New Features and Updates

for ZKBio CVSecurity 5.2.0_R

Previous Version: ZKBio CVSecurity 5.1.1_R

Date: October 2022

Doc Version: 1.0

English

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

ZKTeco 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 have 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 http://www.zkteco.com.

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 www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturers of RFID and Biometric (Fingerprint, Facial, and 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 **New Features and Updates for ZKBio CVSecurity 5.2.0_R**.

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	**Description**
Bold font	Used to identify software interface names e.g., **OK**, **Confirm**, **Cancel**.
>	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.
/	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.
	The general information which helps in performing the operations faster.
	The information which is significant.
	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 KEY UPDATES **6**

2 FUNCTIONAL UPDATE DETAILS **8**

    2.1 INTRUSION ALARM MODULE **8**

        2.1.1 INTRUSION DEVICE 8

        2.1.2 REAL-TIME MONITORING 14

        2.1.3 MAP CONFIG 17

    2.2 LOCKER MANAGEMENT MODULE **18**

        2.2.1 DEVICE 18

        2.2.2 PARAMETERS 21

        2.2.3 VISUAL PANEL 22

        2.2.4 LOCKER REPORT 23

    2.3 ACCESS CONTROL MODULE **25**

        2.3.1 DEVICE REPLACEMENT 25

        2.3.2 IMPORT OR EXPORT ACCESS LEVEL 27

    2.4 INTELLIGENT VIDEO MODULE-FAST TARGET SEARCH **29**

    2.5 VISITOR MODULE-RESPONDENT SELF-APPROVAL **32**

PRIVACY POLICY 37

I. COLLECTED INFORMATION 37

II. PRODUCT SECURITY AND MANAGEMENT 37

1   Key Updates

Implemented Change	Description
Intrusion Alarm	Intrusion systems apply to places requiring boundary control and real-time monitoring. For example, when an intruder enters the restricted area, it will trigger a corresponding alarm, ensuring the area's safety. Currently, ZKBio CVSecurity integrates with BOSCH and RISCO, the third-party alarm controllers, offering functions such as arming, disarming, alarm record query and displaying defence zones on the map. The corresponding models and devices are as follows: BOSCH: B Series: B6512, B5512, B4512, B3512; G Series: B9512G, B8512G. RISCO: LightSYS32; LightSY50.
Locker Management	A New Module of ZKBio CVSecurity. This locker module manages an electronic locker system in a unified platform. As a result, administrator can manage multiple lockers simultaneously. Currently, the locker module supports the LockerPad-7B device, and offers the following functions: 1. Supports facial recognition and multi-tech cards verification. 2. Supports online and offline working modes. 　　a. Online mode: With ZKBio CVSecurity's security platform, administrator can unify the locker users' allocation, advertising resources distribution, data recording and other functions of multiple devices. 　　b. Offline working mode: To manage device parameters, data records, locker users' allocation and advertisement displaying through the LockerPad-7B. 3. Supports locker users' management and set different usage rules according to the type of users: 　　a. Fixed users: e.g., permanent staff in factories and offices. 　　b. Temporary users: e.g., supermarket customers, generally random allocation 　　c. Fixed users + Temporary users: e.g., in some tourist areas, available for staff and tourists to use the locker at the same time. 4. Supports cabinet allocation for one user, one cabinet for multi-users, one user for multi-cabinets. 5. Supports digital advertisement placement with image and video (3GP, MP4, MKV, WEBM, PNG, JPG, JPEG, GIF) to increase commercial value and drive foot traffic. 6. Provides storage-pick-up records review. 7. Offers basic functions such as parameter setting, multi-language (Simplified Chinese & English) switching.
Device Replacement	In the actual use of service, there are often cases of equipment failure; re-adding equipment means that you need to reset the device parameters.

	ZKBio CVSecurity's latest function of replacing equipment, to achieve a one-click device replacement application. When the same type of equipment fails to operate, you only need to enter the serial number of the new device to restore previous settings.
Fast Target Search	When a suspicious person is found during real-time video viewing or playback, you can zoom in and take screenshots, and quickly track the suspicious person by using the quick "Target Search" button to achieve a person track search.
Respondent Self-approval	Optimize the visitor process, after the visitor invitation email is sent, 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.
Import or Export Access Level	Support import or export "access level". Batch import of "person information" and "access level" via Excel to quickly complete the access control configuration in the project.

2 Functional Update Details

2.1 Intrusion Alarm Module

Intrusion systems apply to places requiring boundary control and real-time monitoring. For example, when an intruder enters the restricted area, it will trigger a corresponding alarm, ensuring 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.
Un bypass	Points that are Service Bypassed can produce Extra Point events.

Table - Key Words Description

2.1.1 Intrusion Device

Device mainly includes the Device connection, Synchronize Data and Time, Device panel connection, as well as some of the invasion of some defence area and partition configuration.

Intrusion Device

Add New Device:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Device**].

Step 2: Click [**New**] with the mouse, and the interface of adding a device will pop up.

Step 3: In the interface of adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure below.


Figure - Adding Device Interface

Update Device Information:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Device**].

Step 2: Select device, click [**Update Device Information**], and the interface of Update Device Information will pop up. As shown in the Figure below.

Step 3: Select the device information you want to obtain, and then click [**Start**].
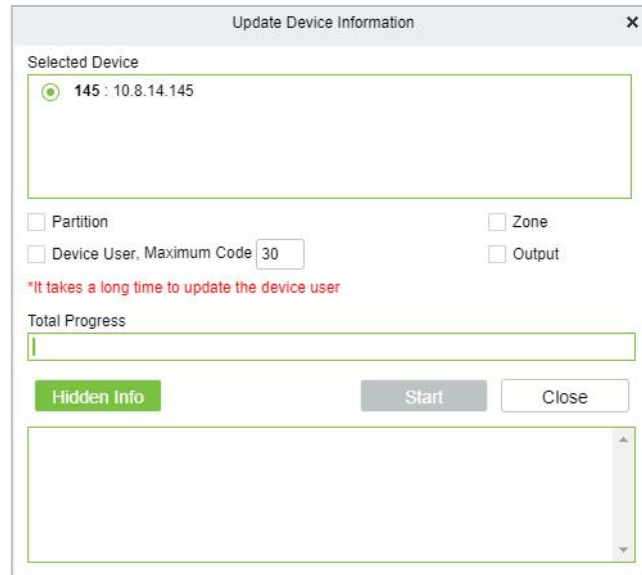
Figure - Update Device Information

2.1.1.1 Partition

Edit Partition:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Partition**].

Step 2: Click icon ✎ , select Area Name or fill Remarks, then click [**OK**].
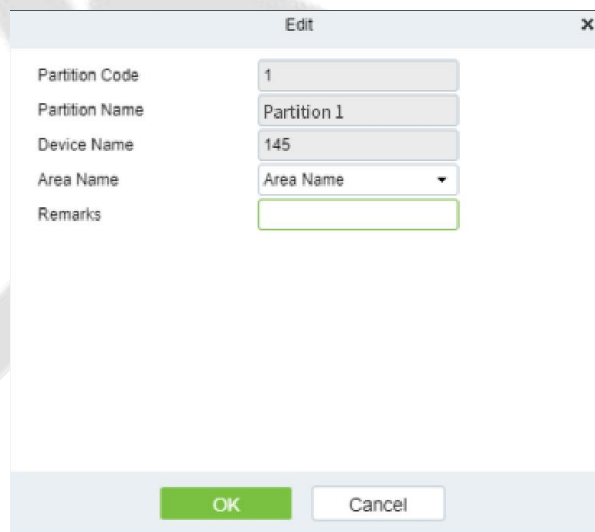
Figure - Edit Partition

Defence Deployment:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Partition**].

Step 2: Click icon ☑ , fill the User Password, then click [**OK**].
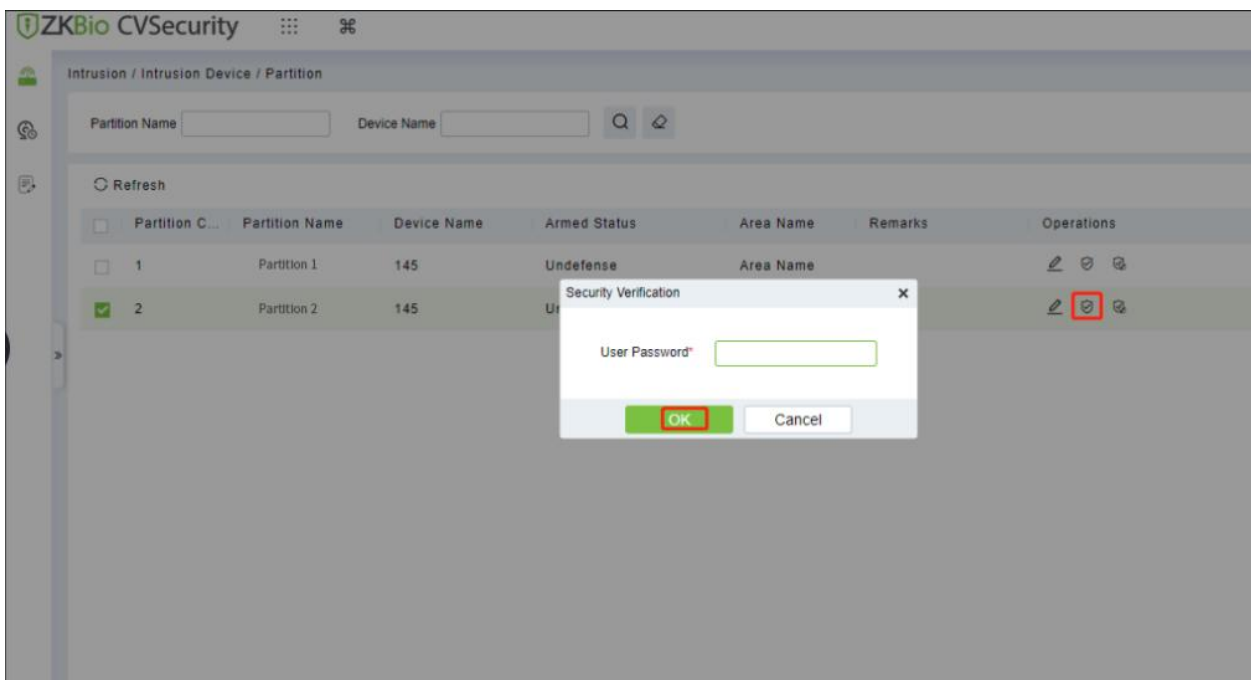
Figure - defence Deployment

Disarm:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Partition**].

Step 2: Click icon ☑ , fill the User Password, then click [**OK**].
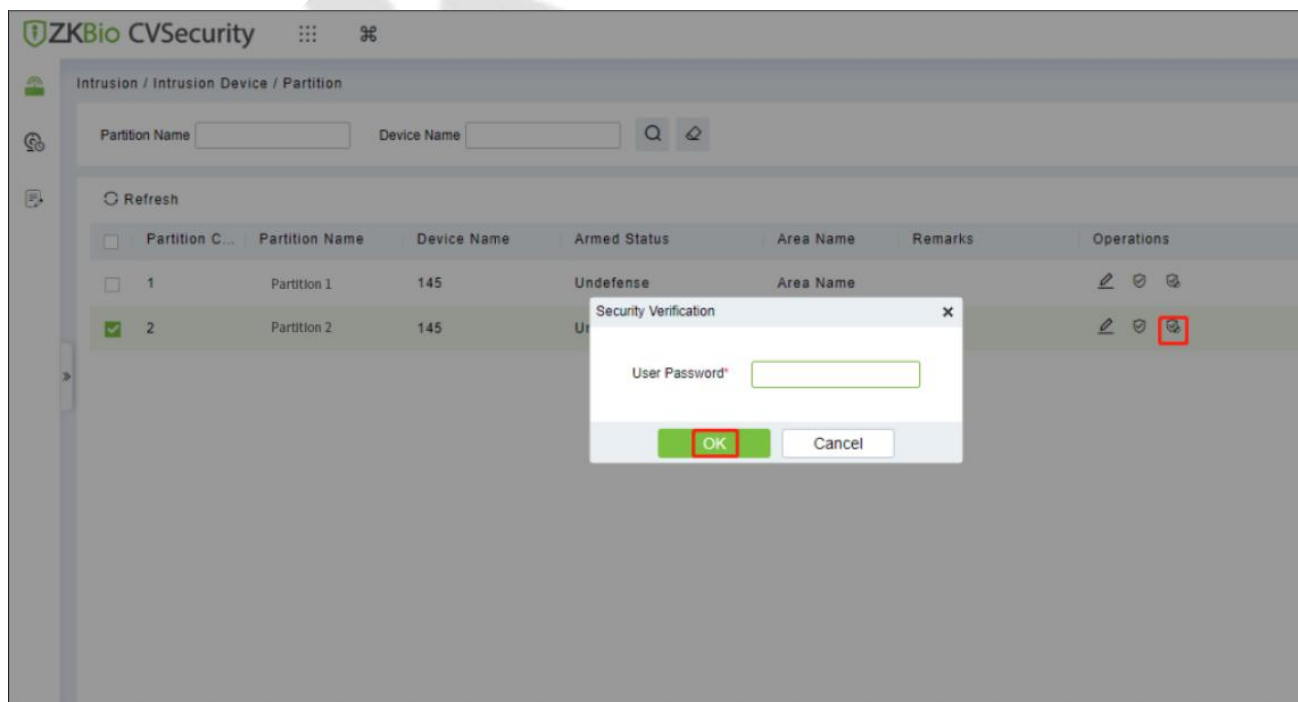
Figure - Disarm

2.1.1.2 Zone

Edit Zone:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Zone**].

Step 2: Click icon ✎ , fill Remarks, then click [**OK**].
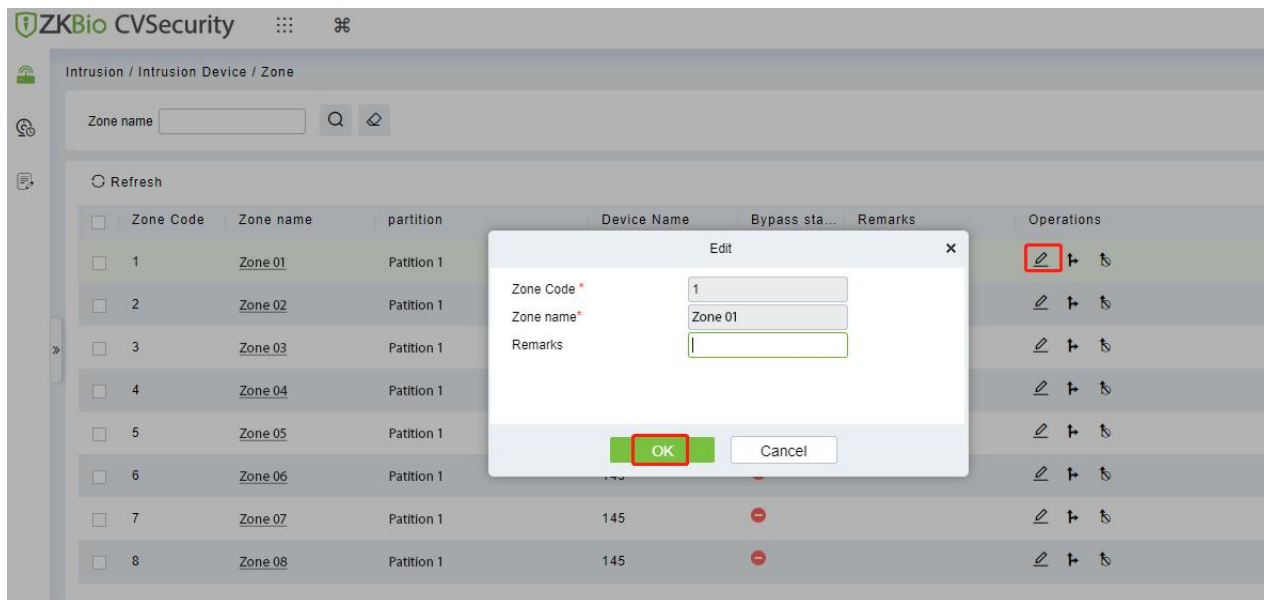
Figure - Edit Zone

Bypass:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Partition**].

Step 2: Click icon ⊬ , then click [**OK**].
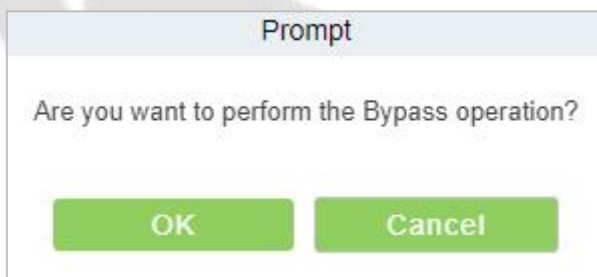
Figure – Bypass

Cancel Bypass:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Partition**].

Step 2: Click icon 🖱 , then click [**OK**].
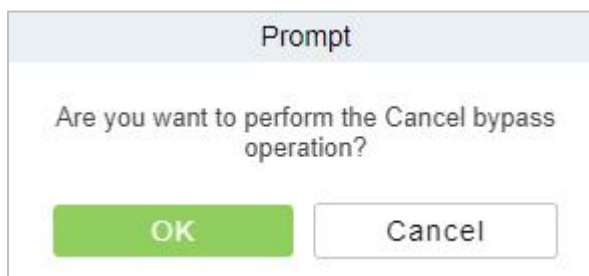
Figure - Bypass

2.1.1.3 Device User

New:

Step 1: Go to [**Intrusion**] > [**Intrusion Device**] > [**Device User**].

Step 2: Click [**New**] with the mouse, and the interface of adding a device will pop up.

Step 3: In the interface of adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure below.
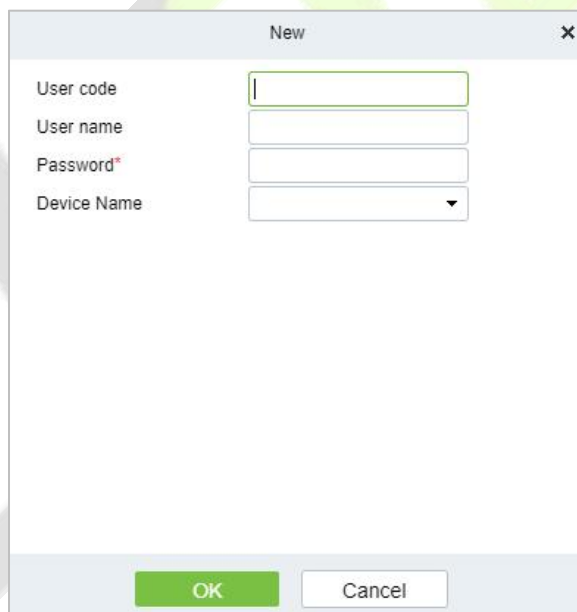
Update Device User:

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 below.
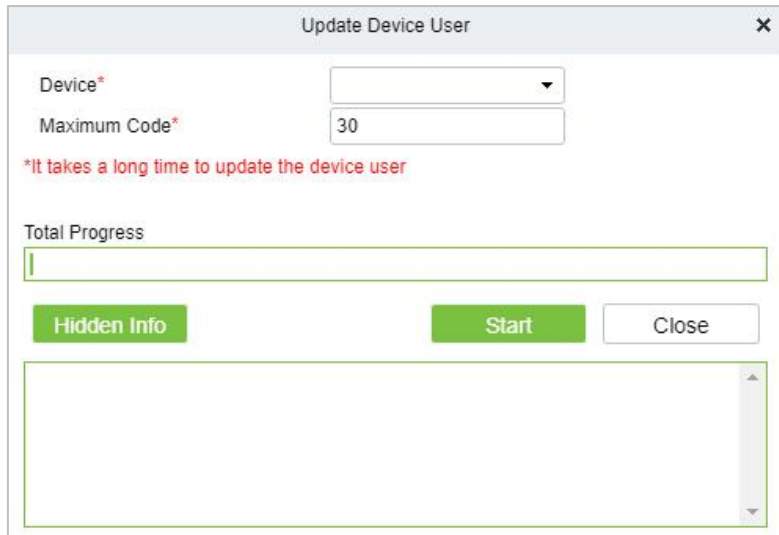
2.1.2 Real-Time Monitoring

Real-Time Monitoring:
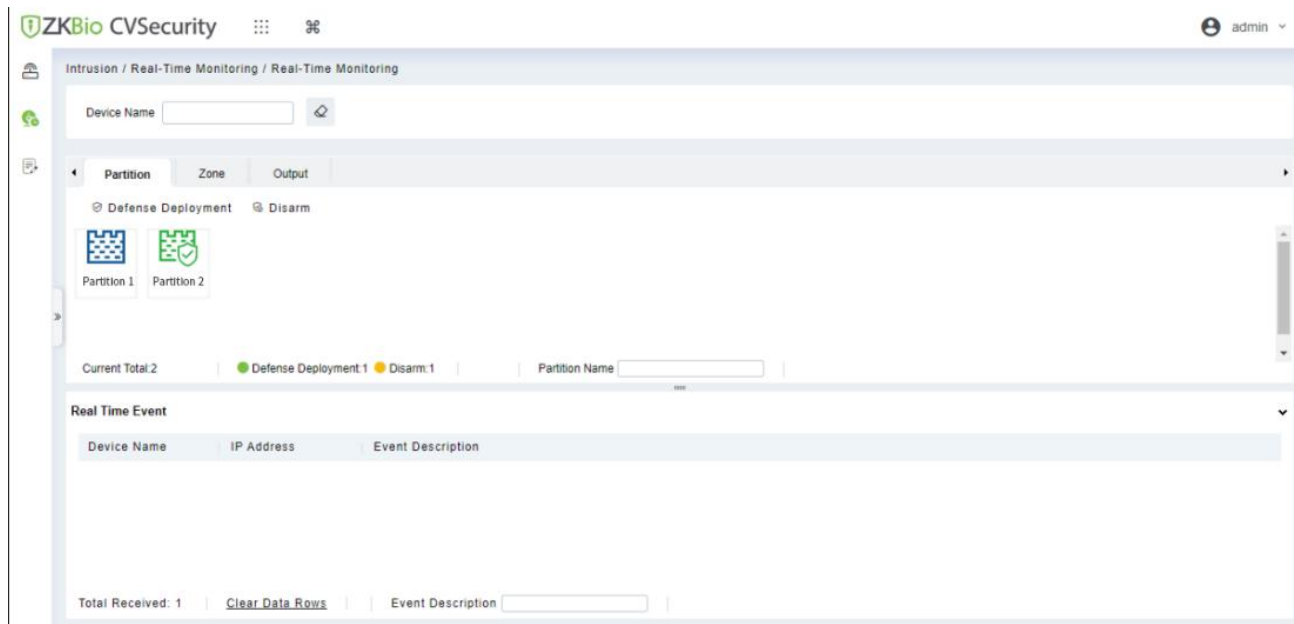
Partition:

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**.

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, Cancel Bypass**.
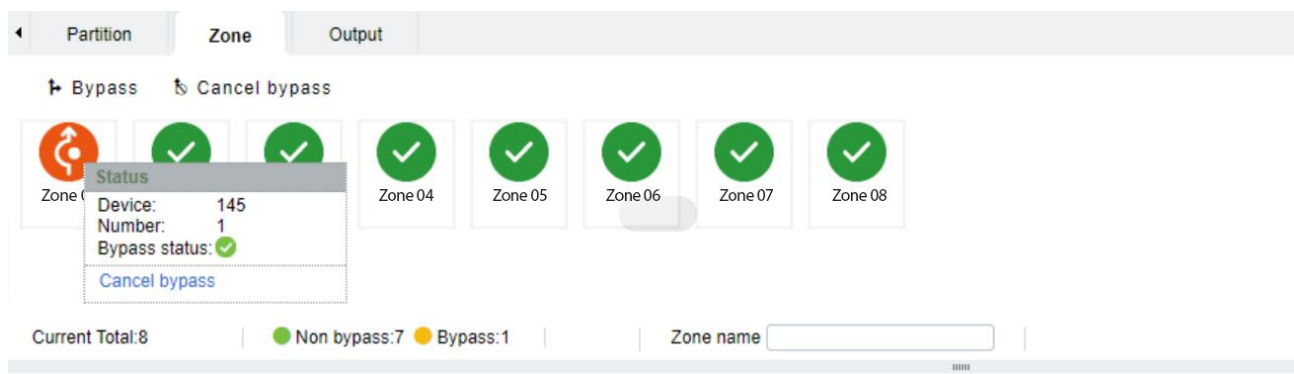
Output:

We can view the status of Alarm Panel's Output. We can also click on the point and operate it quickly, such as Activate Output and Deactivate Output.
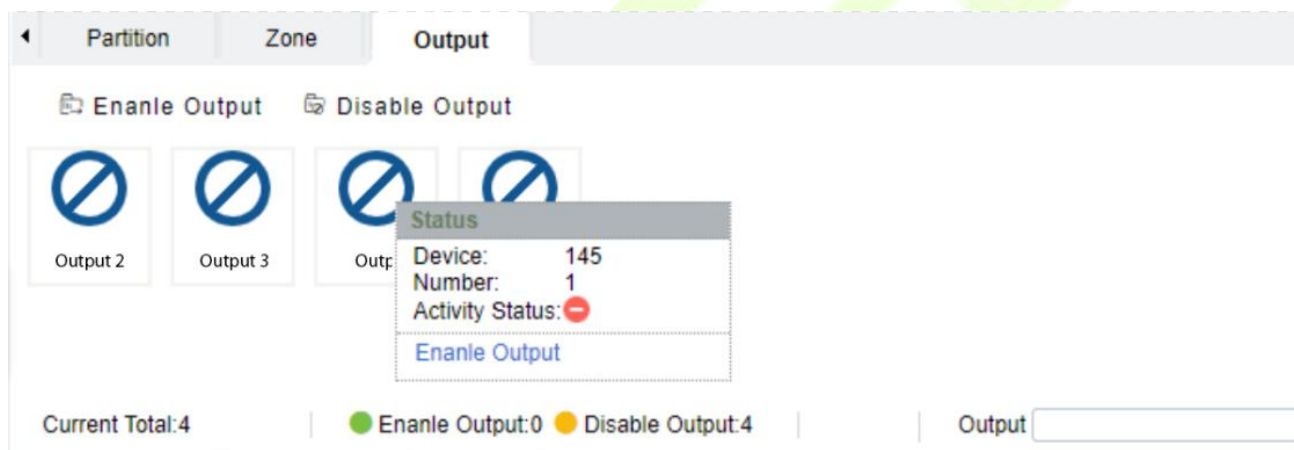
Intrusion Record

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**], as shown in Figure below.
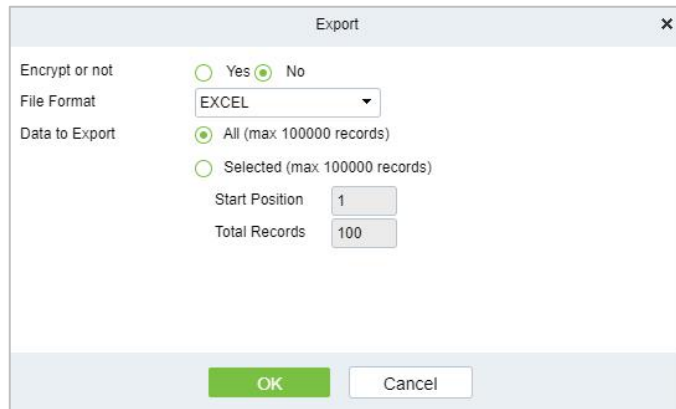
Clear All Data:

Click [**Clear All Data**] to pop up prompt and click [**OK**] to clear all transactions.
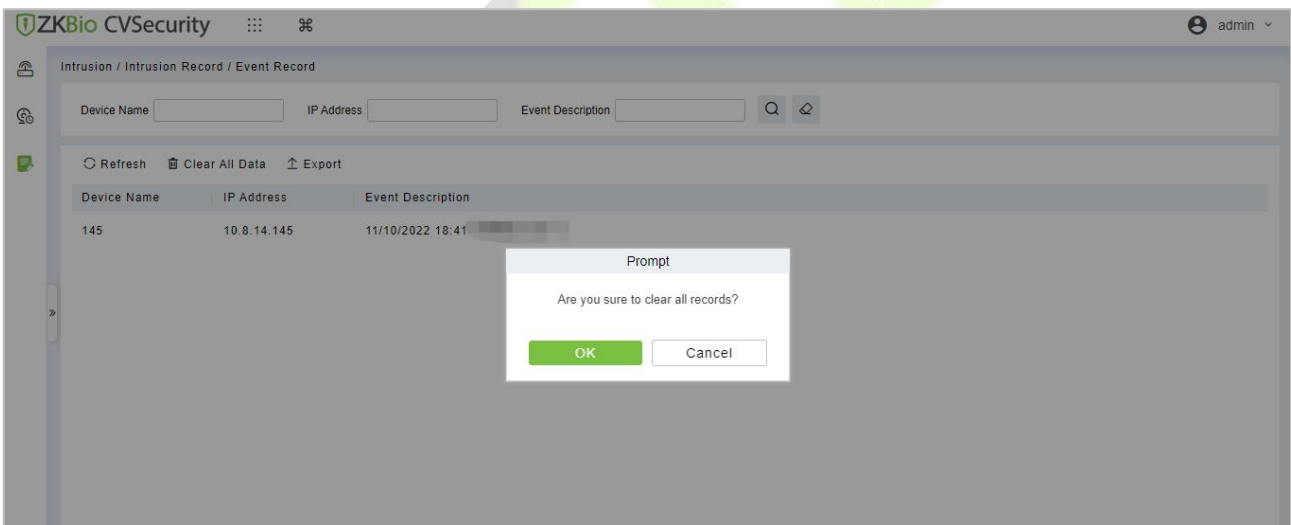
2.1.3 Map Config

We can view the Intrusion Alarm states in real time through the map center.

Add Defence Area:

Step 1: Go to [**Service Center**] > [**Map Service**] > [**Map Config**]. Click 🔓 , start adding defence area.

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 or zone.

2.2 Locker Management Module
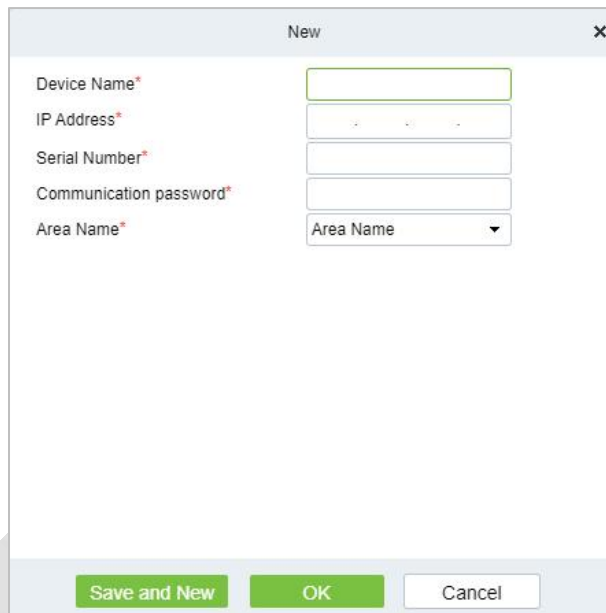
2.2.1 Device

Add Devices (New):

Step 1: Go to [**Locker**] > [**Locker Device Management**] > [**Device**].

Step 2: Click [**+New**], the interface of adding a device will pop up.

Step 3: In the interface of adding a device, fill in the corresponding parameters according to the adding requirement, as shown in the Figure below. Please refer to Table - Adding Device Parameters for the description of parameter filling.

Figure - 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 - Adding Device Parameters

Control:

Administration has permission to set the administrator permission to device. Select the person, click [**>**], then click [**OK**].
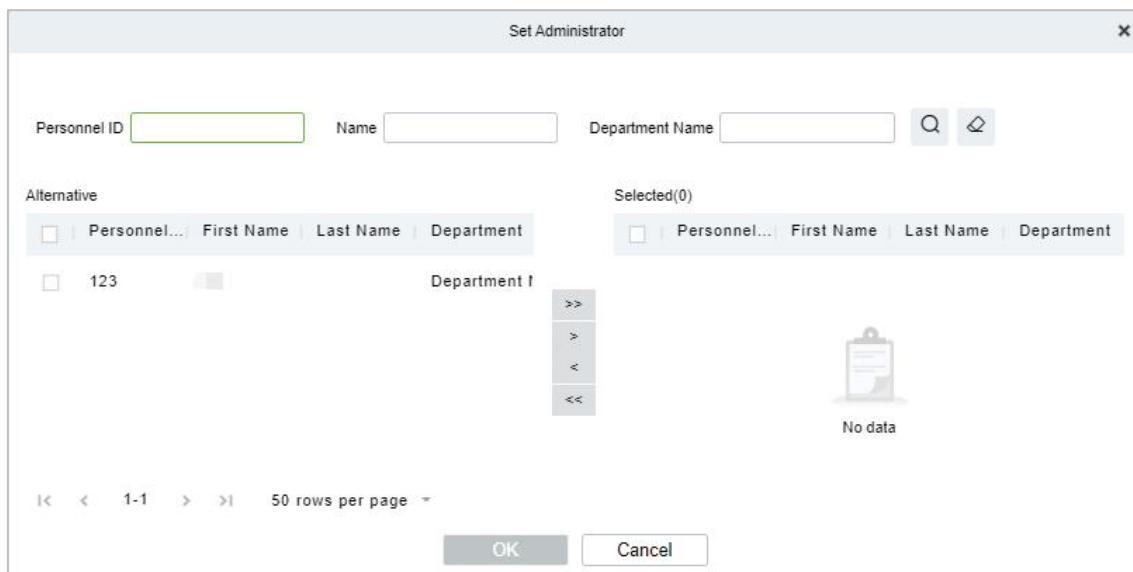
Figure - Set Administrator Interface

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.
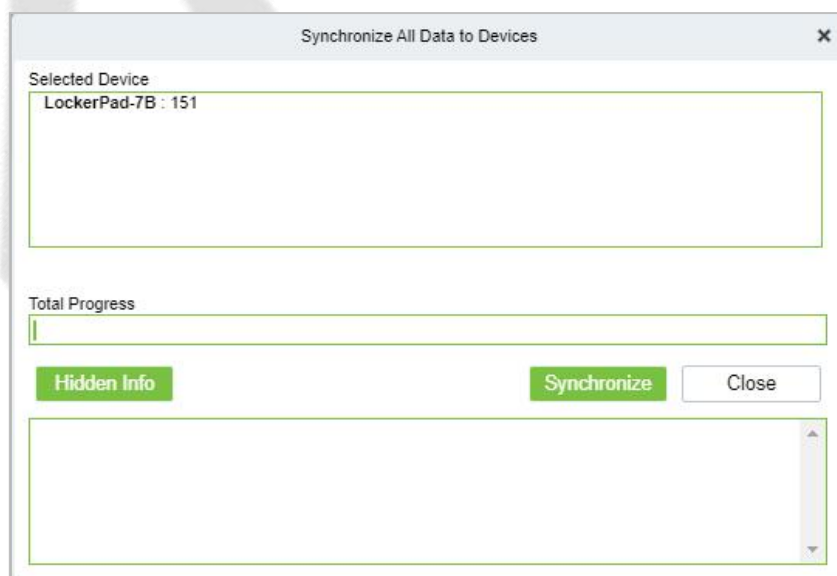
Figure - Synchronize All Data to Devices Interface

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**].
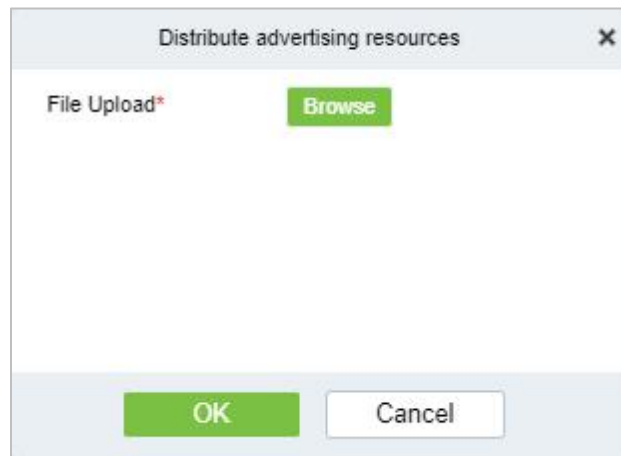
Figure - Distribute Advertising Resources Interface

Clear All Ads:

Clears all ads resources from the selected device.

2.2.2 **Parameters**

In **Locker** module, click [**Locker Device Management**] > [**Parameter**] to set the parameters.
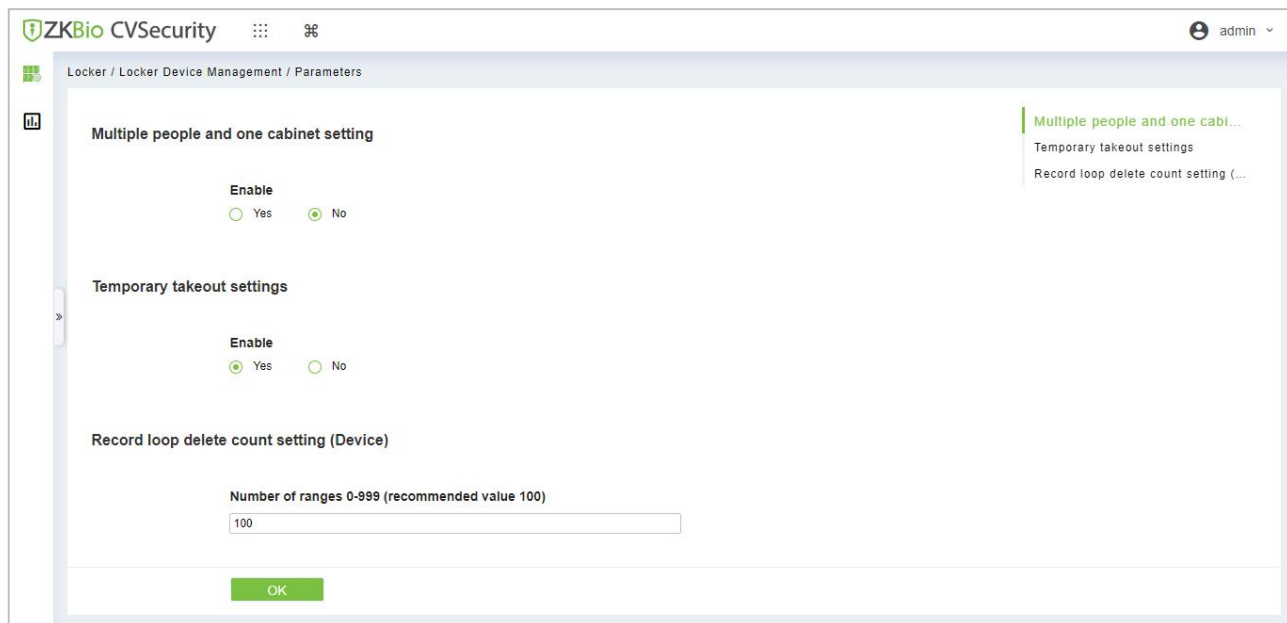
Figure - Parameters

Item	Description
Multiple people and one cabinet setting	Enabling it means that a cabinet can be shared by multiple users.
Temporary takeout settings	Enabling it means users can remove items without losing access to the cabinet.
Record loops delete count setting	When the record storage reaches the maximum threshold, the storage data will be deleted from the beginning.

Table - Parameter

2.2.3 Visual Panel

In this function, admin can bind users in the software to the corresponding cabinet.

Steps:

Step 1: In the **Locker** module, click [**Locker Device Management**] > [**Visual Panel**], as shown in Figure below.
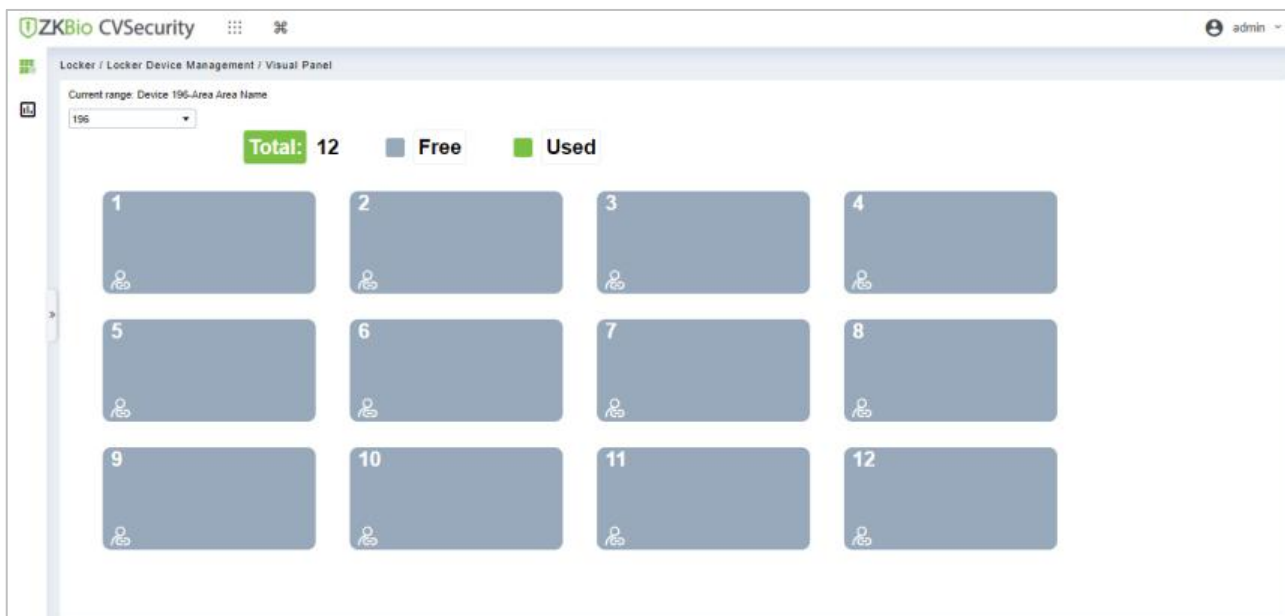
Figure - Visual Panel

Step 2: Select a panel, click , **Selected Person** will pop up. As shown in the Figure below.
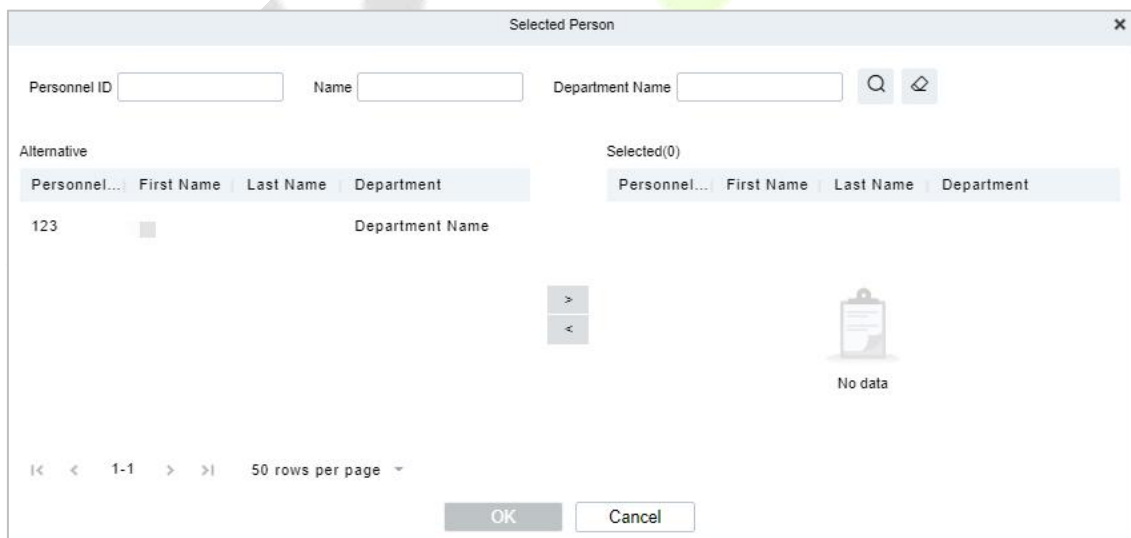
Figure - Select Person Interface

Step3: Select the user that the admin wants to bind with the cabinet. Then click [**>**] and [**OK**].
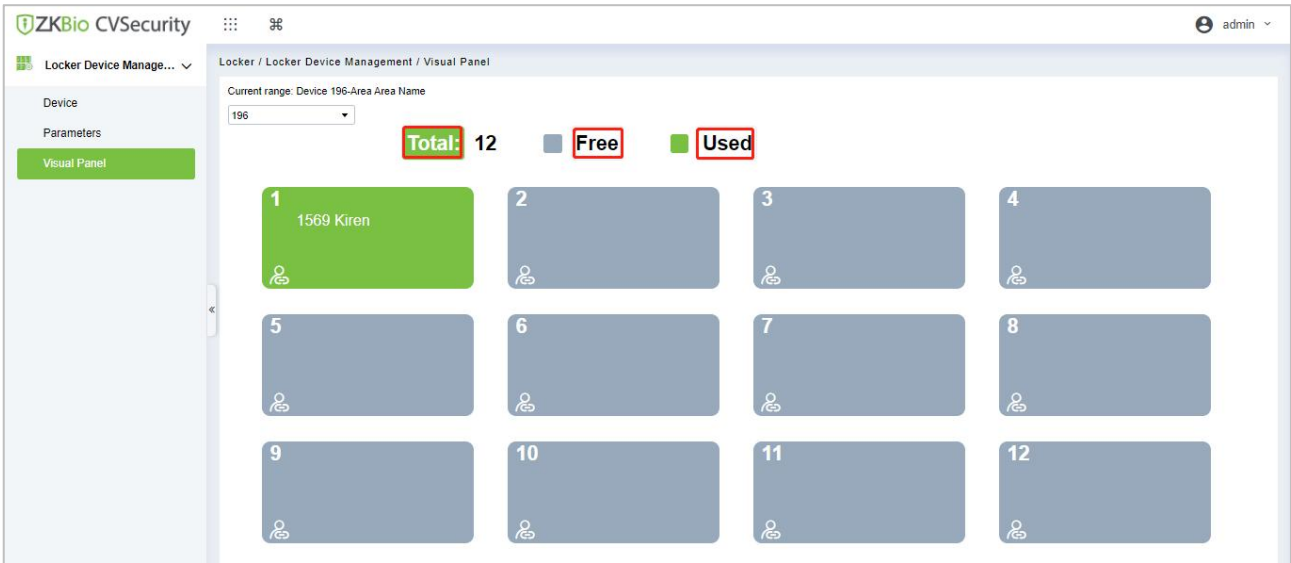
Figure - Visual Panel Interface

Note:

1. When clicking [**Total**], all cabinets will be displayed.
2. When clicking [**Free**], all unoccupied cabinets will be displayed.
3. When clicking [**Used**], all occupied cabinets will be displayed.

2.2.4 Locker Report

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 the "search" symbol to complete the query of all records, as shown in Figure below.
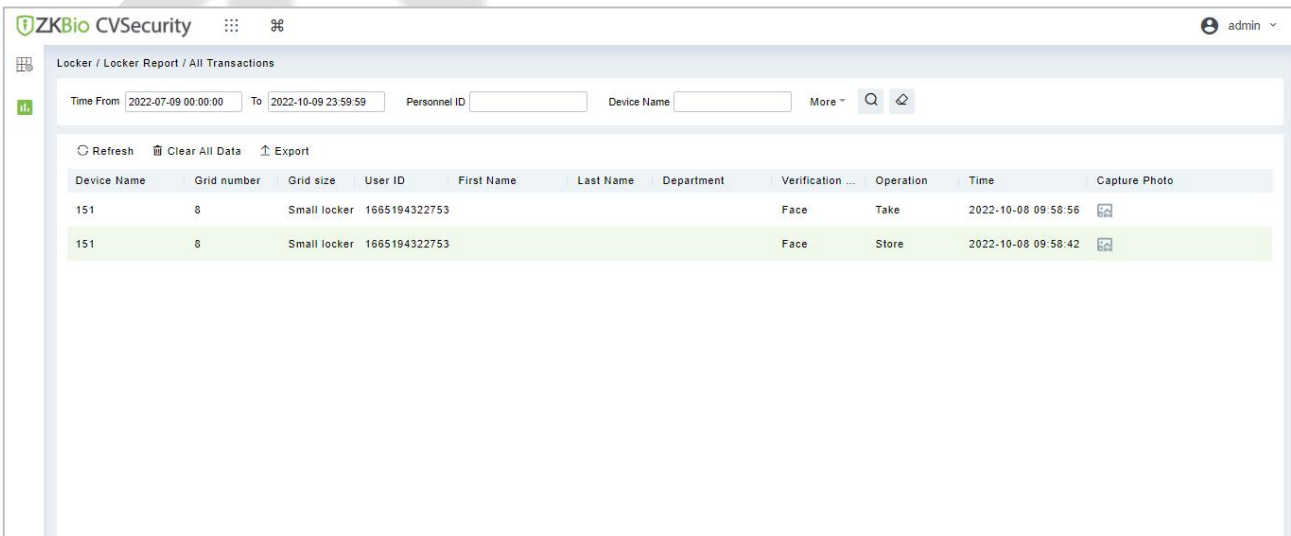
Figure - Report Query Page

Step 3: 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**], as shown in Figure.
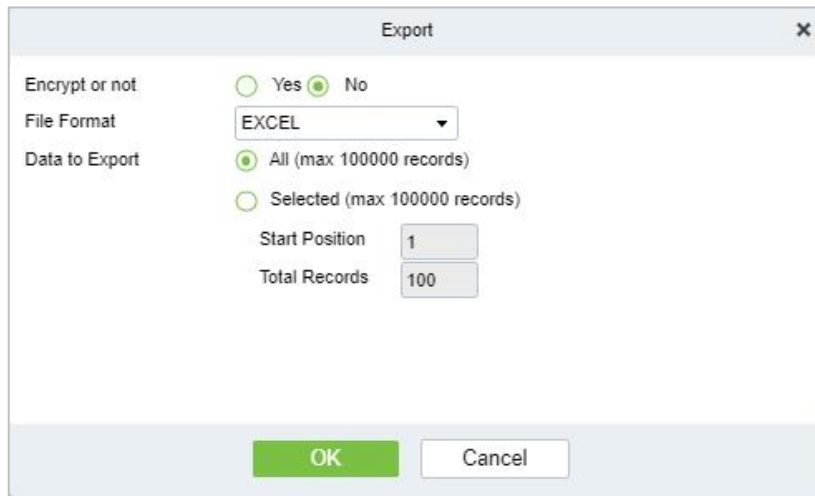
Figure - Report Export Page

Figure - Event Export

Clear All Data:

Click [**Clear All Data**], then click [**OK**] to clear all transactions on the [**Prompt**] interface.
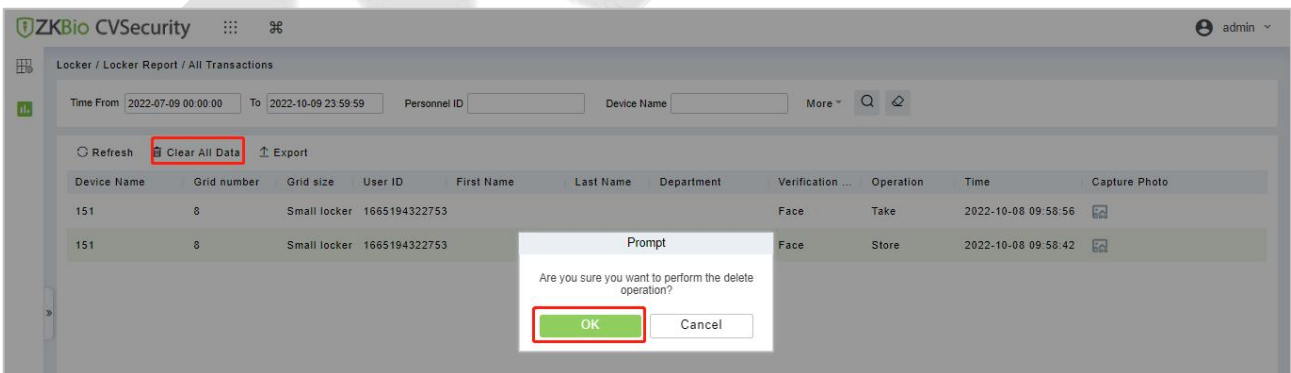
Figure - Report Clear All Data

2.3   Access Control Module
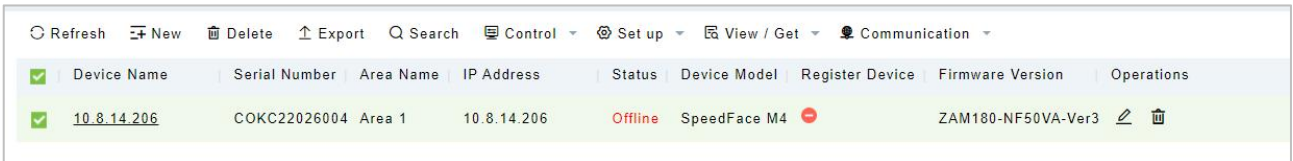
2.3.1 Device Replacement

Introduce the configuration Steps of replacing access control devices in ZKBio CVSecurity.

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

Steps:
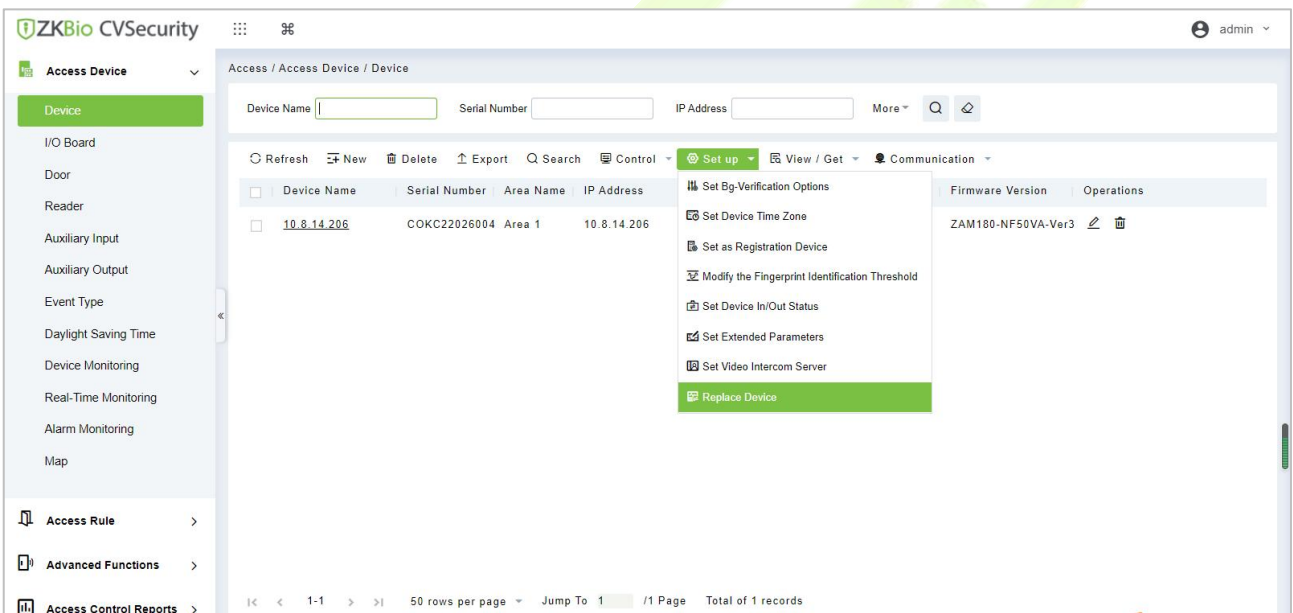
Step 1: Go to the [**Access**] > [**Access Device**], select the unavailable device.

Figure - Select the unavailable device

Step2: Click [**Set up**] > [**Replace Device**].

Figure - Replace Device

Step 3: Enter the serial number of the new device, then click [**OK**].
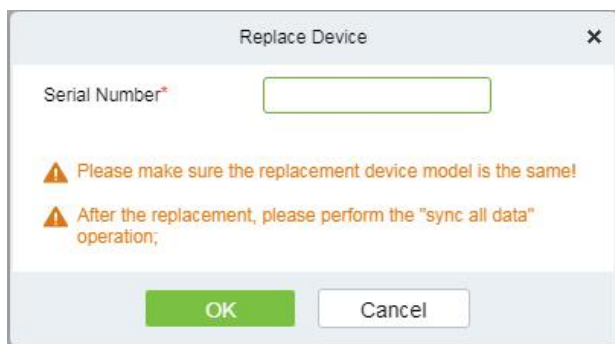
Figure - Input the Serial Number

Step 4: Select the new device, then click [**Control**] > [**Enable**].
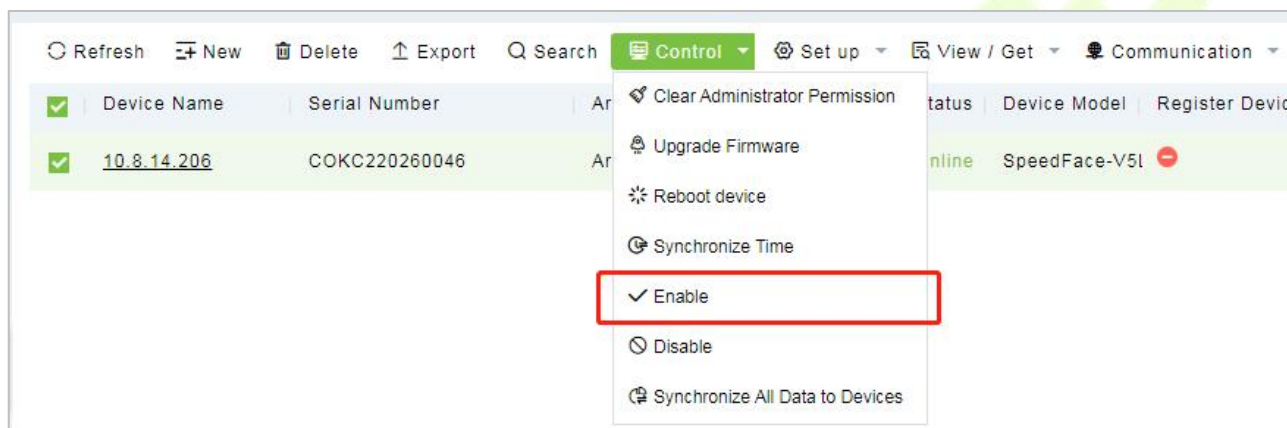
Figure - Enable Device

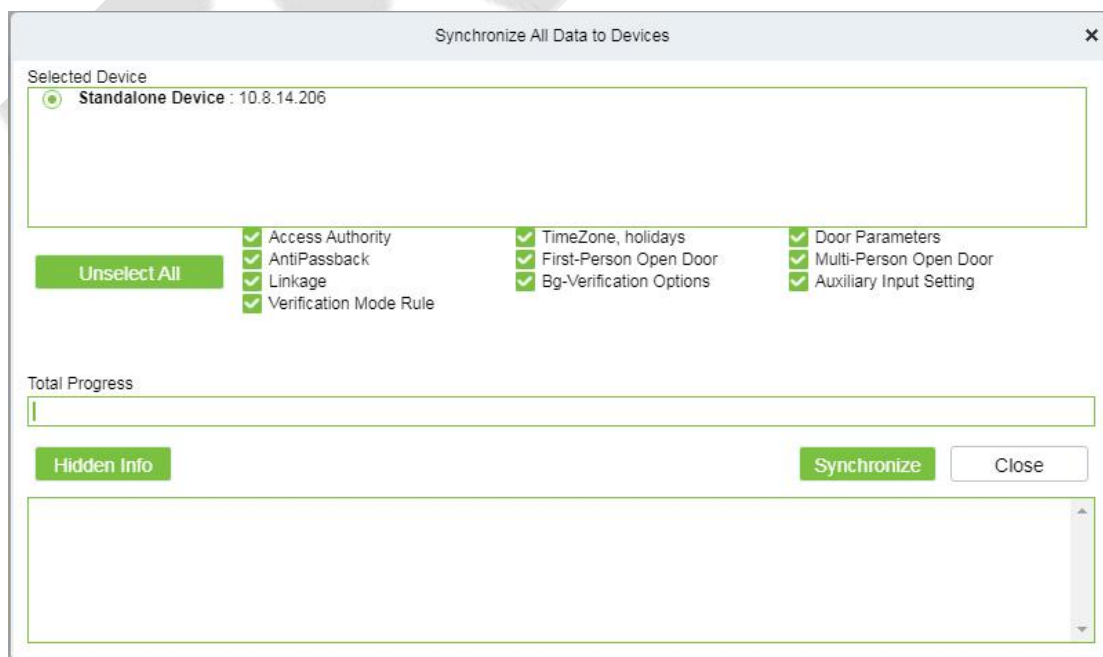**Step 5:** Select the new device, then click [**Control**] > [**Synchronize All Data to Device**].

Figure - Synchronize Device Data

Note:

1. The device needs to set the server address and IP allocation in advance before replacement.

2. Make sure the replacement device model is the same.

3. After the replacement, please perform the "sync all data" operation.

2.3.2 Import or Export Access Level

Export and fill in Access Level Template:

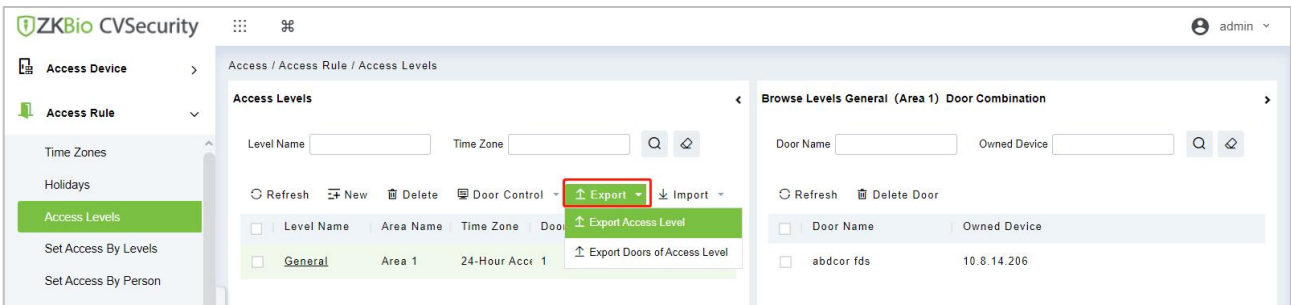In the **Access** module, click [**Access Rule**] > [**Access Levels**] > [**Export**] > [**Export Access Level**], then fill in the Access levels information.

Figure - 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 - 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**].

Import the Access Level Template:

Step 1: In the Access Module, click [**Access Rule**] > [Access Levels] > [**Import**] > [**Import Access Level**], and click [**Browser**] to upload the Access Level Template.
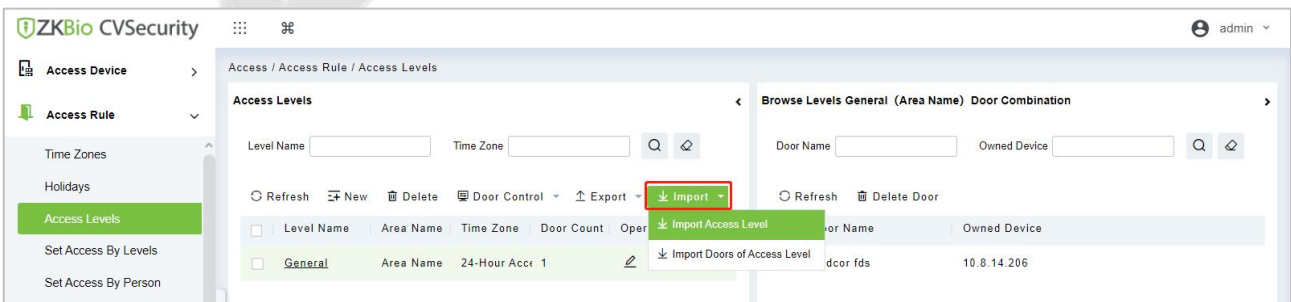

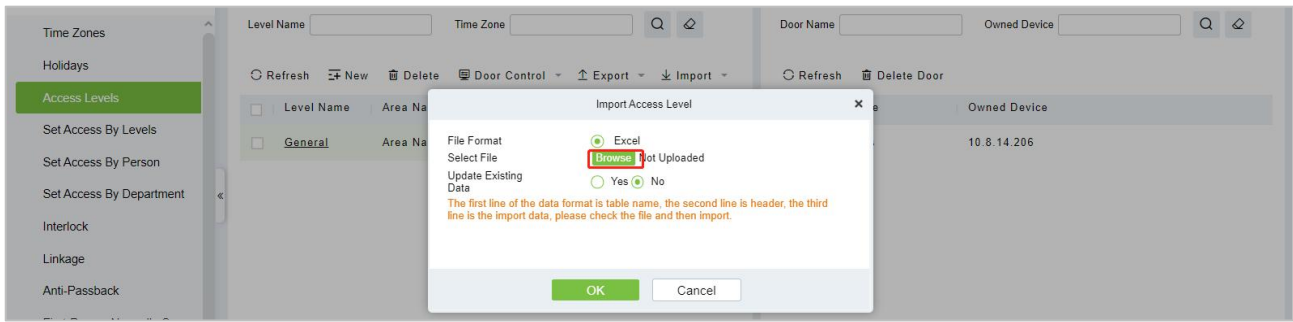**Figure - Import the Access Level Template 1**
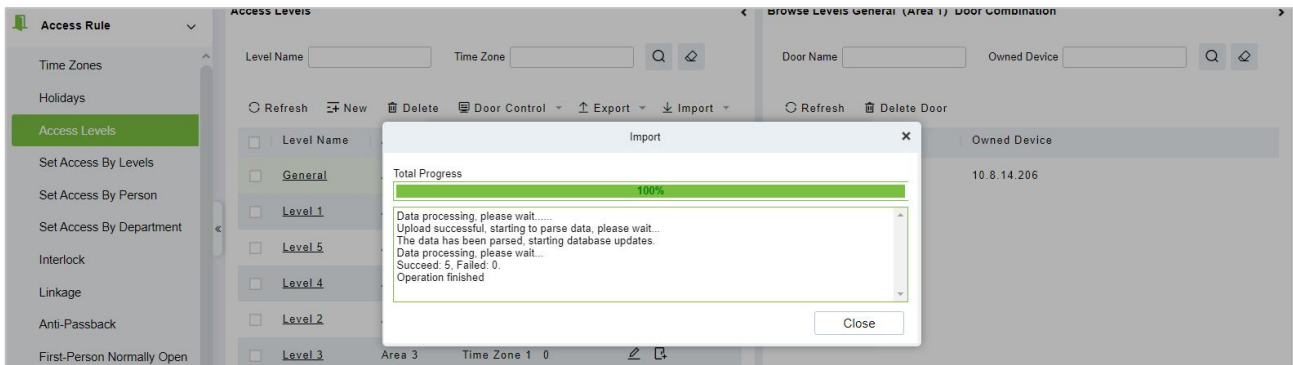
Figure - Import the Access Level Template 2

Figure - Import the Access Level Template 3

Step 2: After the upload is successful, we can view the uploaded level as shown in Figure below.
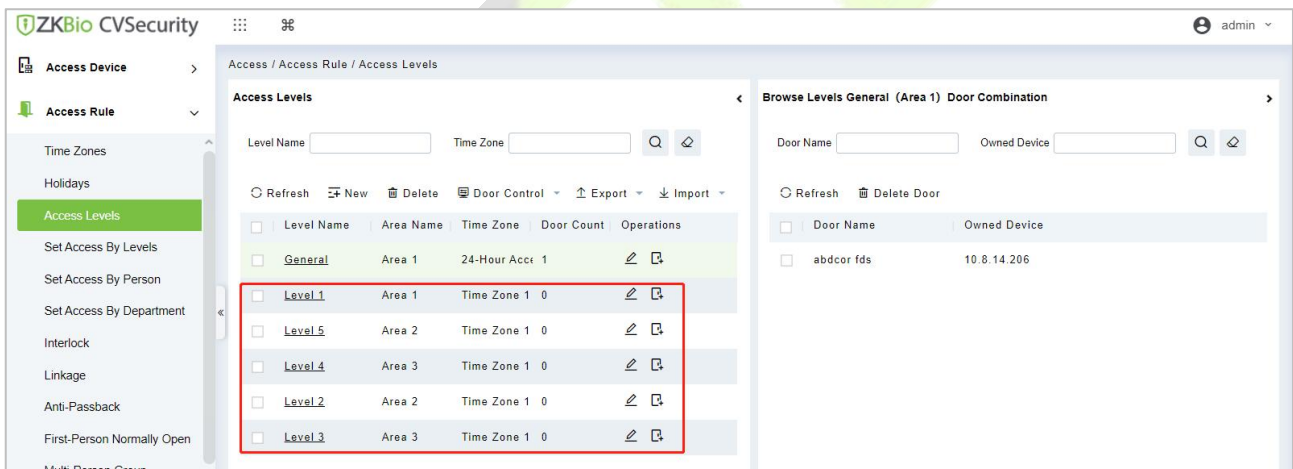

Figure - Import the Access Level Template 4

2.4 Intelligent Video Module-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.

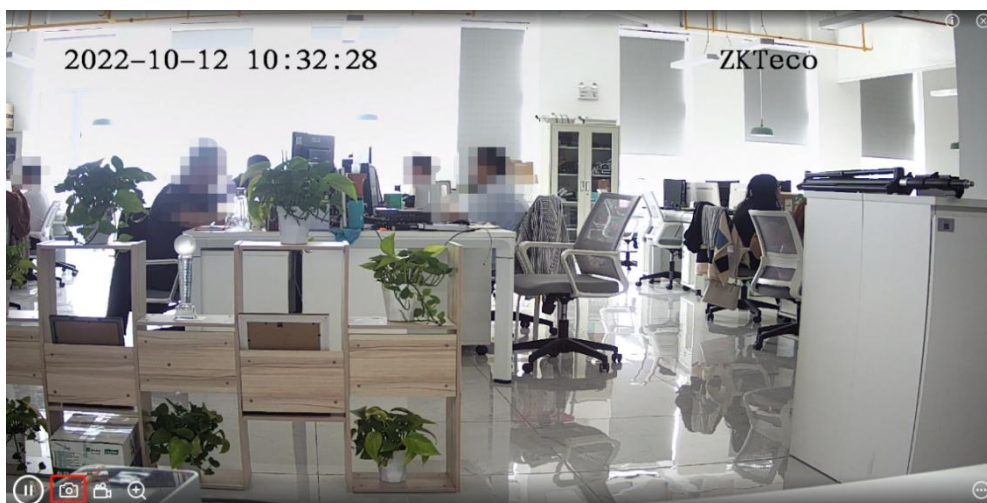**Step 1:** Go to the [**Video Management**] > [**Video Preview**], Click 📷 to snap a screenshot.

Figure - Video Preview

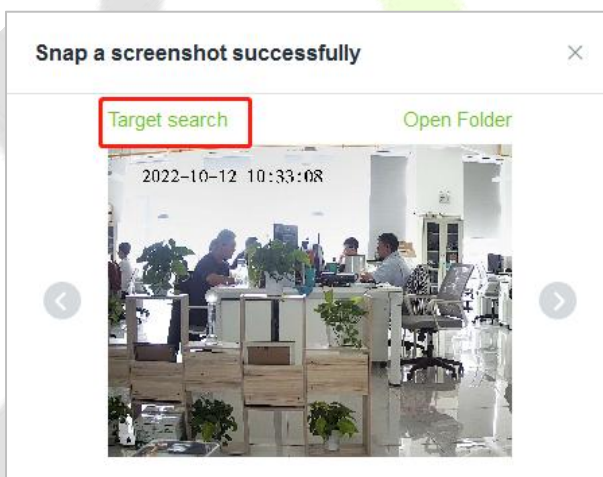**Step 2:** Then click [**Target search**].

Figure - Screenshot
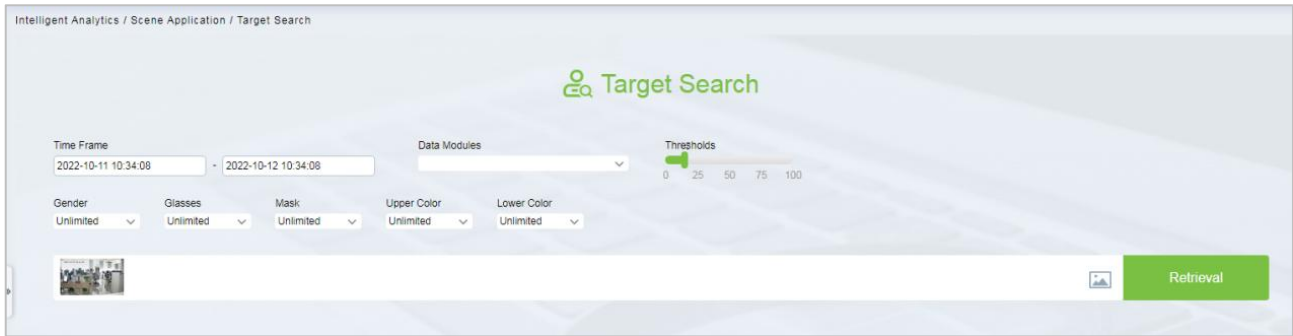
Step 3: Next click [**Retrieval**].

Figure - Target Search

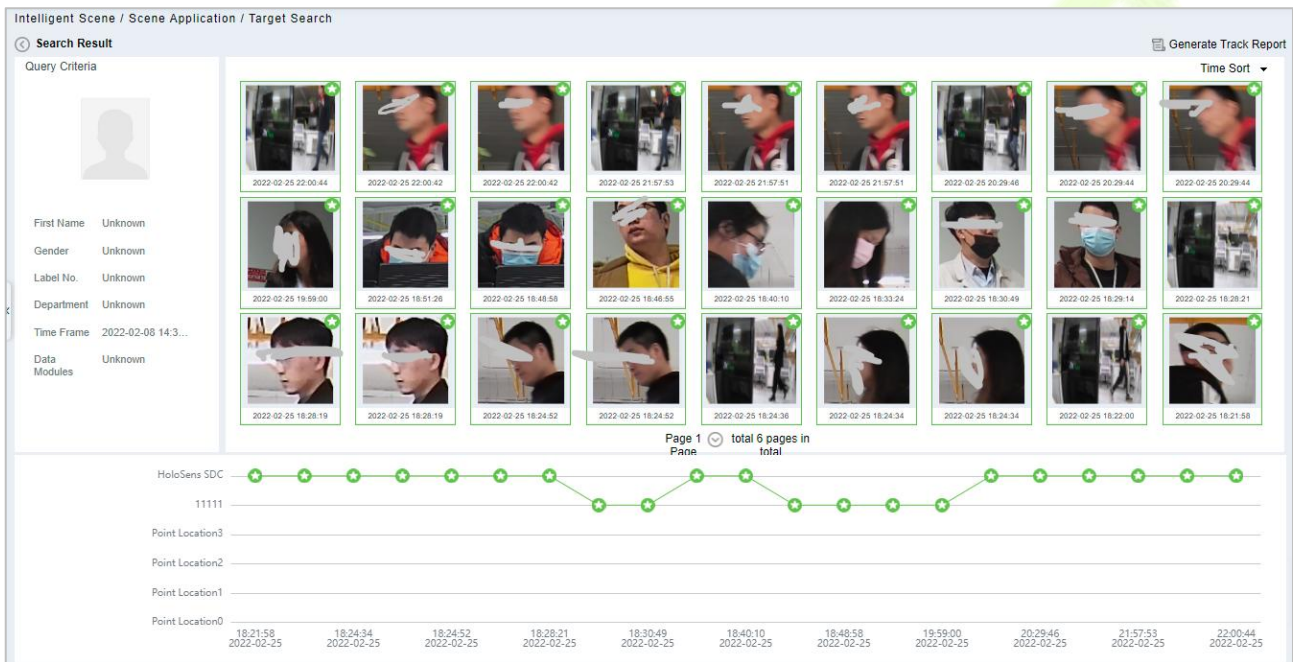**Step 4:** After the retrieval, the retrieval results appear, as shown in Figure below.

Figure - Object Lookup Retrieval Results

Step5: 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 below.
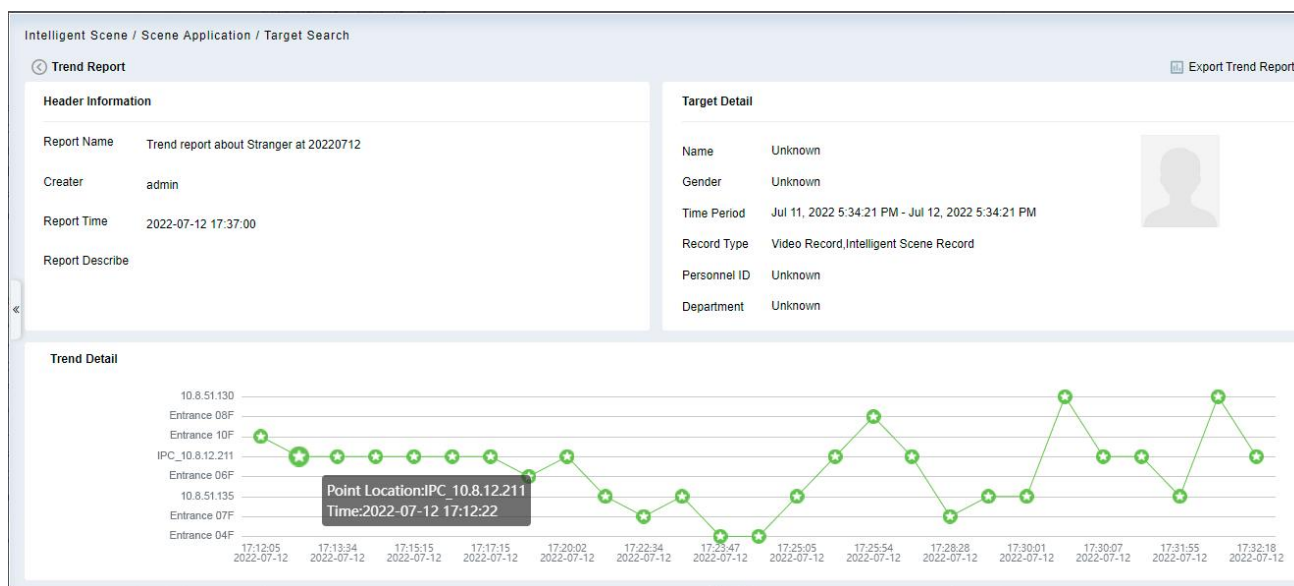

Figure – Trend Report 1

Figure – Trend Report 2

2.5 Visitor Module-Respondent Self-Approval

Optimize the visitor process, after the visitor invitation email is sent, 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:

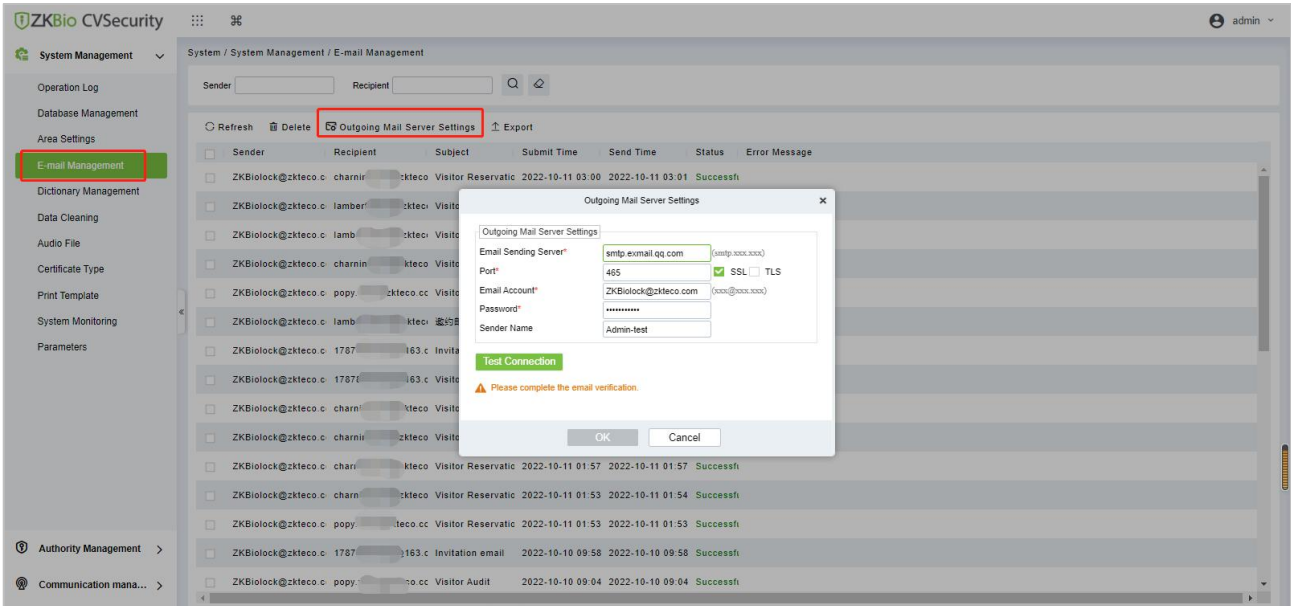**Step 1:** In the System Management, click [**Email Management**] >[**Outgoing Mail Server Settings**].

Figure - Outgoing Mail Server Settings

Step 2: Set the Outgoing Mail Server Settings as Table below:

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. 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 - 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:

In [**Visitor]** module, Click [**Basic Management**] > [**Parameters].**

Select [**No**] for the [**Enable automatic review of guest appointments],** so that the visitors' reservations need to be approved.
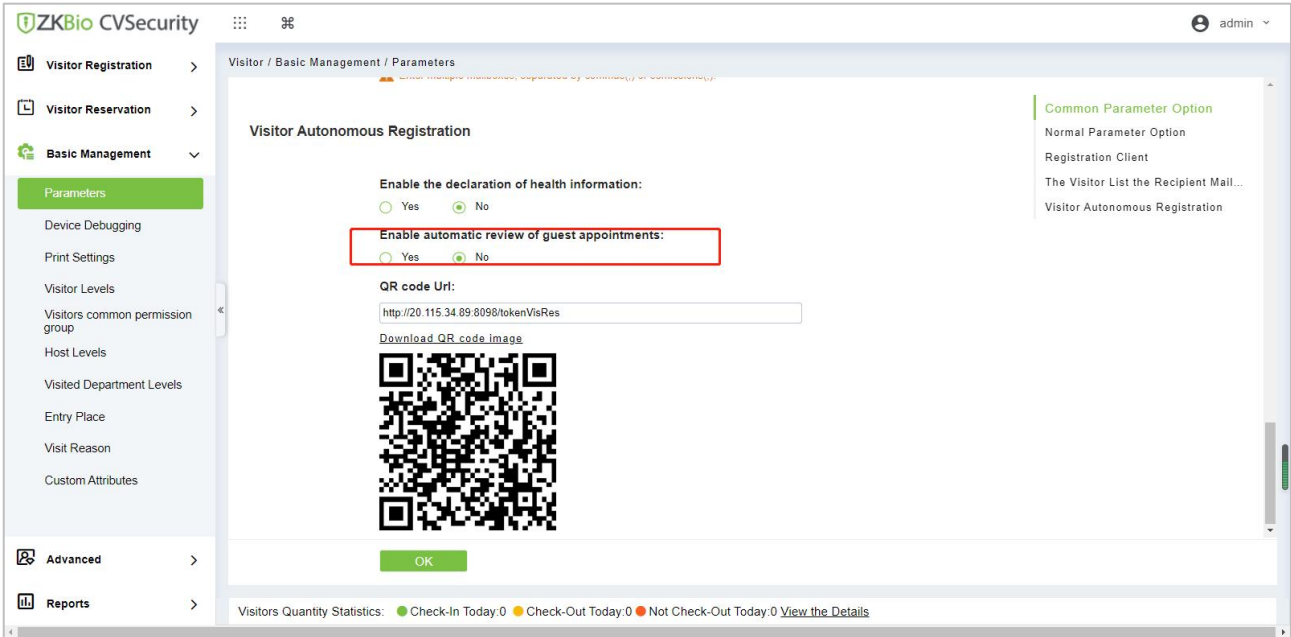

Figure - Enable automatic review of guest appointments

Set the Host Levels:

In the **Visitor** Module, click [**Visitor**] > [**Host Levels**]> [**+New**], select the corresponding personnel, click ⎯, set the host Level for the corresponding personnel.
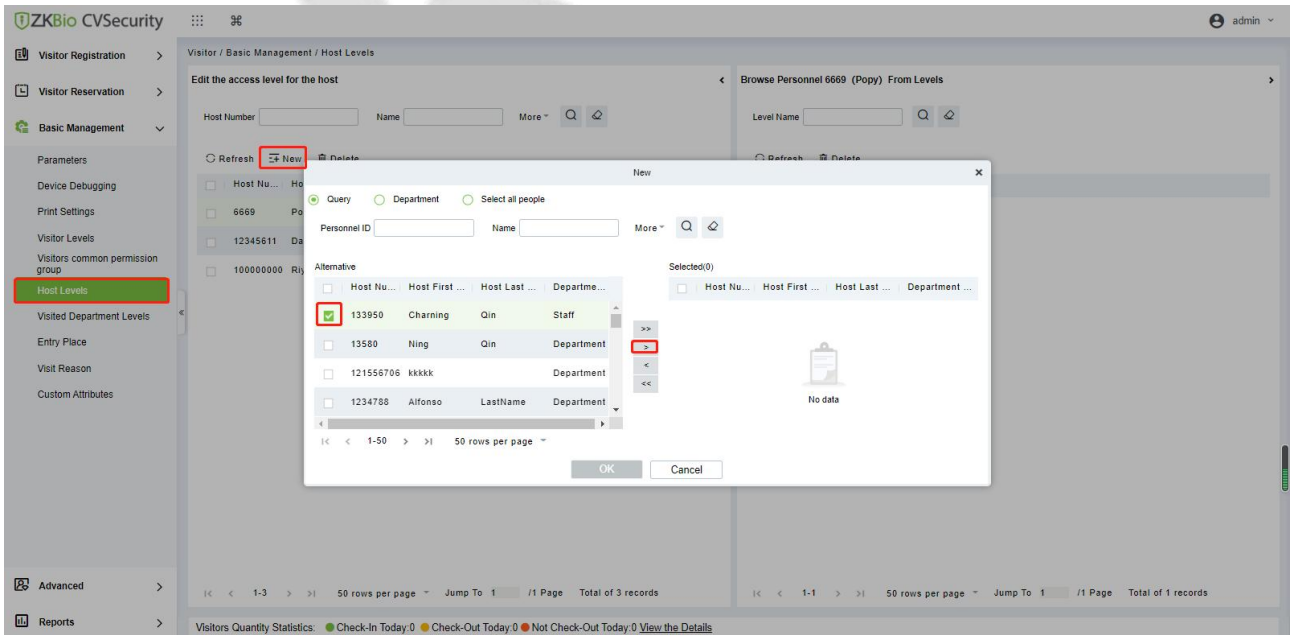

Figure - Adding Host Levels 1

Set the Linkage:

Step 1: Add an Alert Template. Click [**Visitor**] > [**Advanced**] > [**Alert Template**] > [**+New**] and fill in the template information.
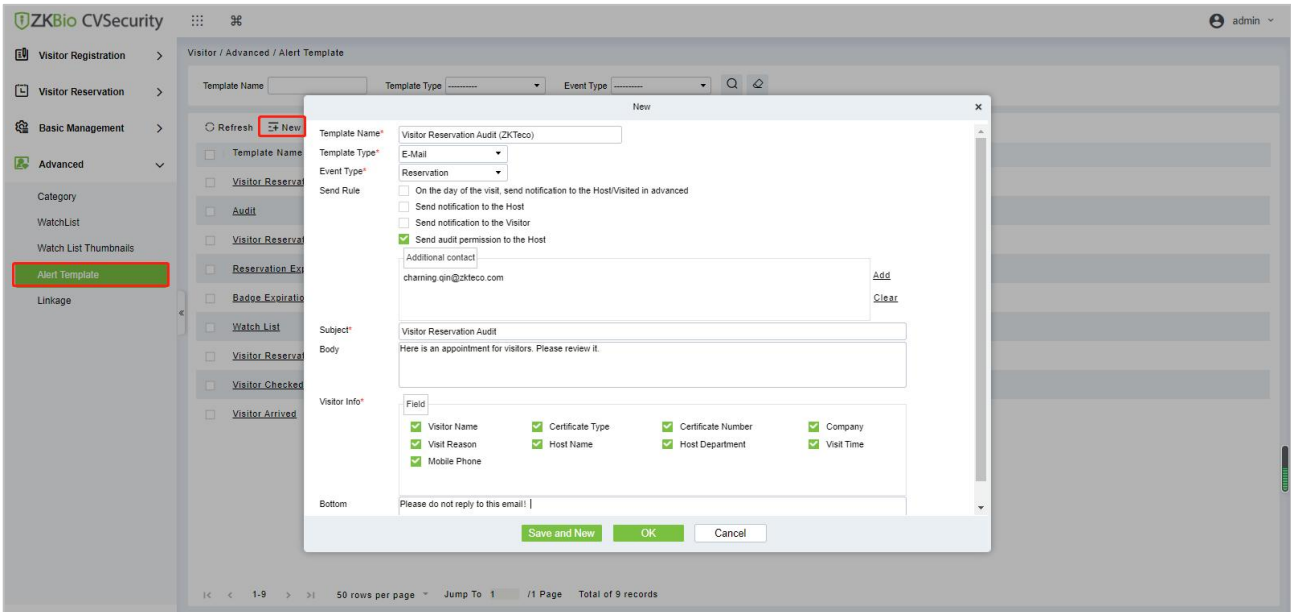

Figure - Add an Alert Template.

Parameter	How to Set Up
Template Type	E-Mail.
Event Type	Reservation.
Send Rule	Select Send audit permission to the Host. Fill in the Additional Contact with the host email.
Subject	Fill in the subject and the body content.
Visitor Info	Select the visitor content to be audited.

Table - Add an Alert Template

Step 2: Add a Linkage. Click [**Visito**r] > [**Advanced**] > [**Linkage**] > [**+New**], and here we select the E-mail template **Visitor Reservation Audit(ZKTeco)** added in **Step 1**.
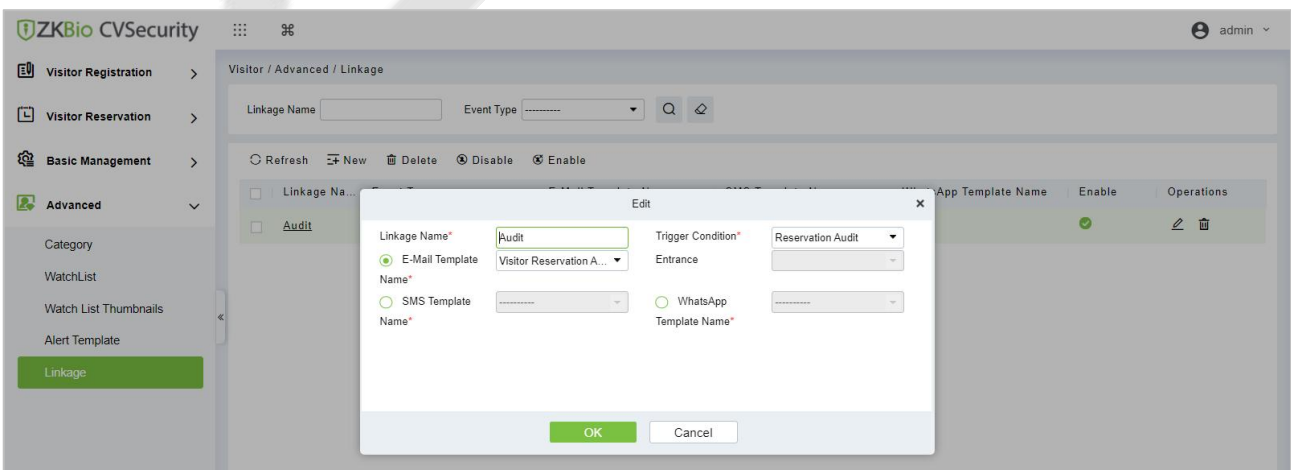

Figure -5 Add a Linkage

Send an invitation E-mail:

Step 1: Click [**Visitor**] > [**Visitor Reservation**] > [**Invite**] > [**+New**], fill in the correct information and save.
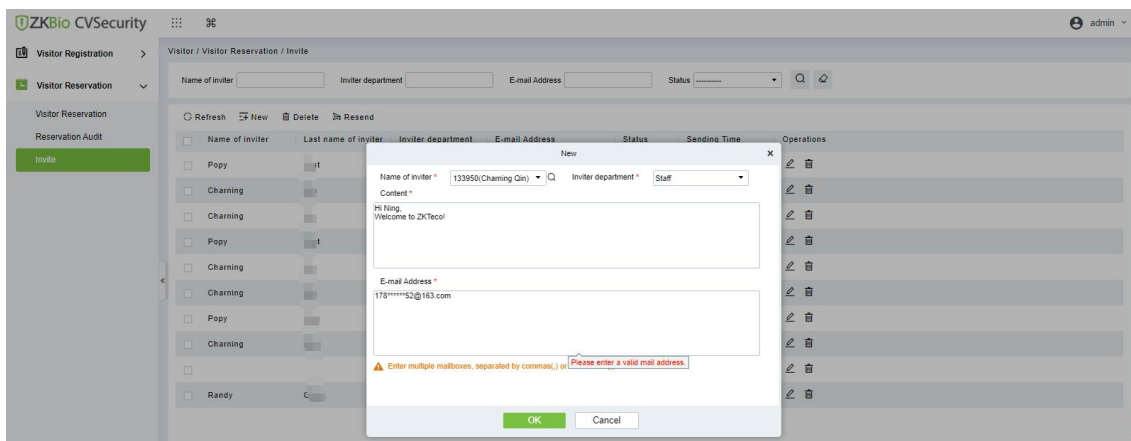
Figure - Send an invitation E-mail 1

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.
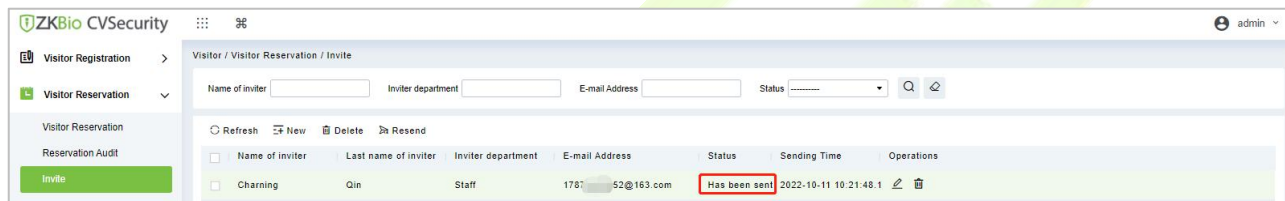
Figure - Send an Invitation E-mail 2

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 - Invitation E-mail

Figure - 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.

Figure - Visitor Reservation Audit

Privacy Policy

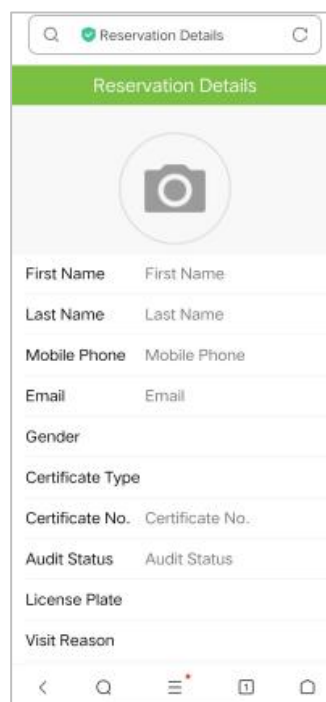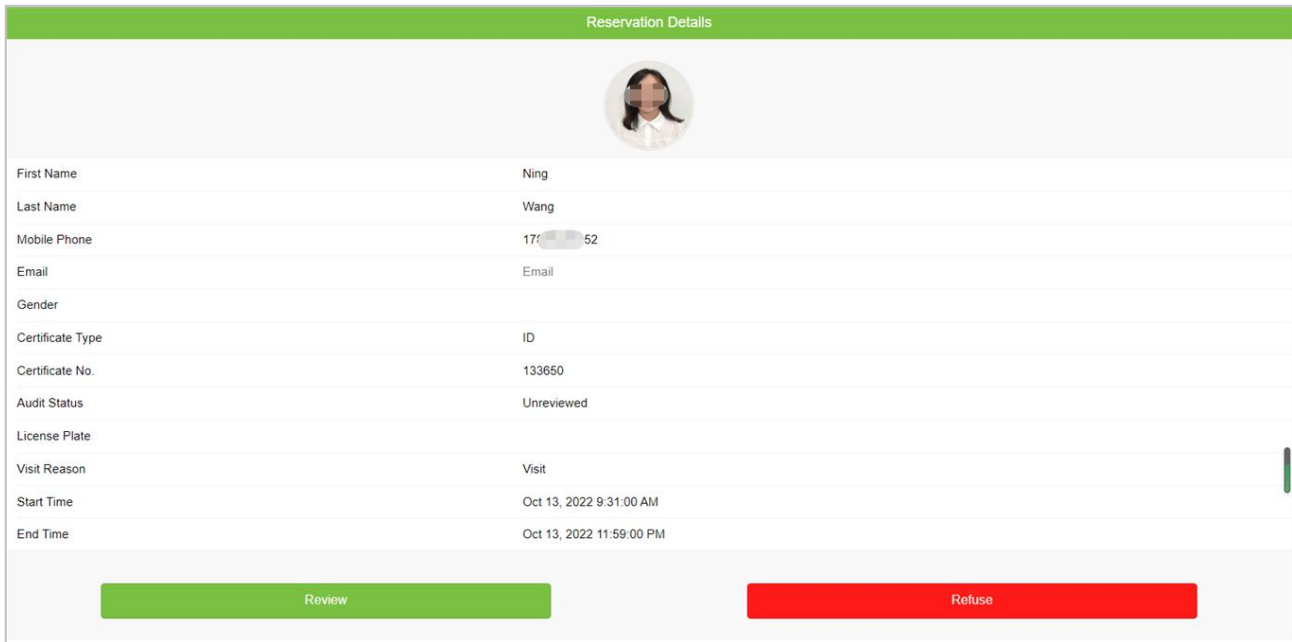**Notice:**

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. **Collected Information**

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. **Product Security and Management**

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com