

EZAccess
Client Software
User Manual

Manual Version: V1.14

Thank you for purchasing our product. If there are any questions, or requests, please do not hesitate to contact the dealer.

Notice






CAUTION!

Please set a password of 9 to 32 characters, including all three elements: letters, digits and special characters.

- The contents of this document are subject to change without prior notice. Updates will be added to the new version of this manual. We will readily improve or update the products or procedures described in the manual.
- Best effort has been made to verify the integrity and correctness of the contents in this document, but no statement, information, or recommendation in this manual shall constitute formal guarantee of any kind, expressed or implied. We shall not be held responsible for any technical or typographical errors in this manual.
- The illustrations in this manual are for reference only and may vary depending on the version or model. So please see the actual display on your device.
- This manual is a guide for multiple product models and so it is not intended for any specific product.
- Due to uncertainties such as physical environment, discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.
- Use of this document and the subsequent results shall be entirely on the user's own responsibility.

Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
 WARNING!	Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.
 CAUTION!	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 NOTE!	Means useful or supplemental information about the use of product.

Contents

1 Introduction	1
2 System Requirements	1
3 Login	1
4 GUI Introduction	2
5 Device Management	2
5.1 Add a Device	3
5.2 Time Sync	3
5.3 Device Upgrade	4
5.3.1 Local Upgrade	4
5.3.2 Online Upgrade	4
6 Personnel Management	5
6.1.1 Organization	5
6.1.2 Add a Person	6
6.1.3 Delete a Person	9
6.1.4 Other Operations	10
7 Visitor Management	10
7.1 Visitor Registration	10
7.2 Visitor Records	14
8 Access Control	14
8.1 Access Permissions	14
8.2 Holiday Management	16
9 Attendance Management	17
9.1 Attendance Regulations	17
9.2 Staff Schedule	18
9.2.1 Set Time Period	18
9.2.2 Shifts Management	20
9.2.3 Schedule Management	21
9.3 Attendance Handling	22
9.3.1 Leave Management	22
9.3.2 Re-Sign In&Out Management	23
9.3.3 Re-Sign In&Out Records	24

9.4 Attendance Statistics	24
9.4.1 Original Data	25
9.4.2 Attendance Details	25
9.4.3 Attendance Summary	26
10 Status Monitoring	27
10.1 Realtime Monitoring	27
10.2 History Records	28
11 System Configuration	28
11.1 Snapshots	28
11.2 Alarm Parameter Configuration	28
11.3 Auto Time Sync	29
11.4 Database Management	29
11.5 System Maintenance	30
11.6 NVR Configuration	31

1 Introduction

EZAccess is an attendance management software application program based on access control and used with access control devices. EZAccess supports device management, personnel management, access control and attendance management. EZAccess supports flexible deployment and meets various demands from small and mid-sized access control and attendance management projects.

2 System Requirements

The computer (PC) that runs the software shall meet the following minimum configuration. The actual system requirements may vary depending on the way EZAccess is used.

Specifications	Requirements
Memory	4GB or more
HDD	At least 20GB free space
Monitor	1440*900 resolution or higher
Operating system	Microsoft Windows 7/10, 64-bit



CAUTION!

- Please disable the antivirus software on your computer before you start installation.
 - If you are using V1.2.0.1 or later, you can upgrade the version by directly installing a higher version without uninstalling the current version.
 - When the client software starts, it automatically disables the sleep mode on the computer. Do not enable sleep mode.
 - If the antivirus software alerts you to risks when scanning the client software, please ignore the alert or add the client software on the trusted list.
-

3 Login

Enter the username and password, click **Login**.

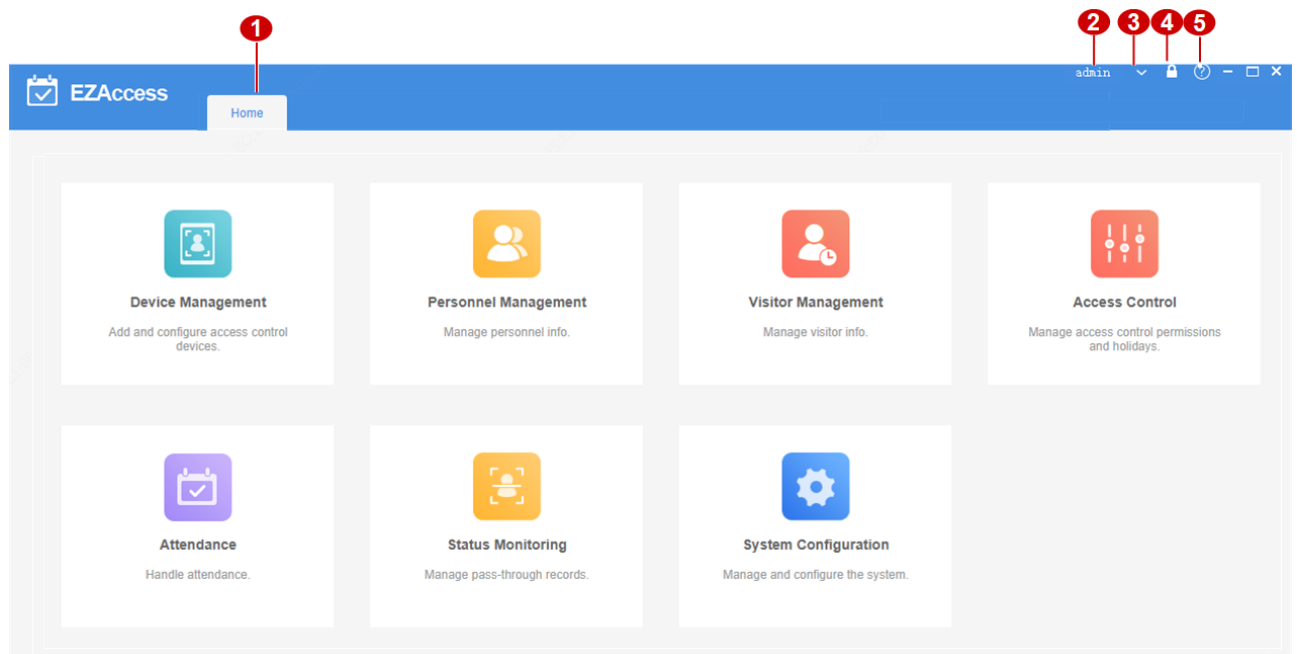


NOTE!

- For first-time login, a page is displayed for you to create new users. Enter the username and password for the new user. Please set a strong password to enhance account security.
 - If **Auto Login** is selected, EZAccess will skip the login page at the next startup and automatically log in using the most recently used username.
-

4 GUI Introduction

The main page is displayed when you are logged in. The main page consists of the Control Panel and some functional buttons.



No.	Description
1	Home page, including Device Management, Personnel Management, Visitor Management, Access Control and Attendance Management, Pass-thru Records and System Configuration modules.
2	Shows the current username. Click to view the user type and login time.
3	Click to change password or log out.
4	Lock button. Click to lock the client software. A password is required to unlock the client software.
5	Help button. Click to view software information, open source software licenses or the user manual.

5 Device Management

Use EZAccess to manage face recognition access control devices and access controllers. Add face recognition access control devices and access controllers for access control and attendance management.

- Face recognition access control device: Refers to access control devices that allow persons to use their face to unlock doors.
- Access controller: Refers to devices that control multiple access control devices.

5.1 Add a Device

1. Click Device Management > Face Recognition/Access Controller on Control Panel.




NOTE!

Click **Add** to add a device with a known IP address. This section describes how to search devices on the same subnet with the PC and add the discovered face recognition access control devices or access controllers.

2. Click **Auto Search**. Face recognition access control devices or access controllers on the same subnet with the PC are discovered.

Auto Search						
+ Batch Add		IP Address: 192.168.2.0 - 192.168.2.255		Status: All	Auto Search	
<input type="checkbox"/>	Status	IP Address	Port	Model	Serial No.	Operation
<input type="checkbox"/>	No	192.168.2.214	80	ET-B31H-M		+

3. To add a device, click  for the device in the **Operation** column. To add multiple devices with the same configurations (username/password), select the devices and then click **Batch Add**. Narrow down the search by setting search conditions:
 - IP address: Search devices within the specified range.
 - Status: Filter devices that have been added or not.
4. Check whether the device is online.



NOTE!

- Up to 32 face recognition access control devices and access controllers are allowed.
- Before you add a face recognition access control device, configure a fixed IP and set a default face library on the device. See the device user manual for detailed information.

5.2 Time Sync

Select the device and click **Time Sync** to synchronize time with the PC. For periodic auto time synchronization, please see [Auto Time Sync](#).

Auto Search							
<input type="checkbox"/>	+ Add	<input type="checkbox"/> Delete	<input type="checkbox"/> Refresh	<input type="checkbox"/> Time Sync			
<input type="checkbox"/>	Device Name	IP Address	Port	Device Type	Model	Status	Operation
<input type="checkbox"/>	A	192.168.2.214	80	Access control	ET-B31H-M	Online	



NOTE!

- Only online face recognition access control devices are available for time sync.
- Newly added or newly online device will be automatically synchronized once.

5.3 Device Upgrade


There are two ways to upgrade a device as follows.



CAUTION!

- Only online face recognition access control devices can be checked for updates and upgrade online.
- Only online devices can be upgraded.
- Do not perform device related operations during upgrade.


5.3.1 Local Upgrade

1. Click **Device Management > Device Upgrade > Face Recognition/Access Controller**.
2. Select the target device to upgrade, click , and then select **Local Upgrade**.



NOTE!

You can upgrade devices of the same type in batches.

3. In the **Select File** dialog box, click  to select the upgrade file. To upgrade face recognition access control devices, select a ZIP file. To upgrade access controllers, select an RCBIN file.
4. Click **OK** to start upgrade.

5.3.2 Online Upgrade



NOTE!

Only face recognition access control devices are available for online upgrade.

1. Click **Device Management > Device Upgrade**.
2. Select devices and click **Check Update** to see whether a new version is available.

<input type="checkbox"/>	Device Name	IP Address	Device Type	Model	Current Version	New Version	Firmware Upgrade	Status
<input type="checkbox"/>	██████████	██████████	Access control	ET-B31H-M@B	QPTS-B2209.6.2.2 10912	QPTS-B2209.6.7.2 20111	--	<input checked="" type="checkbox"/> Online
<input type="checkbox"/>	██████████	██████████	Access control	ET-B31H-M@B	QPTS-B2209.6.2.2 10912	QPTS-B2209.6.7.2 20111	--	<input checked="" type="checkbox"/> Online

3. Select the target device to upgrade, click , and then select **Online Upgrade**.

<input type="button" value="Check Update"/> <input type="button" value="Online Upgrade"/> <input type="button" value="Refresh"/>		Device Name	IP Address	Device Type	Model	Current Version	New Version	Firmware Upgrade	Status
<input type="checkbox"/>	192.168.1.101	192.168.1.101	Access control	ET-B31H-M@B	QPTS-B2209.6.2.2 10912	---	<div style="width: 20%; background-color: #007bff; height: 10px;"></div> 20% Upgrading	<input checked="" type="checkbox"/> Online	
<input type="checkbox"/>	192.168.1.102	192.168.1.102	Access control	ET-B31H-M@B	QPTS-B2209.6.2.2 10912	---	<div style="width: 20%; background-color: #007bff; height: 10px;"></div> 20% Upgrading	<input checked="" type="checkbox"/> Online	

6 Personnel Management

Add persons for attendance management.

6.1.1 Organization

1. Click **Personnel Management** on Control Panel.

The screenshot shows the Personnel Management interface. On the left, there is a 'Department' sidebar with a search bar and a list of departments (dept, 1, 2). The main area has a search bar for 'Name' and 'ID No.', and a 'Search' button. Below the search bar are several action buttons: '+ Add', 'Delete', 'Assign Personnel', 'Batch Import', 'Export', 'Download Template', and 'Batch Import pictures'. A 'Get Personnel' button is also present. The main table displays personnel records with columns for Person ID, Name, Gender, Department, ID No., Card Number, Phone, and Operation. The table contains three rows of data.

Person ID	Name	Gender	Department	ID No.	Card Number	Phone	Operation
<input type="checkbox"/> 001	...	Female	dept				
<input type="checkbox"/> 002	...	Male	dept				
<input type="checkbox"/> 003	...	Male	dept				

2. Click to edit the organization name on the left-side organization list.

3. To create an organization, click right to the root organization, enter the organization name. The organization appears on the organization list. You can add more organizations in the same way. To delete an organization, click . Up to 10 levels of organizations are allowed.



NOTE!

- The root organization cannot be deleted.
- An organization that includes organizations cannot be deleted.

Click an organization to view people in the organization and its sub-organizations.


6.1.2 Add a Person

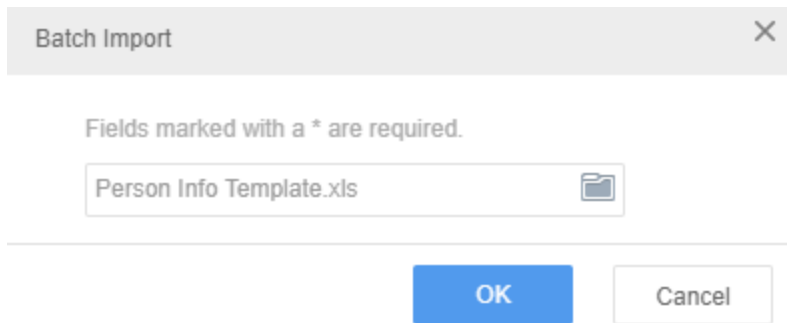


NOTE!

- Totally up to 5000 persons are allowed. Up to 500 persons are allowed in an organization (not including sub-organization).
- If a person ID already exists on the client, then a person with the same person ID cannot be added before the existing person ID is deleted from the client.
- Up to six face images can be uploaded for each person. Only JPG images are allowed. Image size: 10KB-512KB. Max resolution: 1080px*1920px.

1. Add in batches

1. Click **Personnel Management** on Control Panel.
2. To download the default template, click **Download**.
3. Enter the required personal basic information in the template. Fields marked with a * are required.
4. Click Batch Import.
5. In the **Batch Import** dialog box, click  to select the file and then click **OK**.



6. The list updates automatically when data is imported successfully.



NOTE!

- Up to 5000 persons can be imported at a time.
- Import will fail if the imported person ID, ID number, or card number is duplicate. You can view the failure details in the pop-up window.



Person ID	Name	failure reason
001	ZhangSan	Duplicate data
002	XiaoMing	Duplicate data

2. Add one by one

1. Click **Personnel Management** on Control Panel.
2. Select the target organization from the left-side organization list, click **Add**.

Department: Name: ID No.:

Please enter keywords.

<input type="checkbox"/>	Person ID	Name	Gender	Department	ID No.	Card Number	Phone	Operation

3. Complete the required personal information. Fields marked with a * are required.

Add ×

Basic Information

* Person ID: Date of Birth:

* Name: Phone:

Gender: Male Female Unknown Department:

Address: Remarks:

Door Opening Pas...

Card Information

Read Mode: Local Remote

Serial Port for Card...

ID No.: Card Number:

Card Password:

Photo (It is recommended to upload no more than 6 images. Range from 10KB to 512KB and 1080*1920px. JPG only).

4. (Optional) Door opening password can be generated automatically and entered manually. After a door opening password is set, the person can use the password to access specified doors configured in access permissions.



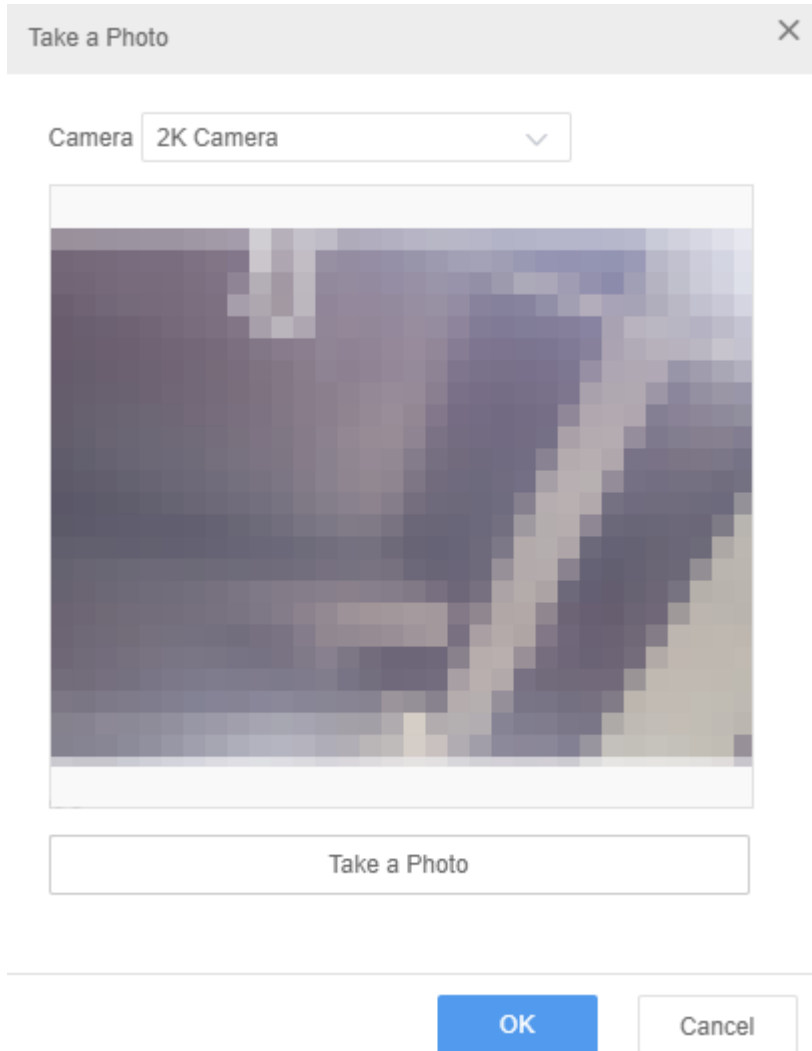
NOTE!

Door opening passwords cannot be duplicate.

5. (Optional) Choose a way to complete the card information.

- Read automatically:
 - Read locally: Select the serial port of the card reader on your PC, and click **Read**. Present your card on the card reader, and the card information will be read automatically.
 - Read remotely: Select a face recognition access control device and click **Read**. Present your card to the device, and the card information will be read automatically.
- Enter manually: Enter the card information directly.

6. (Optional) Click **Add Photo**, and choose one way to add photos.
- Upload: Select a photo from the PC.
 - Take a photo: Select a camera, and view the real-time screen of the selected camera on the client. Click **Take a Photo** and then you can check the photo on the client. Click **Retry** if necessary, or click **OK** to save the photo.



NOTE!

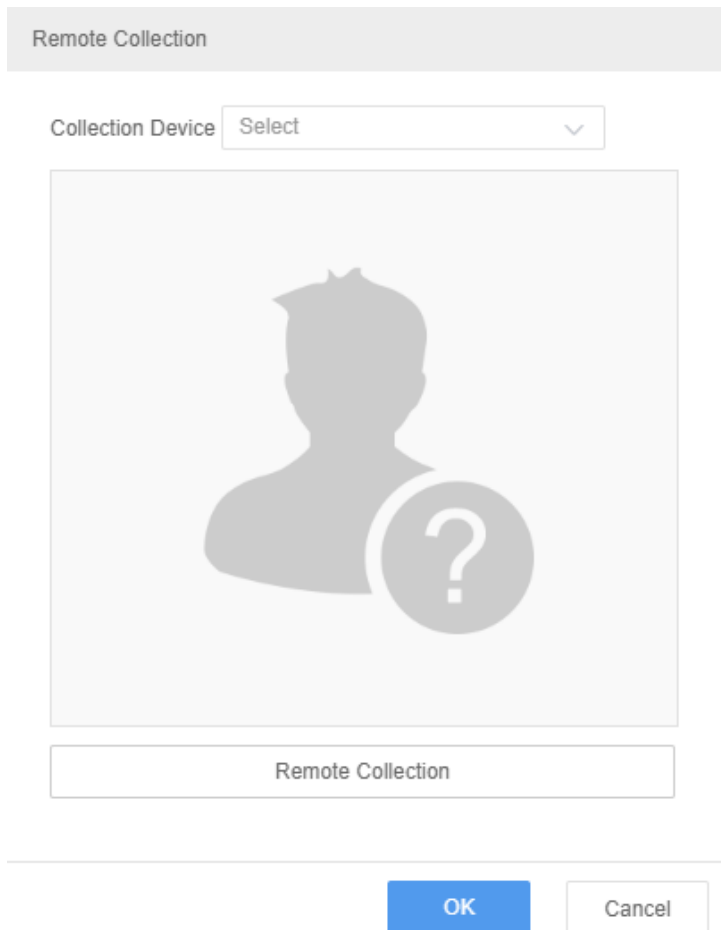
Only cameras that come with the computer and USB cameras are supported. To use a USB camera, you need to connect it to your PC in advance.

- Remote collection: Select a face recognition access control device and click **Remote Collection**. After the device completes face collection, you can check the collected photo on the client. Click **Re-Collect** if necessary, or click **OK** to complete the collection.



NOTE!

Remote collection is only supported by face recognition access control devices.



7. Click **OK**.

Click the organization on the left-side organization list. The persons in the organization are listed on the right side.

3. Import pictures in batches

1. Click Batch Import Pictures.
2. Upload a ZIP file that includes images named in this format: Person ID_OrderNum.
3. Click **OK**. The pictures are imported.

4. Get personnel

1. Click **Get Personnel**, and then select the target device.
2. Click **OK**. The personal information of the device is shown in the table below. The personnel successfully got will be deleted from the device side and assigned to the temporary department. Please assign personnel according to the actual situation.


6.1.3 Delete a Person

1. Delete in batches

1. On the left-side organization list, click the organization that the person belongs to, click **Add**.
2. Select the person you want to delete.

3. Click **Delete**.
4. In the dialog box displayed, click **OK**.

2. Delete one by one

1. On the left-side organization list, click the organization that the person belongs to, click **Add**.
2. Click  below the person you want to delete.
3. In the dialog box displayed, click **OK**.

6.1.4 Other Operations

1. Search personal information

Enter the name or ID number on the top and then click **Search**. Search results are displayed.

2. Export personal information

Click **Export** on the right to export all the personal information.

3. Assign personnel

Select an organization on the left-side organization list, select the personnel to be assigned on the right, and then click **Assign Personnel** to assign the personnel to an organization except temporary department.

7 Visitor Management

Manage visitors by signing in/out and assigning/withdrawing access permissions.

7.1 Visitor Registration

Register visitor information and assign access permissions to visitors.

1. Click **Visitor Registration**. Complete the basic information about the visitor. The field marked with a * is required.

Visitor Registration
✕

1
 Complete Basic Info

2
 Assign Access Permission

Basic Information

<p>* Name: <input style="width: 90%;" type="text"/></p> <p>Gender: <input checked="" type="radio"/> Male <input type="radio"/> Female <input type="radio"/> Unknown</p> <p>Phone: <input style="width: 90%;" type="text"/></p> <p>Remarks: <input style="width: 90%;" type="text"/></p>	<p>Total Visitors: <input style="width: 90%;" type="text"/></p> <p>Organization: <input style="width: 90%;" type="text"/></p> <p>Person to Visit: <input style="width: 90%;" type="text"/></p> <p>Dept. to Visit: <input style="width: 90%;" type="text"/></p>
---	--

Card Information

Read Mode: Local Remote

Serial Port for Card...: Read

ID No.:

Card Password:

Card Number:

Photo (It is recommended to upload no more than 6 images. Range from 10KB to 512KB and 1080*1920px. JPG only).

+

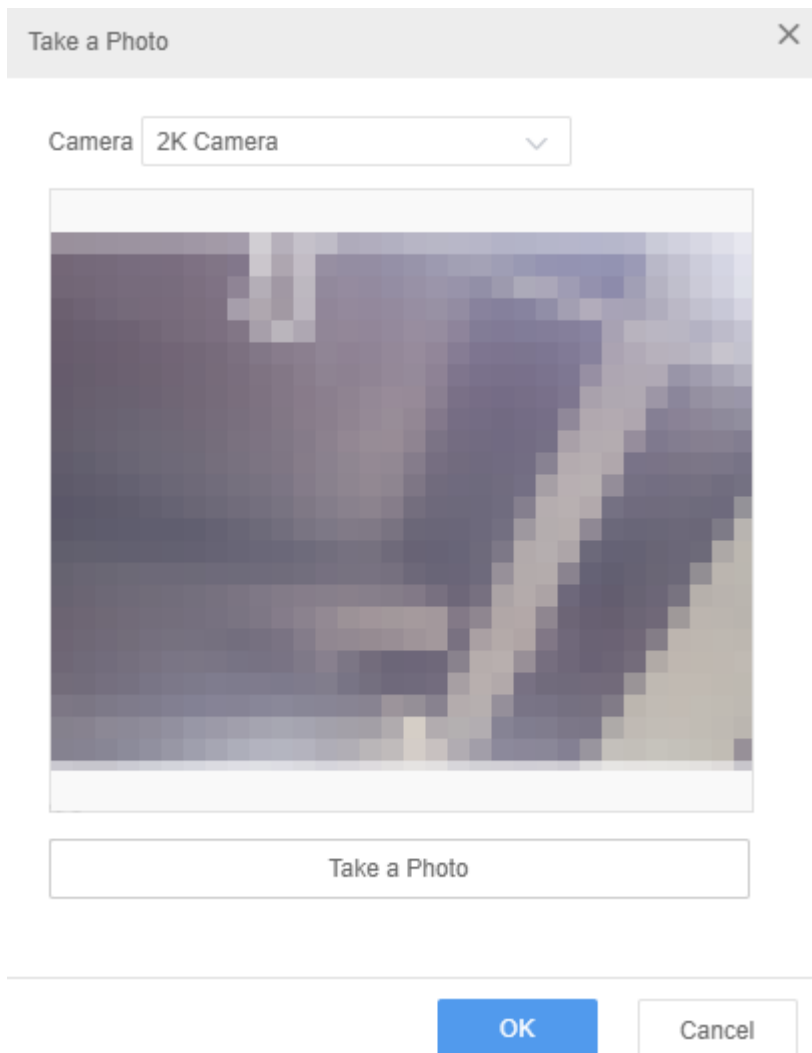
Reset
Next
Cancel

2. (Optional) Choose one way to complete the card information.

- Read automatically:
 - Read locally: Select the serial port of the card reader on your PC, and click **Read**. Present your card on the card reader, and the card information will be read automatically.
 - Read remotely: Select a face recognition access control device and click **Read**. Present your card to the device, and the card information will be read automatically.
- Enter manually: Enter the card information directly.

3. (Optional) Click **Add Photo**, and choose one way to add photos.

- Upload: Select a photo from the PC.
- Take a photo: Select a camera, and view the real-time screen of the selected camera on the client. Click **Take a Photo** and then you can check the photo on the client. Click **Retry** if necessary, or click **OK** to save the photo.



NOTE!

Only cameras that come with the computer and USB cameras are supported. To use a USB camera, you need to connect it to your PC in advance.

- Remote collection: Select a face recognition access control device and click **Remote Collection**. After the device completes face collection, you can check the collected photo on the client. Click **Re-Collect** if necessary, or click **OK** to complete the collection.




NOTE!

Remote collection is only supported by face recognition access control devices.

Remote Collection

Collection Device Select ▼



Remote Collection

OK
Cancel

4. Click **Next**. Set valid access time and accessible doors for the visitor. You can select face recognition access control devices and doors under access controllers at the same time.

Visitor Registration ×

1 Complete Basic Info
 2 Assign Access Permission

Name: ZhangSan

Face Recognition Access Controller

End Time: 🕒 2022-10-11 23:59

Please enter keywords. 🔍

All


- test-controller
 - 🚪 Door1
 - 🚪 Door2
 - 🚪 Door3
 - 🚪 Door4

Previous
OK
Cancel


5. Click **OK**. The visitor has access to the selected doors within the valid time after registration.

Other Operations


- Sign out

Click  in the **Operation** column to sign out. The visitor's access permissions will be cleared after signing out.


- View authorization status

Click  in the **Operation** column to view the authorization status of the visitor's access permissions.

- Edit access permissions

Click  in the **Operation** column to edit the visitor's access permissions as needed.

- Delete signed-in visitors





Click  in the **Operation** column to delete the signed-in visitor. The visitor's access permissions will be cleared after deletion.

7.2 Visitor Records

Click **Visitor Records**, search visitor information within the specified time period.

Sign In Time: - Today Last 7 days Last 30 days Current month Name:

<input type="checkbox"/>	Name	Gender	ID No.	Card Number	Phone	Person to Visit	Dept. to Visit	Sign In Time	Sign Out Time	Operation
--------------------------	------	--------	--------	-------------	-------	-----------------	----------------	--------------	---------------	-----------

- View details: Click  in the **Operation** column to view the visitor's information such as sign-in and sign-out.
- Delete visitor records: Select the records to be deleted and click  Delete , or click  in the **Operation** column.
- Export visitor records: Select the records to be exported, click  Export , and then select a path to save the records.

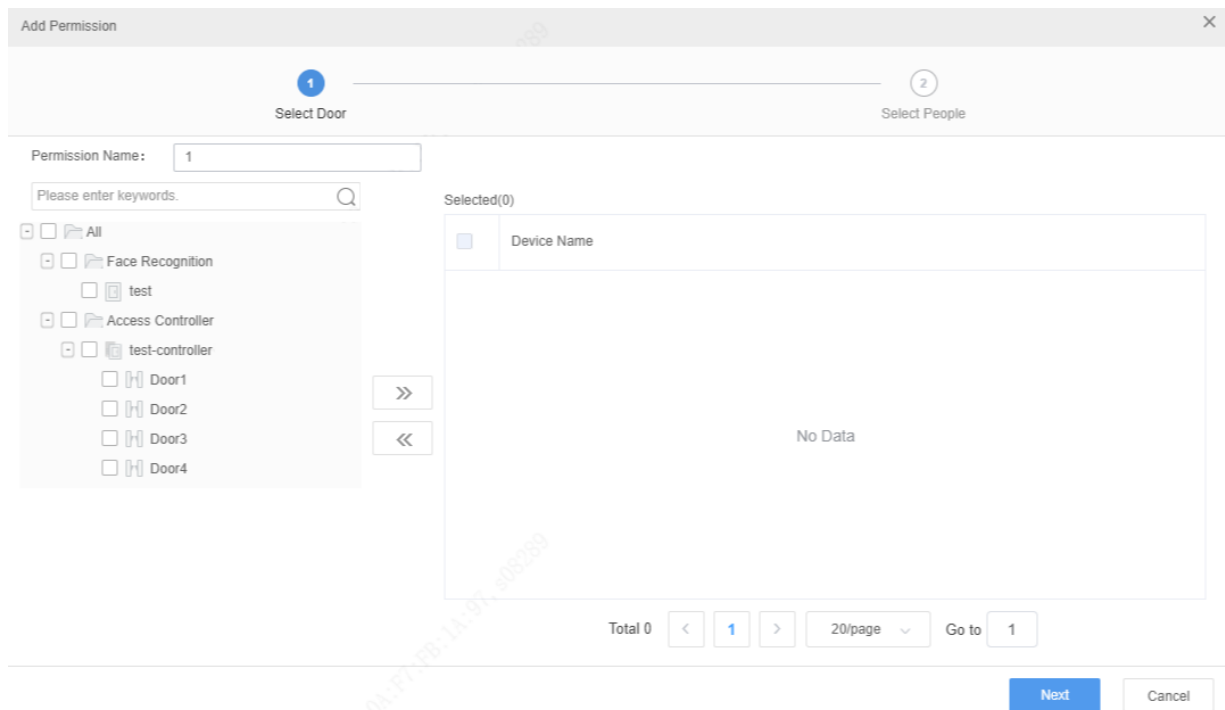
8 Access Control

8.1 Access Permissions

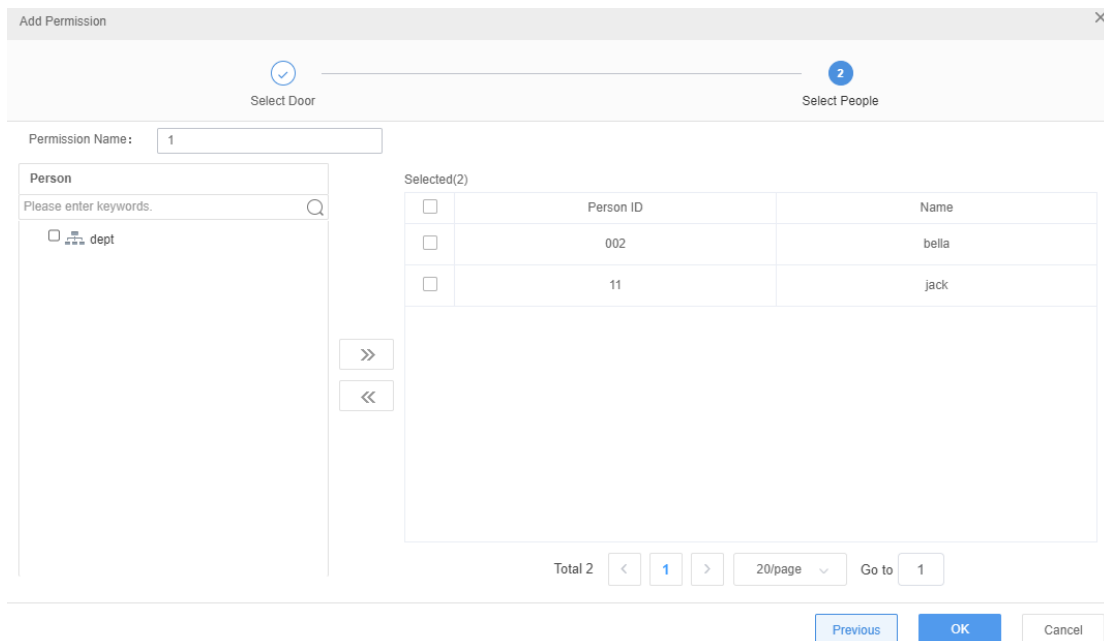
Access Control > Access Permissions

Assign permissions to allow access to specified doors.

1. Click Add Permission.
2. Enter the permission group name, select face recognition access control devices or doors under access controllers.
3. Click . The selected access control devices are added to the right-side list.
4. Click Next.





5. Select the persons you want to assign access permission, click . The selected persons are added to the right-side list.
6. Click **OK**. The specified persons now have access to the specified doors.





The permission group is listed. Click  to view permission assignment status.



A success displayed in the **Config Status** column means permission is successfully synced to the device; otherwise, failure.

On the **Access Permissions** page,  appears in the **Operation** column if permission assignment fails for any person in the permission group, in this case, you can click  to try permission assignment again for the failed person.

Click  or  to edit or delete a permission group.

8.2 Holiday Management

Access Control > Holiday Management

Set public holidays or specified days as holiday. Holiday has higher priority than attendance rules. For example, attendance rules require attendance during 9:00-17:00 from Monday to Friday. If New Year's Day is set as holiday, then holiday attendance rules are applied on New Year's Day.

Holiday Config
✕

*Holiday Name:

*Holiday Period:

Repeat By Year

1. Click **Add**, enter the holiday name and set the holiday period. The holiday name must be unique.
2. (Optional) If **Repeat By Year** is selected, the holiday will repeat every year.
3. Click **OK**.

Click or in the **Operation** column to edit or delete the holiday.



NOTE!

Up to 32 holidays are allowed.

9 Attendance Management

Set attendance regulations, schedule shifts, re-sign in or out for abnormal attendance records, and handle leaves. View attendance details and abnormal attendance summary.



NOTE!

The sign in&out time is only accurate to minute, ignoring second. That is, signing in at 08:00:59 is regarded as 08:00. All attendance calculations are also accurate to minute only.

9.1 Attendance Regulations

Attendance > Attendance Regulations > Attendance Rules

Set attendance rules.

Auto Calculation Time: Set automatic calculation time of attendance. The system will calculate the attendance data of the previous day at the set time every day. You can see attendance data in **Attendance Details**. If the automatic calculation of attendance data fails, please refer to [Attendance Details](#) for manual calculation.

Attendance Rules

* Auto Calculation Time:

🕒 12:00

Save

9.2 Staff Schedule

9.2.1 Set Time Period

Attendance > Staff Schedule > Period Settings

Select a period type and set it accordingly. You can select normal period and flexible period.

- Normal Period: For normal attendance, employees must sign in&out during the specified valid sign in&out time range.
- Flexible Period: For flexible attendance, employees can go to work at any time, and daily attendance duration can be calculated by the selected flexible duration calculation method.



NOTE!

All the times set on this page must be earlier than the auto calculation time of the next day.


Normal Period

Set work hours and valid sign in/out time range.

The screenshot shows the 'Normal Period' configuration interface. It features a search bar on the left with the text '(Normal) Default Period'. The main form contains the following fields and options:

- Period Name:** Default Period
- Period Type:** Normal Period
- Period Settings:**
 - Work Hours Start:** 09:00
 - Work Hours End:** 18:00
 - Valid Sign In Time:** 08:30 ~ 09:30
 - Valid Sign Out Time:** 17:30 ~ 18:30
 - Must Sign In:**
 - Must Sign Out:**
- Absence Settings:**
 - Signed In, Late Than:** 0 min(s), Mark As Late
 - Signed Out, Leave Early Than:** 0 min(s), Mark As Leave Early
 - Not Signed In, Mark As:** Absent
 - Not Signed Out, Mark As:** Absent

A 'Save' button is located at the bottom of the form.

1. Click .
2. Enter a name for the period.
3. Select Normal Period.
4. Set when the work hours start and end. One day will be added automatically (+1) if the **Work Hours End** time is earlier than the **Work Hours Start** time. The **Work Hours Start** time and

Work Hours End time must be within the range of **Valid Sign In Time** and **Valid Sign Out Time**.

5. Set whether sign-in and sign-out are mandatory.

➤ Sign-in and sign-out are mandatory

a Set Valid Sign In Time and Valid Sign Out Time: Specify a valid time range for sign-in and out. The time range includes the boundary values. For example, if the Valid Sign Out Time is 17:30-18:30, then sign-out is allowed during 17:30-18:30.

b Configure absence settings.

– Signed In, Late than x min(s), Mark As Late: If a person signs in within x min(s) after the Work Hours Start time, the attendance status is normal. x is no more than 999.

– Signed Out, Leave Early Than x min(s), Mark As Leave Early: If a person signs out within x min(s) before the Work Hours End time, the attendance status is Normal. x is no more than 999.

➤ Clear the checkboxes if sign-in and sign-out are not mandatory.

6. Click **Save**.



NOTE!

The valid sign-in time range must not overlap with the valid sign-out time range.

Flexible Period

The screenshot shows the 'Flexible Period' configuration interface. On the left, there is a list of periods: '(Normal) 1' and '(Flexible) 2'. The '(Flexible) 2' period is selected. On the right, the configuration form for the selected period is shown. It includes the following fields:

- * Period Name: 2
- * Period Type: Flexible Period
- * Flexible Duration Calculation: Cumulate Duration by Multiple
- * Valid Sign In&Out Interval: 5 min(s)
- Period Settings
 - * Daily Attendance Duration: 540 min(s)
 - * Switch to the Next Attendance Day At: 00:00

A blue 'Save' button is located at the bottom of the form.

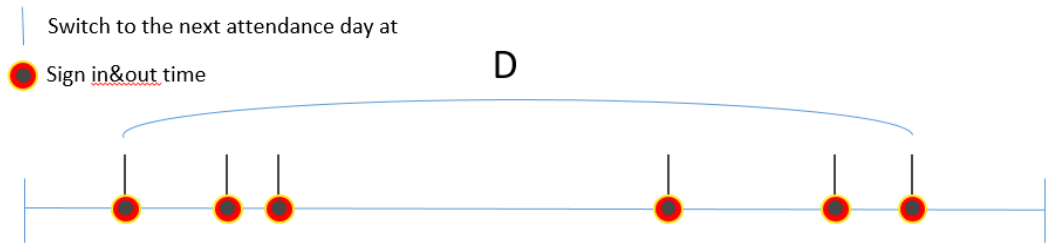
1. Click .

2. Enter a period name.

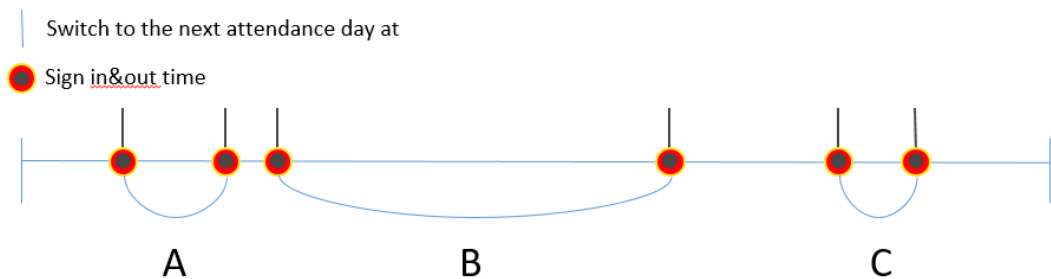
3. Select Flexible Period.

4. Select a method of flexible duration calculation.

➤ **Calculate Duration by First Sign-in and Last Sign-out:** Take the earliest sign-in time and the latest sign-out time during an attendance day to calculate the attendance duration. Taking the following figure as an example, the attendance duration is D.



- **Cumulate Duration by Multiple Sign Ins&Outs:** The attendance duration is cumulated by the duration of every two sign in&out during an attendance day. As shown in the figure below, the attendance duration is the total time period of the A+B+C. If the number of sign-ins&outs on one day is odd, the administrator can resign-in&out according to the actual situation and then calculate the attendance duration, otherwise all the sign ins&outs of the day would be invalid.



5. Set a valid sign in&out interval. The sign in&out is valid only if the interval between the two sign in&out is greater than or equal to the set interval.




NOTE!

Valid Sign In&Out Interval is displayed only when you select **Cumulate Duration by Multiple Sign Ins&Outs** in **Flexible Duration Calculation**.

6. Set a daily attendance duration. Absence will be recorded if the daily working time is less than the set daily attendance duration.
7. Set the time when the attendance day switches to the next attendance day. For example, if 01:00 is set, the attendance day is from today's 01:00 to the next day's 00:59. Signing in&out before 00:59 or at 00:59 in the next day is considered as today's attendance. Signing in&out after 01:00 or at 01:00 in the next day is considered as the next day's attendance.
8. Click **Save**.


Other Operations

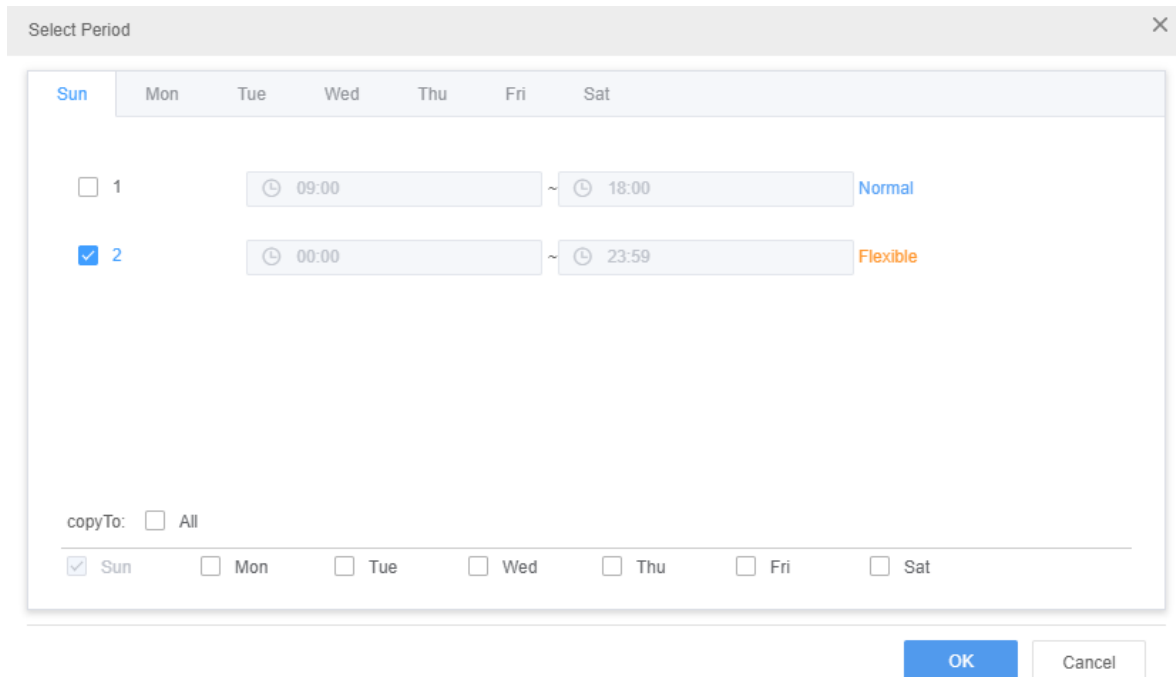
- Edit a period: Click a period name to edit the corresponding information on the right window.
- Delete a period: Select a period that needs to be deleted, click , and then confirm to delete the period.

9.2.2 Shifts Management

Attendance > Staff Schedule > Shift Mgt

Add shifts and set the corresponding time period for each shift.

1. Click , enter the shift name.
2. Click Select Period.



3. Select a workday on which the shift starts.
4. Select a time period (set in [Period Settings](#)).
5. Select workdays for the time period. Select **All** to apply the same settings to every day (Monday through Sunday).
6. Click **OK**.

Click **Empty** to clear all the valid time periods.



NOTE!

Up to 8 periods are allowed for each shift.

9.2.3 Schedule Management

Attendance > Staff Schedule > Schedule Mgt

Specify shifts for a department or a person.

1. Click Schedule.

2. Select the department or persons for which you want to set schedule.
3. Select a shift and set a validity period.
4. Click **OK**.



NOTE!

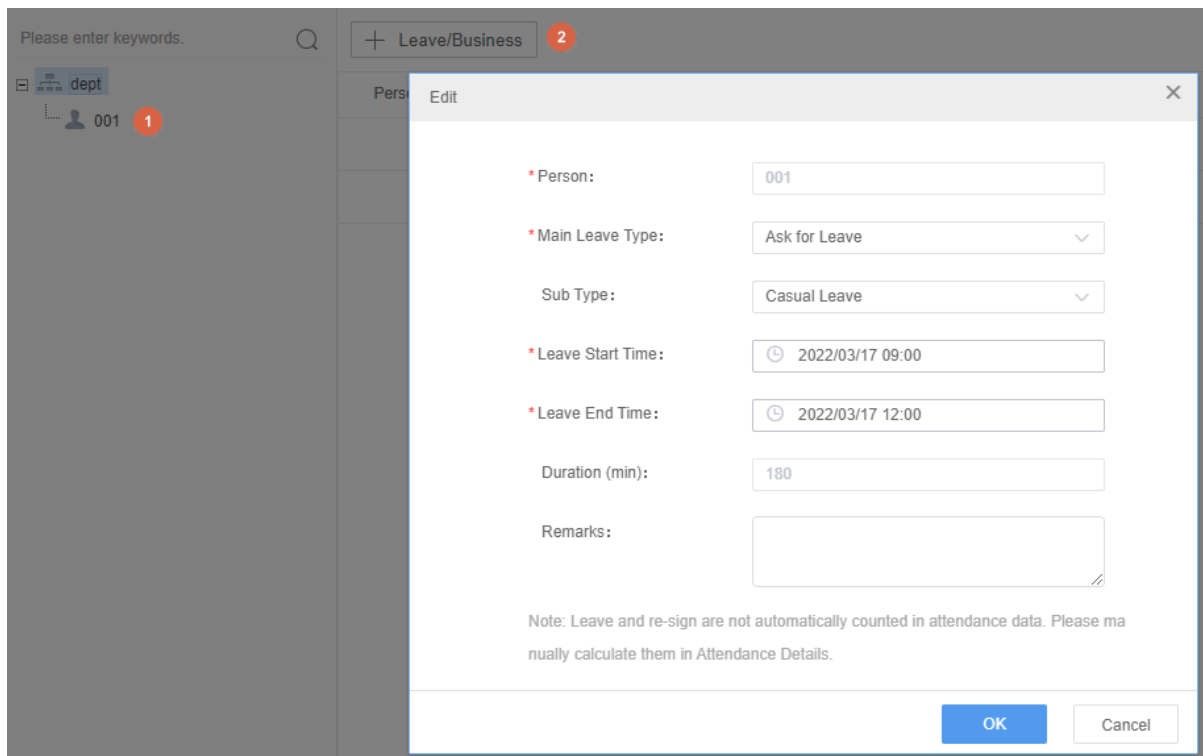
- You can schedule different shifts for a person by setting different validity periods for the shifts.
- Each person can have only one shift every day. If the validity period of the new shift and the old shift overlap, the overlapping part of the validity periods belong to the new shift.

To cancel a shift for a person, select the shift and then click **Cancel Schedule** on the top.



9.3 Attendance Handling

9.3.1 Leave Management

Attendance > Attendance Mgt > Leave Mgt





1. Select the target person on the organization list.
2. Click Leave/Business.
3. In the dialog box displayed, select the main leave type, set the leave start time and leave end time.
4. Select a sub-type. The **Sub Type** drop-down list is displayed only when the main type is **Ask for Leave**.
5. Click **OK**.

Click  or  in the **Operation** column to edit or delete the leave.



9.3.2 Re-Sign In&Out Management

Attendance > Attendance Mgt > Re-Sign In&Out Mgt

For abnormal attendance records such as absence, late arrival, you can modify the attendance records by re-sign in and out operations. After making a re-sign in or out, you can click **Calculate** in [Attendance Details](#) to update the attendance status and absent hours of this day.

Workday	Department	Person ID	Name	Shift Name	Work Hours	Sign In Time	Sign Out Time	Attendance Status	Absent (min)	Operation
2022/03/15	dept	001	001	Default Shift	09:00-18:00	(-)	(-)	Absent	540	 

1. Select the department or person on the left-side organization list.
2. Set a time range. All the abnormal attendance records of the specified department or person within this period are displayed.

3. Click  (re-sign in) or  (re-sign out) in the **Operation** column for the absence record you want to handle.
4. Modify the sign-in time or sign-out time as needed.
5. Click **OK**.



NOTE!


- The re-sign in or out time must be within the effective range, otherwise, the re-sign in or out operation is not effective.
- A person can be re-signed in or out up to 100 times a day. Before more re-sign operations can be performed for this person, you need to clean up re-sign in&out records for this person manually.
- For repeat re-sign or resign-out, the system will use the earliest re-sign in time and latest re-sign out time within the valid time range.


9.3.3 Re-Sign In&Out Records

Attendance > Attendance Mgt > Re-Sign In&Out Records

A record is generated each time a sign-in or sign-out time is modified manually. You can search, edit or delete re-sign in&out records on this page.

1. Select the department or person from the organization list.
2. Specify a time range and type, click **Search**. Search records are displayed.

Click  to modify a re-signed time.

Click  to delete a re-sign in&out record. After the record is deleted, the person's attendance statistics will use the original attendance data during the corresponding time period.

9.4 Attendance Statistics

Attendance statistics only include people in the system and do not include strangers. Entry/exit records of strangers are included in pass-thru records.

[Original Data](#): View all records of people entering or leaving by face recognition or swiping cards during the specified period.

[Attendance Details](#): View attendance details including attendance status and absence duration during the specified time period. One record is generated for each person every day.

[Attendance Summary](#): View the total length of absence during a specified period and the details.

9.4.1 Original Data

Attendance > Attendance Statistics > Original Data

View all the records of people entering or leaving by face recognition or swiping cards during a time period. For example, if there are five entries or exits, then five access records are displayed. Search original data of a department or a person using search criteria including person ID, name, department, date, time, body temperature, whether wearing a mask.

The screenshot shows a web interface for viewing original data. It includes a search bar with the text 'Please enter keywords.' and a magnifying glass icon. Below the search bar is a left-side organization list with a tree view showing 'dept' and a person icon with the number '1'. The main area contains search filters: 'Start and End Time' with a date range from '2021-02-27 00:00' to '2021-02-27 23:59' and buttons for 'Today', 'Last 7 days', 'Last 30 days', and 'Current month'. There are also input fields for 'Temperature(°C)' and 'Mask' (set to 'Unknown' with a '+2' dropdown). 'Search' and 'Reset' buttons are present. Below the filters are 'Export' and 'Sync Original Data' buttons. A table displays the search results with the following columns: Person ID, Name, Department, Device Name, Time, Temperature(°C), and Mask.

Person ID	Name	Department	Device Name	Time	Temperature(°C)	Mask
1	1	dept	206.10.81.13	2021-02-27 11:46	36.5°C	No

1. Select the department or person from the organization list.
2. Set a time range.
3. (Optional) Set a body temperature range and mask wearing status. This feature is available when the access control device supports this feature and the required configurations have been completed.
4. Click **Search**.

Search results are displayed. You can click **Export** to export the data.

Sync Original Data

Sync the original data reported by face recognition access control devices from the NVR to the client. You need to configure the NVR first in [NVR configuration](#).



NOTE!

Original data refers to the pass-thru records of staff members (not including visitors). To sync pass-thru records of all persons including visitors, go to **Status Monitoring > History Records**.

1. Click Sync Original Data.
2. Select the time period for the data you want to sync.
3. (Optional) To sync the pass-thru snapshots to the client, select **Sync Snapshot**.
4. Select the target face recognition access control device(s).
5. Click **OK**.

9.4.2 Attendance Details

Attendance > Attendance Statistics > Attendance Details

View attendance details including attendance status and absence duration during a specified period. One record is generated for each person every day.

All the original data of a day will be generated at the automatic calculation time on the next day. If automatic calculation fails, or if any shifts have changed, you can select the department or person on the left-side organization list, set the start and end time, and then click **Calculate** to re-calculate attendance and generate attendance details.



NOTE!

When you calculate attendance for a certain day, if abnormal shifts are detected for this day, or if any shifts in this day are not yet started or ended, then attendance data of the relevant persons in this day will be deleted and will not be calculated.

You can search attendance statistics of a department or a person by setting search criteria including person ID, name, department, date, time, sign-in/out time.

Workday	Department	Person ID	Name	Shift Name	Work Hours	Sign In Time	Sign Out Time	Attendance Duration (min)		Attendance Status	Absent (min)	Remi
								Actual	Valid			
2022-03-15	dept	001	001	Default Shift	09:00-18:00	(~)	(~)	0	0	Absent	540	

The search results appear in the list. Click **Export** to export personnel attendance details.

9.4.3 Attendance Summary

Attendance > Attendance Statistics > Attendance Summary

View the total length of absence during a specified time period and the details. For example, the total length of late arrivals, leave early, and absence during one month.

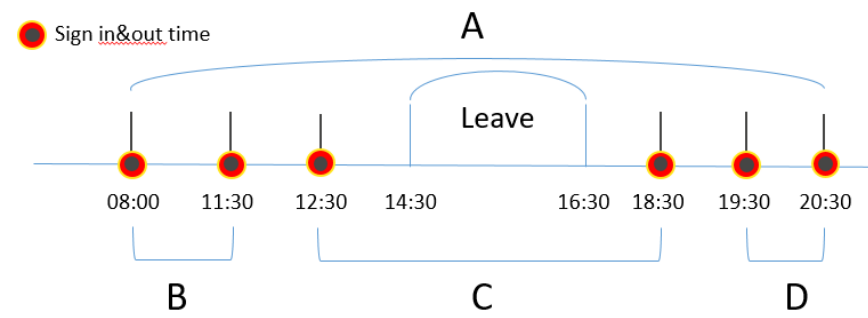
You can set search criteria to view personnel information of a specified department or personal information of a about a person, including person ID, name, department, attendance status and details.

Department	Person ID	Name	Late (min)	Leave Early (min)	Attendance Duration (min)		Absent (min)	Ask for Leave (min)	Attendance Details
					Actual	Valid			
dept	001	001	30	30	0	0	540	0	



NOTE!

The leave time will not be deducted from the flexible attendance duration or absence duration. See the figure below, if you select **Calculate by First Sign-in and Last Sign-Out**, the attendance duration is A; If **Cumulate Duration by Multiple Sign Ins&Outs**, the attendance duration is B+C+D. Absence duration is the specified daily attendance duration minus the actual attendance duration.



The search results appear in the list. Click **Export** to export personnel attendance summary.

Click  in the **Attendance Details** column to view detailed attendance information of the person.

View Details												×
Workday	Department	Person ID	Name	Shift Name	Work Hours	Sign In Time	Sign Out Time	Attendance Duration (min)		Attendance Status	Absent (min)	Remarks
								Actual	Valid			
2022/03/15	dept	001	001	Default Shift	09:00-18:00	(~)	(~)	0	0	Absent	540	


10 Status Monitoring

10.1 Realtime Monitoring









Status Monitoring > Realtime Monitoring

View real-time status of access control devices and pass-thru records.

Open Door Remotely
Refresh
Please enter keywords.



Door

Time	Device Name	Name	Personal ID	Department	Authentication	Card Number	Mask Status	Temperature(C)	Snapshot	Library Photo	Operation
2022-08-29 10:56	Door				Face		Unknown	-			
2022-08-29 10:56	Door				Face		Unknown	-			
2022-08-29 10:56	Door				Face		Unknown	-			
2022-08-29 10:56	Door				Face		Unknown	-			

Open door remotely

Select a device you want to open in the device list, click **Open Door Remotely** to open the door.



NOTE!

This function is only available to face recognition access control devices.

View realtime pass-thru records

- Select an online device to view the last 20 pass-thru records of the selected device.
- If you do not select any device, you can view the last 20 pass-thru records of all devices in the device list.

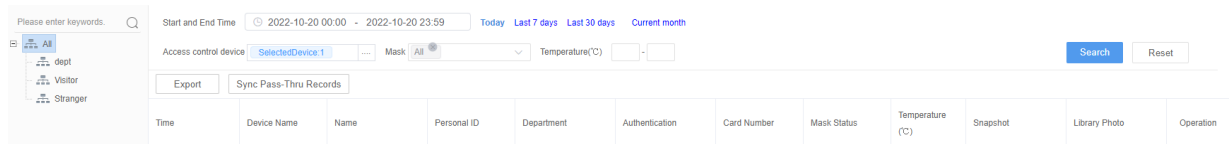
Click  in the **Operation** column to view the pass-thru details.

10.2 History Records

Status Monitoring > History Records

View historical pass-through records.


Select a department you want to search in the organization list on the left. Set the face recognition access control devices or doors under access controllers, date, mask wearing status and body temperature. Click **Search**, then the search results will be displayed.



- Sync Pass-Thru Records

Sync pass-thru records reported by face recognition access control devices from the NVR to the client. You need to configure the NVR first in [NVR configuration](#).

- (1) Click **Sync Pass-Thru Records**.
- (2) Select the time period for the data you want to sync.
- (3) (Optional) To sync the pass-thru snapshots to the client, select **Sync Snapshot**.
- (4) Select the target face recognition access control device(s).
- (5) Click **OK**.

- To view detailed information about a record, click  in the **Operation** column.
- To export search results, click **Export**.

11 System Configuration

11.1 Snapshots

Set a path for saving snapshots. The PC's disk storage status is displayed. Choose a disk with sufficient space. Snapshots will be saved to the specified path.

11.2 Alarm Parameter Configuration

1. Click System Configuration > Alarm Settings.
2. Configure alarm parameters. Parameters are described in the table below.

Parameter	Description
Temperature Unit	Choose Celsius or Fahrenheit as temperature unit.
Temperature Detection	Enable/disable temperature detection. When temperature detection is enabled,

Parameter	Description
	an alarm will be reported when the temperature measured exceeds the threshold.
Abnormal Temperature Threshold	Set a threshold for abnormal temperatures. An alarm will be reported when the temperature measured exceeds the threshold.
Mask Detection	Enable/disable mask detection. When mask detection is enabled, an alarm will be reported when a person not wearing a mask is detected.
Alarm Sound	When this feature is enabled, the alarm will sound when an abnormal temperature or a person not wearing a mask is detected. Please enable temperature detection or mask detection first.
Pop-up Alarm Window	When this feature is enabled, an alarm window will pop up when an abnormal temperature or a person not wearing a mask is detected. Please enable temperature detection or mask detection first.

3. Click **Save**.

11.3 Auto Time Sync

Click **Auto Time Sync** to synchronize the device time with the PC.

Turn on the auto time sync and set the interval, the system will sync time once automatically, and then sync time at set intervals automatically.

Auto Time Sync: On Off

Interval:

Save

11.4 Database Management

Enable **Scheduled Backup** or click **Backup** to back up data. Backing up or restoring data may affect client performance, it is recommended to perform backup and recovery when the client is idle.

Restore

Backup

Save Backup To:

Scheduled Backup: On Off

Start Backup On: Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

Start Backup At:

Message:

Previous Backup 20:07 02-23-2021

Next Backup 20:17 02-25-2021


Do not save the backup to the disk where the operating system is installed.

The backup is a copy of the data in the database.

A backup file is encrypted using the current user's password. This password is required when you use this backup file to restore data.

Save

Back up data

1. Click  to set the backup path. The backup files are saved in the EZAccess_config_DB folder. If this folder doesn't exist, it will be created automatically.
2. Back up data:
 - Scheduled backup: Perform scheduled backup according to user's configuration. This function is turned on by default, you can turn it off manually.
 - a) Enable **Scheduled Backup**.
 - b) Set backup date and time. The backup will run automatically on the set date and time on a weekly basis.
 - Manual backup: Click **Backup** to back up immediately.

Only the latest backup file is kept in the backup path.

Restore data

1. Click **Restore**.
2. Enter the file password to decrypt the backup file. Click **OK** to restore the latest backup data.

11.5 System Maintenance

Data migration can be used to quickly configure the client and restore data in some scenarios such as computer replacement and data sharing. Compared with backup and recovery, data migration can also restore face images and images for pass-through records.

Data Migration

Import

Export

Note: Import or export the database and images only.

Export data

1. Click **Export**.
2. Choose a path to save the exported data. The exported files are saved in the EZAccess_config_migration folder. If this folder doesn't exist, it will be created automatically.
3. Click **OK**.

The exported file is named Access_config_migration + *export time* (the export time includes year, month, day, hour, minute and second).

Import data

1. Click **Import**.
2. Choose a file and then enter the file password (the file password is the same as the client login password of the exported user).
3. Click **OK**.

11.6 NVR Configuration

Configure the NVR parameters so that you can sync pass-thru records reported by face recognition access control devices from the NVR to the client.



NOTE!

You need to add a face recognition access control device to the NVR first, and then set the record storage path of the face recognition access control device to the NVR so that it can upload pass-thru records to the NVR. For details, refer to the device user manual.

* IP:

* Port:

* Username:

* Password:

Status: Online

Enter the NVR's IP address, port number, username, and password, and then click **Save**.
When the status is online, it indicates the NVR is connected successfully.