Steps:

Step 1: Introduce the operation Steps to realize the People Control function.

Step 2: Click the **New** button on the application configuration interface, and in the pop-up new function pop-up window, select the **Personnel Control** option page, and set the corresponding control detection conditions, as shown in Figure 5-8. For parameter descriptions, please refer to Table 5-1 shown.

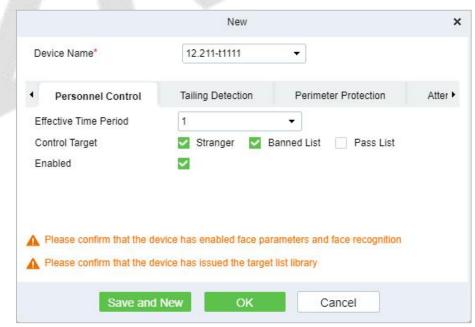


Figure 5-8 Added Personnel Control

Field Name	Field Definition
Device Name	Select the camera device for face control detection.

Effective Time Period	The People Control strategy detection period. Only the time period list can test the content of "16.4 Pre-settings".
Control Target	People Control strategy event record detection control target. For the specific list, please refer to the "16.5.1 Personnel List Settings" section.
Enable	Enable status switch of People Control policy.
	Table 5-1 Personnel Control Setting Parameter Description

Step 3: Click **OK** to save the settings.

Result Verification

Operating Steps:

Step 1: In the Intelligent Analysits module, select Scene Application > Personnel Control.

Step 2: The information displayed on the Personnel Control interface is the real-time monitoring information of the control settings that have taken effect in the system, as shown in Figure 5-9, and the interface description is shown in Table 5-2.

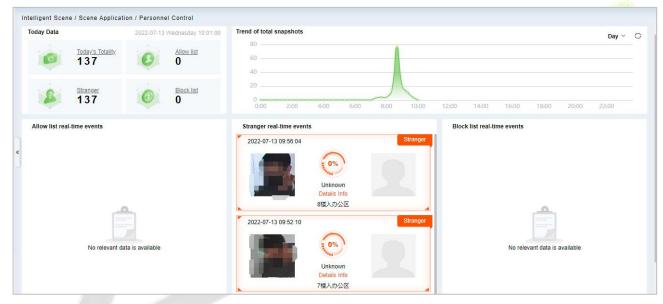


Figure 5-9 Personnel Control Real-Time Monitoring Dashboard

Field Name	Field Definition
Today's data	Relevant data of personnel management and control on the day, including today's data of the total number of snapshots, strangers, banned lists, and allowed lists, and the data is updated in real time.
The total number of snapshots and the situation	The curve chart visually displays the occurrence trend of People Control events, including four-time dimensions of day, week, month, and year.
Allowed/ Strangers/ Forbidden List Real-time Events	 Shows the real-time events of allowed/strangers/banned list personnel in real time. Each personnel control record includes the time of occurrence, snapshot photos, registered photos, similarity, library name, name, viewing related and other elements. Click the record area, support the pop-up box to view the event details of the record, click to view related, support to view other snapshot records of the person.

Table 5-2 Parameter Personnel Control Real-Time Monitoring Dashboard

Right click the Capture pictures of strangers, you can Quickly find through pictures or add personnel.



Figure 5-10 Stranger Real time

Quickly find through pictures: Ability to quickly search for personnel trajectories through captured pictures.

Click **Quickly Find Through Pictures**, would be redirected to the target search interface for image search to generate the trajectory.

igent Scene / Scene Application	n / Target Search					
			e Targe	et Search		
			Eq rurge			
Time Frame		Data Modules		Thresholds 50		
2022-07-12 15:15:16 - 2	022-07-13 15:15:16		~	0 25 50 75 100		
Gender Glasses	Mask	Upper Color	Lower Color			
Unlimited V Unlimited	✓ Unlimited ✓	Unlimited ~	Unlimited 🗸			
1						Retrieva
Trend Report						Mc
and the second second second						
Create Time	Report Name			Report Describe	Creater	Operate

Figure 5-11 Target Search Interface

Add Personnel: Quickly add captured faces to list library.

Personnel ID*	8000035	_	
		_ 1	
Department*	Department Name	- 1	-
First Name*	Rose		
Mobile Phone	343543		
			Browse

Figure 5-12 Add Personnel Option

Note: The system will automatically detect whether the captured face photo is up to standard, and the pixel is not clear will prompt the addition to fail.

	Add personnel	×
PersonnelList*	Pass List	
Personnel ID*	8000035	1
Department*		
First Name*		
Mobile Phone	Face detection failed due to:Pictur 80000 pixels	e resolution below

Figure 5-13 Add Personnel Option

5.1.3 Tailing Detection

The video face recognition is linked with the door opening event record of the **Access Control** module, and the Intelligent camera captures the face and compares it to determine the identity and job number of the person and compare it with the job number of the access control event. Entering, the snapshot cannot confirm the identity of the stranger, and realizes the key monitoring and prevention of Tailing Detection (CBL223-C01/ZKIVA-Edge T1 supported).

5.1.3.1 Tailing Detection

Prerequisites:

please enable CBL223-C01 or ZKIVA-EdgeT1 face recognition function, and sync the face library, please refer to People Control.

Operating Steps:

Step 1: In the **Intelligent Analysits** module, select **Service Configuration > Application Configuration**.

(Personnel Control	Tailing Detection	Perimeter Protection	Atter
Ef	fective Time Period	Default Time Period	*	
Bir	nd Door	10.8.14.125-1	•	
Fo	llowing of direction	💿 In Out		
Bo	und Barrier Gate	10.8.14.183-1-Out	•	
	abled			

Figure 5-14 New Tailing Detection Settings

Parameter Name	Parameter Description
Device Name	Select the camera to set the Tailing Detection function.
Effective Time Period	Set the effective time period of the Tailing Detection function, and the time period list can refer to the content in "16.4 Pre-settings".

Binding Door	Binding Door Select the door information bound to the camera with the Tailing Detection function.
Monitoring Direction	Set the direction of entrance and exit to be monitored.
Binding Channel	Select the channel information that the Tailing Detection function is bound to the camera.
Enable	The Tailing Detection settings enable switch.
	Table 5- 3 Description of Tailing Detection Parameters

Step 2: Click **OK** to save the settings.

5.1.3.2 Result Verification

Operating Steps:

Step 1: In the Intelligent Analysits module, select Scene Application > Tailing Detection.

Step 2: Perform real-time monitoring and viewing of relevant records according to the Tailing Detection doors, as shown in Figure 5-15.

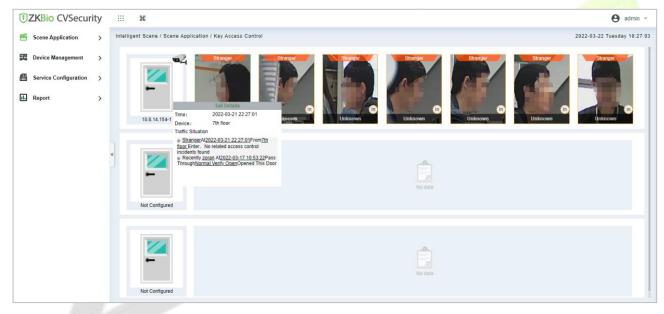


Figure 5-15 Tailing Detection Interface

5.1.4 Perimeter Protection

Through the intelligent camera crossline analysis function, Perimeter Protections are delineated in the anti-crossing areas in passages, boundaries, entrances and exits, and alarms are triggered when crossing the fence. The crossing fence realizes the empowerment and supplementation of equipment such as access gates, physical fences, and security gates, and analyzes and warns illegal crossing behaviors through computer vision.

Operating Steps:

Step 1: Access the camera web page, set the line statistics, and draw lines, as shown in Figure 5-16.

Note:

1. Please refer to the hardware suggestion list to check the supported camera. access the web page and select "Tripwire" to set the line crossing.

¢.		>	Global Configuration Intrusion Loitering Tripwire	Enter Exit Fast Move	ement			
	Network		1.Area Settings 2.Alert Plan 3.Linkage P	olicy				
	Intelligent Analysis			Detection Settings				
×	Intelligent Alarms		2022-07-13 10:50:50:59: Jane 1 111	Alarm check interval (s) Recognition mode	5 Center	~		
۵	Common Intelligence		A REAL	Sensitivity	50			
Lo.	Face Detection			Detection object	-		Non-motor vehicle	
х'n	Heat Map		P And the a	(Note: The tripwire crossing of		d rule. That is, when y	upported.) you stretch your palm outward wi direction, and the opposite is the	
鼤				Detection Areas	e anecaon your mano ponto	ia canco une positive	uncease, and the opposite is an	e negative direction.)
				🖉 Draw 🕝 Measure	Pixels			
			د ا		click Save to save the area tha	at you drew.)		
				Name No.	Name		tatus	Operation
				1	Line 1			۵ (Defended)
				Save (Note: Enabl	le global configuration before	saving the settings.)		

Figure 5-16 Set the Camera Line Crossing to Draw the Line

2. About the ZKIVA-Edge T1 setting, please refer to Perimeter alarm setting.

Step 2: In the Intelligent Scenario module, select **Service Configuration** > **Application Configuration**.

Step 3: In the application configuration interface, click **New** button, select the **Perimeter Protection** tab, and set the relevant parameters, as shown in Figure 5-17. For parameter descriptions, please refer to Table 5-4.

Device Name* 66-174-11 ● Personnel Control Tailing Detection Perimeter Protection At Effective Time Period Default Time Period Enabled ▲ Please confirm that the device has enabled the line detection function	
Effective Time Period Enabled	
Enabled	Atter •
Please confirm that the device has enabled the line detection function	
Please confirm that the device has enabled the line detection function	
Please confirm that the device has enabled the line detection function	
Save and New OK Cancel	

Figure 5-17 New Perimeter Protection Settings

Parameter Name	Parameter Description
Device Name	Select the camera to set the line-crossing function.
Effective Time Period	Set the effective time period of the perimeter protection function
Enable	The Tailing Detection settings enable switch.
	Table 5-4 Cross Fonce Parameter Sottings

Table 5- 4 Cross Fence Parameter Settings

Step 4: Click OK to save the settings.

5.1.4.1 Result Verification

Operating Steps:

Step 1: In the Intelligent Analysits module, select Scene Application > Perimeter Protection.

Step 2: View real-time monitoring data on this interface, as shown in Figure 5-18.

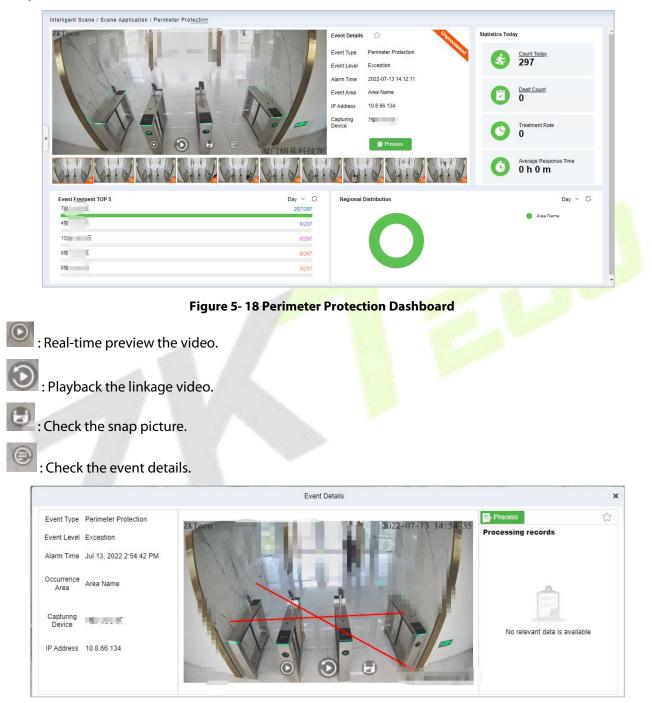


Figure 5-19 Perimeter Protection Event Details

Click Process

,you can deal with and mark the event.

20	Audit Ev	ent	×
TEST			
Add Ter	nplates - <u>Collapse Templates</u>		
Resolve	d or processed 🗴 Someone has b	een sent to the scene to confirm 🗙	
False al	arm, no abnormal condition 🗴		
Relevan	t personnel have been informed by em	ail 🗙	
The scr	eenshot has been saved 🗙 123 🗙	TEST ×	
	ОК	Cancel	
	Figure 5- 20 Perimeter Pr	otection Audit Event	
After auditing the event	s, the icon will mark to	sysmbol.	
Intelligent Scene / Scene Application / Perim		Event Details	Statistics Today
		Event Type Perimeter Protection	Count Today 327
		Event Level Exception Alarm Time 2022-07-13 14:57:02	
		Event Area Area Name P Address 10.8.66.134	Dealt Count 1
	•	Capturing 7楼入办公区 Device	C Treatment Rate 0.31%
		Process	Average Response Time
	a wat va wat va <u>wat v</u> at v	🖌 VAR 🗸 VAR 🗸 VAR 🗸	0h 6m
Event Frequent TOP 5 7楼。	Day 🗸 🗘 319/319	Regional Distribution	Day 🗸 🔿 🌑 Area Name
a de la companya de l	0/319		
1	0/319		
1 9************************************	0/319 0/319 0/319	0	

Figure 5-21 Perimeter Protection Event Interface

5.1.5 Attandance Checking Detection

Through the intelligent camera people counting function to realize the monitoring and alarm of leaving work and leaving the post, by demarcating the monitoring area, setting the monitoring of leaving work and leaving the post, the camera calculates the number of people in the area in real time, and triggers the alarm of leaving work and leaving work when no one is on duty. This function is mainly used for monitoring security Business scenarios that need to be always on duty, such as rooms, monitoring rooms, and sentry posts.

Preconditions:

The camera supports (D series) and the Crowd Density function parameter is enabled. See **Crowd Density** (Please refer to the hardware suggestion list to check the supported devices).

5.1.5.1 Attandance Checking

Operating Steps:

Step 1: Log in to the camera settings interface, select the **Crowd Density** tab in the **Advanced Configuration > Intelligent Analysis > General Intelligence** interface, and check to enable the Crowd Density function, as shown in Figure 5-22.

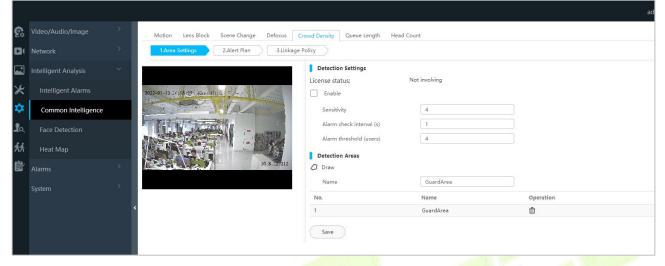


Figure 5-22 Crowd Density Monitoring with Built-In Camera

Step 2: In Intelligent Analysits module, choose Service Configuration > Application Configuration > New. Select Attendance Checking.

Tailing Detection Peri	meter Protection	Alle	ndance Checking Detection
	Default Time Period	i 🔹	
nabled			
uty plan			Shift schedule
	1	-	management

Figure 5-23 Add Attandance Checking

Parameter Name	Parameter Description
Device Name	Select the camera to set the cross-limit bar function.
Effective Time Period	Set the effective time period of the attendance checking.
Enable	Enable attendance checking detection.
Duty Plan	Click shift schedule management to set the duty plan.
	Table 5- 5 Resignation Parameter Description

Step 4: Click OK to save the settings.

5.1.5.2 Result Verification

Operating Steps:

Step 1: In the **Intelligent Analysits** module, select **Scene Application > Attendance Checking Detection.**

Step 2: The relevant data can be viewed in this real-time monitoring interface, as shown in Figure 5-24.

TXBio CVSecurity		9
😤 Scene Application 🗸	Intelligent Scene / Scene Application / Attendance Checking Detection	
Target Search	Attendance Checking Monitoring	
Personnel Control	Departure Situation Today X	
Tailing Detection	Point Location* 前台在两监测 Leave Frequency* 0	
Perimeter Protection Attendance Checking		
Detection People Counting	On Guard Departure Rate [®] 0%	
Live Alarm	前台在岗监则 Last Leave* Not Configured Not Configured Not Configured Not Configured	onfigured
My Dashboard	Close Close	
	Point Location Con Guard Rest	
2-2.11	REFEREN	
Device Management >		
Service Configuration >		
II. Report >	0000 0200 0400 0600 0800 1000 1200 1400 1600 1800 2000 2200	23:59

Figure 5-24 Attandance Checking Dashboard

Step 3: Click the **On Guard** icon, you can check the departure situation today, and generate the offduty report.

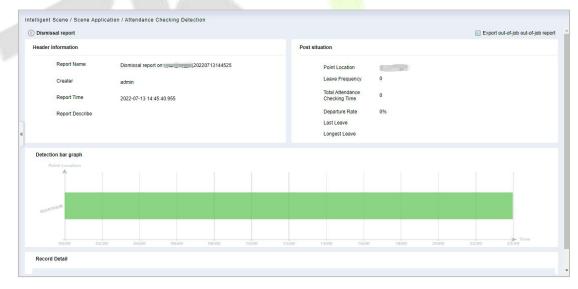


Figure 5-25 Report

5.1.6 People Counting

Counting the number of people entering and leaving the area through the crossing line statistics function of the Intelligent camera, entering +1, going out -1, setting the area capacity, calculating the number of people in the area, dynamically displaying whether the area can enter the state, and realizing its business needs, especially to meet the current epidemic situation. In the context, the passenger flow control of supermarket stores.

5.1.6.1 Result Verification

Operating Steps:

Step 1: In the Intelligent Analysits module, select Scene Application > People Counting.

Step 2: The relevant dynamic data can be viewed in the real-time monitoring interface of regional people statistics, as shown in Figure 5-43.



Figure 5- 26 People Counting Dashboard

You can change the icon that fits this area, click the icon that you can change it.



Figure 5-27 Icon Setting

Also you can check the Peak periods of passenger flow and footfall.



Figure 5-28 Passenger Flow Statistics

5.1.7 Live Alarm

Alarm events generated by all devices in the **Intelligent Analysits** module.

5.1.8 My Dashboard

Users can customize the personal data dashboard according to conditions.

Operation Guide:

Step 1: Go to **Intelligent Analysits > Service Configuration > Dashboard Configuration**.

Step 2: Click New Button, according to the condition to set the dashboard.

		New			
Configuration Name*	Today's not processed eve	Add Filter	Audit E	vent 👻	
Limit Count*	10	Is it public?	O Yes	No	
Condition					
Audit Event	Unpro	cessed 🔻			

Figure 5-29 New My Dashboard

Parameter	Parameter description			
Configuration Name	User-defined the dashboard name.			
Add Filter According to your dashboard to add the filter events				
Limit Count	The number that needs to be displayed			
ls it public?	Is it an individual view or can be seen by everyone			
Condition	Configure the condition according to the filter			
	Table 5- 6 Parameter dashboard			

Result Verification:

Go to **Scene Application** > **My Dashboard** to check the dashboard.

æ						θ	admi
elligent Scene	e / Scene Applicatio	n / My Dashboard					
					Dashboard configuration Today's not proces 👻		
oday's not pro	ocessed events					V	Û
Image	Person Na	ame Event Name	Occurred Time	Area	Operations		
No.	Unknown	Intrusion detectio	2022-07-13 16:17:43	Area Name	e		•
See .	Unknown	Zone enter detect	2022-07-13 16:17:40	Area Name	e		
	Unknown	Stranger Abnorma	2022-07-13 16:17:20	Area Name	e		
	Unknown	Stranger Abnorma	2022-07-13 16:17:20	Area Name	e		Ţ
ecord of peo	ple in the 🏦	Yesterday's latest personr	nel capture record 👔	Today's earliest personnel capture record	Yesterday's latest snapshot record o	f the	1
					personnel in the allowed list database		
		Stranger 20:28:41		Stranger 07:37:04	1225 18:31:53		
		DATE OF A DESCRIPTION OF A	Stranger 20:24:33	Strang 07:37:2	er		

Figure 5- 30 My Dashboard

5.2 Device Management

Two device addition methods are supported, one is IPC directly connecting to ZKBio CVSecurity through SDK, and the other is ZKIVA-Edge connection.

5.2.1 IPC Connection (Currently, Only Support HWSDK Camera Connection, Please

Check the Hardware Suggestion List)

Step 1: Go to **Intelligent Analysits** > **Device Management** > **Camera**, you can click Search or **New** to add the HWSDK Camera.

In	telli	gent Scene / Device Mar	nagement / Camera			
	De	vice Name	Q &			
1	С	Refresh 🔤 New 🛍	i Delete ∠ Edit Q Search Q Vi	deo storage 🛛 🛣 Modify SDK conr	nection password 🛛 🗱 Reboot	🕅 Target List Library 🛛 O Synchronize Time
		Device Name	Device Mr		× St Opera	tions
		前台在岗监测	DDS522-1 Device Name*	test	⊙ (7
		10.8.12.211	CBL223-(IP Address*	10 . 8 . 12 . 222	•	3
		10.8.12.212	DBL222-C User name*	6061 admin	• (7
«		10.8.12.115	C2120-10 SDK Password		⊙ (2
		9楼入办公区	Area Name* CBL223-(Area Name 🔹	•	<u>a</u>
		10楼入办公区	CBL223-0		⊙ (J
] 8楼入办公区	CBL223-C Save and	d New OK C	ancel 💿 (J.
		6楼入办公区	CBL223-C01 10.	8.66.115 Area Name (Dnline 🥏 💽 (2
		7楼入办公区	CBL223-C01 10.	8.66.134 Area Name (Dnline 🥏 💽 🕻	7

Figure 5-31 Add Camera

Step 2: Click ^{Leg}, access the camera's web page to set the intelligent function.

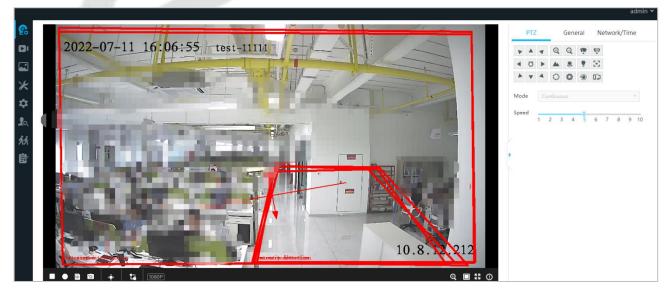


Figure 5-32 Access IPC Web Page

Q Video storage Click this button to support directly adding IPC to NVR as a storage application. (NVR needs to be added to the **Video Management** module in advance).

Int	telliger	nt Scene / Device I	Management	/ Camera								
	Device	e Name		Q @								
	O R	efresh 🛨 New	💼 Delete	🖉 Edit	Q Search	Video storage	🔓 Modify SDK c	onnection	password	🔆 Reboot	🛱 Target List Library	🔿 Synchronize Time
		Device Name		Devic	e Model	IP Address	Area Name	Status	Storage	St Operat	tions	
		前台在岗监测		DDS5	22-01		o storage	;	< •	⊙ (ø	
		10.8.12.211		CBL2	23-C01	Primary Device* ZKI	NVR-ZKNVR	-	2		ø	
		10.8.12.212		DBL2	22-01					• Ç	ø	
»		10.8.12.115		C212	0-10-CI(6	ОК	Close		2	• Ç	7	
		9楼入办公区		CBL2	23-C01	10.8.66.174	Area Name	Online	0	• Ç	7	
		10楼入办公区		CBL2	23-C01	10.8.66.198	Area Name	Online	0	• c	ø	

Figure 5-33 Video Storage

After the completion, the Storege status would be change to 🥙 .

A Modify SDK connection password Click this button to modify camera SDK password.

Intellige	ent Scene / Device Management	/ Camera							
Devi	ce Name	Q @							
OF	Refresh ∓ New 💼 Delete	🖉 Edit 🛛 Q Search	🖸 Video storage	🔓 Modify SDK co	onnection password	Reboot [Target List Library	🔾 Synchronize Time	Synchronize Device
	Device Name	Device Model	IP Address	Area Name	Status Storage St.	. Operation	15		
	前台在岗监测	DDS522-01	10.8.64.239	Modify	y SDK connection password	t	×		
	10.8.12.211	CBL223-C01	10.8.12.211	User name* SDK Password*	admin				
	10.8.12.212	DBL222-01	10.8.12.212	New Password*					
»	10.8.12.115	C2120-10-CI(6mm)	10.8.12.115	Confirm Password*					
	9楼入办公区	CBL223-C01	10.8.66.174						
	10楼入办公区	CBL223-C01	10.8.66.198	Save and New	ОК	Cancel			
	8楼入办公区	CBL223-C01	10.8.66.156	Area Name	Online 🥝	ی ا			
	6楼入办公区	CBL223-C01	10.8.66.115	Area Name	Online 🥥	• •			

Figure 5-34 Modify Sdk Password

EXTarget List Library Click this button to sync the face library (only CBL223-C01 supported), please select a list lirabry, and sync.

	Targ	et List Library				
Device Name 10楼入办公区 🔹 Name of the list lib	rary Q 🖉	Personnel ID	Nam	1e	Status	• Q &
🔿 Refresh 🔟 Select list library 🛛 🕼 Resync P	PersonnelList 🛍 Delete	C Refresh	島 Resync 薗 Dele	te		
List Library List Library Number of	Operations	Personn	e First Name	Status De	scription	
Forbidden List Banned list lib 4	≙ +	32001	ZZZ	Succeed		
Pass List Allow List Libr 54	<u>음</u> +	32004	xuyang	Succeed		
		3200334	wwwwww	Failed un	nown_error	
		3200333	ZZZ	Failed Co	mmon error.	
i< < 1-2 > >i 50 rows per page ⇒	Total of 2 records	اد د 1-4	> > 50 rov	ws per page 👻	Total of 4 records	

Figure 5-35 Sync Xface Library

O Synchronize Time Click this button to Sync time to device.

Reboot Device:

It will reboot the selected device.

Synchronize Devices:

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

Note: Synchronize 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.

5.2.2 ZKIVA-Edge Connection (Currently, Only Support ZKIVA-Edge T1 Connection)

	(Smart	Box)
--	--------	------

Step 1: Go to Intelligent Analysits > Device Management > Smart Box, click New to add the Edge.

Smart Box				<
Device Name		More - Q 🖉		
O Refresh	ΞŦNew ⊿ Edit	窗 Delete 辈 Active Report	··· More 👻	
Device		New	×	us
12.220	Device Name*	Test		ne
18.6	IP Address*	192 . 168 . 34 . 43	0	ne
-	User Name*	admin		
	Password*			
	Device Model* Area Name*	ZKIVA-Edge-X Area Name		

Figure 5-36 Add ZKIVA-Edge

Step 2: Please add camera via RTSP. Select an Edge, click **New** on the right page, enter the details of the camera 's RTSP Stream.

e	Intelligent Scene / Device Management / Smart Box			
毘	Smart Box	<	< Channel	
₿	Device Name More * Q 🖉		Channel Name More + Q Q	
	C Refresh ∓ New ∠ Edit 音 Delete 莘 Active Report … Mon		C Refresh	
	12.220 Area Name 10.8.12.220 ZKIVA-Edge-X	Online	INGM	x 66.156:554/Live A
*	18.6 Area Name 10.8.18.6 BioServer-N3	Online	Area Name* Area Name 👻	66.174:554/Live A
			12.2: Example of RTSP video stream on ZKTeco device: rtsp://username:password@IP:554/LiveMedia/ch1/Media1 Please confirm the video stream format for other manufacturers'	12.211:554/Livel A
			equipment.	66.156:554/Live A

Figure 5- 37 Add Camera to ZKIVA-Edge

Note: RTSP Format

- a. **ZKBio X series**: rtsp://username:password@IP:554/LiveMedia/ch1/Media1.
- b. **ZKIPC series**: rtsp://sername:password@IP:554/ch01.
- c. **Other Branchs:** Please contact the vendor to get the corresponding RTSP format.

Result:

After adding, you can check the status and preview the video.

annel						>
Channel Name	More	Q Q				
C Refresh ⊒ New	∠ Edit 💼 Delete					
Channel Name	IP Address N	fain Stream	Area Name	Status	Storage St	Operation
66.156z	10.8.66.156 rf	tsp://admin:admin123.@10.8.66.156:554/Live	Area Name	Online	•	•
66-174-11	10.8.66.174 rt	tsp://admin:admin123.@10.8.66.174:554/Live	Area Name	Online	•	•
	10.8.12.211 rt	tsp://admin:admin123.@10.8.12.211:554/Livel	Area Nama	Online	•	•





Figure 5-39 Preview

Step 3: Click a camera, click 📧 to config the channel.

ZKIVA-Edge T1: Support 2 intelligences: Face Recognition and Perimeter Alarm.

ZKIVA -Edge T1(16CH): Supports up to 16 channels, and can be intelligently functioned with 16 channels (16 face recognition or 16 perimeter protection, or 8 faces + 8 perimeters, etc.)



Figure 5-40 Channel Config

Perimeter Alarm: Based on Line crossing, it implements the functions of intrusion detection and perimeter protection.

Face Recognition: Based on the face recognition function, it realizes the classification and linkage management of personnel identification of different list databases

5.2.2.1 Face Recognition

	Channel Config	×
Channel Model*	Face Recognition 👻	

Figure 5- 41 Face Recognition Config

5.2.2.2 The Configuration of The Target List Library

Operation Guide: More 🔻

Step 1: Select an Edge, click Target List Library, select list library, and sync the personnel.

Note: Please go to Personnel module to creat the list library firstly.

		1	Farget List Library	¥.		
Device Name 12.220 Library Name	Q 🖉	Perso	nnel ID		Name	Status Q
🔾 Refresh 🛛 🖲 Select Personnel List		OR	efresh 🛍 De	elete Personnel	3 Resync	
List Library List Library Number of	Operations		Personne	First Name	Status	Description
Pass List Allow List Libr 54	<mark>8</mark> +		71202	kara071202	Failed	Pass List kara071202 Delivery failed Reason for f
Forbidden List Banned list lib 4	8+		71201	kara071201	Failed	Pass List kara071201 Delivery failed Reason for f
			2841	LEO	Failed	Pass List LEO Delivery failed Reason for failure:N
			47474747	higher	Succeed	
			7060722		Failed	Pass List Delivery failed Reason for failure:No fac
			70606	Leo	Failed	Pass List Leo Delivery failed Reason for failure:N
			70605	kara070605	Failed	Pass List kara070605 Delivery failed Reason for f
			70603	kara070603	Failed	Pass List kara070603 Delivery failed Reason for f
			70604	kara070604	Failed	Pass List kara070604 Delivery failed Reason for f
	E.		70607	kara070607	Failed	Pase List karan7nen7 Dalivary failad Rasson for f

Figure 5-42

Step 2: Select an Edge, click Active Report to report the picute to ZKIVA-Edge, as shown in Figure 5-43.

ΰZ	ZKBio CVSecurity III	¥				
B	Intelligent Scene / Device Manageme	nt / Smart Box				
\$	Smart Box		<	Channel		
8	Device Name	More* Q 🖉		Channel Name	Mo	ore = Q 🖉
	C Refresh ∓ New ⊿ Edit	i Delete I III Active F	Report ··· More 👻	⊖ Refresh = ∓ New	🖉 Edit 🛛 🛅 Del	ete Q Video storage
	Device Name Area Na	me IP Address	Device Model Status	Channel Name	IP Address	Main Stream
	2 12.220 Area N		Active Report	×	10.8.66.156	rtsp://admin:admin123.@
	18.6 Area N	Server Address*	https://10.8.12.63:8999/uplo	ad/T1/report	10.8.66.174	rtsp://admin:admin123.@
	»	Resend Interval*	1		10.8.12.211	rtsp://admin:admin123.@
	-	Resend times*	3		10.0.12.211	rtsp.//aunin.aunin/125.@
		Date Type*	Capture+Identification		10.8. <mark>12</mark> .115	rtsp://admin:admin123.@
		Report Feature	~		1066.156	rtsp://admin:admin123.@
		Report Picture	×		1000.150	rtsp.//admin.admin123.@
		Report Panorama	<u>~</u>		10.8. <mark>12</mark> .115	rtsp://admin:admin123.@
		Save and N	ew ОК	Cancel	t 10.8.12.211	rtsp://admin:admin123.@

Figure 5-43 Active Report

Description
Enter the addres <mark>s</mark> of the ser <mark>ver to</mark> report
Sets the resend interval for t <mark>he sam</mark> e event
Sets the number of resendings for the same event
Set the reporting data type, and the option supports "capture, recognition, capture + recognition"
Select whether to enable character reporting
Select whether to enable report images
Select whether to enable report panoramas

Result:

Please refer to the setting, after config, please check the people control dashboard.

TKBio CVSecurity	::: ¥		e admin
😤 Scene Application 🗸	Intelligent Scene / Scene Application / Personnel Control		
Target Search Personnel Control Tailing Detection Perimeter Protection Attendance Checking	Today Data 2022-07-12 Tuesday 16.36.5 Image: Stranger 361 Image: Stranger 361 Stranger 361 Image: Stranger 00	5 Trend of total snapshots	Day ~ 0
Detection People Counting Live Alarm My Dashboard	Allow list real-time events	Stranger real-time events	
Device Management Service Configuration		Unknown Details Info	

Figure 5- 44 People Control

5.2.2.3 Perimeter Alarm



Figure 5-45

Figure 5-45 Channel Configuration option

Step 1: Go to Channel Config and select Perimeter Alarm, click Go draw a line.



Figure 5-46 Draw A Line

Result:

Please refer to Perimeter Protection setting, after setting, please go to **Perimeter Protection** to check the dashboard.

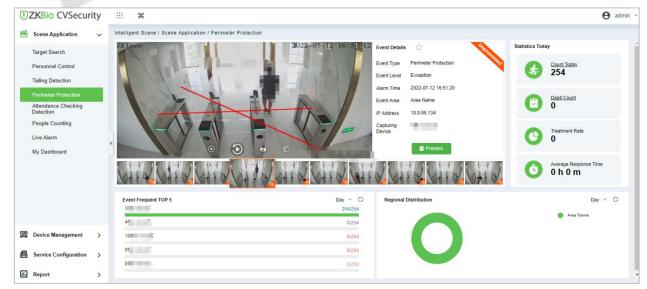


Figure 5-47 Perimeter Protection Interface

It will reboot the selected device.

Synchronize Time:

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

Synchronize Devices:

Synchronize data of the system to the device. Select device, click **Synchronize Devices** and click **OK** to complete synchronization.

Note: Synchronize 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.

Delete All Faces:

This option will help you to delete all recorded faces.

5.3 Service Configuration

5.3.1 Timezone

Operating Steps:

Step 1: In the Intelligent Analysits module, select Service Configuration > Time Zones.

Step 2: Click the **New** button and set the daily time period in the pop-up time period new function pop-up window, as shown in Figure 5-48.

												Ne	W							
Time 2 Rema		Vam	ie*																	
Û	Delete	e all																		
Мо	0	1	2	1	4	1	6	1	8		10	1	12	14		16	18	20	22	24
Tu	0		2		4		6		8		10		12	14		16	18	20	22	24
We	0	j.	2	ĩ	4	1	6	j.	8	j.	10	ĩ	12	14	į.	16	18	20	22	24
Th	0		2	1	4	1	6	1	8	1	10		12	14		16	18	20	22	24
Fr	0	1	2	1	4	1	6	1	8	1	10	1	12	14		16	18	20	22	24
Sa	0		2		4		6		8		10		12	14		16	18	20	22	24
Su	0	ĵ	2	ì	4	1	6	ĩ	8	1	10	ĩ	12	14	ĵ	16	18	20	22	24
									New		_		ЭК			Canc				

Figure 5-48 Time Period Configuration

Step 3: Click OK to save the settings.

5.3.1.1 Delete

In the **Intelligent Analysits > Service Configuration > Time zone**, select the time zone to be deleted and click **Delete or Delete icon** button under Operations. Click **OK** to delete.

IZKBio CVSecurity	¥	
Scene Application	Intelligent Scene / Service Configuration / Time Zones	
Device Management >	Time Zone Name Remarks	Q @
Service Configuration 🗸	C Refresh 🔤 New 🖬 Delete	
Time Zones	Time Zone Name Remarks	Operations
Application Configuration	Default Time Period 7 days/24 hours	
Regional Occupancy Control Configuration	🖾 a	_ ₫
Custom Icon	🗆 AA1 TT	<u> </u>
Live Alarm Configuration	Prompt	
Dashboard configuration	Are you sure you want to perform the delete operation?	
Parameter	OK Cancel	

Figure 5- 49 Delete Time Zone

5.3.2 Application Configuration

Operating Steps:

Step 1: In the Intelligent Analysits module, select Service Configuration > Application Configuration.

Per	sonnel Control	Tailing Detection	Perimeter Prote	ection Atter
Effective	Time Period	Default Time Period	*	
Bind Doo	r	10.8.14.125-1	•	
Following	of direction	In ○ Out		
Bound Ba	arrier Gate	10.8.14.183-1-Out	•	
Enabled		~		

Figure 5- 50 New Tailing Detection Settings

Parameters	Parameter Description
Device Name	Select the camera to set the Tailing Detection function.
Effective Time Period	Set the effective time period of the Tailing Detection function, and the time period list can refer to the content in "16.4 Pre-settings".
Binding Door	Binding Door Select the door information bound to the camera with the Tailing Detection function.
Monitoring	Set the direction of entrance and exit to be monitored.

Direction					
Binding Channel	Select the channel information that the Tailing Detection function is bound to the camera.				
Enable	The Tailing Detection settings enable switch.				
Table 5-8 Description of Tailing Detection Parameters					

Step 2: Click OK to save the settings.

5.3.2.1 Delete

In the **Intelligent Analysits > Service Configuration > Application Configuration**, select the Device to be deleted and click **Delete or Delete icon** button under Operations. Click **OK** to delete.

5.3.3 Regional Occupancy Control Configuration

Operating Steps:

Step 1: Access the camera background, and set the line statistics to draw lines.

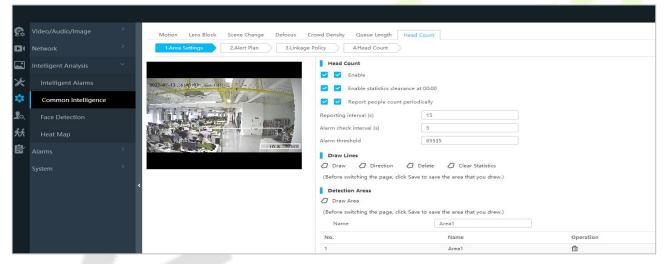


Figure 5-51 Enable Head Count

Step 2: In the **Intelligent Analysits** module, choose **Service configuration** > **Regional Occupancy Control Configuration**.

Step 3: Click the **New** button to set the parameters of the statistical range of the number of people, as shown in Figure 5-52. For parameter descriptions, please refer to Table 5-9.

ID:* Area Name:*		
Area Device:*		
Reset Strategy:	Do not Clear 🔹	
Max. Capacity:*		
Remarks:		

Figure 5- 52 Added Parameter Interface for Statistical Range

Parameter	Parameter description
ID	Custom statistics range number.
Area name	User-defined the area name.
Area device	Select the device which is used to people counting.
Reset strategy	Data statistics automatic clearing strategy setting, providing options of "no clearing" and " clearing at 00:00".
Maximum Capacity	The maximum number of personnel allowed in the custom statistics area.
Remarks	Customize the note information.
	Table 5- 9 Description of New Parameters in Statistical Range

Step 4: Click OK to save the settings.

5.3.3.1 Delete

In the Intelligent Analysits > Service Configuration > Regional Occupancy Control Configuration, select the region to be deleted and click **Delete or Delete icon** button under Operations. Click **OK** to delete.

5.3.4 Live Alarm Configuration

Alarm events generated by all devices in the Intelligent Analysits Module

Step 1: In the Intelligent Analysits module, select Service Configuration > Live Alarm Configuration.

Step 2: Click the **New** button and set the live alarm in the pop-up alarm new function pop-up window.

TZKBio CVSecurity III #	
Scene Application > Intelligent Scene / Service Configuration / Live Alarm Configuration	
Device Management >	
Service Configuration V C Refresh T New 1 Delete	
Time Zones Zuive Alarm Event Type Operations	
Application Configuration	
Regional Occupancy Control Configuration	
Custom Icon	
Live Alarm Configuration New X	
Dashboard configuration Live Alarm Configuration	
Parameter Event Type:	
* Save and New OK Cancel	

Figure 5-53 Add Live Alarm Configuration

Parameter	Parameter Description
Configuration Name	User-defined the dashboard name.
Live Alarm	Enter the live alarm name
Event Type	Enter the event type

Table 5-10 Parameter Live Alarm Configuration

5.3.4.1 Delete

In the Intelligent Analysits > Service Configuration > Live Alarm Configuration, select the Live alarm and click Delete or Delete icon button under Operations. Click OK to delete.

TZKBio CVSecurity	::: ¥	
Scene Application >	Intelligent Scene / Service Configuration / Live Alarm Configuration	
Device Management >	Live Alarm Configuration	
Service Configuration ~	⊖ Refresh 🖙 New 👔 Delete	
Time Zones	Live Alarm Event Type	Operations
Application Configuration	🔯 test Attendance Checking Detection	2
Regional Occupancy Control Configuration		
Custom Icon	Prompt	
Live Alarm Configuration	Are you sure you want to perform the delete operation?	
Dashboard configuration	OK Cancel	
Parameter		

Figure 5- 54 Delete Live Alarm Configuration

5.3.5 Custom Icon

New	×
Browse	
OK Close	

Figure 5-55 New Custom Icon

5.3.6 Dashboard Configuration

Users can customize the personal data dashboard according to conditions.

Operation Guide:

Step 1: Go to **Intelligent Analysits > Service Configuration > Dashboard Configuration**.

Step 2: Click **New** Button, according to the condition to set the dashboard, as shown in Figure 5-56. For parameter descriptions, please refer to Table 5-11.

	Nev	r		×
Configuration Name*	Today's not processed eve	Add Filter	Audit Event -	-]
Limit Count*	10	Is it public?	🔿 Yes 💿 No	
Condition				
Audit Event	Unprocess	sed 👻		
	Save and New O	K Cance	el 👘	

Figure 5-56 New My Dashboard

Parameter	Parameter Description
Configuration Name	User-defined the dashboard name.
Add Filter	According to your dashboard to add the filter events
Limit Count	The number that needs to be displayed
ls it public?	Is it an indi <mark>vid</mark> ual vie <mark>w or c</mark> an be s <mark>een by everyone</mark>
Condition	Configure the condition according to the filter
	Table 5- 11 Parameter Dashboard

5.3.6.1 Delete

In the Intelligent Analysits > Service Configuration > Dashboard Configuration, select the dashboard name and click Delete or Delete icon button under Operations. Click OK to delete.

0	ZKBio CVSecurity	···· • • • • • • • • • • • • • • • • •
B	Scene Application >	Intelligent Scene / Service Configuration / Dashboard configuration
먦	Device Management >	Dashboard name
8	Service Configuration 🗸	O Refresh ∓ New 💼 Delete
	Time Zones	Dashboard name Is it public? Operations
	Application Configuration	Today's earliest personnel capture rec Yes
	Regional Occupancy Control Configuration	Yesterday's latest personnel capture r/Yes
	Custom Icon	To: Prompt
	Live Alarm Configuration	Ye: Are you sure you want to perform the delete
	Dashboard configuration	operation?
	Parameter	OK Cancel

Figure 5-57 Delete Dashboard Configuration

5.3.7 Parameters

IZKBio CVSecurity	
Scene Application >	Intelligent Scene / Service Configuration / Parameter
Device Management >	Privacy protection configuration
Service Configuration ~ Time Zones	Enable allow list privacy protection
Application Configuration	Enable block list privacy protection
Regional Occupancy Control Configuration	
Custom Icon	
Live Alarm Configuration	Algorithm service configuration
Dachboard coofiguration	Enable face comparison service
Parameter	Yes No
<u> </u>	Enable structured analysis service for people goals
	 Yes No
	Linkage alarm configuration
	Alarm event type
	· · · · · · · · · · · · · · · · · · ·
	Whether to enable pop-up alarm
	O Yes No
	Alarm monitoring recipient email
	Example:123@xxxx.com
	Enter multiple mailboxes, separated by commas(.) or semicolons(.).

Step 1: Go to **Intelligent Analysits >Service Configuration >Parameter**.

Figure 5- 58 Parameters

5.3.7.1 Privacy protection configuration

Enable the privacy protection list for Allow list and Block List

5.3.7.2 Algorithum configuration

Enable the algorithm service configuration for face comprasion and structured analysis for people goals

5.3.7.3 Linkage alarm configuration

If alarm event occurs on this door, whether there will be alarm sound reminder for vehicle detection When any Linkage is happening, whom to notify via email.

5.4 Reports

5.4.1 All Records

Step 1: Go to Intelligent Analysits >Reports >All Records.

Step 2: We can check all the records as a list or images format.

Step 3: On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export and Click **OK**.

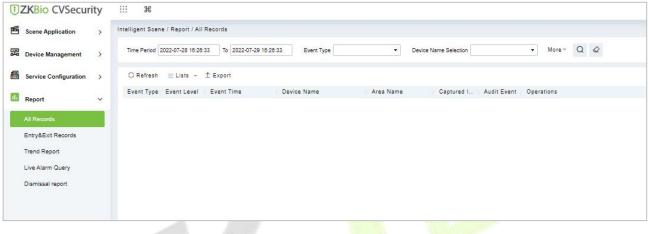


Figure 5- 59 All Records

5.4.2 Entry & Exit Records

Step 1: Go to Intelligent Analysits >Reports >Entry & Exit Records.

Step 2: We can check all the records of entry and exit as a list format.

Step 3: On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export and Click **OK**.

ZKBio CVSecur	rity	···· · · · · · · · · · · · · · · · · ·
Scene Application	>	Intelligent Scene / Report / Entry&Exit Records
Device Management	>	Time Period 2022-07-31 10:38:28 To 2022-08-01 10:38:28 Area Name All 🔹 More + Q 🖉
Bervice Configuration	>	C Refresh ⊥ Export
IL Report	~	Event Triggered Time Event Name Area Name In/Out Status Device Name
All Records		
Entry&Exit Records		
Trend Report		
Live Alarm Query		
Dismissal report		

Figure 5-60 Entry and Exit Records

5.4.3 Trend Reports

Step 1: Go to **Intelligent Analysits > Reports > Trend Records**.

Step 2: We can check all the records of trend as a list format.

Step 3: Click Delete button under Operations. Click OK to delete.

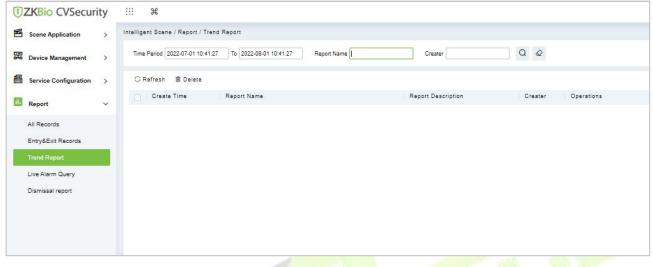


Figure <mark>5-61 Trends Reco</mark>rds

5.4.4 Live Alarm Query

Step 1: Go to Intelligent Analysits >Reports >Live Alarm Query.

Step 2: We can check all the records of live alarm query as a list format.

Step 3: On the All Records screen, click Export, enter the user password in the displayed security verification dialog box, and Click **OK**. Select whether to encrypt the file and the file format to export and Click **OK**.

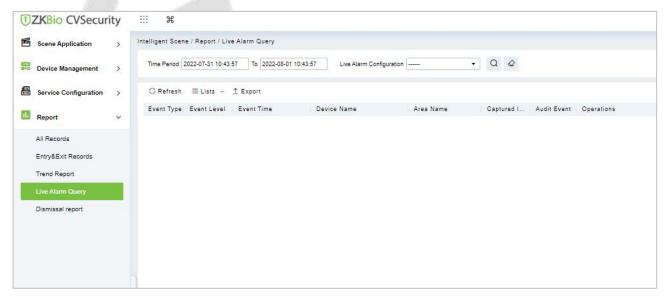


Figure 5-62 Live Alarm Query

5.4.5 Dismissal Report

Step 1: Go to **Intelligent Analysits > Reports > Dismissal Records**.

Step 2: We can check all the records of dismissal as a list format.

Step 3: Click Delete button under Operations. Click OK to delete.



6 Attendance Management

6.1 Operation Scenario

Attendance, also known as time management, carries out attendance function operations such as scheduling for employees, and helps enterprises effectively collect attendance data of employees, enter abnormal attendance data, and calculate attendance results.

6.2 Operation Flow

Introduce the configuration process of attendance management business.

The attendance management business configuration process is shown in Figure 6-1.

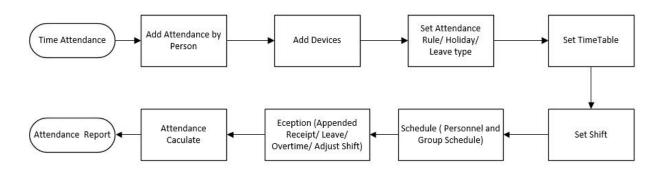


Figure 6-1 Attendance Configuration Process

6.3 Attendance Management

6.3.1 By Area

This action is used to define which persons in the Attendance area can be attended. Only those who are added to the area can be attended.

This paper introduces the configuration Steps of manually setting regional attendance personnel in.

6.3.1.1 Add Area Personnel

Operating Steps:

Step 1: In **Attendance** module, select "Attendance Management > Setting Personnel by Region", select the region to be set in the list on the left, and then click "Add Regional Personnel" on the right.

Step 2: Add personnel information in the pop-up Add Personnel window, as shown in Figure 6-2.

	Add Personnel(Area Name)		×
Personnel ID	Name Q		
🤞 🥫 💆 Subordinate Level Contained	Alternative	Selected(0)	
Department Name	Personnel ID First Name Department	Personnel ID First Name Department	
Soluction			
	No data		
	I< < 0 > >I 50 rows per page ▼	4	•
	OK Cancel		
			-

Figure 6-2 Add by Area

Step 3: Click OK to complete the configuration of adding attendance personnel in the area.

6.3.1.2 Delete Area Personnel

Step 1: On the **Area** interface, select the required ID from the list.

Step 2: Click **Delete** or click on the *icon.to* delete the selected ID.

Step 3: Click Delete, to ensure and delete the selected ID from the list.

	Pr	ompt
	Are you sure you wa	nt to perform the delete
10	ope	ration?

Figure 6-3 Deleting People

6.3.1.3 Export

You can export all transactions in Excel, PDF, CSV format.

Export	×
O Yes 💿 No	
EXCEL -	
 All (max 100000 records) 	
 Selected (max 100000 records) 	
Start Position 1	
Total Records 100	
(<u>177</u>)	
OK Cancel	
	Ves No EXCEL • All (max 100000 records) Selected (max 100000 records) Start Position 1 Total Records 100

Figure 6-4 Export People

6.3.1.4 Import

You can import all transactions in Excel, PDF, CSV format.

Import Area Personnel:

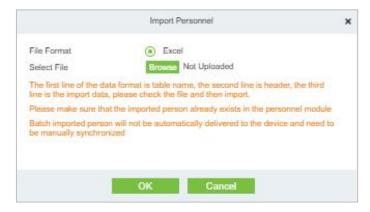


Figure 6-5 Adding People Import Area

Import and Delete Area Personnel:

File Format	 Excel 	
Select File	Browste Not Uploaded	
The first line of the	data format is table name, the second line is header, ta, please check the file and then import.	the third

Figure 6-6 Import Personnel

Download Import Template:

You can download the entire file in Excel, PDF, CSV format.

6.3.1.5 Private Message

Start Time*		
SMS Duration (Minutes)*	80	

Figure 6- 7 Private Message

6.3.2 Attendance Device Description (Attendance Device)

This paper introduces adding attendance device and setting communication parameters of connecting device, including the settings in the system and attendance device. After successful communication, you can view the information of connected devices, monitor the machines remotely, synchronize data and other operations.

Use Attendance Machine as Attendance Data Source

Precondition:

You need to set up the communication of the device first:

- 1. Open "**Communication Settings** > **Network Settings**" on the attendance device and configure the device network information in the pop-up "Network Settings" window.
- 2. Open "**Communication Settings** > **Cloud Service Settings**" and configure cloud server information in the pop-up "Cloud Server Settings" window.

6.3.2.1 Authorized Device

This paper introduces the configuration Steps of adding attendance device in by authorization.

Operating Steps:

Step 1: In the Attendance module, select Attendance Management > Attendance Device, and click "Authorized device".

Step 2: In the **Authorized Devices** window that pops up, add attendance devices, as shown in Figure 6-8.

Figure 6-8 Device Authorization Add Interface

Step 3: In the **Add** window that pops up, configure the device information, as shown in Figure 6-9, and the key parameters are described in Table 6-1.

Device Name*	CIZW202560100
Serial Number*	CIZW202560100
IP Address	10 . 8 . 12 . 126
Attendance Area*	Área Principal
Time zone*	(UTC+8)Beijing, Chines
Registration Machine	
A Time zone or registrar sta	te modification requires the device to restart to take effe
	OK Cancel

Figure 6-9 Adding Device Setup Interface

Parameter	Description
Attendance Area	The device is divided into regions to realize the management of regional data.
Whether To Register the Machine	If it is not checked, the user data uploaded by the device will not be processed (if the attendance record of the device is checked or not, it will be processed); Check, and the user data uploaded by the device will be processed.

Table 6-1 Description of Key Parameters.

6.3.2.2 Delete

Step 1: On the **Device** interface, select the required Device Name from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Device.

Step 3: Click **Delete**, to ensure and delete the selected Device from the list.

6.3.2.3 Device Control

• Upgrade Firmware

Tick the device that needs to be upgraded, click **Upgrade firmwa**re to enter edit interface, then click **Browse** to select firmware upgrade file (named emfw.cfg) provided by Access software, and click **OK** to start upgrading.

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.

Public Message

You can set public message in the device so that the device can display short messages on the page (Not all the devices support this function).

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.

• Synchronize Software 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.

Authorize Area

It can reach certain areas within a period of time after being authenticated.

6.3.2.4 View and Get Information

• Get Device Option

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

• Get the specified personnel data

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.

Attendance Data Checking

Select the device to proofread data, select the proofing date, the software issues a command to proofread the software and device attendance data.

Re-Upload Data

To re-upload the data from the device.

• View Device Parameters

To view the parameters and the specification of the device.

6.3.2.5 Clear Device Data

Clear unexecuted device commands

Select the device to be cleared. It clears the unexecuted operation command issued by the software in the setting.

Clear the attendance photos

This function will clear all the attendance photo records from the device.

• Clear the attendance transactions

Select the device. This function will clear all the attendance data records from the device.

Clear equipment personnel

This function will clear all the equipment personnel records from the device.

6.3.3 Attendance Point

This paper introduces the configuration Steps of using **Access Control** machine as attendance data source in.

6.3.3.1 New

Operating Steps:

Step 1: In the **Attendance** module, select **Attendance Management** > **Attendance Points**, and click **New**.

Step 2: Add **Access Control** attendance points in the pop-up **Add** window, as shown in Figure 6-10. Please refer to Table 6-2 for explanations of key parameters.

	New	×
Attendance Point Name* Device Module* Area Name*	Image: Area Name	
Save and New	OK Cancel	

Figure 6-10 Adding Attendance Point Interface

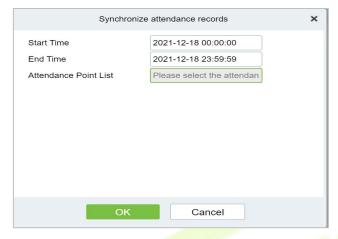
Parameter Description		
Device Module	Device module for setting attendance record source.	
Area Name	The area to which the device belongs.	
Door List	You need to set the door corresponding to the attendance record source.	

Table 6-2 Parameter Description

Step 3: Click OK.

Step 4: Select "**Detailed Report > Original Record Table**" and click **Synchronous Attendance Point Record**.

Step 5: Select the time node and attendance point to be synchronized in the pop-up **Synchronize Attendance Point Record** window, as shown in Figure 6-11.





Step 6: Click OK.

6.3.3.2 Export

You can export all transactions in Excel, PDF, CSV format.

6.3.3.3 Delete

Step 1: On the Attendance Point interface, select the required Attendance Point Name from the list.

Step 2: Click **Delete** or click on the ¹/₁ icon.to delete the selected Attendance Point.

Step 3: Click Delete, to ensure and delete the selected Attendance Point from the list.

6.3.4 Roll Call

The procedure of identifying the availability by calling out a list of names

TERMIN CVSecurity		😝 admin
🛅 Attendance Management 🗸	Attendance / Attendance Management / Roll Call	
By Area	Time From 2022-08-01 15:45:55 To 2022-08-01 23:59:59 Confirm	
Attendance Device Attendance Point	e [×] γ ^K □ Subordinate Level < No Check-in Person	
Roll Call	Department Name Personnel ID First Name Department Number Department Name Status Development	
Command From Server	🗆 🗊 hr	
Device Operation Log	 De test? Dettat? test? 	



6.3.5 Command from Server

6.3.5.1 Clear Command List

Step 1: You can clear command as required. Click **Clear Command** after selecting the corresponding ID.

ZKBio CVSecurity	::: ¥							e admin
🖞 Attendance Management 🗸	Attendance / Atten	idance Manageme	nt / Command From Serve	r				
By Area	Submit Time From		Τα	Serial Number	Return Result		More- Q Q	
Attendance Device	O Refresh	🔋 Clear Command	l List 🕺 Export					
Attendance Point Roll Call	ID	Serial Number	Content		Immediately Cmd	Submit Time	Return Time	Returned
Command From Server								
Device Operation Log								
					~			1111

6.3.5.2 Export

You can export all transactions in Excel, PDF, CSV format.

6.3.6 Device Operation Log

For 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.

TKBio CVSecurity		nin ~
📋 Attendance Management 😞	Attendance / Attendance Management / Device Operation Log	
By Area Attendance Device	Time From 2022-05-01 00:00:00 To 2022-08-01 23:59:59 Device SN Q	
Attendance Point	O Refresh 1 Export	
Roll Call	Device SN Operation Time Operational Content Operation Object Description Object Description 2 Operation Object Description 3	
Command From Server		
Device Operation Log		

Figure 6-14 Device operation Log

6.3.6.1 Export

You can export all transactions in Excel, PDF, CSV format.

6.4 Attendance Setting

Attendance settings affect attendance results, is the core of attendance calculation logic, including attendance rules settings, holiday settings, fake settings.

6.4.1 Attendance Rule Setting

Because the attendance system is different in each company, it is necessary to manually set attendance rules to ensure the accuracy of the final attendance calculation. The setting of attendance rules is the main way to reflect the attendance system of enterprises.

This paper introduces the configuration Steps of attendance rules in.

6.4.1.1 Basic Rule Setting

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in Figure 6-15, and the basic rule parameter description is shown in Table 6-3.

Attendance / Attendance	e Setting / Attendance Rules		
Attendance / Attendance Basic Rule Setti Timetable Shift Personnel Schedule Group Schedule Schedule Details	ng Check-In Rule The Earliest Rule Check-Out Rule The Latest Rule Attendance calculation result for cross-day shift First Day Overtime Statistics Yes Late and Early Leave Counted as Absent No		Basic Rule Setting Non-Leave Calculation Setting Annual Leave Balance Setting Real Time Roll Call Setting Employee Self-Service Login
	Intelligent Matching Shift Rule ③ Least Abnormal Missing Check-In count as Absent	Minutes (?)	
	ок		

Figure 6-15 Attendance Rules

6.4.1.2 Non-Leave Calculation Setting

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Non-Leave Calculation Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in Figure 6-16, and the Non-Leave Calculation description is shown in Table 6-3.

No Check-In			
Overtime			
Not Scheduled			
Adjust Shift			
Rest Day			
Adjust Rest			
Holiday		-	
Minimum Unit*	minute	•	
Rounding Control*			
Up (Carry)		7	
Report Display Sym	bol*		

6.4.1.3 Annual Leave Balance Setting

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Annual Leave Balance Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in Figure 6-17, and the Annual Leave Balance description is shown in Table 6-3.

A To use the annual leave balance function, you need to set the hire date for each employee;
when the hire date is not set, the remaining annual leave of the staff's annual leave balance
table is displayed as empty.
▲ If the current date is greater than the cleaning issue date, this modification will take effect
the following year; If the current date is less than the cleaning issue date, when the cleaning
issue date is reached, it will be cleaned and the annual leave will be reissued.
Annual Leave Clearing and Issuing Date
Annual Leave Cleaning and issuing Date
Every year 1 V Month 1 Day
Calculate According to Work Time Ratio
O Down (Discard) 💿 rounding 🔿 Up (Carry)
Annual Leave Rule 🧿
Working 1 Year, Yes 1 Days of Years S Annual Leave Annual Leave Annual Leave Annual Leave
Years S Annual Leave
1 Year-Working 2 Year, Yes 5 Days of
< Years S Annual Leave
Working 2 Year, Yes 5 Days of

Figure 6-17 Annual Leave balance Setting

6.4.1.4 Real Time Roll Call Setting

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Real Time Roll Call Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in Figure 6-18, and the Real Time Roll Call description is shown in Table 6-3.

Real Time Roll Call	Setting
3	Enable Real Time Roll Call

Figure 6-18 Roll Call Real Time

6.4.1.5 Employee Self-Service Login

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Attendance Rules>Employee Self Service Login Setting.

Step 2: In the Attendance Rule interface, fill in the attendance rules as required, as shown in Figure 6-16.2, and the Employee Self Service Login description is shown in Table 6-3.

Employee Se	If-Service Login
	Whether to enable employee self-service login
	Enable O Disable

Figure 6- 19 Roll Call Real Time

Parameter	Specific Parameters	Description
	Work check-in and card collection rules	 The earliest (by default, the first punch-in record is taken within the valid card taking range) Nearby (take the clock-in record closest to working hours within the valid card-taking range).
	Rules for sign-out and card collection after get off work	 Latest (by default, the last punch-in record is taken within the valid card taking range) Nearby (take the clock-in record closest to the attandance checking time within the valid card-taking range).
Basic Rule	The shortest attendance period should be greater than (10 minutes)	120 (default); Range: 10 to 999; Required
	The longest attendance period should be less than 600 (o (1440 minutes)	600 (default); Range: 10 to 1440; Required
	The shift time period spans days, and the attendance calculation results	 On the first day, if there is a cross-day, count the working hours in the effective shift on the second day to the first day. On the second day, if there is a cross-day, the working

Parameter	Specific Para	ameters	Description
			hours in the effective shift on the first day are counted to the second day.
	Being late and leaving earlis absenteeism		 No (default) If yes, there are cases of being late and leaving early, and this period is recorded as absenteeism.
	Statistical overti	me	 Yes (default) No; If the first switch of overtime statistics is set to No, overtime will not be calculated.
	Minimum overtime time per time (minutes)		This parameter is applied to overtime rule duration statistics. If overtime duration is less than the set minimum overtime duration, it will not be reflected in attendance statistics.
	Exact number points	of decimal	1 (default), 2.
	Failure to si recorded as	gn in is	 Three ways: Absence Be late Incomplete Description: When you are late, you should set the number of minutes you are late. Absence and incompleteness are not valid attendance, but absence is absenteeism and incompleteness is absenteeism. Statistics attendance by setting basic rules in monthly detailed reports and other related reports.
	Unsigned refund as		 Three ways: Absence Be late Incomplete Description When you are late, you should set the number of minutes you are late. Absence and incompleteness are not valid attendance, but absence is absenteeism and incompleteness is absenteeism. Statistics attendance by setting basic rules in monthly detailed reports and other related reports.
		Minimum unit	Calculate the smallest unit of this arix
Non-Pseudo Class Calculation Settings	Class(includingcontrolCalculationbeinglate,		 Down (discard): discard the decimal part, as long as the integer. Rounding: If the first decimal place is greater than 5, the integer will be added with 1, otherwise, the integer will be taken. Up (carry): With decimal, discard decimal, integer plus 1
			Symbols for associated report presentation

Parameter	Specific Parameters		Description
	Annual leave cleared and issued date	Set the annual leave clearing date	 Description Using the annual leave balance function requires setting the entry
Setting of Annual Leave Balance	Calculated according to the proportion of working hours	 There are three ways to calculate the proportional duration: Down (discard): discard the decimal part, as long as the integer. Rounding: If the first decimal place is greater than 5, the integer will be added with 1, otherwise, the integer will be taken. Up (carry): With decimal, discard decimal, integer plus 1 	time for each person; When the induction time is not set, the remaining annual leave in the personnel annual leave balance table is displayed as blank. • If the current date is greater than the clearing and issuing date, the revised content will take effect the following year; If the current date is less than the zero-clearing issue date, the annual leave will be cleared and reissued when the zero- clearing issue date is reached. For example Zhang San joined the company on September 1 last year Setting of annual leave balance The clearing and issuing date is January 1 of each year; According to the proportion of work rounded calculation; There are 3 days" annual leave when the length of service is less than or equal to 1 year, and 5 days"
	Rules of annual leave duration	Set annual leave days according to length of service, which can be added by symbols	annual leave when the length of service is less than or equal to 3 years Annual leave entitlement calculation It enjoyed 4/12 x3 = 1.0 days from September 01 to December 31 last year This year's 01-01 to 12-31 enjoys 4.0 days (this year's 01-01 to 08-31 enjoys 8/12 x3 = 2.0 days + this year's 09-01 to 12-31 enjoys 4/12 x5 \approx 2.0 days)
Real-Time RollCall Setting	Turn on the real-time roll displayed in the "sign-in Tabl		he sign-in status of personnel will be
Employee Self Service Login	The frequency of setting atte 20 seconds/time, 30 seconds	•	otain records includes (10 seconds/time, ~ 8 minutes/time).

Table 6- 3 Description of Basic Rule Parameters

6.4.2 Holidays

This paper introduces the configuration Steps of manually adding holidays in.

6.4.2.1 New

Operating Steps:

Step 1: In the Attendance module, select "Attendance Settings > Holidays" and click New.

Step 2: Configure holiday information in the pop-up Add window.

New	×	
1		
2021-12-18		



Step 3: Click OK.

6.4.2.2 Delete

Step 1: On the Holiday interface, select the required Holiday Name from the list.

Step 2: Click Delete or click on the 🔟 icon.to delete the selected Holiday list.

Step 3: Click Delete, to ensure and delete the selected Holiday from the list.

6.4.3 Leave Type

This paper introduces the configuration Steps of adding Leave Type.

6.4.3.1 New

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Leave Type and click Add.

Step 2: Configure fake information in the pop-up **Add** window, as shown in Figure 6-21. Please refer to Table 6-4 for explanations of key parameters.

	New	×	
Name*			
Whether to substract work	Yes 🔹		
hours* Minimum Unit*	minute •		
Rounding Control*	Down (Discard)		
Report Display Symbol*			
Save and New	OK Cancel		
Save and New	Calicel		

Figure 6-21 New Leave Type

Parameter	Description
Name	Character length 30, required.
Whether To Deduct Working Hours	Whether the working hours should be deducted for setting this kind of leave, for example, maternity leave/marriage leave/annual leave are all legal holidays, and the working hours are not deducted.
Minimum Unit	Calculate the smallest unit for this alias.
Rounding Control	Down (discard): discard the decimal part, as long as the integer; Rounding: If the first decimal place is greater than 5, the integer will be added with 1, otherwise, the integer will be taken; Up (carry): There are decimals, decimals are discarded, integers are added by 1.
Report Presentation Symbol	Symbols for the presentation of the associated report.

Table 6- 4 Description of Key Parameters

Step 3: Click OK.

6.4.3.2 Delete

Step 1: In the Leave Type interface, select the required Leave from the list.

Step 2: Click Delete or click on the 🛄 icon.to delete the required Leave from the list.

Step 3: Click Delete, to ensure and delete the selected Leave from the list.

6.4.4 Automatic Report

The Automatic reporting feature helps you to send the reports to the designated person at the specified time.

6.4.4.1 New

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Automatic Report and click New.

Step 2: Click to New to configure all the details.

eport Setting					Send Mode Setting	1
Report Type*	Transactions	s	19 4 8		Send Mode*	Mailbox Delivery Met
ile Name*						
ate Format	yyyyMMdd		1000		Mail Setting	
ile Type"	EXCEL		1979		Receiver Setting	Set by Personnel -
and Frequency					Mail Address*	Please enter a valid email address, if more than one address is entered, separate with',' Example:123@foxmail.com,456@foxmail.com
Gend Frequency	By Day		•			
	-	hour :		 minute 	Title Setting*	The Maximum Length50
	- •	hour :		 minute 	Body Setting	The Maximum Length200
		hour :		 minute 		
		hour :		 minute 		
		hour :		- minute		
		hour :		→ minute		

Figure 6-22 Automatic Report

6.4.4.2 Delete

Step 1: In the Automatic Report interface, select the required File from the list.

Step 2: Click **Delete** or click on the ¹/₁ icon.to delete the required File from the list.

Step 3: Click Delete, to ensure and delete the selected File from the list.

6.4.4.3 Enable/Disabled

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.

6.4.5 Process Settings

To achieve the approval function, it is necessary to maintain the relationship between positions at all levels in the personnel module and assign them to the corresponding personnel. Then setup the approval process for different process types and different positions.

6.4.5.1 New

Operating Steps:

Step 1: In the Attendance module, select Attendance Settings > Process Settings and click New.

Step 2: Click to New to configure all the details.

		Nev	v		×
Number* Choose position* Inform the person	•] Clear	Name* Flow Type*	Appended Log	•
=+ New					_
The name of the no Th	e a Position of	f Inform the	person Operation	15	
Directly under the leac			2 0		

Figure 6-23 Processing Setting

6.4.5.2 Enable/Disabled

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

6.5 Regular Shift Setting Schedule

Regular shifts can choose one or more normal time periods to form a regular shift according to laws. Regular shifts are often used in regular occasions, such as office buildings, governments, banks, etc.

6.5.1 Timetable

6.5.1.1 Add Normal Timetable

This paper introduces the configuration Steps of adding normal time period to the regular shift configuration of VAORIDA.

Operating Steps:

Step 1: In the **Attendance** module, select **Schedule Management > Time Period** and click **Add Normal Time Period**.

Step 2: Configure the time period information in the **Add Normal Time** Period window, as shown in Figure 6-24. Please refer to Table 6-5 for the explanation of key parameters.

Check-In Time*	09 : 00 (HH:MM)	Check-Out Time*	18 : 00 (HH:MM)	
Before going to Work*	60 Check-In is valid within	Before Going Off Duty*	60 Check-In is valid within	
	minutes		minutes	
After Work*	60 Check-In is valid within	After Work*	60 Check-In is valid within	
	minutes		minutes	
Allow Late(Minutes)	0	Allow Early Leave(Minutes) (?)	0	
Must Check-In*	Yes	Must Check-Out*	Yes	
Auto Deduct Break Time	e* No 🔻	Work Time (Minutes)*	540	
On Duty 0 C overtime hours 0	Check-In Minutes ago for Overtime , Start counting overtime minutes late			
overtime hours 0				

Figure 6-24 New Time Period

Parameter	Description
Before/after work, Before/after work	Set the valid range of check-in/check-out for this time period, and the check-in/check-out records outside this range are invalid records. The valid sign-in time after going to work and the valid sign-out time before going off work cannot overlap, which must be filled in.
Minutes allowed to be late/leave early	Refers to how long it is allowed to be late and leave early within the specified time points for going to and from work, and the

Parameter	Description
	minutes allowed to be late and leave early must be within the valid time range of sign-in and sign-out before they can take effect.
You must sign in/return	In the selected time range, set whether you must sign in and sign out when going to and from work.
Whether it is deducted between segments	When used for attendance calculation, whether to subtract the number of minutes defined by inter-segment deduction for this time period.
Start counting overtime before/after N minutes from work/work, with the shortest overtime minutes and the maximum overtime hours limited	Select whether to record the verification records before and after work as overtime.
Enable flexible hours to work	It refers to the flexible working parameter that people who go to work early can get off work early and people who work at night need to get off work late. When checked, you need to set the number of minutes that can be advanced/delayed, and it must be within the valid sign-in/sign-out time range.
Table	6-5 Description of Key Parameters

Step 3: Click OK.

6.5.1.2 Add Flexible Timetable

Operating Steps:

Step 1: In the **Attendance** module, select **Schedule Management** > **Time Period** and click **Add Flexible Timetable**.

Step 2: Configure the time period information in the Add Flexible Timetable window.

Flexible Duration Calculation	Curr	nuk	tive t	ime for 🔻
Check-In Start Time*	09		00	(HH:MM)
Check-Out End Time*	18]:	00	(HH:MM)

Figure 6-25 Adding Flexible TimeTable

6.5.1.3 Delete

Step 1: In the **Timetable** interface, select the required Type from the list.

Step 2: Click **Delete** or click on the 🔟 icon.to delete the required Timetable Type from the list.

Step 3: Click **Delete**, to ensure and delete the selected Type from the list.

6.5.1.4 Add Regular Shift

Operating Steps:

Step 1: In the **Attendance** module, select '**Schedule Management > Shift**" and **click** "Add Regular Shift".

Step 2: Configure shift information in the "Add Regular Shift" window, as shown in Figure 6-26. Please refer to Table 6-6 for explanation of key parameters.

		New		×
Basic Setting		Number*		
Unit* Period Start Type*	Day Period Start Date	Cycle(1-99)* Cycle Shift in one Month* (?)	Yes •	
Cycle Start Date* (?) dvanced Setting	2021-12-18			
Work Type* 🕐	Normal Work	Attendance Mode* ⑦	Punch According to	
Overtime Mode*	Computer Automatic			
	Save and New	OK Cancel		

Figure 6- 26 New Shift

Parameter	Description
Unit	Set the unit of the cycle, and the default is "day". There are three types of units: • Day • Week • Month
Period	 Defines the number of cycles of a shift, and the cycle of the shift = cycle number * units. If the unit is "day", the range is 1 to 99. If the unit is "week", the range is 1 to 15. If the unit is "month", the range is 1 to 12.
Period starting type	 This field is displayed only when the cycle unit is Day, Description It is not displayed when the units are "week" and "month". There is cycle start date and scheduling start date, and the default is cycle start date. If you select Scheduling Start Date, the start date when scheduling is the first day of the cycle.
Period start date	This field is displayed only when the cycle start type is Cycle Start Date. Define the start date of the shift, and the date before the start date is not affected by the shift. The default system start date is the current system date.
Type of work	 Normal work: This shift is a normal work shift Overtime on rest days: This shift is overtime on rest days Overtime on holidays: This shift is overtime on holidays.

Parameter	Description
Attendance mode	 Swipe the card normally according to the shift: the default item of the system, and punch in normally according to the punch in. Brush a valid card once a day: only need to brush the card once in the swiping interval defined by the time period within one day, even if it is normal to punch in. Punch-in-free: Setting this shift can avoid punch-in.
Overtime mode	 Computer automatic calculation: It is connected with "whether the delay counts overtime" in the time period. When "whether the delay counts overtime" is "no", the delayed overtime is not calculated, and the overtime time of the overtime bill is not calculated at the same time. Overtime must be applied: delayed overtime is not calculated, only the overtime order shall prevail; When the signing-back time is less than the end time of overtime, the overtime time is not calculated. Not counting overtime: overtime hours are not counted for delayed overtime or overtime application.

Table 6- 6 Description of Key Parameters

Step 3: Click OK.

6.5.1.5 Add Flexible Shift

Step 1: In the shift interface, click **Set Time Period** under the operation bar of the added regular shift, and configure the time period information in the pop-up **Set Time Period** window.

asic Setting			Number*		
Jmit*	Day		Cycle(1-99)*		
Period Start Type*	Period Start Date	-	Cycle Shift in one Month* (?)	Yes	•
Cycle Start Date* 🧑	2022-07-26				

Figure 6-27 Adding Flexible Shift

6.5.1.6 Delete

Step 1: In the Shift interface, select the required Shift Type from the list.

Step 2: Click **Delete** or click on the 🔟 icon.to delete the required Shift Type from the list.

Step 3: Click Delete, to ensure and delete the selected Shift Type from the list.

6.5.1.7 Clear Timetable

	Set Timetable	×
Timetable		
Please select the timetable		•
Timetable Details		
Cycle		<u>^</u>
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Sunday		-
	OK Close	

Figure 6-28 Adding Time Periods

Step 6: Click **OK** to complete the addition of time period, and the specific time period is displayed in the time period details on the right.

6.5.2 Personnel Schedule

Personnel scheduling operations is completely same as group scheduling, but when scheduling personnel, the object of choice is personnel at the top left corner of the interface.

6.5.2.1 Cycle Schedule

Step 1: In the **Attendance** module, select **Schedule Management > Personnel Schedule** and click **Cycle Schedule**.

	2.	
Schedule Type*	Normal Schedule	*
Start Time*	0	
End Time*	6.5.	
10 O.V.	**	
Name	Number Shift Type	
	No data	
	No data	

Figure 6-29Adding Personnel Schedule

6.5.2.2 Temporary Schedule

Step 1: In the **Attendance** module, select **Schedule Management > Personnel Schedule** and click **Temporary Schedule**.

ïmetable		0		A	ugust 2022		<< TODA	\Y >>
iorario24h(09:00-0	08:59)	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		01	02	03	04	05	06	Â
		08	09	10	11	12	13	
Nork Type*	Normal Work	15	16	17	18	19	20	
Attendance Mode*	Punch According to Normal Shift 👻							
Overtime Mode*	Computer Automatic Calculation 🔻	22	23	24	25	26	27	
ontrol to schedule.	imetable to a single date in the calendar ntrol, double-click a single date to schedule. ntrol, press and hold the mouse to select.	29	30	31	10	02		

Figure 6- 30 Adding Temporary Schedule

6.5.2.3 Clear Cycle Schedule

Step 1: In the **Attendance** module, select **Schedule Management > Personnel Schedule** and then click on the Personnel ID that you want to delete, and click **Clear Cycle Schedule**.



Figure 6-31 Clear cycle schedule

6.5.2.4 Clear Temporary Schedule

Step 1: In the **Attendance** module, select **Schedule Management > Personnel Schedule** and then click on the Personnel ID that you want to delete, and click **Clear Temporary Schedule**.

F	ompt
schedule from 2022	ar "raj" the temporary -08-01 to 2022-09-01?

Figure 6-32 Clear Temporary Schedule

6.5.3 Group Schedule

Grouping scheduling means grouping people, and then scheduling people in batches by grouping. This paper introduces the configuration Steps of grouping cycle scheduling in.

6.5.3.1 Edit Personnel for Group

New

Step 1: In the Attendance module, select Schedule> Group Schedule and click New.

Step 2: Configure the Schedule Name in the **Group Schedule** interface.

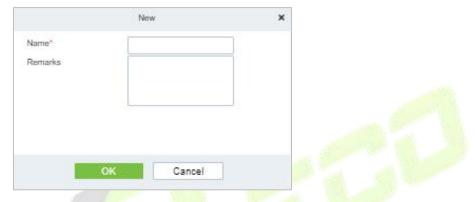


Figure 6-33 Adding Elastic Time Period

Parameter	Description
Name	Can not contain special symbols, period name can not be duplicated, length is 30 characters, required.
Remarks	Mentioning comments.
A CONTRACTOR	Table 6.7 Description of Koy Parameters

Table 6-7 Description of Key Parameters

Step 3: Click OK.

• Delete

Step 1: In the **Schedule** interface, select the required Shift Type from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Shift Type from the list.

Step 3: Click Delete, to ensure and delete the selected Shift Type from the list.

6.5.3.2 Browse the Group Personnel

Delete Personnel

Step 1: In the Schedule interface, select the required Personnel ID from the list.

Step 2: Click Delete or click on the iii icon.to delete the required Personnel ID from the list.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

Cycle Schedule

Step 1: In the **Attendance** module, select **Scheduling Management > Personnel Scheduling**, check the personnel under the department that needs scheduling or the designated personnel, and click "Periodic Scheduling".

Step 2: Configure scheduling information in the pop-up **Cycle Scheduling** window, as shown in Figure 6-34. Please refer to Table 6-8 for parameter description.

		Cycle	Schedule		×	
Schedul Start Tin End Tim		Normal S	Schedule	•		
	Name	Number	Shift Type			
	Fexible sł	2	Flexible Shift			
	1	1	Regular Shift			
		ОК	Cancel			

Figure 6-34 Cycle Scheduling

Parameter	Description
Scheduling Type	 Normal Shift Scheduling: Only one shift can be selected for normal shift scheduling Intelligent scheduling: Intelligent scheduling can select multiple shifts. Select intelligent scheduling, and the software will automatically judge the most suitable shift according to the punch-in record for attendance calculation.
Start Time/End Time	Set which date segment the schedule works on.
Select Shift	Select the shift to use for scheduling.
Tak	ble 6-8 Description of Key Parameters of Cycle Scheduling

Step 3: Click OK to complete the configuration of personnel cycle scheduling.

• Temporary Schedule

Step 1: In the **Attendance** module, select 's**cheduling Management > Personnel Scheduling**", check the personnel under the department that needs scheduling or the designated personnel, and click "Periodic Scheduling".

Step 2: Configure scheduling information in the pop-up **Temorary Schedule** window, as shown in Figure 6-35. Please refer to Table 6-9 for parameter description.

Step 3: Click OK to complete the configuration of temporary personnel scheduling

		T	emporary Schedu	le				
Timetable		0			July 2022		<< TODA	(Y >>
horario24h(09:00-	08:59)	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		27	28	29	30	01	02	
		04	05	06	07	08	09	-
		11	12	13	14	15	16	
Work Type* Attendance Mode*	r enerriedening te riterinit entre							
Overtime Mode*	Computer Automatic Calculation 🔻	18	19	20	21	22	23	
control to schedule. 2. In the calendar op	timetable to a single date in the calendar antrol, double-click a single date to schedule. antrol, press and hold the mouse to select	25	26	27	28	29	30	

Figure 6-35 Group Temp<mark>orary</mark> schedule

Parameter	Description
Type of Work	 Normal work: This shift is a normal work shift. Overtime on rest days: This shift is overtime on rest days. Overtime on holidays: This shift is overtime on holidays.
Attendance Mode	 Swipe the card normally according to the shift: the default item of the system, and punch in normally according to the punch in Brush a valid card once a day: only need to brush the card once in the swiping interval defined by the time period within one day, even if it is normal to punch in. Punch-in-free: Setting this shift can avoid swiping cards.
Overtime Mode	 Computer automatic calculation: It is connected with "whether the delay counts overtime" in the time period. When "whether the delay counts overtime" is "no", the delayed overtime is not calculated, and the overtime time of the overtime bill is not calculated at the same time. Overtime must be applied: delayed overtime is not calculated, only the overtime order shall prevail; When the signing-back time is less than the end time of overtime, the overtime time is not calculated. Not counting overtime: overtime hours are not counted for delayed overtime or overtime application.

Table 6-9 Description of Key Parameters of Temporary Scheduling

• Clear Cycle Schedule

Step 1: In the **Attendance** module, select **Scheduling Management > Personnel Scheduling**, check the personnel under the department that needs scheduling or the designated personnel, and click **Periodic Scheduling**.

Step 2: Configure scheduling information in the pop-up Clear Cycle Schedule window.

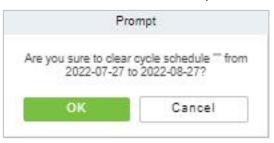


Figure 6-36 Group Clear cycle Schedule

6.5.4 Schedule Details

After setting the attendance time period and shift, you can schedule the personnel.

6.5.4.1 Delete

Step 1: In the **Schedule** interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.5.4.2 Export

You can export all transactions in Excel, PDF, CSV format

6.6 Exception

6.6.1 Appended Log

In the case of personnel going out on business or forgetting to punch in, the manual supplementary recording of attendance records in the attendance report is called supplementary signing card, which is generally summarized and entered by the management personnel according to the attendance results and the attendance system of the enterprise after the attendance cycle ends.

6.6.1.1 New

Operating Steps:

Step 1: In the Attendance module, select Exception Management > Appended Log and click Add.

Step 2: Configure the card replacement information in the pop-up **Add** window, first select the "Department" where the person to be resigned is located, then select the person to be resigned, and finally enter the date and time of the card replacement.

	New	×
Personnel ID	Name Q	
🖌 🧏 🗹 Subordinate Level Contained	Alternative Selected(1)	
Department Name	💆 Personnel ID First Name Last Name Department 💆 Personnel ID First Name Last Name	D
Soluction	I Soluction I	SI
Punch Date [®] 2021-1 Punch Time [®] 15:42		•
	Save and New OK Cancel	

Figure 6-37 Replacement Card

Step 3: Click OK.

6.6.1.2 Delete

Step 1: In the Appended Log interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the icon.to delete the required Personnel ID from the list.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

6.6.1.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.1.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.1.5 Import

You can import all logs in Excel, PDF, CSV format.

6.6.2 Ask For Leave

When encountering special circumstances, people may need to take time off for different reasons, and hope that the time off can be displayed in the system statistics.

6.6.2.1 New

Operating Steps:

Step 1: In the Attendance module, select Exception Management > Leave and click New.

Step 2: Configure the leave form information in the pop-up **Add** window, first select the "Department" where the person to take leave is located, then select the leave person, finally enter the leave time, and optionally upload the leave attachment.

		New		×
Personnel ID	Name	\$		
د ^م م ^{لا} Subordinate Level Contained ☐ Department Name ☐ Soluction	Alternative Personnel ID First Name 1	Last Name Department	Selected(1) Image: Personnel ID First Name Last Name Image: Imag	D' St
Leave Type"	IC C 1-1 >>I 50 rov	vs per page 👻	4	•
Start Time*	021-12-17 15:43:51 021-12-18 15:43:51	Browse	No Pictures	
	Save and New	OK Cancel		

Figure 6-38 Leave Request Form

Step 3: Click OK.

6.6.2.2 Delete

Step 1: In the Leave interface, select the required Personnel ID from the list.

Step 2: Click Delete or click on the 🛄 icon.to delete the required Personnel ID from the list.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

6.6.2.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.2.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.2.5 Import

You can import all logs in Excel, PDF, CSV format.

6.6.3 Overtime

6.6.3.1 New

Step 1: In the Attendance module, select Exception Management > Overtime and click New.

Step 2: Configure overtime form information in the pop-up **Add** window, first select the "Department" where the person to work overtime is located, then select the overtime person, and finally enter overtime hours.

		New		×
Personnel ID	Name	Q		
🤞 🧏 💆 Subordinate Level Contained	Alternative		Selected(1)	
Department Name		Last Name Department	Personnel ID First Name Last Na	me D
Soluction	🖬 1	Soluction	🗹 1	Si
And a subserve of the second	I< < 1-1 > >I 50 rows -12-18 15:45:12 -12-18 15:45:12	Overtime Duration(Minutes) Remarks		•
	Save and New	OK Cancel		

Figure 6-39 Overtime Form

Step 3: Click OK.

6.6.3.2 Delete

Step 1: In the Overtime interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the 🛄 icon.to delete the required Personnel ID from the list.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

6.6.3.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.3.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.3.5 Import

You can import all logs in Excel, PDF, CSV format.

6.6.4 Adjust Rest

6.6.4.1 New

Operating Steps:

Step 1: In the Attendance module, select Exception Management > Leave Adjustment and click New.

Step 2: In the pop-up **Add** window, configure the information of the leave adjustment form, first select the "Department" of the person to be transferred, then select the person to be transferred, and finally enter the leave adjustment time.

6	New		×
Personnel ID	Name Q Q		
🧖 🦽 🔽 Subordinate Level Contained	Alternative	Selected(0)	
Department Name	Personnel ID First Name Last Name	Department Personnel ID First Name Last Name D	
Soluction	2 1	Department	
Adjust Date* 2021-	I< < 1-1 > >I 50 rows per page ▼ -12-20	Remarks	
	Save and New OK	Cancel	

Figure 6-40 Leave Adjustment Form

Step 3: Click OK.

6.6.4.2 Delete

Step 1: In the Adjust Rest interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the iii icon.to delete the required Personnel ID from the list.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

6.6.4.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.4.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.4.5 Import

You can import all logs in Excel, PDF, CSV format.

6.6.5 Shift Adjustment

6.6.5.1 New

Operating Steps:

Step 1: In the Attendance module, select Exception Management > Shift Adjustment and click New.

Step 2: In the pop-up **Add** window, configure the shift adjustment list information, first enter the shift adjustment "Personnel Number", then select "shift Adjustment Date", and finally select "shift Adjustment Name".

		New		×
Adjust Type Personnel ID* First Name	Adjust the personal s			
Department Name	Soluction			
Adjust Date* Remarks	2021-12-18	Adjust Shift Name	▼	
	Save and New	ОК Сапсе	21	

Figure 6-41 Leave Adjustment Form

Step 3: Click OK.

6.6.5.2 Delete

Step 1: In the Adjust Shift interface, select the required Personnel ID from the list.

Step 2: Click Delete or click on the iii icon.to delete the required Personnel ID from the list.

Step 3: Click **Delete**, to ensure and delete the selected Personnel ID from the list.

6.6.5.3 Approval

Passed: The approval by the Supervisor, and more than a certain number of days approved by the Manager.

Refused: The denial of leave by the immediate Supervisor and the Manager.

6.6.5.4 Export

You can export all logs in Excel, PDF, CSV format.

6.6.5.5 Import

You can import all logs in Excel, PDF, CSV format.

6.7 Attendance Detail Report

6.7.1 Manual Calculation

In the Attendance Report, you can view the clock-in record of a person and check whether the attendance status of the person is correct through attendance calculation. If it is correct, it means that the attendance business configuration is completed.

Operating Steps:

Step 1: In Attendance Module, select Detailed Report > Manual Calculation, check the person who needs to perform attendance calculation, and click Attendance Calculation.

Attendanc	e Calculation	×	
Start Time* End Time* Including resigned personnel	2021-12-01 00:00:00 2021-12-18 23:59:59 Yes No		
Attendance optional time rar	ige: the first two months to the c	ay!	
Attendance Calcula	Close		

Figure 6-42 Manual Calculation

6.7.1.1 Attendance Calculation

Step 1: In the **Attendance Calculation** window, configure the attendance calculation information, and click **Attendance Calculation**.

Processing command	×
Total Progress	
100%	
The filtration condition is ready! Initialization of database has completed! Initialization of exception data has completed! Start calculating! Attendance Calculation100% End the calculation! The operation succeeded!	* *
The window will close after 3 second(s). Suspend Close	Close

Figure 6-43 Attendance Calculation

Step 2: After the calculation is completed, you can view related reports.

6.7.2 Attendance Transaction Transaction

Attendance records of all employees will be displayed on this interface, including the attendance record of uploaded attendance transactions. The record of the normal punch on the device will be uploaded to the software as the original record. When a particular data is selected, the details will be displayed on the right side of the page.

Operating Steps:

Step 1: In the Attendance module, select Detailed Report > Transaction.

Step 2: In the original record table interface, fill in the corresponding query information, and click the **Query** symbol to complete the query of all record tables.

Atte	ndance / Attendan	ice Detail Report / T	Fransactions						
-	Time From 2022-08-	01 00:00:00 Ta 2	022-08-01 23:59:59	Personnel ID		Name	More = Q	0	
,	O Refresh	± Export - ± I	mport U Disk Records	Synchronize at	endance records				
	Personnel ID	First Name	Last Name	Department Name	Attendance Area	Serial Number	Attendance Point	Attendance time	Attendanc

Figure 6-44 Report Query Interface

6.7.2.1 Export

Step 1: In the original record table interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and click **OK**.

	Export	×
Encrypt or not		
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	O Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	
	OK Cancel	

Figure 6-45 Report Export Interface

Step 2: After selecting the address where the corresponding file is stored, the export of the file can be completed.

6.7.2.2 Import U Disk Records

The "Import U disk record" feature allows you to import the device data (including access control, parking, Facekiosk, Video records) to the transaction table.

6.7.2.3 Synchronize attendance records

The access control records can be synchronized to attendance records through this function. Select the start time and end time to import, check the attendance point list and click **OK**.

Start Time	2017-12-07 00:00:00	
End Time	2017-12-07 23:59:00	
Attendance Point List	Please select the attendan	

Figure 6-46 Synchronize Attendance Records

6.7.3 Daily Attendance

The table shows personnel's daily attendance status, punch time, the early leaving time, the latest time, the detailed punch time during the selected period.

TKBio CVSecurity	::: #			e admin ~
Attendance Management >	Attendance / Attendance Deta	il Report / Daily Attendance		
Attendance Setting	Time From 2022-07-01	To 2022-07-26 Personnel ID	Department Name	More - Q Q
🛱 Schedule >	x* 7 ⁶	 ♦ O Refresh		
Exception >	Department Name Development	Personnel ID First Name Last Name	Department Name Record Date	Record Counts Earliest Time Late
🚹 Attendance Detail Report 🗸	(1) hr ∡ (⊡) test9			
Manual Calculate	I test8 I test7			
Transactions				
Daily Attendance				
Daily Report				

Figure 6-47 Daily Attendance

6.7.3.1 Export

It will export the daily attendance record data. Currently it can be exported either in three types of file EXCEL/PDF/CSV. You can also choose the amount of data to be exported or select the maximum amount which supports up to 40,000 records.

The File Type	EXCEL File	~						
Export Mode	 All data (Can export up to 40000 data) 							
	O Select the amou	nt of data	a to export (Can ex	port up	to 40000 data)			
	From the article	1	Strip, is derived	100	Data			

Figure 6-48 Export Daily Attendance

6.7.4 Daily Report

This function is used to get the daily report within the specified range of date and time attendance details of personnel, including attendance, late arrival, early leaving, overtime and so on.

JZKBio CVSecurity	::: ¥									9 admin		
Attendance Management >	Attendance / Attendance Deta	il Report /	Daily Report									
Attendance Setting	Time From 2022-07-01	То	2022-07-28	Personnel ID		epartment Name		More = Q	Q			
Schedule >	x" x ^k	۲	O Refresh	∱ Export								
Exception >	Department Name		Personnel		Department Name	Attendan	Timetable Details	Punch	Punch	Expecte		
	Development		ID	First Name Last Name			Name Work Ti	me		Should		
Attendance Detail Report 🗸	∠ B test9		1	уу	Department Name	2022-07-01			0	0.0		
Manual Calculate	C1 test8 C1 test7		1	yy	Department Name	2022-07-02			0	0.0		
Transactions			1	уу	Department Name	2022-07-03			0	0.0		
Daily Attendance			1	уу	Department Name	2022-07-04			0	0.0		
Daily Report			1	уу	Department Name	2022-07-05			0	0.0		
Monthly Detail Report				1	уу	Department Name	2022-07-06			0	0.0	
Appended Log Details					1	уу	Department Name	2022-07-07			0	0.0
Leave Details										1000		
Exception Report			1	уу	Department Name	2022-07-08			0	0.0		
Work Time Report			1	уу	Department Name	2022-07-09			0	0.0		
Annual Leave Balance Sheet			1	уу	Department Name	2022-07-10			0	0.0		
			1	уу	Department Name	2022-07-11			0	0.0		

Figure 6- 49 Daily Report

6.7.4.1 Export

It will export the Daily report data. Currently it can be exported either in three types of file EXCEL/PDF/CSV. You can also choose the amount of data to be exported or select the maximum amount which supports up to 40,000 records.

The File Type	EXCEL File	~			
Export Mode	All data (Can exp	ort up to	40000 data)		
	O Select the amoun	nt of data	a to export (Can ex	port up	to 40000 dat
	From the article	1	Strip, is derived	100	Data

Figure 6- 50 Export Daily report

6.7.5 Monthly Detail Report

This function will automatically give the report for a selected month on a daily basis. The report includes attendance status and characters, and summarizes the actual attendance time, absence, leave, business trips and outings in the month.

JZKBio CVSecurity	::: ¥									e admin								
Attendance Management >	Attendance / Attendance Deta	il Report /	Monthly Detail	Report														
Attendance Setting	Time From 2022-07-01	То	2022-07-28	Personnel ID		Department	Name		More - Q Q									
Schedule >	x* x ^k	•	O Refresh	∱ Export														
Exception >	Department Name		Personnel		Departme	2022-07-01	2022-07-02	2022-07-03	2022-07-04	2022-07-05								
	Development		ID	First Name Last Name														
Attendance Detail Report V	I hr → E test9		9999	K-TEST	Department I	Rest	Rest	Rest	Rest	Rest								
Manual Calculate	 Image: book to be the test to be test to b		9527		Department I	Rest	Rest	Rest	Rest	Rest								
Transactions			666	chen	Department I	Resi	Rest	Rest	Rest	Resi								
Daily Attendance			555	fe	Department I	I NS	NS	NS	NS	NS								
Daily Report											5	уууу	Department I	I NS	NS	NS	NS	NS
Monthly Detail Report								4	W9	Department I	I NS	NS	NS	NS	NS			
Appended Log Details			3		Department I	NS	NS	NS	NS	NS								
Leave Details																		
Exception Report			2222	уди	Department I	NS	NS	NS	NS	NS								
Work Time Report			2	Isf	Department I	I NS	NS	NS	NS	NS								
Annual Leave Balance Sheet			12135		Department I	Rest	Rest	Rest	Rest	Rest								

Figure 6-51 Monthly Details Report

The attendance status is displayed as per following priority at the bottom of the interface.

6.7.5.1 Export

It will export the Monthly Detail Report data. Currently it can be exported either in three types of file EXCEL/PDF/CSV. You can also choose the amount of data to be exported or select the maximum amount which supports up to 40,000 records.

The File Type	EXCEL File	~			
Export Mode	All data (Can exp	ort up to	40000 data)		
	O Select the amoun	t of data	to export (Can ex	port up	to 40000 dat
	From the article	1	Strip, is derived	100	Data

Figure 6-52 Export Monthly Details Report

6.7.6 Appended Log Details

Appended Log Details is to get the personnel in case the person is out on a business trip.

UZKBio CVSecurity		🕒 admin ~
Attendance Management >	Attendance / Attendance Detail Report / Appended Log Details	
Attendance Setting >	Time From 2022-08-01 00:00:00 To 2022-08-01 23:59:59 Personnel ID I Name More - Q 🖉	
Schedule >		
Exception >	Department Name Personnel ID First Name Last Name Department Name Punch Time Status Development	Remarks
🚺 Attendance Detail Report 🗸	r In → Dr test9	
Manual Calculate	> □ test8 > □ test7	
Daily Attendance		
Daily Report		
Monthly Detail Report		
Leave Details		



6.7.6.1 Export

You can export all logs in Excel, PDF, CSV format.

6.7.7 Leave Details

Personnel may need leave at different circumstances. They can apply and the leave will be displayed here:

IZKBio CVSecurity	# #	😝 admin 👻
Attendance Management >	Attendance / Attendance Detail Report / Leave Details	
Attendance Setting >	Time From 2022-08-01 00:00:00 To 2022-08-01 23:59:59 Personnel ID Name More ~ Q	0
Schedule >	x ^a x ^k	
Exception >	Department Name Personnel ID First Name Last Name Department N Leave Type Start Time Development	End Time
🚺 Attendance Detail Report 🗸	nr 10] ∞ Este9	
Manual Calculate Transactions	→ Ch test3 → Ch test7	
Daily Attendance Daily Report		
Monthly Detail Report		
Appended Log Details		
Leave Details		
Exception Report		

Figure 6-54 Leave Details

6.7.7.1 Export

You can export all logs in Excel, PDF, CSV format.

6.7.8 Exception Report

U	ZKBio CVSecurity	111 X								\varTheta admin -
	Attendance Management >	Attendance Attendance Deb	al Report	Exception Repr	et i					
5	Attendance Setting	Time From 2022-08-01	To	2022-08-01	Personnel	0	Department	kama	Mars * Q	0
-	Schedule >	22	e,	G Refresh	1 Export					
6	Exception >	③ Department Name		Personnel			Department A	tiendarice _ Timeti	sble Detaile	Late(minute)
-	CALCULATE AL	Development Development		10	First Name	Lost Name		Name	Work Time	
	Attendance Detail Report \sim	 D 1850 								
	Manual Calculate	+ 🗅 testő								
	Transactions	> 🗅 best7								
	Daily Attendance									
	Daily Report									
	Monthly Detail Report									
	Appended Log Details									
_	Leave Details									
	Exception Report									
	Work Time Report									
	Annual Leave Balance Sheet									



6.7.8.1 Export

You can export all logs in Excel, PDF, CSV format.

6.7.9 Work Time Report

This will be the total effective time of this shift. It is automatically set by the system as per the Checkin/out details.

TKBio CVSecurity	::: ¥					e admin
Attendance Management >	Attendance / Attendance Detail R	eport / Work Time Repo	rt			
Attendance Setting	Time From 2022-08-01	To 2022-08-01	Personnel ID	Department Name	More - Q Q	
Schedule >	x" x"	G Refresh	↑ Export			
Exception >	Department Name	Personnel ID	First Name Last Name	Department 2022-08-01	Total Work Hours	
	Development hr	9999	K-TEST	Department Nan 0:00	0:00	
L Attendance Detail Report ~	≠ B test9	9527		Department Nan 0:00	0:00	
Manual Calculate	 Citest8 Citest7 	666	chen	Department Nan 0:00	0:00	
Transactions		555	fc	Department Nan 0:00	0:00	
Daily Attendance		5	уууу	Department Nan 0:00	0:00	
Daily Report		4	W9	Department Nan 0:00	0:00	
Monthly Detail Report						
Appended Log Details		3		Department Nan 0:00	0:00	
Leave Details		2222	ygv	Department Nan 0:00	0:00	
Exception Report		2	tsf	Department Nan 0:00	0:00	
Work Time Report		12135		Department Nan 0:00	0:00	
Annual Leave Balance Sheet		12134	name1	hr 0:00	0:00	



6.7.9.1 Export

You can export all logs in Excel, PDF, CSV format.

6.7.10 Annual Leave Balance Sheet

Personnel ID	Department Nat	те	Name	Q @			
x* x ^k	< C Refresh	∱ Export					
Department Name	ID	First Name	Last Name	Department Hire Date	Working Years	Remaining A	Total Annual
Development In	10002	raj	h	hr			
e 🕒 test9	10001			Department Nan			
 C) test8 C) test7 	9527			Department Nan			
	666	chen		Department Nan			
	2	tsf		Department Nan			
	1	tang	OP1	Department Nan			
	9999	K-TEST		Department Nan			

Figure 6- 57 Annual Leave Balance Sheet

6.7.10.1 Export

You can export all logs in Excel, PDF, CSV format.

6.8 Calculate Report

6.8.1 Leave Summary

The report summarizes the valid time for all valid leave records, leave type, within the selected date range. Select the time range from which you want to view the leave record.

JZKBio CVSecurity			e admin
Attendance Management >	Attendance / Calculate Report / Leave Summary		
Attendance Setting	Time From 2022-07-01 00.00.00 To 2022-07-28 23:59:59 Personnel ID Department Name	More - Q	2 @
Schedule >	e ² x ⁴		
Exception >	E Development	(h Marriage Leave(D	
Attendance Detail Report >	Counts Dura	ation Counts Duration	Counts Duration
🎐 Calculate Report 🗸 🗸 🗸	 ▶ □ test8 ▶ □ test7 		
Leave Summary			
Monthly Staff Report			
Monthly Departmental Report			
Roll Call Report			

Figure 6-58 Leave Summary Report

6.8.1.1 Export

It will export the leave summary data. Currently it can be exported either in three types of file EXCEL/ PDF/CSV. You can also choose the amount of data to be exported or select the maximum amount which supports up to 40,000 records.

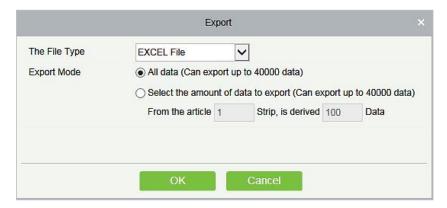


Figure 6- 59 Export Leave Summary Report

6.8.2 Monthly Staff Report

Select the Month to get the detail record of all the staff. Details include details of all personnel in the department, attendance, late, leaving early, and so on.

TZKBio CVSecurit	y ii	×											0	admin
Attendance Management		endance / Calculate Repor	t i Marthly	Staff Report									0	8
Attendance Setting		Time From 2022-00-01		2022-08-01	Personnel (D		Depar	tereni Name			More -	Q 0		
Schedule	·	a ^e ¢ Department Name Development Iv	C Refresh	1 Export										
Exception	3	the state of the s		Personnel		Departme		EActual(mi		Late(min		Early(min		Qve
Attendance Detail Report		BW		99999	First Name Last Name X-TEST	Department /	Should 0.0	Actual 0.0	Walid .	Ouration 0.0	Counts	Duration 0.0	Counts	We
Calculate Report	•	* x ⁴ Department Name Development D tv to test8 + C1 test8 + C1 test7		9527		Department I	0.0	0.0	0.0	0.0	0	0.0	0	6.6
Leave Summary				000	chen	Department 1	0.0	0.0	0.0	0.0	0	0.0	9	0.0
Monthly Staff Report				555	10	Department I	0.0	0.0	0.0	0.0	0	0.0	α	0.0
Monthly Departmental Repo	ort			8	37777	Department (0.0	0.0	0,0	0.0	0	0.0	d .	0.0

Figure 6-60 Monthly Staff Report

6.8.2.1 Export

You can export all logs in Excel, PDF, CSV format.

6.8.3 Monthly Departmental

Select the date to get the detail record of all departments. Details include details of all personnel in the department, attendance, late, leaving early, and so on.

IZKBio CVSecurity	::: ¥												0 =	admin
Attendance Management >	Attendance / Calculate Repor	t / Monthly	Departmental R	eport										
Attendance Setting	Time From 2022-07-01	То	2022-07-29	Department	Name			a @						
Schedule >	x2 x4	*	O Refresh	± Export										
Exception >	Department Name		Department		Expected	d/Actual(mi	nute)	Late(minu	ute)	Early(min	ute)	Overtime	(hour)	
	Development In		Number	Name	Should	Actual	Valid	Duration	Counts	Duration	Counts	Weekd	Weeke	Halid
Attendance Detail Report >	∠ B test9		3	hr	0.0	0.0	0.0	0.0	Late(minute) Early(minute) Overtime(hour) Duration Counts Duration Counts Weekd Weeke 0.0 0 0.0 0 0.0 0.0 0.0 0.0	0.0				
😗 Calculate Report 🛛 🗸	C1 test8 C1 test7		1	Department Name	0.0	0.0	0.0	0.0	0	0.0	0	0.0		0.0
Leave Summary			2	Development	0.0	0.0	0.0	0.0	0	0.0	0	0.0	0.0	0.0
Monthly Staff Report														
Monthly Departmental Report														



6.8.3.1.1 Export

You can export all logs in Excel, PDF, CSV format.

6.8.4 Roll Call Report

The procedure of identifying the availability by calling out a list of names

IZKBio CVSecurity	/ ::: ¥					e admin ~
Attendance Management	Attendance / Calculate Report / I	Roll Call Report				
Attendance Setting	Time From 2022-08-01 00:00:00	To 2022-08-01 23:59:59	9 Status	Q @		
Schedule	x* x ^k	< G Refresh	<u>↑</u> Export			
Exception	Department Name	Personnel ID	First Name	Department Name Check In Time	Status	
	Development	10002	raj	hr	No Check-In	
Attendance Detail Report	→ E→ test9	10001		Department Name	No Check-In	
Calculate Report		10	tang	Department Name	No Check-In	
Leave Summary		9527		Department Name	No Check-In	
Monthly Staff Report		666	chen	Department Name	No Check-In	
Monthly Departmental Repo	t	2	tsf	Department Name	No Check-In	
Roll Call Report		9999	K-TEST	Department Name	No Check-In	
		12135		Department Name	No Check-In	

Figure 6-62 Roll Call Report

6.8.4.1 Export

You can export all logs in Excel, PDF, CSV format.

7 Consumption

This module allows the user to set up a consumption system with the device and realize their functions. The device can be set as either a "Consumer Machine", a "Cashier Machine" or a "Subsidy Machine". The "Consumer machine" type combines various consumption modes to meet the diversified consumption requirements such as fixed value mode or amount mode. The "Cashier Machine" type realizes the device recharge and refund function. The "Subsidy machine" type is used to receive allowances/subsidies. This module will collect the data from the device and summarize it on the various consumption reports. It can also perform various operations like issue card, card return, card suspend and resume, and other operations through the card reader connected to the software.

Operation Scenario:

Online consumption management controls online consumption device through software, and sets different consumption patterns on the software side, thus realizing diversified consumption forms. Diversified consumption reports support multi-dimensional analysis and statistics of consumption data.

Operation Flow:

This paper introduces the configuration process of online consumption management.

The configuration process of online consumption management is shown in Figure 7-1.

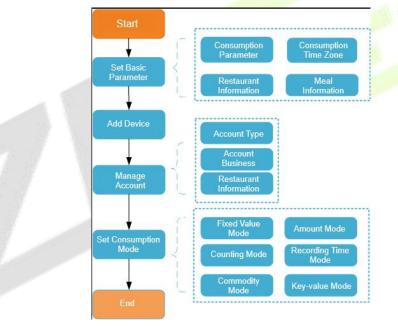


Figure 7-1 Online Consumption Configuration Process

7.1 Consumption Basic Information

This paper introduces that before using the consumption function in, it is necessary to set the relevant basic parameters, and then configure other functions, including Piecewise Fixed Value, Consumption time Zone, Restaurant Information, Meal Information, Commodity Information, Key Value Information, and Card Information.

Click Consumption, then select Consumption Basic Information.

7.1.1 Piecewise Fixed Value

Piecewise Fixed value is the value and validity of a card which is supposed to be used on the consumer device.

Piecewise Fixed Value		Number		Name		Is It Effective	• Q @	
Consumption Time Zone		O Refres						
Restaurant Information								
Meal Information		Number	Name	Amount	Start Time	End Time	Is It Effective Remarks	Operation
wearmornation		1	Default 1	10.0	00:00	1 <mark>0:00</mark>	Yes	0
Commodity Information		-	p. d. u.b.	10.0	10.01	44.00	N	0
Key Value Information		2	Default 2	10.0	10:01	14:00	Yes	<u>v</u>
Card Information		3	Default 3	10.0	14:01	20:00	Yes	0
our monaton		<u>4</u>	Default 4	10.0	20:01	23:59	Yes	2
		<u>5</u>	Default 5	10.0	00:00	10:00	No	2
		<u>6</u>	Default 6	10.0	10:01	14:00	No	2
	«	Z	Default 7	1 <mark>0.0</mark>	14:01	20:00	No	0
		8	Default 8	10.0	20:01	23:59	No	0

Figure 7-2 Piecewise Fixed Value

• Edit

By default, there are eight values, click \swarrow on the operation column to open the modification dialog box.

Name*	Default 1	
Start Time*	00 : 00	
End Time*	10 : 00	
Is It Effective	Yes	•
Amount*	10	
Remarks		

Figure 7-3 Edit Piecewise Fixed Value

In the dialog box, you can select the required **Name**, **start time**, **End time**, **Is It Effective**, **Amount** and **Remarks** (optional), as shown in the above figure 3.2. After providing the information, click **OK** to save and exit.

7.1.2 Consumption Time Zone

By default, the system has some Consumption Time zones, you can select and edit according to your preferences.

Click Consumption > Consumption Basic Information , then select Consumption Time Zo

Consumption Basic Inf	~ 0	consumption / Consumpt	ion Basic Informatio	n / Consumption Time	Zone		
Piecewise Fixed Value		Name	Is It Effectiv	/e	• Q &		
Consumption Time Zone		C Refresh					
C Refresh	Is It Effective	Remarks	Operation				
		Fixed Time Period	08:00	09:00	Yes		0
		Fixed Time Period	10:00	14:00	Yes		<u>@</u>
		Fixed Time Period	17:00	19:00	Yes		0
		Fixed Time Period	20:00	23:59	Yes		2
		Fixed Time Period	08:00	09:00	No		0
		Fixed Time Period	10:00	14:00	No		<u>@</u>
	«	Fixed Time Period	17:00	19:00	No		0
		Fixed Time Period	20:00	23:59	No		<u>@</u>
		Second Batch	08:00	09:00	Yes		0

Figure 7-4 Consumptio<mark>n Tim</mark>e Zone

• Edit

Click \checkmark on the operation column to open the modification dialog box.

Name*	Fixed Time Period	
Start Time*	10 : 00	\$
End Time*	14 : 00	\$
Is It Effective	Yes	•
Remarks		
		2

Figure 7-5 Edit Consumption Time Zone

In the dialog box, you can select the required **Name**, **start time**, **End time**, **Is It Effective**, **Amount** and **Remarks** (optional), as shown in the above figure 3.2. After providing the information, click **OK** to save and exit.

7.1.3 Restaurant Information

By default, a Restaurant name is already added, you can edit it and add new ones.

Click Consumption > Consumption Basic Information, then select Restaurant Information.

Piecewise Fixed Value	Restaurant Number	Res	taurant Name	Q	<
Consumption Time Zone	0				
Restaurant Information	⊖ Refresh =+ New	🗓 Delete			
hereite and the second s	Restaurant Nu.	Restaurant Name	Remarks	Operations	
Meal Information		Headquarters	Default Data		
Commodity Information					
Key Value Information					
Card Information					



7.1.3.1 New

Click **Consumption** > **Consumption Basic Information** > **Restaurant Information**, then select **New**, to add a new restaurant.

Restaurant Number*	ĺ.	_
Restaurant Name*	<u>L</u>	
Remarks		_
Remarks		

Figure 7-7 Add New Restaurant.

Fields are as Follows:

Parameter	Description
Restaurant Number	Enter Resaurant Number.
Restaurant Name	Enter Restaurant Name.
Remarks	Enter Remarks.

Table 7-1 Add New Restaurant

Click **OK**, to save and exit, or click **Save and New** for continue adding.

7.1.3.2 Delete

Click Consumption > Consumption Basic Information > Restaurant Information, then select Delete.

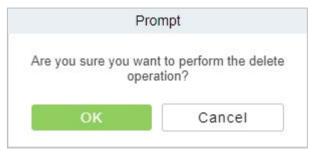


Figure 7-8 Delete Restaurant Information

7.1.4 Meal Information

Click Consumption > Consumption Basic Information, then select Meal Information.

Piecewise Fixed Value	Meal Number		Meal Name	Is It E	ffective	- Q @	
Consumption Time Zone	O Refresh						
Restaurant Information	Meal Number	Meal Name	Is It Effective	Start Time	End Time	Remarks	Operatio
Meal Information	1	Breakfast	Yes	00:00	10:00		0
Commodity Information	2	Lunch	Yes	10:01	14:00		2
Key Value Information	3	Dinner	Yes	14:01	20:00		0
Card Information	4	Midnight Snack	Yes	20:01	23:59		2
	5	Meal 05	No	00:00	10:00		2
	<u>6</u>	Meal 06	No	10:01	14:00		<u></u>
	« <u>7</u>	Meal 07	No	14:01	20:00		2
	8	Meal 08	No	20:01	23:59		0

Figure 7-9 Meal Information

7.1.5 Commodity Information

Click Consumption > Consumption Basic Information, then select Commodity Information.

Consumption Basic Inf \vee	Consumption / Consumption Basic Infor	mation / Commodity Informatio	n		
Piecewise Fixed Value	Commodity Number	Commodity Name	Q	2	
Consumption Time Zone	⊖ Refresh ∓ New 💼 Delete				
Restaurant Information		Mama - Unit avias	Discount/0/3	Deserte	. On a set land
Meal Information	Commodity Nu Commodity	/ Name Unit price	Discount(%)	Barcode	Operations
Commodity Information					
Key Value Information					
Card Information					



7.1.5.1 New

To add New Commodity Information, Click Consumption > Consumption Basic Information > Commodity Information, then select New.

Commodity Number*	Ī		
Commodity Name*			
Unit price*	1	-	
Discount(%)*	0		
Barcode			
		18	

Figure 7-11 Add New Commodity Information

Fields are as follows:

Parameter	Description
Commodity Number	Enter Commodity number.
Commodity Name	Enter Commodity name.
Unit Price	Enter unit price as required.
Discount	Set Discount.
Barcode	Enter the barcode.

Table 7-2 New Commodity Information

Click **OK** to save and exit.

7.1.5.2 Delete

Click Consumption > Consumption Basic Information > Commodity Information, then select Delete.

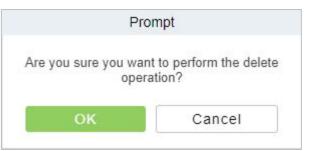


Figure 7-12 Delete Commodity Information

Click **OK** to save and exit.

7.1.6 Key Value Information

Click **Consumption** > **Consumption Basic Information**, then select **Key Value Information** to enter the unit value in the consumer device as shown below:

Consumption Basic Inf 🗸	С	onsumption / Cons	umption Basic Info	ormation / Key Value Information
Piecewise Fixed Value		Key Value Number		Q &
Consumption Time Zone Restaurant Information		C Refresh		
		Key Value Nu	Unit price	Operations
Meal Information		1	0.0	0
Commodity Information		2	0.0	2
Key Value Information			0.0	
Card Information		3	0.0	0
		<u>4</u>	0.0	2
		<u>5</u>	0.0	0
		<u>6</u>	0.0	2
	«	Z	0.0	0
		<u>8</u>	0.0	<u>/</u>
		9	0.0	0

Figure 7-13 Key value information

7.1.7 Card Information

Click Consumption > Consumption Basic Information, then select Card Information.

Piecewise Fixed Value	Card Type Number	Card Typ	oe Name	Discount(%)	
Consumption Time Zone	ORefresh ∓New on	Delete				
Restaurant Information	G Refresh 1+ New U	Delete				
	Card Type Disc	ount Max. Daily Co	Max. Daily Co	Max. One-time	Max. Meal Co	Max. M
Meal Information	Employee Card 10	0.0	0	0.0	0.0	0
Commodity Information						
Key Value Information						

Figure 7-14 Card Information

7.1.7.1 New

Click Consumption > Consumption Basic Information > Card Information, then select New.

Zone* Iax. Daily Consumption 0 mount* Times* Iax. One-time 0 Max. Meal Consumption 0 onsumption Amount* Amount* Iax. Meal Consumption 0 Max. Meal Consumption 0 imes* 0 Max. Meal Consumption 0 Iax. Meal Consumption 0 Min. Card Balance* 0 imes* Iax. Card Balance* Vailable Meal ✓	Card Type Number*		Card Type Name*		Ĩ
Iax. Daily Consumption 0 Max. Daily Consumption 0 mount* Times* Iax. One-time 0 Max. Meal Consumption 0 0 onsumption Amount* Amount* Iax. Meal Consumption 0 Min. Card Balance* 0 onsumption 0 Min. Card Balance 0 onsumption 0 onsumption 0 Min. Card Balance 0 onsumption 0 onsumption 0 Min. Card Balance	Discount(%)*	0 -	Consumption Time	Fixed Time Period 🔹	Î
mount* Times* lax. One-time 0 onsumption Amount* Amount* lax. Meal Consumption 0 Amount* Min. Card Balance* lax. Card Balance* 0 vailable Meal			Zone*		
Iax. One-time 0 Max. Meal Consumption 0 onsumption Amount* Amount* Amount* Iax. Meal Consumption 0 Min. Card Balance* 0 imes* Iax. Card Balance* 0 Iax. Card Balance* 0 vailable Meal Image: Card Balance 0 Image: Card Balance* 0	Max. Daily Consumption	0	Max. Daily Consumption	0	1
onsumption Amount* Amount* lax. Meal Consumption 0 imes* 0 lax. Card Balance* 99999 Effective Use Of Days* 0 vailable Meal Available Device 	Amount*		Times*		
Iax. Meal Consumption 0 imes* 0 Iax. Card Balance* 99999 Effective Use Of Days* 0 vailable Meal Available Device 	Max. One-time	0	Max. Meal Consumption	0	
imes* lax. Card Balance* 99999 Effective Use Of Days* o vailable Meal Available Device	Consumption Amount*		Amount*		
Iax. Card Balance* 99999 Effective Use Of Days* 0 vailable Meal Image: Card Balance Control of Days Control o	Max. Meal Consumption	0	Min. Card Balance*	0	
vailable Meal Available Device	Times*				
	Max. Card Balance*	99999	Effective Use Of Days*	0	
emarks	Available Meal	-	Available Device		
	Remarks				
		016	0		
		OK	Cancel		

Figure 7-15 New (Add Card Information)

Parameter	How to set
Card Type Number	A positive integer between 1 and 254, which cannot be repeated.
Card Type Name	Non-special characters, maximum 4 bits.
Maximum amount of daily consumption	The maximum amount consumed every day, the effective range is an integer between 0 and 600, and 0 represents unlimited.
Maximum number of daily consumptions	The maximum number of times consumed every day, the effective range is an integer between 0 and 255, and 0 represents unlimited.
Maximum amount of secondary consumption	The maximum amount of each consumption, the effective range is an integer between 0 and 600, and 0 represents unlimited.
Maximum amount of meal consumption	The maximum amount consumed for each meal every day, the effective range is an integer between 0 and 600, and 0 means unlimited.
Maximum number of meals consumed	The maximum number of times of consumption of each meal every day, the effective range is an integer between 0 and 255, and 0 means unlimited.
Minimum/Maximum Card Balance	Integer \ge 0, minimum card balance \le maximum card balance, and the maximum card balance cannot exceed the upper limit of account balance set by parameter.
Effective use days	Set the effective use days of the account.
Consumption Time Zone	Select the consumption time batch, and the accumulation of effective time periods of the same batch is the total effective consumption time period of the batch.
Available meal	Select the appropriate valid meal range and distribute it to the device. If not, all valid meals will be distributed.
Discount (percentage)	Select the discount percentage, which is an integer between 0 and 100.

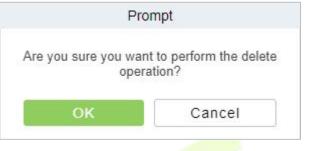
Parameter	How to set
Available device	Select the device to be distributed by the household class.
Remarks	Any character, up to 50 characters.

Table 7-3 Add Card Information

Click OK to save exit.

7.1.7.2 Delete

Click Consumption > Consumption Basic Information > Card Information, then select Delete.





7.2 Consumption Device

This module is used to manage consumer devices and set basic parameters of the consumer system.

7.2.1 Consumption Device

Click Consumption > Consumption Device, then select Consumption Device.

Consumption Basic Inf >	Consumption / Consumption Device / Consumption Device
Consumption Device ~	Device Name Serial Number Device Type Q
Consumption Device	C Refresh : 會 Delete : Q. Search : 嬰 Device Control ▾ 匠 View And Get Information ▼ 窗 Clear Device Data ▼
Consumption Parameter	Device Name Serial Num Device Type IP Address Status Number Of Device M Firmware Version Push Protocol V Operations

Figure 7-17 Consumption Device

7.2.1.1 Delete

Click Consumption > Consumption Device > Consumption Device, then select Delete.



Figure 7-18 Delete Consumption Device

7.2.1.2 Search

Click Consumption > Consumption Device > Consumption Device, then select Search.

		Search		×
Search				
otal Progress				
IP Address	Device Type		Serial Number	
IP Address	Serial Number	Device Model	Operations	
A The current syste	em communication port is 8088, p	blease make sure the de	evice is set correctly.	
		Close		

Figure 7-19 Search Consumption Device

Search Consumption Device by entering **Total Progress, IP Address, Device Type, and Serial Number.**

7.2.1.3 Device Control

Reboot Device

It will reboot the selected device.

• Synchronize Software Data to Device

Synchronize data from the software to the device

7.2.1.4 View and Get Information

• Collect All Data

Click Consumption > Consumption Device > Consumption Device > View and Get Information then select Collect All Data.

Select a device in the device list below, click and select the device from the list, click to collect all data, and the following dialog box will pop up. According to the operator's needs, check the data that needs to be synchronized. Click Start and wait for the data to sync until the synchronization is complete.

7.2.1.5 Clear Device Data

Click **Consumption** > **Consumption Device** > **Consumption Device**, then select **Clear Device Data**.

• Clear Swipe Card Data

Click Consumption > Consumption Device > Consumption Device > Clear Device Data, then select Clear Swipe Card Data.

The operation here is to select the device first, then you can check the type of the card record, you can select all, click **Start** will clear the data of the selected card record, click **Close** will close the current

dialog box, no operation.

• Clear Consumer Machine Settings

Click Consumption > Consumption Device > Consumption Device > Clear Device Data, then select Clear Consumer Machine Settings.

• Delete Device Command

Click Consumption > Consumption Device > Consumption Device > Clear Device Data, then select Delete Device Command.

7.2.2 Consumption Parameter

Parameter setting is the most basic setting in consumption management, and the parameter setting here is taken as the global setting.

Click Consumption > Consumption Device > Consumption Device, then select Consumption Parameter.

TZKBio CVSecurity	::: ¥		😝 admin
Consumption Basic Inf >	Consumption / Consumption Device	e / Consumption Parameter	
Consumption Device	Basic Settings		Basic Settings
Consumption Device			Currency Unit Card Setting
Consumption Parameter		Card Balance Limit 09090	
		Card Issuing Master Sector 1st sector	
		Card Issuing Sector 2nd sector -	
	Currency Unit		
		z roporton I •	
	Card Setting		
Consumption Card Ma >		The consumer device version must match the card mode. System Parsword	
Consumption Detail >		Confirm Password	
Anual Supplement >		Mode	
Subsidy >		 Single Wallet Mode (A5) After adding a device, the system password and mode are not allowed to be modified 	
II. Consumption Report >		again.	
Consumption Statistic >		ок	

Figure 7-20 Consumption Parameter

Fields are as follows:

Parameter	Description
Basic Setting	Set Card balance limit for 5 characters, Card Issuing Master Sector, and Card Issuing Sector.
Currency Unit	Enter Symbol and Proportion for Currency Unit.
Card Setting	Set System Password and set Mode.

Table 7-4 Consumption Parameter

Click **OK** to save and exit.

7.3 Consumption Card Management

7.3.1 Card Service

Click Consumption > Consumption Card Management, then select Card Service.

Using this option, you can issue different types of cards and set their usage limits. You can also manage the already existing cards.

The initial interface of this module is shown below:

	Consumption Basic Inf >	Consumption / Consumption Card Management / Card Service
≝	Consumption Device >	🗞 Modify card information
	Consumption Card Ma 🗸	Card Service
	Card Service	
	Card Management	$=$ \rightarrow $+$
	Income And Expenses	Card Issue Return Card Supplementary Card
		Card Consumption
		* + + + + + + + + + + + + + + + + + + +
		Device Driver
_		Device driver installation status: Detected Device Driver is not installed: Driver Download
		Figure 7-21 Card Service

7.3.1.1 Card Issue

Empty Password* Card Original Password*		\otimes	
ard Information	<u>.</u>		
Card Type*	Ordinary Card	•	
Consumer Card Type*	Employee Card	•	
Person Name*		Q	
Card Account*	[]		
Amount*	0.00		
Card Cost*	0.00		
Management Fee	0.00		
Excess Password*	123456		

Figure 7-22 Card Issue

If the card is previously used before initialization, you can set blank password or keep the original password of the card. After setting the card type and consumer card type in this wi or pw, click the icon beside the Person's name field and select the required personnel (you need to add the required personnel in the personnel module before issuing card). Then set the **Card Account, Amount, Card Cost, Management Fee, Excess Password**, click **Write Card** to complete.

Prerequisites:

- 1. Make sure the required person is already added in the personnel module before issuing card.
- 2. The card needs to be initialized before issuing the card.

7.3.1.2 Return Card

	Return Card	×	
Card Account			
Personnel ID			
First Name			
Last Name			
Department Name			
Account Balance			
Card Balance			
Refund Cost			
Read (Card Cancel		
incuu i	Ouncer		

Figure 7-23 Retu<mark>rn Car</mark>d

Return Card operation is performed to stop the card being used further in the consumption software system.

After clicking **Return card**, a pop-up window will give additional information for the operation. Put the card on the card reader, click on the card to read, the card information will be displayed, check the information, and click OK to block or revoke the card.

Prerequisite:

To withdraw a card approval, you must have an issued card.

Enter details for Parameters Card Account, Personnel ID, First Name, Last Time, Department Name, Account Balance, Card Balance, and Refund Cost.

Click Read Card.

7.3.1.3 Supplementary Card

Prerequisite:

This function is used when a card is reported lost.

Card Information			
Card Type*	Ordinary Card	•	
Consumer Card Type*	Employee Card	•	
Person Name*		Q	
Card Account*	1		
Amount*	0.00		
Card Cost*	0.00		
Management Fee	0.00		
Excess Password*	123456		
Please keep all the device in uneven accounts.	the consumer system onlin	ne, otherwise it may lead	

Figure 7-24 Supplementary Card

Click the search icon beside the Person Name field and select the person who has lost the card. Click to write the card with the same information as the lost card. After the card is issued, the balance and other information in the original card will be written into the new card. (The used card needs to be initialized, and the card can be set to a blank password or a card original password at the initialization interface.)

7.3.1.4 Top Up

Note: Please ensure that all devices in the consumption system are online. Otherwise, the processing result after the above operation cannot be synchronized to other devices. And the original card can still be used for consumption, resulting in the card balance being inconsistent with the actual amount and the account being uneven. Please be careful with Top Up.

Card Account		
Personnel ID		
First Name		
Last Name		
Department Name		
Account Balance		
Card Balance		
Added Balance		
Card Flow Number		
Top Up Amount*	0.00	

Figure 7-25 Top Up

This function is used to add an extra amount to the card balance. Click the top up button to open the Top-up interface. Put the card on the card reader, click on the card to confirm the card information. Enter the amount you need to recharge and then click OK to execute the operation.

7.3.1.5 Refund

	Refund	×	
Card Account			
Personnel ID			
First Name			
Last Name			
Department Name			
Account Balance			
Card Balance			
Amount After Refund			
Card Flow Number			
Refund Amount*	0.00		
Read C	ard Cancel		
Reau C	Cancer		

Figure 7-26 Refund

Refund operation is used to return a specified amount to the card. Click the refund button to open the refund interface, put the card on the card reader, click on the Read card to confirm the card information. Enter the amount you need to refund and click OK to execute the operation.

7.3.2 Card Management

Click Consumption > Consumption Card Management, then select Card Management.

This function is used to perform two operations; **Logout Management Card, Non-Card Return Card, and Export**. And on this interface, you can also view the card information that has been issued till date.

Consumption Basic Inf >	Consumption / Consumption Card Management / Card Management		
Consumption Device >	Personnel ID Name	Card Account More -	Q @
🥃 Consumption Card Ma 🗸	🔾 Refresh 🖞 Logout Management Card 🛛 🛱 Non-card Return Ca	rd 🛧 Export	
Card Service	Personnel ID First Name Last Na Department N	Department Card Number Card Typ	e Card Type Name Balance Card Status Card Issue Date
Card Management			



7.3.2.1 Logout Management Card

This function is used to log out the management and the operation card. After the logout operation, the management card or operation card will be invalid.

Click Consumption > Consumption Card Management > Card Management, then select Logout Management Card.

7.3.2.2 Non-card Return Card

Click **Consumption** > **Consumption Card Management** > **Card Management**, then select Non-card Return Card.

Click **Non-card return card**, select the desired refund option and click **OK**. If the card is eligible for the refund, the amount will be refunded to the card and a refund record will be generated in the system.

The card will not be used in this consumer system after the card is not returned.

Solution Note: Non-card return card Please ensure that all devices in the consumption system are online before operation. Otherwise, the processing result after operation may not be synchronized to other devices in time. The card can still be consumed, resulting in the card balance being inconsistent with the actual amount and unbalanced situation. Please be careful with this!

7.3.2.3 Export

Click Consumption > Consumption Card Management > Card Management, then select Export.

It exports the current report data.

Solution Solution Solution And American Solution Solution

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL	
Data to Export	 All (max 100000 records) 	
	Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	
	OK Cancel	

Figure 7-28 Export

7.3.3 Income and Expenses

This function will show all the payments and due amount data of all the cards in the consumption system.

Click Consumption > Consumption Card Management, then select Income and Expenses.

	Consumption Basic Inf >	Consumption / Consumption Card Management / Income And Expenses
≞	Consumption Device >	Operating Time From 2022-04-29 00:00:00 To 2022-07-29 23 59:59 Personnel ID More * Q Q
8	Consumption Card Ma 🗸	C Refresh ⊥ Export
	Card Service	Personnel ID First Name Last Na Department N Card Num Type Name Type Subsidy T Amount Balance Upload Time Operating Time Serial Number Device Flow Nu Record Type
	Card Management	
	Income And Expenses	

Figure 7-29 Income and Expenses

7.3.3.1 Export

Click Consumption > Consumption Card Management > Income and Expenses, then select Export.

This feature allows you to export consumption details in EXCEL, PDF, CSV format files.

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
	OK Cancel	

7.4 Consumption Detail

Click Consumption, then select Consumption Detail.

7.4.1 Consumption Detail Report

Click Consumption > Consumption Detail, then select Consumption Detail Report.



Figure 7-31 Consumption Detail Report

7.4.1.1 Export

Click Consumption > Consumption Detail > Consumption Detail Report, then select Export.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	¥	
Data to Export	All (max 10000)	00 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
		1	
	ОК	Cancel	

Figure 7-32 Export

7.4.1.2 Error Correction

Click Consumption > Consumption Detail > Consumption Detail Report, then select Error Correction.

7.4.1.3 Import U Disk Record

Click Consumption > Consumption Detail > Consumption Detail Report, then select Import U Disk Record.

If the equipment consumption record is found inconsistent with the software, you can export the consumption records of the machine

	Import	×
File Format	● txt	
Select File	Choose File No file chosen	
	number_pos_time", Please Check And Import (for example:	
	_20190730144700.txt)	

Figure 7-33 Import U Disk Record

7.4.2 Consumption Exception Report

Click Consumption > Consumption Detail, then select Consumption Exception Report.

Consumption Basic Inf >	Consumption / Consumption Detail / Consumption Exception Report
Consumption Device >	Consumption Time From 2022-04-29 00:00:00 To 2022-07-29 23 59 59 Personnel ID More * Q 🖉
Consumption Card Ma >	C Refresh ↑ Export @ Correct
Consumption Detail ~	Personnel ID First Name Last Na Card Sta Department Nu Department Card Acc Type Na Amount Of Consump Bala Consumption Restaurant N Meal Na Serial Num Device Flow N Card Flow
Consumption Detail Report Consumption Exception Report	

Figure 7-34 Consumption Exception Report

7.4.2.1 Export

Click Consumption > Consumption Detail, then select Consumption Exception Report.

	Export		×
incrypt or not	🔿 Yes 💿 No		
ile Format	EXCEL -		
ata to Export	 All (max 100000 records) 		
	O Selected (max 100000 red	cords)	
	Start Position 1	1	
	Total Records 100		
	ок с	ancel	

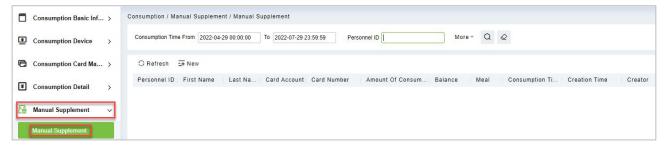
Figure 7-35 Export Consumption Exception Report

7.5 Manual Supplement

It is used to enter some consumptions record details manually in the system.

Solution Note: Before performing this operation, you need to have the relevant operation card.

Click Consumption, then select Manual Supplement.





7.5.1 Manual Supplement

Click Consumption > Manual Supplement, then select Manual Supplement.

You need to cross-check the relevant information of the card. When the user puts the relevant card into the card reader, click on read card to read the detailed data such as the Card Account, Card Number, First Name, Last Name, Personnel ID, Balance, Card Flow Number, Meal, Available Device, Consumption Time, and Amount of Consumption.

	Ê		
Card Account			
Card Number			
First Name			
Last Name			
Personnel ID			
Balance			
Card Flow Number			34 B.
Meal*			5
Available Device*		¥	
Consumption Time*			
Amount Of Consumption*	0		
Read Card	Cancel		

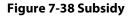
Figure 7-37 New (Add new Manual supplement)

7.6 Subsidy

Click **Consumption**, then select **Subsidy.** To enter the subsidy page, you can perform different function related to subsidy.

Solution Note: Before the subsidy operation, you need to add personnel in the Personnel module.

٦	Consumption Basic Inf	Consumption / Subsidy / Subsidy Management
₫	Consumption Device	Personnel ID I Name Whether To Receive More + Q Q
6	Consumption Card Ma	🖓 Refresh 🗷 Subsidy Registration 🔓 Review 🕹 One-Click Review 🖼 Reissue The Command 🛍 Delete ৬ Import \cdots More 👻
¥	Consumption Detail	Personnel ID First Name Last Na Subsidy Amo Receiving Am Card Bala Whether To Receive Whether To Pa Auditors Subsidy Receive Effective Time Of S Remarks Operations
ß	Manual Supplement	
	Subsidy	
	Subsidy Management	



7.6.1 Subsidy Registration

Click Consumption > Subsidy > Subsidy Management, then select Subsidy Registration.

Personnel ID*	sidy Registration	0	×
Subsidy Amount* Effective Time Of Subsidy* Remarks	þ		
ОК	Cancel]	1

Figure 7-39 Subsidy Registration

Fields are as follows:

Parameter	Description
Personnel ID	Enter Personnel ID.
Subsidy Amount	Enter Subsidy amount.
Effective Time OF Subsidy	Mention Effective time of Subsidy.
Remarks	Mention remarks if any.

Table 7-5 Subsidy Registration

Click **OK** to save and exit.

7.6.2 One- Click Review

Click Consumption > Subsidy > Subsidy Management, then select One- Click Review.

This function is mainly to review the unapproved subsidies in the system and will not deal with the subsidy records that have been approved. During the review process, if the unapproved subsidy cannot be approved for some reason (such as the user has already returned the card), the subsidy will not be processed.

Pr	ompt
Are you want to perfor	rm the One-Click Review ration?
ope	i duori :

Figure 7-40 One-Click Review

7.6.3 Review

Click Consumption > Subsidy > Subsidy Management, then select Review.

This function is mainly to review the audit. Before performing audit, you need to select the subsidy (select in the multi-select box). After clicking the review, an audit dialog box will pop up. The dialog box will display the person number and name as selected by the user.

7.6.4 Reissue the Command

Click Consumption > Subsidy > Subsidy Management, then select Reissue the Command.

This function is primarily used to re-issue the subsidy to the subsidy machine. Select the required subsidy(s), then click Reissue the command. The dialog box will display the person number and name selected by the user, click OK to reissue the subsidy order to the subsidy machine.

7.6.5 Delete

Click Consumption > Subsidy > Subsidy Management, then select Delete. Prompt Are you sure you want to perform the delete operation? Cancel Figure 7-41 Delete Subsidy

7.6.6 Import

Click Consumption > Subsidy > Subsidy Management, then select Import.

This function is used to import subsidies in batches.

File Format	 Excel 	
Select File	Browse Not Uploaded	
	ata format is table name, the second line is header, the third check the file and then import.	line is the
		line is the

Figure 7-42 Import Subsidy

7.6.7 More

Click Consumption > Subsidy > Subsidy Management, then select More.

In More you can operate options like **Export** and **Download Template**.

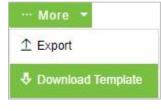


Figure 7-43 More

7.6.8 Export

Click Consumption > Subsidy > Subsidy Management > More, then select Export.

This function is used to export the queried subsidies.

Encrypt or not	○ Yes No	
File Format	EXCEL	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
1		
2	OK Cancel	

Figure 7-44 Export

7.6.9 Download Template

Click Consumption > Subsidy > Subsidy Management > More, then select Download Template.

7.7 Consumption Report

Click Consumption, then select Consumption Report.

The statistical report consists of 9 modules: Issue Card Report, Top Up Report, Refund Report, Subsidy Report, Report of Return Card, Card Cost Report, Card Balance Report, Non-Card Return Card Report, and Report of Resume the Card.

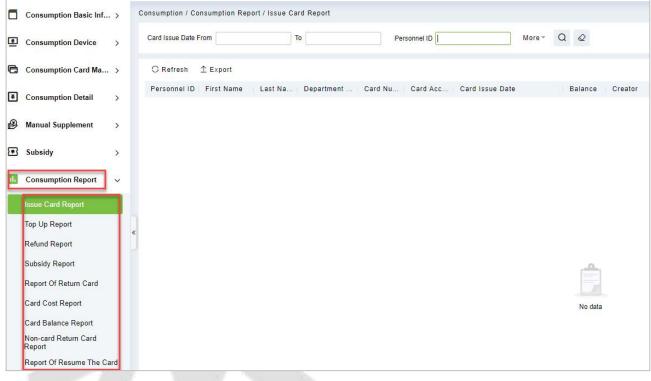


Figure 7-45 Consumption Report

7.7.1 Issue Card Report

Click Consumption > Consumption Report, then select Issue Card Report.

7.7.1.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Issue Card Report, then select Export.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	O Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	
	OK Cancel	

Figure 7-46 Export

7.7.2 Top Up Report

Click Consumption > Consumption Report, then select Top Up Report.

7.7.2.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Top UP Report, then select Export.

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL 👻	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
	OK Cancel	
	Figure 7-47 Export	

7.7.3 Refund Report

Click **Consumption** > **Consumption Report**, then select **Refund Report**.

7.7.3.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Refund Report, then select Export.

		xport	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	eren i Transformation	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Selected (max Start Position	100000 records)	

Figure 7-48 Export Refund Report

7.7.4 Subsidy Report

Click Consumption > Consumption Report, then select Subsidy Report.

7.7.4.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Subsidy Report, then select Export.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	All (max 100000 records)	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
	OK Cancel	
	Caller	

Figure 7-49 Export Subsidy Report

7.7.5 Report of Return Card

Click **Consumption** > **Consumption Report**, then select **Report of Return Card**.

7.7.5.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Report of Return Card, then select Export.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	•	
Data to Export	All (max 10000)	00 records)	
	O Selected (max	100000 records)	
	O Ociceted (max	100000 (ecolus)	
	Start Position	1	

Figure 7-50 Export Report of Return Card

7.7.6 Card Cost Report

Click Consumption > Consumption Report, then select Card Cost Report.

7.7.6.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Card Cost Report, then select Export.

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	
	OK Cancel	

Figure 7-51 Export Card Cost Report

7.7.7 Card Balance Report

Click **Consumption** > **Consumption Report**, then select Card balance Report.

7.7.7.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Card Balance Report, then select Ex
--

Encrypt or not	Yes No	
File Format	EXCEL	
Data to Export	 All (max 100000 records) 	
	Selected (max 100000 records)	
	U,	
	Start Position 1	

Figure 7-52 Export Card Balance Report

7.7.8 Non-Card Return Card Report

Click Consumption > Consumption Report, then select Non-Card Return Card Report.

7.7.8.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Non- Card Return Card Report, then select Export.

	E	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL		
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	ОК	Cancel	

Figure 7-53 Export Non-Card Return Card Report

7.7.9 Report of Resume the Card

Click Consumption > Consumption Report, then select Report of Resume the Card.

7.7.9.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Report > Report og Resume the Card, then select Export.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	*	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position		
	Start Position	1	

Figure 7-54 Export Report of Resume the Card

7.8 Consumption Statistics

The statistical report contains the statistical information of consumption system module.

It includes **Personal Consumption Report, Department Summary, Restaurant Summary, Device Summary, Income** and **Expenses Report,** and **Meal Summary.**

Click Consumption, then select Consumption Statistics.

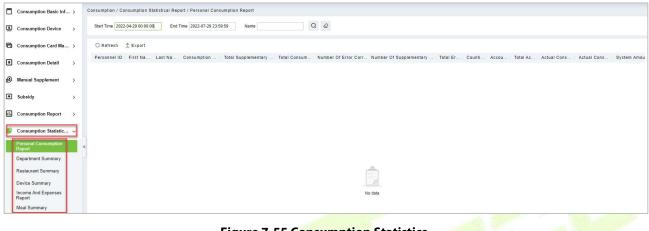


Figure 7-55 Consumption Statistics

7.8.1 Personal Consumption Report

Click **Consumption > Consumption Statistics** then select **Personal Consumption Report.**

7.8.1.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Statistics > Personal Consumption Report, then select Export.

	1	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	T	
Data to Export	All (max 10000)	00 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	ОК	Cancel	

Figure 7-56 Export Personal Consumption Report

7.8.2 Department Summary

Click Consumption > Consumption Statistics then select Department Summary.

7.8.2.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Statistics > Department Summary, then select Export.

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	All (max 100000 records) Selected (max 100000 records) Start Position Total Records 100	
	OK Cancel	

Figure 7-57 Export Department summary

7.8.3 Restaurant Summary

Click **Consumption > Consumption Statistics** then select **Restaurant Summary**.

7.8.3.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Statistics > Restaurant Summary, then select Export.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL]	
Data to Export	All (max 100000 record)	ds)	
	Selected (max 10000)	records)	
	Start Position 1	records)	

Figure 7-58 Export Restaurant Summary

7.8.4 Device Summary

Click Consumption > Consumption Statistics then select Device Summary.

7.8.4.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Statistics > Device Summary, then select Export.

	Export	×	
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL -		
Data to Export	 All (max 100000 records) 		
	 Selected (max 100000 records) 		
	Start Position 1		
	Total Records 100		

Figure 7-59 Export Device Summary

7.8.5 Income and Expenses Report

Click Consumption > Consumption Statistics then select Income and Expense Report.

7.8.5.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > C	onsumption Statistics >	Income and Expenses Re	port, then select Export
-----------------------	-------------------------	------------------------	--------------------------

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL •	
Data to Export	All (max 100000 records)	
	Selected (max 100000 record	ds)
	Start Position 1	
	Start i Usidoni i	

Figure 7-60 Income and Expenses Report

7.8.6 Meal Summary

Click Consumption > Consumption Statistics then select Meal Summary.

7.8.6.1 Export

Click the **Export** button at the top of the list to open an export dialog box, as shown below. Click **OK** to export the data according to the query conditions and export conditions. The export format type can be selected as Excel, PDF, or CSV files.

Click Consumption > Consumption Statistics > Meal Summary, then select Export.

Encrypt or not	Export Ves No	×
File Format	EXCEL	
Data to Export	All (max 100000 records) Selected (max 100000 records) Start Position Total Records 100	
	OK Cancel	
	Figure 7-61 Export Meal Summary	

8 Elevator Control Management

8.1 Operation Scenario

Elevator control management, also known as elevator access control management, realizes the unified management of personnel entering and leaving the elevator through the configuration of floors and personnel authority groups.

Elevator control solves the elevator floor arrival authority of registered personnel, that is, in a certain period, on certain floors, authorized personnel can be verified and passed.

8.2 Operation Flow

Introduce the configuration process of Elevator control management business.

The business configuration process of Elevator control management business is shown in Figure 8-1

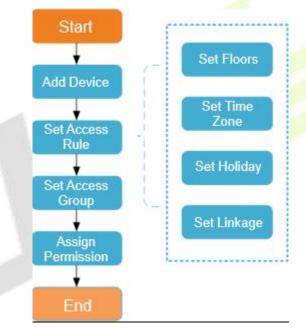


Figure 8-1 Elevator Control Configuration Flow

8.3 Elevator Device

There are two ways to add Elevator Devices.

8.3.1 Manually Add Elevator Control Device (Device)

This paper introduces the configuration Steps of adding Access Control device in platform.

Through the new way, the Elevator control device is added by TCP/IP communication. After filling in the corresponding information, Click **OK** to complete the addition, which is convenient to operate.

8.3.1.1 Add device (New)

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control device > device".

Step 2: In the device management interface, click the New button to pop up the New box.

Step 3: Fill in the corresponding parameter information in the new box. The new box of device is shown in the figures below. Please refer to below table for parameter setting instructions.

Step 4: Click OK to complete the operation of adding Elevator control device.

TCP/ IP communication mode

RS485 communication mode

Ne	ew	×	N	ew	>
Device Name [*] Communication Type [*] IP Address [*] Communication port [*] Communication Password Number of Expansion Board Each expansion board relay number	I ● TCP/IP ○ RS485 · · · 4370 0 16		Device Name [®] Communication Type [®] Serial Port Number [®] RS485 Address [®] RS485 Address Code Figure	ON KE	
Number of negative floors	0 Area Name		Baud Rate* Communication Password	38400 🔻	
Clear Data in the Device when Adding Accept a contract of the Device when A (except event record), please use		ce	Number of Expansion Board Each expansion board relay number Number of negative floors Area*	0 • • 16 • • • • • • • • • • • • • • • •	
			Clear Data in the Device when Adding (Clear Data in the Device when / (except event record), please us		vice
Save and New	OK Cancel		Save and New	OK Cancel]

Figure 8-2 Add Elevator Control Configuration Flow

Parameter	How to set
Device Name	Customize the name of this device
Communication Mode	Choose the communication mode of TCP/IP
IP Address	Fill in the IP address of Elevator control device
Communication Port	The default device communication port is 4370
Communication Cipher	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Plates	The Elevator control device can control the expansion of the number of floors
Number of Relays Per Expansion Board	Each expansion board has 16 relays
Region	The device is divided into regions, and the device can be filtered according to the regions during real-time monitoring

Parameter	How to set
Delete Data in Device When Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.

Table 8-2 Description of Settings for Adding Devices

8.3.1.2 Delete

Step 1: On the **Device** interface, select the required Device from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Device.

Step 3: Click Delete, to ensure and delete the selected Device from the list.

8.3.1.3 Export

You can export all transactions in Excel, PDF, CSV format.

Encrypt or not File Format	Ves No EXCEL	•	
Data to Export	 All (max 10000 Selected (max 	00 records) 100000 records)	
	Start Position Total Records	1	

Figure 8-3 Export Elevator Control Configuration Flow

8.3.1.4 Search And Add Elevator Control Device (Search)

This paper introduces the configuration Steps of adding Elevator control device in by searching.

Through the way of searching, the Elevator control device in the local area network is searched, and the Elevator control device that has been searched out is directly added, which is convenient to operate.

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control Device > Device".

Step 2: In the device management interface, click the Search button to pop up the search box.

Step 3: Click "**Start Search**" in the search box to display the Elevator control devices that can be added, as shown in Figure 8-4.

		Search	×
Search No de	evice found? Download Search Tools to	Decal Disk	
Total Progress	100%	No device found!	
IP Address	Device Type	Serial Number	
IP Address	MAC Address Subnet Mask	Gateway Add Serial Number Device Type S	Set Server Operations
7			
A The current system	communication port is 8088, please make		
		Close	

Figure 8-4 Device Search Add Interface

Step 4: Optional: Modify the IP address of Elevator control device and click "**Modify IP Address**". Modifying IP address will restart the device, and the IP address modification will be completed after restarting.

Step 5: For the Elevator control device searched, click the **Add** button in the operation bar to add the device; The device addition settings are shown in Figure 8-5, and the parameter settings are shown in Table 8-1.

Device Name*			
Communication Password			
Number of Expansion Board	0 🔻		
Each expansion board relay	16		
number			
Area*	Area Name 🔹 🔻		
Clear Data in the Device when Adding		1	
(Clear Data in the Device whe (except event record), please	en Adding] will delete data in the use with caution!	device	

Figure 8-5 Add Interface

Parameter	How to set
Device Name	Customize the name of the device.
Communication Cipher	Fill in the communication password of the device. If there is no password, it does not need to be filled in, and it can only be added after successful verification. For new factory device and initialized device, the communication password is empty. In order to ensure that the device is not used by others, the user can enter the IP address of the device through the Web page and enter the background to customize the verification password.
Number of Expansion Plates	Elevator control device can control the expansion of the number of floors.
Number of Relays Per Expansion Board	Each expansion board has 16 relays.
Region	The device is divided into regions, and the device can be filtered according to the regions during real-time monitoring.
Delete Data in Device When Adding	Set whether the original Elevator control event data in the device will be automatically emptied after the device is added.
L	Table 8-1 Device Search Added Settings Description

Step 6: Click **OK** to complete the operation of adding Elevator control device.

Step 7: Click **Close** to close the Device Search Add interface.

8.3.1.5 Control

Upgrade Firmware

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

∞ **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.

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.

• 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.

8.3.1.6 Set Up

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: Communication password shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password setting can improve the device's 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

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.

• Set extended Parameters

We can set the extended parameters of device like temperature detection and mask detection

8.3.1.7 View/Get

• 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.

Get Transactions

Get transactions from the device into the system. Two options are provided for this operation: Get New Transactions and Get All Transactions.

8.3.2 Expanding Board

This introduces the configuration Steps of adding Expanding Board device in the platform.

8.3.2.1 Add device (New)

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control device > Expanding Board".

Step 2: In the expanding board interface, click the **New** button to pop up the Newbox.

Step 3: Fill in the corresponding parameter information in the new box. The new box of device is shown in Figure 8-4. Please refer to Table 8-2 for parameter setting instructions.

Step 4: Click **OK** to complete the operation of adding Expanding board interface.

Device Name*	Click to select
Expansion board type*	EX-316 =
RS485 Address*	
	175

Figure 8-6 Add Expanding Board

8.3.2.2 Delete

Step 1: On the Expanding Board interface, select the required Device from the list.

Step 2: Click **Delete** or click on the ^{IIII} icon.to delete the selected Device.

Step 3: Click Delete, to ensure and delete the selected Device from the list.

8.3.3 Reader

Each elevator device has a reader, the reader information can be set.

Operating Steps:

Click Elevator Device > Reader, s	select a reader name in the reader list:
-----------------------------------	--

Perate Interval* 2 254) erification Mode* Card or Fingerprint ▼ he above Settings are ↓	Device <mark>Name*</mark>	192.168.1.53	
254) erification Mode* Card or Fingerprint ▼ he above Settings are ▼	Name*	192.168.1.53-Reader	
erification Mode* Card or Fingerprint he above Settings are	Operate Interval*	2	second(0-
he above Settings are		254)	
-	√erification Mode*	Card or Fingerprint	•
	The above Settin <mark>g</mark> s are		•
opied to	Copied to	1	
	spied to		

Figure 8-7 Edit Reader interface

Parameter	How to set
Device Name	It is not editable.
Name	The default format is "Device Name - Reader", editable in 30 characters.
Operate Interval	The interval between two veri <mark>fications.</mark> The default value is 2 seconds, the range is 0 to 254 seconds.
Verification Mode	The default setting is "Card or Fingerprint". The Wiegand reader supports" Only Card", "Only Password", "Card or Password", "Card and Password", "Card or Fingerprint". The RS485 reader supports "Card or Fingerprint". Make sure the reader has a keyboard when the verification mode is "Card and Password".
The above settings are copied to	Apply the above settings to all readers within the current user's level. Click OK to save and exit.

8.3.4 Floor Floor Setting

The setting of floor parameters affects the logical judgment of Elevator control verification.

8.3.4.1 Edit

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control device > Floor".

Step 2: In the floor management interface, click the **Edit** button in the floor selection operation bar to pop up the floor parameter setting box.

Step 3: In the floor parameter setting interface, fill in the corresponding parameters according to the addition requirements, as shown in Figure 8-5. Please refer to Table 8-3 for parameter filling instructions.

	Edit	
Device Name	192.168.1.53	
Floor Number	1	
Floor Name*	192.168.1.53-1	
Floor Active Time Zone*	24-Hour Accessible	•
Floor Passage Mode Time Zone		•
Button Open Duration*	5 (254)	second(0-
The above Settings are Copied to		•

Figure 8-8 Floor Parameter Setting

Parameter	How to set
Owned Device	Displays the basic in <mark>formation of t</mark> his floor <mark>, and res</mark> et is <mark>not</mark> supported.
Floor Number	The system automatically numbers the device according to the number of relays.
Floor Name	It defaults to "device Name-Flo <mark>or Nu</mark> mber", which can be repaired as needed, and can be filled in with a maximum of 30 arbitrary characters.
Effective Time Period of Floor	When editing a floor, the effective time period of the floor is required. Only after the effective time period of the floor is set can the close floor button be continuously released.
Time Period for Continuously Releasing Keys	It must be valid within the effective period of the floor. It is recommended to set the continuous release period of the floor. The setting is included in the effective period of the floor.
Key Holding Time	Used to control swiping cards or pressing fingerprints, within the range of time, you can press the floor buttons of elevators. The default is 5 seconds, and the range is 0-254.
Copy The Above Settings To	Set which floors the above floor parameters also apply to. The options are: all floors of current device and floors of all device.

Table 8-3 Instructions for Setting Floor Parameters

Step 4: Click OK to complete the operation of adding Elevator-controlled floors.

8.3.4.2 Remotely Release the Button

It determines whether the corresponding key to the selected floor can be pressed. You can customize the key release duration (15s by default) or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

8.3.4.3 Remotely Lock the Button:

This normal event is triggered if a user remotely locks a button successfully.

8.3.4.4 Remote Normal Opening

The person having open door permission punch effective card at the opened door to trigger this normal event.

8.3.4.5 Enable Intraday Passage Mode Timezone

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.

8.3.4.6 Disable Intraday Passage Mode Timezone

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.

8.3.5 Auxilary Input

It is mainly used to connect to devices, such as the infrared sensor or smog sensor.

8.3.5.1 Edit

Operating Steps:

Step 1: Click Elevator Device > Auxiliary Input on the Action Menu, enter into the following page.

Step 2: Click Edit to modify the parameters

Number*	192.168.214.66
Name*	Auxiliary Input-9
Printed Name*	IN9
Remark	

Figure 8-9 Auxiliary Input Add Interface

Parameter	How to set
Device Name	You can customize the name according to your preference.
Number	Displays the Number.
Name	It displays the default name of "Auxilary Input"
Printed Name	The printing name in the hardware, for example IN9.
Remark	Displays the Comment.

8.3.6 Event Type

Display the event types of the elevator devices.

Operating Steps

Step 1: Click **Elevator Device** > **Event Type**, the following page is displayed:

Event Name	Event No.	Event Level	Device Name	Serial No.
Normal Punch Open	0	Normal	192.168.90.235	0013130700074
Punch during Passage Mode Time Zone	1	Normal	192.168.90.235	0013130700074
Open during Passage Mode Time Zone	5	Normal	192.168.90.235	0013130700074
Remote Release	8	Normal	192.168.90 <mark>.</mark> 235	0013130700074
Remote Locking	9	Normal	192.168.90.235	0013130700074
Disable Intraday Passage Mode Time Zone	10	Normal	192.168.90.235	0013130700074
nable Intraday Passage Mode Time Zone	11	Normal	192.168.90.235	0013130700074
lormal Fingerprint Open	14	Normal	192.168.90.235	0013130700074
Press Fingerprint during Passage Mode Time	Zc 16	Normal	192.168.90.235	0013130700074
operate Interval too Short	20	Exception	192.168.90.235	0013130700074
Button Inactive Time Zone(Punch Card)	21	Exception	192.168.90.235	0013130700074
llegal Time Zone	22	Exception	192.168.90 <mark>.</mark> 235	0013130700074
access Denied	23	Exception	192.168.90.235	0013130700074
Disabled Card	27	Exception	192.168.90.235	0013130700074
Card Expired	29	Exception	192.168.90.235	0013130700074
assword Error	30	Exception	192.168.90.235	0013130700074
Press Fingerprint Interval too Short	31	Exception	192.168.90.235	0013130700074

Figure 8-10 Event Type Interface

8.3.7 Device Monitoring

8.3.7.1 Export

By default, it monitors all devices within the current user's level, click **Elevator Device** > **Device Monitoring**, and lists the operation information of devices: Device Name, Serial No., Area, Operation Status, current status, commands List, and Related Operation.

Area	Status		Device Name	Serial N	umber	\otimes	
Export							
Device Name	Serial Number	Area	Operation Status	Current Status	Commands List	Recently The Abnormal State	Operations
192.168.214.66	0013130700074	Area Nameaa	Get real-time event	Normal	0	None	Clear Command View Command

8.3.8 Real Time Monitoring

8.3.8.1 Operating Steps

Click **Elevator Device** > **Real-Time Monitoring**, real-time monitor the status and real-time events of elevator controllers in the system, including normal events and abnormal events (including alarm events).

rea	Dev	ice Name	Kernotely	Release the Button Remotely Lo	CK III E BUILOTI			
Time	Area Name	Device Name	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2017-02-10 16:11:12	Area Namea	192.168.214.66(00131	192.168.214.66-2	Remote Release				Other
017-02-10 16:11:12	Area Name:	192.168.214.66(00131	192.168.214.66-1	Remote Release				Other
017-02-10 16:11:01	Area Namea	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint
017-02-10 16:10:47	Area Namea	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint
017-02-10 16:10:44	Area Namea	192.168.214.66(00131	192.168.214.66-Rea	Disabled Card	2338484	2829(xinxiao yang	192.168.214.66-Read	Card or Fingerprint

Figure 8-12 Real Monitoring

8.3.8.2 Remotely Release the Button

Click Remotely Release Button:

Security Verification		×
User Password*		l
ок	Cancel	

Figure 8-13 Security Verification

Input the user password (the system logging password), click Next Step:

Remotely Release the Button	×
	*
∡	
192.168.1.53-1	
192.168.1.53-2	
192.168.1.53-3	
192.168.1.53-4	
192.168.1.53-5	
192.168.1.53-6	
192.168.1.53-7	
192.168.1.53-8	
192.168.1.53-9	
192.168.1.53-10	
192.168.1.53-11	
192.168.1.53-12	
	*
Previous Step Next Step Cancel	

Figure 8-14 Remotely Release Button

Select the floor, and click **Next Step**:

Remotely Release the Button Remote release: 5 second(1-254)	×
 Enable Intraday Passage Mode Time Zone 	
Sustained release button	
Previous Step Complete Cancel	

Figure 8-15 Remotely Release Button

8.3.8.3 Remotely Lock the Button

Same as "Remotely Release the button".

Remote Release:

It determines whether the corresponding key to the selected floor can be pressed. You can customize the key release duration (15s by default) or select Enable Intraday Passage Mode Time Zone. You can also directly set the current status of the floor to continuously release. In this case, the floor is not subject to restrictions of any periods, including Floor Active Time Zone, Floor Passage Mode Time Zone, and Button Open Duration. That is, the floor will be continuously released in 24 hours every day.

Enable Intraday Passage Mode Time Zone:

To close a floor, you must first set Disable Intraday Passage Mode Time Zone to prevent the case that the floor is opened because other continuous open periods take effect. Then, you need to set to close the Remote Lock Button.

Sustained Release Button:

The floor that is set to the continuously release state is not subject to restrictions of any periods, that is, the floor will be continuously released in 24 hours every day. To close the floor, you must select Disable Intraday Passage Mode Time Zone.

Solution Note: If a failure message is always returned for the remote release key, check whether there are too many currently disconnected devices on the device list. If yes, check the network connection.

Select the options, click **Complete** to finish enabling the button.

8.4 Elevator Control Rules

8.4.1 Time Period SettingTime Zones

In Elevator control, time period is a very important basic concept, which is used to set the use time of floors and specify that Elevator control can be used in effective time period.

This paper introduces the configuration Steps of manually adding time periods in.

8.4.1.1 New

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control Rules > Time Period".

Step 2: Click Add to pop up the interface of adding time period.

Step 3: Add the interface in the time period and set the corresponding content according to the new requirements, as shown in Figure 8-6. Please refer to Table 8-4 for parameter setting instructions.

Initial conday 00 : 00	0 : 00
uesday 00 : 00 <th< th=""><th>0 : 00</th></th<>	0 : 00
dnesday 00 : 00 <t< th=""><th></th></t<>	
ursday 00 : 00 00 : 00 00 : 00 00 00 00 00 00	0 : 00
	0 : 00
riday 00 : 00 00 : 00 00 00 00 00 00 00 00 00	0 : 00
aturday 00 : 00 00 : 00 00 00 00 00 00 00 00 00	0 : 00
unday 00 : 00 00 : 00 00 00 00 00 00 00 00 00	0 : 00
lay Type 1 00 : 00 00 : 00 00 : 00 00 00 00 00 00	0 : 00
lay Type 2 00 : 00 00 : 00 00 : 00 00 00 00 00 00	
	0 : 00
ay Type 3 00 : 00 00 : 00 00 : 00 00 00 00 00 00	
unday 00 : 00 00 : 00 00 : 00 00 : 00 00 : 00 00 ay Type 1 00 : 00 00 : 00 00 : 00 00 : 00 00 : 00 00 </td <td>0</td>	0

Figure 8-16 New Time Period

Parameter	How to set
Time Period Name	Custom setting time period name for easy memory.
Remarks	Custom Setting Notes Description.
Time Interval	Set the start and end time in each time interval. Time period includes one week and three holiday type time intervals.
Copy Monday time to other working days	You can quic <mark>kly co</mark> py Mon <mark>day s</mark> ettings to other workdays.
	(No. Description of The Lateral

Table 8-4 Description of New Parameter Settings in Time Interval

Step 4: Click **OK** to complete the addition of this time period.

8.4.1.2 Delete

Step 1: On the **Time Zone** interface, select the required time zone from the list.

Step 2: Click **Delete** or click on the \square icon.to delete the selected time zone.

Step 3: Click Delete, to ensure and delete the selected time zone from the list.

Pr	ompt
Are you sure you wa	int to perform the delete ration?
ohe	ration :

Figure 8-17 Delete Time Period

8.4.2 Holiday Setting

The Elevator control time on holidays may be different from the usual Elevator control time. For simple operation, the system supports setting the Elevator control time separately on holidays.

This paper introduces the configuration Steps of manually adding holidays in.

8.4.2.1 New

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control Rules > Holidays".

Step 2: Click **New** to pop up the holiday adding interface.

Step 3: In the holiday new interface, set the corresponding content according to the new requirements, as shown in Figure 8-7; Please refer to Table 8-5 for parameter setting instructions.

Holiday Name [*]		
Holiday Type*	Holiday Type 1 🔹	
Start Date*	2021-12-18	
End Date [*]	2021-12-18	a a
Recurring	No 🔻	
Remarks		1
		2

Figure 8-18 New Holidays

Parameter	How to set			
Holiday Name	Customize the holiday name for easy memory.			
Holiday Type Customize the holiday type: Holiday Type 1, Holiday Type 2, Holiday Type 1, Holiday Type 2, Holiday type is set and selected in the "Time Period" addition				
Start Time/End Time	Set the time range for this holiday.			
Annualized Cycle	Set whether this holiday cycle year by year: Yes, no. For example, if New Year's Day is January 1 of each year, it can be set to "Yes"; Mother's Day is the second Sunday in May every year. If the date is uncertain, it will be set to "No".			
Remarks	Custom settings description.			

Table 8-5 Parameter Setting Description for Holidays

Step 4: Click OK to complete the operation of Elevator-controlled holidays.

8.4.2.2 Delete

Step 1: On the Holidays interface, select the required holidays from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected holidays.

Step 3: Click Delete, to ensure and delete the selected holidays from the list.

8.4.3 Elevator Levels

Elevator levels indicate that one or several selected doors can be opened by verification of a combination of multi person within certain time zone. The combination of multi-person set in Personnel Access Level option.

8.4.3.1 New

Operating Steps:

Step 1: Click **Elevator** > **Access Levels** > **New** to enter the Add Levels editing interface.

Level Name*	l	
Time Zones*	24-Hour Accessible 🔻	
Area"	Area Name 👻	1.

Figure 8-19 Elevator Level Add Interface

Step 2: Set each parameter: Level Name (unrepeatable), Time Zone and Area.

Step 3: Click **OK**, the system prompts" Add floors to the current elevator control level immediately", click **OK** to add floors, click **Cancel** to return the elevator levels list. The added level is displayed in the list.

Floor Number Floor Name Floor Name 1 192 168 1.53-1 Image: Selected(0) 2 192 168 1.53-2 Image: Selected(0) 3 192 168 1.53-2 Image: Selected(0) 4 192 168 1.53-3 Image: Selected(0) 5 192 168 1.53-4 Image: Selected(0) 6 192 168 1.53-6 Image: Selected(0) 7 192 168 1.53-7 Image: Selected(0)			Prom	pt		
Floor Number Floor Name Image: Constraint of the current query conditions: None terrative Selected(0) Floor Number Floor Name 1 192 168.1.53-1 2 192 168.1.53-2 3 192 168.1.53-3 4 192 168.1.53-3 5 192 168.1.53-4 6 192 168.1.53-6 7 192 168.1.53-7 0 100 100 100 100 000				tely?	evel	
Floor Number Floor Name 1 192 168 1.53-1 2 192 168 1.53-2 3 192 168 1.53-3 4 192 168 1.53-4 5 192 168 1.53-6 6 192 168 1.53-6 7 192 168 1.53-7		Figure 8-20 Ele			face	
Floor Number Floor Name 1 192 168.1.53-1 2 192 168.1.53-2 3 192 168.1.53-3 4 192 168.1.53-4 5 192 168.1.53-6 6 192 168.1.53-7 7 192 168.1.53-7	loor Number	Floor Name		Q 🗇		
1 192 168 1.53-1 2 192 168 1.53-2 3 192 168 1.53-3 4 192 168 1.53-4 5 192 168 1.53-5 6 192 168 1.53-6 7 192 168 1.53-7		ons: None		Selected(0)		
2 192.168.1.53-2 3 192.168.1.53-3 4 192.168.1.53-4 5 192.168.1.53-5 6 192.168.1.53-6 7 192.168.1.53-7	Floor Number	Floor Name		Floor Number	Floor Name	
3 192,168,1.53-3 4 192,168,1.53-4 5 192,168,1.53-6 6 192,168,1.53-6 7 192,168,1.53-7			Î			
5 192.168.1.53-6 6 192.168.1.53-6 7 192.168.1.53-7	3	192.168.1.53-3				
5 192.168.1.53-5 6 192.168.1.53-6 7 192.168.1.53-7 6 192.168.1.53-7	⊒ 4	192.168.1.53-4	>			
6 192.168.1.53-6 7 192.168.1.53-7		192.168.1.53-5				
· · · ·	5		66			
		192.168.1.53-6				
	6					

Figure 8-21 Elevator Level Add Interface

EXNote: Different floors of different elevator controllers can be selected and added to an elevator level.

8.4.3.2 Delete

Step 1: On the Elevator Level interface, select the required level from the list.

Step 2: Click **Delete** or click on the ^{IIII} icon.to delete the selected level floors.

Step 3: Click Delete, to ensure and delete the selected level from the list.

8.4.4 Set Access by Levels

Operating Steps:

Step 1: Click Elevator > **Set by Levels** to enter the edit interface, Click an Elevator level in left list, personnel having right of opening door in this access level will display on right list.

Step 2: In the left list, click **Add Personnel** under Operations to pop-up the Add Personnel box; select personnel (multiple) and click is to move it to the right selected list, then click **OK** to save and complete.

Step 3: Click the level to view the personnel in the right list. Select personnel and click **Delete Personnel** above the right list, then Click **OK** to delete.

8.4.4.1 Delete Personnel

Step 1: On the Access Level interface, select the required Personnel ID from the list.

Step 2: Click **Delete** or click on the <u>selected</u> Personnel ID.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

8.4.5 Set Access by Person

Add selected personnel to selected elevator levels or delete selected personnel from the elevator levels.

Operating Steps:

Step 1: Click **Elevator** > **Elevator Levels** > **Set by Person**, click employee to view the levels in the right list.

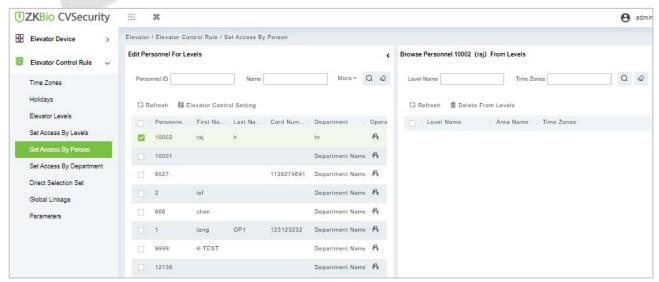


Figure 8-22 Set Access by Person Interface

8.4.5.1 Delete from Levels

Step 1: Select Level (multiple) in the right list and click **Delete from levels** above the list, then click **OK** to delete the selected levels.

8.4.5.2 Elevator Control Setting

Setting Levels for Selected Personnel:

Step 1: Select a person in the list on the left and click **Elevator Control Setting**. The following page is displayed:

Superuser	No	~
Set Valid Time		

Figure 8-23 Elevator Control Setting

Step 2: In the left list, click **Add Personnel** under Operations to pop-up the Add Personnel box; select personnel (multiple) and click to move it to the right selected list, then click **OK** to save and complete.

8.4.6 Set Access by Department

Operating Steps:

Step 1: Add selected department to selected elevator levels or delete selected department from the elevator levels. The access of the staff in the department will be changed.

dit De	fault Levels For Dep	partment			<	Browse Department 1 (D)epartment Name)Def	ault Levels		
Depa	rtment Number	Depa	tment Name	Q	Q	Level Name	Time Zo	nes	Q	Q
OR	lefresh					🔾 Refresh 🗴 🛍 Dele	te From Default Level	5		
	Department N	Department Name	Parent Departm	Operations		Level Name	Area Name	Time Zones		
	1	Department Name		8						
	2	Development		8						
	3	hr		8						
	9	test9		8						
	8	test8	test9	8						

Figure 8-24 Set Access by Department Interface

8.4.6.1 Delete from Default Levels

Select Level (multiple) in the right list and click **Delete from levels** above the list, then click **OK** to delete the selected levels.

8.4.7 Direct Selection Set

8.4.8 Linkage Setting Global Linkage

The use method and scene of linkage are very flexible. After a specific event is triggered at an input point in the Elevator control system, a linkage action will be generated at the designated output point to control the events such as door opening, alarm and abnormality in the system.

8.4.8.1 New

Operating Steps:

Step 1: In the Elevator Control module, select "Elevator Control Rules > Global Linkage".

Step 2: In the linkage setting interface, select and click the **Add** button, as shown in Figure 8-9, and refer to Table 8-6 for linkage parameter setting.

	New			×
Linkage Name*	Ap Ap	ply to all personnel		
Linkage Trigger Conditions* Add		out Point* Add		
Output Point Video Li	nkage Active Time	e E-mai	I Linkage Voice Prom	ints 🕨
Floor Add				pto
Action type* Close	▼			
	▼			

Figure 8-25 New Linkage Configuration Interface

Parameter	How to set
Linkage Name	Custom setting linkage name for easy reference
LinkageTrigger Condition	Select the condition that the linkage operation triggers, that is, the type of event generated by the selected device
Input Point	Select the input point to set the device input

Output Point	Select the output point to set the output of the device
Linkage Action Setting	Select and set linkage action, including device operation at output point, video linkage and mail

Table 8-6 New Linkage Parameter Setting Description

Step 5: Click **OK** to complete the linkage configuration.

8.4.8.2 Delete

Step 1: On the Elevator interface, select the required linkage from the list.

Step 2: Click **Delete** or click on the ¹/₁ icon.to delete the selected linkage.

Step 3: Click **Delete**, to ensure and delete the selected linkage from the list.

8.4.8.3 Enable/Disable

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.

8.4.8.4 Delete Personnel

Step 1: On the **Elevator** interface, select the required Personnel ID of the Global Linkage from the list.

Step 2: Click **Delete** or click on the icon.to delete the selected Personnel ID.

Step 3: Click Delete, to ensure and delete the selected Personnel ID from the list.

8.4.9 Parameters

Operating Steps:

Step 1: Click Elevator > Elevator > Parameters:

pe of Gettin	g Transaction	IS							Type of Getting Transaction
	5								Real Time Monitoring
	O Period	ically							
	Interval								
	Interval								
	1					- hour(s	i)		
	Set the	Time for Obt	aining New Tra	insactions	Select All	Cancel			
	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	
	A Getting	transactions a	and synchroniz	ation time will	be done at the	e same time.			
eal Time Mor	nitoring								
	The Real Ti	me Monitoring	Page Pop-up	Photo Size N	/lax Height				
	140					ox(80	- 500)		

Figure 8-26 Parameters Interface

Parameter	How to set
Type of Getting Transaction	Start from the setting and efficient time, the system attempts to download new transactions every time interval.

Real Time	When an access control event occurs, the personnel photo will pop up, set the size of
Monitoring	the pop-up photos, the range is 80-500px.

Table 8-7 Parameter Setting Description

8.5 Elevator Control Reports

8.5.1 All Transaction

Because the data size of elevator access control event records is large, you can view elevator access control events as specified condition when querying. By default, the system displays the latest three months transactions.

8.5.1.1 Clear All Data

Operating Steps:

Step 1: Click **Reports** > **All Transactions** to view all transactions:

Time From 2015-0	2-26 00:00:00	To 2015-05-26 2	23.59.59 Personnel ID		Device I	lame	0	More~ Q	8		
The current menu co	editions: Time E	am (2015.02.26.00.00.0	00) To:(2015-05-26 23:59:59)						~		
			00) 10.(2010-00-20 23.09.09)								
C Refresh	Clear All Data	Export									
Time	Device	Event Point	Event Description	Media File	Personnel ID	First Name	LastName	Card Number	Department		Verification Mode
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-1	Trigger global linkage	S (0)	11	jolly	wei	3406918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3405918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 17:01:00	192.168.60.53	192.168.60.53-2	Trigger global linkage	•	11	jolty	wei	3406918	General	192.168.60.53-Rr C	ard or Pass
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Normal Punch Open		11	jolly	wei	3406918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-1	Trigger global linkage	•	11	jolly	wei	3406918	General	192.168.60.53-Ri C	ard or Passi
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Normal Punch Open		11	jolly	wei	3405918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 17:00:49	192.168.60.53	192.168.60.53-2	Trigger global linkage	•	11	jolly	wei	3406918	General	192.168.60.53-Ri C	ard or Pass
2015-05-22 16:58:26	192.168.60.53	192 168 60 53-2	Normal Punch Open		11	jolly	wei	3405918	General	192.168.60.53-R/ C	ard or Passi

Figure 8-27 All Transaction Interface

Step 2: Click Clear All Data to pop up prompt and click OK to clear all transactions.

8.5.1.2 Export

Step 1: You can export all transactions in Excel, PDF, CSV format.

Time: 2017-09-18 0	0 : 00 : 00 - 2017-12	18 23 - 69 - 59				All Transactions						
Time	Device	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department	Reader Name	Verification Mode	Area	Remark
2017-12-15 10:35 43	192.168.218.65	192.168.218.65-8	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 43	192.168.218.65	192.168.218.65-5	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.66- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 43	192.168.218.65	192.168.218.65-9	Normal Punch Open	3	Leo	Hou	13260079	General	192.168.218.66- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 39	192.168.218.65	192.168.218.65-1	Normal Punch Open	- 1	Jerry	Wang	9505930	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	í.
2017-12-16 10:35: 39	192.168.218.65	192.108.218.65-4	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35	192.168.218.65	192.168.218.65-3	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35	192.168.218.65	192.168.218.65-2	Normal Punch Open	1	Jerry	Wang	9505930	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-16 10:35: 36	192.168.218.65	192.168.218.65-8	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 36	192.168.218.65	192.168.218.65-10	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35 36	192.168.218.65	192.168.218.65-9	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 38	192.168.218.65	192.168.218.65-7	Normal Punch Open	2	Lucky	Tan	13271770	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35	192.168.218.65	192.108.218.05-0	Normal Punch Öpen	2940	Sherry	Yang	4461253	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 31	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4481253	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35: 31	192.168.218.65	192.168.218.65-7	Normal Punch Open	2940	Sherry	Yang	4481253	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:35 31	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4481253	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-15 10:32: 51	192.168.218.65	192.168.218.65-5	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.188.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-16 10:32	192.168.218.65	192.168.218.65-8	Normal Punch Open	2940	Sherry	Yang	4461253	General	192.168.218.65- Reader	Card or Fingerprint	Area Name	
2017-12-16 10:32:	192.168.218.65	192.168.218.65-6	Normal Punch	2940	Sherry	Yang	4461253	General	192.168.218.65-	Card or Fingerprint	Area Name	

Figure 8-28 All Transaction Export Interface

8.5.2 All Exception Events

8.5.2.1 Clear All Data

Operating Steps:

Step 1: Click **Reports** > **All Exception Events** to view exception events in specified condition. The options are same as those of **All Transactions**.

2022-041	22 00:00:00 To 2022-07-	22 23:59:55 Personn	el ID	Device Name	More - Q	Q					
Refresh 🔋 🤅	Clear All Data 🛛 🛧 Exp	port									
me	Device Name	Event Point	Floor	Event Description	Personnel ID First Name	Last Name	Card Number	Department	Reader Na	Verification	Are

Figure 8-29 All Exception Events Interface

Step 2: Click Clear All Data to pop up prompt, click OK to clear all exception events.

8.5.2.2 Export

Step 1: You can export all exception events in Excel, PDF, CSV format.

Time	Area	Device	Event Point	Event Description	Card Number	Personnel ID	First Name	Last Name	Department	Reader Name	Venfication Mode	Remark
2017-12-15 10:29	Area Name	192.169.218.65	192.168.218.65- Reader	Disabled Card	9505930	1	Jerry	Wang	General	102.188.218.65- Reader	Card or Fingerprint	
2017-12-15 10:29:	Area Name	192.168.218.65	192.168.218.65- Reader	Disabled Card	4481253	2940	Sherry	Yang	Oenaral	192.168.218.65- Reader	Card or Fingerprint	
2017-12-15 10:29:	Area Name	192.168.218.65	192.168.218.65- Reader	Disabled Card	13260079	3	Leo	Hou	General	192.168.218.65- Reader	Card or Fingerprint	
2017-12-15 10:29	Area Name	192.169.219.65	192.168.218.65- Reader	Operate Interval too Short	13260079	3	Leo	Hou	General	192.168.218.65- Reader	Card or Fingerprint	

Figure 8-30 All Exception Events Export Interface

8.5.3 Access Rights by Floor

Operating Steps:

Step 1: Click **Reports** > **Access Rights by Floor**, the data list in the left side shows all floors in the system, select a floor, the personnel having access levels to the floor will display on the right data list.

Access Rights By Fle	Dor		Browse 192 168 214 66-1(1) Opening Personnel			
Floor Name	Device Name	Q Q	C Refresh	Export		
The current query cor	uditions: None		Personnel ID	FirstName	LastName	Department
C- Retresh			2952			General
Floor Name	Floor Number	Owned Device				
192.168.214.66-1	1	192.168.214.66				
192 168 214 66-2	2	192.168.214.66				
192.168.214.66-3	3	192 168 214 66				

Figure 8-31 Access Right by Floor Interface

8.5.3.1 Export

Step 1: You can export all the personnel having access levels to the floor data in Excel, PDF, CSV format

) Opening Personnel	
Personnel ID	First Name	Last Name	Department
2940	Sherry	Yang	Hotel
1	Jerry	Wang	General
2	Lucky	Tan	Development Department
3	Leo	Hou	Financial Department
5	5 Necol		Marketing Department
6	Amber	Lin	Financial Department
8	Glori	Liu	Marketing Department
9	Lilian	Mei	Developmen Department

Figure 8-32 Access Right By Floor AExport Interface

8.5.4 Access Rights by Personnel

Operating Steps:

Step 1: Click **Reports** > **Access Rights by Personnel**, the data list in the left side shows all doors in the system, select personnel, the personnel having access levels to the door will display on the right data list.

Elevator / Elevator C	Control Reports / Acc	ess Rights By Perso	nnel		
Access Rights By P	ersonnel			٢	Floor
Personnel ID	Name	More *	Q @		⊖ Refresh 1 Export
					Floor Number Floor Name
O Refresh					
Personnel ID	First Name	Last Name	Depart		
9999	K-TEST		Departme		
12135			Departme		



8.5.4.1 Export

Step 1: You can export all the floor information in Excel, PDF, CSV format.

Floor Number	Floor Name
1	192.168.218.65-1
2	192.168.218.65-2
3	192.168.218.65-3
4	192.168.218.65-4
5	192.168.218.65-5
6	192.168.218.65-6
7	192.168.218.65-7
8	192.168.218.65-8
9	192.168.218.65-9
10	192.168.218.65-10

Figure 8-34 Access Right by Personnel Export Interface

8.5.5 First In and Last Out

Click Elevator Controls Reports > First In And Last Out to view the First and the Last time interval.

8.5.5.1 Clear All Data

Click **Clear All Data** to pop up prompt and click **OK** to clear all transactions.

8.5.5.2 Export

You can export all transactions in Excel, PDF, CSV format.



9 Parking Management

9.1 Operation Scenario

In modern parking lot management, vehicle management is an important aspect, especially for special parking lots, parks and communities, it is required to strictly manage all kinds of vehicles in real time, strictly monitor their entry and exit time, and register and identify all kinds of vehicles (including internal vehicles and external vehicles). In a large-scale field, there are many vehicles coming in and out. For example, every vehicle must be judged manually, which is time-consuming and not conducive to management and inquiry, and the security work is difficult and inefficient. In order to improve this management mode, which is not commensurate with modern parking lots, residential areas, etc., It is necessary to realize the automatization and intelligence of vehicle management as soon as possible, and manage it in the form of computer network, so as to monitor and manage all the vehicles at the entrance and exit effectively and accurately. It is required that the system provide corresponding application software to realize the high efficiency and intelligence of parking lot management.

9.2 Operation Flow

This paper introduces the configuration process of parking management business. The parking management business configuration process is shown in Figure 9-1.

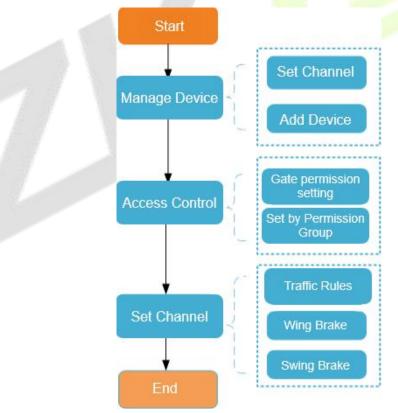


Figure 9-1 Parking Configuration Flow

9.3 Basic Parking Setting

9.3.1 Parking Settings

This paper introduces the public parameters of the parking lot under.

Operating Steps:

Step 1: In the Parking module", select "Parking Basic Management > Parking Settings".

Step 2: In the Parking setting interface, as shown in Figure 9-1, fill in relevant parameters. Please refer to Table 9-2 for parameters.

ZKBio CVSecurity	*	😝 admin 🗸
Parking / Basic parking manageme	ant / Parking Lot Settings	
D Parking : 9	Setting Cempany Name Cempany Name Cempany Company Cempany Company Cempany Company Cempany Company Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempany Cempa	Parking Setting Channel Entrance and Edit S Charge Management Seting Flord Venicle Setting Voice and district settings Other Settings Offline Settings
Channel	Entrance and Exit Setting	
	C Enable Fixed Vehicle Multiple in and Out	
	Enable Temporary Vehicle Multiple In and Out	,

Figure 9-1 Parking Parameter Setting Interface

Parameter	Specific Parameters	Parameter Description
	Company Name	You can customize the Parking company name, which can be displayed in the billing receipt.
Parking Setting	Parking Mode	 One car per person: means that only one fixed car can be authorized in one parking space at present. Multiple cars per person refers to a parking space that allows multiple fixed cars to be authorized.
	Display Parking Space Number	You can choose whether to display the parking space number or not, and you can specify a certain parking space number.
	Enable the. fixed or temporary vechicles are multiple In and out.	Allow the fixed or Temporary vechicles to the parking area and vechicle are multiple in and out.
Channel Entrance and	Matching Precision of Entrance and Exit	Vechicles are allowed by exact match and 5 or 6digits registration numbers to the entrance and exit area of the parking.
Exit Setting	Special license plate contains characters	Enter the special license plates contains characters wherever required.
	Duplicate license plate waiting time	In Duplicate license plate waiting time Mention the timings of single channel mode and normal mode

Parameter	Specific Parameters	Parameter Description
	Enable the fixed car charging standard	If the fixed car charging standard has been set in advance, check this setting, and when the fixed car is authorized and postponed, it will be implemented according to this charging standard; If it is not checked, you can only manually enter the extension time and amount.
	Print the charge receipt	If the receipt printer is set and connected, the corresponding receipt will be printed when the charge is successful.
ChargeEnable consumptionEnableManagementdiscountsEnableSettingsOutputOutput	Set the "Discount Strategy" in advance and then check the Enable Consumption Discount System, and the consumption discount will be carried out.	
Settings	Unmatched processing mode	There are two existing ways to deal with mismatches: "free release" and "opening the gate after charging fees"; Manual release is to open the gate directly, and when the gate is opened after charging, a charge confirmation box will pop up during manual release (only for temporary vehicles).
	Synchronize data to the cloud	After opening, offline parking data will be uploaded to the cloud platform synchronously.
Enable online payment Enable the payment method under the scenarion and WeChat payment.	Enable the payment method under the scenario of Alipay and WeChat payment.	
	Statistic parking space of fixed car	 If it is checked, the number of cars will not be deducted after authorization, and the number of cars will be counted in real time when vehicles enter and leave the field. If it is not checked, the number of fixed cars will be deducted after authorization.
Fixed Vehicle Setting	Enable fixed vehicles to switch to temporary vehicles	 If this option is checked, the fixed car will be automatically converted into a temporary car after it expires, and the charge will be made according to the temporary charging method. If it is not checked, this option will require manual release for the fixed car to come out when it expires.
	Warning days for fixed vehicles	If the warning days are set to 5 days, it is necessary to prompt the vehicles to postpone the fixed vehicles when entering and leaving the field within 5 days.
	Enable external display	Checking this parameter will display the relevant parking data on the external display.
Voice And	The entrance shows the remaining parking spaces	Display the remaining parking spaces at the entrance of the parking lot.
Display Settings	lay Statistics of car Parking The statistics of the number of cars in the cor	The statistics of the number of cars in the corresponding booth in the big Parking area include the number of cars in the small Parking area.
	Vehicle entry and exit broadcast license plate	If this parameter is checked, the license plate will be broadcast when the vehicle enters and exits.
	Display color	Set the display color of parking machine.

Parameter	Specific Parameters	Parameter Description
	Maximum vehicle stay time	Set the maximum stay time of on-site vehicles. If the on-site vehicles have not left after this time, the records of on-site vehicles will be displayed in the "On-site Stay Timeout Vehicles" report.
Other Settings	Save days of snapshot photos	Set snapshot photos saved more than the set number of days photos will be automatically deleted, if you do not want to delete snapshot photos will change the parameter set to 0 days.
	Snapshot Save Path	You can customize the path where photos are saved.

Table 9-2 Description of Parking Parameters

Step 3: After setting the parameters, Click **OK**.

9.3.2 Device

For 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.

9.3.2.1 Edit or Delete a Device

Step 1: Click Device Name or click **Edit** to access the edit interface.

Step 2: Select device, click Delete, and click OK to delete the device

9.3.2.2 Reboot Device

It will reboot the selected device.

9.3.2.3 Synchronize Time

It will synchronize time with server's current time.

9.3.2.4 Get Device Parameters

Click Get Device Parameters Users can get device parameters which is they need from the system.

9.3.2.5 Delete Device command

Click DeleteDevice command, to delete the selected device command' data.

9.3.2.6 Get Device Version

Click Device version to get selected device version.

9.3.3 Parking Area

This paper introduces the Step configuration of and Parking area.

9.3.3.1 Add New

Operating Steps:

Step 1: In the Parking module, select Parking Basic Management > Parking Area.

Step 2: In the **Parking Area** interface, click **Add New** and fill in the relevant parameters, as shown in Figure 9-3. Please refer to Table 9-4 for parameter description.

	New	×
Area type of car yard*	Large Car Area 🔹]
Parking Area Name*	I]
Parking Spaces*		
Remarks		

Figure 9-3 New Interface in Parking Area

Set whether the current Parking area is a big Parking or a small Parking.
The name of the Parking area cannot be duplicated.
Set total number of parking spaces in this area.
Text description.

Table 9-4 Parameter Description of Parking Area

Step 3: Click OK to complete the setting of the Parking area.

9.3.3.2 Edit

Click a parking area name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

9.3.3.3 Delete

Select one or more parking areas and click **Delete** at the upper part of the list and click **OK** to delete the selected parking areas. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single parking area.

9.3.3.4 Refresh

Click **Refresh** at the upper part of the list to load new parking areas.

9.3.4 Entrance And Exit Area

This paper introduces the Step configuration of parking entrance and exit area.

9.3.4.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Basic Management > Entrance and Exit Area".

Step2: In the interface of Entrance and Exit Area, click **Add New** and fill in relevant parameters, as shown in Figure 9-5. Please refer to Table 9-6 for parameter description.

Ne	2W	×
Yard Area [*] Import and Export Area Name [*]		
ОК	Cancel	

Figure 9-5 Add Interface of Entrance and Exit Area

Parameter	Description
Parking Area	The name of Entran <mark>ce and</mark> Exit Ar <mark>ea cannot b</mark> e duplicated.
Name Of Entrance and Exit Area	The Parking area to which the Entrance and Exit Area belongs.

Table 9-6 Description of Parameters of Entrance and Exit Area

Step 3: Click **OK** to complete the setting of Entrance and Exit Area.

9.3.4.2 Edit

Click an entrance and exit area name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

9.3.4.3 Delete

Select one or more entrance and exit areas and click **Delete** at the upper part of the list and click **OK** to delete the selected entrance and exit areas. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single entrance and exit area.

9.3.4.4 Refresh

Click **Refresh** at the upper part of the list to load new entrance and exit areas.

9.3.5 Guard Booth

This paper introduces the Step configuration of ZKBio CVSecurity Guard Booth. After the configuration is completed, you can check and monitor the Guard Booth interface and operate the gate opening.

9.3.5.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Basic Management > Guard Booth".

Step 2: In the **Guard Booth** interface, click **Add New** and fill in the relevant parameters, as shown in Figure 9-7. Please refer to Table 9-8 for parameter description.

	New	V		×	
Guard Booth Name [*] Channel Entrance and Exit Name [*] Booth Parameters	<u> </u>	Computer IP Address* Yard Area*	192 . 168 . 5 . 208		
Temporary Vehicle Free* Enable Replacement of Vehicle* Temporary Vehicle Fast Exit*	Yes Yes Yes	Enable Manual Release* One Channel Mode*	Yes No		
	ОК	Cancel			

Figure 9-7 Added Guard Booth Interface

Parameter	Description	
Falameter	Description	
Name of Guard Booth	Set the name of the booth.	
Guard Booth Computer IP	When the booth mode is browser, the IP address of the booth needs to be set.	
Guard Booth Mode	 There are two modes of Guard Booth: Browser: You need to set the IP of the booth computer Platform: Automatically generate platform registration code 	
Platform Registration Code	When the booth mode is a platform, it is automatically generated for CS booth registration.	
Name Of Entrance and Exit Area	Entrance and Exit Area to which the booth belongs.	
Parking Area	After selecting the Entrance and Exit Area, the information of the parking lot area will be read, which is read-only.	
Allow Temporary Cars Free of Charge	Set whether the temporary car is free or not, check the interface of opening the billing result of the temporary car, and there will be a "Free" button to allow the temporary car to be free.	
Enable Replacement Models	Set whether the replacement vehicle is enabled or not and check the temporary vehicle charging result interface to change the temporary vehicle type of the vehicle. Different vehicle types have different charging standards, so the charging result will also change.	
Enable Manual Clearance	Set whether to enable manual release. After checking Enable, you can manually control the gate to open for vehicle release.	

Parameter	Description
Temporary Cars Come Out Quickly	Set whether to enable the temporary car to come out quickly. If the temporary car does not incur parking fees after checking the enable, the billing result confirmation interface will not pop up, and the gate will be opened and released directly.
Single Channel Mode	Set whether to enable the single channel mode. After checking Enable, the previous channel of the current scene application can be used for both entry and exit. However, in terms of logical settings, it is recommended to establish different logical channels to bind different IPC devices.

Table 9-8 Parameter Description of Guard Booth

9.3.5.2 Edit

Click a guard booth name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

9.3.5.3 Delete

Select one or more guard booths and click **Delete** at the upper part of the list and click **OK** to delete the selected guard booths. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single guard booth.

9.3.5.4 Refresh

Click **Refresh** at the upper part of the list to load new guard booths.

9.3.6 Channel

This paper introduces the configuration of relevant Steps of parking passage.

9.3.6.1 Add New

Operating Steps:

Step 1: In the Parking module, select Parking Basic Management > Passage.

Step 2: Click **Add New** in the channel interface and fill in the relevant parameters, as shown in Figure 9-9. Please refer to Table 9-10 for parameter description.

IPC1 IP*	hannel Status* ideo Preview indow(IPC1)*
Fixed Vehicle Open Type* Direct Pass Te	ideo Preview //indow(IPC2) emporary Vehicle Open Confirm Pass //pe*
Limit Line Mode Forbids Vehicle Type Small Vehicle A Small Vehicle B Temporary Small Vehicle A	Medium Vehicle

Figure 9-9 New Channel Interface

Parameter	Description
Channel Name	You can customize the channel name here
Name of Guard Booth	Select the corresponding booth
Import And Export Status	Select the channel properties of the entrance and exit of the corresponding booth entrance and exit area
IPC1_IP/IPC1 Corresponds to Video Port Position	The ip address of device 1, and the corresponding video port position is the monitoring position where the device is located
IPC2_IP/IPC2 Corresponds to Video Port Position	The ip address of device 2, and the corresponding video port position is the monitoring position where the device is located
Opening Mode of Fixed Car	Direct release (open the gate directly after identifying the license plate) Confirm the release (pop up the confirmation box and click the button manually to open the gate)
Temporary Vehicle Opening Mode	Pick up and release (open the gate directly after identifying the license plate) Confirm the release (pop up the confirmation box and click the button manually to open the gate)
Type of Vehicles Prohibited from Passing in Limited Mode	You can set those car types not to pass here, and you can choose multiple

Table 9-10 Description of Channel Parameters

Step 3: Click **OK** to complete the channel setting.

9.3.6.2 Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.3.6.3 Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single channel.

9.3.6.4 Refresh

Click **Refresh** at the upper part of the list to load new channels.

9.3.7 Vechicle Definition

This paper introduces the configuration of related Steps of vechicle definition.

9.3.7.1 Add New

Operating Steps:

Step 1: In the Parking module, select Parking Basic Management > Vehicle Definition.

Step 2: Click **Add New** in the vechicle definition interface and fill in the relevant parameters, as shown in Figure 9-11. Please refer to Table 9-12 for parameter description.

New	×	
Fixed Vehicle 🔹		
I		
Enable 👻		
Cancel		
	Fixed Vehicle I Enable	Fixed Vehicle

Figure 9-11 New vechicle definition

Parameter	Description	
Vehicle Definition	Select the corresponding. vechicle	
Vehicle Type	Vehicle type of the charging standard	
Status	Select the vechicle status enable or disable	
Remarks	Text description	

Table 9-12 Description of vechicle definition Parameters

9.3.7.2 Editing the Vehicle Type

Step 1: Click a vehicle type name or Edit in the operation column. The Edit page is displayed.

	Edit	×
Vehicle Definition	Fixed Vehicle	
Vehicle Type*	Fixed Vehicle A	
Status*	Enable	•
Remark		
OF	Cancel	

Figure 9-13 Edit Vechicle Type

Step 2: Set Vehicle Type, select a Status, and enter the vehicle type description in Remark.

Step 3: Click OK to save and exit.

9.3.7.3 Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a vechicle definition.

9.3.7.4 Refresh

Click **Refresh** at the upper part of the list to load new vechicle definitions.

9.3.8 Shift Settings

This paper introduces the configuration of related Steps of parking shift.

9.3.8.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Basic Management > Shift Setting".

Step 2: In the Shift Setting interface, click Add Newto fill in relevant parameters, as shown in

Figure 9-14. Please refer to Table 9-15 for parameter description.

	New	×
Shift Name [*] Guard Booth Name [*] Start Time [*] End Time [*]	00 : 00 : 00 00 : 00 : 00 Cross Day	
OK	Cancel	

Figure 9-14 New Shift Interface

Parameter	Description	
Shift name	Distinguish the difference between shifts by setting the device name	
Name of Guard Booth	Distinguish the differences between booths by setting device names	
Start time	Select the time when the shift starts	
End time	Select the time when the shift ends	
Across the sky	Is the shift time set across days	

Table 9-15 Shift Parameter Description

Step 3: Click **OK** to complete the setting of adding shift settings.

9.3.8.2 Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.3.8.3 Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a shift setting.

9.3.8.4 Refresh

Click **Refresh** at the upper part of the list to load new shift settings.

9.3.9 Manual Release Reason

A manual release reason must be selected when the manual release function is used on the online monitoring page.

9.3.9.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Basic Management > Manual Release Reason

Step 2: In the **Manual Release Reason** interface, click **Add New**to fill in relevant parameters, as shown in Figure 9-16. Please refer to Table 9-17 for parameter description.

	New	
Manual Release Reason* Remarks		
ОК	Cancel	

Figure 9-16 New Manual Release Reason Interface

Parameter	Description
Shift Name	Distinguish the difference between shifts by setting the device name
Name Of Guard Booth	Distinguish the differences between booths by setting device names
Start Time	Select the time when the shift starts
End Time	Select the time when the shift ends
Across the Sky	Is the shift time set across days

Table 9-17 for Manual Release Reason parameter description

9.3.9.2 Edit

Click a channel name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.3.9.3 Delete

Select one or more channels and click **Delete** at the upper part of the list and click **OK** to delete the selected channels. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a manual release reason.

9.3.9.4 Refresh

Click **Refresh** at the upper part of the list to load new Manual Release Reason.

9.4 Charge Management

This paper introduces the related configuration of parking charge management, mainly setting the charging rules of various car types in the parking lot and the discount strategy of merchants.

9.4.1 Fixed Cars Are Charging Rules

This paper introduces the operation Steps of periodic charging rules for fixed cars in.

9.4.1.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Charge Management > Fixed Car Charge Rules"

Step 2: In the fixed car charging rules interface, click **Add New** and fill in the corresponding parameters, as shown in Figure 9-18. Please refer to Table 9-19 for parameter description.

Fixed Charge Name*		
Vehicle Type*	-	
Cycle Type*	Monthly -	
Cycle*		
Charge Amount *		
OK	Cancel	

Figure 9-18 Fixed Car Charge Rules Interface

Parameter	Description
Name of Fixed Car Charge	Set the name of the charging standard for fixed cars, which cannot be repeated.
Car Type	Select the car type corresponding to the fixed car charging standard, and each car type can only be set once.
Periodic Type	Fixed car charging cycle type, monthly/daily.
Period	Set the cycle time, that is, the effective time of the fixed car.
Amount	Set the amount charged.

Table 9-19 Parameter Description of Fixed Car Charging Rules

9.4.1.2 Edit

Click a fixed charge name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.4.1.3 Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single fixed vehicle charge.

9.4.1.4 Refresh

Click **Refresh** at the upper part of the list to load new fixed vehicle charge.

9.4.2 Temporary Car Charging Rules

This paper introduces the Step configuration of temporary car charging rules in.

9.4.2.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Charge Management > Temporary Car Charge Rules".

Step 2: In the Temporary Car Charge Rules interface, click **Add New.** and fill in the corresponding parameters, as shown in Figure 9-20. Please refer to Table 9-21 for parameter description.

	New	
Temporary Vehicle Charging Rules		Test Charging Rule:
Name [*] Vehicle Type [*] Daily Highest Amount		Vehicle Type In Time* Out Time*
Free Minutes*	0 minutes	Save and test
Cross Time Split	nse plate in Circulation within 24 Multiple access with the highest fees	Amount Receivable:
Detail (Accord	ding to time period O According to cycle	0.0
Time Period1	+	•
Time Period*	00 : 00 🔹 to 00 : 00 🐨 🗌 Cross Day	
Charge by Times		
Maximum Charge*	ОК Сапс	

Figure 9-20 Temporary Car Charge Rules Interface

Parameter	Description
Name of Temporary Car Charging Rules	Set the name of temporary car charging rule, which cannot be duplicated.
Car Type	Select the vehicle type corresponding to the charging standard.
Maximum Amount for The Whole Day	The maximum charge within one day (for example, 10 yuan per hour, 240 yuan for a full day; If the maximum charge amount for the whole day is set to 100 yuan, just charge 100 yuan).

Parameter	Description
Free Minutes	There is no charge for parking time within this value range.
Billing Time Includes Free Minutes	 Check this item, assuming that the free minute is 30 minutes, and the parking time is 31 minutes. If the parking time exceeds the free minute, the parking time will be charged according to 31 minutes at this time. If this item is not checked, assuming that the free minute is 30 minutes and the parking time is 31 minutes, if it exceeds the free minute, the parking time at this time is 1 minute (31 minutes minus 30 minutes).
Intertemporal Splitting	 Suppose that the charge for period 1 is set at 1 yuan every 15 minutes from 9:00 to 10:00, the charge for period 2 is set at 10 yuan every 15 minutes from 10:00 to 11:00, and the parking time is from 9:43 to 10:30. If this item is not checked, 1 yuan will be charged from 9:43 to 9:58, and if it is only two minutes and less than 15 minutes from 9:58 to 10:00, it will be supplemented from 10:00 to 10:13, then charged according to time period 2 from 10:13 to 10:28, and so on. If this item is checked, 1 yuan will be charged from 9:43 to 9:58, only two minutes will be less than 15 minutes from 9:58 to 10:00, 1 yuan will be charged according to time period 2 from 10:13 to 10:28, and so on.
Enable The Same License Plate to Enter and Leave the Maximum Charge for Multiple Times in A Cycle of 24 Hours (24 Hours on Natural Days)	That is, rolling charges. If the accumulated fees for the same license plate entering and leaving the parking lot for many times exceed this value, no fees will be charged within the set period. The cycle can be set as 24 hours on a natural day or 24 hours on a cycle: 24 hours on a natural day refers to 0:00-24: 00; Cycle 24 hours refers to the time from the admission time to the next day.
By Time Period	 Time period: Set the charging standards for different time periods, and check the cross-day, but to ensure that the cumulative sum of all time periods is 24 hours, multiple time periods can be added, and the time periods remain continuous. Charge by time: If this item is checked, the first time charge, the amount of unit time charge cannot be filled in, only the highest charge is charged, and the fee set in "Maximum Charge" is charged every time; If this item is not checked, the fee will be charged according to the first time charge, and the remaining time exceeding the first time charge setting will be charged according to the unit time; If the first time charge is not set, the charge will be charged directly according to the unit time, and the unit minute must be a multiple of 15. If the charge exceeds the charge set in the "Maximum Charge", it will be charged according to the maximum charge amount. First time charge: Set the first time within how many minutes, the amount of charge. Maximum charge: the maximum amount of charge in the setting period. Charge amount per unit time: Set the charge amount for how many minutes in this time period.
Periodically	• Cycle: From the admission time, the next 1440 minutes (24 hours) can be divided into multiple cycle charging standards.

Parameter	Description	
	 Charge by time: set whether to charge by time in the cycle. After checking, you can only set the maximum charge amount in the cycle, but you cannot set the charge amount per unit time. Maximum charge: the maximum amount of charge in the setting period. Charge amount per unit time: Set the charge amount for how many minutes within the minutes of the cycle. 	

Table 9-21 Parameter Description of Temporary Car Charging Rules

9.4.2.2 Edit

Click a temporary charge name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.4.2.3 Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single temporary vehicle charge.

9.4.2.4 Refresh

Click **Refresh** at the upper part of the list to load new temporary vehicle charge.

9.4.3 Overtime Charging Rules

This paper introduces the operation Steps of charging rules when vehicles time out in.

9.4.3.1 Add New

Operating Steps:

Step 1: In the Parking module, select Parking Charge Management > Overtime Charge Rules.

Step 2: In the **Overtime Charge** Rule interface, click **Add New**and fill in the corresponding parameters, as shown in Figure 9-22. Please refer to Table 9-23 for parameter description.

		New		×
Name of Over Time C Rule [*]	Charge	Status*	Enable •	
Detail				
Temporary Small	Allowable Retention Time *	Include	Over Time Charge Rules *	
Vehicle A	minutes	Retention Time	/Hour	
Temporary Small	Allowable Retention Time *	Include	Over Time Charge Rules *	
Vehicle B	minutes	Retention Time	/Hour	
Temporary Medium	Allowable Retention Time *	Include	Over Time Charge Rules *	
Vehicle	minutes	Retention Time	/Hour	
Temporary Large	Allowable Retention Time *	Include	Over Time Charge Rules *	
Vehicle	minutes	Retention Time	/Hour	
	ОК	Cancel		

Figure 9-22 Interface of Timeout Charging Rules

Parameter	Description	
Overtime Charge Standard	Set the name of timeout charging standard, which cannot be duplicated.	
Status	Select whether to enable the charging standard.	
Detailed Settings	Set the allowed detention time of each temporary vehicle type after the central payment and the charging standard after exceeding the time.	
Allowable Residence Time The detention time allowed in the garage after the central payment; In case overtime, you need to charge again.		
Including Residence Time	Assume that the allowed detention time is 30 minutes, and the detention time is 31 minutes after payment. If this item is checked, it will be charged according to the timeout of 31 minutes; If this item is not checked, it will be charged according to the timeout of 1 minute.	
Overtime Charging Rules	The billing standard for exceeding the allowable residence time.	

Table 9-23 Parameter Description of Overtime Charge Rules

9.4.3.2 Edit

Click a name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.4.3.3 Delete

Select one or more temporary vehicle charge and click **Delete** at the upper part of the list and click **OK** to delete the selected temporary vehicle charge. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a singlover time charging rules.

9.4.3.4 Refresh

Click **Refresh** at the upper part of the list to load new over time charging rules.

9.4.4 Discount Strategy

This paper introduces the Step configuration of parking discount strategy for parking discount.

9.4.4.1 Add New

Operating Steps:

Step 1: In the Parking module, select Parking Charge Management > Discount Strategy.

Step 2: In the discount policy interface, click **Add New**and fill in the relevant parameters, as shown in Figure 9-24. Please refer to Table 9-25 for parameter description.

	New	×
Name [*] Discount Type [*] Free	Free	•
	OK Cancel]

Figure 9-24 New Discount Policy Interface

Parameter	Description
Policy Name	Set the name of discount policy, which cannot be duplicated.
Discount Type	 Select the discount type: Free, no charge. The amount of reduction and exemption, the cost is directly deducted from the fixed amount. Reduce minutes, subtract minutes from parking time and then charge. Percentage of reduction and exemption, percentage of expense deduction.
At present, the discount type is reduction amount, and the correspond Amount of Relief name is reduction amount; If it is another type, it corresponds to the corres unit. When the discount type is free, this item is not filled in.	

Table 9-25 Discount Strategy Parameter Description

9.4.4.2 Edit

Click a name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

9.4.4.3 Delete

Select one or more discount policies and click **Delete** at the upper part of the list and click **OK** to delete the selected discount policies. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single discount strategy.

9.4.4.4 Refresh

Click **Refresh** at the upper part of the list to load new discount policies.

9.4.5 Business Management

This paper introduces the operation Steps of merchant management in.

9.4.5.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Parking Charge Management > Business Management ".

Step 2: In the **Business Management** interface, click **Add New** fill in the corresponding parameters, as shown in Figure 9-26. Please refer to Table 9-27 for parameter description.

	New	×
Business Name* Name* Contact		
Business Phone		
Business Address		
_		
	OK Cancel	

Figure 9-26 Business Management New Interface

Parameter	Description
Merchant Name	Set the merchant's name, which cannot be duplicated.
Discount Method	Choose a discount strategy.
Contact Person	Set up merchant contacts.
Merchant Telephone Number	Set the contact number of the merchant.
Merchant Address	Set the merchant contact address.

Table 9-27 Description of Business Management Parameters

9.4.5.2 Edit

Click a name or **Edit** in the operation column to go to the Edit page. Modify and click **OK** to save modifications.

9.4.5.3 Delete

Select one or more vendors and click **Delete** at the upper part of the list and click **OK** to delete the selected vendors. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single vendor.

9.4.5.4 Refresh

Click **Refresh** at the upper part of the list to load new vendors.

9.4.6 Financial Reconciliation

This paper introduces the operation Steps of accounting reconciliation in.

Operating Steps:

Step 1: In the Parking module, select "Parking Charge Management > Financial Reconciliation".

Step 2: In the account reconciliation interface, click **Reconciliation**, as shown in Figure 9-28. Please refer to Table 9-29 for parameter description

	Reconcil	iation		\$
Duty Officer ID	1	Discount Amount	0	
Duty Officer Name	admin	Advance Amount	0	
Duty Start Time	2018-04-04 13:58:35	Turnover	100	
Duty End Time	2018-04-04 14:01:09	The Total Amount	100	
The number of free release vehicle	0	The Actual Amount	100]
The number of manual release	0	Confirm Time	2018-04-04 16:21:19]
Confirmor	admin	Confirm Amount*]
Remark	0			
	ок	Cancel		

Figure 9-28 Accounting Reconciliation New Interface

Parameter	Description
Duty Officer Name	Duty officer name
Duty Officer Id	Duty officer ID
Duty Starts Time	Duty starts time
Duty End Time	Duty end time
The Number of Free Release Vehicle	Number of vehicles released free of charge
The Number of Manual Releases	Number of vehicles released manually
Confirmor	Reconciliation personnel
Advance Amount	Amount prepaid to the guard booth (for changes).
Turnover	Paid amount
The Total Amount	Advance amount + Turnover
The Actual Amount	Amount entered by the duty officer during the shift change.
Confirm Time:	Current time
Confirm Amount:	Amount confirmed by the reconciliation personnel
Remark	Remark to be added.

Table 9-29 Parameter Description of Accounting Reconciliation

9.5 Vechicle Management

9.5.1 License Plate Registeration

This paper introduces the operation Steps of License.Plate Registration.

9.5.1.1 Add New

Operating Steps:

Step 1: In the Parking module, select "Vechicle.Management > License.Plate Registration ".

Step 2: In the License.Plate Registration interface, click **Add New**, as shown in Figure 9-30. Please refer to Table 9-31 for parameter description

	New	3
Name * License Plate*		



Parameter	Description
Name	Enter the person's name
License Plate	License Plate numbers to be added for registration

Table 9-31 for parameter description of License.Plate Registration

9.5.1.2 Edit

Click **Edit** at the end of each line or click the corresponding Personnel ID and modify personnel license plate registration information in the Edit dialog box.

9.5.1.3 Delete

Select one or more license plate registration information and click **Delete** at the upper part of the list and click **OK** to delete the selected registration information. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single registration information.

9.5.1.4 Download License Plate Import Template

This function will help you to downlad the licence plate import template.

6	A	В
		License Plate Import Template
	Personnel ID	License plate number (multiple license plates, separated)

Figure 9-31(1) License.Plate Download Template

9.5.1.5 License Plate Import

This function will help you to upload the licence plate import template.

	License Plate Import	
File Format	Excel	
Select File	Browse Not Uploaded	
	data format is table name, the second line is hea ta, please check the file and then import.	ader, the third
		ader, the third
		ader, the third

Figure 9-32 License.Plate Registration Import Interface

9.5.2 Vehicle Authorization

This paper introduces the configuration of vehicle authorization Steps in. Only authorized vehicles can normally use the parking module process.

9.5.2.1 Add New

Operating Steps:

Step 1: In the **Parking** module, select **Vehicle Management > Vehicle Authorization**.

Step 2: Click **Add** and fill in the relevant parameters, as shown in Figure 9-33. Please refer to Table 9-34 for parameter description.

Name *			
Parking Space Number*	1	1	
Entrance and Exit Area*	· · · · · · · · · · · · · · · · · · ·	1	
Vehicle Type*		1	
Fixed Charge Name*		1	
Start Time*	2022-07-22	1	
End Time*			
Fee *			
the second	I area, must pass the large yard a	area, the system	
default authorized correspon	nding large parking area!		

Figure 9-33 Vehicle Authorization Interface

Parameter	Description
Name	In the input box, enter one or more characters contained in the name or number of the owner, and you can find the owner vaguely.
Parking Space Number	Enter the total number of parking spaces in this area
Entrance And Exit Area	Set the Entrance and Exit Area where this license plate can pass. After selecting the parking space number, filter and only display the Entrance and Exit Area of the parking lot area to which the parking space number belongs.
Car Type	Select the vehicle type to which the vehicle belongs.
Fixed Charge Name	Unique name of a fixed vehicle charge
Start Time/End Time	Refers to the time/deadline for authorizing the license plate to take effect. If the fixed car charging standard is enabled, this parameter is filled in by default.
Amount Collected	Record the fees charged for this authorization; If the fixed car charging standard is enabled, this parameter is filled in by default.

Table 9-34 Description of Vehicle Authorization Parameters

Step 3: Click OK to complete the setting of vehicle authorization.

9.5.2.2 Fixed vechicle Batch Authorization

On the Vehicle Management page, click Fixed vehicle Batch Authorization. The Fixed vehicle Batch Authorization page is displayed as in the following figure:

		New			×
Name Lice	ense Plate	Show authorized personnel	No 🔻	Q @	
Alternative		Selected(0)			
🗌 First Name Last Nam	ne 🔰 License Plate	🗌 First Name	Last Name	License Plate	
Zorro	SC1030U	>> > <	Ê		
∢ < < 1-1 > > 50 ro	ws per page ♥	4	No data		Þ
Authorization Yard Area"	ws per page *	Start Time*	No data		Þ
Authorization Yard Area" Channel Entrance and Exit Name"	ws per page *	Start Time* End Time*			•
Authorization Yard Area"	ws per page *	Start Time*			•

Figure 9-35 Fixed vechicle Batch Authorization New Interface

Select one or more license plates to be authorized from the list on the left. Click > in the middle to add the license plate to the list on the right. Enter the vehicle type, entrance, and exit area, fee, start time and end time in the Authorization area, and click OK to save the information and authorize fixed vehicles in batches.

9.5.2.3 Temporary Vechicle Authorization

On the **Vehicle Management** page, click **Temporary Vehicle Authorization**, the Temporary Vehicle Authorization page is displayed as shown in the following figure. Only the entrance and exit areas to be authorized need to be selected.

Entrance and Exit Area*			
Authorize the small	vard area	must pass the la	arde vard area
system default authorize			

Figure 9-36 Temporary vechicle Authorization Interface

9.5.2.4 Fixed Vechicle Authorization: Delete

Select multiple check boxes in the first column of the license plate list and click Delete to cancel license plates in batches or click Delete at the end of each line to cancel a single license plate.

9.5.2.5 Export

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

	I	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	The second se	
Data to Export	All (max 10000)	0 records)	
	Selected (max	100000 records)	
	Start Position	100000 records)	

Figure 9-37 Fixed vechicle Authorization Export

9.5.3 Fixed Vechicle Extension

9.5.3.1 Fixed Vechicle Authorization: Delete

Select multiple check boxes in the first column of the license plate list and click **Delete** to cancel license plates in batches or click **Delete** at the end of each line to cancel a single license plate.

9.5.3.2 Batch Extension

Select a fixed license plate for which the valid time needs to be extended and click **Batch Extension** at the end of a fixed license plate. The **Batch Extension** page is displayed.

		New		
Authorization end time 2022-04-22	To 2022-07-29	Vehicle Definition	Small Vehicle A 🔹	More 👻 📿
Alternative		Selected(0)		
🗌 First Name Last Nam	e License Plate	🗌 First N	ame Last Name	License Plate
		>>		
		>		
No data		< .		
			No data	
	•			
< < 0 > > 50 ro	vsperpage 🔻	4		
Batch extension				
Fixed Charge Name*	-	Fee*		
If the parking space number is displayed number.	and the authorization has expire	ed, you need to select the imp	ort and export area first, an	d assign the parking space
	Confirm	Close		

Figure 9-38 Fixed vechicle Authorization Batch Extension

Set Extended Deadline and Fee. Click OK to save and exit.

9.5.4 Block&Allow List Management

9.5.4.1 Add New

Operating Steps:

Step 1: In the Parking module, select Vehicle Management > Block&Allow List Management.

Step 2: Click **Add New** and fill in the relevant parameters, as shown in Figure 9-39. Please refer to Table 9-40 for parameter description.

License Plate*	1	
License Plate Type*	Allowlist 🔹	
Start Time*	2022-07-22	
End Time*		

Figure 9-39 Block&Allow List Management New Interface

Parameter	Description
License Plate	License plate numbers to be <mark>added</mark> to the <mark>blocklist or</mark> allowlist
License Plate Type	The value can be block list or allowlist
Start Time/End Time	Time when the allowlist takes effect & expires (This parameter is not available for the blocklist).

Table 9-40 Description of Block&Allow List Management Parameters

9.5.4.2 Edit

Click a **license plate** number or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

9.5.4.3 Delete

Select one or more license plate numbers and click **Delete** at the upper part of the list and click **O**K to delete the selected license plate numbers. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single license plate number.

9.5.4.4 Refresh

Click **Refresh** at the upper part of the list to load the latest blocklist and Allowlist.

9.5.4.5 Synchronize Blocklist

Click Synchronize Blocklist, click OK to synchronize all blocklists, click Cancel to cancel.

When the device is off-line, the device will automatically synchronize blocklist and broadcast voice. It should be noted that the device must be equipped with an SD card.

9.5.4.6 Synchronize Allowlist

Click Synchronize Allowlist, click OK to synchronize all Allowlists, click Cancel to cancel.

When the device is off-line, the device will identify the Alowlist synchronized and automatically open the gate. It should be noted that the device must be equipped with an SD card.

9.6 Report Management

9.6.1 Vechicle Inside

9.6.1.1 Remove

Remove from Device function lets you to remove or eliminate the transmitted Work Codes from the Device.

9.6.1.2 Export

Device information can be exported in EXCEL, PDF, CSV file forma	at.
--	-----

Encrypt or not	○ Yes No	
File Format	EXCEL 👻	
Data to Export	 All (max 100000 records) 	
	Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	

Figure 9-41 vechicle Inside Export Interface

9.6.1.3 License Plate Correction

Make modifications of the License Plate Number.

New	×
License Plate Search	
Total Search Records: 0	
License Plate Number Correction	
License Plate Correction Close	

Figure 9-42 License Plate Correction

It will provide the details of the vehicle which entered into the parking.

Click **Report Management** > **Entry Record**. Select the desired time period, vehicle owner and license plate number, and click \bigcirc to query Entry records. Click **More** to query based on other conditions.

9.6.2.1 Export

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

	Export	×
Encrypt or not	Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	O Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	
	OK Cancel	
	Calicer	

Figure 9-43 Entry Record of Export Interface

9.6.3 Exit Record

It will provide the details of the vehicle which exited out of the parking.

Click **Report Management** > **Exit Record**. Select the desired time period, vehicle owner and license plate number, and click to query Exit records. Click **More** to query based on other conditions.

9.6.3.1 Export

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

Encrypt or not	🔿 Yes 💽 No	
File Format	EXCEL	
Data to Export	All (max 100000 i)	records)
	O Selected (max 10	0000 records)
	Start Position	1
	Total Records	100

Figure 9-44 Exit Record of Export Interface

9.6.4 Charge Record

The Charge Record Details module provides reports of charging information of all exit vehicles (records with fee of 0 are also generated for fixed vehicles and charging-free temporary vehicles).

9.6.4.1 Export

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

Encrypt or not	🚫 Yes 💽 No		
File Format	EXCEL	•	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	

Figure 9-45 Export interface for Charge Record

Choose **Report Management** > **Charge Details**. Select the desired time period and operator name and click \ to query charging details. Click **More** to query based on other conditions. The page is shown in the following figure.

9.6.5 Expired Vehicle

9.6.5.1 Incoming Unusual Vehicles

It will provide the details of the vehicle which incoming unusually of the parking.

Click **Report Management** > **Incoming Unusual Vehicles**. Select the desired time period, vehicle owner and license plate number, and click **Q** to query Exit records. Click **More** to query based on other conditions.

9.6.5.2 Export

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

	1	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	T	
Data to Export	All (max 10000)	00 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	ОК	Cancel	

Figure 9-46 Incoming Unusual Vehicles of Export Interface

9.6.6 Fixed Vehicle Authorization Record

It will provide the details of the vehicle which fixed authorization records of the parking.

Click **Report Management** > **Fixed Vechicle Authorization Record**. Select the desired time period, vehicle owner and license plate number, and click \bigcirc to query Exit records. Click **More** to query based on other conditions.

9.6.6.1 Export

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

Encrypt or not	🚫 Yes 💽 No		
File Format	EXCEL	•	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	

Figure 9-47 Fixed vehicle Authorization Record of Export Interface

9.6.7 Device Opreation Record

ZKBio CVSecurity	:	:: ¥							
Basic parking manage >	Pa	arking / Rep	or <mark>t</mark> Management	/ Device Operation Reco	rd				
Charge Management >		IP Address		Device Name	Q	0			
😝 Vehicle Management >		O Refres	h 🗊 Delete						
III Report Management ✓			ddress	Device Name	Operating Time	Operation Result	Operation Type	Object	Operatio
The port management		1 92	.168.20.254	d	2022-07-18 03:42:11	Turn off the device	The operation succeed		Ū
Vehicle Inside		192	.168.20.254	d	2022-07-13 03:26:44	Connecting device	The operation failed!		前
Entry Record		102	.168.20.254	d	2022-07-08 03:56:13	Connecting device	The operation failed!		ŵ
Exit Record		192	.100.20.254	ŭ	2022-07-08 03.30.13	Connecting device	The operation failed		
Charge Record		192	.168.20.254	d	2022-07-07 09:04:25	获取功能参数	The operation failed!		Û
Expired Vehicle		192	.168.20.254	d	2022-07-04 12:29:01	Get device parameters	The operation failed!		Û
Incoming unusual vehicles	«	192	.168.20.254	d	2022-07-04 12:28:51	Connecting device	The operation failed!		Ŵ
Fixed Vehicle Authorization Record	U	192	.168.20.254	LPR-300 Bangalore	2022-07-04 12:17:27	Turn off the device	The operation succeed		Ē.
Device Operation Record		192	.168.20.254	LPR-300 Bangalore	2022-07-04 11:54:36	Synchronize Time	The device is offline, i		Û
Handover Statistics		192	.168.20.254	LPR-300 Bangalore	2022-07-04 11:54:25	Enable	The device is offline, i		面

Figure 9-47.1 Device Opreation Record Interface

9.6.7.1 Delete

Select one or more device operation record and click **Delete** at the upper part of the list and click **OK** to delete the selected device operation record. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single device operation record.

9.6.8 Handover Statistics

The Handover Record provides reports of handover records.

Choose **Report Management** > **Handover Statistics.** Select the desired time period and operator name and click \ to query handover records. Click **More** to query based on other conditions. The page is shown in the following figure.

9.6.8.1 Export

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

	I	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL		
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	<u> </u>	,	
	Start Position	1	

Figure 9-48 HandOver Statistics of Export Interface

9.6.9 Daily Income Statistics

The Daily Report provides reports of the total amount of charges per day for each shift in each duty guard booth.

Choose **Report Management** > **Daily Reports**. Select the desired time period and click \ to query the total amount of charges for each shift in each duty guard booth. The page is shown in the following figure.

9.6.9.1 Export

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

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL	
Data to Export	All (max 10000)	0 records)
	O Selected (max	100000 records)
	Start Position	1
	Total Records	100
	Total Necolus	100

Figure 9-49 Daily Income Statistics of Export Interface

9.6.10 Monthly Income Statistics

The Monthly Report provides statistics of parking fees for each day of the month.

Choose **Report Management > Monthly Reports**. Select the desired time period and click **1A** to query the parking fees the page is shown in the following figure.

9.6.10.1 Export

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

	Export	×
Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	Selected (max 100000 records)	
	<u> </u>	
	Start Position 1	

Figure 9-50 Export Interface of Monthly Income Statistics

9.7 Real-Time Monitoring

This paper introduces the configuration of real-time monitoring in parking module and can view the monitoring dynamics in real time in this interface.

9.7.1 Sentry Booth Monitoring

This paper introduces that the configuration of monitoring related information can be viewed in the booth monitoring interface in, and the administrator can view the monitoring dynamics in the booth monitoring interface.

Operating Steps:

Step 1: In the Parking module, click "Parking Real-time Monitoring > Sentry Booth Monitoring".

Step 2: In the booth monitoring interface, you can view related monitoring videos and events, as shown in Figure 9-51.

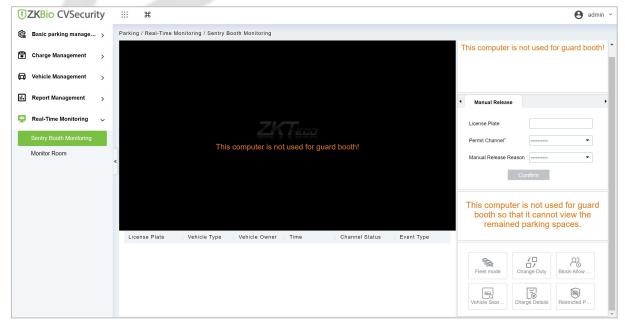


Figure 9-51 Guard Booth Monitoring Interface

9.7.1.1 Manual Release

This paper introduces the manual release function of Guard Booth monitoring, and the administrator can operate the vehicle release in this interface.

Operating Steps:

Step 1: In the **Parking** module, click "**Parking Real-time Monitoring > Box Monitoring > Manual Release**".

Step 2: Under manual release, the administrator can operate vehicle release here, and when the vehicle is not recognized, manual release can be performed, as shown in Figure 9-52.

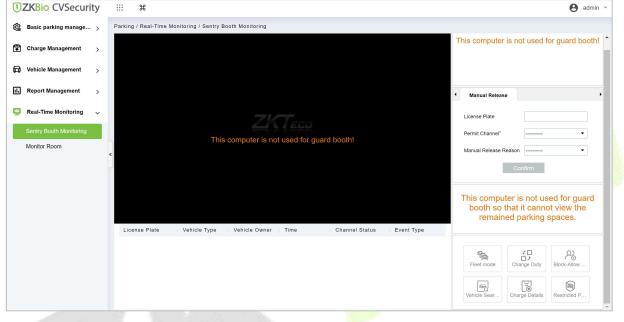


Figure 9-52 Manual Pass Interface

9.7.1.2 Change Shifts

This paper introduces the information configuration of personnel shift change in, where you can view the data information of shift change handover when exchanging shifts.

Operating Steps:

Step 1: In the Parking module, click "Parking Box Monitoring > Shift Change".

Step 2: Set the relevant shift information, as shown in Figure 9-53, and refer to Table 9-54 for parameter description.

	Shift confin	mation	
Duty Officer Name	admin	Duty Officer ID	1
Duty start time	2017-05-17 14:20:15	Advance amount*	100
Duty end time	2017-05-17 14:55:44	Turnover	0
The number of free release	3	The total amount	100
vehicle			
The number of artificial	0	The actual	100
release		amount*	
	ОК	Cancel	

Figure 9-53 Shift Change Interface

Parameter	Description
-----------	-------------

Parameter	Description
Name of Duty Officer	Show the name of the person on duty
Working Hours	Show the working hours of the personnel on duty
Attandance Checking Hours	Display the attandance checking time of the attendant
Number of Vehicles Released Free of Charge	Number of vehicles allowed to be released free of charge
Number of Manual Switches	Number of times of manual release through manual gate opening
Advance Amount	Such as reserve amount, such as reserve for change
Preferential Amount	Amount of parking discount
Turnover	Business amount generated by parking lot charges
Total Amount	Total amount of car park revenue
Actual Amount	Actual amount of parking lot income (net income)

Table 9-54 Description of Shift Change Parameters

Step 3: Enter the account number and password of the shift changer.

Step 4: Click **OK** to complete the setting of booth shift change.

9.7.2 Monitor Room

This paper introduces that the configuration of monitoring related information can be viewed in the monitoring room interface in, and the administrator can view the monitoring dynamics in the monitoring room interface.

Operating Steps:

Step 1: In the Parking module, click "Parking Real-Time Monitoring > Monitor Room".

Step 2: You can view relevant monitoring videos and data statistics in the monitoring room interface, as shown in Figure 9-55.

JZKBio CV	Security III	H						0	admin ~
Parking / Re	al-Time Monitoring / Moni	itor Room							
7					Traffic statistics	App O App	Day	Month	Year
Ψ					1				
a					0.8				
					010				
					0.4				
a la					0.2				
					00 01 02 03 04 05 0	6 07 08 09 10 11 12 13 14	15 16 17 18 19	9 20 21 2	22 23
译	Unab	le to preview, proces	sing methods are as follows:		Charge statistics		Day	Month	Year
*		Please click do	or the version of the video co ownload controls:		1				
If you ha	ave already installed		y. Please check the user UAC minimum).	level (adjusted to the	0.8				
	After the		d restart or refresh the browse		0.6				
					0.4				
0					0.4				
Parking Are	a 1 🔹	Guard Booth	Channel	Open	0 01 02 03 04 05 0	6 07 08 09 10 11 12 13 14	15 16 17 18 19	20 21 2	22 23
Parking	Area Guard Boott	License Plate	Vehicle Type Time	Channel Stati	Residual parking statis	stics			
r to king	dia	License Flate	venicie type	Channel Statt	7				
					6 5				
					4				
					2				
					0,	· · · · · · · · · · · · · · · · · · ·			

Figure 9-55 Monitoring Room Interface

9.7.2.1 Manual Barrier Opening

This paper introduces the Step configuration that the administrator can open the Barrier manually, which can be used to open the Barrier manually when the vehicle is not recognized.

Operating Steps:

Step 1: In the Parking module, click "Parking Real-time Monitoring > Monitor Room".

Step 2: In the monitor room interface, click "Open Gate-Enter License Plate Number-Confirm Open Gate", as shown in Figure 9-56.

1	Parking / Real-Time Monitoring / Monitor Room		
		Traffic statistics	Yea
Ē			
ø		0.8	
		0.6	
•••		0.4	
	ZKTeco	0.2 0 0 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 2	2 23
	Unable to preview, processing methods are as follows: 1.Your computer does not install a video control, or the version of the video control is not the l	Charge statistics Day Month	Yea
	» Please click download controls;		
	If you have already installed the browser correctly. Please check the user UAC level (adjusted default or minimum).	d to the 0.8	
	After the operation, you should restart or refresh the browser.	0.6	
		0.4	
		0.2	
	Parking Area 1 Guard Booth Channel Open	0 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 2	2 23
	•	Residual parking statistics	

Figure 9-56 Switch Interface

10 Visitor Management

10.1 Operation Scenario

By registering visitor's certificates, photos and other effective ways, and issuing corresponding Access Control/Elevator control/passage/witness authority, visitors can be managed safely and efficiently.

10.2 Operation Flow

Introduces the configuration process of visitor management business.

The business configuration process of the visitor management business is shown in Figure 10-1.

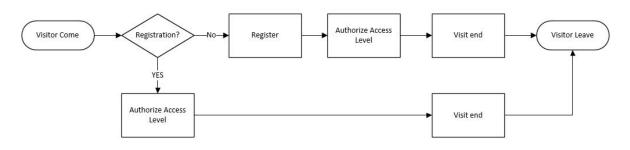


Figure 10- 1 Visitor Config<mark>uratio</mark>n Process

10.3 Visitor Registration

10.3.1 Entry Registration

10.3.1.1 Entry Registration

There are two ways to register visitors:

- 1. PC side (computer)
- 2. Visiting the passenger plane (ZKBioCVSecurity visits and logs in)

• PC-Side Registration (Direct Registration)

This paper introduces the configuration Steps of PC registration (Direct registration) in.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Registration** > **Entry Registration**.

Step 2: In the Entry registration interface, click **Visit Registration** to enter the registration interface for visitor registration, as shown in Figure 10-2.

			New			×
Host/Visited * Certificate Type* First Name* Company Country/Region Email	Enter the Query Co	Q Visit Department * Certificate No.* Last Name Mobile Phone Visitor Quantity*	· · · · · · · · · · · · · · · · · · ·	Visit Reason* Entrance* Gender License Plate Carrying Goods	Visit	
Permission Visitor Level Card Number		Start Time*	2021-12-20 11:35:08	End Time*	2021-12-20 23:59:59	
Capture Any exposure to succeed cases City visited in past of ays Remarks on health	O Yes O No		Any symptoms in the I st 14 days Body Temperature(°C/ °F)	None Cough	Fever Respiratory Issues	
		Save and New	ОК Са	ncel		

Figure 10- 2 Direct Register Visitor Interface

Parameter	Description
Host/Visited	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visit Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the Visit Reason of Basic Management.
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop- down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Entrance	Select the entry place for the visitor. You can add an entry place in the Entry Place of Basic Management .
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Visitor Quantity	Enter the number of visitors.
Start and End Time	Enter the start and end times of the visit.
Personnel Details	Enter the personnel details.
Capture	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 10-1 Description of Parameters of Entry Registration

• Pc Registration (Second-Generation Id Card Reservation Registration)

This paper introduces the configuration Steps of Registration through the Visitor Reservation.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation** > **Visitor Reservation**.

Step 2: In the visitor reservation interface, click **New** to complete the reservation registration before visitors visit, as shown in Figure 10-3.

		New		×
Certificate Type* Certificate No.* First Name* Mobile Phone Start Time Visit Reason* Company	ID I I I I I I I I I I I I I I I I I I	Host/Visited * Visit Department * Last Name Email End Time License Plate	Enter the Query Co Q	
Portrait	Personnel Detail			
		Captured Photo		<u> </u>
	Save and New	OK Cano	cel	

Figure 10- 3 Reservation Interface

Parameter	Description
Host/Visited	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visit Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the Visit Reason of Basic Management .
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop- down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Start and End Time	Enter the start and end times of the visit.
Personnel Details	Enter the personnel details.
Portrait	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 10-2 Description of Parameters Reservation

Step 3: Select **Visitor Registration > Entry Registration > Entry Registration** to enter the registration interface for visitor registration. Enter the **First Name** to directly obtain the ID number, thus displaying the visitor information of reservation registration, then select the visitor authority, and click **OK** to complete the visit registration, as shown in Figure 10-4.

				New			×
Host/Visited * Certificate Type* First Name* Company Country/Region Email	ID	• Q • •	Visit Department * Certificate No.* Last Name Mobile Phone Visitor Quantity*	· · · · · · · · · · · · · · · · · · ·	Visit Reason* Entrance* Gender License Plate Carrying Goods	Visit	
ermission Visitor Level Card Number		•	Start Time*	2021-12-20 11:35:08	End Time*	2021-12-20 23:59:59	
Capture Any exposure to su cted cases City visited in past ays Remarks on health	14 d			Any symptoms in the la st 14 days Body Temperature("C/ "F)	None Cough	Fever Respiratory Issues	,
			Save and New	OK Can	icel		

Figure 10- 4 Second Generation Identity Registration Interface

Parameter	Description
Host/Visited	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visit Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the Visit Reason of Basic Management .
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop- down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking icon.
Entrance	Select the entry place for the visitor. You can add an entry place in the Entry Place of Basic Management .
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Visitor Quantity	Enter the number of visitors.
Start and End Time	Enter the start and end times of the visit.
Personnel Details	Enter the personnel details.
Capture	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

 Table 10-2 Description of Parameters of Second Generation Identity Registration

Notes:

For different browsers, the contents of tips are different, the actual browser display prevails, just choose the shared camera, and allow the system to access the camera.

If the entry place supports a network camera, scanner, high camera, it will not pop up this tip.

You can select card number, fingerprint, password, or code scanning for registration (set in the parameter setting).

10.3.1.2 Visitor Cloning

Application scenario: Similar to an entourage copying some information from the previous person, visitors only need to show their credentials and snap photos to complete the registration. It mainly includes the following attributes: Host, visit department, visit reason, Entrance, company, country, visitor level, start time, end time.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Registration** > **Entry Registration**.

Step 2: In the visitor registration interface, click **Visitor Cloning** to enter the registration interface for visitor cloning.

Host/Visited *	12135	 Q Visit Department * 	Department Name 🔹	Visit Reason*	Visit	•
Certificate Type*	ID .	 Certificate No.* 		Entrance*	BLR	•
First Name*		 Last Name 		Gender	1 <u>-1-1-1-1-1-1</u>	-
Company		Mobile Phone		License Plate		
Country/Region		 Visitor Quantity* 	1	Carrying Goods		
Email						
Permission						
Visitor Level		✓ Start Time*	2022-07-22 09:43:12	End Time*	2022-07-22 23:59:59	
Card Number	72204508	Device Verification Password		Biometrics Type		\$
Capture	Personnel Detail					•
		A No camera connecte	d.	A No cam	era connected.	
	Captured Photo	Capture	Certificate Photo	C	apture	

Figure 10- 5 Visitor Cloning interface

Parameter	Description
Host/Visited	Select the department the visitor will visit.
Visit Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the Visit Reason of Basic Management .
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop- down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking a icon.
Entrance	Select the entry place for the visitor. You can add an entry place in the Entry Place of Basic Management .

Parameter	Description
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Visitor Quantity	Enter the number of visitors.
Start and End Time	Enter the start and end times of the visit.
Personnel Details	Enter the personnel details.
Capture	The captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.

Table 10-3 Description of New Parameters for Positions

10.3.1.3 Batch

Batch option will help you to do multiple check-in and check-out at a time.

ZKBio CVSecurity	::: ¥			
Visitor Registration V	Visitor / Visitor Registration / Entry Registration			
Entry Registration	Name Certificate No.	Certificate Type	▼ More ▼ Q &	
Visitor	⊖ Refresh & Entry Registration & Exit Registrati	on 🕑 Visitor Cloning 📃 Batch 🝷		
	Visitor Code Certificate Certificate Fi		ost Last Visit Reason V	/isit Status Card
	800000008 123456 ID tes	st Ratch CheckOut	Visit	heck-Out 722
	«			

Figure 10-6 Batch Interface

Batch Check-in

Batch Check-in option will help you to do multiple check-in at a time. For that you need to create a reservation for the visitors. Then you can be able to see details in the **Batch Checkin** option for multiple check-ins at a time.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation** > **Visitor Reservation**. In the reservation interface, click **New** to complete the reservation registration.

Step 1: In the Visitor module, select Visitor Registration > Entry Registration.

Step 2: In the Entry Registration interface, select the visitor to do the check-ins and click **Batch > Batch checkin** to do multiple check-in of visitors at a time.

				New			×
sitor Info							
Name	Ce	ertificate No.		Certificate Type	▼ More *	Q @	
🗌 First Na	Last Na Ce	ertificate Ce	rtificate No. 👔	Host First Host Last	Visit Department	Mobile Phone En	nail
				<u> </u>			
				B			
				No data			
				No data			
6				No data			
4	> >/ 50 rd	ows per page 🍝	Jump To 1		cords		,
∢ I< < 0. armission	> >i 50 rd	ows per page *	Jump To 1		cords	_	þ
	> >1 50 m		Jump To 1 Start Time		cords End Time	2022-07-22 23:59:5	

Figure 10-7 Batch Check in interface

Step 3: Click OK to check in the selected visitors.

Batch Check Out

Batch check in option will help you to do multiple check out of visitors at a time.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Registration > Entry Registration**.

Step 2: In the Entry Registration interface, select the visitor to do the checkouts and click **Batch > Batch checkout** to do multiple checkouts of visitors at a time.

Visitor Registration	. Visit	tor / Visitor Registr	ation / Entry Reg	istration							
Entry Registration		Name	Certif	licate No.		Certificate Type	 More * 	Q @			
Visitor		CRefresh & Er	try Registration	유 Exit Regist	tration 🗿 Vis	itor Cloning = Batch +					
		Visitor Code	Certificate	Certificate	First Name	Last Name 🖗 Batch Checkin	Host Last	Visit Reason	Visit Status	Card Number	Enter Time
		80000010	43534	ID	jo	R Batch CheckOut		Visit	Check-Out	72200956	2022-07-22 07:24
		80000009	1234	ID	ani			Visit	Check-Out	72208206	2022-07-22 07:24
		80000008	123456	ID	test			Visit	Check-Out	72209192	2022-07-22 04:12:
						Prompt		1			
						Are you want to perform the B	atch CheckOut				
						operation?					
						ок	Cancel				
	*										

Figure 10-8 Batch Check out interface

Step 3: Click OK to check-out the selected visitors.

10.3.2 Visitor

Visitor interface provides the complete details about the registered visitors such as Visitor Code, First Name, Last Name, Certificate Type, Certificate No., Company etc. You can delete, disable or enable and export the selected visitor.

Visitor Registration 🗸	Visitor	/ Visitor Registra	ation / Visitor											
Entry Registration	Nar	ne [Certi	icate No.	(Certificate Type	•	More * Q	0					
Visitor	0	Refresh 🗴 De	lete 🛞 Disabl	e 🛞 Enable	∱ Export									
		Visitor Code	First Name	Last Name	Certificate Type	Certificate No.	Company	License Plate	Mobile Pho	Category	Enable	Created Time	Remarks o	City visited
		80000008	test		ID	123456				NORMAL	0	2022-07-22 04:12		
		80000007	www		ID	789				NORMAL	0	2022-07-21 12:48		
		80000006	wwws		ID	112				NORMAL	0	2022-07-21 11:50		
		80000005	RRR		ID	123				NORMAL	0	2022-07-21 11:49:		
		80000004	test		ID	354354354		sdfdst32434		NORMAL	0	2022-06-29 07:47		
		80000003	Popy12		ID	468779578968886		ADC354354	15878965	BOLO	0	2022-06-29 03:08		DongG
		80000001	test		ID	354354354			453543453	NORMAL	0	2022-05-26 02:56		
	«													



10.3.2.1 Deleting a Visitor (Delete)

In **Visito**r module click **Visitor Registration** > **Visitor**, select a visitor, and click **Delete**.

Entry Registration	Name	Certificate No.		Certificate Type	More ∗ Q Q		
Visitor	🔾 Refresh 📋 De	elete 🖲 Disable 🚿 Enable	1 Export				
	Visitor Code	First Name Last Name	Certificate Type	Certificate No. C	ompany License Plate Mobile Pho	Category	Enab
	<u>80000008</u>	test	ID	123456		NORMAL	0
	80000007	www	ID	789		NORMAL	0
	<u>80000006</u>	wwws	ID	112		NORMAL	0
	80000005	RRR	ID	123		NORMAL	0
	80000004	test	ID	354354354	sdfdst32434	NORMAL	0
	80000003	Popy12	ID	468779578968886	ADC354354 15878965	BOLO	0
	80000001	test	ID	354354354	Prompt	AL	0
	«				Are you sure you want to perform the de operation?	elete	

Figure 10- 10 Deleting Visitor

Click **OK** to delete the selected visitor.

10.3.2.2 Disabling a Visitor (Disable)

In Visitor module Click Visitor Registration > Visitor, select a visitor, and click Disable.

Visitor Registration ~											
Entry Registration		Name		Certificate No.		Certificate Type	*	More * Q	0		
Visitor		C R	efresh 🛍 Del	ete 🖲 Disable 🏾 🕄 Enable	∱ Export						
			Visitor Code	First Name Last Name	Certificate Type	Certificate No.	Company	License Plate	Mobile Pho	Category	Enab
			80000008	test	ID	123456				NORMAL	0
			<u>800000007</u>	www	ID	789				NORMAL	0
			80000006	WWWS	ID	112					0
		80000005		RRR	ID	123				NORMAL	
			<u>800000004</u>	test	ID	354354354		sdfdst32434		NORMAL	o
			<u>800000003</u>	Popy12	ID	468779578968886		ADC354354	15878965	BOLO	0
			<u>800000001</u>	test	ID	354354354		Pro	mpt	AL	0
	«							Are you sure to di	sable the 1 visitor	?	
								ок	Cancel		

Figure 10- 11 Disabling Visitor

Click **OK** to block the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor is blocked.

10.3.2.3 Enabling a Visitor (Enable)

In **Visito**r module Click **Visitor Registration** > **Visitor**, select a blocked visitor, and click **Enable**.

Entry Registration		Name	Certificate No.		Certificate Type	More - Q 🖉		
Visitor		⊖ Refresh 💼 De	elete 🖲 Disable 🛞 Enable	⊥ Export				
		Visitor Code	First Name Last Name	Certificate Type	Certificate No. Company	License Plate Mobile Pho	Category	Ena
		80000008	test	ID	123456		NORMAL	•
		80000007	www	ID ID ID ID	789		NORMAL	0
		<u>80000006</u>	wwws		112		NORMAL	0
		<u>800000005</u>	RRR		123		NORMAL	0
		<u>80000004</u>	test		354354354	sdfdst32434	NORMAL	0
		<u>80000003</u>	Popy12		468779578968886	ADC354354 15878965		0
		<u>80000001</u>	test	ID	354354354	Prompt	AL	0
	*					Are you sure to enable the 1 visite OK Cancel		

Figure 10-12 Enabling Visitor

Click **OK** to enable the visitor. The enable entry for the corresponding selected visitor will show Sindicates the visitor is enabled.

10.3.2.4 Export

You can export visitor details into an Excel, PDF, or CSV file. See the following figure 10-20.

Operating Steps:

Step 1: In **Visito**r module click **Visitor Registration > Visitor > Export** to export the visitor records to Excel sheet or PDF or CSV. Enter the User password in the prompt.

TZKBio CVSecurity		¥							
関 Visitor Registration 🗸	Visitor	Visitor Registra	tion / Visitor						
Entry Registration	Nam	e	Certificate No.		Certificate Type	▼ More ▼ Q	Q		
Visitor	O F	Refresh 🔟 De	lete 🖲 Disable 🚿 Enable	1 Export					
		Visitor Code	First Name Last Name	Certificate Type	Certificate No.	Company License Plate	Mobile Pho	Category	Ena
		80000008	test	ID	123456			NORMAL	0
		<u>80000007</u>	www	ID	789			NORMAL	0
		80000006	wwws	ID	112			NORMAL	0
		800000005	RRR	ID	123			NORMAL	0
		<u>800000004</u>	test	ID	354354354	sdfdst32434		NORMAL	0
		<u>800000003</u>	Popy12	ID	468779578968886	ADC354354	15878965	BOLO	0
		80000001	test	ID	354354354	Security Verification		×	0
	*					User Password*	Cancel		

Figure 10- 13 Export Interface

Step 2: Select the file format and click OK.

Encrypt or not	Yes No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	O Selected (max 100000 records)	
	Start Position 1	
	Total Records 100	
	Total Records 100	

Figure 10- 14 Export Interface

10.4 Visitor Reservation

10.4.1 Visitor Reservation

Visitor Reservation helps you to do reservations before the visitor's visit.

10.4.1.1 Adding a Visitor Reservation (New)

Creating new Reservations for Visitors.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation** > **Visitor Reservation**.

Step 2: In the reservation interface, click **New** to complete the reservation registration before the visitor's visit.

		New		×
Certificate Type* Certificate No.* First Name* Mobile Phone Start Time Visit Reason* Company	□	Host/Visited * Visit Department * Last Name Email End Time License Plate	Enter the Query Co Q 2021-12-20 23:59:59	
Portrait Pe	rrsonnel Detail			,
	Save and New	Captured Photo		

Figure 10-15 Reservation Interface

Parameter	Description
Host/Visited	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Visit Department	Select the department the visitor will visit.
Visit Reason	Select the visit reason. You can also input a new reason, and the reason will be added in the Visit Reason list in the Visit Reason of Basic Management .
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking a icon.
Certificate No.	The numbers and letters are legal; the max length is 20.
First Name	Enter the first name of the visitor.
Start and End Time	Enter the start and end times of the visit.

Personnel DetailsEnter the personnel details.PortraitThe captured photo and certificate photo can be taken separately or at the same time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access to this page.	Parameter	Description
Portrait time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access	Personnel Details	Enter the personnel details.
	Portrait	time (which can be set in Parameter Settings). If there is a camera (High-Speed Portable HD Doc Scanner) connected to the server, you can click Capture to take the visitors' photos. The browser may block the camera to access, please click in the IP address bar to select the camera and change the setting to allow access

Table 10- 4 Description of Parameters of Adding a Visitor Reservation

After the reservation visitors can complete the visit registration using Entry Registration option to know more about the registration process.

10.4.1.2 Deleting a Visitor Reservation (Delete)

In the **Visitor** module, select **Visitor Reservation** > **Visitor Reservation** select a visitor reservation and click **Delete**.

Visitor Registration	> Vi		Reservation / Visitor Re						
Visitor Reservation	~	Visiting time from	m	To More	- Q @				
Visitor Reservation		C Refresh	국 New 💼 Delete	🛓 Import 🛛 & Download template					
Reservation Audit		Host N	lumber Host First	Host Last Visit Department	First Name Last Name	Certificate Type	Certificate No.	Mobile Phone	Comp
Invite		<u>9999</u>	K-TEST	Department Name	wwws	ID	112		
		1119	multibio	Department Name	Popy12	ID	468779578968886	15878965	
		1114	Md. Jalal	Development	test	ID	354354354	453543453	
							Prompt		
	«					Are you sure you o	want to perform the delet peration?	e	
						ок	Cancel		

Figure 10-16 Deleting Visitor Reservation

Click **OK** to delete the selected visitor reservation.

10.4.1.3 Import

You can import visitor reservation details into the software as in Excel format. See the following Figure 10-17.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation > Visitor Reservation**, select a visitor reservation and click **Import**.

TZKBio CVSecurity	::: ¥		
Visitor Registration >	Visitor / Visitor Reservation / Visitor Reservation		
Uisitor Reservation V	Visiting time from To	More * Q Q	
Visitor Reservation	⊖ Refresh I New 🖻 Delete 😾 Import 💠 Dov	nload template	
Reservation Audit	Host Number Host First Host Last Vis	it Department First Name Last Name Certificate Type	Certificate No. Mobile Phone Company
Invite	9999 K-TEST	Import	×
	Tile File File File File File File File F	rmat 💿 Excel	3779578968886 15878965
		File <u>Browse</u> Not Uploaded d line of the data format is table name, the second line is header, the third he import data, please check the file and then import.	4354354 453543453
		OK Cancel	
3			

Figure 10- 17 Import Visitor Reservation

Step 2: Click the **Browse** button to import the visitor reservation template data (You can download the template from the software by clicking **Download Template**) into the system, as shown in Figure 10-17.

Step 3: Click OK, and the interface displays the result of importing and adding visitor reservations.

Step 5: Click Close to complete the import and addition of visitor reservations.

10.4.1.4 Download Template

You can download templete visitor reservation details into the software as in Excel format.

Operating Steps:

Step 1: In the **Visitor** module, select **Visitor Reservation** > **Visitor Reservation** select a visitor reservation and click **Download Template**.

Step 2: Click OK, and the interface displays the result of importing and adding visitor reservations.

ZKBio CVSecurity		Ħ											θ	admin
Visitor Registration	Visitor	/ Visitor Reservat	tion / Visitor Res	ervation										
Visitor Reservation 🗸	Visiti	ing time from		То	More	~ Q @								
Visitor Reservation	01	Refresh 🖅 Nev	v 💼 Delete	± Import ₹	Download template									
Reservation Audit		Host Number	Host First	Host Last	Visit Department	First Name	Last Name	Certificate Type	Certificate No.	Mobile Phone	Company	Visit Reason	Visit start time	Opera
Invite		<u>10002</u>	raj	h	hr	Cesar		ID	2343253			Visit	2022-08-03 11:13	admin
		9999	K-TEST		Department Name	wwws		ID	112			Visit	2022-07-21 17:20	admir
		<u>1119</u>	multibio		Department Name	Popy12		ID	468779578968886	15878965		Visit	2022-06-29 11:05	
		<u>1114</u>	Md. Jalal				Export	_	×	453543453		Visit	2022-05-26 10:55	admir
	«				File Format	EXCEL	÷							
							_		_					
						ОК	Can	cel						



10.4.2 Reservation Audit

Allow the administrator to review and block the employee's self-reservation visitors.

10.4.2.1 Review

Allow the administrator to review the employee's self-reservation visitors.

Operating Steps:

Step 1: In the Visitor module, select Visitor Reservation > Reservation Audit.

Step 2: In the **Reservation** interface, select the visitor to be reviewed and click **Review** to review the visitor.

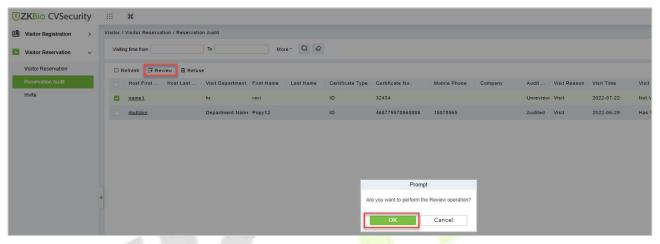


Figure 10- 19 Review Visitor Reservation

Step 3: Click **OK** to perform the review operation.

10.4.2.2 Refuse

Allow the administrator to block the employee's self-reservation visitors.

Operating Steps:

Step 1: In the Visitor module, select Visitor Reservation > Reservation Audit.

Step 2: In the **Reservation** interface, select the visitor to be reviewed and click **Refuse** to block the visitor.

Visitor Registration	>	Visitor / Visitor Reservation / Reservatio	n Audit							
Visitor Reservation	~	Visiting time from	То	More* Q 🖉						
Visitor Reservation		🔾 Refresh 📑 Review 💼 Refus								
Reservation Audit		🔲 Host First Host Last	Visit Department	First Name Last Name	Certificate Type	Certificate No.	Mobile Phone	Company	Audit	Visit
Invite		name1	hr	ravi	ID	32434			Unreview	Visit
		multibio	Department Name	Popy12	ID	468779578968886	15878965		Audited	Visit
						Prompt				
							Polyco operation?			
	4	«			A	re you want to perform the	Netuse operation?			

Figure 10-20 Refuse Visitor Reservation

Step 3: Click **OK** to perform the refuse operation.

User Manual

10.4.3 Invite

10.4.3.1 Sending Invitations (New)

You can send invitations to the needed visitors by using this option.

Operating Steps:

Step 1: In the Visitor module, select Visitor Reservation > Invite.

Step 2: In the **Invite** interface, click **New** to send the invitation to the visitors and the details as shown in Figure 10-21.

Step 3: Click OK to send the invitation.

TZKBio CVSecurity	::: ¥
Visitor Registration >	Visitor / Visitor Reservation / Invite
☑ Visitor Reservation ~	Name of inviter Inviter department E-mail Address Status Q Q
Visitor Reservation	G Refresh 🖅 New 🗈 Delete 🔉 Resend
Reservation Audit	Name of inviter Last name of inviter Inviter department E-mail Address Status Sending Time Operations
Invite	□ K-TEST New X
	multibio Name of inviter * Enter the Query Co • Q Inviter department * -29 03:03:59.2 🖉 👜
	yyyy Content* -29 02:59:33.0 ∠ 10 E-mail Address * E-mail Address * ▲ Enter multiple mailboxes, separated by commas() or semicolons(). OK Cancel

Figure 10-21 Invite Interface

Parameter	Description
Name of the Inviter	Select the visited personnel. Click the input box to filter the query according to the input characters or click the query button to pop up the list of the visited personnel to select the visited personnel.
Inviter Department	Select the department of the inviter.
Content	Enter the content or reason of the invitation.
Email Address	Enter the Email address.

Table 10-5 Description of Parameters of Invite Visitors

10.4.3.2 Delete Invitations

To delete the visitor invitations.

Operating Steps:

Step 1: In Visitor module click Visitor Reservation > Invite.

Step 2: In the invite interface select the invitation to be deleted and click Delete.

Step 3: Click **OK** to delete the invitation.

Visitor Registration >	Visitor / Visitor Reservation / Inv				
Visitor Reservation v	Name of inviter	Inviter department	E-mail Address	Status	• Q @
Visitor Reservation	C Refresh ∓ New 💼 🛙	Delete 🗟 Resend			
Reservation Audit	Name of inviter	Last name of inviter Inviter department	E-mail Address	Status Sending Time	Operations
Invite	K-TEST	Department Name	k123556@gmail.com	Has been sent 2022-07-22 09:44:4	1.3 🖉 🛍
	K-TEST	Department Name	kkk123456789@gmail.com	Has been sent 2022-07-22 07:18:1	2.1 🖉 🛍
	🔲 multibio	Department Name	popy.xiao@zkteco.com	Has been sent 2022-06-29 03:03:5	9.2 🖉 🖻
	🔲 уууу	Department Name	popy.xiao@zkteco.com	Has been sent 2022-06-29 02:59:3	8.C 🖉 🖻
		Prompt	_		
		Are you sure you want to perform operation?	the delete		

Figure 10-22 Delete Invitations

10.4.3.3 Resend Invitation

To Resend the visitor invitations.

Operating Steps:

Step 1: In Visitor module click Visitor Reservation > Invite,

Step 2: In the invite interface select the invitation to be resend and click Resend.

Step 3: Click OK to resend the invitation.

Visitor Registration >	Visitor / Visitor Reservation	17 Invite					
Visitor Reservation ~	Name of inviter	Inviter departm	ent	E-mail Address	Stat	us •	Q &
Visitor Reservation	C Refresh 🔤 New	Delete 🔉 Resend					
Reservation Audit	Name of inviter	Last name of inviter	Inviter department	E-mail Address	Status	Sending Time	Operations
Invite	K-TEST		Department Name	k123556@gmail.com	Has been sent	2022-07-22 09:44:41.3	_ ₪
	K-TEST		Department Name	kkk123456789@gmail.com	Has been sent	2022-07-22 07:18:12.1	_ ₫
	🗌 multibio		Department Name	popy_xiao@zkteco.com	Has been sent	2022-06-29 03:03:59.2	_ ₫
	🔲 УУУУ		Department Name	popy_xiao@zkteco.com	Has been sent	2022-06-29 02:59:38.0	_ ₫
					Pr	ompt	
	«			Ar	e you want to perfor	m the Resend operation?	
				6	ОК	Cancel	

Figure 10-23 Resend Invitations

10.4.4 Respondent Self-Approval

Optimize the visitor process, after sending the visitor invitation email, ZKBio CVSecurity will send an audit email to the host. The host can complete the operation of "Review or Reject" by clicking on the audit link of the email, then quickly complete the review.

Set the Outgoing Mail Server Settings:

Step 1: In **System Management** module, click **Email Management** > **Outgoing Mail Server Settings**:

JZKBio CVSecurity		😝 admin 🕤
😩 System Management 🗸 🗸	System / System Management / E-mail Management	
Operation Log	Sender Recipient Q Q	
Database Management Area Settings	C Refresh 🛱 Delete 🛱 Outgoing Mail Server Settings ⊥ £ Export	
E-mail Management	Sender Recipient Subject Submit Time Send Time Status Error Message ZKBiolock@zkteco.c.c.harmir tkteco Visitor Reservatic 2022-10-11 03:01 2022-10-11 03:01 Successfi	2
Dictionary Management	ZKBlolock@zkteco.c lamber zkteci Visite Outgoing Mail Server Settings ×	
Data Cleaning Audio File	ZKBiolock@zkteco.c lamb zkteci Visite Outgoing Mal Server Settings	
Certificate Type	ZKBiolock@zkteco c charnin kteco Visite Port* a65 SL_TLS	
Print Template	ZKBiolock@zkteco.cc visite Email.Account* ZKBiolock@ztteco.cc visite Password* (ccc@ccc.vcc)	
System Monitoring Parameters	ZKBiolock@zkteco.c lamb ktec. 2503 Sender Name Admin-test	
	ZKBiolock@zkteco.c 17872 163.c Visitc Please complete the email verification.	
	ZKBiolock@zkteco.c charni tteco Visito	
	ZKBiolock@zkteco.c charnie zkteco Visite OK Cancel	
	ZKBiolock@zkteco.c chari kteco Visitor Reservatic 2022-10-11 01:57 2022-10-11 01:57 Successfi	
	ZKBiolock@zkteco.c charm citeco Visitor Reservatic 2022-10-11 01:53 2022-10-11 01:54 Successfi ZKBiolock@zkteco.c popy teco.cc Visitor Reservatic 2022-10-11 01:53 2022-10-11 01:53 Successfi	
Authority Management >	ZKBiolock@zkteco.c 1787	
Communication mana >	ZKBiolock@zkteco.c popy: ==o.cc Visitor Audit 2022-10-10 09:04 2022-10-10 09:04 Successfi	

Figure 10- 24 Outgoing Mail Server Settings

Step 2: Set the Outgoing Mail Server Settings as Table 2.5-1.

Parameter	How to set up
Email server address/port	You can customize the email server address and port. The email products that provide the SMTP server can be used, such as NetEase 163 email, Tencent QQ email, and Foxmail email. The specific address and port configurations must be obtained from the corresponding provider.
Email username and password	Enter the user's name and password for the mailbox.
Name of sender	Sets the name of the sender on the received message.
	Table 10- 6 Outgoing Mail Server Settings

Step 3: After setting, click Test Connection to receive the email, indicating that the test has passed.

Step 4: Click OK to finish setting email parameters.

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

Set Visitor Parameters:

Step 1: In Visitor module, Click Basic Management > Parameters.

Step 2: Select **No** for the **Enable automatic review of guest appointments**, so that the visitors' reservations need to be approved.

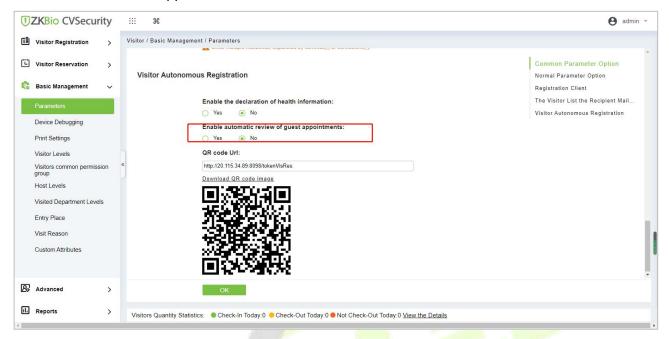


Figure 10-25 Enable automatic review of guest appointments

Set the Host Levels:

In the **Visitor** module, click **Visitor** > **Host Levels**> **+New**, select the corresponding personnel, click is a set the host Level for the corresponding personnel.

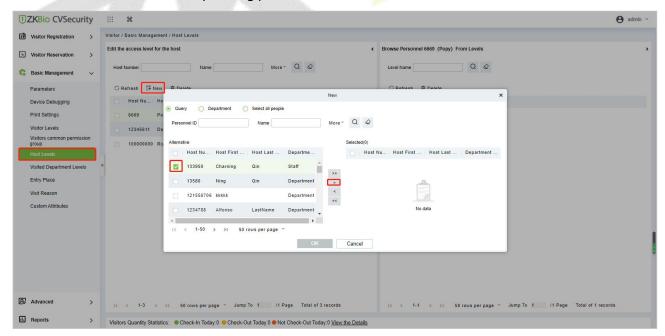


Figure 10-26 Adding Host Levels 1

				New					
Query OD	epartment	Select all people							
Personnel ID		Name		More *	Q	\Diamond			
Alternative					Selecte	d(1)			
Host Nu	Host First	Host Last	Departme			Host Nu	Host First	Host Last	Department
13580	Ning	Qin	Department	>>		133950	Charning	Qin	Staff
121556706	kkkk		Department	>					
1234788	Alfonso	LastName	Department	< <<					
1234888	Rusell	lastName	Department						
4	> >1 50	rows per page 1	•						

Figure 10-27 Adding Host Levels 2

Set the Linkage:

Step 1: Add an alert template.

Click **Visitor** > **Advanced** > **Alert Template** > **+New**, and fill in the template information.

IZKBio CVSecurity	······································	😝 admin 👻
Visitor Registration >	Visitor / Advanced / Alert Template	
Visitor Reservation >	Template Name Template Type Event Type New X	
Basic Management >	C Refresh Template Name Vustor Reservation Audit (ZKTeco)	
🕼 Advanced 🗸 🗸	Template Name Template Name Template Type* EAtal Extent Type* Extent Extent Type* Visitor Reservation Cut the day of the visit, send notification to the Host/Visited in advanced	
Category WatchList	Audit Send online up on et sus a send numeration to de nos readed in sortanced	
Watch List Thumbnails	Visitor Reservat Send audi permission to the Host	
Alert Template	Additional contact charing qingtafeco com Add	
Linkage	Bados Excitato	
	Valch List Subject Visitor Reservation Audit	
	Visitor Reservan Body Here is an appointment for visitors. Please review it.	
	Wattor Arrived Patel Visitor Arrived Patel Visitor Arrived Patel Visitor Arrived Value Name Visitor Arrived Visitor Name Visitor Name Visitor Correliante Bottom Piesse do not repty to this email Save and Name OK Cancel	
	I< < 1-9 > >I S0 rows per page * Jump To 1 /I Page Total of 9 records	

Figure 10-28 Add an Alert Template.

How to set up
E-Mail
Reservation
Select Send audit permission to the Host Fill in the Addtional Contact with the host email.
Fill in the subject and the body content.
Select the visitor content to be audited.

Table 10- 7 Add an Alert Template.

Step 2: Add a linkage.

Click **Visitor** > **Advanced** > **Linkage** > **+New**, and here we select the E-mail template *Visitor Reservation Audit(ZKTeco)* added in Step 1.

User Manual

ZKBio CVSecurity

ZKBio CVSecur	ity	::: ¥							e admin
Visitor Registration	>	Visitor / Advanced / Linka	ge						
Visitor Reservation	>	Linkage Name	Even	nt Type	• Q &				
Basic Management	>	◯ Refresh 📴 New	🗊 Delete 🛞 Dis	sable 🔇 Enable					
Advanced	~	🔲 🛛 Linkage Na	e .e	- · · · · · · · · · · · · · · · · · · ·	Edit		App Template Name	Enable	Operations
Category WatchList Watch List Thumbnails Alert Template Linkage	*	Audit	Linkage Name"	Audit Visitor Reservation A	Trigger Condition* Entrance WhatsApp Template Name*	Reservation Audit		0	2 1
				ОК	Cancel				

Figure 10- 29 Add a Linkage

Send an invitation E-mail:

Step 1: Click Visitor > Visitor Reservation > Invite > +New, fill in the correct information and save.

ZKBio CVSecurity	::: ¥				e admin								
Visitor Registration >	Visitor / Visitor Reservatio	n / Invite											
Visitor Reservation \sim	Name of inviter	In	iter department E-mail Address Status	• Q @									
Visitor Reservation	© Refresh ∓ New B Delete Na Resend												
Reservation Audit	Name of inviter	Last name	of inviter Inviter department E-mail Address Status Sending Time										
Invite	Рору	şt	New	× ∠ ū									
	Charning		Name of inviter * 133950(Charming Qin) Q Inviter department * Staff Content *	<u>e</u>									
	Charning		Hi Ning, Welcome to ZKTecol	<i>L</i> ū									
	Рору	t		∠ 前									
	Charning			<u>l</u> ā									
	« Charning		E-mail Address * 178****52@163.com	∠ 前									
	Рору	1.0		<u> </u>									
	Charning			<u>e</u> ū									
			Enter multiple malboxes, separated by commas(,) or Please enter a valid mail address.	<u>e</u> ū									
	Randy	c		<u>e</u> û									
			OK Cancel										

Figure 10- 30 Send an invitation E-mail 1

Step 2: We can view the record of this invitation email. If the status of the email is Has been sent, the email is sent successfully.

TKBio CVSecurity	::: ¥					😝 admin 👻
Visitor Registration >	Visitor / Visitor Reservation / Invite					
Visitor Reservation V	Name of inviter	Inviter department	E-mail Address	Status	Q &	
Visitor Reservation	◯ Refresh 🖅 New 💼 Dele	ete 🔉 Resend				
Reservation Audit	Name of inviter	ast name of inviter Inviter department	E-mail Address Sta	atus Sending Time (Operations	
Invite	Charning C	2in Staff	1787 52@163.com Ha	s been sent 2022-10-11 10:21:48.1	2 0	

Figure 10-31 Send an invitation E-mail 2

Visitor Registration:

Visitors who have received the invitation will receive an email as follows, then the visitor click **Click here** to register as a visitor.



Figure 10-32 Invitation E-mail

Rese	rvation Details	
	0	
First Name	First Name	
Last Name	Last Name	
Mobile Phone	Mobile Phone	
Email	Email	
Gender		
Certificate Type	a	
Certificate No.	Certificate No.	
Audit Status	Audit Status	Sec. In
License Plate		E.
Visit Reason		

Figure 10-33 Visitor Registration

Visitor Reservation Audit:

When a visitor submits registration information, host will receive a review email as shown below:

Click **Review** if you agree to make an appointment;

Click **Refuse** if you refuse the appointment.

	Reservation Details
First Name	Ning
Last Name	Wang
Mobile Phone	17: 52
Email	Email
Gender	
Certificate Type	D
Certificate No.	133650
Audit Status	Unreviewed
License Plate	
Visit Reason	Visit
Start Time	Oct 13, 2022 9:31:00 AM
End Time	Oct 13, 2022 11:59:00 PM
Review	Refuse

Figure 10-34 Visitor Reservation Audit

10.5 Basic Management

10.5.1 Parameters

In **Visito**r module Click **Basic Management** > **Parameter** to set the parameters.

Common Parameter Option	
Carrying Goods Capture	
Carrying Goods Capture Photo Exit Registration	
Open the Visitor Exit Function	
Automatic Sign Out <u>Set Automatic Sign Out Place</u> Viology exited from the set reader, will be automatically checked out	
Sign Out Expired Visitors The invalid Visitors that having not been checked out manuality, will automatically be checked	
out/performed every 30 minutes).	
Sign Up Enable automatic sign-in function Set automatic sign-in location immediately	
Support the QR code (face) from the set reader to sign in, and sign in will be performed automatically.	
Permission O Without Permission	
Permission is Required Whether to issue Card Ze Password is Required	
Scan Code is Required	
Select the Required Field YostVristed Visit Department	
Visitor Vehicle Authorization Mode	
O Temporary Vehicle	
Normal Parameter Option	
Kormal Parameter Option	
Capture	
C capture the Dorinal and Certificate Privo Together ⊙ capture the Portnal and Certificate Privo Separately Visitor History Internation	
Open the Pop-Up Box to Display Visitor History Information	
Copy ID Number as Card Number Automatically	
Copy ID Number as Card Number	
WatchList Option C On Entry Prompt If Name Matche	
Match Type firstName Only	
 On Enhy Match by Certificate On Enhy Match by Country Region 	
On Entry Match by Company	
Maximum visitor check	
Maximum number of visits 100	
Open single-day single-person maximum visitor visits monitoring Maximum number of visits [30	
Registration Client	
Device Driver	
Certificate Recognition Driver Installation Status: Detected Certificate Recognition Driver is not Installed	
Certificate Recognition	
OCR Oldereder Registration Code*	
Rogister	
Download OCR V10 Driver Opunload OCR V2.0 Driver Certificate No. Automatic Backfill Type	
Document No. Personal No.	
The Visitor List the Recipient Mailbox	
Send the visitors information during the day by email. Sending Time:	
15 • 30 •	
Example 123@xxx.com,456@xxx.com	
Enter multiple mailboxes, separated by commas() or semicolons().	
Visitor Autonomous Registration	
Enable the declaration of health information:	
 Yes Ho Enable automatic review of guest appointments: 	
Ves 🛞 No	
QR code Urt: https://cvidemo.vmtkteco.com/app/r1/MaRes	
Download OR code image	
OK	
Visitors Quantity Statistics: Check-In Today 3 Check-Out Today 3 Not Check-Out Today 0 View the Details	

Figure 10- 35 Parameter

Common Parameter Option:

Carrying Goods Capture: Enable it to take the photo to the goods carried by the visitor.

Exit Registration: Enable or disable the auto sign-off function. Auto sign-out means a visitor leaves by directly punching a card or using his/her fingerprint at the preset auto sign-out place, without performing the Exit Registration operation in the software. Setting automatic sign-out place means specifying some readers as the auto sign-out place. Click **Set Automatic Sign Out Place**. Then click **OK** to finish.

Automatic Exit Place		×	
Access		•	
Automatic Exit Place CL63202960014(ZKT_Korea-1-Out) COKC220260046(Speedface-M4-夏门SI- 1-In)	<u>New</u> <u>Select All</u> <u>Deselect All</u>		
Check-in location and check the same OK Car		•	

Figure 10- 36 Automa<mark>tic Exi</mark>t Place

Sign Out Expired Visitors: Expired visitors who have not been manually signed out will be automatically signed out after a specified interval.

Permission:

Whether to Issue Card: Whether to issue card for the visitor.

Fingerprint Registration is Required: Whether to register the fingerprint for the visitor.

Password is required: If selected, it will make password mandatory.

Scan Code is Required: If selected, it will code scan mandatory

Select the Required Field: You can set whether the Host (Personnel) and visited departments would be required in the registration page and the reservation page.

Visitor Vehicle Authorization Mode: You can set this option as per the reliability of the vehicle. If you want to make all vehicle details to be noted, then select Temporary Vehicle. If only one or some vehicle enters on a regular basis, then you can keep them in whitelist.

Normal Parameter Option:

Capture: Whether to capture the portrait and certificate photo together.

Visitor History Information: You can select the display parameters of the visitor history. Selecting the Open the Pop-Up Box to Display Visitor History Information check box displays the visitor information with photo and fingerprint of the visitor (These two will be auto-selected).

Copy ID Number as Card Number Automatically: Enable this if you want to use the same ID number as the Card number.

WatchList Option:

Select the Watchlist parameter as given below:

- On Entry Prompt if the Name matches. It can be first name only or Last name First name.
- On Entry Match by the certificate provided by the visitor.
- On Entry Match by the Country/Region of the visitor.
- On Entry Match by the Company of the visitor.

Maximum visitor check: You can define the parameters to limit the number of visitors and the number of visit times.

Note: When the number of visitors reaches the default upper limit set on the day, a prompt will pop up when entering the registration page:

Registration Client:

Step 1: If there is no driver installed in the system, the **Download Driver** link is displayed. Click the link to download and install the driver.

Registration		
	Device Driver	
	Certificate Recognition Driver Installation Status: Detected Certificate Recognition Driver is not installed	
	Certificate Recognition	
	OCR O IDReader	
	Registration Code*	
	· · · · · · · · · · · · · · · · · · ·	
	Register	
	Download OCR V1.0 Driver O Download OCR V2.0 Driver	
	Certificate No. Automatic Backfill Type	
	Document No. Personal No.	

Figure 10-37 Registration Client

Step 2: Enter the corresponding registration code and click Register.

Note: Click System > Authority Management > Client Register to view the registration code.

The Visitor List the Recipient Mailbox:

Configure the recipient's mailbox and the time for system to send the list of visitors today.

Send the visitors in	nformation during	the day by email.	ending Time:
15	•	30	*
Example:123@xxx.con	n;456@xxx.com		
15			

Figure 10- 38 Visitor List the Recipient Mailbox

Visitor Autonomous Registration:

Enable or disable the declaration of visitor's health information and automatic view of guest appointments.

10.5.2 Device Debugging

Device Debugging option will provide information about Entry Place, Print installation, Device Driver installation, and USB Camera.

In **Visito**r module Click **Basic Management** > **Device Debugging** to know about the current location details (including IP address), Printer-driver installation information, device driver installation, calibrate the scanners, and USB camera information.

Entry Place	e	
	Current Location	
	Place Name: BLR	
	IP Address: 127.0.0.1	
	Picture Collection Device: USB Camera Document Collection Device: USB Camera	
	Jocarion Concellen Device. USB centere	
		_
Print contro	ol	
	The print control is not installed: Download the printer driver, please restart the browser after the print driver is	1
	installed	
Device		
Device		
	Device Driver	
	Device Driver Installation: Device Driver is properly installed.	
	Other Scanner	
	Scanning Recalibrate	
	For the first time, the scanner must be calibrated; the scanned image is not clear, and the repair can be attempted.	
	High-Speed Portable HD Doc Scanner	
	Parameters	
	Size Setting	
	Resolution	
	Open Close	
	High-Speed Portable HD Doc Scanner belongs to camera components, if prompted to open High-Speed Portable HD Doc Scanner failure, please check whether if has been opened as a camera.	
	A High-Speed Portable HD Doc Scanner will be reopened after the resolution change, if prompt preview failed,	
	please open it manually! USB Camera	
	USB Camera	
	USB Camera	
	Open Close	
	M When the camera is occupied, please check if it is used by other browsers or programs; If at the same time using High-Speed Portable HD Doc Scanner, please check whether the use of camera	

Figure 10-39 Device Debugging Interface

Parameter	Description
Entry Place	Displays the information of the current entry place, such as the name of the entry place, IP, Mode of picture/document collection.
Print Control	It shows the Printer-driver installation information
Device	Display device driver installation, you can debug, calibrate the scanner. Set the High-Speed Portable HD Doc Scanner parameters, and information of USB camera. (IE browser does not display USB device debugging).
	Table 10-8 Description of Parameters of Device Debugging

10.5.3 Print Settings

In **Visito**r module Click **Basic Management** > **Print Setting** to go to the printer settings.

Global Settings (Receipt Printer):

Select **Receipt Printer** to set the global setting of the printer.

Select Printer	Туре	
	Receipt Printer Card Printer	
Global Setting	gs	
Global Setting		
Global Setting	gs Template Selection	
Global Settin		
Global Settin	Template Selection	
Global Settin	Template Selection Visitor receipt	

Figure 10- 40 Global Settings of Printer

Parameter	Description
Template Selection	Select a template to print the template, if the template does not meet the print content, you can add or edit the template (the default template cannot be edited, deleted). Available Templates are Visitor Receipt, Visitor Print Card and Visitor Print Card (Horizontal).

Table 10-9 Description of Parameters of Printer Setting

Local Settings (Receipt Printer):

You can set the options for the printer, the type of paper to be printed, or the custom paper size, and view the effect by clicking Print Preview / Direct Print. At last, you can save the current setting for the printout of the visitor badge.

Print control	
The print control is not installed: <u>Download the printer driver</u> , please restart the brow	vser after the
print driver is installed	
Use Printer	
Select Paper Type	
Paper Type	_
The paper type can only use the system default types. Please check in the print prev will work.	riew to see if it
O Custom Paper Size	a lite
Custom Paper Width	
71	mm
Custom Paper Height	
140	mm
Custom Paper Width, Highly Adaptive	
Custom Paper Width	
71	mm

Figure 10-41 Local Settings of Printer

Parameter	Description					
Use Printer	Select the printers from the available list of printers.					
Paper Type	Select the Paper Type					
Custom Paper Size	You can customize the paper size like paper height and width.					
Table 10- 10 Description of Parameters of Local Settings of Printer						

Card Printing:

In the parameter setting interface, you can set the parameters of card. Initially, define the template (refer to personnel card printing), and then set the card printing function. If the automatic card printing is selected, printer connection is required. After the visitor registration is completed, user can print the card directly.

	 Receipt Printer Card Printer 		
Global Settings			
	Template Selection		
	Visitor receipt	•	
	Preview		
	Visitor Card Printing Setting		
	Print Card after the visitor Checked-In		
Local Settings			Er
	Use Printer		
		•	

Figure 10- 42 Printer Setting of Card Printer

Parameter	Description
Template Selection	Select a template to print the template, if the template does not meet the print content, you can add or edit the template (the default template cannot be edited, deleted). Available Templates are Visitor Receipt, Visitor Print Card and Visitor Print Card (Horizontal).
Visitor Card Printing Setting	Select the visitor card printing settings (like after visitor check in)
Use Printer	Select the printer from the available list of printers.
le la	Table 10- 11 Description of Parameters of Printer Setting of Card Printer

10.5.4 Visitor Levels

The visitor can be allocated Access or Elevator levels within registration after the visitor level has been set.

In Visitor interface Click Basic Management > Visitor Levels:

Visitor / Basic Management / Visitor Levels	
Edit the Visitors for Authorization Group	< Browse Levels General (Access) opening visitors
Level Name Belongs Module Q Q	Name More + Q 2
⊖ Refresh 🔄 Add permission group 👻 💼 Delete	C Refresh
Level Name Belongs M Visitor Count Operations	Visitor Code First Name Last Name Card Number
General Access 0	

Figure 10-43 Visitor Level Interface

10.5.4.1 Add Permission Group

In this option you can give access, elevators, and entrance control permissions to the visitors

Add Access Levels

To add Access Levels.

Operating Steps:

Step 1: In the Visitor Module, click Basic Management > Visitor Levels > Add Access Levels

		Add Access Level(s)	×
Level Name	Q @		
Alternative		Selected(0)	
Level Name	Access Control Time Zone	Level Name Access Control Time	e Zone
test	24-Hour Accessible		
multibio	multibio	>>	
K-Test	24-Hour Accessible	× <	
		No data	
< < 1-3 >	>I 50 rows per page ♥		
		OK Cancel	

Figure 10- 44 Add Access Level Interface

Step 2: Set a visitor level name, select one or more access levels, click > or >> to move into the Selected menu. Click **OK**.

Step 3: Allocate the Access levels for the visitor when registering.

• Add Elevator Levels

To add Elevator Levels.

Operating Steps:

Step 1: In the Visitor Module, click Basic Management > Visitor Levels > Add Elevator Levels.

	Add Elevator Level(s)	×
Level Name		
Alternative	Selected(0)	
Level Name Elevator Contorl Time Zone	Level Name Elevator Contorl Time Zone	
No data	>> < << No data	
I< < 0 > >I 50 rows per page ❤	OK Cancel	

Figure 10-45 Add Elevator Level Interface

Step 2: Set a visitor level name, select one or more access levels, click >>> or >>>> to move into the Selected menu. Click **OK**.

Step 3: Allocate the Elevator levels for the visitor when registering.

Add Entrance Control Level

To add Entrance Control Levels.

Operating Steps:

Step 1: In the **Visitor Module**, click **Basic Management** > **Visitor Levels** > **Add Entrance Control Level**

Step 2: Set a visitor level name, select one or more access levels, click >>> or >>>> to move into the Selected menu. Click **OK**.

Step 3: Allocate the Elevator levels for the visitor when registering.

	Add Entrance Control Level(s)	×
Level Name general Q		
Alternative	Selected(0)	
Level Name	Level Name	
No data	>> < </td <td></td>	
I< < 0 > >I 50 rows per page ❤	OK Cancel	

Figure 10-46

Figure 10-41 Add Entrance Control Level Interface

10.5.4.2 Delete Levels

In the **Visitor** module, click **Basic Management** > **Visitor Levels**, select a visitor level and click **Delete** to delete the visitor level.

	ZKBio CVSecurity		æ					
Ð	Visitor Registration >	Visitor	/ Basic Manager	ment / Visitor Lev	vels			
E	Visitor Reservation >	Edit th	ne Visitors for Au	thorization Grou			٠	Browse Levels G
G	Basic Management 🗸 🗸	Lev	el Name		Belongs Module -	Q @		Name
	Parameters	0	Refresh =+ Ac	dd permission gr	oup = 🖬 Delet			C Refresh
	Device Debugging		Level Name	Belongs M	Visitor Count	Operations		Visitor (
	Print Settings		General	Entrance Con	t 0	<u>음</u> +		
	Visitor Levels		General	Access	0	<u>8</u> +		
	Visitors common permission group							
	Host Levels							
	Visited Department Levels							
	Entry Place						Prompt	
	Visit Reason	«					Are you sure you want to perform the del	ate
	Custom Attributes						operation?	
							OK Cancel	

Figure 10- 47 Delete Level Interface

Click **OK** to perform the delete operation.

10.5.4.3 Add Visitors to Levels (Browse Level)

Adding visitors to levels

Operating Steps

Step 1: In the **Visitor** module, click **Basic Management** > **Visitor Levels**.

Step 2: Select the Visitor name click on the icon ² under the operation categories.

Step 3: Select one or more visitors, click >> or >> to move into the Selected menu. Click OK.

TKBio CVSecurity	······································
Visitor Registration >	Visitor / Basic Management / Visitor Levels
Visitor Reservation >	Edit the Visitors for Authorization Group Control Cont
Ca Basic Management ~	Level Name Belongs Module — V Q Q
Parameters	C Refresh 🛱 Add permission group 🕆 🖹 Delete C Refresh 🛱 Remove the Visitors
Device Debugging	Level Name Belongs M Visitor Count Operations
Print Settings	test Access 0 🛃
Visitor Levels Visitors common permission	multiblo Access 0 Add Visitors X
group	K-Test Access 1 Personnel ID First Name More Q Q
Host Levels	General Entrance Cont 1
Visited Department Levels Entry Place	General Access 0 Alternative Selected(0) Selected(0) Selected(0) Selected(0) Selected(0)
Visit Reason	800000008 test123 72504260
Custom Attributes	× • • • • • • • • • • • • • • • • • • •
	ee Noda
	No data
	IC C 1-1 > >I 50 rows per page *
	OK. Cancel

Figure 10- 48 Add Visitor Interface

Step 4: After clicking OK the processing window will appear like Figure 10-49 shows below.

Total Draggers		
Total Progress	100%	
Start processing Complete		

Figure 10-49 Processing Command Interface

10.5.4.4 Remove Visitors from Browse Level

Removing visitors from the levels.

Operating Steps:

Step 1: In the Visitor Module, click Basic Management > Visitor Levels

Steps 2: Select the visitor details to be deleted, Click Remove the Visitor as shown in Figure 10-50.

ZKBio CVSecurity

TZKBio CVSecurity	::: ¥										
Visitor Registration >	Visitor / Basic Manager	ment / Visitor Level	Is								
Visitor Reservation >	Edit the Visitors for Au	thorization Group				К В	Browse	Levels test (Ac	cess) opening	visitors	
🔓 Basic Management 🗸 🗸	Level Name	в	elongs Module	α @			Name		More	- Q Q	
Parameters	⊖ Refresh 📑 A	d permission grou	p 👻 💼 Delete				O Re	efresh 🗊 Rei	move the Visito	rs	
Device Debugging	Level Name	Belongs M	Visitor Count	Operations				Visitor Code	First Name	Last Name	Card Number
Print Settings	🗆 test	Access	3	음 *				80000008	test123		72504260
Visitor Levels	multibio	Access	0	≗ ⁺				800000018	test456		72503190
Visitors common permission group	K-Test	Access	1	≙ +				800000019	test456		72503190
Host Levels	General	Entrance Cont	1	음 +							
Visited Department Levels	General	Access	0	≗ ⁺							
Entry Place					Prompt		1				
Visit Reason	«				Are you sure you want to perform t	he delete					
Custom Attributes					operation?						
					OK Cano	cel					



Figure 10-45 Remove Visitors from Browse Level

Step 3: Click OK to perform the delete operation.

10.5.5 Visitor Common Permission Group

This interface displays a list of all visitor permission groups in the visitor system. After setting up the visitor permission group, you can assign access control/passage/witness permission to visitors when registering visitors.

10.5.5.1 Add Permission Group

In this option you can give access, elevators, and entrance control permissions to the visitors.

Add Access Level

To add Access Level Group

Operating Steps:

Step 1: In the Visitor module, select Basic Management > Visitor Common Permission Group.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Access Level**, and then add the corresponding permissions.

1	Add Entrance Control Level(s)	
Level Name Q		
Iternative	Selected(0)	
Z Level Name	Level Name	
General		
	>>	
	•	
	<	
	<< No data	
	NO GAIL	
(< < 1-1 > >) 50 rows per page ▼		
	OK Cancel	

Figure 10-51 Visitor Permission Group Adding Interface

Set a visitor level name, select one or more access levels, click >>> or >>>> to move into the Selected menu. Click **OK**.

Step 3: In the **Visitor** module, select **Visitor Registration** > **Entry Registration** interface, and click **Entry Registration** to assign personnel visitor permissions.

			New			×
Host/Visited * Certificate Type* First Name* Company Country/Region Email	Enter the Query Co Q ID	Visit Department * Certificate No.* Last Name Mobile Phone Visitor Quantity*	· · · · · · · · · · · · · · · · · · ·	Visit Reason* Entrance* Gender License Plate Carrying Goods	Visit • 1 •	
Permission Visitor Level Card Number	· · · · · · · · · · · · · · · · · · ·	Start Time*	2021-12-20 11:35:08	End Time*	2021-12-20 23:59:59	
Capture Any exposure to succeed cases City visited in past ays Remarks on health	Yes No]	Any symptoms in the st 14 days Body Temperature(°C °F)	None Cough		
		Save and New	ОКСа	ancel		

Figure 10- 52 Visitor Add Visitor Permission Interface

Add Elevator Level

To add Access Level Group

Operating Steps:

Step 1: In the Visitor module, select Basic Management > Visitor Common Permission Group.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Elevator Level**, and then add the corresponding permissions.

	Add Elevator Level(s)	×
Level Name Q		
Alternative	Selected(0)	
Level Name Elevator Contorl Time Zone	Level Name Elevator Contorl Time Zone	
No data	>> < << No data	
I < 0 > >I 50 rows per page ▼		
	OK Cancel	

Figure 10-53 Visitor Permission Group Adding Interface

Set a visitor level name, select one or more access levels, click >>> or >>> to move into the Selected menu. Click **OK**.

Add Entrance Control Level

To add Access Level Group

Operating Steps:

Step 1: In the Visitor module, select Basic Management > Visitor Common Permission Group.

Step 2: In the Visitor Permission Group interface, click **Add Permission Group**, select **Add Entrance Control Level**, and then add the corresponding permissions.

Level Name Q		
liternative	Selected(0)	
Z Level Name	Level Name	
🔽 General		
	>>	
	> < <<	
	<	
	No data	
< < 1-1 > > 50 rows per page →		
IC C 141 9 91 So tows per page 9		
	OK Cancel	

Figure 10- 54 Visitor Permission Group Adding Interface

Set a visitor level name, select one or more access levels, click > or >> to move into the Selected menu. Click **OK**.

10.5.5.2 Delete Levels

In the Visitor Module, click Basic Management > Visitor Common Permission Group, select a visitor level and click Delete to delete the visitor level.

TZKBio CVSecurity		
Visitor Registration >	Visitor / Basic Management / Visitors common permission group	
Visitor Reservation >	Edit the Visitors for Authorization Group	Brow
Basic Management ~	Level Name Belongs Module Q	N
Parameters	⊖ Refresh 🔄 Add permission group 👻 💼 Delete	C
Device Debugging	Level Name Belongs M Visitor Count	
Print Settings	K-Test Access 0	
Visitor Levels	General Access 0	
Visitors common permission group		
Host Levels		
Visited Department Levels		
Entry Place	Prompt	
Visit Reason		
Custom Attributes	Are you sure you want to perform the de operation?	lete
	Cancel	

Figure 10- 55 Delete Level Interface

Click **OK** to perform the delete operation.

10.5.5.3 Remove Visitors from Browse Level

Operating Steps:

Step 1: In the Visitor Module, click Basic Management > Visitor Common Permission Group

Step 2: Select the visitor details to be deleted, Click **Remove the Visitor**.

TRANSPORTATION	::: ¥			
Visitor Registration >	Visitor / Basic Management / Visitors common permission group			
Usitor Reservation	Edit the Visitors for Authorization Group	٠	Browse Levels General (Access) opening visitors	
🤤 Basic Management 🗸 🗸	Level Name Belongs Module		Name More + Q Ø	
Parameters	C Refresh Ξ+ Add permission group ∞ 💼 Delete		C Refresh 🛍 Remove the Visitors	
Device Debugging	Level Name Belongs M Visitor Count		💟 Visitor Code First Name Last Name C	ard Number
Print Settings	General Access 1		800000018 test456 7:	2503190
Visitor Levels				
Visitors common permission group		Prompt	-	
Host Levels		Are you sure you want to perform the dele operation?	ite	
Visited Department Levels		OK Cancel		
Entry Place				
Visit Reason	•			

Figure 10- 56 Remove Visitors from Browse Level

Step 3: Click OK to perform the delete operation.

10.5.6 Host Level

After setting up the visitor permission group, you can set the visitor permission group according to the visited person or department in the Personnel module. After setting up, visitors who visit the visited person or department have this assigned permission by default.

10.5.6.1 Set Up Permission Groups by Interview (New)

This paper introduces the configuration Steps of setting permission groups according to the interview in.

Operating Steps:

Step 1: In the Visitor module, select Basic Management > Host Level.

Step 2: In the Setting Permission Group by Interviewee interface, click **New** to add interviewee information.

	New
Query Department Select all people Personnel ID Name	More - Q 🐼
Alternative	Selected(0)
Host Nu Host First Host Last Department .	Host Nu Host First Host Last Department
1 Soluction	>> < <No data
IC C 1-1 > >I 50 rows per page T	K Cancel

Figure 10- 57 New Interface for Interviewee

Step 3: After the new information is successfully added, click **Add Visited Levels** under operations. After the respondent adds the corresponding permissions, this permission group will be distributed to the visitor when the visitor registers, and the visitor will have the permissions possessed by this permission group.

Ad	d Visited Level(s)	×
Belongs Module Level Name	Q &	
Alternative	Selected(0)	
Level Name Belongs Module	Level Name Belongs Module	
No data	>> < << No data	
I< < 0 → >I 50 rows per page ▼	Cancel	

Figure 10- 58 Add Visitor Permissions Interface

10.5.6.2 Delete Levels

In the **Visitor** module, click **Basic Management** > **Host Level**, select a Host and click **Delete** to delete the Host level.

TZKBio CVSecurity	H #
Visitor Registration >	Visitor / Basic Management / Host Levels
Visitor Reservation >	Edit the access level for the host < Browse Personnel 666 (chen) From Levels
G Basic Management ~	Host Number Name More * Q Q Level Name Q
Parameters	C Refresh 👎 New 💼 Delete 🕼 Authorized exemption invitation C Refresh 🖨 Delete
Device Debugging	Host Nu Host First Host Last Department Na Authorized exe Operations
Print Settings	🖻 566 chen Department Name o 🦳
Visitor Levels	1 tang OP1 Department Name ø 🖗
Visitors common permission group	
Host Levels	
Visited Department Levels	
Entry Place	Prompt
Visit Reason	Are you sure you want to perform the delete
Custom Attributes	ve you sue you take to point the period
	OK Cancel

Figure 10- 59 Delete Level Interface

Click **OK** to perform the delete operation.

10.5.6.3 Authorized Exemption Invitation

To send authorized exemption invitation to the interviewee.

Operating Steps:

Step 1: In the Visitor module, click Basic Management > Host Level, select Interviewee

Step 2: Click **Authorized Exemption Invitation** and select **Yes** or **No** from the drop-down list as shown in Figure 10-60.

JZKBio CVSecurity	···· *	
Visitor Registration >	Visitor / Basic Management / Host Levels	
Uisitor Reservation >	Edit the access level for the host	Browse Personnel 666
🖀 Basic Management 🗸 🗸	Host Number Name More * Q Q	Level Name
Parameters	C Refresh ⊒ New 🖬 Delete 🔍 Authorized exemption invitation	🔾 Refresh 🗴 🗴 Del
Device Debugging	Host Nu Host First Host Last Department Na Authorized exe Operations	Level Name
Print Settings	🕎 666 chen Department Name 🧑 🖗	General
Visitor Levels	1 tang OP1 Department Name 🧑 🖗	
Visitors common permission group		
Host Levels		
Visited Department Levels	Exemption from review invitation authorization	n 🗙 🦯
Entry Place	Select interviewee* 666	
Visit Reason	«	
Custom Attributes	Authorized exemption Yes	-
	IIYYIdUVII	
	OK Cancel	

Figure 10-60 Authorized Exemption Invitation Interface

Step 3: Click OK to send authorized exemption invitation to the interviewee.

10.5.6.4 Remove Visited Host Level from Browse Level (Delete)

Removing visitors from the levels.

Operating Steps:

Step 1: In the Visitor module, click Basic Management > Host Level.

Step 2: Select the visited level details to be deleted, click Delete.

TZKBio CVSecurity	
Visitor Registration >	Visitor / Basic Management / Host Levels
Visitor Reservation >	Edit the access level for the host < Browse Personnel 666 (chen) From Levels
🔓 Basic Management 🗸	Host Number Name More * Q Q
Parameters	C Refresh ∓ New 🖹 Delete ③ Authorized exemption invitation C Refresh 🛱 Delete
Device Debugging	📄 Host Nu Host First Host Last Department Na Authorized exe Operations 🖉 Level Name Belongs Module
Print Settings	🗌 666 chen Department Name 🕢 🤌 🕎 General Access
Visitor Levels	1 tang OP1 Department Name 👳 🦻
Visitors common permission group	
Host Levels	
Visited Department Levels	
Entry Place	Prompt
Visit Reason	* Are you sure you want to perform the delete
Custom Attributes	Are you sure you Warff operiorm me deere operation?
	Cancel

Figure 10-61 Remove Visited Level from Browse Level

Step 3: Click OK to perform the delete operation.

10.5.7 Set Up Permission Groups by Visited Department (Visited Department

Level)

This paper introduces the configuration Steps of setting permission groups by department in.

10.5.7.1 Add Permission Group by Visited Department (New)

Operating Steps:

Step 1: In the Visitor module, select Basic Management > Visited Department.

Step 2: In the Setting Permission Group by Visited Department interface, click **New** to add the visited department.

		New		×
Select all department				
Department Number	Department Name		Q &	
Iternative			Selected(0)	
Visited Dep Visite	d Dep Parent Department		Visited Dep Visited Dep Parent Department	
2 Soluc	tion	_		
🗌 1 Depa	rtment Na	>>	-	
		<		
		<<		
			No data	
< 1-2 > >	50 rows per page 🔻			
	ОК		Cancel	

Figure 10-62 Add Department Interface

Step 3: In the interface of editing permission group for visited department, click Add Visited Level

under Operation. After adding the corresponding permission, when the visitor registers, this permission group will be distributed to the visitor, and the visitor will have the permission of this permission group.

Add	Visited Level(s)	×
Belongs Module Level Name	Q &	
Alternative	Selected(0)	
Level Name Belongs Module	Level Name Belongs Module	
No data	>> < << No data	
I< < 0 → >I 50 rows per page ▼	Cancel	

Figure 10-63 Add Department Permission Interface

10.5.7.2 Delete Levels

In the **Visitor** module, click **Basic Management** > **Host Level**, select a visited department and click **Delete** to delete the Host level.

TKBio CVSecurity	¥		
Visitor Registration >	Visitor / Basic Management / Visited Departme	ent Levels	
Visitor Reservation >	Edit the access level for the visited department	nt	< Brow
Ca Basic Management 🗸 🗸	Department Name	a @	μ
Parameters	🔾 Refresh 🛛 🛱 New 💼 Delete		c
Device Debugging	💟 Visited Dep Visited Dep Pare	ent Dep Operations	
Print Settings	🗾 9 test9	R	
Visitor Levels			
Visitors common permission group			
Host Levels			
Visited Department Levels			
Entry Place			Prompt
Visit Reason	«		
Custom Attributes			Are you sure you want to perform the delete operation?
			OK Cancel

Figure 10- 64 Delete Visited Department Interface

Click **OK** to perform the delete operation.

10.5.7.3 Remove Visited Department Level from Browse Level (Delete)

Removing visitors from the levels.

Operating Steps

Step 1: In the Visitor module, click Basic Management > Host Level

Steps 2: Select the visited Level details to be deleted, click Delete.

IZKBio CVSecurity		
Visitor Registration >	Visitor / Basic Management / Visited Department Levels	
Visitor Reservation >	Edit the access level for the visited department	< Browse Department 9 (test9) From L
🧟 Basic Management 🗸 🗸	Department Name Q Q	Level Name
Parameters	C Refresh ∓ New a Delete	🔾 Refresh 🔳 Delete
Device Debugging	Usited Dep Visited Dep Parent Dep Operations	Z Level Name Belo
Print Settings	🗆 9 test9 🔗	💟 General Acc
Visitor Levels		
Visitors common permission group	Prompt	
Host Levels	Are you sure you want to perform the delete operation?	
Visited Department Levels	Cancel	
Entry Place		

Figure 10-65 Remove Visited Level from Browse Level

Step 3: Click **OK** to perform the delete operation.

Only the registered platform (including PC platform and visitor plane) can register and sign off visitors.

This interface displays a list of all registered places in the visitor system. Displays fields such as enlistment location name, IP address, area name, and so on.

10.5.8.1 Non-Use Of Passenger Planes (New)

Introduces the configuration Steps of registering locations in ZKBio CVSecurity.

Operating Steps:

Step 1: In the **Visitor** module, select **Basic Management > Entry Place**.

Step 2: In the registration location interface, click **New** and select **Ordinary Computer** as the visitor machine type, as shown in Figure 10-66. Please refer to Table 10-12 for parameter description.

Place Name*	[]	
P Address*	127 0 0 1	
hysical information*	QkZFQkZCRkYwMDA5ME	
isitor Machine Type	Ordinary Computer 🔹	
Photo Collection	USB Camera 👻	
Document Collection	USB Camera 🔹	
Default permissions		
Area Name*		

Figure 10-66 Ordinary Computer Entry Place Interface

Parameter	Description
Name of Registration Place	Any character, no more than 50, not repeatable.
IP Address	Register the IP address of the computer used by the platform of visitor information and read the IP address of the local computer by default, which can be edited.
Physical Information	The physical information of the computer used by the platform for registering visitor information is automatically filled in by default and cannot be edited.
Type of Visitor Machine	By default, it is an ordinary computer. When connecting the visitor machine, select the visitor machine type: desktop visitor machine second generation, ID2000.
Photo Collection	Select the type of camera installed by customers, which is divided into USB camera, webcam, and dual-camera altimeter. Description: The server side of the box does not currently support external "dual camera high camera".
Certificate Collection	Select the certificate collection equipment installed by customers, which is divided into USB camera, altimeter, scanner, and dual-camera altimeter. Description: The box server does not support external "altimeter, scanner and dual-camera altimeter" for the time being.

Parameter	Description
Default Permissions	Select the default access rights for visitors registered at this level of location.
Area Name	Add the name of the area to which the registration place belongs, and the visiting registration record of each registration place will be filtered according to the area of the registration place

Table 10- 12 Description of Entry Place Parameters

10.5.8.2 Use Of Visitor Machine

Introduces the configuration Steps of registering locations in ZKBio CVSecurity.

Operating Steps:

Step 1: In the **Visitor** module, select **Basic Management > Entry Place**.

Step 2: In the registration location interface, click **New**, and select the visitor type as **Desktop Visitor Second Generation**, **ID2000**, as shown in Figure 10-62. Please refer to Table 10-12 for parameter description.

IP Address* 192 . 168 . 5 . 208 Physical information* MTc4QkZCRkYwMEE1ME Visitor Machine Type Ordinary Computer • Photo Collection USB Camera • Document Collection USB Camera •	Physical information* MTc4QkZCRkYwMEE1ME Visitor Machine Type Ordinary Computer Photo Collection USB Camera Document Collection USB Camera		New	×	
Physical information* MTc4QkZCRkYwMEE1ME Visitor Machine Type Ordinary Computer • Photo Collection USB Camera • Document Collection USB Camera •	Physical information* MTc4QkZCRkYwMEE1ME Visitor Machine Type Ordinary Computer Photo Collection USB Camera Document Collection USB Camera Default permissions Image: Computer Area Name* Image: Computer	Place Name*			
Visitor Machine Type Ordinary Computer Photo Collection USB Camera Document Collection USB Camera	Visitor Machine Type Ordinary Computer Photo Collection USB Camera Document Collection USB Camera Default permissions Image: Computer Area Name* Image: Computer	IP Address*	192 . 168 . 5 . 208		
Photo Collection USB Camera	Photo Collection USB Camera Document Collection USB Camera Default permissions Image: Collection Area Name* Image: Collection	Physical information*	MTc4QkZCRkYwMEE1ME		
Document Collection USB Camera	Document Collection USB Camera Default permissions Area Name*	Visitor Machine Type	Ordinary Computer	2	
	Default permissions Area Name*	Photo Collection	USB Camera 🔹		
Default permissions	Area Name*	Document Collection	USB Camera 🔹		
		Default permissions	•		
Area Name* 🗸	Test Connection	Area Name*	•		

Figure 10-67 Interface of Visiting Passenger Airline Entry Place

Parameter	Description
Name of Registration Place	Any character, no more than 50, cannot repeat.
IP Address	Register the IP address of the computer used by the platform of visitor information and read the IP address of the local computer by default, which can be edited.
Physical Information	The physical information of the computer used by the platform for registering visitor information is automatically filled in by default and cannot be edited.
Type of Passenger Plane	By default, it is an ordinary computer. When connecting the visitor, select the visitor type: desktop visitor second generation, ID2000.
Photo Collection	Select the type of camera installed by customers, which is divided into USB camera, webcam, and dual-camera altimeter. Description: The server side of the box does not support the external "dual-camera altimeter" equipment for the time being.

Parameter	Description
Certificate Collection	Select the certificate collection equipment installed by customers, which is divided into USB camera, altimeter, scanner, and dual-camera altimeter. Description: The box server does not support external "altimeter, scanner and dual-camera altimeter" for the time being.
Default Permissions	Select the default access rights for visitors registered at this level of location.
Area Name	Add the name of the area to which the registration place belongs, and the visiting registration record of each registration place will be filtered according to the area of the registration place

 Table 10-12 Description of Registration Location Parameters

10.5.8.3 Delete

Operation Steps:

Step 1: In the Visitor Module, click Basic Management > Entry Place, select the place name to be deleted.

Visitor Registration >	Visito	or / Basic Management / Entry Place	,					
Visitor Reservation >	Pla	ace Name	2 @					
🖹 Basic Management 🗸 🗸	C	Refresh 🖅 New 💼 Delete	🕲 Automatic Exit	Place				
Parameters		Place Name	IP Address	Area Name	Visitor Machin	Photo Collection	Document Coll IP Camera Na	Operations
Device Debugging		<u>H13A</u>	192.168.134.103	Area Name	FaceKiosk	USB Camera	USB Camera	_ ₪
Print Settings		BLR	127.0.0.1	Area Name	Ordinary Compute	USB Camera	USB Camera	2 🖻
Visitor Levels		PC Iberia	127.0.0.1	Area Name	Ordinary Compute	USB Camera	USB Camera	2
Visitors common permission group		test	192.168.134.68	Area Name	Ordinary Compute	USB Camera	USB Camera	_ ₪
Host Levels		server	127.0.0.1	Area Name	Ordinary Compute	USB Camera	USB Camera	
Visited Department Levels								
Entry Place						_	Prompt	
Visit Reason	æ						you sure you want to perform the delete	
Custom Attributes						Are	operation?	

Figure 10-68 Interface of Visiting Passenger Airline Entry Place

Step 3: Click OK to perform the delete operation.

10.5.8.4 Automatic Exit Place

To set automatic Exit place.

Operation Steps:

Step 1: In the **Visitor Module**, click **Basic Management > Entry Place**, click **Automatic Exit Place** option.

Step 2: Select the place to be set as automatic exist place and click OK.

Visitor Registration >	Visitor / Basic Management / Entry Place	Q @							
Basic Management 🗸 🗸	⊖ Refresh 🖅 New 🗴 Delete	@ Automatic Exit	Place						
Parameters	Place Name	IP Address	Area Name	Visitor Machin	Photo Collection	Document Coll	IP Camera Na	Operation	15
Device Debugging	<u>H13A</u>	192.168.134.103	Area Name	FaceKiosk	USB Camera	USB Camera		2 🖻	
Print Settings	BLR	127.0.0.1	Area Name	Ordinary Compute	USB Camera	USB Camera		2 🖻	
Visitor Levels	DC Iberia	127.0.0.1	Area Name	Ordinary Compute	USB Camera	USB Camera		_ 0	
Visitors common permission group	test	192.168.13 <mark>4</mark> .68	Area Name	Ordinary Comput		Automatic Exit I	Place	×	×
Host Levels Visited Department Levels Entry Place Visit Reason Custom Attributes	server	127.0.0.1	Area Name	Ordinary Comput		114(ZKT_Korea-1-In)	New Select All Deselect All Deselect All	not be 🗸	
				l		ок	Cancel		

Step 3: Click **New** to add place as automatic exit place and select the place reader name (Device place) from the appeared window. Click **OK** to save the data.

Reader name	Automatic Exit Place	
Alternative	Selected(0) Device serial Reader name	
CL63202960014 ZKT_Korea-1-Out	>> <	
I< < 1-1 > >I 50 rows per page ▼	No data	

Figure 10- 70 Add Place as Automatic Exit Place

Step 4: Repeat the step 2 to set the newly added place as automatic exit place.

10.5.9 Visit Reason

You can Add, Delete or Edit visit reason in this interface, so that you can select either from them at the entry registration page.

10.5.9.1 To Add Visit Reason (New)

Operation Steps:

Step 1: In the Visitor module, click Basic Management > Visit Reason > New.

	New	
Visit Reason*		

Figure 10-71 Add Place as Automatic Exit Place

Step 2: Click OK to finish.

10.5.9.2 Delete

Operation Steps:

Step 1: In the Visitor module, click Basic Management > Visit Reason, select visit reason to be deleted.

Step 2: Click Delete to delete the selected visit reason.

TZKBio CVSecurity	::: ¥		
Visitor Registration >	Visitor / Basic Management / Visit	Reason	
Visitor Reservation >	Visit Reason	Q @	
😰 Basic Management 🗸 🗸	C Refresh ∓ New 値 Del	ete	
Parameters	Visit Reason	Create Time Last Update Time	Operations
Device Debugging	Visit	2022-05-06 09:34:45 2022-05-06 09:34:45	5
Print Settings	visit1	2022-06-30 03:54:37 2022-06-30 03:54:37	7 _ 🖻
Visitor Levels			
Visitors common permission group			
Host Levels			
Visited Department Levels			
Entry Place			Prompt
Visit Reason			
Custom Attributes			Are you sure you want to perform the delete operation?
			Cancel

Figure 10-72 Delete Visit Reason

Step 3: Click **OK** to perform the delete operation.

10.5.10 Custom Attributes

If you want to add or delete a specific field on the registration page, then you can use this function.

10.5.10.1 To Add Custom Attributes (New)

In this interface you can add any specific field on the registration page.

Operation Steps:

Step 1: In the **Visitor Module**, click **Basic Management > Custom Attribute**s, click **New** to add a specific field on the registration page.

Step 2: Enter the Attribute name, select the field type as Pull down, Multiple Choice, Single Choice or Text.

If you select any of the type except Text, then you have to mention the attribute value(s). Use a semicolon to separate the values. Enter Row and Column as required and choose Yes or No according with requirement.

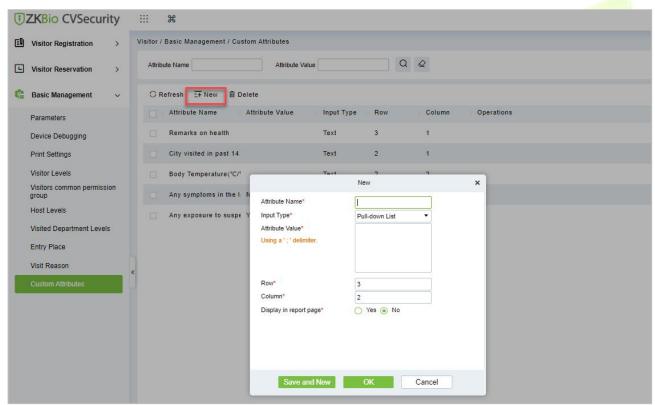


Figure 10-73 Custom Attribute Interface

Step 3: Click **OK** to add the attribute.

Parameter	Description		
Attribute Name	Enter the attribute name.		
Input Type	Select the input type from the drop-down list such as Pull down, Multiple Choice, Single Choice or Text.		
Attribute Value	Enter the attribute value. n attribute has multiple values, you can separate them with a semicolon. If you select text as input type of the attribute, then no need to add the attribute value.		
Row	Enter the row number as required.		

Parameter	Description		
Column	Enter the column number as required.		
Display in Report Page	If an attribute should be displayed on report pages, select Yes . Otherwise select No.		

Table 10-13 Description of Entry Place Parameters

10.5.10.2 Delete Custom Attributes

To delete customized attributes.

Operation Steps:

Step 1: In the **Visitor** module, click **Basic Management** > **Custom Attributes** and select the attribute to be deleted.

Step 2: Click Delete to delete a specific field on the registration page.

	ZKBio CVSecurit	y :		ж				
Ð	Visitor Registration	> Vi	(isitor / I	Basic Management / Custom Attributes				
C	Visitor Reservation	>	Attribu	te Name Attribute Value		Q «	2	
G	Basic Management	~	O Re	sfresh ∓ New 💼 Delete				
	Parameters			Attribute Name Attribute Value	Input Type	Row	Column	Operations
	Device Debugging			Remarks on health	Text	3	1	
	Print Settings			City visited in past 14	Text	2	1	
	Visitor Levels			Body Temperature(°C/°	Text	2	2	
	Visitors common permission group	n		Any symptoms in the I None;Cough;Fever;Re	Multiple Choic	1	2	
	Host Levels			Any exposure to suspe Yes;No	Single Choice	1	1	
	Visited Department Levels							
	Entry Place							Prompt
	Visit Reason	«						Are you sure you want to perform the delete
	Custom Attributes							operation?
								OK Cancel

Figure 10-74 To Delete Custom Attribute

Step 3: Click **OK** to perform the delete operation.

10.6 Advanced

10.6.1 Category

This interface allows you to add or delete the visitor category.

10.6.1.1 To Add New Visitor Category

Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Category** and click **New** to add a new category.

Step 2: Enter the type of category and remarks as shown in Figure 10-75.

TZKBio CVSecurity	::: ¥			
Visitor Registration >	Visitor / Advanced / Category			
Visitor Reservation >	Category Q			
Basic Management >	◯ Refresh 📴 New 🖬 Delete			
🕼 Advanced 🗸 🗸	Category Remarks	Operation	ns	
Calegory WatchList Watch List Thumbnails Alert Template Linkage	BOLO			
			New	×
	«		Type * Remarks	
			Save and New New 1	Close
			7	

Figure 10-75 Category Interface

Step 3: Click OK to save the data.

Parameter	Description		
Туре	Enter the type of category.		
Remarks	Enter the remarks about the category <mark>(Opti</mark> onal).		
	Table 10-14 Description of Category Parameters		

To Delete Category 10.6.1.2

Operation Steps:

Step 1: In the Visitor module, click Advanced > Category and select the category to be deleted.

ZKBio CVSecurity Ħ Visitor / Advanced / Category Usitor Registration 3 QQ Category L Visitor Reservation > Basic Management C Refresh ∓ New @ Delete 3 Z Category Remarks Operations Advanced BOLO WatchList Prompt Watch List Thumbnails Are you sure you want to perform the delete operation? Alert Template Cancel Linkage

Step 2: Click Delete and then click OK to perform the delete operation.



10.6.2 WatchList

Watch List interface displays the list of visitor information, and you can Add, Delete, Enable, or Disable the visitors.

10.6.2.1 To Add Visitor (New)

Step 1: In the **Visitor** module, click **Advanced** > **WatchList** and click **New** to add visitor.

Step 2: Enter the Visitor details such as Type, Full Name, Category, Certificate Type and Certificate Number.

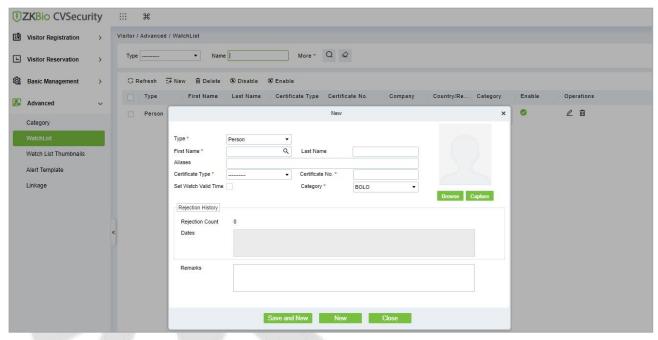


Figure 10-77 WatchList Interface

Step 3: Click Save and	New to save the details.
------------------------	---------------------------------

Parameter	Description
Туре	Select type from the drop-down list; Available types are Person, Company, Category/Country.
First and Last Name	Select visitor name using search icon. If you selected company as type, then enter the company name.
Aliases	You can enter the more familiar name of visitor if it needed.
Certificate Type	Passport, Driving License, ID Card, and Others are available to choose from the drop-down list. If the ID Scan OCR function is activated, visitor information will display automatically after clicking Region.
Certificate No.	The numbers and letters are legal; the max length is 20.
Category	Select the visitor category from the drop-down list.
Set Watch Time	You can set watch time for the selected visitor by clicking on the check box. Then enter the Start Date and end Date.
Rejection counts and Dates	Displays how many times the business rejected the visitor and rejected dates.

Table 10-15 Description of WatchList Parameters

10.6.2.2 Delete WatchList

Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **WatchList** and select the visitor watch list to be deleted.

Step 2: Click Delete to delete the selected watch list.

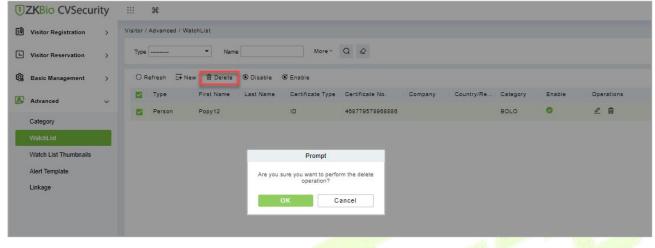


Figure 10-78 To Delete WatchList

Step 3: Click OK to perform the delete operation.

10.6.2.3 Enable WatchList

In **Visito**r module Click **WatchList** > **Advance**, select a blocked visitor, and click **Enable**.

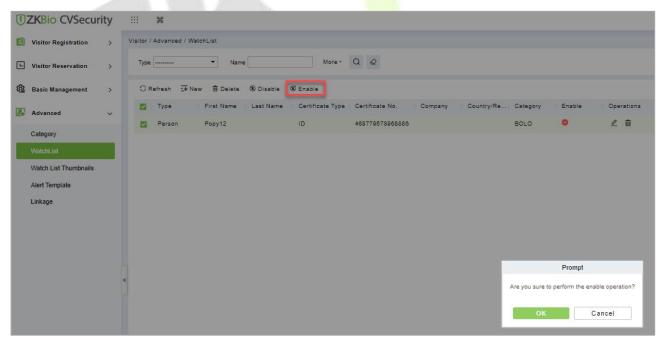


Figure 10-79 Enabling WatchList

Click **OK** to enable the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor's Watch list is enabled.

10.6.2.4 Disable WatchList

In Visitor module Click WatchList > Advance, select a visitor, and click Disable.

Usitor Registration Visitor / Advanced / WatchList Visitor Registration Visitor Reservation Visitor Reservation Percent Name More Refresh IF New IDelete Objection & Enable Type First Name Category WatchList WatchList WatchList WatchList WatchList WatchList Or Percent Popy12 ID 48077867806888 BOLO Pormpt Are you sure to perform a disable operation? OK	
Visitor Registration >	Visitor / Advanced / WatchList
	Type Name More + Q Q
Basic Management >	⊖ Refresh 📴 New 💼 Delete 🔞 Disable 🕏 Enable
Advanced Category Watch List Watch List Watch List Linkage Linkage	
Category	💆 Person Popy12 ID 488779578968886 BOLO 🖉 🖉 î
WatchList	
Watch List Thumbnails	Brownt
Alert Template	
Linkage	Are you sure to perform a disable operation /
	Cancel
	<

Figure 10-80

Figure 10-75 Disabling WatchList

Click **OK** to block the visitor. The enable entry for the corresponding selected visitor will show indicates the visitor's Watch list is blocked.

10.6.3 Watch List Thumbnails

Displays the thumbnail of watchlist person's image.

IZKBio CVSecurity	※ 発
Visitor Registration >	Visitor / Advanced / Watch List Thumbnails
■ Visitor Reservation >	Category Name More - Q @
Basic Management >	() Refresh
🛃 Advanced 🗸 🗸	ALC: NO DECISION OF THE OWNER OWNER OF THE OWNER OWNER OWNER OWNER OWNER OWNE
Category	
WatchList	
Watch List Thumbnails	Popy12
Alert Template	BOLO
Linkage	2022-08-29 00:00:00
	2022-06-30 23:59:00

Figure 10-81 WatchList Thumbnails Interface

10.6.4 Alert Template

This feature can add, edit the message templates. Different events have different template types. When a visitor reserved, checked in, checked out, reserved timeout, and visited timeout, the system will alert the visitor and the host via email or SMS.

10.6.4.1 To Add Alert Template (New)

Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Alert Template** and click **New** to add Alert Template.

Step 2: Enter the Details such as Template Name, Template Type, Event Type and Visitor Information.

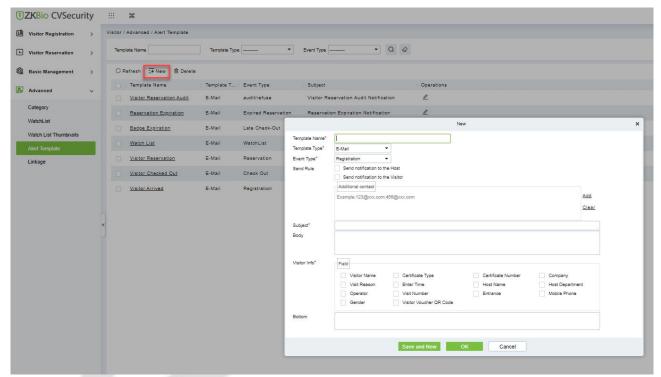


Figure 10-82 Alert Template Interface

Step 3: Click Save and New to save the alert template.

Parameter	Description
Template Name	Enter the Template Name
Template Type	Select template type such as E-mail or SMS.
Event Type	Select the event type from the drop-down list such as Registration, Reservation, Check-out, Watch List etc.
Send Rule	You can set the send rule by clicking on check boxes. By using this option admin can send notification to the Host as well as visitor about the events (like Registration, Check Out Timing, etc.). Admin can add additional Email in Additional Contact column.
Subject And Body	Enter the template's subject and message to send to the host or visitor.
Visitor Info	Admin can add visitor information like Visitor Name, Visit Reason, Certificate Type etc. by clicking on the check boxes.

Table 10-16 Description of Alert Template Parameters

10.6.4.2 Delete Alert Template

Operation Steps:

Step 1: In the **Visitor Module**, click **Advanced** > **Alert Template** and select the template to be deleted.

Step 2: Click **Delete** to delete the selected template.

ZKBio CVSecurity	::: ¥					
Visitor Registration >	Visitor / Advanced / Alert Template					
Visitor Reservation >	Template Name	Template Type	•	Event Type	• Q Ø	
😫 Basic Management >	O Refresh 🔤 New 🗃 Delete					
🛃 Advanced 🗸 🗸	Template Name	Template T	Event Type	Subject		Operation
	Visitor Reservation Audit	E-Mail		Prompt	udit Notification	2
Category WatchList	Reservation Expiration	E-Mail		vant to perform the delete peration?	on Notification	2
Watch List Thumbnails	Badge Expiration	E-Mail	ОК	Cancel	ification	2
Alert Template	Watch List	E-Mail			Notification	2
			-			n

Figure 10-83 To Delete Alert Template

Step 3: Click OK to perform the delete operation.

10.6.5 Linkage

This feature allows you to create a linkage function for each event. You can select the event, entrance and the Email template.

10.6.5.1 To Add Linkage

Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Linkage** and click **New** to add linkage.

Step 2: Enter Linkage name and select Entrance, SMS Template and E-mail Template.

Visitor Registration	> Vis	itor / Advanced	/ Linkage							
] Visitor Reservation	>	Linkage Name		Event Type	······ •	4				
Basic Management	>	O Refresh	F New 🗑 Delete	Oisable	& Enable					
Advanced	~	Linkage M	Va Event Type		E-Mail Template Name	SMS Template Nam	e En	able Og	perations	
Huvanceu	· ·	Check in	Registration	1	Visitor Arrived		0	6	2 💼	
Category		test1	Check Out		Visitor Checked Out		0	6	2 10	
WatchList		ind the					270			_
Watch List Thumbnails						New				×
Alert Template					Linkage Name*		Trigger Condition	on* Registration	•	
Linkage					E-Mail Template		Entrance			
	_				Name*					
					Name*					- 1
										- 1
										- 1
										_

Figure 10-84 Linkage Interface

Step 3: Click Save and New to save the details.

Parameter	Description
Linkage Name	Enter the Linkage Name.
Trigger Condition	Select trigger condition such as registration, reservation, check out etc.
Email Template	Select E-mail template from drop-down list.
SMS Template	Select SMS template from drop-down list.
Entrance	Select the Entry place.

Table 10-17 Description of Linkage Parameters

10.6.5.2 Delete Linkage

Operation Steps:

Step 1: In the **Visitor** module, click **Advanced** > **Linkage** and select the linkage to be deleted.

Step 2: Click **Delete** to delete the selected linkage.

TKBio CVSecurity			
Visitor Registration >	Visitor / Advanced / Linkage		
Visitor Reservation >	Linkage Name Event Type Q		
🙆 Basic Management >	C Refresh ⊒+ New 💼 Delete 🛞 Disable 🛞 Enable		
🕼 Advanced 🗸 🗸	Linkage Na Event Type E-Mail Template Name SMS Template Name	Enable	Operations
	Check in Registration Visitor Arrived	0	L û
Category WatchList	14511 Check Out Visitor Checked Out	ø	<i>∠</i> û
Watch List Thumbnails	Prompt		
Alert Template	Are you sure you want to perform the delete operation?		
	Cancel		

Figure 10-85 To Delete Linkage

Step 3: Click **OK** to perform the delete operation.

10.6.5.3 Enable Linkage

In the **Visitor** module, click **Advanced** > **Linkage**, select a blocked Linkage to enable that, and click **Enable**.

Visitor Registration	>	Visitor / Advanced / L	inkage					
Visitor Reservation	>	Linkage Name	Ev	ant Type Q	٥			
Basic Management	>	🔾 Refresh 📑 N	New 前 Delete 🛞 D	isable 🖲 Enable				
Advanced	~	Linkage Na	Event Type	E-Mail Template Name	SMS Template Name	Enable	Operations	
		Check in	Registration	Visitor Arrived		0	_ ₫	
Category WatchList		test1	Check Out	Visitor Checked Out		O	_ û	
Watch List Thumbnails				Prompt				
Alert Template				Are you want to perform the Enable operati	on?			
Linkage								

Figure 10-86 Enabling Linkage

10.6.5.4 Disable Linkage

In the **Visitor** module, click **Advanced** > **Linkage**, select linkage to be disable, and click **Disable**.

Visitor Registration	>	Visitor / Advanced / Linkage				
] Visitor Reservation	>	Linkage Name	Event Type	Q Q		
Basic Management	>	O Refresh <u>∓</u> New 💼) Delete 🖲 Disable 🛛	CEnable		
Advanced	~	Linkage Na Ever		E-Mail Template Name SMS	Template Name Enable	Operations
Category WatchList			istration ick Out	Visitor Checked Out	0	2
Watch List Thumbnails				Prompt		
Alert Template			Are you v	vant to perform the Disable operation?		

Figure 10-87 Disabling Linkage

Click **OK** to block the linkage. The enable entry for the corresponding selected linkage will show indicates the linkage is blocked.

10.7 Visitor Reports

10.7.1 Last Visited Location

In the **Visitor** module, click **Reports** > **Last Visited Location** to view the reports. The reports can be filtered by different conditions.

You can export the data into an Excel, PDF, or CSV file. See the following figure by clicking **Export** option.

Encrypt or not	🔿 Yes 🖲 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	 Selected (max 100000 records) 	
	Start Position 1	
	Total Records 100	

Figure 10-88 Export Option

Select file format and data to be export, then click **OK**.

Last Visited Location										
Visitor Code	First Name	Last Name	Event Date	Enter Time	Event Point	Event Description	Reader Name	Verification Mode	Area	Stay Time
80000020	usuop	SSS	2022-07-27 09:42:13	2022-07-27 09:41:24	10.10.20.73-1	Normal Verify Open	10.10.20.73-1- In	Only Pin	Area Name	00:00:48

Figure 10-89 Last Visited Location Record

10.7.2 Visitor History Record

In the **Visitor Module**, click **Reports** > **Visitor History Record** to view the reports. The reports can be filtered by different conditions.

TZKBio CVSecur	rity	333	Ħ												
Usitor Registration	>	Visitor / F	Reports / Visito	or History Record											
Visitor Reservation	>	Entry ti	me from 2022-0	44-27 00:00:00 To 2022-07-2	7 23:59:59 Vi	sitor Code	More~ Q	Q							
Basic Management	>	O Re	fresh 🗃 De	lete 🛨 Export											
Advanced	>		Visitor Code	First Name Last Name	Visit Reason	Host Number	Host First Host Last	Visit Status	Card Number	Enter Time	Entrance	Exit Time	Exit Place	Carrying Good	. C:
			800000019	test456	Visit	1115	Zorro	Check-Out	72503190	2022-07-25 09:54	BLR	2022-07-26 02:00			
11. Reports	~		800000018	test456	Visit	1115	Zorro	Check-Out	72503100	2022-07-25 09:54	BLR	2022-07-28 02:00			
Last Visited Location			80000008	test123	Visit	9999	K-TEST	Check-Out	72504260	2022-07-25 08:55	BLR	2022-07-26 02:00			
Visitor History Record			800000010	jo	Visit	1119	multibio	Check-Out	72200956	2022-07-22 07:24	BLR	2022-07-22 07:24	BLR		
			800000009	ani	Visit	12135		Check-Out	72208200	2022-07-22 07:24	BLR	2022-07-22 07:24	BLR		
			80000008	test	Visit	12135		Check-Out	72209192	2022-07-22 04:12	BLR	2022-07-22 04:41	: BLR		
			800000007	www	Visit	1115	Zorro	Check-Out	72104066	2022-07-21 12:48	BLR	2022-07-22 02:00			
			80000005	RRR	Visit	12135		Check-Out	72100141	2022-07-21 11:49	BLR	2022-07-22 02:00			
			800000004	test	Visit	1119	multibio	Check-Out	62901816	2022-06-29 07:47	test	2022-07-01 02:00			
			80000003	Popy12	Visit	1119	multibio	Check-Out		2022-06-29 07:43	test	2022-08-29 07:50	test	手撮包	₹

Figure 10-90 Visitor History Record Interface

10.7.2.1 Export

You can export the records into an Excel, PDF, or CSV file. See the following figure by clicking **Export**.

	E	Export	>
Encrypt or not	🔿 Yes 🖲 No		
File Format	EXCEL		
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	ОК	Cancel	

Figure 10-91 Export Option

Select file format and data to be export, then click **OK**.

								Visito	or Histo	ory Re	cord								
Visitor Code	First Name	Last Name	Visit Reason	Host Number	Host First Name	Host Last Name	Visit Status	Card Numbe r	Enter Time	Entrance	Exit Time	Exit Place	Carrying Goods In	Carr ying Goo ds Out	Remark s on health	City visited in past 14 days	Body Temper ature(°C/°F)	Any sympto ms in the last 14 days	Any exposit re to suspect ed cases
800000 019	test456		Visit	1115	Zorro		Check- Out	725031 90	2022-07- 25 09:54:03	BLR	2022-07- 26 02:00:02								
800000 018	test456		Visit	1115	Zorro		Check- Out	725031 90	2022-07- 25 09:54:01	BLR	2022-07- 26 02:00:02								
800000 008	test123		Visit	9999	K- TEST		Check- Out	725042 60	2022-07- 25 08:55:34	BLR	2022-07- 26 02:00:02								
800000 010	jo		Visit	1119	multibio		Check- Out	722009 56	2022-07- 22 07:24:36	BLR	2022-07- 22 07:24:49	BLR							
800000	ani		Visit	12135			Check- Out	722082 06	2022-07- 22 07:24:18	BLR	2022-07- 22 07:24:49	BLR							
800000 008	test		Visit	12135			Check- Out	722091 92	2022-07- 22 04:12:48	BLR	2022-07- 22 04:41:36	BLR							

Figure 10-92 Visitor History Record

10.7.2.2 Delete Visitor History

Operation Steps:

Step 1: In the **Visitor** module, click **Reports** > **Visitor History Record** and select the visitor's history to be deleted.

Step 2: Click Delete to delete the visitor history.

	ZKBio CVSecuri	ty :		H					
▣	Visitor Registration	> V	isitor /	Advanced / Alert Templat	e				
E	Visitor Reservation	>	Temp	late Name	Те	emplate Type	•	Event Type Q	
¢	Basic Management	>	OR	lefresh ∓ New 🛅 D	elete				
2	Advanced	~		Template Name	Tem	iplate T	Event Type	Subject	Operations
	Category			Visitor Reservation Aud	lit E-M	lail	audit/refuse	Visitor Reservation Audit Notification	2
	WatchList			Reservation Expiration	E-M	lail	Expired Reservation	Reservation Expiration Notification	2
	Watch List Thumbnails			Badge Expiration	E-M	lail	Late Check-Out	Badge Expiration Notification	2
				Watch List	E-M	lail	WatchList	Watch List Matched Notification	2
	Linkage			Visitor Reservation	E-M	lail	Reservation	Visitor Reservation Notification	2
				Visitor Checked Out	E-M	lail	Check Out	Visitor Checked Out Notification	2
				Visitor Arrived	E-M	lail	Registration	Visitor Arrived Notification	2
						Prom	ıpt		
		<			Are you sure	e you want i operati	to perform the delete on?		
					ок		Cancel		

Figure 10-93 To Delete Alert Template

Step 3: Click **OK** to perform the delete operation.

11 Patrol Management

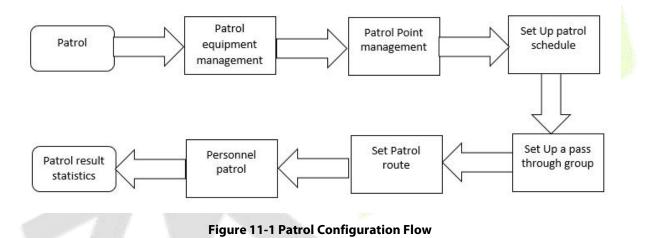
11.1 Operation Scenario

Patrol management business can realize the effective supervision and management of patrol personnel, patrol plan and patrol route by enterprise managers, and at the same time, it can also make regular statistics and analysis on patrol route and results.

11.2 Operation Flow

Introduce the configuration process of patrol management.

The patrol management configuration process is shown in Figure 11-1.



11.3 Patrol Route Monitoring

11.3.1 Patrol Monitoring

Displays all the scheduled routes in the patrol plan on the same day. When the patrol personnel patrol normally as planned, the patrol points in the corresponding patrol routes will turn green; If you don't patrol according to the rules, the patrol point will turn red. This interface is shown in the patrol monitoring interface, as shown in Figure 11-2. Refer to Table 11-1 for status description.



Figure 11-2 Patrol Monitoring

Parameter	Description
Normal Patrol	Personnel complete patrol in a normal time period according to normal sequence rules.
Wrong Patrol	The personnel completed the patrol within the normal time period but did not follow the regular route.
Leakage Patrol	The personnel did not complete the patrol within the normal time period, that is, one or part of the patrol points did not patrol.
Absence	Personnel has not completed the patrol within the normal time period, that is, the whole patrol route has not completed one patrol.
۲	The patrol route is wrong/missed.
۲	Normal patrol.
۲	Not patrolling.

Table 11-1 Patrol Status Description

11.4 Basic Settings (Patrol Basic Management)

11.4.1 Device Addition (Device)

11.4.1.1 Add device (New)

Select a device to be used as the patrol device from the access control devices. Click **Basic Management** > **Device** > **New**. In the **Alternative** box, add available devices and click **OK** to save the setting. The page is displayed as follows:

	New	×
Device Name		
Alternative	Selected(0)	
Device Name Device M Area Name Serie	ial Num Device Name Device M Area Name S	erial Num
☐ ZKT_Korea ProFace X[T Area Name CL6:	3320296001	
I< < 1-1 > >I 50 rows per page ▼		
	OK Cancel	

Figure 11-3 Add Device (New)

Precondition:

Before the patrol operation, it is necessary to add patrol device in the **Access Control** module and patrol personnel in the **Personnel** module.

Parameters	Instructions
Device Name	Customize the name of this device
Serial Number	Customize the device serial number.
Area Name	Divide the area for the device.
Device Model	Manufacturer of the device.

Table 11-2 Access Control

11.4.1.2 Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol group

11.4.1.3 Edit

Click a device name or Edit in the operation column to go to the Edit page. Make modifications and click OK to save modifications.

11.4.2 Checkpoint

11.4.2.1 Add Checkpoint (New)

Step 1: Click **Basic Management** > **Checkpoint** > **New**. The page is displayed as follows:

Checkpoint*			
Device Module*	Access Control	•	
Area Name [*]		•	
Device Name [*]		.	
Patrol Tag*			
Installation Position			

Figure 11-4 New Checkpoint

Step 2: After the setting (parameters with * are mandatory), click **OK** to save the setting. You can also click **Save and New** to save the current setting and add another checkpoint. Click **Cancel** to cancel the setting and return to the upper-level menu.

Parameters	Description
Checkpoint	Unique name which can identify a route.
Device Module	Displays the device number.
Area Name	It can support typing anything alphabet but can't typing the common.
Device Name	Manufacturer of the device.
Patrol Tag	Currently, only access control readers are supported
Installation Position	Set a suitable name for the position. Any character, maximum combination of 100 characters. Position names should not be repeated.
Operations	The patrol operation, it is necessary to add patrol device in the Access Control module.

Table 11-3 New Checkpoint

11.4.2.2 Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the checkpoint

11.4.2.3 Edit

Click a device name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

Note: Patrol tags that have been used by checkpoints cannot be used again when you add another checkpoint.

11.4.3 Parameters

Step 1: Click Patrol > Basic Management > Parameters.

Step 2: Set the interval for patrol statistics collection.

Step3: Click **OK** to save the setting.

Patrol Statistics		
	Automatically Calculate Report Interval:	
	30 🗸	minutes

Figure 11-5 Parameters

11.5 Patrol Management

11.5.1 Set Up a Patrol Plan

11.5.1.1 Add Plan (New)

Operating Steps:

Step 1: In the Patrol module, select "Patrol Management > Patrol Plan" and click New.

Step 2: In the **New** window that pops up, configure the patrol plan information, as shown in Figure 11-6, and describe the key parameters as shown in Table 11-1.

New	×
Plan Name* I Start Time* 00 : 00 ♀ Cross the Day ↔	
By Date O By Week O By Month	
By Date	
Start Date* 2021-12-20 End Date* 2021-12-20	
Save and New OK Cancel	

Figure 11-6 Patrol Plan

Parameter	Instructions
Time Period	You can set the time to be set in a day, or you can set it across days.
By Date	The patrol plan is scheduled daily. Check by Date to set the start date and end date of the patrol plan.
By Week	The patrol plan is scheduled on a weekly basis.
By Month	The patrol plan is scheduled monthly. There are two ways to implement the monthly plan: daily implementation or regular implementation. Choose the patrol plan to perform the patrol task every day in the selected month; If you choose to perform regularly, you will perform the patrol task within the specified date in the month.

Table 11-4 Parameter Setting Description

Step 3: Click OK.

Parameter	Instructions
Plan Name	Customize the Plan Name.
Cycle Type	Customize the Cycle Type.
Plan	A maximum of three patrol shifts can be added for a patrol plan.
Time Zone	This abnormal event is triggered if a user with the floor opening right punches his/her card beyond the effective periods

Operations The patrol operation, it is necessary to add patrol device in the **Access Control** module.

Table 11-5 Parameter Setting

11.5.2 Designated Patrol Personnel Group (Patrol Group)

11.5.2.1 Add Patrol Group (New)

Operating Steps:

Step 1: In the Patrol module, select "Patrol Management > Patrol Group" and click New.

Step 2: In the pop-up **New** window, configure the patrol personnel group information, as shown in Figure 11-5.

	New	×	
Patrol Group Name* Patrol mode*	 Any Person Verification All People Verification 		
Remarks			
Save and New	OK Cancel		

Figure 11-7 Patrol Personnel Group

Step 3: Click OK.

Step 4: Under the operation of the patrol group interface, click "Add Personnel".

Step 5: In the **Add Person** window that pops up, configure the person information, as shown in Figure 11-8.

atrol Group		Patrol Personnel
Patrol Group		Name ansh Q
CRefresh ☲ New 💼 Delete		🔿 Refresh 💼 Delete
Patrol Grou Patrol mode Remarks Operations		Add Person
ansh Any Person Ve 🖉 😫	Query O Department	
	Personnel ID Name	Department Name Q
	Alternative	Selected(0)
	📄 Perso First Last Department	Perso First Last Department
	1112 Anwar Hi Development	Í
	1111 Esha Tes Development	»
	1113 Abdulla Development	<
	1115 Zorro Development	<< No data
	Department Name	•
	I< < 1-18 > >I 50 rows per page ▼	

Figure 11-8 Adding Patrol Team Personnel

Step 6: Click OK.

11.5.2.2 Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol group.

Parameters	Instructions
Patrol Group	Click a patrol group from the list on the left. Personnel in the patrol group are displayed in the list on the right.
Patrol Mode	A patrol group cannot be edited or deleted when it is used by a patrol route.
Remarks	Custom Setting Notes Description.
Operations	The patrol operation, it is necessary to add patrol device in the Access Control module.
Personnel ID	Click Add Personnel under Operation in the list on the left. The page for adding personnel is displayed (or adding by department). Add personnel to the list on the right and click OK to finish the setting.
First Name/ Last Name	The maximum length cannot exceed 50, does not support comma; value sources Personnel field, cannot add, modify, delete.
Department Name	Select from the pull-down menu and click OK . If the department was not set previously, only one department named Company Name will appear.

Table 11-6 Delete Personnel

11.5.3 Set Up Patrol Routes (Route)

11.5.3.1 Add Route (New)

Operating Steps:

Step 1: In the Patrol module, select "Patrol Management > Patrol Route" and click Add.

Step 2: In the pop-up **Add** window, configure the patrol route information as shown in Figure 11-9 and Figure 11-10, and describe the key parameters as shown in Table 11-7.

Route Name*		
Plan Name*		
Limited Time*	0	minutes
Deviation*	0	minutes
Patrol Subject*	Select patrol personnel	Patrol Group

Figure 11-9 The First Step of The Patrol Route

R	loute Defin	ition		
Route Order Order V Checkpoint Area Name Q	8			
The ourrent query conditions: None Alternative		Select	sd(4) 🛉 🖡	
Checkpoint			Checkpoint	
	>> <			
I < < 0 > >I 50 rows per page * Total of 0 records				
Previous Step	Compl	ete	Cancel	

Figure 11-10 The Second Step of The Patrol Route

Parameters	Instructions			
Route Name	Customize the Route Name.			
Plan Name	Customize the plan Name.			
Patrol Subject	Select the patrol personnel.			
Checkpoint Order	In the patrol route, all checkpoints are 2 types of order and disorder routes.			
Limited Time	Set up the desired Limited Time.			
Deviation	Set up the required Deviation Time.			
Route Status	Displays the route status.			
Sort Type	Fill in the number of the superior department.			
Operations	The patrol operation, it is necessary to add patrol route in the Access Control module.			

Table 11-7 Second Step of Patrol Route

11.5.3.2 Delete

Select personnel in the list on the right and click **Delete** above the list to delete the personnel from the patrol route.

11.5.3.3 Enable/ Disable

Select device, click **Enable/Disable** 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.

Parameter	How to set
Error	Allowable error time setting for patrol. Assuming that the patrol plan is not 9:00-12:00, and the allowable error time is 5 minutes before and after, then the records in the period of 8:55-12:05 are valid records, and those beyond the above range

Parameter	How to set
	are invalid records, which will not be counted. As long as the patrol is not within the above time range, it is invalid.
Orderly Route	When carrying out the patrol plan, there is no time limit between the patrol points, and the patrol personnel can complete the patrol work of each patrol point in sequence according to their own habits within the limited time of the route.
Unordered Route	 Complete disorder: There is no order in all patrol points of the patrol route, and the patrol personnel can complete the patrol work of each patrol point within the total time limit according to their own habits. Disorder outside the first point: in the patrol route, other patrol points except the designated patrol starting point are disordered. Disorder outside the tail point: in the patrol route, other patrol points except for the last patrol point of the designated patrol route are disordered. Disorder outside the beginning and end points: In the patrol route, except for the first and last patrol points in the designated patrol route, other patrol point are disordered.

Table 11-8 Parameter Setting Description

Step 3: Click OK.

11.6 Result Validation(Patrol Reports)

In the patrol report, you can query the "All Records", "Patrol Records Today's", "Patrol Route Statistics" and "Patrol Personnel Statistics" report. You can choose to export all or export records after querying.

This paper introduces the configuration Steps of report query and export, taking the "all records" report operation as an example.

11.6.1 All transactions

Click **Reports** > **All transactions** to view all transactions, that is, all event records generated by the patrol device.

You can export all transactions into an Excel, PDF, or CSV file. See the following figure.

Operating Steps:

Step 1: In the Patrol module, select Report > All Records.

Step 2: In the All Records interface, fill in the corresponding query information and click the **Query** symbol to complete the query of all record tables, as shown in Figure 11-11.

Patrol / Patrol Reports / All Transactions		
Time 2021-09-20 00:00:00 To 2021-12-20 23:59:59 Person	nnel ID Device Name	Retract 🔺 📿 🖉
Name Route Name	Verification Mode 🔹	
Card Number Checkpoint	Area Name	

Figure 11-11 All Records

Step 3: In the full record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in Figure 11-12.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	*	
Data to Export	All (max 10000)	00 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	

Figure 11-12 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

					ZKT	ECO					
0017 00 1E 0	0 : 00 : 00 - 2017-12-	15 00 - 50 - 50			All Tran	isactions					
Time Time	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
017-12-15 13:53: 51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
017-12-15 13:53: 51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
017-12-15 13:53: 49	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53: 48	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53: 46	192.168.218.6D	7	Jacky	Xiang	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53: 46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 18	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 17	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 15	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 14	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 08	192.168.2 <mark>1</mark> 8.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 07	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53: 48	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53: 47	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53: 44	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53:	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	

Figure 11-13 Report Export File

Parameters	Instructions
Time	Set the start and end time in each time interval. Time period includes one week and three holiday-type time intervals.
Personnel ID	Displays the Personnel ID number.
Device Name	Manufacturer of the device.
Name	Select the desired name.
Route Name	Displays the Route name.
Verification Mode	You can set verification mode as following options: Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.
Card Number	The max length is 10, and it should not be repeated.
Checkpoint	Displays the Type of checkpoint.
Area Name	Customize the Area name.

Table 11-9 Report Export File

11.6.2 Patrol Records Today

Click **Reports** > **Patrol Records Today** to view event records generated by the patrol device today.

You can export patrol records today into an Excel, PDF, or CSV file. See the following figure.

-	D					ords Today	D		N		
Time 017-12-15 13:53:	Device Name	Personnel ID	First Name	Last Name	Card Number	Device Module	Route Name	Checkpoint	Verification Mode	Area Name	Remark
51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53: 51	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
017-12-15 13:53: 49	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53: 48	192.168.218.60	8	Glori	Liu	6189166	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 13:53: 46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint2	Only Card	Area Name	
2017-12-15 13:53: 46	192.168.218.60	7	Jacky	Xiang	6323994	Access	Route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 18	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 17	192.168.218.60	8	Glori	Liu	6189166	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 15	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 14	192.168.218.60	7	Jacky	Xiang	6323994	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:54: 10	192.168.218.60	5	Necol	Ye	13260079	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 08	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:54: 07	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53: 48	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53: 47	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	
2017-12-15 11:53: 44	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint1	Only Card	Area Name	
2017-12-15 11:53: 43	192.168.218.60	2	Lucky	Tan	6155266	Access	route1	checkpoint2	Only Card	Area Name	

Figure 11-14 Patrol Records Today

Parameters	Description
Personnel ID	Displays the Personnel ID number.
Card Number	Displays the Card Number.
Name	Select the required Name.
Device	Manufacturer of the device.
Verification Mode	Displays the Automatic Recognition, Fingerprint, PIN, Password, Card, Fingerprint/ Password, Fingerprint/Card, PIN+Fingerprint, Fingerprint+Password etc.
Route Name	Displays the Route name.
Checkpoint	Displays the Type of checkpoint.
Area Name	Customize the Area name.
Time	Set the start and end time in each time interval. Time period includes one week and three holiday type time intervals.
Remarks	Custom Setting Notes Description.

Table 11-10 Patrol Record Today

11.6.3 Patrol Route Statistics

Click **Reports** > **Patrol Route Statistics** to view all normal and abnormal situations collected during the patrol process.

You can export patrol route statistics into an Excel, PDF, or CSV file. See the following figure.

				ZKTECO Patrol Route Statistics				
Route Name	Plan Name	Statistics time	Supposed Patrol Times	Real patrol times	Missed patrol times	Wrong patrol number	Absence times	Patrol Subject
route 1	plan1	2017-12-15 13:30: 00	2	2	D	O	O	Amber Lin,Necol Ye,Jacky Xiang, Glori Liu,Lilian Me Jerry Wang,Berry Cao,Lucky Tan, Sherry Yang,Leo Hou,
Route1	plan1	2017-12-15 16:00: 00	2	2	O	1	0	Lucky Tan, Jerry Wang, Necol Ye Leo Hou, Sherry Yang, Lilian Mei, Berry Cao, Ambe Lin, Jacky Xiang Glori Liu,

Figure 11-15 Patrol Route Statistics

Parameters	Description
Route Name	Displays the required route name.
Plan Name	Displays the type of plan name.
Statistics time	Displays the Time and date of patrol route statistics.
Supposed Patrol Times	Number of times that the patrol personnel should normally patrol.
Real Patrol Times	Number of times that the patrol personnel patrol
Wrong Patrol Times	Number of times that the patrol personnel do not patrol based on the patrol route.
Missed Patrol Times	Number of times that the patrol personnel miss one or more checkpoints in the patrol route within the patrol time.
Absence Times	Number of times that the patrol personnel do not patrol.
	Table 11-11 Patrol Route Statistics

11.6.4 Patrol Personnel Statistics

Click **Reports** > **Patrol Personnel Statistics** to view patrol statistics of patrol personnel.

You can export patrol personnel statistics into an Excel file. See the following figure.

				Patrol Perso	nnel Statistics				
Personnel ID	Person Name	Route Name	Plan Name	Statistics time	Supposed Patrol Times	Real patrol times	Missed patrol times	Wrong patrol number	Absence times
4	Berry Cao	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
3	Leo Hou	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
8	Glori Liu	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
2940	Sherry Yang	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
6	Amber Lin	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
5	Necol Ye	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0
7	Jacky Xiang	route1	plan1	2017-12-15 13:30:00	2	2	0	0	0

Figure 11-16 Patrol Personnel Statistics

Parameters	Description
Supposed Patrol Times	Number of times that the patrol personnel should normally patrol.
Real Patrol Times	Number of times that the patrol personnel patrol
Wrong Patrol Times	Number of times that the patrol personnel do not patrol based on the patrol route.
Missed Patrol Times	Number of times that the patrol personnel miss one or more checkpoints in the patrol route within the patrol time.
Absence Times	Number of times that the patrol personnel do not patrol.

Table 11-12 Patrol Personnel Statistics



12 Entrance Control

12.1 Operation Scenario

This system connects the gate control board through channel Device (such as TDA integrated machine), and directly controls the relevant parameters of the gate through software, thus controlling the entry and exit of the gate and realizing the automatic management of the gate.

12.2 Operation Flow

Introduce the configuration process of channel service.

The channel business configuration process is shown in Figure 12-1.

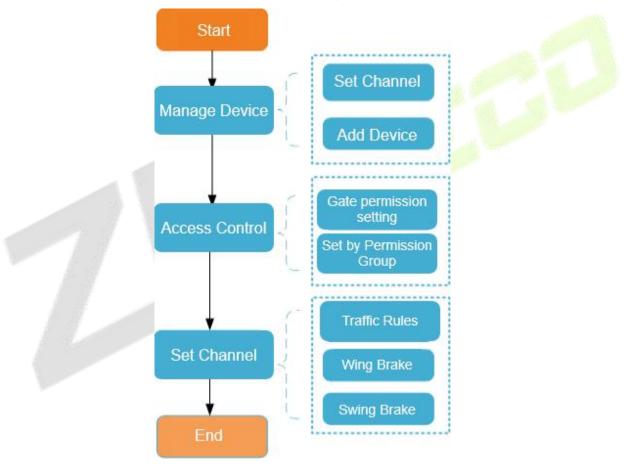


Figure 12-1 Channel Configuration Flow

12.3 Channel Device

Add channel integrated machine Device, and the integrated machine communicates with the gate control board through RS485 to control the gate

12.3.1 Passage

Setting the area to which the channel belongs is convenient for users to manage the channel Device in a specific area. After setting the channel, the Device under the channel can be filtered according to the area during real-time monitoring.

This paper introduces the Steps of creating and configuring channels in ZKBio CVSecurity.

12.3.1.1 To Add Passage (New)

Operating Steps:

Step 1: In the Entrance Control module, select Channel Device > Passage.

Step 2: In the channel interface, click **New** and fill in the relevant parameters, as shown in Figure 12-2. Please refer to Table 12-1 for parameter description.

Rank* Area Name Remarks	Passage Name*	[
	Rank* Area Name*	Area Name 👻	

Figure 12-2 New Channel Interface

Parameter	How to set
Passage Name	Any character, a combination of up to 20 characters, cannot be repeated.
Rank	Only numbers are supported, up to six digits, and repeatable. The smaller the ranking, in real-time monitoring, the display will move forward.
Area Name	Select the region to which the channel belongs.
Remarks	Any character with a maximum character length of 100.

Table 12-1 Description of New Channel Parameters

Step 3: Click **OK** to complete the channel setting.

12.3.1.2 Delete Passage

Operation Steps:

Step 1: In the **Entrance Control module**, select **Channel Device > Passage** and select the template to be deleted.

Step 2: Click Delete to delete the selected template Click OK to perform the delete operation

Channel device v	Entrance Control / Channel o	levice / Passage				
Passage	Passage Name	Q 4	2			
Device	O Refresh 🖅 New	🗊 Delete				
Gate Reader	Passage Name	Rank	Area Name	Remarks	Operations	
Auxiliary Input	Market State	102	Area Name		2	
Event Type	<u>123</u>	458	Area Name		_ ⊡	
Daylight Saving Time	wejście	100	Area Name		<u>/</u> 1	
Device Monitoring			Prompt			
Real-Time Monitoring			want to perform the delete peration?			
		ок	Cancel			

Figure 12-3 To Delete Passage

12.3.2 Device

12.3.2.1 Searching for Additional Channel Devices (Search)

Introduces the configuration Steps of searching for additional channel devices in ZKBio CVSecurity.

Precondition:

- 1. Set up IP allocation before adding channel devices.
- 2. Before searching and adding the device, it is necessary to set the address pointing to the server in advance and set the IP address and port of the current server, that is, the IP address and port installed by the current.

Operating Steps:

Step 1: In the Entrance Control module, select Channel Device > Devices.

Step 2: In the device interface, click "**Search**" to pop up the search box.

Step 3: Click **Search** in the search box to display the channel devices that can be added, as shown in Figure 12-4.

otal Progress	100%		Searched device Number of device					
IP Address	Devic	ж Туре	Serial N	iumber	(×		
IP Address	MAC Address	Subnet Mask	Gateway Add	Serial Number	Device Type	Set Server	Operations	
192.168.134.10	04	255.255.255.0	192.168.134.1	CM2J211260002	PGIC10-SV		This device has been added	

Figure 12-4 Device Search Interface

Step 4: For the channel Device found, click the **Add** button in the operation bar to **Add** the device, and fill in the parameters of device addition, as shown in Figure 12-5. Please refer to Table 12-2 for parameter description.

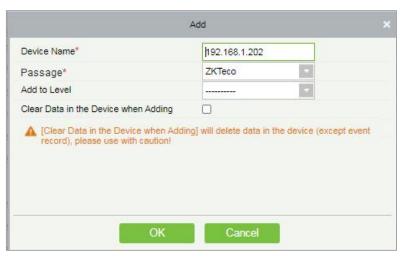


Figure 12-5 Device Addition Interface

Parameter	Description
Device Name	Any character, a combination of up to 20 characters, cannot be repeated.
Channel	Select the channe <mark>l to which the d</mark> evice belongs.
Add to Permission Group	Automatically adds the devi <mark>ce to</mark> the sele <mark>cted pe</mark> rmission group.
Delete Data in Device When Adding	When the device is added, the data in the device except the event record is deleted.

Table 12-2 Description of Device Addition Parameters

Step 5: Click OK to complete the addition of channel device.

12.3.2.2 Delete

Operation Steps:

Step 1: In the Entrance Control, click Channel Device > Device and select device to be deleted.

Step 2: Click **Delete** to delete the device.

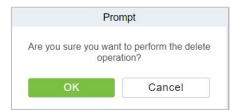


Figure 12-6 Delete Device

Step 3: Click **OK** to perform the delete operation.

12.3.2.3 Control

In this option admin can upgrade firmware and LCD screen firmware. Also, this option helps to reboot the device, enable and disable the devices, and synchronize time and all data.

Passage	Device Name		Serial Number	IP Addr	e55	More =	Q @
Device	O Refresh	Q Search 🔞 🛙	Delete 🛛 🗐 Control 🕞	@ Set up ≁ ित View / Ge	t 👻 🗣 Communication 🤫	e	
Gate			Upgrade Fir	mware			
Reader			💩 Upgrade LC	D screen firmware			
Auxiliary Input			🔅 Reboot				
Event Type			@ Synchronize	Time			
Daylight Saving Time			✓ Enable				
Device Monitoring			S Disable				
Real-Time Monitoring			(₽ Synchronize	All Data to Devices			

Figure 12-7 Device Control Interface

Upgrade Firmware

Select the device to be upgraded and click **Upgrade Firmwa**re to open the setting page. Click **Browse**, select the firmware upgrade file (file name is emfw.cfg). Click **Start** to start upgrading the firmware.

Notes:

Please be cautious while upgrading the firmware. If the firmware has not been updated properly, it may lead to device failure. If you have any queries, please contact the representative or pre-sales technical support team.

Upgrade LCD Screen Firmware

Admin can upgrade LCD screen firmware of device using this option. Select the device to be upgraded and click **Upgrade LCD Screen Firmware** to open the settings page. Click **Browse** and select the firmware upgrade file. Click **Start** to start upgrading the firmware.

• Reboot the Device

Admin can send a restart command to the device to automatically restart. Select the device to be reboot and click **Reboot** to restart the device.

• Synchronize Time

When the device's time is not accurate, select the device to be synchronized and then click **Synchronize Time** to synchronize the server time to the device.

Disable/Enable

Select the device and click **Disable/Enable** to stop/start using the device. When communication between the device and the system is interrupted or there is a problem with the device, the device may be automatically displayed as disabled. After adjusting the network or device, click **Enable**. The system reconnects to the device, and the communication status of the device is restored.

Synchronize All Data to Devices

This option synchronizes the data in the system to the device. Select the device, click **Synchronize All Data to Devices**, and click the **Synchronize** button to synchronize data:

	S	ynchronize All Data to Devices		×
ected Device				
Device Control : 1	92.168.1.105			
Unselect All	✓Passage Authority ✓Linkage	✓Passing rules for barrier gate ✓AntiPassback	√ Gate Parameters	
otal Progress				
			Our shares and shares	Olasa
Hidden Info			Synchronize	Close
Hidden Info			Synchronize	Close
Hidden Info			Synchronize	
Hidden Info			Synchronize	
Hidden Info			Synchronize	^

Figure 12-8 Synchronize All Data to Devices Interface

Notes:

The operation of synchronizing all data will first delete the existing data in the device (excluding event records) and then download all the setting information again. When performing this operation, please try to ensure that the network is unblocked and avoid power failure. When the device is running normally, please use this operation with caution. It is recommended to synchronize the data when the device is unused.

12.3.2.4 Set up

In this interface help you to set the time zone, registration, daylight saving time, fingerprint identification information and LCD screen display of the selected device.

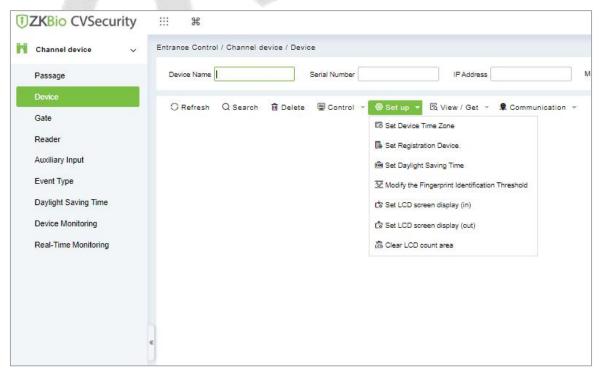


Figure 12-9 Set up Options

• Set Device Time Zone

Set Device Time Zone allows you to set the accurate time zone, if device shows wrong time zone. For that in **Entrance Control** interface, click **Channel Device > Device > Set-up**, select the device to be set up. Then click **Set Device Time Zone** to set up the selected device.

• Set Registration Device

The passage standalone device can only automatically upload the personnel and other data entered by the device when the registration device is set. For that in **Entrance Control** interface, click **Channel Device > Device > Set-up**, select the device to be set up. Then click **Set Registration Device** to set up the selected device.

• Set Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. To meet the DST requirement, a special function can be customized. You may adjust the clock one hour forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

In the **Entrance Control** interface, click **Channel Device** > **Device** > **Set-up** and select the device to be set Daylight Saving Time. Then click **Set Daylight Saving Time to set** up the selected device.

• Modify the Fingerprint Identification Threshold

The user can modify the fingerprint comparison threshold in the device, ranging from 35 to 70, and the factory default value is 55. When a new device is added, the system will read the value from the device, and the user can view the current fingerprint comparison threshold size through the device list (Please make sure the device supports the fingerprint function).

In the **Entrance Control** interface, click **Channel Device** > **Device** > **Set-up** and select the device to be modify the fingerprint identification. Then click **Modify the Fingerprint Identification Threshold** to set up the selected device.

The fingerprint	identification thr	reshold*	\$ 5	(35-70)
			100	- possible and



• Set LCD Screen Display (In)/(Out)

Select the device and set the LCD screen display (in/out). The upper part is the video area 30%, the middle part is the gate channel display area 30%, and the lower part is the picture cycle 40%. Each area can be corresponding to the video and background, The image browsing and clearing operations are confirmed and sent to the LCD screen of the controller for display.

In the **Entrance Control** interface, click **Channel Device > Device > Set-up** and select the device to be set LCD screen display. Then click **Set LCD Screen Display (In)/(Out)** to set up the selected device.

• Clear the LCD Counting Area

Select the device, clear the middle counting area of the LCD screen, and restart counting.

Pr	rompt
Are you sure you wa	ant to perform the Clear
LCD count a	area operation?

Figure 12-11 Clear LCD Counting Aera

In the Entrance Control interface, click **Channel Device > Device > Set-up** and select the device to clear the LCD counting area. Then click **Clear the LCD Counting Area** to clear counting aera the selected device.

12.3.2.5 View/ Get

In this interface admin can view device options, personal information and transaction details

Channel device 🗸 🗸					
Passage	Device Name		Serial Number	IP Address	
Device	O Refresh Q	Search 🕅 Delete	🖲 Control 👻 🐵 Set up 👻	🗟 View / Get 👻 오 Commun	ication
Gate	0.000		Touris Court	Get Device Option	
Reader				Get Personnel Information	
Auxiliary Input				🗟 Get Transactions	
Event Type				Query Device Capacity	
Daylight Saving Time					
Device Monitoring					
Real-Time Monitoring					

Figure 12-12 View/Get Option

• Get Device Option

This option allows you to view the common parameters of the device. For example, get the firmware version after the device is updated.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view device options. Then select **Get Device Option** to view device options.

• Get Personnel Information

This function obtains the data of Persons, Fingerprints, and Palmprints in the device or obtains the corresponding number.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view personnel information. Then select **Get Personnel Information** to view personnel information.

Get Transaction

This function obtains the event records in the device to the system, and the user can choose to obtain new records or all the records.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to get transaction. Then select **Get Transaction** to view transaction information.

	Get Transactions	×
ected Device		
Entrance Terminal : 192.168.2	13.185	
Get New Transactions	O Get All Transactions	
tal Progress		
-		
Hidden Info	Start	Close
		1
		× 1

Figure 12-13 Get Transactions

When the network is in good condition and the communication between the system and the device is normal, the system will obtain the event record in the device in real-time and saves it in the database. When the communication is interrupted, the event record in the device is not uploaded to the system in real-time. At this time, the user can perform this operation to manually obtain the event records in the device.

Query Device Capacity

Here, the user can view the capacity information of the device in the software and manually obtain the usage information (person, fingerprint, finger vein, face, palmprint) in the device. When the user finds that the information obtained from the software and the device is inconsistent, the user can manually synchronize the data.

In the **Entrance Control** interface, click **Channel Device > Device > View/Get** and select the device to view the capacity information of the device. Then select **Query Device Capacity** to view the user can view the capacity information of the device in the software and manually obtain the usage information.

12.3.2.6 Communication

In the **Entrance Control** interface, click **Channel Device > Device > Communication** to modify IP address and communication password.

ZKBio CVSecurity	/ !!! ¥
🖞 Channel device 🗸 🗸	, Entrance Control / Channel device / Device
Passage	Device Name Serial Number IP Address More * Q
Device	⊖ Refresh Q. Search min Delete ■ Control + @ Set up + ಔ View / Get + 👤 Communication +
Gate	
Reader	Modify Communication Password
Auxiliary Input	
Event Type	
Daylight Saving Time	

Figure 12-14 Communication Option

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

Select a device and click **Modify Communication Password** to open the modification interface 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: Communication passwords shouldn't contain spaces; it is recommended to use a combination of numbers and letters. Communication password settings can improve the device's security. It is recommended to set communication passwords for each device.

12.3.3 Gate

In the Entrance Control module, select Channel Device > Gate.

ZKBio CVSecurity	
Channel device 🗸 🗸	Entrance Control / Channel device / Gate
Passage	Barrier Gate Name Owned Device Area Name V More V Q 🖉
Device	🔾 Refresh 🖬 Remote Opening (In) 🕅 Remote Opening (Out) 🗳 Cancel alarm 🕅 kul Remote Normally Open \cdots More 👻
Gate	
Reader	Barrier Gate Name Area Name Owned Device Serial Number Barrier Gate Number Enable Verification Mode Operations
Auxiliary Input	
Event Type	
Daylight Saving Time	
Device Monitoring	
Real-Time Monitoring	«

Figure 12-15 Channel Device Gate

12.3.3.1 Remote Gate Opening (in)/(out)

In the **Entrance Control** interface, click **Channel Device** > **Gate** interface allows the user to control one gate or all gates. To control a single gate right-click over it and click **Remote Opening (In/Out)** in the pop-up dialog box. To control all gates, directly click **Remote Opening (In/Out)** behind Current All.

12.3.3.2 Cancel the Alarm

Once an alarm door is displayed on the interface, the alarm sound will be played. Alarm cancellation can be done for a single gate or all gates.

In the **Entrance Control** interface, click **Channel Device** > **Gate** and select the alarm gate to be modified. Then click **Cancel the Alarm** to cancel the alarm.

Note: If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

12.3.3.3 Remote Normally Open

It will set the gate as normal open by remote.

In the **Entrance Control** interface, click **Channel Device** > **Gate** and select the gate to be set as normal open. Then click **Remote Normal Open** to set the gate as normal open by remote.

12.3.3.4 More Options

In the **Entrance Control** interface, click **Channel Device** > **Gate** >**More** to activate the door lockdown status (remote lock and unlock).

• Remote Lock:

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

• Remote Unlock:

It will unlock a locked door. This function is supported only by certain devices.

• Enable / Disable Intraday Passage Mode Time Zone

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 (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**.

12.3.4 Reader

Each Entry device has a reader, user can view the reader information in this interface.

Operating Steps

Click **Entrance Control** > **Channel Device** > **Reader** to view the reader information such as reader name, barrier gate name, bound camera and it in/out details.

TKBio CVSecurity	H	
🕅 Channel device 🗸 🗸	Entrance Control / Channel device / Reader	
Passage	Reader Name Q 🖉	
Device	⊖ Refresh	
Gate		
Reader	Reader Name Barrier Gate Name Number IN/OUT Bound camera	Operations
Auxiliary Input		
Event Type		
Daylight Saving Time		
Device Monitoring		
Real-Time Monitoring		

Figure 12-16 Reader Interface

12.3.5 Auxiliary Input

It is mainly used to connect to the devices, such as the infrared sensors or smog sensors.

Click **Entrance Control** > **Channel Device** > Auxiliary Input, to access below shown interface.

Channel device 🗸 🗸	Entrance Control / Cha	nnel device / Auxiliary In	put				
Passage	Name	Device Name		Printe	ed Name	Q @	
Device Gate	O Refresh						
Reader	Name	Device Name	Number	Printed Name	Bound camera	Remarks	Op
Auxiliary Input	Auxiliary Input-1	ZKT_Korea	1	IN1			0
Event Type	Auxiliary Input-1	10.10.20.144	11	IN1			4
Daylight Saving Time	Auxiliary Input-1	192.168.134.101	1	IN1			0
Device Monitoring	Auxiliary Input-1	10.10.20.73	1	IN1			4
Real-Time Monitoring							

Figure 12-17 Auxiliary input

• Bind/Unbind Camera

Through this option, the reader can be connected to the cameras, and the system will make a video linkage (pop-up videos, videos, or screenshots) once there is a corresponding event occurs. For this, the interaction setting in Linkage or in Global Linkage should be done before.

Note: An auxiliary input point can bind more than one channel.

12.3.6 Event Type

The Event Type is mainly used to display various event types included in the channel device. Click **Entrance Control** > **Channel Device** > **Event Type**, and the following interface appears

	12 1	1223 14			
Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Normal verification opening	0	Normal	192.168.1.105	CM2J205360032	Edit
Verify during normal open time peric	1	Normal	192.168.1.105	CM2J205360032	Edit
Emergency password opening	4	Normal	192.168.1.105	CM2J205360032	Edit
Opening during normal open time pr	5	Normal	192.168.1.105	CM2J205360032	Edit
Linkage event triggered	6	Normal	192.168.1.105	CM2J205360032	Edit
Cancel alarm	7	Normal	192.168.1.105	CM2J205360032	Edit
Disable intraday normal open time p	10	Normal	192.168.1.105	CM2J205360032	Edit
Enable intraday normal open time p	11	Normal	192.168.1.105	CM2J205360032	Edit
Remote open auxiliary output	12	Normal	192.168.1.105	CM2J205360032	Edit
Remote close auxiliary output	13	Normal	192.168.1.105	CM2J205360032	Edit
Illegal time period	22	Exception	192.168.1.105	CM2J205360032	Edit
Illegal access	23	Freedom	192.168.1.105	CM2J205360032	Edit

Figure 12-18 Event Type

• Set the sound

Here, the user can set the event sound. First, select the event to be set sound and then click **Set up Sound** on the page.

Channel device 🗸 🗸	Entrance Control / Channel device / Ev	ent lype				
Passage	Event Name	Event Number		Event Level	▼ More *	Q @
Device	◯ Refresh 🕼 Set Audio					
Gate	Event Name	Event Number	Event Level	Device Name	Serial Number	Operations
Reader	Normal Verify Open	0	Normal	ZKT_Korea	CL63202960014	L
Auxiliary Input	Verify During Passage Mode 1	r 1	Normal	ZKT_Korea	CL63202960014	2
Event Type						0
Daylight Saving Time	First-Personnel Open	2	Normal	ZKT_Korea	CL63202960014	2
Device Monitoring	Multi-Personnel (Set Audio	1	L63202960014	2
Real-Time Monitoring	Emergency Passi Event Sour	nd 💿 Alre	ady Exists 🔿 Uplo		L63202960014	L
	Open during Pas		•	Play	L63202960014	2
	Linkage Event Tr				L63202960014	2
	Cancel Alarm	ОК	Cance	4	L63202960014	2

Figure 12-19 Set Sound Option

The audio file can be uploaded locally. The file must be in way or mp3 format, and the size cannot exceed 10MB.

12.3.7 Daylight Saving Time

DST, also called the Daylight-Saving Time, is a system to adjusting the official prescribe local time to save energy. The unified time adopted during the implementation of known as the "DST". Usually, the clocks are adjusted forward one hour in the summer to make people sleep early and get up early. It can also help to save energy. In autumn, clocks are adjusted backwards. 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 forward at XX (hour) XX (day) XX (month) and one hour backward at XX (hour) XX (day) XX (month) if necessary.

12.3.7.1 Add DST (New)

Operation Steps:

Step 1: Click **Entrance Control** > **Channel Device** > **Daylight saving Time** > **New**.

TKBio CVSecurity		¥												
Channel device 🗸 🗸	Entrance	Control / Channel	device / Dayli	ight	Saving T	ime								
Passage	O Ref	fresh 🔤 New	🖻 Delete	<u>e</u> o	IST Setti	19								
Device		DST Name	Start Tim	e			End	1 Tin	1e			Op	perations	
Gate		USA Daylight Savi	ng MAR Sec	ond	Sunday	2ho	ur NO	V Fi	rst S	Sund	lay 2hour			
Reader					N	ew						×		
Auxiliary Input		DST Name*	I]							
Event Type		Start Time*	MAR		Second	•	Sunday	•	2	*	o'clock			
Daylight Saving Time		End Time*	NOV	•	First	•	Sunday	•	2	•	o'clock			
Device Monitoring														
Real-Time Monitoring			Save and N	iew		ок		Ca	ince	1				

Figure 12-20 Daylight Saving Mode

Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set as "second Monday in March, 02:00". The system will be advanced one hour at the start time. The system will go back to the original time at the end time.

Parameter	Description
DST Name	Any character, a combination of up to 20 characters, cannot be repeated.
Start and End Time	Enter the start and end time. Set as Month-Weeks-week hour: minute format.

Table 12-2 Description of New DST Parameters

12.3.7.2 Delete

Operation Steps:

Step 1: Click **Entrance Control** > **Channel Device** > **Daylight saving Time** and select DST information to be delete.

Step 2: Click Delete and click OK to delete the DS	Step	2: Click	Delete	and	click	OK to	delete	the D	ST.
--	------	----------	--------	-----	-------	-------	--------	-------	-----

ZKBio CVSecurity	
Channel device 🗸 🗸	Entrance Control / Channel device / Daylight Saving Time
Passage	O Refresh I New Delete DST Setting
Device	DST Name Start Time End Time Operations
Gate	USA Daylight Saving MAR Second Sunday 2hour NOV First Sunday 2hour
Reader	Prompt
Auxiliary Input	Are you sure you want to perform the delete operation?
Event Type	
Daylight Saving Time	OK Cancel
Device Monitoring	

Figure 12-21 Daylight Saving Mode Delete

12.3.7.3 DST Setting

Operation Steps:

Step 1: Click **Entrance Control** > **Channel Device** > **Daylight Saving Time** and select DST information to be modify.

Channel device 🗸 🗸	Entran	ce Control / Channel d	levice / Daylight Saving Time		
Passage	0	Refresh ∓ New I	🖻 Delete 🖉 DST Setting		
Device		DST Name	Start Time	End Time	Operations
Gate		USA Daylight Savir	ng MAR Second Sunday 2hour	NOV First Sunday 2hour	
Reader			DST Setting	×	
Auxiliary Input		Device			
Event Type					
Daylight Saving Time					
Device Monitoring					
Real-Time Monitoring					
	«				

Step 2: Click DST Setting and select device from the appeared window.

Figure 12-22 DST Setting

Step 3: Click OK to save the settings.

12.3.8 Device monitoring

By default, it monitors all devices within the current user's level. You may click **Entrance Control** > **Channel 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.

Channel device 🗸 🗸	Entrance Control /	Channel devic	e / Device Monito	ring					
Passage	Area	•	Status	•	Device Name	More	- @		
Device	∱ Export 🗎	Clear all comm	nands						
Gate	Device Name	Serial Num			Operation Status	Current Status	Commands List	Recently Abnormal State	Operation
Reader	Device Name	Senariyum	iber Ale	3	Operation Status	Current Status	Commands List	Recently Abnormal State	operation
Auxiliary Input									
Event Type									
Daylight Saving Time									
Device Monitoring									
Real-Time Monitoring									

Figure 12-23 Device monitoring interface

12.3.8.1 Export

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

Click Entrance Control > Channel Device > Device Monitoring > Export to export the device commands.

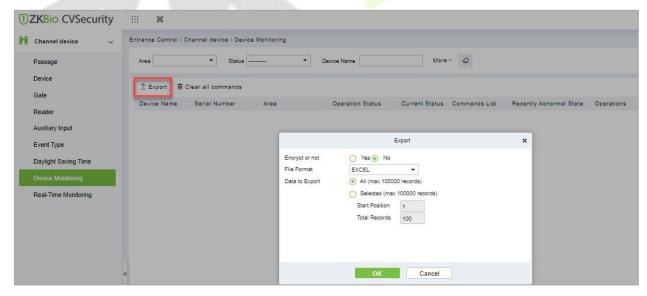


Figure 12-24 Device monitoring Export Option

12.3.8.2 Clear Command

This option allows the users to clear the unwanted command. Click **Entrance Control > Channel Device > Device Monitoring** and select the commands to be delete. Click **Clear Command** in operations column.



Figure 12-25 Device monitoring Clear command

Click **OK** to clear selected commands.

12.3.9 Real-Time monitoring

On the real-time management screen, the status of the added device is displayed, and the device can be opened or closed. At the same time, the dynamic of real-time events is monitored. If the gate opening can be verified and corresponding access control events can be generated, the access control management service configuration is complete.

12.3.9.1 Remote Gate Opening (in)/(out)

In the **Entrance Control** interface, click **Channel Device** > **Real Time Monitoring** interface allows the user to control one gate or all gates.

Operation Steps:

Step 1: Check whether the device is online. Check whether the icon status of the added device is online. Click **Barrier Gate** to check and modify the real-time status of the added devices

JZKBio CVSecurity	H #
Channel device 🗸 🗸	Entrance Control / Channel device / Real-Time Monitoring
Passage Device Gate Reader Auxiliary Input Event Type Daylight Saving Time Device Monitoring Read-Time Monitoring	Area Status Cevice Name Nore *
	Current Total 0 Online 0 Disable 0 Offine 0 Unknown 0 Barrier Gate Name
	Time Barrie Passa Event Point Event Description Area Person Card Number Device Reader Nam

Figure 12-26 Barrier Gate Option in Real-Time Monitoring Interface

Step 2: Remote opening in/out verification, taking remote opening in as an example. Select the online barrier gate device, click **Remote opening in**, enter the user password in the pop-up security verification, and click **OK**.

On the remote door opening screen, enter the time to open the door and tap OK. If Operation

succeeded in is displayed, the remote door opening Operation is complete.

12.3.9.2 Cancel the alarm

In the **Entrance Control** interface, click **Channel Device > Real Time Monitoring** interface and select the alarm gate to be modified. Then click **Cancel the Alarm** to cancel the alarm.

Note: If **Cancel the Alarm** fails, check if any devices are disconnected. If found disconnected, check the network.

12.3.9.3 Remote Lock

In the **Entrance Control** interface, click Channel Device > Real-Time Monitoring and select the barrier to modify the lock status Then click Remote Lock to activate the door lockdown status (remote lock and unlock).

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

12.3.9.4 Remote Unlock

In the **Entrance Control** interface, click **Channel Device** > **Real**-**Time Monitoring** and select the barrier to modify the lock status Then click **Remote Unlock** to activate the door lockdown status (remote lock and unlock).

It will unlock a locked door. This function is supported only by certain devices.

Auxiliary Input:

In this interface, the user can identify real-time connected sensor devices such as infrared sensors or smog sensors.

To view the list of real-time connected devices, click **Entrance Control** > **Channel Device** > **Real-Time Monitoring** and select **Auxiliary Inputs**.

12.4 Entrance Control

By setting the gate authority group and assigning it to the corresponding personnel, the gate authority of the personnel can be controlled. At the same time, it is also possible to set the response rules to the gate through Anti-Passback and linkage, to meet the requirements of different entry and exit scenarios.

12.4.1 Barrier Gate Permission Group

Gates added to the system should be set in the form of permission groups. Set the corresponding permission group, add gates to the permission group, and define the area where the permission group belongs.

12.4.1.1 To Add Gate Permission (New)

Operating Steps:

Step 1: In the **Entrance Control** module, select **Entrance Control** > **Barrier Gate Permission Group**. In the barrier gate permission group interface, click **New** in the left column of the mouse to pop up the gate permission group adding interface.

Step 2: In the **New** interface of gate permission group, set the corresponding content according to the new requirements, as shown in Figure 12-27. Please refer to Table 12-3 for parameter filling instructions.

	New	>
Level Name*	[
Area*	Area Name	•
	~	
Save and New	ОК	Cancel

Figure 12-27 Add Gate Permission Group Interface

Parameter	How to set
Level Name	Any character, consisting of up to 30 characters, cannot be repeated.
Aera	Permission groups belong to a zone to which users assigned permissions can manage permission groups under the zone.

Table 12-3 Description of Added Gate Permission Parameters

Step 3: Click **OK** to complete the configuration of the access control authority group.

Step 4: In the gate permission group interface, click **Add Barrier Gate** icon ¹⁴ on the right side of the created gate permission group, and the interface of selecting Add Gate will pop up, and the corresponding gate will be added according to the requirements, as shown in Figure 12-26

		Add	Barrier Gate			×
E	Barrier Gate Name	Serial Number		Q &		
Alt	ternative		Selecte	d(0)		
	Barrier Gate N Owned Device	Serial Number		Barrier Gate N	Owned Device	Serial Number
			_			
	_		>>			
			<			
	No data		<<		No data	
1	< 0 > > 50 rows pe	rpage 🔻				
		ОК	Cance	ł		

Figure 12-28 Adding Gate Interface

Step 5: Click **OK** to complete the setting of gate permissions.

12.4.1.2 Delete

Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Barrier Gate Permission Group** and select gate permission group to be delete.

Step 2: Click Delete and click OK to delete gate permission group.

TZKBio CVSecurity		
Channel device >	Entrance Control / Entrance Control / Barrier Gate Permission Group	
Entrance Control 🗸 🗸	Barrier Gate Permission Group	< Brows
Barrier Gate Permission Group	Level Name Q Q	Barr
Set Access By Levels	O Refresh ∓ New 💼 Delete	0
Anti-Passback	Level Name Area Name Number of Barrier Gates Operations	
Linkage	😰 <u>test1</u> T Campus O 🖉 kd	
Parameters	General Area Name 0 Prompt	
	Are you sure you want to perform the delete operation?	
	Cancel	

Figure 12-29 Deleting Gate Interface

12.4.1.3 Delete Barrier Gate

Operation Steps:

Step 1: Click **Entrance Control** > **Entrance Control** > **Barrier Gate Permission Group** and select barrier gate name to be delete.

Step 2: Click Delete and click OK to delete barrier gate from the group.

P	rompt
Are you sure you wa	ant to perform the delet
ope	eration?

Figure 12-30 Delete Barrier Gate

12.4.1.4 Export

You can export barrier gate details into an Excel, PDF, or CSV file. See the following figure 12-31.

Operating Steps:

Step 1: In **Entrance Control > Entrance Control > Barrier Gate Permission Group > Export** to export the barrier gate records to Excel sheet or PDF or CSV. Enter the User password in the prompt.

Channel device >	Entrance Control / Entrance Control / Barrier Gate Permission Group	
Entrance Control 🗸	Barrier Gate Permission Group	c Browse Levels test1 (T Campus) Barrier Gate combination
Barrier Gate Permission Group	Level Name Q	Barrier Gate Name Owned Device
Set Access By Levels	ORefresh ⊒+New 🗎 Delete	◯ Refresh 🔮 Delete Barrier Gate 🛨 Export
Anti-Passback	Level Name Area Name Number of Barrier Gates Operations	Barrier Gate Name Owned Device
Linkage Parameters	🖾 <u>testi</u> T Campus 0 🖉 M	Export X
	General Area Name 0 🖉 M	Encrypt or not 🚫 Yes 🕢 No
		File Format EXCEL •
		Data to Export () All (max 100000 records)
		Selected (max 100000 records) Start Position 1
		Total Records 100

Figure 12-31 Export Interface

Step 2: Select the file format and click OK.

12.4.2 Set Access by Levels

Assign the added gate permission group to the person.

Introduces the operation Steps of allocating personnel authority according to authority group in ZKBioCVSecurity.

12.4.2.1 Add Person

Operating Steps:

Step 1: In the **Entrance Control** module, click **Entrance Control** > **Set Access By Levels**.

Step 2: Click **Add Person** icon in the operation bar of the corresponding permission group to open the interface of adding person. Select the corresponding person as needed, as shown in Figure 12-31.

Channel device >	Entrance Control / Entrance Control / Set Access By Levels		
Entrance Control 🗸	Barrier Gate Permission Group	•	Browse Personnel test1 (T Campus) From Lev
Barrier Gate Permission Group	Level Name Q		Personnel ID First Name
Set Access By Levels	O Refresh		⊖ Refresh 🝵 Delete Personnel 🛧 Exp
Anti-Passback	Level Name Area Name Personnel Quantity Opera	tions	Personnel ID First Name Last N
Linkage	test1 T Campus 1 8*		668 chen
Parameters	General Area Name 14	Add Personnel	×
	- -	eterome ID I Name Card Number anative Card Gen. Dep 1 0002 rsj h h h 1 0001 C c	More - Q Q st Last Card Gen Deps
		2 taf C	No data

Figure 12-32 Add Person Option

Step 3: Click OK to complete the assignment of personnel permissions.

12.4.2.2 Delete Personnel

Operation Steps:

Step 1: Click Entrance Control > Entrance Control > Set Access By Levels and select person to be delete.

Step 2: Click Delete Personnel and click OK to delete barrier gate from the group.

TKBio CVSecurity	::: ¥		
Channel device >	Entrance Control / Entrance Control / Set Access By Levels		
Entrance Control 🗸	Barrier Gate Permission Group		Browse Personnel test1 (T Campus) From Levels
Barrier Gate Permission Group	Level Name Q		Personnel ID First Name More - Q Q
Set Access By Levels	O Refresh		⊖ Refresh 💼 Delete Personnel 🛧 Export
Anti-Passback	Level Name Area Name Personnel Quantity Operations		Personnel ID First Name Last Name Card Number Departm
Linkage	test1 T Campus 1 🐣		🛃 666 chen Departm
Parameters	General Area Name 14 🙎		
		Prompt	
		Are you sure you want to perform the delete operation?	
		OK Cancel	

Figure 12-33 Delete Person

12.4.2.3 Export

You can export barrier gate details into an Excel, PDF, or CSV file. See the following figure10-32.

Operating Steps:

Step 1: In **Entrance Control > Entrance Control > Set Access by Levels > Export** to export the persons records to Excel sheet or PDF or CSV. Enter the User password in the prompt.

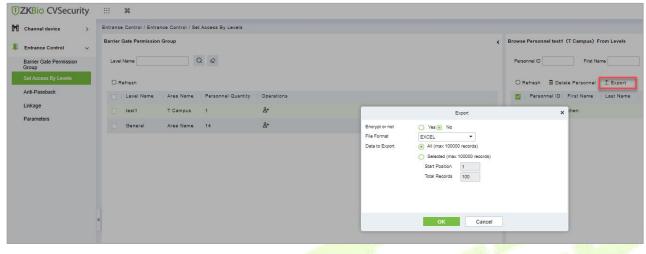


Figure 12-34 Export Interface

Step 2: Select the file format and click OK.

12.4.3 Anti-Passback

At present, it supports Anti-Passback in and out. On some occasions, people who require card swiping verification must swipe their cards from another channel when they come in from one channel, and the card swiping records must be strictly corresponding to one entry and one exit. Users can use this function when they enable it in settings, which is generally used in special units, scientific research, bank vaults and other occasions.

12.4.3.1 To Add Anti-Passback

This paper introduces the configuration Steps of adding Anti-Passback effect in.

Operating Steps:

Step 1: In the Entrance Control module, select Entrance Control > Anti-Passback and Click New.

Step 2: Select the specified device.

Description:

When adding Anti-Passback, you can't see the device that has been set up in Anti-Passback in the device list. After deleting the set Anti-Passback information, the device returns to the device list.

Anti-Passback settings of all-in-one machine: Anti-Passback, Anti-Passback and Anti-Passback.

Step 3: Select the Anti-Passback rule and click **OK** to complete the setting, as shown in Figure 12-35. The newly added Anti-Passback settings are displayed in the list of selected Anti-Passback rules.

Entrance Control / Entrance Control / Anti-Pa	assback	
Device Name Q	Q	
O Refresh 📴 New 💼 Delete		
Device Name Anti-Pass	sback Rules	
N	lew	×
Device Name* Click to select		- 1
Anti-Passback Rules*	*	- 11
		- 8
	Device Name Q C Refresh + New Delete Device Name Anti-Pass Device Name Q	Device Name Q Q C Refresh H New Delete Device Name Anti-Passback Rules New Device Name* Click to select

Figure 12-35 Add Anti-Passback Interface

12.4.3.2 Delete

Operation Steps:

Step 1: Click Entrance Control > Entrance Control > Anti-Passback and select device name to be delete.

Step 2: Click Delete and click OK to delete Anti-passback from the group.

Are you sure you	vant to perform the dele
	peration?
ОК	Cancel

12.4.4 Linkage Setting

After a specific event is triggered at a certain input point in the channel system, a linkage action will be generated at the specified output point to control the events such as verification opening, alarm and anomaly in the system, which will be displayed in the corresponding event list monitored.

Precondition:

Before linking new configurations, you need to do the following:

- 1. Gate device, input point, output point, read head binding camera add settings.
- 2. Mailbox parameter configuration.

12.4.4.1 Add Linkage

Operating Steps:

Step 1: In the **Entrance Control** module, select **Entrance Control > Linkage**.

Step 2: In the linkage setting interface, select and click the **New** button to fill in the corresponding parameters, as shown in Figure 12-37. Please refer to Table 12-4 for linkage parameters.

IZKBio CVSecurity	III #				
Channel device >	Entrance Control / Entrance Control / Links	age			
📕 Entrance Control 🗸 🗸	Linkage Name	Device Name Q	2		
Barrier Gate Permission Group	⊖ Refresh ∓ New 💼 Delete				
Set Access By Levels	Linkage Name Device Name	Linkage Trigger Conditions	Operatio	ons	
Anti-Passback					
Linkage			New		×
Parameters		Linkage Name* test1	Device*	Click to select	
		Linkage Trigger Conditions* Add	Input Point*		
	•	Output Point* Video Linka Barrier Gate Action type* Open	•	ancel	, b

Figure 12-37 New Linkage Interface

Parameter	Description
Linkage Name	Custom setting linkage name for easy reference.
Device	Customize and select the added access control device.
Linkage Trigger Conditions	Select the condition under which the linkage operation is triggered, that is, the type of event generated by the selected device.
Input Point	Select the input point to set the device input.
Output Point	Select the output point to set the output of the device.
Action Type	Choose to set up linkage action, including device operation of output point, video linkage and mail. Refer to Table 12-5 for configuration description of the three modes.

Table 12-4 Description of New Linkage Parameters

Parameter	Description
Output Point	Set the action type of output point: closed, open and normally open. Sets the delay time if the output point action is on.
Video Linkage	Pop-up video, display duration: check the pop-up video in the real-time monitoring interface and set the pop-up duration. Video recording and video recording duration: Check to record and set the video recording duration. Capture: Set whether the linkage action takes pictures: If you take pictures, you also need to set whether it pops up in the real-time monitoring interface and the display time.
E-mail	Set the email address of the received linkage content when the linkage event occurs.

Table 12-5 Explanation of Output Action Parameters

Step 3: Click OK to complete the linkage configuration.

12.4.4.2 Delete

Operation Steps:

Step 1: Click **Entrance Control > Entrance Control > Linkage** and select the linkage name to be delete.



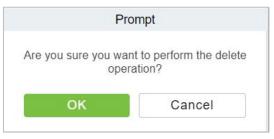


Figure 12-38 Delete Linkage

12.4.5 Parameters

Click Entrance Control > Entrance Control > Parameter to enter the parameter setting interface.

Type of Gettin	g Transactior	IS						
	O Period	lically						
	Interval							
	1					- hour(s)	
	Set the	e Time for Obt	aining New Tra	insactions	Select All	Cancel		
	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
	A Getting	transactions a	and synchroniz	ation time will	be done at the	e same time.		
Real Time Mor	nitoring							
Real Time Mor	The Real T	ime Monitoring	Page Pop-up	Photo Size	V <mark>ax Heig</mark> ht	- Contract	500)	
Real Time Mor	The Real T					px(80	1 - 500)	
Real Time Mor	The Real T		Page Pop-up			px(80	i - 500)	
Real Time Mor Alarm Monitor	The Real T 140 A Refres	h the real-time	monitoring pay			px(80	1 - 500)	
	The Real T 140 A Refres ing Recipient	h the real-time	monitoring pa			px(80	1 - 500)	
	The Real T 140 A Refres ing Recipient	h the real-time	monitoring pa			px(80) - 500)	

Figure 12-39 Add Parameters

Type of Getting Transactions:

• Periodically

Start from the setting and efficient time, the system attempts to download new transactions every time interval.

• Set the Time for Obtaining New Transactions

The selected Time is up, the system will attempt to download new transactions automatically.

The Real Time Monitoring Page Pop-up Staff Photo Size: When an access control event occurs, the personnel photo will pop up. The size of pop photos shall be between 80 to 500 pixels.

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

12.5 Passage Settings

By maintaining the gate traffic rules (control time period and traffic mode) and setting the gate parameters corresponding to the gate, the gate function can be directly controlled by software.

12.5.1 Barrier gate passing Rules

Set the passage time and passage mode of the gate, so that the gate can set different entry and exit passage modes in different time periods. It can be applied to flap Barrier and swing Barrier.

12.5.1.1 Add Barrier Gate Passing Rules

This paper introduces the configuration Steps of gate traffic rules in ZKBioCVSecurity.

Operating Steps:

Step 1: In the Entrance Control module, select Passage Settings > Barrier Gate Passing Rules.

Step 2: Click **New** with the mouse, and the interface for adding gate traffic rules will pop up.

Step 3: In the new interface, set the corresponding contents according to the new requirements, as shown in Figure 12-40. Please refer to Table 12-6 for parameter setting instructions.

of the Barrier Gate Passing Rule* Interval 1 Interval 2 Inter	e Pass Mode
Image Start Time End Time Pass Mode Start Time End Time Pass Mode Start Time End Time Monday 00 : 00	e Pass Mode
Monday 00 : 00 <th< th=""><th></th></th<>	
	0
Tuesday 00 . 00 00 . 00 • 00 . 00 • 00 . 00 • 00 . 00	10 •
/ednesday 00 : 00 00 : 00 ▼ 00 : 00 00 : 00 ▼ 00 : 00 00 : 0	10 •
Thursday 00 : 00 00 : 00 ▼ 00 : 00 00 : 00 ▼ 00 : 00 00 : 00	10 •
Friday 00 : 00 00 : 00 ▼ 00 : 00 00 : 00 ▼ 00 : 00 00 : 00	10 •
Saturday 00 : 00 00 : 00 ▼ 00 : 00 00 : 00 ▼ 00 : 00 00 : 00	10 •
Sunday 00 : 00 00 : 00 ▼ 00 : 00 00 : 00 ▼ 00 : 00 00 : 0	10 •

Figure 12-40 Interface of Adding Gate Traffic Rules

Parameter	Description
Name of Gate Traffic Rules	Any character, up to 30 characters.
Remarks	The explanation of the current time period and the main application occasions shall consist of 5 0 characters at most.

Time Interval	A gate passage rule contains up to five-time intervals in a week.
Time Interval-Start/End Time	Set the start and end time in each time interval.
Pass Mode	Set the traffic mode in each time interval and select it from drop-down. There are 10 traffic modes by default: "Two-way controlled", "free entry and exit controlled", "controlled entry and exit free", "two-way freedom", "forbidden entry and exit controlled", "forbidden entry and exit free entry", "free entry and exit forbidden entry", "two-way prohibition", "remote normal opening".
Copy Monday Time to Other Working Days	You can quickly copy Monday settings to other workdays.

Table 12-6 Parameter Description of Gate Traffic Rules

Step 4: Click **OK** to complete the addition of the gate traffic rules.

12.5.1.2 Delete Passage

Operation Steps:

Step 1: In the **Entrance Control** module, select **Passage Settings** > **Barrier Gate Passing Rules**. and select the rule to be deleted.

Step 2: Click Delete to delete the selection	cted rule.
--	------------

TKBio CVSecurity	::: ¥		
Channel device >	Entrance Control / Passage Settings / Barrier Gate Pa	issing Rules	
Entrance Control	Time Zone Name Remarks	Q Ø	
🎁 Passage Settings 🗸 🗸 🗸	◯ Refresh 🖅 New 💼 Delete		
Barrier Gate Passing Rules	Name of the Barrier Gate Passing Rule	Remarks	Operations
Flap Barrier	test1		2 1
Swing Barrier	24-Hour Accessible	24-Hour Accessible	
	4 Are yo	Prompt u sure you want to perform the delete operation? OK Cancel	

Figure 12-41 To Delete Barrier Gate Passage Rule

Step 3: Click **OK** to perform the delete operation.

12.5.2 Flap Barrier

Introduces the parameter configuration Steps of wing Barrier in ZKBioCVSecurity.

Operating Steps:

Step 1: In the Entrance Control module, select Passage Settings > Flap Barrier.

Step 2: In the flap Barrier interface, click the **Edit** button under the name or operation of the flap Barrier to enter the flap Barrier parameter editing interface, as shown in Figure 12-42. Please refer to Table 12-7 for parameter description.

Device Name*	192.168.255.241	
Barrier Gate Name*	192.168.255.241	
Barrier Gate Passing Rules*	24-Hours	
Opening Speed	Low	
Closing Speed	Low	
Gate Closing Delay Time	10 S (0-1	.0)
Unattended Time	10 S (5-6	50)
Verification in Passage	V	

Figure 12-42 Flap Barrier Parameter Configuration Interface

Parameter	How to set
Device Name	Name of flap Barrier device, non-editable.
Barrier Gate Name	Custom Setting Notes Description.
Barrier Gate Traffic Rules	Drop-down selection, the option is taken from the data of Passage Setting > Barrier Gate Passing Rules.
Opening Speed/ Closing Speed	Low speed, medium speed and high speed, set the speed of opening and closing the gate.
Gate Closing Delay Time	After passing through the last pair of infrared channels, set the delay closing time. You can set 0 to 10s, and the default is 0s.
Unattended Time	The maximum waiting time after verification is 5 to 60s, and the default value is 10s. If no pedestrians pass beyond the set time, the gate will be closed.
Verification in Passage	 No authentication in the channel is allowed. When checked the verification in the channel can open the gate; If it is not checked, the gate cannot be opened for verification in the channel, and the gate can be verified only after exiting the gate.

Table 12-7 Explanation of Flap Barrier Parameters

Step 3: Click **OK** to complete the configuration of flap Barrier parameters.

12.5.3 Swing Barrier

This paper introduces the parameter configuration Steps of swing Barrier in ZKBioCVSecurity.

Operating Steps:

Step 1: In the **Entrance Control** module, select **Passage Settings > Swing Barrier**.

Step 2: In the swinging interface, click the **Edit** button under the swinging name or operation to enter the swinging parameter editing interface, as shown in Figure 12-43. Please refer to Table 12-8 for parameter description.

Device Name*	192.168.255.241		
Barrier Gate Name*	192.168.255.241		
Barrier Gate Passing Rules*	24-Hours		
Opening Speed	Low		
Closing Speed	Low		
Gate Closing Delay Time	10	S (0-10)	
Unattended Time	10	S (5-60)	
Verification in Passage	V		

Figure 12-43 Swing Barrier Parameter Configuration Interface

Parameter	How to set
Device Name	The name of the swing Barrier device cannot be edited.
Barrier Gate Name	The gate name corresponding to the swing gate device is generally one all-in-one device corresponding to one gate, which cannot be edited.
Barrier Gate Traffic Rules	Drop-down selection, the option is taken from the data of Passage Setting > Barrier Gate Passing Rules.
Opening Speed/ Closing Speed	Low speed, medium speed and high speed, set the speed of opening and closing the gate.
Gate Closing Delay Time	After passing through the last pair of infrared channels, set the delay closing time. You can set 0 to 10s, and the default is 0s.
Unattended Time	The maximum waiting time after verification is 5 to 60s, and the default value is 10s. If no pedestrians pass beyond the set time, the gate will be closed.
Verification in Passage	 Whether authentication in the channel is allowed. When checked the verification in the channel can open the gate; If it is not checked, the gate cannot be opened for verification in the channel, and the gate can be verified only after exiting the gate.

Table 12-8 Description of Swing Barrier Parameters

Step 3: Click OK to complete the configuration of wing Barrier parameters.

12.6 Channel Reports

In the Channel report, you can query the All Transactions, Today's Access Records, Person's Last Access Location, and All Exception Events. You can choose to export all or export records after querying.

12.6.1 All Transactions

This paper introduces the configuration Steps of report query and export in, taking All Transaction report operation.

12.6.1.1 Export

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports> All Transactions.

Step 2: In the All Records interface, fill in the corresponding query information and click the **Query** symbol to complete the query of all record tables, as shown in Figure 12-44.

ime From 2021-09-20 00:00:00	To 2021-12-20 23:59:59 Personnel ID	Device Name		Retract +	Q
Department Number	Department Name	Event Description	•		
Card Number	Reader Name	Verification Mode	-		
Area Name	Event Point	Name			

Figure 12-44 All Transactions

Step 3: In the full record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in Figure 12-45.

Encrypt or not	🔿 Yes 💽 No	
File Format	EXCEL	×.
Data to Export	All (max 10000)	0 records)
	O Selected (max	100000 records)
	Start Position	1

Figure 12-45 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

12.6.1.2 Clear All Data

This option allows user to clear all data available in all transaction interface.

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports> All Transactions.

Step 2: Click the Clear All Data to clear all transactions.

TZKBio CVSecurity		III ¥		
Channel device	E	Entrance Control / Channel Reports / All Transactions		
D Entrance Control		Time From 2022-05-01 00:00:00 To 2022-08-01 23:50:50 Personnel ID	Device Name	More + Q Q
Passage Settings		⊖ Refresh 💼 Clear All Data 🛧 Export		
Channel Reports		Time Area Device Name Event Point Barrier Ty	pe Passage Name	Event Descripti Media File Personnel t Personnel ID First Name Last Name
		2022-07-25.03:35:31 Area Nam 192.168.134.104	wejście	Disconnected
All Transactions		2022-07-25 01:14:03 Area Nam 192.188.134. Prompt	wejście	Disconnected
Today's Access Records Personnel Last Access		2022-07-22 15:03:43 Area Nam 192.188.134. Are you sure to clear all records?	? wejście	Gate is not conn
Location All Exception Events		2022-07-22 15:03:41 Area Nam 192.188.134.	wejście	Device start
An Exception Events		2022-07-22 14:47:31 Area Nam 192.168.134.	wejście	Gate is not conn
		2022-07-22 14:32:22 Area Nam 192:168:134:104 192:168:134:104-1	wejście	Gate is not conn
		2022-07-22 14:32:20 Area Nam 192.168.134.104 192.168.134.104-1	wejście	Device start
		2022-07-22 14:20:46 Area Nam 192.188.134.104 192:188.134.104-1	wejście	Gate is not conn
		2022-07-22 14:20:44 Area Nam 192.168.134.104 192.168.134.104-1	wejście	Device start
	*	2022-07-22 14:02:31 Area Nam 192.188.134.104 192.188.134.104-1	wejście	Gate is not conn
		2022-07-22 14:02:20 Area Nam 192.188.134.104 192.188.134.104-1	wejście	Device start
		2022-07-22 10:08:56 Area Nam 192:188:134:104 192:188:134:104-1	wejście	Gate is not conn
		2022-07-22 10:08:54 Area Nam 192.168.134.104 192.168.134.104-1	wejście	Device start

Figure 12-46 Clear All Data Option

Step 3: Click OK to clear all records.

12.6.2 Today's Access Record

The access records for today are displayed in this option.

12.6.2.1 Export

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports > Today's Access Record.

Step 2: In Today's Access Record interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in Figure 12-47.

Personnel ID	Device Name	Retract + Q 🖉	
Department Number	Department Name	First Name	
	Department Name	That Name	
Area Name	Verification Mode	✓ Reader Name	
Name	Event Description	Card Number	

Figure 12-47 Today's Access Record

Step 3: In the access record interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in Figure 12-48.

	Ð	port	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL		
Data to Export	All (max 100000)	records)	
	O Selected (max 1	00000 records)	
	Start Position	1	

Figure 12-48 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

12.6.2.2 Clear All Data

This option allows users to clear all data available in today's access record interface.

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports> Today's Access Record.

Step 2: Click the Clear All Data to clear access records.

Pro	mpt
Are you sure to (clear all records'
ок	Cancel

Figure 12-49 Clear All Data Option

Step 3: Click OK to do the delete operation.

12.6.3 Personnel Last Access Location

Displays the last location visited by persons with access rights. It is convenient for users to quickly locate the location of personnel.

12.6.3.1 Export

Operating Steps:

Step 1: In the **Entrance Control** module, select **Channel Reports > Personnel Last Access Location**.

Step 2: In Personnel Last Access Location interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in Figure 12-50.

Entrance Control / Channel Reports / F	Personnel Last Access Location		
Time From 2022-05-01 00:00:00 To	2022-08-01 23:59:59 Personnel ID	Device Name	Retract * Q
Department Number	Department Name	Event Description -	
Reader Name	Verification Mode	✓ Area Name	
Name	Card Number	Event Point	

Figure 12-50 Today's Access Record

Step 3: In the access location interface, click Export, enter the user password in the pop-up security

verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in Figure 12-51.

	E	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	T	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records		

Figure 12-51 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

12.6.3.2 Clear All Data

This option allows users to clear all data available in Personnel Last Access Location interface.

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports > Personnel Last Access Location.

Step 2: Click the **Clear All Data** to clear the access location records of the persons, as shown in Figure 12-49.

Step 3: Click OK to do the delete operation.

12.6.4 All Exception Events

Click **Channel Report > All Exception Events** to view the abnormal events (including alarm events) such as unregistered persons, illegal entry, gate opening timeout, and failure to connect to the server under specified conditions (including alarm events).

12.6.4.1 Export

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports > All Exception Events.

Step 2: In All Exception Events interface, fill in the corresponding query information and click the **Query** symbol to complete the query of access record tables, as shown in Figure 12-52.

Entrance Control / Channel Repo	rts / All Exception Events		
Time From 2022-05-01 00:00:00	To 2022-08-01 23:59:59 Personnel II	D Device Name	Retract 🔶 Q
Department Number	Department Name	Event Description	•
Reader Name	Verification Mode	✓ Area Name	
Name	Card Number	Event Point	

Figure 12-52 All Exception Events

Step 3: In the All-Exception Events interface, click **Export**, enter the user password in the pop-up security verification, and click **OK**. Select whether to encrypt and export the file format, and Click **OK**, as shown in Figure 12-53.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL		
Data to Export	All (max 100000 records)		
	O Selected (max	100000 records)	
	Start Position	1	

Figure 12-53 Report Export Interface

Step 4: After selecting the address where the corresponding file is stored, the export of the file can be completed.

12.6.4.2 Clear All Data

This option allows users to clear all data available in All Exception Events interface.

Operating Steps:

Step 1: In the Entrance Control module, select Channel Reports> All Exception Events.

Step 2: Click the **Clear All Data** to clear exception events record.

TKBio CVSecurit	y	::: ¥				
Channel device	>	Entrance Control / Channe	al Reports / All Exception Events			
D Entrance Control	>	Time From 2022-05-01 00	00:00 To 2022-08-01 23:59:59 Pe	rsonnel ID	Device Name	More *
Passage Settings	>	🔾 Refresh 🔳 Clear	All Data 🛨 Export			
Channel Reports	~	Time	Event Descripti Event Point	Device Name Barrier Type	•	Media File Car
All Transactions		2022-07-25 03:35:31	Disconnected	192.168.134.104	wejście wejście	
Today's Access Records Personnel Last Access		2022-07-22 15:03:43	Gate is not connec 192.168.134.104-1	192.168.134.104	wejście	
Location All Exception Events	Т	2022-07-22 14:47:31	Gate is not connec 192.168.134.104-1	192.168.134.104 Prom	wejście	
		2022-07-22 14:32:22	Gate is not connec 192.168.134.104-1	192. Are you sure to cle		
		2022-07-22 14:20:46	Gate is not connec 192.168.134.104-1 Gate is not connec 192.168.134.104-1	192.	0	
		2022-07-22 14:02:31	Gate is not connet 192.168.134.104-1	192. ОК	Cancel	

Figure 12-54 Clear All Data Option

Step 3: Click OK to do the delete operation.

13 Temperature Detection

MTD (Mask and Temperature Detection) module is primarily designed to work with access control devices which have body temperature detection and mask detection features. It provides real-time monitoring of temperature and mask detection of all the users and various analysis reports.

13.1 Operation Scenario

Under the epidemic situation, the device measures the body temperature of real-time monitoring personnel, alarms and monitors the abnormal body temperature records, and summarizes and warns these records, so that managers can take timely measures and play an active role in epidemic prevention.

13.2 Operation Flow

This paper introduces the configuration process of epidemic prevention management business. The configuration process of epidemic prevention management business is shown in Figure 13-1.

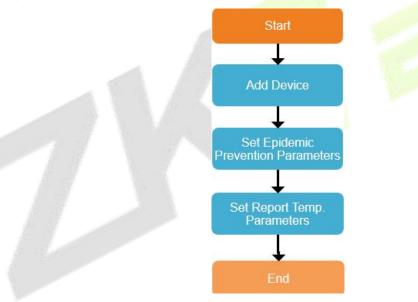


Figure 13-1 Epidemic Prevention Configuration Process

13.3 Setting Of Epidemic Prevention Parameters

This paper introduces the configuration Steps of epidemic prevention parameters in ZKBioCVSecurity.

Precondition:

In "Access Control Management", add a device supporting body temperature detection, please refer to 3.3 for adding a device.

Operating Steps:

Step 1: In the Access Control module, select Device > Device.

Step 2: After selecting the device, click "**settings** > **Setting Extension Parameters**" to pop up the interface.

Step 3: In the interface of setting extended parameters, you can view the epidemic prevention parameters on the device, as shown in Figure 13-2. Please refer to Table 13-1 for parameter configuration.

Description:

Epidemic prevention parameters are set and changed on the device side.

ŪΖ	KBio CVSecurity	::: ¥			
-	Access / Access Device / D	Device			
ŋ	Device Name	Serial Number	IP Address	More - Q 🖉	
D »	C Refresh 🛨 New	ื⊡ Delete ⊥ Export Q Search	■ Control → 🕲 Set up → 🗟 View	/ Get 👻 👤 Communication 👻	
	Device Name	Serial Number Area Name II	P Address III Set Bg-Verification Optio	Firmware Version	Operations
	ProfaceX	CN3M21246000 Area Name 1	92.168.134.168	ZAM170-NF-Ver1.5.8	_ ₫
			Set as Registration Devi	ice	
			Modify the Fingerprint Id	lentification Threshold	
			E Set Device In/Out Status	ŝ	
x	»		E Set Extended Parameter	rs	
	2				

rigare 13-2 Setting interface of Epidemic Trevention Farameters				
Parameter	Description			
Body Temperature Detection Attribute	 Open: turn on the temperature measurement function. Close: Turn off the temperature measurement function. 			
Abnormal Body Temperature Is Impassable	 Open: abnormal body temperature passes. Close: Abnormal body temperature does not pass. 			
Upper Limit of Temperature Detection Threshold	Set the threshold of device body temperature, if it exceeds, the body temperature will be abnormal.			
Temperature Correction Deviation Value	Adjust the deviation value of device body temperature.			
Temperature Unit	Celsius, Fahrenheit			
Infrared Temperature Measuring Distance	Near, medium, and far.			
Mask Detection Attribute	 Open: Test mask. Close: Do not test masks.			
Trigger The External Alarm Function	Open: Open the external alarm function.Turn off: Turn off the external alarm function.			
Allow Unregistered Personnel to Pass	Carry out normal temperature measurement.			

Figure 13-2 Setting Interface of Epidemic Prevention Parameters

Table 13-1 Description of Epidemic Prevention Parameters

Step 4: Click OK to complete the configuration of epidemic prevention parameters.

13.3.1.1 Result Validation

In the real-time monitoring interface of epidemic prevention management, the real-time events of temperature measurement and epidemic prevention can be obtained correctly, and the information can be displayed correctly, which represents the completion of epidemic prevention management business configuration.

Precondition:

In the Epidemic Prevention module, select "Epidemic Prevention Management > Parameter

Setting" to set the temperature threshold setting, which is used for the data statistical basis in the epidemic prevention report, as shown in Figure 13-3.

Temperature Dete	ection / Temperature Management / Parameters	
Temperatu	re threshold setting	Temperature threshold setting
	Body temperature'	
	37.3	
	Unit	
	⊙ x ⊙ x	
	⇒oκ	

Figure 13-3 Parameter Setting Interface of Epidemic Prevention Report

Operating Steps:

Step 1: In the Epidemic Prevention module, select "Epidemic Prevention Management > Real-time Monitoring".

Step 2: After opening the real-time monitoring interface, carry out temperature measurement verification on the temperature measuring device.

Step 3: In the real-time monitoring interface, events are generated, and data are displayed correctly, which represents the completion of epidemic prevention management business configuration, as shown in Figure 13-4.

Temperature Detection / Temperature Management / Real-Time Monito	ring
Real-Time Monitoring	Normal temperature
Normal temperature Temperature No Masks 0 0 0	
O% People	Temperature abnormal No Masks
- 076	

Figure 13-4 Real-Time Monitoring Interface for Epidemic Prevention

13.4 Temperature Management

13.4.1 Real-Time Monitoring

Click **Temperature Detection** > **Temperature Management** > **Real-Time Monitoring**.

IZKBio CVSecurity	::: ¥		e admin
🛐 Temperature Managem 🗸	Temperature Detection / Temperature Management / Real-Time Monitori	ing	
Real-Time Monitoring	Real-Time Monitoring	Normal temperature	
Statistics Panel			
Temperature Raw Record			
Individual Temperature Record			
Abnormal Temperature Record	Normal temperature Temperature abnormal No Masks		
Department Daily Statistic			
Monthly Statistics		>>> Temperature abnormal	
Automatic Report			
Parameters	e Temperatur Nu Maiks Opeople		
	- Normal temperature	No Masks	

Figure 13-5 Real-Time Monitoring

The Real-Time Monitoring interface allows the user to monitor the body temperature of the users with their image captured during verification. The mask and temperature data are collected at every entry and exit point of the premises if the personnel are registered in the device. The data will be cleared every time after being refreshed or the page is loaded. There are 3 different categories of records that are displayed on the monitoring page. They are:

Personnel with Normal temperature (masked or unmasked).

Personnel with Temperature abnormal.

Personnel with No Mask.

13.4.2 Statistic Panel

Click Temperature Detection > Temperature Management > Statistic Panel.

JZKBio CVSecurity	::: ¥	🛛 admin ~
🙆 Temperature Managem 🗸	Temperature Detection / Temperature Management / Statistics Panel	
Real-Time Monitoring	Event statistics	View Normal temperature Person's record
Statistics Panel	Time Today 👻	Personnel ID Department Name More * Q 🖉
Temperature Raw Record		
Individual Temperature Record		O Refresh
Abnormal Temperature Record		Personnel ID Event Date Body te First Name Last Name Department Department Name
Department Daily Statistic		
Monthly Statistics	P	
Automatic Report		
Parameters		
Parameters		
		i i i i i i i i i i i i i i i i i i i
	Lo	No data
	Normal temperature	
	Intersperature interperature abnormal unmeasured body temperature	

Figure 13-6 Statistic Panel

The statistics panel provides statistical data for the Administrators to analyze the number of users with normal body temperature, abnormal temperature, and unmeasured body temperature in a specific

time period. The statistics can be filtered by time i.e., Today, This Week, and This Month.

You can also click on any category on the Pie-chart and the corresponding personnel details will be displayed on the right side of the interface. Also, personnel can be searched by entering the Personnel ID or Department Name on the top-right corner of the interface. Click **More** > **Person Type** > Choose **Personnel/Visitor**.

Parameters	Description
Personnel ID	The default maximum length of personnel ID is 9, and the effective range is 1-799999999, which can be configured according to the actual situation. Value sources Personnel field, cannot be added, modified, or deleted.
Event Date	It displays the date of the Event.
Body Temperature	The "Original body temperature" is usually measured by the device, and it can't be modified. But the "Body Temperature" can be revised in the "Abnormal Temperature Record".
First Name/Last Name	The maximum length cannot exceed 50, does not support comma; value sources Personnel field, cannot add, modify, delete.
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	Any combination of a maximum of 100 characters. In the case of different levels, the department names can be repeated.

Table 13-2 Statistic Panel

EXAMPLE The statistics are only available for system personnel.

13.4.3 Temperature Raw Record

Click Temperature Detection > Temperature Management > Temperature Raw Record.

The **Temperature Raw Record** displays the reports in event-time order that is sequential as it happens regardless of the Normal

Temperature/Abnormal Temperature /Department/Masked/Unmasked. It also displays the Department Name, Body Temperature, Status, and Photo which a user can check instantly after verification.

Export:

Step 1: Click Export.

JZKBio CVSecurity	:	#												e admin
👌 Temperature Managem 🗸	Те	emperature	Detection / Temperate	ure Managemer	nt / Temperature R	aw Record								
Real-Time Monitoring Statistics Panel Temperature Raw Record Individual Temperature Record Abnormal Temperature Record Department Daily Statistic Monthly Statistics		Time From	2022-04-28 00:00:00	To 2022-07-2	3 23:59:59 Na	ame	Stat	JS	▼ Mor	re - Q 🖉				
Statistics Panel		O Refres	sh 1 Export											
		Recor		Area Name		Event Point		First Na Last	Name	Department Mask	Body te	Original	Sta Photo	
Record		7532	2022-07-27 09:42:1	Area Name	10.10.20.73	10.10.20.73-1	800000020	usuop sss		(Visitor)			Unmea	
Record		479	2022-07-27 00:54:1	Area Name	ZKT_Korea	ZKT_Korea-1	9999	K-TEST		Department Na	36.4	38.4	Norma	
		477	2022-07-21 00:25:2	Area Name	ZKT_Korea	ZKT_Korea-1	9999	K-TEST		Department Na	36.5	36.5	Norma	
Automatic Report		476	2022-07-21 00:25:1	Area Name	ZKT_Korea	ZKT_Korea-1	0000	K-TEST		Department Na	36.5	38.5	Norma	
Parameters	«	475	2022-07-21 00:25:1	Area Name	ZKT_Korea	ZKT_Korea-1	9999	K-TEST		Department Na	36.5	36.5	Norma	
		-1	2022-06-18 17:42:1	ХМ	192.168.10.221	192.168.10.221-1	1	уу		Department Na			Unmez	
		-1	2022-06-18 17:42:1	XM	192.168.10.221	192.168.10.221-1	1	уу		Department Na			Unmea	
		-1	2022-06-18 17:41:1	ХМ	192.168.10.221	192.168.10.221-1	1	уу		Department Na			Unmea	
		-1	2022-06-18 17:09:0	ХМ	192.168.10.221	192.168.10.221-1							Unmea	
		-1	2022-06-18 17:09:C	ХМ	192.168.10.221	192.168.10.221-1							Unmea	

Figure 13-7 Export Temperature Raw Record

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

Step 3: You can view the file on your local drive.

EXAMPLE Note: 10000 records are allowed to export by default, you can manually input them as required.

Parameters	Description
Time	It Displays the Time.
Name	Required Name of the person.
Status	It can enable or disable the charging standard.
Area Name	The name of the area the entry place belongs to, and the registration record for each entry place is filtered according to the area of the entry place.
Device Name	Time and attendance device name, any character up to 20.
Personnel ID	The default maximum length of personnel ID is 9, and the effective range is 1-799999999, which can be configured according to the actual situation. Value sources Personnel field, cannot be added, modified, or deleted.
Department Name	Obtained automatically based on Personnel ID.
Mask	It displays whether mask or no mask.
IVIASK	It displays whether mask or no mask.

Table 13-3 Exp<mark>ort</mark> Tempe<mark>rature</mark> Raw Record

Click the **IMAGE** icon to view the captured photo.



Figure 13-8 Capture Photo

1						Temp	perature+Raw+Reg	cord					
2	Record number	Event Date	Area Name	Device Name	Event Point	Personnel D	First Name	Last Name	Department Name	Mask	Body temperature	Original body temperature	s
3	3772	2020-07-01 14:12:04	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	37.0	37.0	N
4	3771	2020-07-01 14:12:02	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.9	36.9	N
5	3764	2020-07-01 14:06:23	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	iuliu1	Department Name	Yes	36.7	36.7	N
6	3763	2020-07-01 14:06:21	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	iuliu1	Department Name	Yes	36.8	36.8	N
7	3761	2020-07-01 14:06:18	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	Yes	36.7	36.7	N
8	3760	2020-07-01 14:06:10	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	liuliu1	Department Name	None	36.9	36.9	N
9	3759	2020-07-01 14:06:08	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	iuliu1	Department Name	None	36.9	36.9	N
10	3758	2020-07-01 14:06:06	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六大的	iuliu1	Department Name	None	37.2	37.2	N
11	3751	2020-07-01 14:05:32 Temperature+Raw+	Area Name	192.168.214.249防疫	192.168.214.249-1	4146	六六的	iulu1	Department Name	Yes	36.5	36.5	N

Figure 13-9 Export Temperature Raw Record

∕≤Note:

If the Personnel ID field is blank, it represents a Visitor.

The "Original body temperature" is usually measured by the device, and it can't be modified. But the "Body Temperature" can be revised in the "Abnormal Temperature Record".

13.4.4 Individual Temperature Record

This report displays all the body temperature details of a User or Personnel daily.

Export:

Step 1: Click Export:

TZKBio CVSecurity	::: ¥							😝 admi	n
🚺 Temperature Managem 🗸	Temperature Dete	ction / Tempera	ture Management	/ Individual Temp	erature Record				
Real-Time Monitoring	Time From 2022	-04-28 00:00:00	To 2022-07-28 2	3:59:59 Nan	Personnel ID	More + Q 🖉			
Statistics Panel Temperature Raw Record	O Refresh	1 Export							
Individual Temperature	Personnel ID	First Name	Last Name	Department	Department N Event Date	Body temperature	Status	Operations	
Record Abnormal Temperature	0000	K-TEST		4	Department Name 2022-07-21	38.5,38.5,38.5	Normal	e	
Record Department Daily Statistic	0000	K-TEST		4	Department Name 2022-07-27	38.4	Normal	®	
Monthly Statistics	1	tang	OP1	1	Department Name 2022-08-18		Unmeasured	e	
Automatic Report					Security Verification	×	Unmeasured	e	
Parameters	ĸ				User Password*				
					OK Cancel				

Figure 13-10 Individual Temperature Record

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

Step 3: You can view the only in your local drive.

∕≤Note:

10000 records are allowed to export by default, you can install manually them input as required.

Click **Body Temperature** to view the details of each record.

13.4.5 Abnormal Temperature Record

It displays the record of exceptional body temperatures i.e., above the body temperature threshold and the temperature of personnel that is not detected.

Click Temperature Detection > Temperature Management > Abnormal Temperature Record.

Export:

Step 1: Click Export.

TKBio CVSecurity		\rm e admin ~
🙆 Temperature Managem 🗸	Temperature Detection / Temperature Management / Abnormal Temperature Record	
Real-Time Monitoring	Time From 2022-04-28 00:00:00 To 2022-07-28 23 59:59 Name Processing status More + More + Q 🖉	
Statistics Panel	C Refresh	
Temperature Raw Record Individual Temperature Record	Event Date Area Na., Device Name Perso., First N., Last Name Depart., Mask Bo., Ori., Sta., Processing time Proce., Proce., Rem., Proc.,	Photo C
Abnormal Temperature Record		
Department Daily Statistic Monthly Statistics		
Automatic Report	Security Ventication X	
Parameters	User Password*	
	Cancel	
	No data	

Figure 13-11 Abnormal Temperature Record

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

Step 3: You can view the file on your local drive.

EXNote: 10000 records are allowed to export by default, you can manually input them as required.

Edit:

Click the **Edit** option to revise the user's body temperature by manual detection. The edit window pops up as shown below:

Manual measurement
admin
After manual measure the body temperature, it is normal.
1

Figure 13-12 Edit Temperature Record

Enquiry of Persons in Close Contact with Suspected Cases:

It will help the user to check the personnel who had contact with any suspected persons. Enter the contact time, 1 to 120 minutes is applicable.

ZKBio CVSecurity	Time From 2020-04-01 00:00:00 To 2020-07-01 23:59:59 Name Processing status		DI V
(La consecunty	The current query conditions Time From (2020-04-01 00:00 00) To (2020-07-01 23:59:59)		
🔯 Temperature Managem 🗸	- Refresh C Export Q, Engury of Persons in Close Contact with Suspected Cases		
Real-Time Monitoring	Event Date Area Name Device Name Personnel First Lapt Name Departme Mask		Status P
Statistics Panel	ID Name Name	temper	
Temperature Raw Record	2020-07-01 15 35:55 Area Name 192:168:214:24:4146 666de Bullut Departmen None	37.5	Distert
Individual Temperature	2020-07-01 15:35:53 Area Name 192:168 Condition	37.4	Except
Record Abnormal Temperature	2020-07-01 15 35 49 Area Name 192 168 Close contact time (minutes)* []	37.5	Except
Russi	2020-07-01 15 33-46 Area Name 192 168	37.4	Except.
Department Daily Statistic	2020-06-30 15:33 13 Area Name 192:162 A Query the time condition of close contact with the person in the	37.3	Sceede 20
Monthly Statistics	2020-06-30 15 33 07 Area Name 192 164		Except
Automatic Report			Except
	UN 1.400		
Parameters	* 2020-06-30 15:01:05 Area Name 192:168	37.4	Bicept
	2020-06-30 14:59:05 Area Name 192:168 214:24 None	37.5	Except
	2020-06-30 14:58:46 Area Name 192:168:214:24: Yes	37.3	Except

Figure 13-13 Enquiry of Person in Close Contact with Suspected Cases

Click **OK** to view the search results.

			In	timate Contact of S	Suspected Ca	se						
Abnormal Temperature	List of Persons in Clos	e Contact										
	Event time	Area Name	Device name	Event Point	Personnel ID	First Name	Last Name	Department Name	Mask	Body temperatu	Status	Phot
37.6°C Person ID: 678 First Name: William Last Name: Mask: Yes Department: Department Name Time: 2020-06-18 Time: 11:53:27	 2020-06-18 11:55: 	Area Name	192, 168, 5, 239	192.168.5.239-1					Yes	37.2	Normal	
	۲ ۲۲ ۲۰۱ که ۲۰۱	50 rows pe	erpage 👻 Jum	10 To 1 /1 Pa	age Total o	f 1 records						

Figure 13-14 List of Person

13.4.6 Department Daily Statistics

It displays the department-wise temperature detection records. A user can select a department from the list of departments in the left panel which displays the number of persons with normal temperature, abnormal temperature, and unmeasured in the specific department daily. It also displays the proportion of abnormal body temperature.

JZKBio CVSecurity	::: ¥							
Temperature Managem 🗸	Temperature Detection / Temperature	Management / D	epartment Daily Stati	stic				
Real-Time Monitoring	Time From 2022-06-28 00:00:01 To 20	022-07-28 23:59:51	Department Number		Departme	nt Name	Q	0
Statistics Panel Temperature Raw Record	🦉 🤊 🖉 Subordinate Level	O Refresh	∱ Export					
Individual Temperature Record	Department Name	Depart	Department N	Event Date	Number of	Number of	Number of	Actual Attendance People
Abnormal Temperature Record	Development In	1	Department Name	2022-07-27	1	0	0	1
Department Daily Statistic	✓ E test9 → E test8	1	Department Name	2022-07-21	1	0	0	1
Monthly Statistics	▶ 🗅 test7							

Figure 13-15 Department Daily Statistics

Export:

Step 1: Click Export.

Temperature Managem 🗸	Temperature Detection / Temperature	Management / De	epartment Daily Stat	istic				
Real-Time Monitoring	Time From 2022-06-28 00:00:01 To 2	2022-07-28 23:59:51	Department Numbe	r	Departme	nt Name	0	2 @
Statistics Panel Temperature Raw Record	🤞 🛪 🕊 💟 Subordinate Level	C Refresh						
Individual Temperature Record Abnormal Temperature Record	Department Name Development F hr	Depart 1	Department N Department Name		Number of	Number of	Number of	Actual Attendance People
Department Daily Statistic	✓ B test9 → C test8	1	Department Name	2022-07-21	1	0	0	1
Monthly Statistics	► 🗅 test7		Encrypt or not	🔿 Yes 💿 I	Export			×
Parameters «			File Format Data to Export	EXCEL	• 00000 records)			
				-	max 100000 records	5)		
				_				

Figure 13-16 Export

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

Step 3: You can view the file on your local drive.

Solution Solution Solution

Parameters	Description
Department Number	Letters and numbers are ava <mark>ilable.</mark> It cannot be identical to the number of another department. The number shall not exceed 30 digits.
Department Name	Obtained automatically based on Personnel ID.
Event Date	It displays the date of Event.
Number of Abnormal Temperatures	It displays the number of normal temperatures.
Number of Normal Temperatures	It displays the number of normal temperatures.
Number of Unmeasured	It displays the number of unmeasured.
Actual Attendance People	It displays the Attendance of people.

Table 13-4 Export

13.4.7 Monthly Statistics

Click Temperature Detection > Temperature Management > Monthly Statistic to view the infographics of monthly temperature detection.

JZKBio CVSecurity	#	\varTheta admin 👻
🛐 Temperature Managem 🗸	Temperature Detection / Temperature Management / Monthly Statistics	
Real-Time Monitoring	Monthly Statistics	
Statistics Panel	Month 2022-07	
Temperature Raw Record	Abnormal Virmessured	
Individual Temperature Record	Abnormal Vinteasured	
Abnormal Temperature Record	1	
Department Daily Statistic		
Monthly Statistics		
Automatic Report		
Parameters	c 2	
	Abnormal: 0	
	Normal: 0	
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	

Figure 13-17 Monthly Statistics

13.4.8 Automatic Report

The Automatic reporting feature helps you to send the reports to the designated person at the specified time.

Click **Temperature Detection** > **Temperature Management** > **Automatic Report.**

TRANSPORT	···· 38
💼 Temperature Managem 🗸	Temperature Detection / Temperature Management / Automatic Report
Real-Time Monitoring	File Name Report Type
Statistics Panel	⊖ Refresh 🖅 New 💼 Delete 🗸 Enable 🛇 Disabled
Temperature Raw Record	
Individual Temperature Record	Send Mode Report Type Send Frequency Time Send Inter Status Operations
Abnormal Temperature Record	
Department Daily Statistic	
Monthly Statistics	
Automatic Report	
Parameters	«



13.4.8.1 Delete

Select File name in the list on the right and click **Delete**.

Enable/Disable 13.4.8.2

Select device, click Enable/Disable 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.

13.4.8.3 New

Click the **New** button to open the adding automatic export page.

end Mode Setting				Mail Setting		
Send Mode*	Mailbox Delivery Me	t =		Receiver Setting	Set by Personnel 🔻	
Seport Setting				Mail Address*	Please enter a valid email address. if more than one address is entered, separate with',' Example:123@foxmail.com,456@foxmail.co	
Report Type*	Temperature Raw R			Title Setting*	The Maximum Length50	
File Type*	EXCEL -		Body Setting	The Maximum Length200		
1ail Delivery Time	Setting					
Send Frequency	By Day	•				
	• hour :		- minute			
	+ hour :		- minute			
	+ hour :		→ minute			
	+ hour :					
	+ hour :	20.60 A	✓ minute			
	+ hour :		✓ minute			

Figure 13-19 Add Automatic New report Interface Page

Send Mode Setting

Send Mode: The reports can be sent through Email or FTP.

• Report Setting:

Report Type: The report types that can be sent are Transactions or Daily Attendance.

File Name: The File Name is composed of three parts: Custom file name + YYMMDD + HHMMSS (For example, Test Department Transactions 201911011143).

The first text box is for the custom file name.

The second drop-down box is to select the Day/Month/Year format: yyyymmdd and yyyy-mmdd are currently supported.

The third drop-down box is to select the Hour/Minute/Second format: HHmmss is currently supported.

Parameters	Description
Field	It displays the field name and field number of the currently selected report
File Type	It currently supports EXCEL, TXT.
Content Format	Exports the content format of the attached report, such as {department Name}, {department Name}, {person Pin}, {person Name}, {devices}, {device Name}, {area Name}, {add Date time}. You cannot delete the content format when the file type is EXCEL; When the File type is TXT, the content format is editable.
Sending Frequency	The report sending frequency can be a day or by month.
By Day	It supports up to 6-time points per day and can only be sent once per hour. Set the Hour and Minute to send the report from the drop-down boxes

Table 13-5 Export

Send Frequency	By Day						
		• 1	hour	:		•	minute
		•	hour	;		•	minute
		• 1	hour	;	1. 1997 -	٠	minute
		• 1	hour	:		•	minute
		• 1	hour	:		٠	minute
		• 1	hour				minute

Figure 13-20 Report Setting

By Month: It supports Support last day, first day, and a specific date of each month.

			and the second
Send Frequency	By Month		
	Last day of the month		23 200
	First day of the month		
	Specific Date - ▼	(1-	
	28)		

Figure 13-21 Report Setting

Mail Setting: Mail setting is required when the sending mode is Mailbox Delivery Method.

Parameters	Description
Receiver Setting	You can select the recipient by person, department, or area.
Set by Personnel- Email Address	Enter the valid Email Address of the recipient. If there are multiple recipients, then the Email address can be separated by a semicolon.
Set by Department	Select a department in the department tree diagram and the report will be sent to all the persons whose Email Addresses are configured under the department.
Set by area- Attendance area	Select an area in the area tree, and the report will be sent to all the persons whose Email Addresses are configured under the area.
Title Setting	The Maximum length of the report title is 50 characters.
Title Setting	The Maximum length of the message content is 200 characters

Table 13-6 Mail Setting

13.4.9 Parameters

It allows the user to set the body temperature threshold which determines the category to which the recorded temperature falls-in i.e., Abnormal Temperature or Normal Temperature. For example, assume that the threshold temperature is set to 37.3°C. If the recorded temperature is 37°C, it will be saved as "Normal Temperature" and if the recorded temperature is 38°C, it will be saved as "Abnormal Temperature". The temperature unit can also be chosen between °C and °F.

ZKBio CVSecurity		\rm e admin
🗓 Temperature Managem 🗸	Temperature Detection / Temperature Management / Parameters	
Real-Time Monitoring Statistics Panel	Temperature threshold setting	Temperature threshold setting
Temperature Raw Record Individual Temperature Record Abnormal Temperature Record Department Daily Statistic Monthly Statistics Automatic Report Parameters	Body temperature* 27.3 Unit ● ℃ ● 7	

Figure 13-22 Parameters

∕≤Note:

After setting the body temperature threshold, the Real-Time Monitoring Page will refresh, and the persons will be categorized according to the new threshold temperature.

The value is rounded off to one decimal place.

14 Service Center

This module integrates the device and event logging of the system module. Users can import a map to the map center to view the distribution of monitoring points and alarm sources. When an alarm occurs, users can view the location and surrounding conditions of the alarm source, select a suitable monitoring point, and view video live, playback, and human movement functions.

14.1 Device Center

14.1.1 Device

Devices added to the access control and video module are displayed on the screen, and basic device information is displayed, as shown in Figure 14-1.

Device Name	Q @							
🔾 Refresh 🛛 🛱 Device synchroniz	ation							
Serial Number	Device Name	Device Model	Firmware V	IP Address	Belong Areas	Source Mo	Status	Operati
CN3M212460001	ProfaceX	TDB08M-TI/M	ZAM170-NF-Ve	192.168.134.168	Area Name	Access	•	ప
21024127099SL8000137	192.168.134.59	DBL522-01		192.168.134.59	Area Name	Intelligent Vide	•	ప
f673eae8ab854805b3874535b6b56	AS1700	IVS1800		192.168.134.101		Intelligent Vide	0	బ

Figure 14-1 Device Display Page

Device Synchronization:

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

Note: Synchronize 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.

14.2 Event Center

Through the definition of the event level and type, it makes the level prompt for the record generated under real-time monitoring.

14.2.1 The Event Type

The software contains event types by default. You cannot add new event types. You can customize the level of the event type.

This section describes how to modify Step.

• Modify Event Type

Operation Step:

Step 1: In the Service Center module, choose Event Center > Event Type.

Step 2: On the **Event Type** page, select the event type to be modified and click **Event Level**. The Event Level dialog box is displayed.

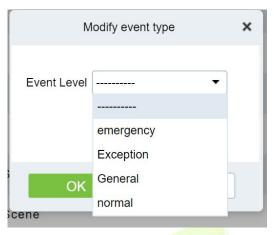


Figure 14-2 Modify Event Level Page

Step 3: After selecting the desired level, Click **OK** to complete changing the event type level.

14.2.2 The Event Record

This screen records all events generated on the platform, as shown in Figure 14-4.

tt	time 2021-12-20 00:00:00	To 2021-12-20 23:59	59 Eve	ent Level	 Processing state 		▼ More ▼ Q	0		
Re	efresh 🖲 Confirm									
	Event object	Event name	Event L	Event time	Event source	Area	Source Capture	Panora	Process Processing	remark
	1	Visitor Registration	normal	2021-12-20 11:52:45	1	Popy-Building	Visitor		Unconfirme	

Figure 14-3 Event Recording Page

14.3 Notification Center

Notification Record

This interface records the notification reminding events generated by the attendance and visitor module.

IZKBio CVSecur	ity	::: ж								
Device Center	>	Service Center / Notification Center / Notification Record								
! Event Center	>	title	Reader Type		Source Module Q					
Notification Center	~	C Refresh								
Notification Record		title	Notification Type	Source Mo	Value	Create Time	Operations			
	-	Visitor Reservation	Visitor Dynamics	Visitor	Reservatioin: visitor(ravi) will visit name1 at 2022-07-22 13:	2022-07-22 09:00:51				
		Visitor Checked Out	Visitor Dynamics	Visitor	Exit: 2022-07-22 07:24:49 visitor(ani) exit at BLR	2022-07-22 07:24:49				

Figure 14-4 Notification Record Page

14.4 The Map Center

You can import a map to set monitoring points. When an alarm occurs, you can immediately view the location of the alarm source and surrounding conditions, select an appropriate monitoring point, and view live videos, playback, and personnel movements.

14.4.1 Real-Time Monitoring

Alarms generated in the access control and video modules are displayed on the real-time monitoring interface. You can query access control and video events by category. When an alarm is generated, you can view the location of the alarm source and surrounding conditions, select a suitable monitoring point, and view the live video, playback, and personnel movement. Operation that can handle doors in batches.

14.4.1.1 Personnel Movement

This paper introduces the configuration Step for real-time monitoring of personnel movement in the service center module.

Operation Step

Step 1: In the Service Center module, choose "Map Center > Real-time Monitoring".

Step 2: On the real-time monitoring screen, click the icon on the right 4 in the personnel Trend window that is displayed, set related parameters.

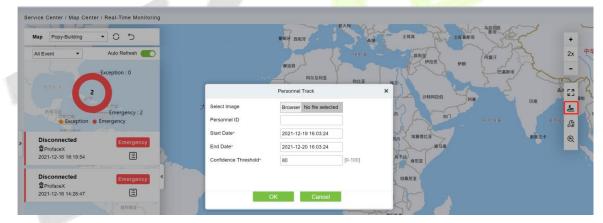


Figure 14-5 Page for Querying Personnel Trends

Step 3: Click **OK** to display the movement chart on the map.

14.4.1.2 Batch operation

This paper introduces the configuration Step for real-time monitoring of batch operation in the service center module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Real-time Monitoring".

Step 2: On the real-time monitoring screen, click the icon on the right ² In the personnel Trend window that is displayed, set related parameters,

Remote Opening / Remote 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 (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**.

 $\mathfrak{A} \gg$ **Note:** If **Remote Opening /Closing** fails, check whether the devices are disconnected or not. If disconnected, check the network.

Activate Lockdown:

It will remotely set the door status to locked status. After this, the door wouldn't receive any operations, such as card reading and remote operations. This function is supported only by certain devices.

Deactivate Lockdown:

It will unlock a locked door. This function is supported only by certain devices.

Cancel Alarm:

Once an alarming door is displayed on 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.

 $\mathscr{A} \gg$ **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

14.4.1.3 Search Device

This paper introduces the configuration Step for real-time monitoring of search device in the service center module.

• Add a Door

This paper introduces the configuration Step of map configuration and door addition in the service center module.

Operation Step:

Step 1: In the service Center module, choose "Map Center > Map Configuration".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of

the screen $^{\textcircled{O}}$ To add the gate.

Step 3: In the Add Door list on the left of the page, drag the required **Access Control** device to place it on the map,

Step 4: Click Submit under the left door bar to complete the operation of adding a door on the map.

• Adding a Camera

This section describes how to add camera Step for map configuration in the Service Center module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Map Configuration".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen to add a camera.

Step 3: In the Add Camera list on the left of the screen drag the required camera device to place it on the map,

• Others

This section describes how to add others Step for map configuration in the Service Center module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Real Time Monitoring".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen to add a Others

Step 3: In the Add Other list on the left of the screen drag the required other device to place it on the map,

Map

Click the Map: It will show the area of the map

Defense Area

It will show the defence area in the map

14.4.1.4 Handle Video Alarm Details

This section describes the Step configuration for handling video alarm event details in the Service Center module.

Operation Step

Step 1: In the Service Center module, choose "Map Center > Real-time Monitoring".

Step 2: On the real-time monitoring screen, select a video alarm in the left pane and click ⁽²⁾ To display detailed information. As shown in Figure 14-6.

Instructions:

Function description of the detailed information interface:

- 1. Preview: Displays the live view of the current video device.
- 2. Playback: Plays back the records generated by alarm events.
- 3. Trend: record the corresponding trend record of personnel.
- 4. Report: You can note the event status.

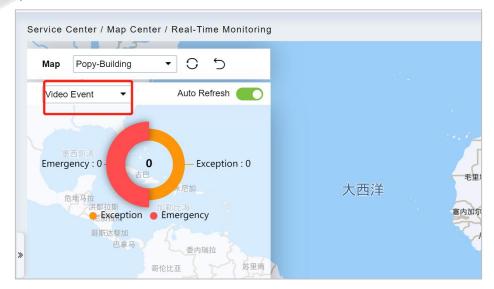


Figure 14- 6 Video Alarm Details Screen

Step 3: After viewing the detailed information and remarks, click Submit.

14.4.1.5 Handle Door Alarms in Details

This section describes the Step configuration for handling gate alarm event details in the Service Center module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Real-time Monitoring".

Step 2: On the real-time monitoring page, select the event for which the access control alarm is generated in the left pane and click e The detailed information is displayed.

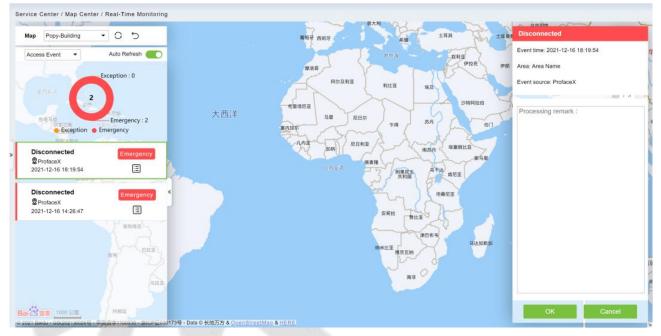


Figure 14-7 Access Alarm Details Page

Step 3: After filling in the report remarks, click Submit.

14.4.2 Map Configuration

By importing the map and configuring the corresponding monitoring points, the distribution of the current monitoring points can be intuitively displayed.

Instructions:

Table 14-1 describes the ICONS on the map configuration page.

lcon	Instructions
23	Full screen.
0	The refresh.
5	Return to the previous level.
Å	Drag ICONS of Access Control and camera and move coordinates; After Operation is finished, click, can be saved.
C.	Add the icon of the Access Control device.

lcon	Instructions
Q.	Add a camera icon.
2	Add submaps.
+ 11x -	Operation to zoom in and out of the map.
1 移除图标	Move the mouse over the "door or Video" device on the map and right click it out.
==	Add a map.
0	The editor.

Table 14-1 Map Configuration Icons

The Premise Conditions:

- 1. The access control device is added to the **Access Control** module.
- 2. Add the camera device under the video module.

14.4.2.1 Add a Map

This section describes how to add Step of map configuration in the Service Center module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Map Configuration".

Step 2: In the map configuration screen, click on the left bar \pm . The page for adding a map is displayed, as shown in Figure 14-8. For details about the parameters, see Table 14-2.

	New		×
- +	Мар Туре*	General Map 🔹	
Browser No file selected			
	· · · ·	▼ + Map Type*	Map Type General Map

Figure 14-8 Add Map Page

The Map Type	Parameter	Instructions
Normal	Name	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
Mapping (Using the map drawn by the user, as the background loading,)	Map Path	 Select the map you want to add, that is, the map image file that exists on the local server in advance. Instructions Map is supported formats. Jpe \. JPG \. Jpeg \. GIF \. PNG \. BMP \. Ico \. SVG \. SVGZ \. Tif \. Tiff \. Ai \. DRW \. PCT \. PSP \. XCF \. PSD \. Raw \. Webp image file.

The Map Type	Parameter	Instructions
		• Map image file size should not exceed 1120×380 px.
	Name	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
	Map Path	
	Route Analysis Path	To set up a GIS server, set parameters on the server, and then set these parameters.
	Projection	·
Hypergraph	The Center X/Y Coordinate	Fill in the latitude and longitude.
	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	Maximum Zoom Level/Minimum Zoom Level	Custom map zoom size.
	Area	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
Google Maps	The Map Key	Log on to the platform for https://cloud.google.com/maps- platform for registration for the key. Instructions: You need to turn on the Directions API on Google's platform to map people's movements.
	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	The Center X/Y Coordinate	Fill in the latitude and longitude.
	Area	Select the area to which you want to add the map. For details about how to configure regions, see 18.2 Region Settings.
Paidu Man	The Map Key	Log in to http://lbsyun.baidu.com/ to register and obtain the key.
Baidu Map	Initialize The Scaling Level	The general choice for initial scaling is around 13.
	The Center X/Y Coordinate	Fill in the latitude and longitude.

Table 14-2 Parameters for Adding a Map

Step 3: Set parameters based on the type of the map to be added and Click **OK** to finish adding the map.

14.4.2.2 Add Submap (Optional)

This section describes how to add sub-map configuration Step on the map in the **Service Center** module.

Operation Step:

Step 1: In the Service Center module, choose "Map Center > Map Configuration".

Step 2: On the map configuration screen, select a region map and click on the right ^{CA} To add submaps.

Step 3: In the Add Map list on the left of the page, drag a submap to place it on the map.

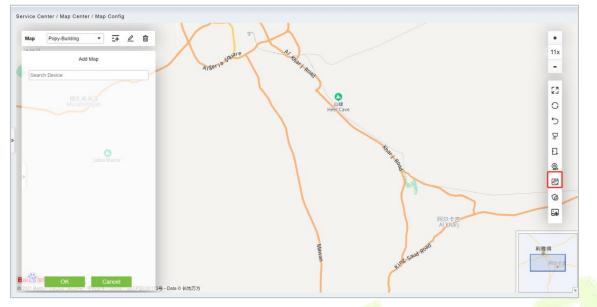


Figure 14-9 Add Submap Page

Step 3: Click submit under add map on the left to complete the configuration of the sub-map.

14.4.2.3 Add a Door

This paper introduces the configuration Step of map configuration and door addition in the service center module.

Operation Step

Step 1: In the service Center module, choose "Map Center > Map Configuration".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of

the screen \Box to add the gate.

Step 3: In the Add Door list on the left of the page, drag the required **Access Control** device to place it on the map, as shown in Figure 14-10.



Figure 14- 10 Add Door Page

Step 4: Click Submit under the left door bar to complete the operation of adding a door on the map.

14.4.2.4 Adding a Camera

This section describes how to add camera Step for map configuration in the Service Center module.

Operation Step

Step 1: In the Service Center module, choose "Map Center > Map Configuration".

Step 2: On the map configuration screen, select the map of the desired area and click on the right of the screen to add a camera.

Step 3: In the Add Camera list on the left of the screen, drag the required camera device to place it on the map, as shown in Figure 14-11.

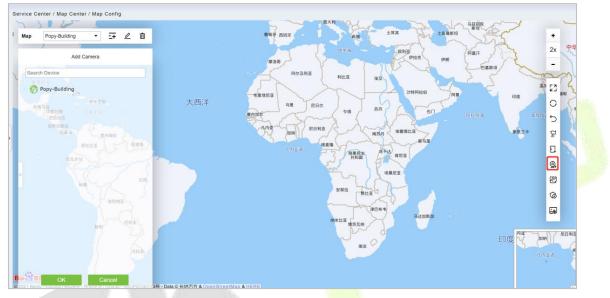


Figure 14- 11 Add Came<mark>ra Scr</mark>een

Step 4 Click **Submit** in the left column of Adding a camera to complete the configuration of adding a camera to the map.

14.4.2.5 Add Defence Area

We can view the Intrusion Alarm states in real time through the map center.

Step 1: Go to Service Center > Map Center > Map Config. Click ^G, start adding defence area.



Figure 14-12 Adding Defense Interface

Step 2: Click the **Adding Defence Area** on the left of the screen, drag the required partition or zone to place it on the map.

Step 3: Click **OK** the left column of **Adding Defence Area** to complete the configuration of adding a partition.

14.4.2.6 Map

Click the Map: It will show the area of the map.

14.5 Push Center

14.5.1 Push Configuration

Add New

Operation Step:

Step 1: In the Service Center module, choose "Push Center > Push Configuration".

Step 2: In the **Push Configuration** interface, click **Add New** and fill in the relevant parameters, as shown in Figure 14-13. Please refer to Table 14-3 for parameter description.

	New	×
Configuration name*		
Push URL*		
Connection test		
Push Types		
Access		
Event Log Capture Photo		
Attendance		
Attendance Record Attend	lance Photo	
Elevator		
Event Log		
Entrance Control		
Event Log		
FaceKiosk		
Faceklosk		

Figure 14-13 Add Push Configuration

Parameter	Description
Configuration Name	Enter the configuration name
Push URL	Enter the push URL

Table 14-3 Parameters for New

• Delete

Select one or more push configuration and click **Delete** at the upper part of the list and click **OK** to delete the selected. push configuration Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single push configuration.

Docking Example

It will show the example of data format as a code.

<pre>Data format document download SpringBoot package com.example.demo; import org.slf4j.Logger; import org.slf4j.LoggerFactory; import org.springframework.stereotype.Controller; import org.springframework.web.bind.annotation.RequestBody; import org.springframework.web.bind.annotation.RequestMapping; import org.springframework.web.bind.annotation.ResponseBody; import com.alibaba.fastjson.JSONObject; @Controller @RequestMapping(value = "/other") public class ReceiveController { private final Logger logger = LoggerFactory.getLogger(ReceiveController.class);</pre>
<pre>backage com.example.demo; import org.slf4j.Logger; import org.slf4j.LoggerFactory; import org.springframework.stereotype.Controller; import org.springframework.web.bind.annotation.RequestBody; import org.springframework.web.bind.annotation.RequestMapping; import org.springframework.web.bind.annotation.ResponseBody; import com.alibaba.fastjson.JSONObject; @Controller @RequestMapping(value = "/other") bublic class ReceiveController {</pre>
<pre>import org.slf4j.Logger; import org.slf4j.LoggerFactory; import org.springframework.stereotype.Controller; import org.springframework.web.bind.annotation.RequestBody; import org.springframework.web.bind.annotation.RequestMapping; import org.springframework.web.bind.annotation.ResponseBody; import com.alibaba.fastjson.JSONObject; @Controller @RequestMapping(value = "/other") public class ReceiveController {</pre>
<pre>@RequestMapping(value = "/receive") @ResponseBody public String receive(@RequestBody JSONObject requestBody) { logger.info("receive requestBody = {}", requestBody); return "200"; } }</pre>

Figure 14- 14 Docking Example

14.5.2 Push Exception Record

• Delete

Select one or more push exception record and click **Delete** at the upper part of the list and click **OK** to delete the selected. push exception record Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single push exception record.

Re-push

If the data sync failed one time it will re-sync the data automatically to the software and device.

Manual Push

Manual push is we need to sync the data from device to the software.

15 System management

15.1 System Management

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

15.1.1 Operation Log

Operation Step

```
Step 1: Click System > System Management > Operation Log.
```

perator	Tu	me 2022-05-01 00:00:00	To 2022-	08-01 23:59:	59 More	- Q @		
Refresh	∱ Export							
Operator	Time	IP Address	Module	Object	Operation	Operation Detail	Result	Time (ms)
sdmin	2022-08-01 10:14:38	14.97.160.178	System	User	User Login	User Login:admin;	Success	12
admin	2022-08-01 10:14:01	14.97.160.178	System	User	User Login	User Login:admin;	Success	22
admin	2022-08-01 10:12:36	14.97.160.178	System	User	Logout	Logout	Success	16
admin	2022-08-01 09:47:20	14.97.160.178	System	User	User Login	User Login:admin;	Success	16
admin	2022-08-01 09:46:38	223.197.183.130	System	User	User Login	User Login:admin;	Success	21
admin	2022-08-01 09:46:09	183.250.208.207	System	User	User Login	User Login:admin;	Success	12

Figure 15-1 Operation Log Interface

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

15.1.1.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the operation log.

15.1.1.2 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. See the following figure.

	E	export	×
Encrypt or not	🔿 Yes 💽 No		
File Format	EXCEL	÷	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	OK	Cancel	

Figure 15-2 Export Option

15.1.2 Database Management

Operation Step

ZKBio CVSecurity		H							e admin
🔋 System Management 🗸 🗸	System /	System Man	agement / Database Mana	gement					
Operation Log	Opera	itor	Q &						
Database Management	O R	efresh 🔗 B	Backup Immediately 👩 🕅	ackup Schedule	FTP Server Setting				
Area Settings		Operator	Start Time	Database Version	Backup Immediately	Backup Status	Backup Path	Operations	
E-mail Management		admin	2022-07-29 18:00:05	4.0.0.1	•	0	C:\SecurityDBBack\	5 0	
Dictionary Management		0.22555			0	0	1. 		
Data Cleaning		admin	2022-07-25 19:59:02	4.0.0.1			C:\SecurityDBBack\	4 <u>0</u>	
Audio File		admin	2022-07-22 18:00:04	4.0.0.1	•	0	C:\SecurityDBBack\	Ф <u>0</u>	
Certificate Type		admin	2022-07-15 18:00:05	4.0.0.1	•	0	C:\SecurityD8Back\	÷ 🖞	
Print Template		admin	2022-07-08 18:00:04	4.0.0.1	•	0	C:\SecurityDBBack\	令 前	
System Monitoring		admin	2022-07-01 18:00:05	4.0.0.1	0	0	C:\SecurityDBBack\	↓ (i)	
Parameters		admin	2022-06-24 18:00:05		•	0	C:\SecurityD8Back\	小	

Step 1: Click System > System Management > Database Management.

Figure 15-3 Database Management Interface

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

15.1.2.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the operation log.

15.1.2.2 Backup Immediately

Step 1: Click Backup Immediately.

Backup database to the path set in installation right now.

Are you su	ure you want to back up data now?	
Back u	up to FTP server at the same time	
Prompt		
Ally	ou select this check box, data will be backed u	in to
	configured FTP server.	1. A. A.

Figure 15-4 Back up Immediately Option

Solution: Solution: Solution and Solution Solution and Solution and Solution Solution Solution Solution and Solution Solution Solution Solution and Solution Solution and Solution Solu

15.1.2.3 Backup Schedule

Step 1: Click Backup Schedule:

	sckup time:2022-07-29	9 18:00:05	
The next b			
	ackup time:2022-08-04	6 18:00:00,Jeft 4 day 12 hour 38 minute 11 second.	
4000	ndare - ma		
Back	up to FTP server at the	e same time	
Prompt			
1. Identific			
		tabase, the database server and the server must be on the	
sam	a computer. If the back	kup fails, please refer to the user manual FAQ.	

Figure 15-5 Back up Schedule Option

Step 2: Set the start time, set interval between two automatic backups, click OK.

15.1.2.4 FTP Server Setting

When send mode is FTP Send Method, FTP parameters should be set. The parameters are FTP Server Address, Server Port, Folder Location, Username, and Password.

Port* 21 Folder location folder1/folder2 User name* 20 Password* 20	FTP server address*	127.0.0.1	
User name*	Port*	21	
	Folder location	folder1/folder2	
Password*	User name*		
	Password*		
	Test Connection		

Figure 15-6 FTP Server Setting

Parameter	Description
FTP Server Address	Enter the address FTP Server Address E.g.: such as 192.168.1.10.
Port	Enter the port number.
Folder Location	Enter the Folder location.
Username	Enter the Username of the FTP server.
Password	Enter the password for the FTP server.
Test Connection	After configuring the FTP parameters, click Test Connection to test whether the FTP server is communicating normally.

Table 15-1 Description of FTP Server Setting Parameters

After the setup is completed, click the **OK** button, save and return to the Database Management interface.

15.1.3 Area Settings

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 **Headquarters** and numbered **1**.

15.1.3.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Aera setting page.

15.1.3.2 New

Step 1: Click System > System Management > Area Setting > New.

Step 2: Click OK to finish adding.

Area Number*	1	
Area Name*		1977 (S.
Parent Area*	Area Name 👻	
Remarks		16

Figure 15-7 Aera Setting

Parameter	Description
Area Number	Enter the Aera number. It must be unique.
Area Name	Enter the aera name. Any characters with a length less than 30.
Parent Area	Determine the area structure of system.

Table 15-2 Description of Aera Setting Parameters

15.1.3.3 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

	1	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	.	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	
	otart i contoni	1	

Figure 15-8 Export Option

15.1.3.4 Edit/Delete an Area

Click **Edit** or **Delete** as required under **Operation** to go to the edit or delete page. Then click **OK** to save the setting.

15.1.3.5 Import

If there is a personnel file in your computer, you can Import it into the system.

Step 1: Click Import

Area N	lumber		Area Name	Q Q	
O Re	fresh ∓ New	🗊 Delete	↑ Export	± Import -	
	Area Number	Area Name	Parent	± Import	Operations
-	1	Area Name		<u> </u>	0

Figure 15-9 Import Interface

Step 2: Select the file format to be imported (default is Excel) and choose the file to be imported.

File Format	Excel	
Select File	Browge Not Uploaded	
The first line of the	All the state of t	and the second
	e data format is table name, the second line is heade data, please check the file and then import.	s, me mira
		r, the bard
		r, the third

Figure 15-10 Import Option

Step 3: If you want to download the sample template excel file for importing, click the **Download Area Import Template.**

		area import template	e	
Area Number	Area Name	Parent Area Number	Parent Area Name	Remarks

Figure 15-11 Aera Import Template

Step 4: Once the sample excel is downloaded, you can fill your data into it and save it. Then upload the saved file.

15.1.4 E-mail Management

Set the email sending server information. The recipient e mail should be set in Linkage Settings.

Step 1: Click System > System Management > Email Management

15.1.4.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Email management page.

15.1.4.2 Delete

Click **Delete** as required under operation to go to the edit or delete page. Then click **OK** to save the setting.

15.1.4.3 Outgoing Mail Server Settings

Click System > System Management > Email Management > Outgoing Mail Server Settings.

Email Sending Server*	smtp.exmail.qq.com	(sniip.xxx.xxx)	
Port*	465	SSL TLS	
Email Account*	Soluction.dep@zkteco.dep	200 (XXX@XXX.XXX)	
Password*			
Sender Name	Admin-ZKTeco		
Test Connection	ail verification.		

Figure 15-12 Outgoing Mail Server Setting

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

15.1.4.4 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	*	
Data to Export	All (max 10000)	0 records)	
	O Selected (max	100000 records)	
	Start Position	1	

Figure 15-13 Export Option

15.1.5 Dictionary Management

Data dictionary management function, users can find the meaning of error code and self-check software errors.

System / System Man	agement / Dictionary Manageme	nt	
Module	Dictionary classifica	tian	• Q @
Module	Dictionary classification	Key name	Value
System	Gender	м	Male
System	Gender	F	Female

Figure 15-14 Dictionary Management Interface

15.1.6 Data Cleaning

To save disk storage space, the expired data generated by the system must be cleaned up regularly

Click **System** > **System Management** > **Data Cleaning**. The data cleaning frequency can be set to Day/Week/Month.

15.1.6.1 Record

This option helps you to set the frequency of retain the recent data of the access transaction, attendance transaction, elevator transactions and visitor transactions etc.

	Cleaning frequency is executed once reserved months. Execution Time refers to the time whe When you click OK, the system will au user's settings.	n the system starts to perfor	m a data clean-up.	Record Disk space cleanup System
Record				
	Access Transactions * Retains the recent			
	15	Month	*	
	Execution Time			
	01:00:00		•	
	(Carefully clean up)			
	Attendance Transactions * Retains the recent			
	15	Manth	-	
	Execution Time			
	03:00:00		-	
	(Carefully clean up) Elevator Transactions * Retains the recent			
	15 -	Month		
	Execution Time			
	01:00:00		-	
	(Carefully clean up)			
	Visitor Transaction *			
	Retains the recent			
	15	Month	+	
	Execution Time			
	01:00:00		-	
	(Carefully clean up)			
	Parking Transactions * Retains the recent			
		Month	-	
	15 • • Execution Time	Watter		
			527	
	01:00:00		•	
	(Carefully clean up)			
	Patrol Transactions *			

Figure 15-15 Record Interface

15.1.6.2 Disk Space Cleanup

In this option you can set the frequency of the retains the recent and also clean up the selecyted days data.

Disk space c	cleanup		
	IVS Alarm Photos*		
	Retains the recent		
	7 • Day	•	
	Execution Time		
	01:00:00	•	
	Immediately Clean Up		

Figure 15-16 Disk Space Cleanup Interface

15.1.6.3 System

This option helps you to clean up the system operation log, device commands and database backup file.

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		

Figure 15-17 System Interface

15.1.7 Audio File

Click **System > Basic Management > Audio File** to open the following interface:

ZKBio CVSecurity	H				😫 admin 🛩
🔋 System Management 🗸 🗸	System / System Manag	gement / Audio Fili	9		
Operation Log	File Alias	Q	0		
Database Management Area Settings	O Refresh 🕁 Ne	w 🔋 Delete			
	File Alias	Size	Suffix	Operations	
E-mail Management	Alarm	20KB	W25V	<u>_</u>	
Dictionary Management					
Data Cleaning					
Audio File					

Figure 15-18 Audio File Interface

15.1.7.1 New

Operation Steps

Step 1: Click **System > System Management > Audio File > New**, the following window appears:

		New			×		
File Upload* File Alias* Size Suffix A Please upload	Brows a way or MPC	Not Uploaded		Play			
Save	and New	ОК	Cancel				

Figure 15-19 New Option

Step 2: Browse to upload an audio file locally. The file format must be in WAV or mp3 format and must not exceed 10MB in size.

Parameter	Description
File Alias (Name)	Enter the file name. Any character, up to 30 characters.
Size	After uploading the file, the file size is automatically generated.
Suffix	After uploading the file, the suffix of the file is automatically generated.

Table 15-3 Description New option parameter

15.1.7.2 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the Audio file page.

15.1.7.3 Edit

Click the file name or **Edit** to edit the audio file details which support replacing the audio files and editing the file name. The "size" and "suffix" automatically change depending on the size and type of audio file being uploaded. After editing, click **OK** and **Exit**.

15.1.7.4 Delete

Select the specified audio file to delete and click Delete. Then click **OK** to save the setting.

15.1.8 Certificate Type

The system initializes 9 certificate types. User can add the required certificate type for personnel and visitor registration.

Step 1: Click System> Basic Management > Certificate Type.

~	tefresh ∓ New 🗿	and the first state of the stat	
	Certificates number	Certificates Name Operations	
	1	ID	
	3	Passport	
	4	Driver License	
	8	Others	1
			1 the
			122

Figure 15-20 Certificate Type Interface

15.1.8.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the certificate type page.

15.1.8.2 New

Operation Step:

To add the certificates, click **System > Basic Management > Certificate Type> New:**

Certificate Name: Enter the certificate name.

	New	
Certificates Name*	1	 T.

Figure 15-21 New Option

15.1.8.3 Delete

Select the specified certificate to delete and click **Delete.** Then click **OK** to save the setting.

15.1.9 Print Tempalate

You can manage the template for different cards: Personnel card template, Visitor receipt template/Card template are all configured here. The system initializes 5 types of personnel and visitor print templates.

Step 1: Click System> Basic Management> Print template.

O Re	fresh ∓ New 😰 Delete			
	Template Name	Module	Operations	
	Visitar receipt	Visitor	(e)	
	Visitor print card(horizontal)	Visitor	(e)	
	Visitor print card	Visitor	(0)	
	Personnel print card(horizontal)	Personnel	(ø)	
	Personnel print card	Personnel	æ	

Figure 15-22 Print Template

15.1.9.1 Refresh

Click Refresh at the upper part of the list to get the most updated version of the Print Template page

15.1.9.2 Add

Step 1: To add the certificates, click **System > System Management > Print Template> New**:

Module Name* () Visitor () Personnel
Front*
Back*

Figure 15-23 New Option

15.1.9.3 Delete

Select the specified template to delete and click **Delete.**

15.1.10 System Monitoring

The system monitoring function displays the server processor usage, host memory usage, processor information, memory information, java virtual machine memory usage and other information.

Step 1: Click System> System Management > System Monitoring.

Proce	essor Usage	PC Memory	Usage		jvm Men	nory Usage
30 20 10 0	50 60 80 80 90 90 90 90 90 90 90 90 90 90 90 90 90	40 50 30 20 0 71.369	60 72 80 90		40 20 10 0 61	50 60 70 80 25% 100
Processor Info	rmation		Memory Informa	ation		
Attributes	Value		Attributes		Physical Host	jvm
Core Number	2		Total Space		8GB	1.86GB
System Usage	4.0196		Use Space		5.71GB	1.14GB
User Usage	65.32%		Remaining Space		2.29GB	737.17MB
Idle Rate	0%		Usage Rate		71.36%	61.25%
Usage Rate	80.33%					
Number Of Th	reads: 231				system Info	ormation
id	Name		Status		Attributes	Value
14	Druid-ConnectionPool-Create-1304522697		WAITING	.	OS Name	Windows Server 2019
15	Druid-ConnectionPool-Destroy-1304522897		TIMED_WAITING		OS Architecture	amd64
17	Catalina-utility-1		TIMED_WAITING		Java Version	1.8.0_265
18	Catalina-utility-2		WAITING		JVM runtime	8days 47min 49s
	container-0		TIMED_WAITING	-		
				*		
Number Of Net	twork Ports: 1					
	ipv4	Maximum Transmission Unit	Maximum Speed	Receiving Spe		ding Speed

Figure 15-24 System Monitoring Interface

15.1.10.1 Caching

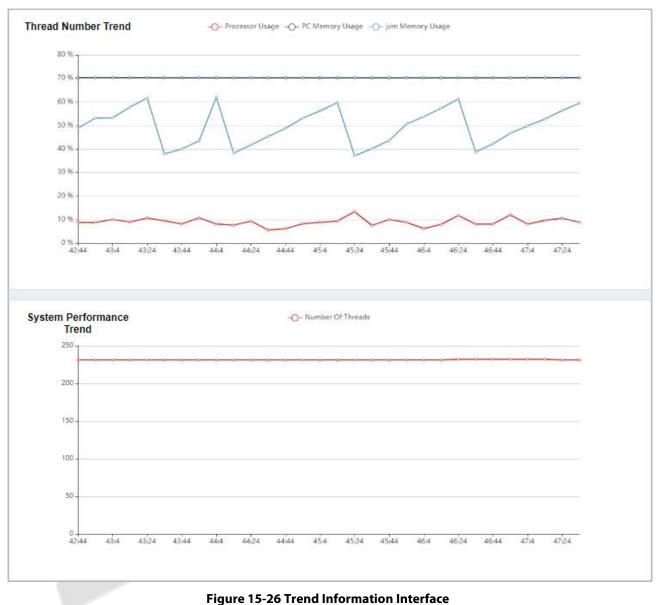
This option helps you to know about memory information, Redis information, client information and also current data base.

Abritules	Station	Alterrutes	Value
Number of Connected Clambs	39	Hada Vatalon	3.2.100
Number of Blockest Citeria	ů.	OS Architecture	Windowa 84
		opensition hours	8daya 4in 20min 25a
Memory Information		Statistics	
Allritules	Value	Allritulus	Value
Hax Memory	1.81M	Connectiona Received	et
Allocated space	5.82M	Comments Processed	41155531
Merrory Peak	13.90M	Instantations Ope Per Sec	35
Max Memory	25	Expired Keys	32355
Fragmanilation Katio	1.00	Evicled Keys	a
		Keyapaca Hita	63/7210
		Keyspiece Masses	2148666
Current Database:			
Allzfaules	Volum		
Number of keys	754		
Expired Keys	250		
Average TTL	32246591		

Figure 15-25 Caching Interface

15.1.10.2 Trend Information

This opton shows the graphical representation of processor usage , Pc memory usage and jvm memory usage.



15.1.11 Parameters

15.1.11.1 QR Code Setting

Step 1: Click System> System Management > Parameter > QR Code Setting.

00.0.1.0.1			QR Code Setting
QR Code Setting			DateTime Format Settings
	Enable QR Code		Video watermark
	🔿 Na 🖲 Yes		
	Qrcode Type		
	Static 💿 Dynamic		
	Valid Time:		
	300	second(30-300)	
	Switch between static QR code and dynamic QR code should be careful, frequent swit to device emort	ch may lead	

Figure 15-27 QR Code Setting interface

Step 2: Enable QR code Click System > System Management > Parameter > YES or NO for Enable the QR code

Step 3: Enable QR code If YES click **YES** > **Static**. It will be fixed the QR information same manner for the rest of time.

Step 4: Enable QR code If YES click **YES**> **Dynamic** > **Valid Time**. It will generate new QR code every 30 seconds.

15.1.11.2 Date Time Format Setting

Here you can set the date and time format.

Date	
2022-01-01	-
Time	
00:00:00	-

Figure 15-28 Date and Time Format Setting Interrface

15.1.11.3 Video Watermark

This option helps you to add watermark and tile to your videos.

Enable watermark	
🔿 No 💿 Yes	
Enable tiling	
🔿 No 💿 Yes	

Figure 15-29 Video WaterMark Setting

15.2 Authority Management

15.2.1 User

15.2.1.1 New

This section describes how to configure Step to add an administrator user in ZKBio CVSecurity.

Operation Step

Step 1: In the System module, choose Authority Management > User.

Step 2: Click Add to pop up the new user interface.

Step 3: On the Add role page, set role rights as required, as shown in the below Figure and the below Table describes parameters to be set.

	New	×	
Username*	Username should be composed between 1-30 characters	1	
	and in letters,numbers,or symbols (@/./-/+/_).	and the second	
Password*			
	Password is a composition of 4 to 18 characters, default		
	is 111111.		
Confirm Password*			
State	Enable 👻		
Multiple Login			
Maximum Number			
	Limit multiple login for the same account		
Superuser State			
Role	-		
Auth Department	· ·		
1	If you don't select department you will not have full		
	departmental permission.		
Authorize Area			
	If you don't select zone you will not have full zone		
	permission.		
Email			
First Name		_	

Figure 15-30 Adding User Interface

Parameter	How to set up
User Name/Password	You can customize the user's name and password used for login.
State	Set whether the user can log in and operate the system.
Connection Limit/Maximum Logins	If this parameter is not selected, the number of simultaneous logins is not limited.
Superuser Status	This parameter specifies whether the user has all rights by default. If you click this parameter, the user is a super user, and no role is required.
Role	Set a role for the user. The user has all Operation permissions configured for the role.
Authorize Department	Authorization Sets the department permissions of the user.

Parameter	How to set up
Authorized Permission	Authorization Sets the area rights that the user has.
Email	Customizes this user's mailbox, which can be used to retrieve the password.
The Name	Custom sets the name of this user.
The Fingerprint Registration	Register this user's fingerprint.

Table 15-4 Parameters for Adding a User

Step 4: Click **OK** to finish configuring the new user.

15.2.1.2 Edit/Delete

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

15.2.2 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.

15.2.2.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the user page.

15.2.2.2 New

Operation Steps:

Step 1: Click System > Authority Management > Role > New.

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

Step 3: Click OK to save.

				New	1					
Role Code* Role Name* Assign Permissions*										
Personnel	Access	Attendance	posid_module	Consumption	Elevator	Visitor	Parking	Patrol	Entrance Control	•
🗌 🖾 Card Manager										
	ment									

Figure 15-31 Add Role Option

15.2.2.3 Edit/Delete

Click Edit or Delete as required.

15.2.3 API Authorization

15.2.3.1 Refresh

Click **Refresh** at the upper part of the list to get the most updated version of the API authorization page.

15.2.3.2 New

Operation Steps:

Step 1: Log in to the system (as the super user, for exaportal.min) to enter the software. Click **System** > **Authority Management** > **API Authorization** >**New**, which must be unique, and a client secret, which will be used when the API is invoked.

Step 2: Only when the client ID and secret are added can the next API operation page be displayed normally. Otherwise, the access is abnormal):

		New	×	
	Client Id*	1		
	Client Secret*			
		Ł		
6 - 1				
0.5	C	K Cancel		

Figure 15-32 API Authorization Option

15.2.3.3 Browse the API

After the client ID and secret are added, click Browse API on the API Authorization page to skip to the API operation page (The page of the ZKBioSecurity system must be open for normal access of the API operation page). This page provides multiple APIs.

ZKBio CVSecurity	::: ¥				e admin
System Management >	System / Authority Mar	nagement / API Authorization			
🕽 Authority Management 🗸 🗸	Client Id	a @			
User	O Refresh 🐺 N	ew 🗊 Delete 🛱 Browse the API			
Role	Client Id	Client Secret	Creation Time	Operations	
API Authorization	SJC	EEB4F91EA8D070B47E378FC28FD99DFFDD430EBEC8BF3CC98DAEBBE110	2022-08-01 10:26:55	L û	
Client Register	lest	4ACBE6B07F9722F820E033C1C8C722FE063DDCB23096742AE1B81F054C96	2022-05-10 12:49:50	e û	
Security Parameters					

Figure 15-33 Browse the API

ZKBio CVSecurity	https://20.115.34.89/api/api-docs		Explore
AccDevice : acc device			
AccDevice : acc device		Show/Hide List Operations	
AccLevel : acc level		Show/Hide List Operations	
AccReader : acc reader		Show/Hide List Operations	Expand Operations
AccTransaction : acc transaction	1	Show/Hide List Operations	Expand Operations
AdMedia : ins adMedia		Show/Hide List Operations	Expand Operations
AttApply : att apply		Show/Hide List Operations	Expand Operations
AttAreaPerson : att area person		Show/Hide List Operations	Expand Operations

Figure 15-34 ZKBIO CV Security API Interface

When APIs are invoked, URLs of all request APIs must contain the access token parameter, whose value is determined by the client key configured on the background (if there are multiple keys, only one is selected), for example:



Figure 15-35 Request URL

The access token parameter must be added when the API is invoked (one request URL can be invoked):

http://localhost:8091/system/swagger/index.html?clientId=165391495<mark>3805#!</mark>/Person/getByPinUsingG ET.

15.2.3.4 Edit

Click the **Edit** icon to edit the API AUthorization details Enter the required Details. After editing, click **OK** and exit

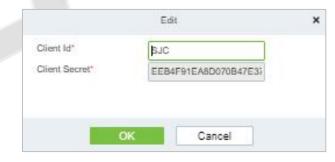


Figure 15-36 Edit Option

15.2.3.5 Delete

Select the specified Client id to delete and click **Delete.**Then Click **OK** to confirm the operation.

Pr	ompt
Are you sure you wa	nt to perform the delete ration?

Figure 15-37 Delete Option

15.2.4 Client Register

You can add client types for the system and generate registration codes for client registrations of each module function. The number of allowed clients is controlled by the number of allowed points.

IZKBio CVSecurity	##		e admin -
🕸 System Management >	System / Authority Management / Client Register		
🛿 Authority Management 🗸 🗸	Registration Code Client Type	• Q Q	
User	O Refresh ∓ New 😫 Reset 👔 Delete		
Role	Registratio Client name Registration K	Key Activ Activated D Creation Date Client Type Operations	
API Authorization	AE4C7E	○ 2022-06-20 08:08 APP Client-Ad 器 前	
Client Register	U OFESS8	⊖ 2022-05-10 05:48 APP Client-Ad 🇱 💼	
Security Parameters	7DB1CD	⊖ 2022-05-09 13:07 APP Client-Ad 闘 前	
	950A1A		
	1C40F0		

Figure 15-38 Client Register Interface

15.2.4.1 New

Step 1: Click **System Management** > **Authority Management** > **Client Authorization** > **New to go to** the **New** page.

	New	×
Client Type*		< 4
Registration Code*	223E15	
907		

Figure 15-39 Add Client Register

Parameter	Description
Client Type	The value can be APP Client, OCR-Personnel, OCR-Visitor, ID Reader- Personnel, ID Reader-Visitor or Signature- Visitor, Card Printing- Personnel, Card Printing-Visitor.
Registration Code	The registration code for APP Client is used under Network Settings on the APP login page and that for Print Card-Personnel is used under Parameter Settings > Client Registration . Only new registration codes added on the server are authorized and one registration code can be used by only one client.

Table 15-5 Description Add Client Register parameter

15.2.4.2 Reset

To reset a client, select the client and click **Reset**.

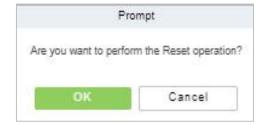


Figure 15-40 Reset Option

15.2.4.3 Delete

To delete a client, select the client and click **Delete**.

	Pr	ompt	
	Are you sure you wa ope	int to perform the delete ration?	
	ок	Cancel	
	Figure 15-41	Del <mark>ete O</mark> ption	
Click OK to delete the client.			

15.2.5 Security Parameters

Click System Management > Authority Management > Set Security Parameters.

			and the second
curity F	Parameters		Security Parameters
	Login Verification Code		
	Prompt after entering an error	•	
	Default Password Strength		
	None Wesk () Medium () Strong ()		
	Failed Login		
	5	▼ Time(s)	
	Account Will Lock		
	10	 minutes 	
	Password Valid Days(Day)		
	90	•	
	Password Modification		
	Forced to modify the password in login	*	
	Security Password Verification		
	Secure Password Authentication Interval		
	Nane	-	

Figure 15-42 Security Parameter Interface

• Login Verification Code Setting

It includes None, always prompt verification code, Prompt after entering an error.

Do not open verification code: The system allows no verification code

Open verification code: Users must fill in the verification code when logging in to the software.

Open after input error: The system will pop-up a verification box after filling in the wrong Username and password.

Password Strength Setting

The path is System -> Authority Management-> Set Security Parameter.

Default	Password 9	Strength	
O None	⊖ Weak ③	O Medium (2)	Strong (*)

Figure 15-43 Password Strength Option

Lock Account

The account will be locked if user fails to login the system as per the software setting. For example, if the system allows user fill in wrong username and password for 2 times. The system will be locked for 10 minutes after exceeding 2 times of operation.

Failed Login	
5	▼ Time(s)
Account Will Lock	

Figure 15-44 Lock Account

Password Valid Day (s)

Users can set the validity as 30days, 60daysor permanent. If password gets expired, user cannot login to the system.

Password Valid Days(Day)	
90	•

Figure 15-45 Password Valid Days

Password Modification

There are 2 options that user can set. Not mandatory and forced to modify the next time you login.

Not mandatory: The system does not need to modify the initial password.

Forced to modify the next time you login: It is compulsory to modify the initial password after the second login.

Forced to modify the password in login	÷
--	---

Figure 15-46 Password Modification Option

• Secure Password Authentication Interval

None	-	
------	---	--

Figure 15-47 Secure Password Authentication Interval

15.3 Communication Management

15.3.1 Device Commands

Step 1: Click **System > Communication Management > Device Commands,** the commands lists will be displayed.

ZKBio CVSecurity	######################################							e admin
2 System Management >	System / Commun	ication managemen	t / Device Commands					
Authority Management >	Submit Time From	1	To Serial Number		Back To Results	✓ More ▼	Q Q	
© Communication mana ~	O Refresh	🛱 Clear Commands	∱ Export					
Device Commands	ID	Serial Number	Content	Immed.	Submit Time	Return Time	Returne	Remarks
Communication Device	793	CKJF201760745	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRe	0	2022-08-03 00:00:47	2022-08-03 00:01:17	-1110	
Product	792	CKJF201760745	SET OPTIONS DateTime=728019247	0	2022-08-03 00:00:47	2022-08-03 00:01:17	-1110	
Authorized device	791	CL63202960014	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRe	•	2022-08-03 00:00:32	2022-08-03 00:00:35	1.	
Communication Monitor	790	CL63202960014	SET OPTIONS DateTime=726019232	0	2022-08-03 00:00:32	2022-08-03 00:00:34	0	
	789	5758204800001	DATA QUERY tablename=transaction,fielddesc=*,filter=NewRe	0	2022-08- <mark>0</mark> 3 00:00:17	2022-08-03 00:00:47	-1110	
	788	5758204800001	SET OPTIONS DateTime=726019217	0	2022-08-03 00:00:17	2022-08-03 00:00:47	-1110	

Figure 15-48 Device Comand interface

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.

15.3.1.1 Export

Export the command lists to the local host. You can export it 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 userauthorizeTi mezoneld=1Auth orizeDoorld=1 Pin=1AuthorizeTi mezoneld=1Auth orizeDoorld=1	false	2017-12-18 10:51:15	2017-12-18 10:51:21	0
1502	20100501999	DATA UPDATE mulcarduser Pin=2CardNo=5d ec02LossCardFla g=0CardType=0 Pin=1CardNo=44 12c5LossCardFla g=0CardType=0	false	2017-12-18 10:51:14	2017-12-18 10:51:21	o

Figure 15-49 Export File

15.3.1.2 Refresh

Click **Refresh** at the upper part of the list to load new temporary Device Commands.

15.3.1.3 Clear Commands

Click Clear Commands to Clear the command lists.

15.3.2 Communication Device

Step 1: Click **System > Communication Management > Communication,** you can view all equipment information and communication in the system. Detailed information such as accessed module, serial number, firmware version, IP address, communication status, and command execution can be viewed.

Madu	le	De	vice Serial Number	Devic	e Name		More - Q	Q		
O R	efresh E	C View authorized do	evice							
	Module	Device Serial	Device Firmware	Device Name	Device IP A	Subnet Mask	Gateway	Enable	Status	Executory Command C
	acc	CL64203960186	ZAM170-NF-1.5.12-TI-7364-03	ProFace X[TI]	10.10.20.73	255.255.254.0	10.10.20.1	0	Offline	21
	acc	5758204800001	ZAM170-NF-Ver1.8.17	xFace600	192.168.134.1	255.255.255.0	192.168.134.1	0	Offline	12
	acc	CKJF201760745	ZAM170-NF-Ver1.5.7	SpeedFace-V5	10.10.20.144	255.255.254.0	10.10.20.1	0	Offline	29

Figure 15-50 Communication Device Interface

15.3.2.1 View Authorized Device

View the authorized device information.

	v	iew authorized device	
P Address	Device Type	Device Serial Number	Q @
P Address MAC Address	Subnet Ma Gateway Addr	Serial Number Module Server Address	Device Type Communic
80.249.195.11		666721340000° att	•
192.168.2.179	255.255.255.(192.168.2.1	CMWN2147600 acc	SpeedFace-V5 😑
192.168.1.219	255.255.255.(192.168.1.1	660620510000; acc	Speedface-V5I 😑
171.103.248.1		CGGG1931600 pos	ProMerc-10 😑
192.168.134.1	255.255.255.(192.168.134.1	575820480000° acc	xFace600 🗢
0.0.0.0	255.255.255.(192.168.0.1	AYGZ19166000 acc	ProCaplure-W 😑
10.8. <mark>14.1</mark> 98	255.255.255.(10.8.14.1	BRID20166014 acc	in810460 Pro 🗢
0.0.0.0		CNN721506000	•
0.0.0.0		2022053112	•
192.168.0.141	255.255.255.(192.168.0.1	CL6320296001 acc	ProFace X[TI]
< 8			•

Figure 15-51 View Authorized Device Interface

15.3.2.2 Refresh

Click **Refresh** at the upper part of the list to load the new temporary Communication Device.

15.3.3 Product

Step 1: Click **System > Communication Management > Product,** and the product lists will be displayed.

ZKBio CVSecurity	::: #					
🕸 System Management >	System / Communication r	anagement / Product				
Authority Management >	Product Name	Product code		Q @		
Communication mana ~	O Refresh 🛛 🛱 New	🔋 Delete				
Device Commands	Product Name	Product code	Creation Time	Remarks	Operations	
Communication Device	LPR-300 Bangal	dJaaxoBI9Y5fVajn57IU	2022-07-04 12:06:39		6	
Product	LPRC300-XIAME	t 2RWBri5PydBoNsRYMFct	2022-07-18 03:35:23		2 1	
Authorized device	LPR-TEST	gLSkgDxAXHazswcvnArz	2022-07-22 09:07:04	for best connect	2 0	
Communication Monitor	best	7wN7Mn0yIS4wD6i75HMg	2022-07-25 08:13:59	best communication	2	

Figure 15-52 Product Interface

15.3.3.1 New

Click **System** > **Communication** Management > **Product** > **New**, to add the new product name.

	New	
Product Name*		
Remarks		ĺ

Figure 15-53 Add Product Option

15.3.3.2 Delete

Click **Delete** to delete the Product Operation.

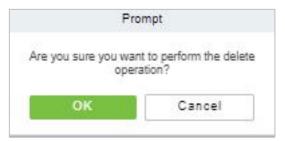


Figure 15-54 Delete Product Option

15.3.3.3 Edit

Click **Edit** to delete the Product information.

Product Name*	LPR-300 Bangalore	
Product code	dJaaxoBI9Y5fVajn57IU	
Remarks		

Figure 15-55 Edit Product Information

15.3.4 Authorized Device

Click **System > Communication Management > Authorized Device,** and the product lists will be displayed.

JZKBio CVSecurity	::: ¥						e admin
System Management >	System / Communica	tion management / Authorized device					
Authority Management >	Serial Number	Q &					
👔 Communication mana 🗸	O Refresh 🗗	New 🛨 Export Key File					
Device Commands	Protocol m	Serial Number Device secret	Product name	Product code	Module	Whether to Remarks	0
Communication Device		6667213400001			att	•	
Product		CGGG193160001			pos	•	
Authorized device	🗌 push	6606205100007			acc	•	
Communication Monitor	D push	CMWN214760004			acc	•	
	push	CKJF201760745			acc	0	

Figure 15-56 Authorized Device Interface

15.3.4.1 New

Click **System > Communication > Authorized Device >New,** to add the authorized product device.

Product name*	LPRC300-XIAM	EN 👻	
^p ratocal mode*	best-w	•	
Serial Number*			
Remarks			
		10	
		12	
		20	

Figure 15-57 Add Authorized Device

15.3.4.2 Export Key File

Click **System > Communication > Authorized Device**, Select the protocols to export and click the **Export Key File**, to export the key file of the authorized product device.

1	ZKBio CVSecurity			Ħ					e admin
8	System Management >	Syst	tem (Comm	unication management / Aut	thorized device			
1	Authority Management >	5	Serial	Number		2 @			
Ø	Communication mana 🗸		OR	efresh	Ξ+ New 🔶 Export Key I	File			
	Device Commands			Proto	col m Serial Number	Device secret	Product name	Product code	Module
	Communication Device				6667213400001				att
	Product				CGGG193160001				pos
	Authorized device			push	6606205100007				acc
	Communication Monitor			push	CMWN214760004				acc
				push	CKJF201760745				acc
				push	COOA221260001				acc
				1	Exp	ort Key File	×		ins
		×		pus)	Number of selected devices	1			acc
				pust	Active Time	hour(s)	1-72)		acc
				pust		-	_		acc
				pusi	Export	Close			acc

Figure 15-58 Export Key Option

15.3.5 Communication Monitor

Click **System > Communication > Communication Monitor**, and the communication mode will be displayed.

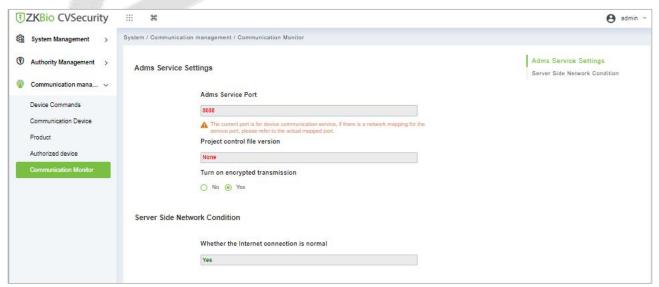


Figure 15-59 Communication Monitor

15.4 Third Party Integration

15.4.1 LED Device

The system integrated outsourcing LED equipment (control card: lumens 3200/4200), provides a window to display data; it can provide customers personnel in the access area quantity statistics, real-time information about personnel going in and out and personnel information in the area, etc.

JZKBio CVSecurity		e admin
System Management >	System / Third Party Integration / LED Device	
③ Authority Management >	Device Name Q	
Communication mana >	C Refresh 🛱 New 🔋 Delete 📽 LED Data 🐻 Manually defined content 📽 Synchronize All Data to Devices 👼 LED Template Management	More
👌 Third Party Integration 🗸	Device Name IP Address Port Default Pass Screen Screen Enable Automatic Dist LED Title	Operations
LED Device		
Digifort Camera		
Line Notification		
AD Management		
SMS Management		

Figure 15-60 LED Device

15.4.1.1 New

Operation Step:

Step 1: Click System> Extended Management> LED Device> New. The page is displayed as follows:

Device Name*	1
P Address*	34 CF - 59
Port*	5200
Default Pass Code*	255 · 255 · 255 ·
Screen Width*	
Screen Height*	
LED Title	
Block Number*	
Show Time	
Automatic Distribute Data	~
Delete data in device when new	
Block Layout	

Figure 15-61 Add LED Device

Parameter	Description
Device Name	Enter the name of the LED device.
IP Address	Enter the IP address of the LED device.

Port	Enter the port number. The default communication port is 5200.
Default Pass Code	Displays the pass code. The default value is 255.255.255.255.
Screen Width	Width of the dot matrix (resolution).
Screen Height	Height of the dot matrix (resolution).
LED Title	Select whether to display the title. If the parameter is left blank, the title is not displayed.
Block Number	Number of blocks that the LED is divided into (Note that the blocks do not contain the title and system time blocks).
Show Time	It will display time on the LED screen. Once you select it, you will find two options to choose from: Single Line and Multiline Display. Choose according to your choice.
Automatic Distribute Data	By default, this parameter is selected. You send data to the LED in the access control module only when you select this parameter. Otherwise, the content to be sent needs to be manually defined.
Delete Data in the Device When New	Delete the original data in the device when adding an LED device.

Table 15-6 Description Add LED Device Parameter

After you click **Block Layout**, the following box is displayed:

	6	Block1	(1280*18	0)		
		Block2	(1280*18	0)		
		Block3	(1280*18	0)		
	E.	Block4	(1280*18	0)		
Starting point Y, the vertex of the X axis, C> Block Layout	starting point o	f Y is I	the X axis	of the selected blo	ock and th	e left
Vertex of the X axis, Provide Block Layout Block1 Block2	starting point o the axis distan From X	fY is t ce. Wi	the X axis	of the selected blo	ock and th 1280 ▼	
Vertex of the X axis, P Block Layout Block1	starting point o the axis distan	fY is t ce. Wi	the X axis idth, heigt	of the selected blo It, width, height.		

Figure 15-62 Block Layout

*∝*Notes:

Parameters must be set for each block.

The height of each block must be equal to or larger than 12. Otherwise, the letters cannot be completely displayed.

The total height of all blocks cannot be larger than the screen height.

15.4.1.2 Delete

Click a device name or **Delete** under Operation in the device list and click **OK** to delete the device or click **Cancel** to cancel the operation. Select one or more devices and click **Delete** above the list and click **OK** to delete the selected device(s) or click **Cancel** to cancel the operation.

15.4.1.3 LED Data

LED data option let you view the details about outsourcing LED equipment such as zone device block details etc. user can add new LED data in this interface also.

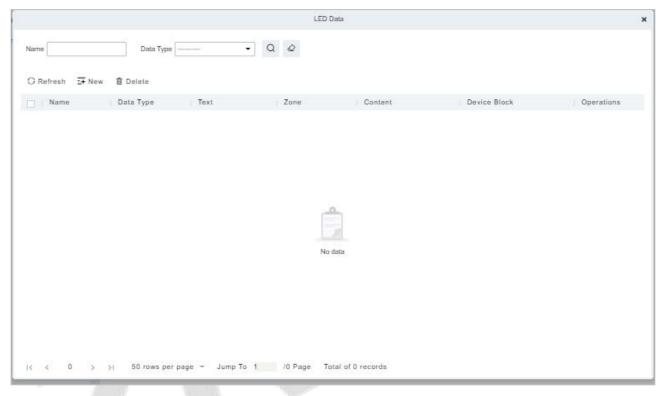


Figure 15-63 LED Data

15.4.1.4 Manually defined content

Select a device and click Manually Defined Content. The page is displayed as follows:

Device Name block-1	192.168.214.138 Please enter the content
DIDCK-1	1 have energied content
block-2	Please enter the content
block-3	Please enter the content

Figure 15-64 Manually Defined Content Option

∕≤Notes:

At least one block must be selected for the distribution of manually defined content.

After the manually defined content is selected, the access control module cannot send data to the LED device.

Contact the technical support team for the intermediate table, line notification, active directory page, and other materials.

15.4.1.5 LED Template Management

Through this function, you can create a template for the blocks. This template you can directly use at the time of adding an LED device. When you are adding an LED device, then after defining the dimensions of the block, you will be prompted to save the template as shown below:

	Template Number Q &		
	S Refresh ⊒ New 1 Delete		
	Template N Template Name Creation Date Operations		
		5	
	No data		
1			
R :			
2. 11	(< < 0 > ⇒) 50 rows per page ~ Jump To 1 /0 Page		

Figure 15-65 LED Template Managemnt

15.4.1.6 Synchronize All Data to Devices

Synchronize the LED block layout and LED data set in the system to the device. Select a device, click **Synchronize All Data to Devices**, and then click **Synchronize** to synchronize the data.

15.4.1.7 Edit

Click a device name or **Edit** under operation to go to the edit page. After editing the device, click **OK** to save the setting.

15.4.1.8 Enable/Disable

Select a device and click **Enable/Disable** to start/stop using the device. If the device is enabled, data is transmitted to the device. Otherwise, no data is transmitted to the device.

15.4.1.9 Restart

After you restart the device, the LED control card system will be restarted, data on the screen is cleared and data saved in the system is restored. After the device is successfully restarted, click **Synchronize All Data to Devices** to display all distributed content on the LED screen.

15.4.1.10 Modify IP Address

Modify the IP address of the device. The default IP address of the control card is 192.168.1.222.

15.4.2 Digifort Camera

It's integrated with third-party camera management system and the client uses "Digifort" to manage the cameras.

15.4.2.1 Sync with Server

It will help you to synchronize device with the server.

15.4.2.2 Delete

Click **Third Party Integration** > **Digifort Camera**, then select a Device Name, and click **Delete** > **OK** to delete.

Pr	rompt
Are you sure you wa ope	ant to perform the delete ration?

Figure 15-66 Delete Option

15.4.2.3 Parameters

Click **Third Party Integration** > **Digifort Camera** > **Parameters** > to update the server details.

	Digifort	
Server Port	8601	
Usemame		
Password		
		Server IP 8601 Usemame

Figure 15-67 Digifort Camera Device Parameters

Parameter	Description
Server Type	By default, the server settings "Digifort".
Server IP	Enter the Arteco Server IP.
Server Port	Enter the Arteco Server Port.Default value is 8601
Username	Enter the Arteco User Username.
Password	Enter the User Password.

Table 15-7 Description Digifort Camera Parameter

15.4.3 Line Notification

Click System > Third Party integration > Line Notification to enter the interface:

ZKBio CVSecurity		\varTheta admin 👻
😰 System Management >	System / Third Party Integration / Line Notification	
Authority Management >	Name Q. Q	
Communication mana >	C Refresh 🕮 Set Contacts 🔁 New 📵 Delete	
📩 Third Party Integration 🗸	Name Event Point Message T Notification Set Valid Ti Message H Message Tail Eff Remarks Contacts	Operations
LED Device		
Digifort Camera		
Line Notification		
AD Management		

Figure 15-68 Line Notification Interface

15.4.3.1 Refresh

Click **Refresh** at the upper part of the list to load the new temporary line Notification.

15.4.3.2 Set Contacts

Step 1: Add Line Integration. Log in ZKBio CVSecurity and go to System > Third Part Integration > Line Integration, then click Set Contacts.

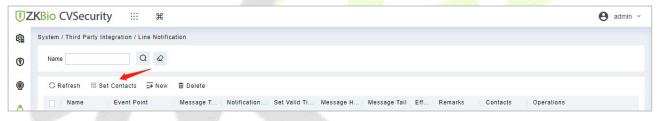


Figure 15-69 Set Contacts Option

Step 2: After the windows is displayed, please click New.

Set Contacts	×
Contacts Q	
⊖Refresh ∓New mi Delete	
Contacts Authorization Code	

Figure 15-70 Add Contacts Option

Step 3: After the windows is displayed, please click **Click to enter**.

	New			
Contacts*	500 1			
Authorization Code*				
			1	
Click to enter the line pa	ge and get the token:	Click to ente	1	
Click to enter the line pa	ge and get the token:	<u>Click to ente</u>	1	
Click to enter the line pa	ge and get the token:	<u>Click to ente</u>	[
Click to enter the line pa	ge and get the token:	<u>Click to ente</u>	1	
Click to enter the line pa	ge and get the token:	<u>Click to ente</u>	1	

Figure 15-71 New Option

Step 4: Line web page, please use the account and password of line to log in.

LINE	
使用其他方式整要 新疆 使用二维码登录	
忘记邮箱或密码?	

Figure 15-72 Line Interface

Step 5: After login, slide down and click Generate token.

2022.05.27 12.37 From: ISP To: young	
Generate access token (For developers) By using personal access tokens, you can configure notifications without having to add a web service.	
Generate token	
LINE Notify API Document	

Figure 15-73 Generate Token option

Step 6: Fill in the name of token and select the group you created earlier, then click Generate token

Note: The group you selected is used to receive Line-linked messages, please make sure that the group members do not disclose information security.

G	enerate token	\times
	ase enter a token name to be displayed before e ification.	each
н	lh	
Sel	ect a chat to send notifications to.	
	Q Search by group name	
	1-оп-т спас with LINE Notity	
	😳 Gr	- 1
	в н	- 1
	🕖 Ha	- 1
	😈 Hh 🛛 🥢	-
	e: Revealing your personal access token can allow a th names of your connected chats as well as your profile :	
	Generate token	

Figure 15-74 Generate Token Option

Step 7: Please click Copy.

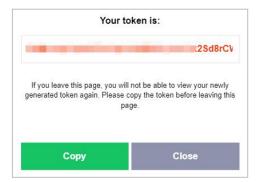


Figure 15-75 Token Interface

Step 8: Back to **ZKBio CVSecurity > System Page**, paste the Authorization Code and fill in Contacts.

Contacts*		
Authorization Code*		
Click to enter the line page a	nd get the token: Click to enter	
ener te enter tre inte page a	ger and tenter.	
	OK Cancel	

Figure 15-76 Add Contact Option

15.4.3.3 New

Step 1: Click **Third Party > Line Notification > New** to enter the Add Levels editing interface:

Name*	<u> </u>	
Event Point*	ZKT_Korea-1 +	
Message Type	All	
Set Valid Time	00 : 00 🔷 - 23 : 59 🗬	
Message Head		
Message Tail		
Effective	Enable 🝷	
Remarks		
Contacts*		

Figure 15-77 Add Line Notification

Step 2: Fill in all the required details and save. Once saved, you will get the template at the Line Notification device adding interface.

15.4.3.4 Delete

Click **Third Party** > **Line management**, then select a receiver, and click **Delete** > **OK** to delete.

15.4.4 AD Management

15.4.4.1 Server Configuration

Operation Step:

Step 1: In the System module, select Third Party Integration > AD Management.

Step 2: In the **AD Management** interface, fill in the **Server Configuration** as required in the details below.

erver conf	iguration	Server configuration AD field setting
Server address Idap://localhost:389 User name Password		Synchronize permission group inf AD data timing import
	Domain no <mark>d</mark> e	

Figure 15-78 Ad Management Interface

15.4.4.2 AD Field Setting

Operation Step:

Step 1: In the System module, select Third Party Integration > AD Management.

Step 2: In the AD Management interface, fill in the AD field setting as required in the details below.

Database Fields		Import AD fields	
Personnel ID	•	Description	•
First Name	•	name	•
Last Name	٠	Last name	•
Department Name	•	Department	•
Mobile Phone	147	Mobile	-
Email	1470	Email	
	•	(• 🛞

Figure 15-79 AD Field Setting

15.4.4.3 Synchronize Permission Group Information

Operation Step:

Step 1: In the System module, select Third Party Integration > AD Management.

Step 2: In the **AD Management** interface, fill in the **Synchronize permission group information** as required in the details below.

Synchroniz	e permission group information
	Synchronization permission group Synchronize members in permission group Domain Node
	Please perform the synchronization permission group first, otherwise the synchronization may fail.
	Test connection

Figure 15-80 Synchronize Permission Group Information

15.4.4.4 AD Data Timing Import

Operation Step

Step 1: In the System module, select Third Party Integration > AD Management.

Step 2: In the AD Management interface, fill in the AD data timing import as required in the details below.

Incremental synchronization (minutes)			
30			
Import now			
Global synchronization			
Every 3 Day	0	Dots	
Import now			
ОК			

Figure 15-81 AD Data Timing Import

15.4.5 SMS Management

The SMS Management feature helps in sending text messages to the personnel in case of any access or elevator event. If the checkbox is selected, the message will be sent to the corresponding person.

TKBio CVSecurity		😝 admin ~
@ System Management >	System / Third Party Integration / SMS Management	
Authority Management >	Receiver Q Q	
Communication mana >	C Refresh	
📩 Third Party Integration 🗸	Receiver Send Time Status	
LED Device		
Digifort Camera		
Line Notification		
AD Management		
SMS Management		

Figure 15-82 SMS Management Interface

15.4.5.1 Refresh

Click **Refresh** at the upper part of the list to load a new temporary SMS Management.

15.4.5.2 Delete

Click **Third Party** > **SMS Management**, then select a receiver, and click **Delete** > **OK** to delete.

15.4.5.3 SMS Parameter Settings

Supports sending text message to Personnel once any access or elevator event occurs.

After selecting the checkbox next to the Mobile Number, the system will send an email to the relevant person once access or an elevator event occurs.

SMS Parameter Settings			
Port*			
Phone Number*			
SMS Service Center Number*		Get	
Receiver Content	Test Send		

Figure 15-83 Modern SMS Parameter Setting

Figure 15-84 AWS-SMS Prameter Settings

16.1 Facekiosk Device

16.1.1 Device

Device	Device Sarial Number Device Name Q &
Set Attendance By Area	
Set Attendance By Person	C Refresh
Set Attendance by Person	Device Serial Number Device Name Device Model IP Address Area Name Enabled Status Register Personnel Commands to be E Operations
	🗌 <u>CGWD205060010</u> <u>CGWD205060010</u> FaceKiosk-H13A 192.168.134.103 Area Name 🥥 Offline 📀 4 3 🖉 💼 🛛

Figure 16-1 Device

16.1.1.1 Delete

Select one or more devices and click **Delete** at the upper part of the list and click **OK** to delete the selected facekiosk device. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single device.

16.1.1.2 Search Device

In the tool bar, select the "Search device" menu. Add the device to the software server.

Solution Note: User need to entry the hardware deivce and setting some paramter which is supported to setting the software server address.

16.1.1.3 Control

Click **FaceKiosk Device** > **Device**, then select Control to Enable/ Disable, Reboot, synchronize software Data, and Issued QRCode Address of the device.

Function	Description
Enable/ Disable	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.
Reboot Device	It will reboot the selected device
Synchronize software Data to the Device	Synchronize data of the system to the device. Select device, click Synchronize All Data to Devices and click OK to complete synchronization.
Issused QRCode Address	Select the Issused QRCode Address.

Table 16-1 Device Control

16.1.1.4 View / Get

Click **FaceKiosk Device** > **Device**, then select View/Get to Get Device Option, View Device Parameters, Reupload Data, and to Gets the Specified Person Data.

Parameters	Description				
Get Device Option	It gets the common parameters of the device. For example, get the firmware version after the device is updated.				
View Device Parameters	Show the capacity detail.				
Reupload Data	Select the device in which you want to upload data. Click to enter the check box to upload the data type: attendance record/personnel information/attendance photo, click the confirmation to get such information again from the device.				
Gets the Specified Person Data	It gets the Specified person Data from the device.				

Table 16-2 Device View/Get

16.1.1.5 Clear Device Data

Click **FaceKiosk Device** > **Device**, then select Clear Device Data to clear Device Command, Verificaton Photo and Validation Record.

Parameters	Instruction
Clear Device Command	Select the device to be cleared. It clears the operation command issued by the software in the setting.
Clear Verification Photo	Select the device. This function will clear all the verificationn photo records from the device.
Clear Validation Record	Select the device. This function will clear all the validation data records from the device.

Table 16-3 Clear Device Data

16.1.1.6 Edit

Click advertisement resources or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

16.1.2 Set Attendance by Area

Click FaceKiosk > FaceKiosk Device, then Select Set Attendance by Area.

JZKBio CVSecurity	::: ¥								
FaceKiosk Device ~	FaceKlosk / FaceKlosk I	Device / Set Attenda	ince By Area						
Device	Area	Area				Browse Personnel XMBelong Areas			
Set Attendance By Area	Area Number	An	ea Name	Q @		Personnel ID Name	More - Q 🖉		
Set Attendance By Person	🔾 Refresh 🛛 🛱 Syr	ichronize People In	The Area			🔿 Refresh 💼 Delete Personnel			
	Area Number	Area Name	Personnel Quantity	Operations	Personnel ID First Name Last Name Department				
	0.1	Area Name	17	<u>음</u> +		1116	Department Name		
	2	ХМ	1	울 +					
	3	T Campus	1	8⁺					

Figure 16-2 Set Attendance by Area

Synchronize People in the Area 16.1.2.1

Click > FaceKiosk > FaceKiosk Device > Set Attendance by Area, then select Synchronize People in The Area.

Click **OK** to save and exit.

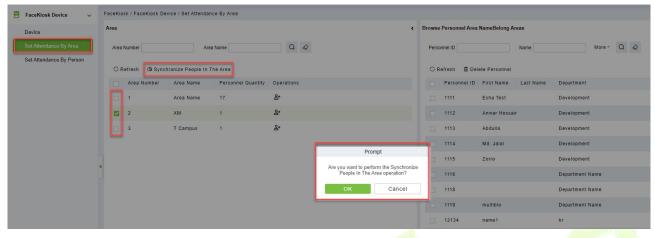


Figure 16-3 Set Attendance by Area

16.1.3 Set Attendance by Person

Click > FaceKiosk > FaceKiosk Device, then Select Set Attendance by Person.

			Name	More *	Q &	Area Number Area Name Q
By Person	Personnel ID		Hume	more	G G	
	C Refresh					◯ Refresh 菌 Delete the area
	Personnel ID	First Name	Last Name	Department Name	Operations	Area Number Area Name
	10002	raj	h	hr	•	1 Area Name
	10001			Department Name	⊡	
	1	tang	OP1	Department Name	\bullet	
	9527			Department Name	•	
	2	tsf		Department Name	•	

Figure 16-4 Set Attendance by Person

16.2 Media Advertisement Resources

16.2.1 Advertisement Resources

Click > FaceKiosk > Media Advertisement Resources, then Select Advertisement Resources.

In the Advertisement resouces module, it can support to create/edit/delete advertisement resources.

16.2.1.1 Add (New)

Support to upload some new advertisement resources to software server.

	New		×		
Medium Type*	Image	*]			
Media Resource Type*	Local Resource				
Media Name*	1				
- 1 - 1	ALL	1 - 1			
File Upload*	Browse Not Upload	aed			
File Upload"	Browse Not Upload	led			
Flie Upload"	Browse Not Upload	ied			
File Upload.	Browse Not Upload	160			
File Upload	Browse Not Upload	Jea			

Figure 16-5 Media advertisement Resources

16.2.1.2 Edit

Click device name or **Edit** in the operation column to go to the Edit page. Make modifications and click **OK** to save modifications.

16.2.1.3 Delete

Select one or more advertisement resources and click **Delete** at the upper part of the list and click **OK** to delete the selected advertisement resources. Click **Cancel** to cancel the operation or click **Delete** in the operation column to delete a single advertisement resource.

16.2.2 Advertisement Settings

Click > FaceKiosk > Media Advertisement Resources, then Select Advertisement Settings.

This module support to create Edit and Delete the advertising.

ZKBio CVSecurity	¥	
FaceKiosk Device >	FaceKiosk / Media Advertisement Resources / Advertisement Settings	
🚇 Media Advertisement 🗸	FaceKiosk Device	< Ad
Advertisement Resources	Device Name	Media Name Q 4
Advertisement Settings	C Refresh	🔾 Refresh 💼 Delete
	Device Serial Number Device Name Operations	Media Name Medium Type
	CGWD205060010 CGWD205060010 國	test Image



16.3 FaceKiosk Reports

16.3.1 Verification Record

Click > FaceKiosk > FaceKiosk Reports, then Verification Record to view specified events in specified condition.

FaceKiosk Device >	FaceKiosk / FaceKiosk Reports / Verifica	tion Record
Media Advertisement >	Time From 2022-05-05 (To 2022-08-05	2 Personnel ID Name More - Q Q
🔟 FaceKiosk Reports 🗸 🗸	^ر م ^{لا}	C Refresh ⊥ Export
Verification Record	Department Name Development hr Detest3 h test3 h test4 h test6 h test7	Personnel ID First Name Last Name Department N Area Name Device Serial Num Verification Time Verify p Data S

Figure 16-7 Verification Record

16.3.1.1 Export

Export the operation log records, save to local. You can export to an Excel, PDF, TXT or CSV file. Click Export See the following figure.

Encrypt or not	🔿 Yes 💿 No	
File Format	EXCEL -	
Data to Export	 All (max 100000 records) 	
	O Selected (max 100000 records)	
1	Start Position 1	
12 3	Total Records 100	
10 11		
0.11		
1997 - Carlos Ca		
	OK Cancel	
15	Cancer	

17 Hotel System

It provides hotel service management functions covering check-in, overstay, check-out, rate settlement, and lock setup and management.

Operation Guide

It helps you quickly understand how to quickly navigate to specific function pages and configure and use the hotel management software.

17.1 Device Management

For 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.

17.1.1 Device

Operation Steps:

Step 1: In the Hotel module, select Device management > Device.

Step 2: On the device interface, click the Search button to pop up a search box.

Step 3: Click "**Start Search**" in the search box to display the **Access Devices** that can be added, as shown in Figure 17-1.

			Search		
Search Total Progress	No device found? Down 100% Devi		Local Disk Searched devices count:1 Number of devices added:1 Serial Number	\otimes	
IP Address	MAC Address	Subnet Mask	Gateway Add Serial Number	Device Type Set Server	Operations
192.168.134.16	38	255.255.255.0	192.168.134.254 CN3M212460001	TDB08M-TI/M	This device has b
A The current sv	stem communication port	is 8088, please make s	ure the device is set correctly.		
			Close		

Figure 17-1 Device Search and Add Interface

Step 4: Optional: Modify the IP address of the **Access Control** device, click "**Modify IP Address**", the device will be restarted after modifying the IP address, and the IP address modification will be completed after the restart.

Step 5: For the searched devices, click the Add button in the operation bar to add the device.

Step 6: Click **OK** to complete the operation of adding devices. After the operation is completed, the device will restart, and the device will be added after the restart is complete.

Step 7: Click **Close** to close the device search and add interface.

TZKBio CVSecurity			e adm
Device Management 🗸	Hotel / Device Management / Device		
Device	Gateway	<	Lock
	Gateway Name Gateway MAC Address Q 🖉		Lock Name Lock MAC Address
	○ Refresh Q Search		O Refresh @ Sync Time
	Gateway Name Gateway MAC Addr Pairing Sta Gateway St Operations		🗌 Lock Name Lock MAC Roo
	«		
			A
	Figure 17-2 Device Interface		397 () - 23 F

• Enable Paring Mode

Select device, click **Enable** to 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.

Disable Paring Mode

Select device, click **Disable** to stop using the device. When **com**munication 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.

• Synchronize Time

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

Emergency Unlock/ Cancel Emergency Unlock

A master card can be used to unlock all the rooms of the hotel within its validity period. By default, Disable Indoor Locked is selected. You can specify whether to enable the Always Open mode. And you can cancel the by clicking **Cancel Emergency Unlock.**

• Get Unlock Records

Select device, click **Get Unlock Records** to start using the device. We can get the unlock doors records.

• Enable

Enable the device. Only enabled devices can be normally used. Select the device to be enabled and click **Enable**.

• Disable

Disabled devices cannot be normally used. Select the device to be disabled and click **Disable**.

• Delete

Select one or more locks to be deleted and click **Delete** to delete lock in batches.

17.2 Room Management

17.2.1 Room Monitor

The function allows users to handle room services and check the hotel room occupancy, such as the total number of rooms, number of available rooms, and number of available rooms of a specific room type.

Operating Steps:

Step 1: In the Hotel module, click Room Management > Room Monitor.

Step 2: You can view relevant monitoring card and data statistics in the monitoring room interface, as shown in Figure 17-3.

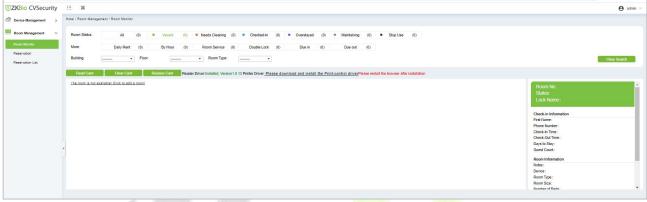


Figure 17-3 Room Monitoring

17.2.2 Reservation

You can check the check-in and reservation status of all rooms in a specified period and process room reservation.

Choose **Hotel Management** > **Room Management** > **Reservation**. The page shown in the following figure appears.

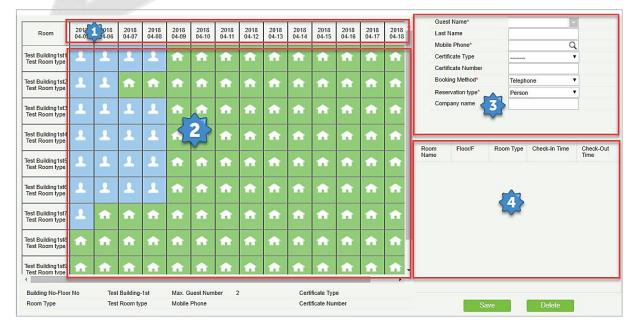


Figure 17-4 Reservation

Page Description:

(Available dates): By default, a 15-day period (starting from the current system date) is displayed. You can change the displayed period with the Reservation Date Range parameter on the Hotel Information page.

The room reservation time ranges from 12:00 on the reservation start date to 12:00 on the reservation due date. You can change the time point with the Default Check-Out Time parameter on the Hotel Information page.

(Available rooms): All rooms in the hotel are displayed. You can specify the start and end time and room type to query for a required room.

Room status **w** indicates that the room can be reserved for the time period.

Room status 🚰 indicates that the room is occupied in the time period and cannot be reserved.

Room status 🛄 indicates that the room has been reserved for the time period.

Solution Note: If a room is used by guests, and will be checked out in the reservation period, the room will be displayed among the available rooms, but cannot be reserved before it is checked out.

Guest information of the reservation.

Information about the rooms selected for reservation.

17.2.2.1 Reservation process

Step 1: Click the room and date for reservation. The selected date of a room turns into red as **1**. You can click the room and date again to cancel the selection. You can select multiple rooms of the same date, multiple dates (continuous only) of one room, or multiple dates (continuous only) of multiple rooms.

After selection, the information about the selected rooms are listed in 4 in the right part of the Reservation Center page.

Step 2: Fill in the guest information, including the name, mobile phone, certificate number, and the booking method (telephone or reception desk).

Step 3: Click Save.

17.2.3 Reservation List

You can query, edit, delete, and handle check-in for a reservation.

Choose **Hotel Management > Room Management >Reservation List**. The page shown in the following figure appears.

You can also enter the guest's name and mobile phone number to query for a required reservation.

TZKBio CVSecurity	H X	\varTheta admin ~
Device Management	Hope/ Ason Management / Reservation Lat	
🛄 Room Management 🗸 🗸	For here E-cel Mon - Q Q	
Room Monitor	Offiches 37 New Bolets	
Reservation	📄 Booking fundeer Frankanne Laar Name Vachle Number Email Booking Time Schedule Chascin	
Reservation List		
	<u>A</u>	
	No data	

Figure 17-5 Reservation list

17.2.3.1 Managing Check-in

Select the guest's name of a reservation, click **Check-In** under **Operations**. The **Individual Check-In** page appears.

evice Management >	Guest Name The current query condition	Mobile Pl	none	Q (8)			
oom Management 🛛 🗸 🗸	C+ Refresh 👚 Delete						
oom Monitor	Guest Name	Mobile Number	Booking Method	Reservation type	Reservation Time	Operations	
eservation	Q Guest2	3214569874	Telephone	Person	2018-04-05 17:54:19	Check-In Edit Delete	
	<u> </u>	elect Guest)			2. Click Check-in	

		dividual Check-In		
Room Name*	Test Building1st2 V			
Certificate Type*	ID 🔻			
Certificate Number*	54445242			
Guest Name*	Guest2		2	
Last Name	хуz			
Gender	T			N
Mobile Phone	3214569874	(Optimal Si	ze 120*140).	3
Booking	3214569874	Ø Browse	Capture	
E-Mail				
Emergency Contact	Please enter mobile phone			
Home Address		2		
Checkin Type*	Daily Rate Room O Ho	ourly Rate Room		
Stay Days*	1	Guest Count	1	•
Check-In Time	2018-04-06 10:08:20	Check-Out Time	2018-04-06 12:00:00	
Discount (%)		Daily Rate*	20.0	
	10.0	Amount Payable*	30.0	
Discount (%)	10.0			

Figure 17-7 Individual check -in

The system automatically loads the reservation information of the room. Modify and complete the guest information and click Check-In. The **Registration or Issuing** page appears as shown below.

oom Name		Test Buildir	ng1st2		
oom Type		Test Room	type		
heck-In Time		2018-04-06	6 10:08:20		
heck-Out Tim	ne	2018-04-07	12:00:00		
nly registered	d, no card				
ertificate Typ	e*	ID	Υ.		
ertificate Nur	nber*	54445242			
uest Name*		Guest2			
ast Name		xyz			
levator/Acces	ss Con <mark>trol</mark>		-		
egistered Ca	rd Quantity: 0	Remaining Guest Qu	uantity: 1		
uest Name	Last Name	Certificate Type	Certificate Number	Card Number	

Figure 17-8 Registering or issuing

Place the guest card on the card writer and click **Write Card** and complete to complete check-in.

Notes: You cannot process check-in for an expired reservation. Check-in can only be processed on site. For details, see Individual check-in in section. The guest can check in before the reserved time.

17.2.3.2 Editing/Deleting Reservation

Select the guest's name of a reservation, click Edit under Operations.

K <mark>Bio</mark> CVSecurity	###		Sec.				
Device Management >	Guest Name	Mobile Pho	50e	Q (8)			
	The current query condition	ns: None					
Room Management 🛛 🗸 🗸	C Refresh 👚 Delete						
Room Monitor	Guest Name	Mobile Number	Booking Method	Reservation type	Reservation Time	Operations	
	Guest2	3214569874	Telephone	Person	2018-04-05 17:54:19	Check-In Edit Delete	
Reservation							
Reservation List							
	1. Se	elect Guest				2. Click Edit	
	1. Se	elect Guest				2. Click Edit	
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit	
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit	
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit)
	1. Se	elect Guest				2. Click Edit)

Figure 17-9 Editing and Deleting Reservation list

The below reservation page will be displayed. You can change a room or modify the guest information for the reservation. Modify the details accordingly and click **Save.**

TZKBio CVSecurity	::: ¥
Device Management >	Hotel / Room Management / Reservation List
🕮 Room Management 🗸 🗸	First Name Mobile Number E-mail More * Q Q
Room Monitor	C Refresh ⊒ New
Reservation	Booking number First Name Last Name Mobile Number E-mail Booking Method Booking Time Scheduled Check-in Time Scheduled
Reservation List	

Figure 17-10 Edit Reservation list

17.2.3.3 Delete

Select the guest's name of a reservation, click **Delete** under **Operations** or the **delete** button on the top of the list to delete the reservation. Click **OK** to confirm the **delete** operation.

17.3 Card Management

You can create different types of cards for setting and managing room locks based on daily hotel business management requirements. Holders of the cards are employees of the hotel. You need to add the holders using the HR module and specify their departments using the hotel module, so that you can select the holders when issuing management cards.

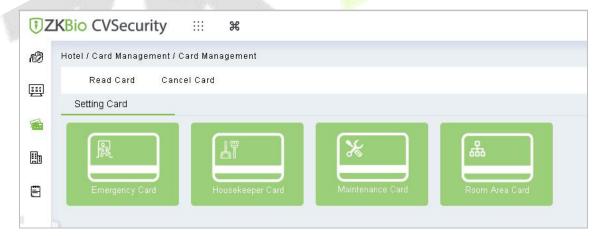


Figure 17-11 Card Management

17.3.1 Read Card

In the **Hotel** module, click **Card Management** > **Read Card**. After download the reader driver, you can read the card.

17.3.2 Cancel Card

In the **Hotel** module, click **Card Management** > **Conceal Card**. After download the reader driver, you can cancel the card.

17.3.3 Setting Card

You can set the basic information, including authorization, time, room number, and area information about locks of the hotel.

17.3.3.1 Room Area Card

In the **Hotel** module, click **Card Management** > **Setting Card** > **Room Area Card**. A room area card is used to unlock rooms in a specified area. If a room is within the specified area, the card can unlock the room.

Cardholder Name*		
Last Name Card Expiration Time* Hotel Facility*	2022-08-02 17:25:36	

Figure 17-12 Room area card

Parameter	Description
Card Holder Name	Enter the Card holder name
Card Expiration Time	Display the card expiration time
Hotel Facility	Display the hotel facilities.

Table 17-1 Parameter Setting Card

17.3.3.2 Emergency card

In the **Hotel** module, click **Card Management** > **Setting Card** > **Emergency Card**. A master card can be used to unlock all the rooms of the hotel within its validity period. By default, **Disable Indoor Locked** is selected. You can specify whether to enable the Always Open mode.

Cardholder Name*		
Last Name		
Card Expiration Time*	2022-08-02 17:26:17	

Figure 17-13 Emergency Card

Parameter	Description
Card Holder name	Enter the Card holder name
Card Expiration Time	Display the card expiration time

Table 17-2 Parameter emergency card

17.3.3.3 Maintenance Card

In the **Hotel** module, click **Card Management** > **Setting Card** > **Maintenance Card**. A maintenance card can be used to maintain and manage room locks of the hotel.

	Maintenance Card		×	
Cardholder Name* Last Name				
Card Expiration Time*	2022-08-02 17:42:3	81		
Building Name*		•		
Floor Name				
Write				
	Card Close			

Figure 17-14 Maintenance Card

Parameter	Description
Card Holder name	Enter the Card holder name
Card Expiration Time	Display the card expira <mark>tion t</mark> ime
Building Name	Display the building Name.
Floor Name	Enter the floor name and number.

Table 17-3 Parameter Maintenance Card

17.3.3.4 House Keeping Card

In the **Hotel** module, click **Card Management** > **Setting Card** > **House Keeping Card**. A house keeping card can be used to unlock rooms in a specified area in unlocking mode within its validity period.for house keeping.

Cardholder Name*			
Last Name			
Card Expiration Time*	2022-08-02 17:4	43:11	
Building Name*		•	
Floor Name		•	

Figure 17-15 Housekeeper Card

Parameter	Description
Card Holder name	Enter the Card holder name
Card Expiration Time	Display the card expiration time
Building Name	Display the building Name.
Floor Name	Enter the floor name and number.

Table 17-4 Parameter Housekeeper Card

17.3.3.5 Employee Card

In the **Hotel** module, click **Card Management** > **Setting Card** > **Employee Card**. You can create various access/elevator control cards, such as master cards and emergency cards for hotel personnel to manage hotel services.

17.4 Hotel Management

17.4.1 Hotel Settings

You can set the basic information about a hotel, including its name, address, phone number, fax number, zip code, website address, and email address. You can also set the function parameters regarding the check-in time, check-out time, check-out reminder, and access/elevator control permissions.

Click **Hotel Management > Hotel Info Settings**. The page shown in the following figure appears.

TZKBio CVSecurity	::: ¥					
Device Management >	Hotel / Hotel Managemen	nt / Hotel Settings				
	Hotel Information					
Room Management >	Hotel Name*					
Card Management >	Telephone					
Card management. 7	Fax					
📕 Hotel Management 🗸	Zip/Post Code					
Hotel Settings	Website					
	E-mail					
Room Type	Hotel Logo Ch	Choose File No file chosen				
Room]				
Hotel Facility						
Booking Method						
	The	e image should not exceed 100KB(JPG, BMP	GIF, and. PNG are supported only). T	The ratio of length to width she	ould be 2:1 to reduce the type variable.	
	Hotel Option Settings					
	Earliest check-in time*	12 V: 00 V (hh:mm)	Default Check-Out Time*	12 V: 00 V (hh:mm	1	
	< Default Check-In Time*) (Half-day room rate will be added.)	
	Latest check-in time*	23 V: 00 V (hh:mm)) (Overstay will be charged on day rate.)	
	Maximum Booking Days"		Housekeeping Window Hours		(minutes)	
	Days to Stay by Default*		Currency Type"	USD 🔻	(minutes)	
	Hours to Stay by Default		Currency type	USD V		
		it* 3 (hour)	2.22		2	
	Тах Туре		Tax Rate		% 	
	Other Charge Type		Other Charge Rate		5	
	Unit of Room Acreage	ft" 🔹				^
						\sim
	Hotel Card Settings					
	Card Password*					
	Repeat Password*	Card sectr	or and password cannot be changed aft	ter issued.		
	Card Sector: Sec	ector 3 •				
	Default Net Card					
	Default Net Card	Cancel Card				

Figure 17-16 Hotel Setting

Parameter	Description
Default Check-In Time	You can set this time yourself. If a guest checks in before this time, the check-out date is the current day if the guest stays for one day. Otherwise, the check-out date is the next day.
Default Check-Out Time	It specifies the end time of a day use room
Overstay Check-Out Time 1/2	You can set this time yourself. If a guest checks out at a time between Overstay Check-Out Time 1 and Overstay Check-Out Time 2, the guest must pay an overstay charge. If a guest checks out at a time after Overstay Check-Out Time 2, the guest must pay for an extra day.
Reservation Date Range	It is the period for which the advance booking can be started.
Default Staying Days	It specifies the default number of days a guest stays. Generally, a guest stays for 1 day.
Default Staying Hours	It specifies the user-defined minimum number of hours a guest may stay. If a guest stays for a period less than this limit, the guest is charged the rate corresponding to this limit.
Elevator/Access Control	After selecting this check box, you can select an access/elevator control level on the card issuing UI, so that an issued card can be used not only as a hotel card, but also used to access the devices corresponding to the selected level. (>> Note: This check box is available on the Hotel Settings page only after you use the access control module and/or elevator control module and obtain and activate a license.)
Tax/Tax Rate:	You can mention the tax name and the percentage below.
Other Charges/Rate	It specifies any other ki <mark>nd of</mark> taxes, depending on the region.
Cleaning Time Limit:	It specifies the time available for cleaning a room after a guest checks out.
Checkout Remind:	It specifies whether to display a reminder one hour before checkout.
Currency Type	It specifies the currency.

Table 17-5 Parameter Hotel Setting

Note: The hotel management system can be used to define buildings, floors, and rooms as well as handle check-in requests only after you set these parameters.

17.4.2 Room Types

You can design information about various types of room, such as the number of beds and number of guests allowed. You can also enable and disable the vacant rooms.

Click **Room Management > Room Type > New**. The page shown in the following figure appears.

	Hotel Information	
tel Information		
otel Name*		
elephone		
эх		
p/Post Code		
lebsite		
-mail		
otel Logo	Choose File No file chosen	
	The image should not exceed 100KB(JPG, BMP, GIF, and, PNG are supported only). The ratio of length to width should be 2:1 to reduce the type	
	variable.	
tel Option Setting	js	
	More	
	\sim	
tel Card Settings		

Figure 17-17 Room types

 $\ll \gg$ Note: When you add a room type, the system checks whether hotel setting is configured. If no, you are redirected to the settings page. All room types must be unique.

17.4.2.1 Delete

Select room type, click **Delete**, and click **OK** to delete the room type.

17.4.2.2 Disable/Enable

Select room type, click **Disable/Enable** to stop/start using the room. The status of the room visible according with the enable or disable option.

17.4.3 Room

17.4.3.1 Adding Guest Rooms

Click **Room Management > Room > New.** The page shown in the following Figure 17-18 appears.

Building No*		•	
Floor No*			
Room Type*		•	
Start Room Number*			
Room Count*			
Remark			
oom name generation ru umber	Iles: Building No. + F	loor No. + Roo	om

Figure 17-18 Add Rooms

Select the desired Building, Floor and Room type.

Description
It specifies the start number of r <mark>ooms</mark>
It specifies the number of rooms to add. The value 1 indicates only one room is added. A value greater than 1 indicates that a batch of rooms is added
It describes about the room

Table 17-6 Parameter Room

✓≫Note: All room names must be unique.

17.4.3.2 Editing Guest Room

Select one guest room and edit the guest room. Duplication of guest room names are not allowed. Guest rooms that have been checked in or booked cannot be edited. See the following figure.

	Edit	
Building No*	BZ	•
Floor No*	20CENG	¥
Room Type*	BZ	•
Start Room Number*	1	
Room Count*	1	
Remark		
Room name generation ru Number	iles: Building No. + Fl	oor No. + Room

Figure 17-19 Edit Room

Editing Guest Rooms in Batches:

Select the check boxes of multiple guest rooms and edit them in batches. Duplication of guest room names is not allowed.

Only the rooms of the same type and belonging to the same building and same floor can be edited in batches. See the following figure.

	Edit	×
Building No*	BZ	
Floor No*	20CENG	•
Room Type*	BZ	
Start Room Number*	1	
Room Count*	8	
Remark		
	-	
Room name generation ru Number	les: Building No. + Fl	oor No. + Room

Figure 17-20 Editing Guest Rooms in Batches

17.4.3.3 Deleting Building and Floor

Select one or more guest rooms and delete them.

Only the guest rooms that have not been checked in or booked can be deleted.

17.4.3.4 Exporting Guest Room Information

Export the data of the guest rooms that have not been checked in or booked.

17.4.4 Booking Methods

You can define methods for booking hotel rooms. During system installation, the basic booking methods are initialized by default and cannot be edited or deleted.

Device Management >	Hotel	/ Hotel Management / Booking	Method			
Room Management >	0	Refresh ∓ New 📋 Delet	e			
		Booking method	Create Time	Last Updated Time	Ope	rations
Card Management >	2	ani	2022-08-02 08:48:06	2022-08-02 08:48:06	0	ŵ
Hotel Management 🗸 🗸		Online Booking	2022-07-27 08:09:34	2022-07-27 06:09:34	0	ŵ
Hotel Settings		Booking by Phone	2022-07-27 08:09:34	2022-07-27 08:09:34	2	۵.
Room Type		Booking by receptionist	2022-07-27 08:09:34	2022-07-27 08:09:34	0	面
Room						
Hotel Facility						
Booking Method						

Figure 17-22 Booking Methods

Click **Hotel Management > Booking Method > New.** The page shown in the following figure 17-23 appears.

3	New	×
Booking Method Name*	[

Figure 17-23 Add Booking Methods

Note: Duplication of booking method names is not allowed. Unused booking methods can be deleted.

17.4.4.1 Delete

In the **Hotel** interface, click **Hotel Management** > **Booking Method**, Select the booking method, click **Delete** under **Operations** or the **delete** button on the top of the list to delete the reservation. Click **OK** to confirm the delete operation.

Device Management	>	Hotel / Hotel Management / Booking Me ○ Refresh ∓ New @ Delete				
Room Management	>	Booking method	Create Time	Last Updated Time	Operations	
Card Management	>	ani ani	2022-08-02 08:48:06	2022-08-02 08:48:06	<u>/</u> 🖻	
Hotel Management	~	Online Booking	2022-07-27 06:09:34	2022-07-27 06:09:34	<u>e</u> 1	
Hotel Settings		Booking by Phone	2022-07-27 06:09:34	2022-07-27 06:09:34	_ ₫	
Room Type		Booking by receptionist	2022-07-27 06:09:34	2022-07-27 06:09:34	<u>/</u> 1	
Room			Present	_		
Hotel Facility			Prompt			
		Are you	sure you want to perform the d operation?	elete		

Figure17-24 Delete Booking Methode

17.4.5 Hotel Facility

In Hotel interface, Click **Hotel Management > Hotel Facility**. The page shown in the following figure 17-20 appears. It will show the Facilities of the hotel including the floor number, room name and room type.

TZKBio CVSecurity	y ::: #	
Device Management >	Hotel / Hotel Management / Hotel Facility	
Room Management	Hotel Facility	SelectedRoom:Public Room
Card Management >	Facility Name Q Q	Building Name
Hotel Management 🗸	C Refresh	🔿 Refresh 🗴 Delete
Hotel Settings	Facility Name Remarks Operations	Room Name
Room Type	Public Room 1	
Room	Public Room 2	
Hotel Facility	Public Room 3	
Booking Method	Public Room 4	
	Public Room 5 L Edit X	
	Public Room 6 2 Facility Name* Public Room 1	
	< Public Room 7 Remarks	
	Public Room 8	
	Public Room 9 🖉 OK Cancel	

Figure 17-21 Editing Guest Rooms in Batches

17.5 Report Management

17.5.1 Guest Check-In Report

To view the guest check-in details report, enter the search conditions and view the records.

Room SR21 F 13 Room SR21 F 5 Room BZ20CENC Room BZ20CENC	Checkin Type Daily Rate Room Daily Rate Room Daily Rate Room	Check-Out Time 2017-05-11 10:13:03 2017-05-13 12:00:00	Check-In Time 2017-05-11 10:12:18	Card Number 509171977	Document No.	Document Type	Guest Name	
Room SR21F 5 Room BZ20CENC Room BZ20CENC	Daily Rate Room		2017-05-11 10:12:18	500474077				
Room BZ20CENG Room BZ20CENG		2017-05-13 12:00:00		2091/19//	2131231	Passport	2828	
Room BZ20CENC	Daily Rate Room		2017-05-12 09:54:46	1080423694	geini1	Passport	12	
		2017-05-12 09:50:43	2017-05-12 09:49:17	1080423694	geini1	Passport	13)
Poom SP21E4	Daily Rate Room	2017-05-12 09:53:33	2017-05-12 09:50:47	1080423694	geini1	Passport	14)
R00III 3R21F4	Daily Rate Room	2017-05-16 14:22:23	2017-05-16 14:22:04	1080423694	12341231	Others	15	
Room SR21F 6	Daily Rate Room	2017-05-13 12:00:00	2017-05-12 09:59:26	665212603	geini1	Passport	16	1
Room SR21F 4	Daily Rate Room	2017-05-16 14:20:51	2017-05-16 14:16:33	1080423694	12341231	Others	12323	1
Room SR21 F 15	Daily Rate Room	2017-05-18 12:00:00	2017-05-16 14:24:51	1080423694	tuandui	Passport	1	0
Room SR21 F 6	Daily Rate Room	2017-05-17 12:00:00	2017-05-16 14:22:23	1080423694	12341231	Others	12323	
Room	Daily Rate Room	2017-05-18 12:00:00	2017-05-16 14:24:51	1080423694	tuandui	Passport	1	

Figure 17-25 Guest Check-in

You can export the records into an Excel, PDF, or CSV file. See the following figure.

					TECO eckin Report				
First Name	Last Name	Document Type	Document No.	Card Number	Check-In Time	Check-Out Time	Checkin Type	Room Name	Room Type
Maryan	Liu	ID	44443333	4117649102	2017-12-15 14:42: 09	2017-12-15 15:18: 49	Daily Rate Room	A1101	A
Carian	Xie	Passport	332454	4117858142	2017-12-15 14:51: 15	2017-12-15 15:14: 20	Daily Rate Room	B1103	A
Lucy	Feng	Passport	232145523	301973533	2017-12-15 14:43: 39	2017-12-15 15:13: 52	Daily Rate Room	A1102	A
Lucy	Feng	Passport	232145523	301973533	2017-12-15 15:13: 52	2017-12-15 15:19: 06	Daily Rate Room	B1105	А
Hook	4	ID	5577556	4117882494	2017-12-15 14:45: 37	2017-12-15 14:50: 09	Daily Rate Room	B1102	А
Maryan	Liu	ID	44443333	4117649102	2017-12-15 14:42: 09	2017-12-15 15:18: 49	Daily Rate Room	A1101	А
Bruno	Ke	Driver License	22322123	4117882494	2017-12-15 14:51: 15	2017-12-15 15:14: 20	Daily Rate Room	B1103	A

Figure 17-26 Export Guest Check-in

17.5.2 Room Occupancy Report

To check the room occupancy information (including the room name, type, check-in type, check-in time, and check-out time), enter the search conditions and view the records. You can export the records into an Excel, PDF, or CSV file. See the following figure.

SR21 F 4 SR Daily Rate Room 2017-05-16 14:22:04 2017-05-16 14:22:23 SR21 F 5 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 SR21 F 13 SR Daily Rate Room 2017-05-11 10:12:18 2017-05-11 10:13:03 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00	SR21 F 4 SR Daily Rate Room 2017-05-16 14:22:04 2017-05-16 14:22:23 SR21 F 5 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 SR21 F 13 SR Daily Rate Room 2017-05-11 10:12:18 2017-05-11 10:13:03 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00						
SR21F5 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 SR21F13 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21F4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00	SR21F5 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 SR21F13 SR Daily Rate Room 2017-05-12 09:54:46 2017-05-13 12:00:00 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21F4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00		Room Name	Room Type	Checkin Type	Check-In Time	Check-Out Time
SR21 F 13 SR Daily Rate Room 2017-05-11 10:12:18 2017-05-11 10:13:03 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	SR21 F 13 SR Daily Rate Room 2017-05-11 10:12:18 2017-05-11 10:13:03 BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00		SR21 F 4	SR	Daily Rate Room	2017-05-16 14:22:04	2017-05-16 14:22:23
BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-12 09:50:43 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	BZ20CENG19 BZ Daily Rate Room 2017-05-12 09:50:47 2017-05-12 09:53:33 SR21 F 4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:59:26 2017-05-12 09:50:43 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	1	SR21 F 5	SR	Daily Rate Room	2017-05-12 09:54:46	2017-05-13 12:00:00
SR21F4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:49:17 2017-05-12 09:50:43 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	SR21F4 SR Daily Rate Room 2017-05-16 14:16:33 2017-05-16 14:20:51 BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:49:17 2017-05-12 09:50:43 SR21F6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21F6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00)	SR21 F 13	SR	Daily Rate Room	2017-05-11 10:12:18	2017-05-11 10:13:03
BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:49:17 2017-05-12 09:50:43 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	BZ20CENG18 BZ Daily Rate Room 2017-05-12 09:49:17 2017-05-12 09:50:43 SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	1	BZ20CENG19	BZ	Daily Rate Room	2017-05-12 09:50:47	2017-05-12 09:53:33
SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	SR21 F 6 SR Daily Rate Room 2017-05-12 09:59:26 2017-05-13 12:00:00 SR21 F 6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	1	SR21F4	SR	Daily Rate Room	2017-05-16 14:16:33	2017-05-16 14:20:51
SR21F6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00	SR21F6 SR Daily Rate Room 2017-05-16 14:22:23 2017-05-17 12:00:00		BZ20CENG18	BZ	Daily Rate Room	2017-05-12 09:49:17	2017-05-12 09:50:43
			SR21F6	SR	Daily Rate Room	2017-05-12 09:59:26	2017-05-13 12:00:00
SR21 F 15 SR Daily Rate Room 2017-05-16 14:24:51 2017-05-18 12:00:00	SR21 F 15 SR Daily Rate Room 2017-05-16 14:24:51 2017-05-18 12:00:00	1	SR21F6	SR	Daily Rate Room	2017-05-16 14:22:23	2017-05-17 12:00:00
			SR21 F 15	SR	Daily Rate Room	2017-05-16 14:24:51	2017-05-18 12:00:00

Figure 17-27 Room Occupancy Report

You can export the records into an Excel, PDF, or CSV file. See the following figure 17-26.

		ZKTECO		
		Room Checkin Repor	t	
Room Name	Room Type	Checkin Type	Check-In Time	Check-Out Time
A1102	A	Daily Rate Room	2017-12-15 14:43: 39	2017-12-15 15:13 52
A1101	А	Daily Rate Room	2017-12-15 14:42: 09	2017-12-15 15:18 49
B1102	А	Daily Rate Room	2017-12-15 14:45: 37	2017-12-15 14:50 09
B1103	A	Daily Rate Room	2017-12-15 14:51: 15	2017-12-15 15:14 20
B1105	А	Daily Rate Room	2017-12-15 15:13: 52	2017-12-15 15:19 06

Figure 17-28 Export Room Occupancy report

17.5.3 Room Charges Report

To check the room expenses record, enter the search conditions (including time, guest name, room name, and room type) and view the records. See the following figure 17-29.

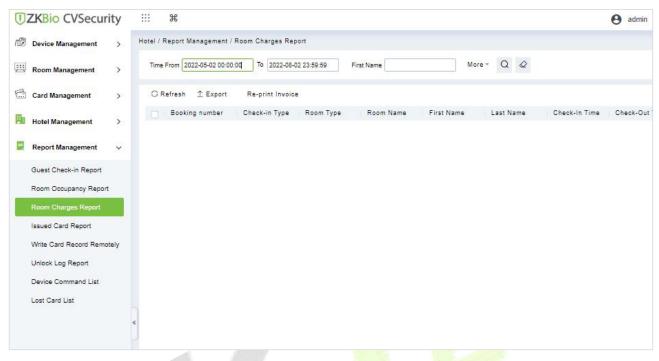


Figure 17-29 Room Ch<mark>arges</mark> Report

Re-Print Invoice:

The old receipt number is cancelled, and a new receipt is created with a new receipt number. A customer who lost their receipt has requested a duplicate receipt with their original receipt number.

17.5.4 Issue Card Report

You can also view all card writing records or search required card writing records with multiple search conditions. Enter the search conditions (including time, card type, card No., issuing date, and expiration date) and check the associated card writing records.

TZKBio CVSecurity	::: ¥	e adı
Device Management >	Hotel / Report Management / Issued Card Report	
Room Management >	Issued Date 2022-05-02 00:00 To 2022-08-02 23:59:59 More + Q	
Card Management >	○ Refresh 🛧 Export 🛱 Clear Card Loss Report 🛱 Report Card Loss	
Hotel Management >	Card Status Card Type Room Name Card No. Physical Card Num Name Last Name	ID Type
📮 Report Management 🗸 🗸		
Guest Check-in Report		
Room Occupancy Report		
Room Charges Report		
Issued Card Report		
Write Card Record Remotely		
Unlock Log Report		

Figure 17-30 Issue Card Report

You can export the records into an Excel, PDF, or CSV file. See the following figure.

					Issue Card Report					
First Name	Last Name	Card Type	Card Number	Document Type	Document No.	Issued Date	Expiration Date	Card Status	Issue Time	Operation Use
Sherry	Yang	Room Name Card	21			2017-12-15 15:26: 51	2017-12-15 15:31: 13	Invalid card	2017-12-15 15:26: 51	admin
Sherry	Yang	Room Area Card	20			2017-12-15 15:25: 57	2017-12-15 15:31: 08	Invalid card	2017-12-15 15:25: 57	admin
Lucy	Feng	Guest Card	19	Passport	232145523	2017-12-15 15:13: 54	2017-12-15 15:19: 03	Invalid card	2017-12-15 15:13: 54	admin
Maryan	Liu	Guest Card	18	ID	44443333	2017-12-15 15:13: 26	2017-12-15 15:18: 44	Invalid card	2017-12-15 15:13: 26	admin
Sherry	Yang	Authorization Card	17			2017-12-15 15:08: 48	2017-12-15 15:25: 38	Invalid card	2017-12-15 15:08: 48	admin
Sherry	Yang	Room Name Card	16			2017-12-15 15:08: 24	2017-12-15 15:31: 18	Invalid card	2017-12-15 15:08: 24	admin
Sherry	Yang	Room Name Card	15			2017-12-15 15:07: 14	2017-12-15 15:31: 43	Invalid card	2017-12-15 15:07: 14	admin
Sherry	Yang	Room Name Card	14			2017-12-15 15:06: 21	2017-12-15 15:06: 34	Invalid card	2017-12-15 15:06: 21	admin
Sherry	Yang	Floor Card	13			2017-12-15 15:05: 35	2017-12-15 15:07: 48	Invalid card	2017-12-15 15:05: 35	admin
Sherry	Yang	Building Card	12			2017-12-15 15:04: 37	2017-12-15 15:08: 37	Invalid card	2017-12-15 15:04: 37	admin
Carian	Xie	Guest Card	11	Passport	332454	2017-12-15 14:55: 55	2017-12-15 15:02: 50	Invalid card	2017-12-15 14:55: 55	admin
Bruno	Ke	Guest Card	10	Driver License	22322123	2017-12-15 14:54: 17	2017-12-15 15:14: 14	Invalid card	2017-12-15 14:54: 17	admin
Hook		Guest Card	9	ID	5577556	2017-12-15 14:47: 30	2017-12-15 14:50: 02	Invalid card	2017-12-15 14:47: 30	admin
Lucy	Feng	Guest Card	8	Passport	232145523	2017-12-15 14:44: 44	2017-12-15 15:13: 54	Invalid card	2017-12-15 14:44: 44	admin
Maryan	Liu	Guest Card	7	ID	44443333	2017-12-15 14:42: 57	2017-12-15 15:13: 26	Invalid card	2017-12-15 14:42: 57	admin
Sherry	Yang	Room Name Card	6			2017-12-15 14:41: 00	2017-12-15 14:41: 50	Invalid card	2017-12-15 14:41: 00	admin
Sherry	Yang	Room Name Card	5			2017-12-15 14:40: 32	2017-12-15 15:04: 13	Invalid card	2017-12-15 14:40: 32	admin
Sherry	Yang	Room Name Card	4			2017-12-15 14:39: 48	2017-12-15 14:40: 16	Invalid card	2017-12-15 14:39: 48	admin

Greated from ZKBIoSecurity software. All rights reserved.

Figure 17-31 Export Issue Card Report

Clear Card Loss Report:

Clear all the details of the loss card reports.

Report Card Loss:

A report loss card is a card that is invalidated and obsolete (usually due to loss or damage of the card) during its validity period.

17.5.5 Write Card Record Remotly

You can read a record card to check the lock opening record. Place the record card on a write card remotely. You can export the records into an Excel, PDF, or CSV file. See the following figure.

JZKBio CVSecurity	··· 36
Device Management >	Hotel / Report Management / Write Card Record Remotely
Room Management >	Issued Date 2022-06-02 00:00:00 To 2022-08-02 25:50:50 Card No. More + Q Q
Card Management >	⊖ Refresh
Hotel Management >	Issued Date Expiration Date Building Floor Room First Name Last Name ID Type ID Number Co Mobile Nu Logical Card Number Physical
Report Management V	
Guest Check-in Report	
Room Occupancy Report	
Room Charges Report	
Issued Card Report	
Write Card Record Remotely	
Unlock Log Report	
Device Command List	
Lost Card List	

Figure 17-32 Write Card Remotely Export

Rewrite Card:

In **Hotel** interface, click **Report Management** > **Write Card Record Remotely**. You can rewrite the same card with the correct information if you wrote any incorrect information on it.

17.5.6 Unlock Log Report

You can read a record card to check the lock opening record. Place the record card on a card writer and click Read Lock Opening Record to obtain all lock opening records of the record card. You can enter search conditions (including the building/floor/room name, start time, and end time) and view the associated records. You can export the records into an Excel, PDF, or CSV file.

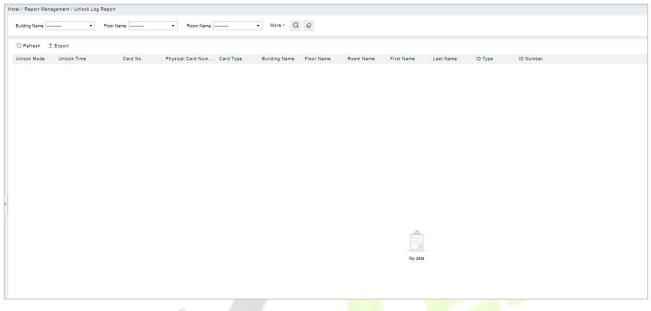


Figure 17-33 Unlock Log report

17.5.7 Device Command List

You can also view all device logs records in the device command list.

ZKBio CVSecurity	
Device Management >	Hotel / Report Management / Device Command List
E Room Management	Look Mac Address Time From 2022-05-02 00:00 00 To 2022-05-02 23:59:59 More + Q
Gard Management >	○ Refresh 🗃 Clear All Commands
Hotel Management >	seq Lock Mac Address Command Descripti Command Body Command Status Submission Time
📮 Report Management 🗸	
Guest Check-in Report	
Room Occupancy Report	
Room Charges Report	
Issued Card Report	
Write Card Record Remotely	
Unlock Log Report	
Device Command List	
Lost Caro Est	
	۹

Figure 17-34 Device Commands List

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

17.5.8 Lost Card List

You can also view all lost card details in the lost card list.

ZKBio CVSecurity	::: ¥									
Device Management >	Hotel / Report Manage	ment / Lost Card List								
Room Management	Card No.	seq	Q &							
Card Management >	O Refresh									
Hotel Management >	C seq	seq	Card Status	Card Type	Name	Last Name	Room Name	Physical Card Num Issued Time	Card Issued Date	Card Expiration Date
Report Management 🗸										
Guest Check-in Report										
Room Occupancy Report										
Room Charges Report										
Issued Card Report										
Write Card Record Remotely										
Unlock Log Report										
Device Command List										
Lost Card List										

Figure 17-35 Lost Card List



18 Intrusion

Intrusion systems are mainly applied to places where people cannot control in real time such as dangerous areas that require boundary control. For example, if an intruder is found in a restricted area, corresponding alarms will be generated, essentially to ensure the area's safety.

Keywords	Description
Partition	A partition consists of multiple zones.
Zone	To manage and control sensors. The sensors are assigned to zones and when a sensor is triggered, the system informs user which zone a sensor has been triggered.
Bypass	Points that are Service Bypassed cannot produce Extra Point events
Unbypass	Points that are Service Bypassed can produce Extra Point events.

Table 18-1 Key Words Description

18.1 Intrusion Device

Device mainly includes the Device docking, Device host docking, Synchronize Data and Time, as well as some invasion of some defense areas and partition configuration.

18.1.1 Device

18.1.1.1 Add devices (New)

Step 1: Go to **Intrusion** > **Intrusion Device** > **Device**.

Step 2: Click New, and the interface for adding a device will pop up.

Step 3: In the interface for adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure 18-1. Please refer to Table 18-2 for the description of parameter.

Manufacturer*	BOSCH -	
Model*	B3512-CHI -	1
Device Name*	Ē.	ĺ
P Address*		
Port*	7700	1
RPS Passcode*		5
Remarks		<u>1</u>

Figure 18- 1 Adding Device Interface

Parameter	Description
Manufacturer	The brand of the alarm host.
Model	Device model of alarm host.
Device Name	Customize the name of the de <mark>vice.</mark>
IP Address	Fill in the IP address of the devi <mark>ce.</mark>
Port	Divide the area for the device.
RPS Passcode	Password for communication (Please configure in Bosch A-link software in advanced and Risco doesn't need that).
Remarks	Text notes of the alarm host.
S - 3	Table 18- 2 Adding Device Parameters

18.1.1.2 Delete

Step 1: Go to Intrusion > Intrusion Device > Device.

Step 2: Select device, click Delete, and the interface of Security Verification will pop up.

٦	KBio CVSecurity III #		
A	Intrusion / Intrusion Device / Device		
Q	Device Name IP Address	Q &	
B	🗘 Refresh 🛛 T New 🛅 Delete 🛱 Synchronize Data and T	Time 🛛 Update Device Information	
	Device Name IP Address Port	Manufacturer Model Remarks Status Operations	
	■ <u>145</u> 10.8.14.145 1000	RISCO LightSYS32 Online 🖉 🖻	
		Security Verification × User Password*	
		Cancel	

Figure 18-2 Security Verification

Step 3: Fill the User Password, then click OK.

18.1.1.3 Synchronize Data and Time

Step 1: Go to Intrusion > Intrusion Device > Device.

Step 2: Select device, click Synchronize Date and Time and Synchronize to complete synchronization.

TKBio CVSecurity	::: ¥
🖀 Intrusion Device 🗸 🗸	Intrusion / Intrusion Device / Device
Device	Device Name IP Address Q
Partition	C Refresh 🖅 New 👜 Delete 📴 Synchronize Data and Time 😂 Update Device Information
Zone Device User	Device Name IP Address Port Manufacturer Model Remarks Status Operations
	<

Figure 18-3 Update Device Information

18.1.1.4 Update Device Information

Step 1: Go to Intrusion > Intrusion Device > Device.

Step 2: Select device, click **Update Device Information**, and the interface for **Update Device** Information will pop up. As shown in the Figure 18-4.

Step 3: Select the device information you want to get, and then click Start.

Update	Device Information		
Selected Device			
145 : 10.8.14.145			
Partition		Z	one
Device User, Maximum Code 30		0	utput
*It takes a long time to update the dev Total Progress	vice user		
Hidden Info	Star	t	Close

Figure 18-4 Update Device Information

18.1.1.5 Edit

Step 1: Go to **Intrusion** > **Intrusion Device** > **Device**.

Step 2: Click icon *A*, fill the Device Name or Remarks, then click **OK**.

Device Name* 145 IP Address* 10 8 14 145 Port* 1000 1000 1000 1000	Manufacturer*	RISCO 👻	
IP Address* 10 8 14 145 Port* 1000	Model*	LightSYS32 👻	
Port* 1000	Device Name*	145	
	IP Address*	10 . 8 . 14 . 145	
Demedia	Port*	1000	
Remarks	Remarks		

Figure 18-5 Edit

18.1.2 Partition

18.1.2.1 Edit

Step 1: Go to **Intrusion** > **Intrusion Device** > **Partition**.

Step 2: Click icon ∠, select Area Name or fill Remarks, then click **OK**.

	Edit	×
Partition Code	1	
Partition Name	Partition 1	
Device Name	145	
Area Name	Area Name 👻	
Remarks]
	-	-
	OK Cancel	
_	Cancel	

Figure 18-6 Edit

18.1.2.2 Defense Deployment

Step 1: Go to **Intrusion** > **Intrusion Device** > **Partition**.

Step 2: Click icon 🧭 , fill user Password, then click **OK**.

ZKBio CVSecurity

TZ	KBio	CVSecurity	у ::: ж					
		n / Intrusion Dev						
-								
B	Part	tion Name	0	evice Name	Q &			
	01	Refresh						
		Partition C	Partition Name	Device Name	Armed Status	Area Name	Remarks	Operations
		1	Partition 1	145	Undefense	Area Name		<u>ℓ</u> © ©
		2	Partition 2	145	Security Verification		×	200
					User Password*	Cancel		

Figure 18-7 Defense Deployment

18.1.2.3 Disarm

Step 1: Go to Intrusion > Intrusion Device > Partition

Step 2: Click icon 🧐 , fill the User Password, then click OK.

1	ZK	Bio (CVSecurity	y ::: ж				
-	In	trusio	n / Intrusion Dev	ice / Partition				
Ð		Partit	ion Name		Device Name	Q @		
Ð		OR	lefresh					
			Partition C	Partition Name	Device Name	Armed Status	Area Name Remarks	Operations
			1	Partition 1	145	Undefense	Area Name	<u>ℓ</u> © &
			2	Partition 2	145	Security Verification	×	200
	*					User Password*		
						ОК	Cancel	

Figure 18-8 Disarm

18.1.3 Zone

18.1.3.1 Edit

Step 1: Go to **Intrusion** > **Intrusion Device** > **Zone**.

Step 2: Click icon ∠ , fill Remarks, then click **OK**.

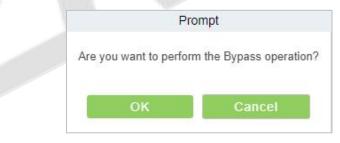
T ZK	Bio	CVSecurity	y ∷ ¥									
a li	ntrusio	n / Intrusion Dev	vice / Zone									
Ð	Zone	name	Q	Q								
Ð	O F	Refresh										
		Zone Code	Zone name	partition	_	Device Name	Bypass sta	Remarks	_	Oper	ation	s
		1	Zone 01	Patition 1			Edit		×	2	ħ	\$
		2	Zone 01	Patition 1	Zone Code * Zone name*	2	1 Zone 01			2	4	\$
»		3	Zone 01	Patition 1	Remarks	Ī		j.		0	ħ	\$
		4	Zone 01	Patition 1						<u>/</u>	ħ	8
		5	Zone 01	Patition 1			Cancel		-11	0	4	ъ
		6	Zone 01	Patition 1			Cancer		_	<u>_</u>	ħ	8
		7	<u>Zone 01</u>	Patition 1		145	•			2	ħ	\$
		8	Zone 01	Patition 1		145	•			2	ħ	\$

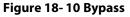
Figure 18-9 Edit Zone

18.1.3.2 Bypass

Step 1: Go to **Intrusion** > **Intrusion Device** > **Partition**.

Step 2: Click icon 1+ , then click OK.





18.1.3.3 Cancel Bypass

Step 1: Go to **Intrusion** > **Intrusion Device** > **Partition**.

Step 2: Click icon 🐧 , then click OK.

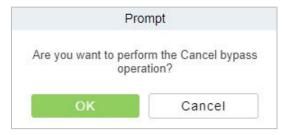


Figure 18-11 Cancel Bypass

18.1.4 Device User

18.1.4.1 New

Step 1: Go to **Intrusion > Intrusion Device > Device User**.

Step 2: Click New, and the interface for adding a device will pop up.

Step 3: In the interface for adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure 18-12. Please refer to Table 18-3 for the description of parameter.

	New		×	
User code	1			
User name				
Password*				
Device Name				
C	ж	Cancel		
Figure 1	8-12 Ad	d Device User		
Figure 1	8-12 Ad	d Device User		

Parameter	Description
User Code	You can customize the user's unique code.
User Name	You can customize the user's name.
Password	You can customize the user's password used for logging in alarm host.
Device Name	Customize the name of the device.

Table 18-3 Adding User Parameters

18.1.4.2 Update Device User

Step 1: Go to **Intrusion** > **Intrusion Device** > **Device User**.

Step 2: Click Update Device User with the mouse, and the interface of Update Device User will pop up.Step 3: In the interface of Update Device User, fill in the corresponding parameters according to the

need for updates, as shown in the Figure 18-12. Please refer to Table3 for the description of parameter filling.

	Update Device	9 User	
Device*		•	
Maximum Code*	30		
It takes a long time to upda	te the device user		
atal Bragrasa			
otal Progress			
		-	1 12
A DESCRIPTION OF A DESC		Start	Close
Hidden Info			

Figure 18-13 Update Device User

Parameter	Description	
Device	Select the alarm host that has been added.	
Maximum Code	Define the maximum code for the alarm host to upload users.	
	Table 18-4 Undate Device User	

18.1.4.3 Delete

Step 1: Go to Intrusion > Intrusion Device > Device User.

Step 2: Select device, click **Delete** or **Delete** option under **Operations**, and the interface of Security Verification will pop up. As shown in the figure 18-14.

ZKBio CVSecurity	::: ¥
🖀 Intrusion Device 🗸 🗸	Intrusion / Intrusion Device / Device User
Device	User name Device Name Q
Partition	⊖ Refresh 📴 New 🐵 Update Device User 💼 Delete
Zone Device User	User code User name Password Device Name Operations
	«

Figure 18-14 Security Verification

Step 3: Fill the User Password, then click **OK**.

18.1.4.4 Edit

Step 1: Go to Intrusion > Intrusion Device > Device User.

Step 2: Click icon ∠ , modify the user name or password, then click **OK**.

18.2 Real-Time Monitoring

Real-Time Monitoring:

Image: Security Image: Security Image: Security	😝 admin 👻
A Intrusion / Real-Time Monitoring / Real-Time Monitoring	
So Device Name	
P Partition Zone Output	,
⊘ Defense Deployment G Disarm	
Partition 1 Partition 2	ĺ
Current Total 2 Defense Deployment 1 Disarm:1 Partition Name	•
Real Time Event	•
Device Name IP Address Event Description	
Total Received: 1 Clear Data Rows Event Description	

Figure 18-15 Real-time Monitoring

Partition:

We can view the device status by placing the mouse cursor on the device. The green indicates the partition is Armed, and the Blue indicates the partition is not armed. We can also select the partition and operate it quickly, such as **Arm Partition**, **Disarm Partition**.

Partition Zone Output	
O Defense Deployment O Disarm Disarm Partition Partition	
Partition 1 Partitio Status Device: 145 Number: 2 Armed Status: In defense Alarm Status: •	
Current Total:2 Defense Deployment Disarm	1 Oisarm:1 Partition Name

Figure 18-16 Real-time Monitoring - Partition

Zone:

We can view the **Zone** status. The green indicates the Zone is on Cancel Bypass, the yellow indicates the Zone is on Bypass. We can also click on the Zone and operate it quickly, such as **Bypass**. **Bypass**.

Partition	Zone	Output					
+ Bypas	s to Cancel by	pass					
6							
Stat	us		7 05			7	
Zone (Dev		Zone 04	Zone 05	Zone 06	Zone 07	Zone 08	
Nun Byp	ass status: 🥑						
Can	cel bypass						

Figure 18- 17 Real-time Monitoring - Zone

Output:

We can view the status of Alarm Host's Outputs. We can also click on the point and operate it quickly, such as Activate Output and Deactivate Output.

	Partition		Zone	Output
	🛱 Enanle	Output	🗟 Disat	ole Output
(\oslash	0	0	Status
	Output 2	Output	3 Outp	Device: 145 Number: 1 Activity Status:
				Enanle Output
с	urrent Total	:4	e E	nanle Output:0 – Disable Output:4 Output

18.3 Intrusion Record

Event Record:

Step 1: Go to Intrusion > Intrusion Record > Even Record.

Step 2: On the Event Record interface, click **Export**, enter the admin password in the displayed security verification dialog box, and click **OK**. Select whether to encrypt the file and the file format to export, and click **OK**.

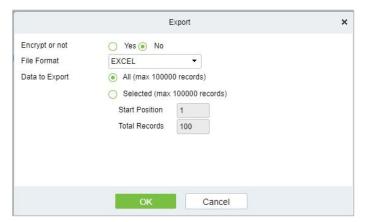


Figure 18- 19 Record Export Page

Clear All Data:

Click **Clear All Data** to pop up prompt and click **OK** to clear all transactions.

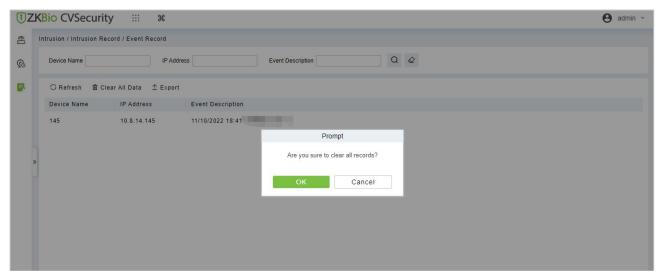


Figure 18- 20 Clear All Data

19 Locker

19.1 Locker Device Management

19.1.1 Device

19.1.1.1 Add Devices (New)

Step 1: Go to Locker> Locker Device Management > Device.

Step 2: Click +**New**, the interface for adding a device will pop up.

Step 3: In the interface for adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure 19-1. Please refer to Table 19-1 for the description of parameter.

	New	×	
Device Name* IP Address* Serial Number* Communication password* Area Name*	Area Name		
Save and New	ок с	ancel	

Figure 19-1 Adding Device Interface

Parameter	Description
Device Name	Customize the name of the device.
IP Address	Fill in the IP address of the device.
Serial Number	Fill the device serial number.
Communication Password	Fill in the communication password of the device. You can add it only after the verification is successful.
Area Name	Divide the area for the device.

Table 19-1 Adding Device Parameters

19.1.1.2 Delete

Step 1: Go to Locker> Locker Device Management > Device.

Step 2: Select device, click **Delete**, then click **OK** to delete device.

JZKBio CVSecurity	::: ¥				
🖁 Locker Device Manage 🗸	Locker / Locker Device Mana	gement / Device			
Device	Device Name	Serial Number	IP Address	More - Q	Q
Parameters Visual Panel	O Refresh ∓ New	🖻 Delete 🛛 🖳 Control 👻			
Visual Faller	Device Name	Serial Number Area Name IP Addres	s Status Device Model	Firmware Version	Operation
	test	CGJ6190760005 Area Name 10.8.14.1	51 Online LockerPad-7B	2.0.1	2 🖻

Figure 19-2 Delete Device

19.1.1.3 Control

Set Administrator:

Administration has permission to set the administrator permission to device. Select the person, click >, and click **OK**.

Set /	Administrator
Personnel ID Name	Department Name
Iternative	Selected(0)
Personnel First Name Last Name Department	Personnel First Name Last Name Department
Department 1	>> < <
	No data

Figure 19-3 Set Administrator Interface

Clear Administrator:

Administration has permission to clear the administration permission from device.

Reboot Device:

It will reboot the selected device.

Synchronize Time:

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

Synchronize All Data to Devices:

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

	ynchronize All Data to Devices	×
elected Device		
LockerPad-7B : 151		
al Progress		
Hidden Info	Synchronize	Close
		-

Distribute Advertising Resources:

Administrator selects the AD resource on the computer and delivers it to lockerpad-7b. Click **Distribute** Advertising Resources, click **Browser**, then select the picture or video and click **OK**.

	ite advertising resources	>
File Upload*	Browse	
ОК	Cancel	

Figure 19-5 Distribute Advertising Resources Interface

Clear All Ads:

Clears all ads resources from the selected device.

19.1.2 Parameters

In Locker module, click Locker Device Management > Parameter to set the parameters.

ŪZ	KBio CVSecurity	¥	\rm e admin ~
	Locker / Locker Device Managem	ent / Parameters	
	Multiple people and one Enab	e	Multiple people and one cabi Temporary takeout settings Record loop delete count setting (
»	Temporary takeout setti Enab @ Y	e	
	Record loop delete cou		
		ок	

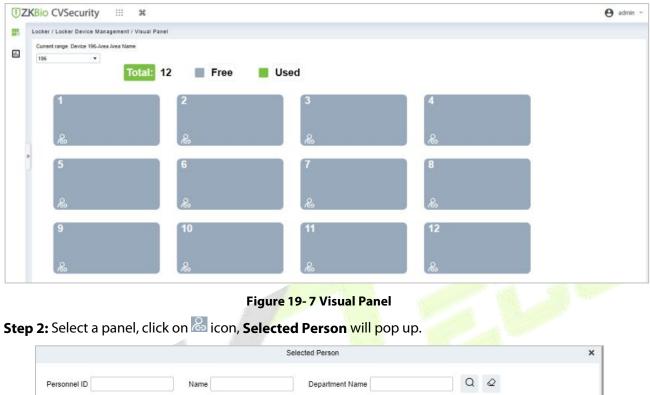
Figure 19-6 Parameter

ltem	Description						
Multiple people and one cabinet setting	Multiple users can share a cabinet when it is enabled.						
Temporary takeout settings	When enabled, users can remove objects without losing access to the cabinet						
Record loop delete count setting (Device)	When a specified number of stored records is reached, a certain number of records will be deleted from the beginning, the number of records you fill in the space.						
Table 19- 2 Parameter Description							

19.1.3 Visual Panel

In this function, admin can link users in the software to the corresponding cabinet.

Step 1: In the Locker module, click Locker Device Management > Visual Panel.



Personnel ID	Name	Department Name Q
Alternative		Selected(0)
Personnel First Name	Last Name Department	Personnel First Name Last Name Department
123	Department Name	
		> < No data
ik k 1-1 > >i	50 rows per page 👻	Cancel

Figure 19-8 Select Person Interface

Step 3: Select the user that the admin wants to bind with the cabinet. Then click > and OK.



Figure 19-9 Visual Panel Interface

Note:

- 1. When you click on **Total**, all cabinets will be displayed.
- 2. When you click on **Free**, all unoccupied cabinets will be displayed.
- 3. When you click on **Used**, all occupied cabinets will be displayed.

19.2 Locker Report

19.2.1 All Transaction

Step 1: Go to Locker > Locker Report > All transaction.

Step 2: On the All Records interface, fill in the corresponding query information and click **Search** symbol to complete the query of all records.

ker / Locker Report											e admin
	Locker / Locker Report / All Transactions										
Time From 2022-07-09 00 00:00 To 2022-10-09 23:59:59 Personnel ID Device Name More ~ Q Q											
⊖ Refresh 🛍 Clear All Data 🛧 Export											
Device Name	Grid number	Grid size	User ID	First Name	Last Name	Department	Verification	Operation	Time	Capture Photo	
151	8	Small locker	166519432275	3			Face	Take	2022-10-08 09:58:56	62	
151	8	Small locker	166519432275	3			Face	Store	2022-10-08 09:58:42	64	
	⊖ Refresh @ Cl Device Name 151	O Refresh 道 Clear All Data 1 Device Name Grid number 151 8	O Refresh IB Clear All Data ⊥ Export Device Name Grid number Grid size 151 8 Small locker	O Refresh 値 Clear All Data	C Refresh Clear All Data	C Refresh B Clear All Data ↑ Export Device Name Grid number Grid size User ID First Name Last Name 151 8 Small locker 1665194322753	C Refresh Bi Clear All Data	© Refresh ∰ Clear All Data ↑ Export Device Name Grid number Grid size User ID First Name Last Name Department Verification 151 8 Small locker 1665194322753 Face	© Refresh ∰ Clear All Data ↑ Export Device Name Grid number Grid size User ID First Name Last Name Department Verification Operation 151 8 Small locker 1665194322753 Face Take	© Refresh III Deta ⊥Export Device Name Grid number Grid size User ID First Name Last Name Department Verification Operation Time 151 8 Small locker 1665194322753 Face Take 2022-10-08 09:58:56	© Refresh @ Clear All Data ↑ Export Device Name Grid number Grid size User ID First Name Last Name Department Verification Operation Time Capture Photo 151 8 Small locker 1665194322753 Face Take 2022-10-08 09:58:56 😭

Figure 19-9 Report Query Page

19.2.1.1 Export

On the **All Records** interface, click **Export**, enter the admin password in the displayed security verification dialog box, and click **OK**. Select whether to encrypt the file and the file format to export, and Click **OK**.

	1	Export	×
Encrypt or not	🔿 Yes 💿 No		
File Format	EXCEL	•	
Data to Export	All (max 10000)	0 records)	
	Selected (max	100000 records)	
	Start Position	1	
	Total Records	100	
	OK	Cancel	

Figure 19-10 Report Export Page

4	A	В	C	D	E	F	G		
1				All Transactions					
2	Device Name	Grid number	Grid size	User ID	First Name	Last Name	Department		
3	196	1	Small locker	1					
4	196	1	Small locker	1					
5	196	1	Small locker	1665310457633					
6	196	1	Small locker	1665310457633					
7	151	8	Small locker	1665194322753					
8	151	8	Small locker	1665194322753					

Figure 19-11 Event Export

19.2.1.2 Clear All Data

Click Clear All Data, then click OK to clear all transactions on the Prompt interface.

ŢΖ	Image: Text State Image: Text State Image: Text State Image: Text State											
⊞	Locker / Locker Report / All Transactions											
	Time From 2022-07-09 00 00 00 To 2022-10-09 23 59 59 Personnel ID Device Name More * Q Q											
	⊖ Refresh 🛱 Clear All Data 🛧 Export											
	Device Name	Grid number	Grid size U	ser ID	First Name	Last Name	Department	Verification	Operation	Time	Capture Photo	
	151	8	Small locker 16	665194322753				Face	Take	2022-10-08 09:58:56	6a	
	151	8	Small locker 16	665194322753		Pro	mpt	Face	Store	2022-10-08 09:58:42	6 2	
	>					Are you sure you wan opera OK						

Figure 19- 12 Report Clear All Data



ZKTeco Industrial Park, No.32, Industrial Road, Tangxia Town, Dongguan, China. Phone :+86 769 - 82109991 Fax :+86 755 - 89602394 www.zkteco.com

Copyright © 2022 ZKTECO CO., LTD. All Rights Reserved.

