

# Face Recognition Access Control Terminal User Manual II

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

## Disclaimer

No part of this manual may be copied, reproduced, translated, or distributed in any form or by any means without prior written consent from us.

The manual may be updated from time to time due to version upgrade or other reasons.

The manual is for reference only. All the statements, information, and suggestions contained herein do not constitute warranties of any kind, express or implied.

We shall not under any circumstances be liable for any special, consequential, incidental or indirect damages arising from the use of this manual or our product, including but not limited to any loss of commercial profits, losses caused by missing data or documents, and anomalies during product running or information leakage due to cyber attacks, hacker attacks, or virus attacks.

## Safety Precautions



---

### CAUTION!

The default password is used for your first login. To ensure account security, please change the password after your first login. You are recommended to set a strong password (no less than eight characters).

---

Before performing operations, be sure to carefully read through and observe safety specifications in this manual.

- Screenshots provided in this document are used as examples only and the UI layout varies with versions.
- This manual applies to multiple models but the models are not completely listed herein. Refer to actual products while reading this manual.
- We reserve the right to modify the content in this manual without prior notice or prompt, but we do not ensure that this manual is completely error-free.
- Subject to uncertain factors such as the physical environment, actual values of data may differ from the reference values described here. In case of any question or dispute, the right of final interpretation resides with us.
- Follow operation instructions in this manual when using the product. We are not responsible for problems caused by the violation of the instructions. Thank you for your cooperation.

## Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.




## Conventions

- The figures, charts or photos in this manual are used for illustration only, which may differ from the actual product.
- This manual applies to multiple models but the models are not completely listed herein. Refer to actual products while reading this manual.

- Subject to uncertain factors such as the physical environment, actual values of some data may differ from the reference values described here. In case of any question or dispute, the right of final interpretation resides with us.
- Follow this manual when using the product. Professional guidance is recommended.
- Notational conventions used in this document are described as follows:

Format	Description
<b>Boldface</b>	Indicates buttons, menus, tabs, window names, dialog names, and parameter names. For example, click <b>OK</b> or select <b>Device Management</b> .
" "	Indicates messages. For example, "Hanging Up" is displayed on the interface.
>	Directs you to go to a multi-level menu. For example, go to <b>Device Management &gt; Add Device</b> . In this example, <b>Add Device</b> is a submenu under <b>Device Management</b> .

- 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
 <b>WARNING!</b>	Contains important safety instructions and indicates situations that could cause bodily injury.
 <b>CAUTION!</b>	Means reader is careful and improper operations may cause damage or malfunction to product.
 <b>NOTE!</b>	Means useful or supplemental information about the use of product.

# Contents

1 Application Scope of the Manual .....	1
2 Product Overview .....	1
3 Product Appearance .....	1
4 Product Installation .....	3
5 Local Operations.....	3
5.1 Initial Interface .....	3
5.2 Main Interface .....	4
5.3 Ad Mode .....	5
5.4 Mask/Temperature Measurement Interface .....	5
5.5 Activation Config .....	10
5.5.1 Basic Info.....	11
5.5.2 Device Location .....	12
5.5.3 Network Setting.....	12
5.5.4 User Management.....	12
5.5.5 Activation Password.....	15
5.5.6 Admin Password .....	16
5.5.7 Authentication Scene .....	16
5.5.8 Volume.....	18
5.5.9 Device Maintenance.....	18
5.5.10 Data Management .....	19
6 Personnel Management .....	20
6.1 Personnel Information Input.....	20
6.2 Personnel Deletion.....	20
7 Web Operations .....	20
7.1 Login .....	20
7.1.1 Preparation .....	20
7.1.2 Logging In to the Web Interface .....	22
7.2 Photo .....	24
7.2.1 Photo List Sorting .....	24
7.2.2 Total Capacity/Available Capacity .....	24
7.2.3 Photo Naming Rules.....	24
7.2.4 Refreshing the Photo Library.....	25
7.2.5 Exporting Records .....	25

7.2.6 Exporting Photos.....	25
7.2.7 Deleting a Photo .....	25
7.2.8 Exporting and Deleting Photos .....	26
7.3 Parameter Configuration .....	26
7.3.1 Common .....	26
7.3.2 Network.....	43
7.3.3 Image.....	44
7.3.4 Intelligent.....	54
7.3.5 Events .....	71
7.3.6 Storage.....	75
7.3.7 Security .....	77
7.3.8 System .....	79
8 FAQs .....	82

# 1 Application Scope of the Manual

Table 1-1 Application Scope of the Manual

Model	Name
OET-213H-NB	Face Recognition Access Control Terminal
OET-523L-NB	Face Recognition Terminal

## 2 Product Overview

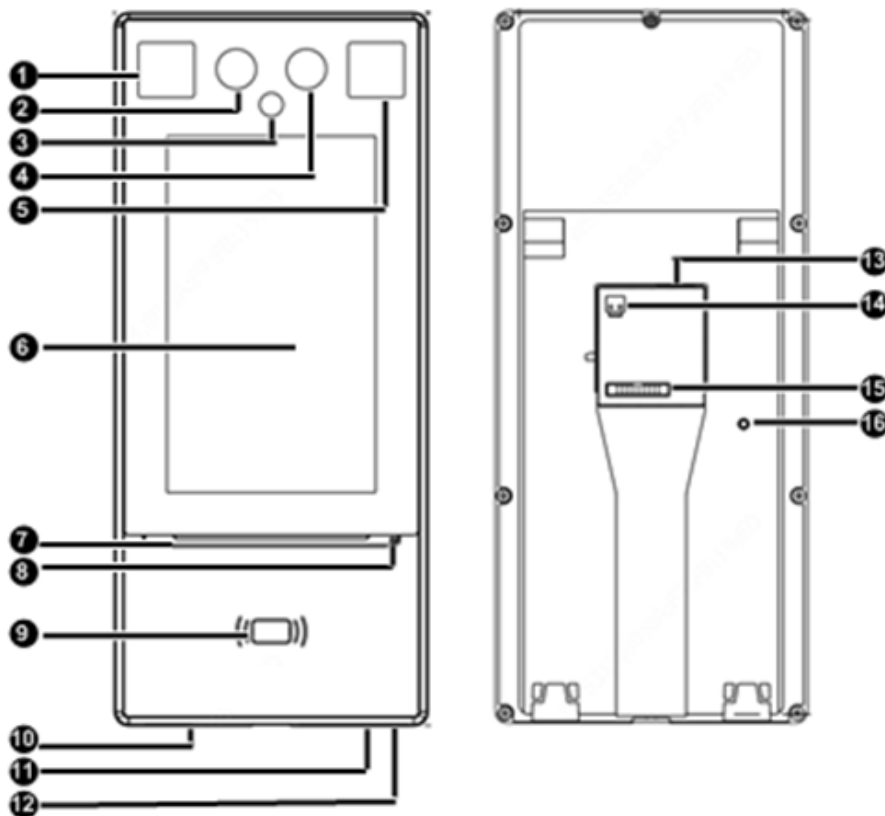
Face recognition access control terminal ("the face recognition terminal" for short) is a face recognition access control product featuring high performance and high reliability. The face recognition technology is perfectly integrated into the access control device, which relies on deep learning algorithm, to support face authentication to open the door and achieve precise control of human. And it can be widely applied to the scenarios of building systems, such as smart communities, public security, parks and other important areas.

## 3 Product Appearance

The figure below shows the structure of the device. The actual device shall prevail.

- OET-213H-NB

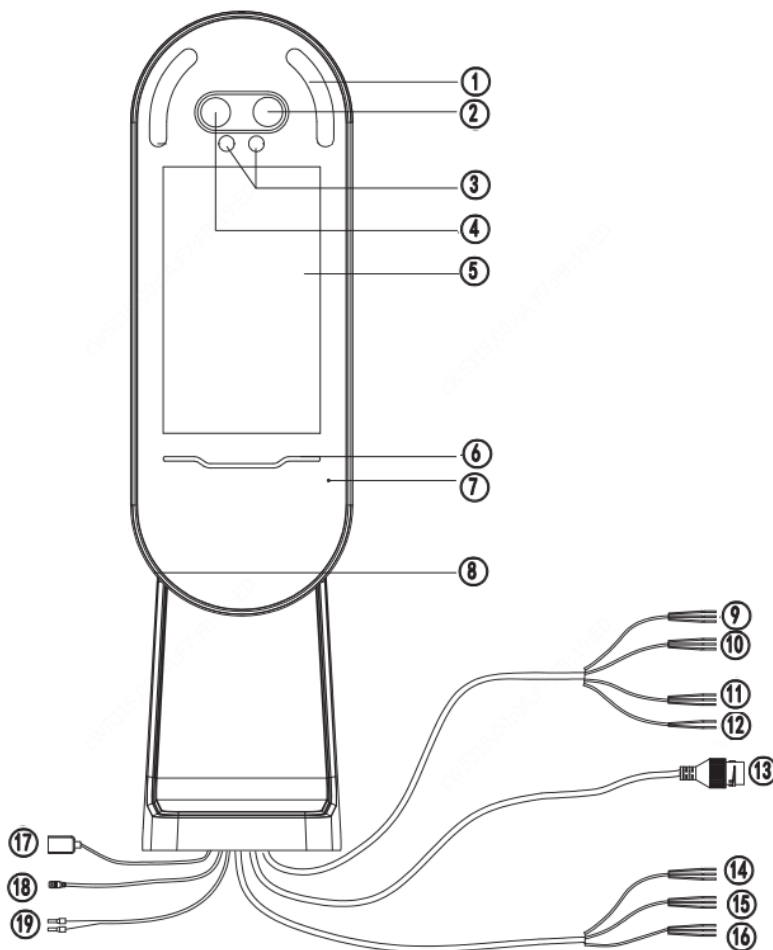
Figure 3-1 Device Structure



1. Light supplement lamp 1	2. Camera 1
3. Infrared light supplement lamp	4. Camera 2
5. Light supplement lamp 2	6. Display screen
7. Pass-through indicator	8. Microphone
9. Card reading area	10. Loudspeaker
11. Reboot	12. USB2.0
13. Network interface	14. Power input (DC 12V±25%)
15. 20-pin interface	16. Tamper proof button

- OET-523L-NB

Figure 3-2 Device Structure



1. Light supplement lampx2	2. Camera 1
3. Infrared light supplement lamp	4. Camera 2
5. Display screen	6. Pass-through indicator
7. Microphone	8. Loudspeaker
9. WIEGAND_OUT	10. WIEGAND_IN
11. RS232	12. RS485
13. Network interface	14. ALARM_IN
15. IO-1	16. IO-2

17. USB	18. Power output (DC 5V)
19. Power input (DC 12V±25%)	

## 4 Product Installation

- Installation of OET-213H-NB

For the wiring and installation of the device, refer to the *Face Recognition Access Control Terminal Quick Guide*.

- Installation of OET-523L-NB

For the wiring and installation of the device, refer to the *Face Recognition Terminal Quick Guide*.

## 5 Local Operations

### 5.1 Initial Interface

When the face recognition terminal is used for the first time or the factory defaults are restored, users need to set the activation password, which is used to log in to the [Activation Config](#) interface.



#### NOTE!

- The password must contain at least eight characters (including at least two of the following types: upper case letters, lower case letters, digits, underscores, and hyphens).
- The activation password is consistent with the password for the **admin** to log in to the Web interface. If the activation password is changed, use the new password to [Logging In to the Web Interface](#)

After the activation password is configured, the [Figure 5-2](#) is displayed. If the activation password needs to be changed later, refer to [Activation Password](#) to change the password.

Figure 5-1 Activation Password Configuration Interface

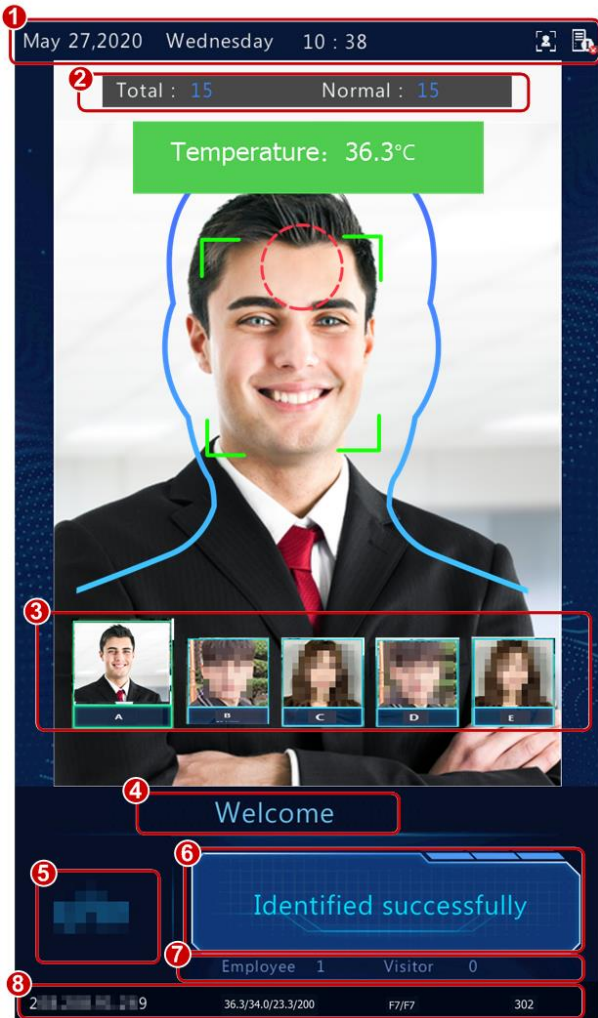
The screenshot shows a web interface with a light blue background and a grid pattern. At the top, it says 'Welcome' in blue. Below that, it says 'Please set an activation password first.' There are three input fields: the first one has 'admin' entered, the second one is empty, and the third one is empty. At the bottom, there is a blue button with the text 'OK'.






## 5.2 Main Interface

The main interface displayed on the face recognition terminal varies with the device type. See [Device Info](#).

Figure 5-2 Main Interface



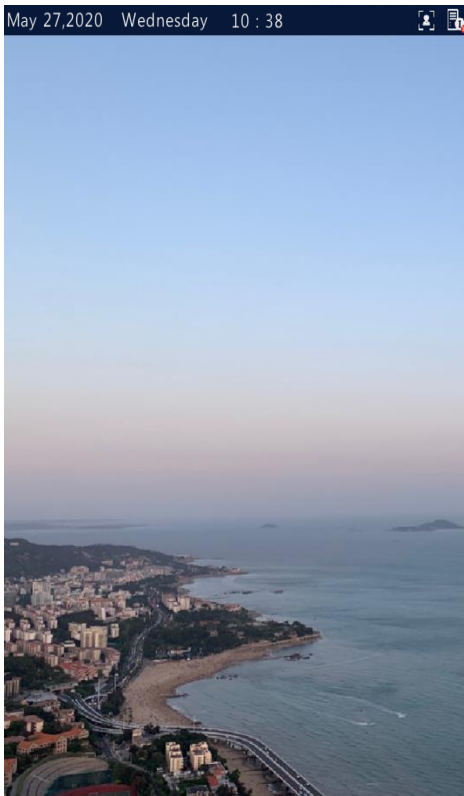
No.	Description
1	<p>Displays the current date, time, and connection status of different services.</p>  indicates the following items from left to right: <ul style="list-style-type: none"> <li>• Whether to enable the face scan mode</li> <li>• Whether server 1 is online</li> </ul> <p> <b>NOTE!</b></p> <p>An icon marked with  indicates "No".</p>
2	<ul style="list-style-type: none"> <li>• Total: total number of detected people.</li> <li>• Normal: Number of people with normal temperature</li> </ul> <p>This interface is only displayed when the temperature measurement function is enabled. For detailed operation description, see <a href="#">Advanced Setting</a>.</p>
3	<p>Displays the photo and name of an identified person in the library. Refer to <a href="#">Recognition Result Display</a> to enable the face recognition terminal to display one or more registered face pictures.</p> <p>When <b>Multiple Faces</b> is selected, information about the latest person identified successfully, is displayed on the left of the screen. The interface can display information about five recent persons identified successfully at most.</p>

No.	Description
4	Title bar, which can be defined by users. For detailed operations, see <a href="#">Custom Logo and Prompt</a>
5	Logo bar, which can be defined by users. For detailed operations, see <a href="#">Custom Logo and Prompt</a>
6	Displays the identification result (such as identified successfully or unregistered person), authentication mode (such as face scan or card swiping), and other information.
7	Displays the number of people in the employee library and that in the visitor library.
8	Status bar at the bottom Displays the device IP address, temperature, temperature collection time, temperature measurement module software and hardware version information and match time.

### 5.3 Ad Mode

The face recognition terminal supports ads (three pictures at most). For the ad configuration, see [Ad Mode](#).

Figure 5-3 Ad Interface



In ad mode, the system does not exit the ad mode if a person passes the authentication (via face scan or card swiping). If a person fails the face scan or taps the screen, the system exits the ad mode and the face recognition terminal displays the [Main Interface](#).

### 5.4 Mask/Temperature Measurement Interface

In response to the current epidemic, companies, parks, and communities take temperatures and check mask wearing for people passing through the entrances and exits. The work is performed by people manually, which is exhausting and increases the risk of cross-infection. The face recognition access control terminal is capable of checking whether people are wearing masks and taking their temperatures (an intelligent digital detection module is required, and either the forehead temperature or wrist temperature can be taken). For people with abnormal

temperature (exceeding the preset maximum temperature threshold) or without masks, the face recognition access control terminal displays an alarm on the GUI, plays a warning sound. And determines whether to open the door based on actual application scenes, thereby achieving epidemic prevention and control. For detailed configuration, see [Advanced Setting](#) and [Authentication Scene](#).



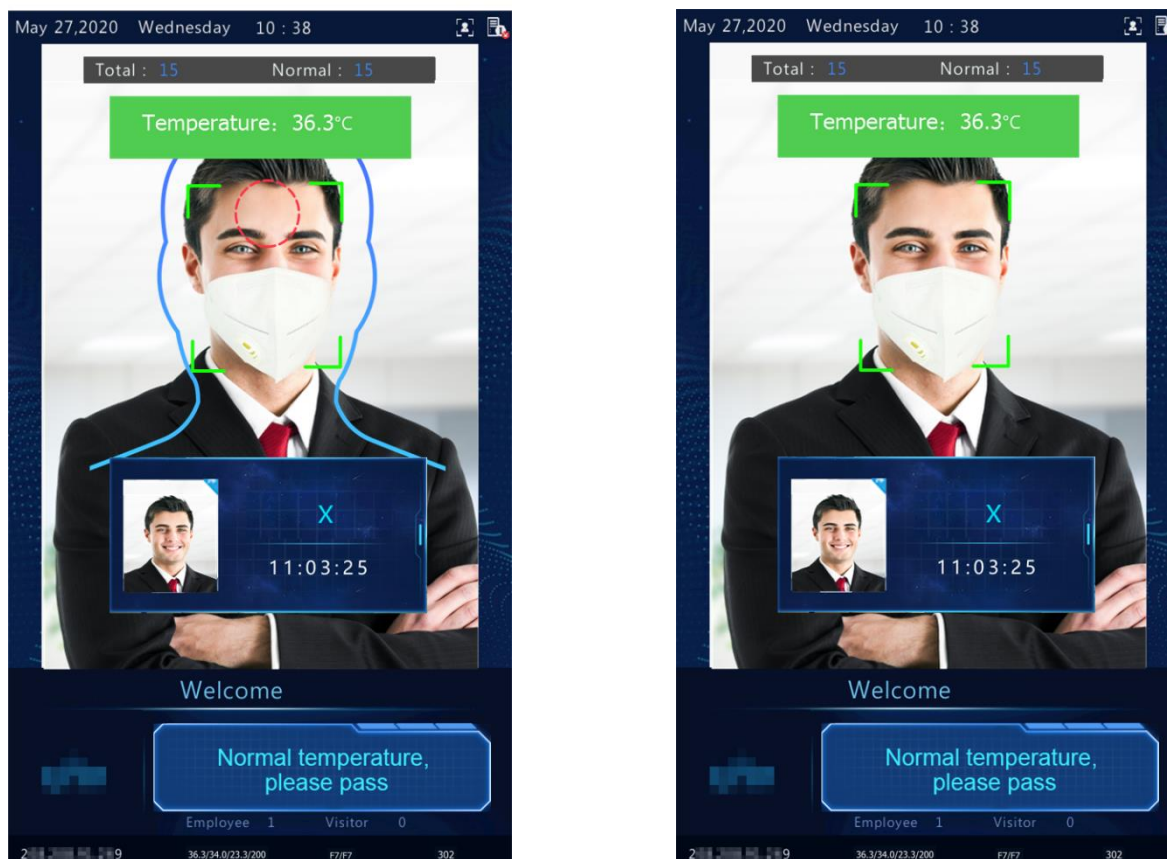
**NOTE!**

- When the temperature measurement function is enabled to take the forehead temperature, a person needs to get close to occupy the human shape on the screen and aim the forehead center at the red circle, as shown in [Figure 5-4](#). When the wrist temperature needs to be taken, a person needs to aim the wrist at the temperature-measuring point of the digital detection module.
- Ensure that the forehead or wrist is at a proper distance from the intelligent digital detection module. For OEP-BTM32-NB, the recommended distance is 0.5–0.7m. For OEP-BTS1-NB, the recommended distance is 1–2.5cm. For OEP-BTS1-BD-NB, the recommended distance is 1–4cm.
- When the forehead temperature needs to be taken, the forehead cannot be covered by fringes, hats, sunglasses, or other objects. When the wrist temperature needs to be taken, the wrist cannot be covered by sleeves, watches, bracelets, or other objects. Such objects, if any, need to be removed from the forehead or wrist 0.5 to 1 minute before the temperature can be taken.
- The temperature measurement function requires an intelligent digital detection module, which can be connected to the face recognition terminal through RS485. For the configuration, see [Serial Port](#).
- Do not use the temperature measurement function together with the safety helmet/safety module function.
- Face Recognition Access Control Terminal with intelligent digital detection module is not for medical use, rather for monitoring temperature for access controlling only.

**1. Mask detection and temperature measurement**

Enable both the mask detection and temperature measurement functions on the visual intercom face recognition terminal. When a person (whose information is stored in the library) passes through the terminal, the GUI displays the detection result.

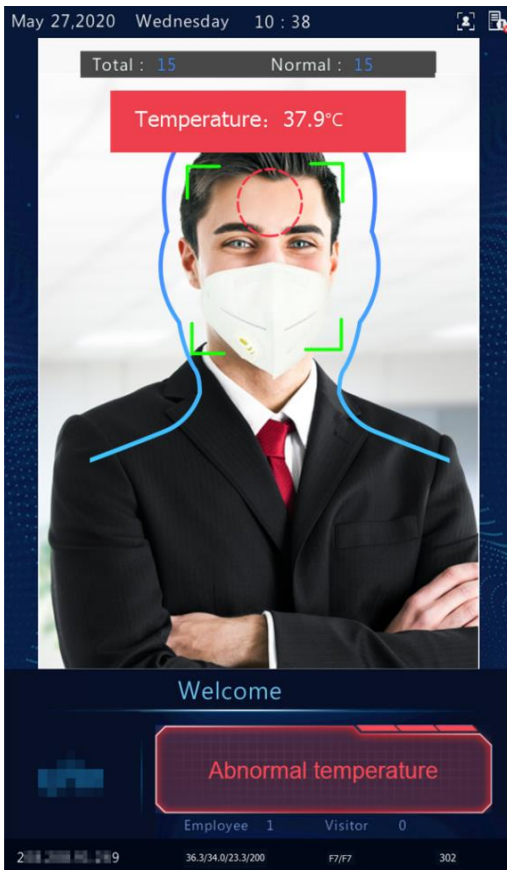
Figure 5-4 Normal Temperature and Mask Worn



### Measure Forehead Temperature

### Measure Wrist Temperature

Figure 5-5 Mask Worn but Abnormal Temperature



Measure Forehead Temperature

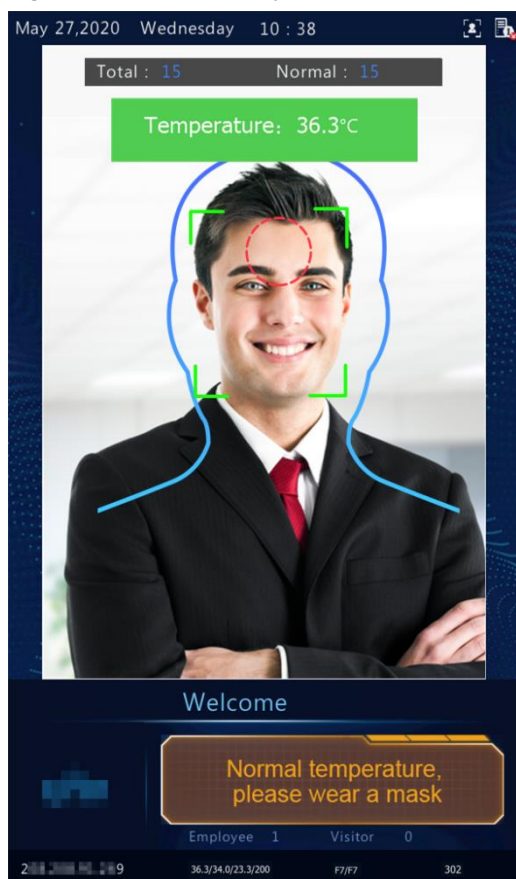
Measure Wrist Temperature



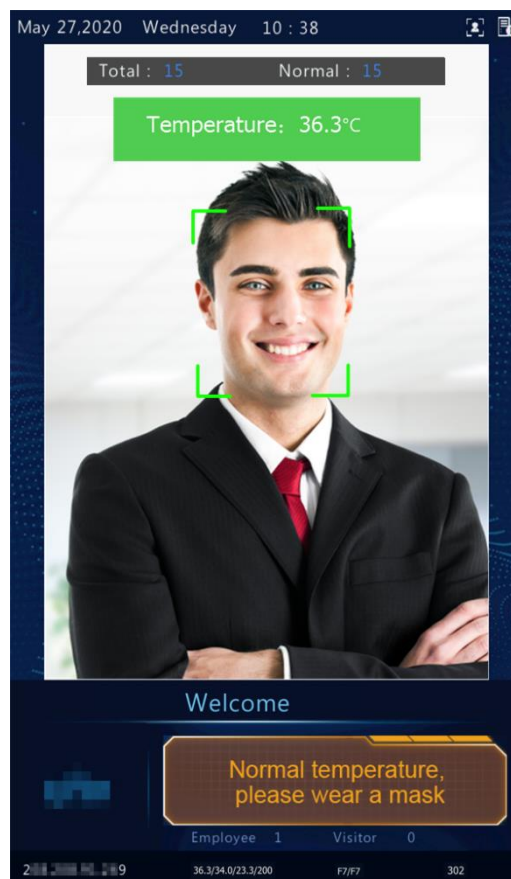
#### NOTE!

When both the temperature measurement and mask detection functions are enabled, temperature measurement is prior to mask detection. Once an abnormal temperature is detected, an "abnormal temperature" alarm is reported on the GUI and the warning sound is played no matter whether the person wears a mask.

Figure 5-6 Normal Temperature but Mask Unworn



Measure Forehead Temperature

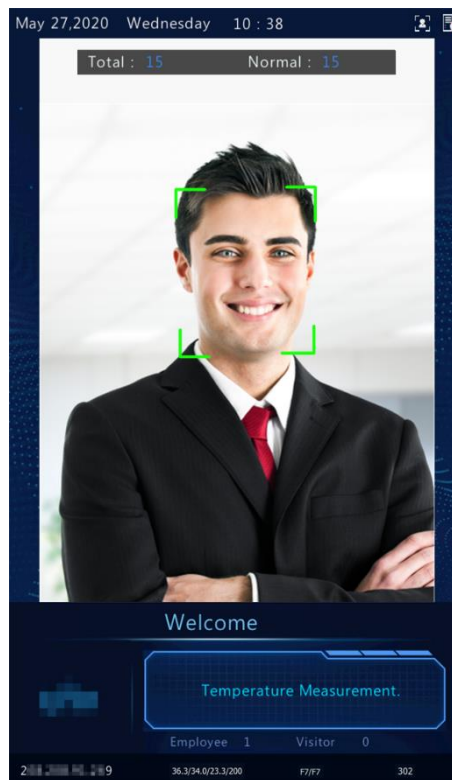
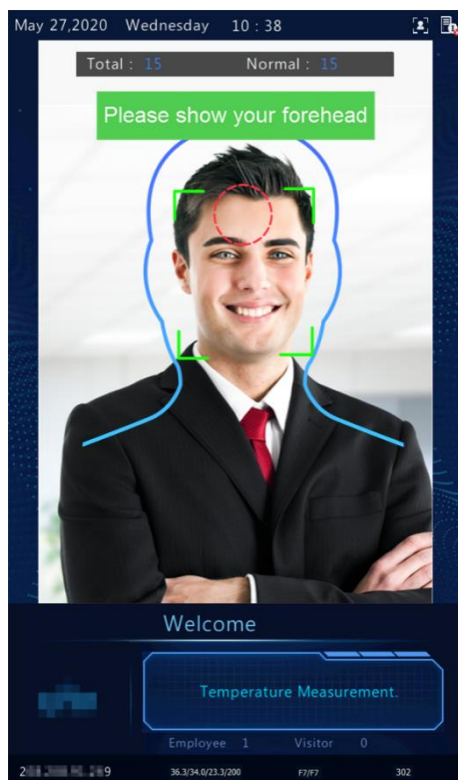


Measure Wrist Temperature

## 2. Temperature measurement mode

The visual intercom face recognition terminal supports pure temperature measurement mode, in which the temperature measurement function is enabled but no authentication mode is configured in the face library (for details, see [Face library management](#)). In this mode, the visual intercom face recognition terminal determines whether to open the door based on actual scenes for persons with abnormal temperature. For detailed configuration, see [Advanced Setting](#).

Figure 5-7 Temperature Measurement Mode



Measure Forehead Temperature

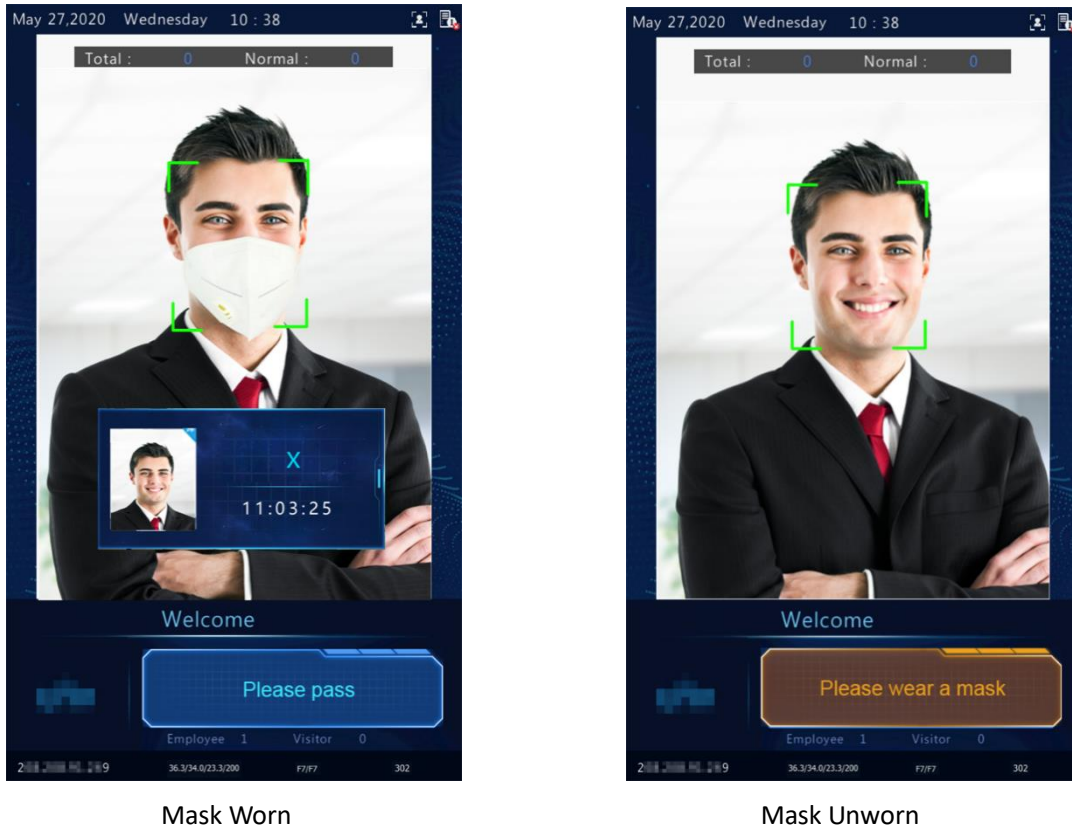
Measure Wrist Temperature

- Normal Temperature: The temperature of a detected person is normal. For the prompt on the GUI and voice prompt, see [Figure 5-4](#).
- Abnormal Temperature: The temperature of a detected person is abnormal. For the prompt on the GUI and voice prompt, see [Figure 5-5](#).

### 3. Mask detection

The visual intercom face recognition terminal supports mask detection. When a person (whose information is stored in the library) does not wear a mask, an alarm is reported on the GUI and a warning sound is played. For those who do not wear masks, the terminal determines whether to open the door based on actual scenes. For detailed configuration, see [Advanced Setting](#).

Figure 5-8 Mask detection



## 5.5 Activation Config

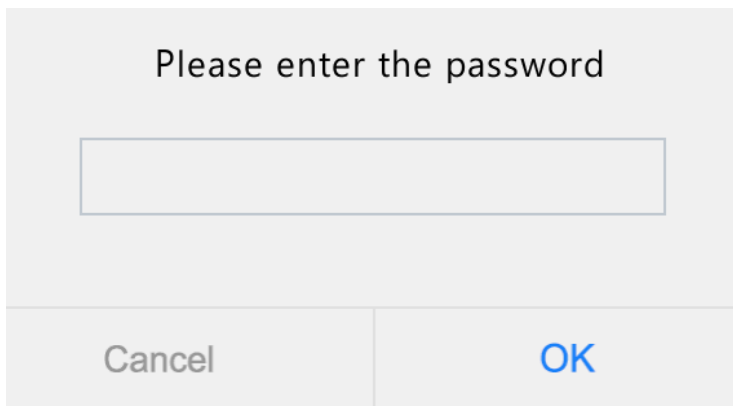
Hold down the main interface of the face recognition terminal for a long period of time (longer than 3s). In the displayed password input interface, enter the configured activation password to go to the **Activation Config** interface. If you forget the password, contact the local dealer to seek help.



**NOTE!**

The initial activation password is configured on the [initial interface](#). If it is changed (on the local device or on the Web interface), enter the new activation password.

Figure 5-9 Activation Password Input Interface



On the **Activation Config** interface, you can view basic information about the face recognition terminal, configure the device location, network, and password, input personnel information, and authentication scene.



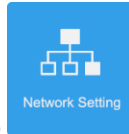


### 5.5.2 Device Location

The configuration is not supported.

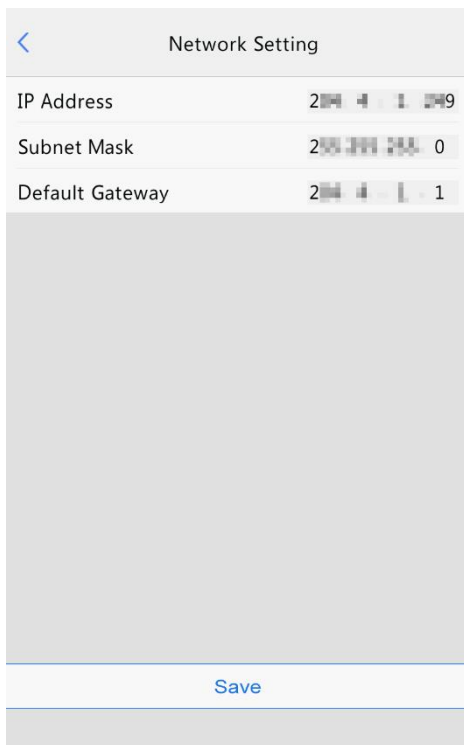
### 5.5.3 Network Setting

On the **Network Setting** interface, you can modify the device IP address and other communication parameters so that the device can communicate with external devices.



(1) On the **Activation Config** interface, tap  to go to the **Network Setting** interface.

Figure 5-12 Network Setting Interface



(2) Set network parameters by referring to the table below.

Table 5-1 Parameter Description

Parameter	Description
IP Address	Enter the IP address of the device. The IP address of the device must be unique across the network.
Subnet Mask	Enter the subnet mask of the device.
Default Gateway	Enter the default gateway of the device.

(3) Tap **Save** to complete network setting.

### 5.5.4 User Management

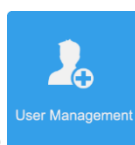
The face recognition terminal allows you to input personnel information. Personnel whose information has been input to the device successfully can swipe cards or credentials, or have their faces scanned for access.

## 1. Face photo collection requirements

When adding a person to the whitelist, collect the face photo by strictly observing the following requirements:

- General requirement: bareheaded full-face photo. Only the face photo of the person under collection is displayed on the screen of the terminal during collection and face photos of other people cannot be contained.
- Range requirement: The photo should show the outline of a person's both ears and cover the range from the top of the head (including all hair) to the bottom of the neck.
- Position requirement: The face must be positioned within the limit box on the interface of the terminal during collection.
- Makeup requirement: There should be no cosmetic color that affects the true appearance during collection, such as eyebrow makeup and eyelash makeup.
- Background requirement: The white, blue, or other pure color background is acceptable.
- Light requirement: Light with appropriate brightness is required during collection. Too dark photos, too bright photos, and light- and dark-colored face photos should be avoided.

## 2. Personnel information input operation process



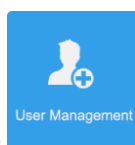
- (1) On the **Activation Config** interface, tap  to go to the **User Management** interface.

Figure 5-13 User Management Interface

A screenshot of a mobile application interface titled "User Management". At the top left is a back arrow. Below the title are several input fields: "Name" (text input), "Face Library" (dropdown menu showing "DefaultEmployeeLib"), and "Card No." (text input). Below these is a "Face Picture" section with a "0/1" indicator and a large grey square containing a white plus sign. At the bottom of the form is a blue "Save" button.

- (2) Configure personnel information input by referring to the table below.


Table 5-2 Parameter Description

Parameter	Description	Remarks
Name	Mandatory. Enter the name of a person.	/
Face Library	Choose the face library. You can configure and manage the face library through the Web	/

Parameter	Description	Remarks
	interface. See <a href="#">Face Library</a> for details.	
Card No.	Enter the card No. of the person. After successful input, the person can swipe the card for access.	At least one of the parameters needs to be set so that personnel information can be input successfully.
Face Picture	Collect and input face photos by referring to the <a href="#">Face photo collection requirements</a> . After successful input, the person can have the face scanned for access.	

(3) Perform the following operations to collect and input a person's face photo.

a Follow the prompt on the interface and ask the person to face the camera.

b When the photo displayed on the GUI meets [Face photo collection requirements](#), tap  to collect the face snapshot. See the figure below.


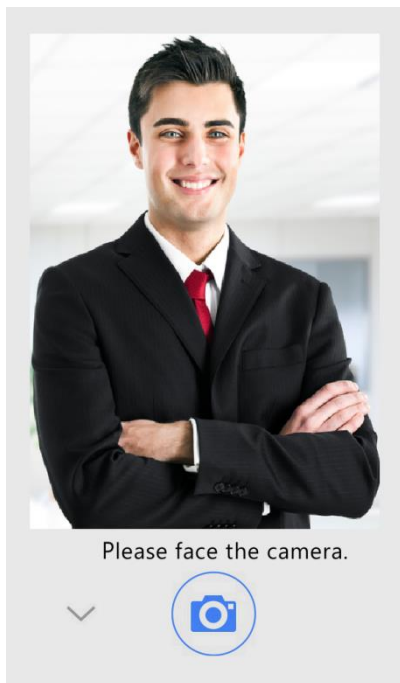

 is the back button.

Figure 5-14 Collecting and Inputting a Face Photo



c On the photo confirmation interface, tap  to confirm the collected photo.


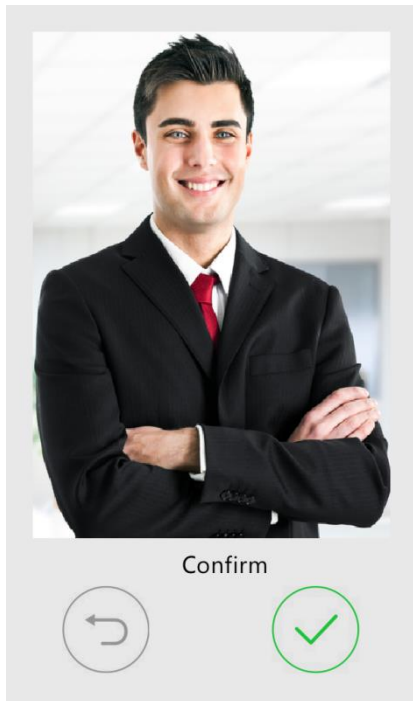
 is the back button.

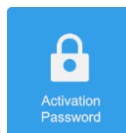
Figure 5-15 Photo Confirmation Interface



(4) On the **User Management** interface, tap **Save** to complete the personnel information input.

### 5.5.5 Activation Password

To change the configured activation password, do as follows:



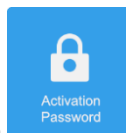
(1) On the **Activation Config** interface, tap  to go to the **Activation Password** interface.

Figure 5-16 Activation Password Interface

A screenshot of the "Activation Password" interface. It has a grey background and a white title bar with a back arrow and the text "Activation Password". Below the title bar are three input fields: "Old Password", "New Password", and "Confirm". A tip is displayed below the "Old Password" field: "Tip: Please enter an 8-character password. At least two from the following are required: uppercase letter(A-Z), lowercase letter(a-z), digit(0-9), underscore(\_) and hyphen(-).". At the bottom of the interface is a blue "Save" button.

(2) Enter the old password, new password, and confirm the new password as required.



**NOTE!**

- The password must contain at least eight characters (including at least two of the following types: upper case letters, lower case letters, digits, underscores, and hyphens).
- The confirmation password must be consistent with the new password.
- The activation password is consistent with the password for the **admin** to log in to the Web interface. If the activation password is changed, use the new password to log in to the Web interface.

(3) Tap **Save** to complete the activation password change.

### 5.5.6 Admin Password

On the Password-based Door Opening, users can enter an admin password to open the door. The admin password is applicable to device managerial personnel (such as people in the management center).

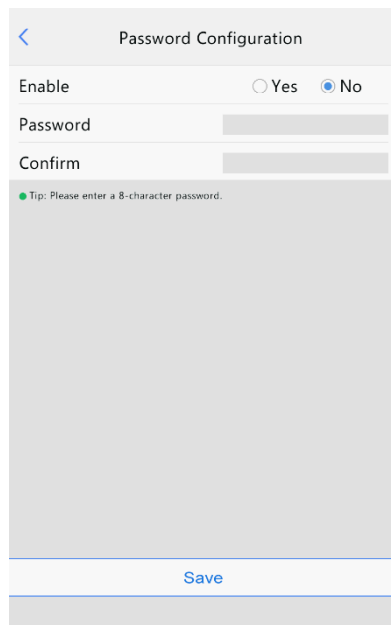
The admin password is disabled by default. If you need to enable the admin password, tap **Yes** and enter passwords in **Password** and **Confirm**.



**NOTE!**

- The password must be a string of eight characters.
- The confirmation password must be consistent with the password.

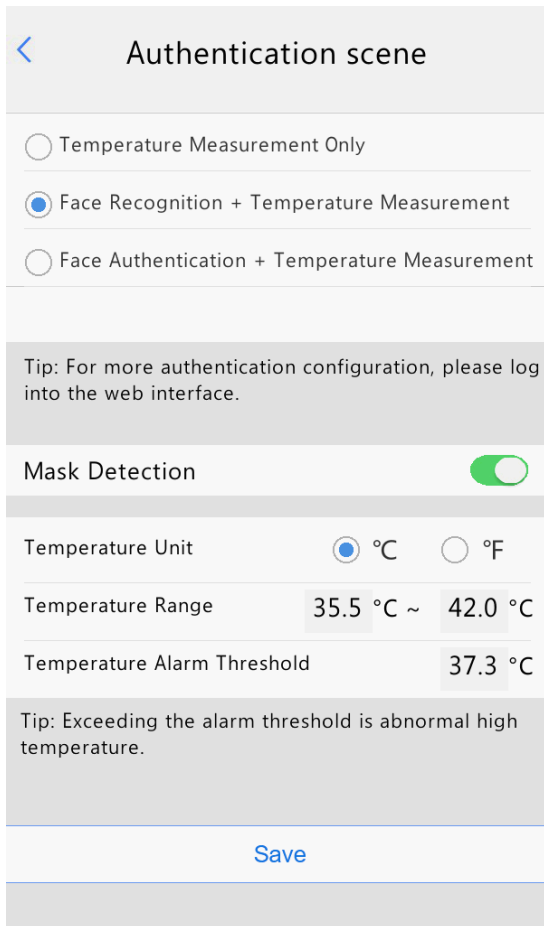
Figure 5-17 Admin Password Configuration Interface



### 5.5.7 Authentication Scene

This interface allows you to configure terminal authentication scenes, temperature measurement range, temperature alarm value, and other data. The table below describes detailed configuration.

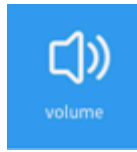
Figure 5-18 Authentication Scene Interface

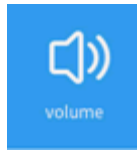


Parameter		Description
Authentication Scene	Temperature Measurement Only	The visual intercom face recognition terminal only measures people's temperatures and does not conduct other authentication. For the prompt on the GUI, see <a href="#">Temperature measurement mode</a> .  Note: In this scene, the authentication modes of all libraries configured in the visual intercom face recognition terminal will be cleared.
	Face Scan + Temperature Measurement	A person is allowed to pass only after the face authentication succeeds and the temperature is normal. For the prompt on the GUI, see <a href="#">Mask detection and temperature measurement</a> .
	Face Authentication + Temperature Measurement	The face whitelist mode + temperature measurement mode are adopted. A person (whose information is stored in the library) is allowed to pass only after the face authentication succeeds and the temperature is normal. For the prompt on the GUI, see <a href="#">Mask detection and temperature measurement</a> .  Note: This scene can be configured only when the default employee library exists under <a href="#">Face library management</a> .
Mask Detection		Enable or disable it based on actual conditions.
Temperature Configuration	Temperature Unit	The options are as follows: <ul style="list-style-type: none"> <li>• °C</li> <li>• °F</li> </ul> Set this parameter based on actual conditions.
	Temperature Measurement Range	Value range: [30–45]; default range: [35.5–42] Configure the range based on actual conditions.
	Temperature Alarm Threshold	When a temperature over the threshold configured here, the terminal will display a message “abnormal temperature” on the screen and play this

Parameter	Description
	message in audio. Value range: [30–45]; default value: 37.3

### 5.5.8 Volume

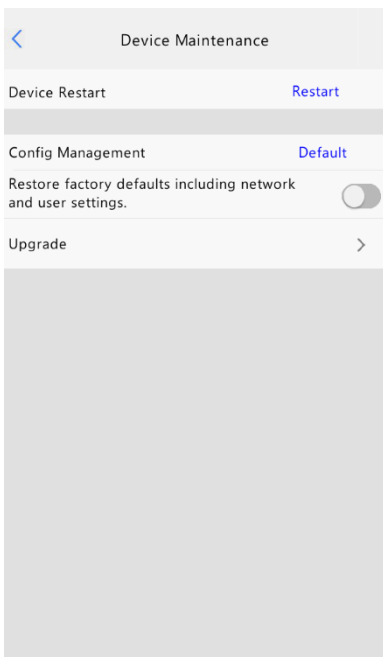




On the **Activation Config** interface, tap  to set the volume.

### 5.5.9 Device Maintenance

On the **Device Maintenance** interface, you can restart the visual intercom face recognition terminal and restore default configuration.

Figure 5-19 Device Maintenance Interface



- Restart: Tap **Restart**, on the displayed **Yes** interface, tap **Yes** to restart the device.
- Default
  - Tap **Default**, on the displayed **Yes** interface, tap **Yes** to restore default configuration.  
All parameters except network setting, system time, admin password and activation password will be restored default configuration.
  - First tap , then tap **Default**, on the displayed **Yes** interface, tap **Yes** to restore factory defaults.  
All parameters are stored factory defaults.
- Upgrade
  - a. Copy the upgrade package to the root directory of a USB flash drive. Only one upgrade package is allowed in the root directory.
  - b. Plug the USB flash drive into the terminal.
  - c. Click  to upgrade the terminal.

d. The terminal will automatically restart after the upgrade is completed.

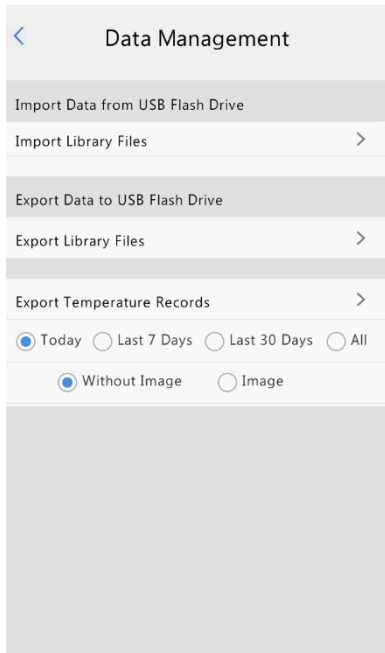



**NOTE!**

- The terminal only supports FAT32 USB drives with one partition.
- Local upgrade is also supported. See [Software Upgrade](#) for details.

### 5.5.10 Data Management

Figure 5-20 Data Management Interface





- Import library files from a USB flash drive
  - a. Save the library file to a USB flash drive.
  - b. Plug the USB drive into the terminal.
  - c. Click  to import the library file to the terminal.
  - d. The terminal will automatically restart and apply the new library after the import is completed.



**NOTE!**

The newly imported library will overwrite the original library in the device.

- Export library files to a USB flash drive
  - a. Plug a USB flash drive with enough free space into the terminal.
  - b. Click  to export the library file to the USB flash drive.
- Export temperature records to a USB flash drive
  - a. Plug a USB flash drive with enough free space into the terminal.
  - b. Select a time period of the records to be exported and whether to export snapshots.
  - c. Click  to export the temperature records to the USB flash drive.





---

**NOTE!**

- To export snapshots, go to **Setup > Intelligent > Face** and enable **Face Cutout**. See [Face](#) for details.
  - The exported temperature records are saved as a CSV file in the root directory of the USB flash drive.
  - The exported snapshots are saved to *Image/SnapPic\_Device IP/Export Time/*. You can also view the path of each snapshot in the CSV file.
- 

## 6 Personnel Management

---

### 6.1 Personnel Information Input

#### 1. Local input

The face recognition terminal allows you to input personnel information locally. For detailed operation, see [User Management](#).

#### 2. Input on the Web interface

You can import personnel information on the Web interface of the visual intercom face recognition terminal. For detailed operation, see [Personnel management](#).

#### 3. Input using the Guard Station software

You can import personnel information through Guard Station software. For detailed operations, see the online documentation in the software.

### 6.2 Personnel Deletion

#### 1. Deletion on the Web interface

You can delete personnel information on the Web interface of the visual intercom face recognition terminal. For detailed operation, see [Personnel management](#).

#### 2. Deletion using the Guard Station software

You can delete personnel information through Guard Station software. For detailed operations, see the online documentation in the software.

## 7 Web Operations

---

### 7.1 Login

#### 7.1.1 Preparation

Install the device by referring to the quick guide of the product (in the delivery accessories of the device). Connect the device to a power supply and start the device. You can manage and maintain the visual intercom face recognition terminal in a visualized manner on the Web browser.

The following uses Internet Explorer 10.0 running on Windows 7.0 as an example.

### 1. Check before login

- The network connection between the client PC and the face recognition terminal is in good condition.
- The PC is installed with Internet Explorer 10.0 or higher.
- (Optional) The resolution is set to 1440 x 900.

### 2. Add the IP address as a trusted site

Figure 7-1 Internet Setting

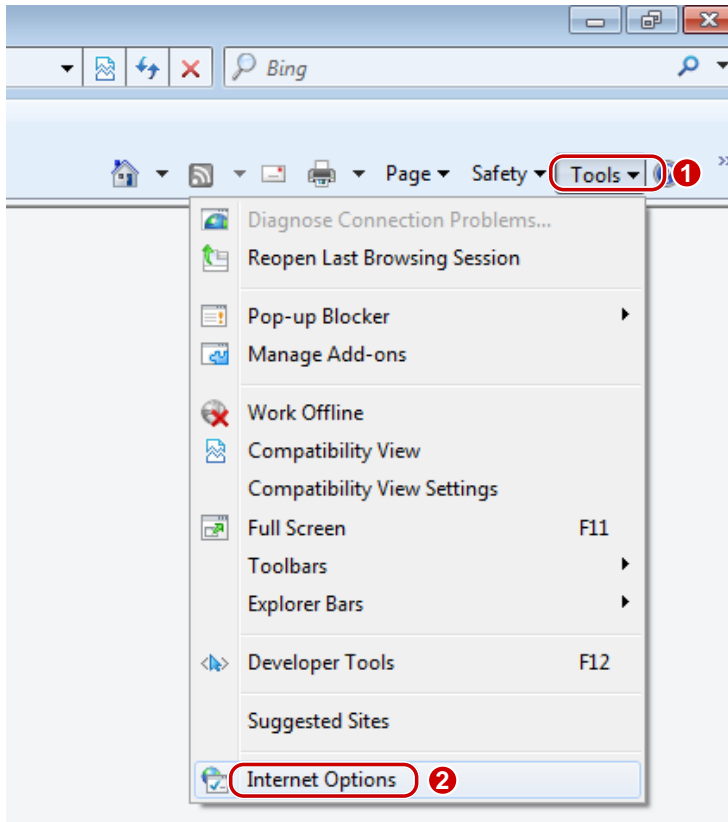
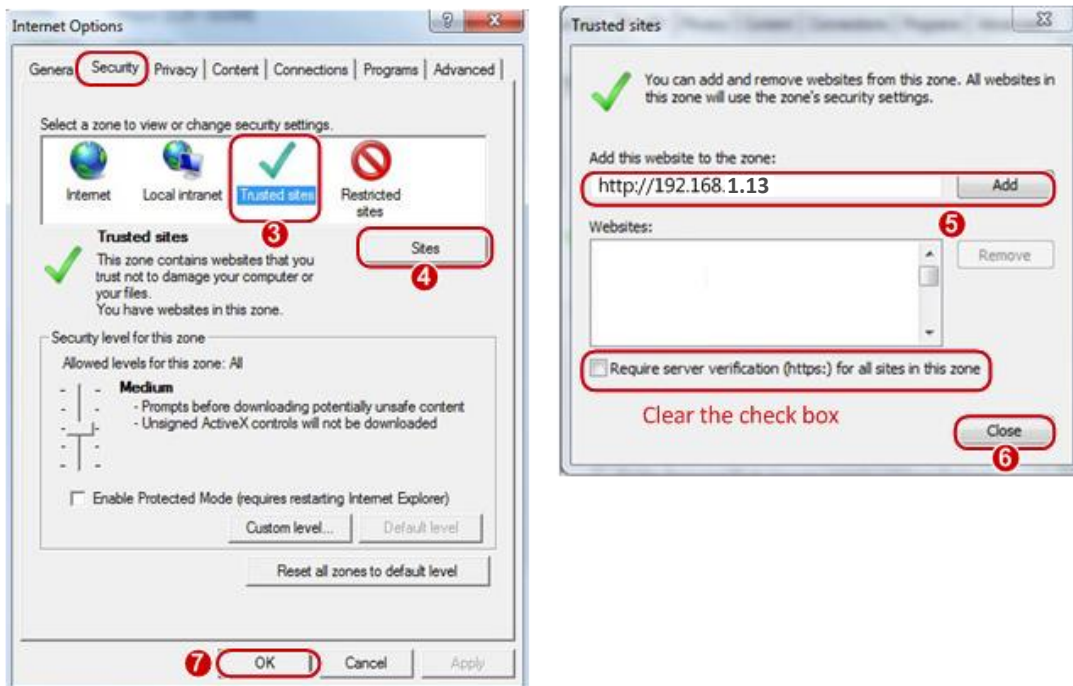


Figure 7-2 Adding the IP Address as a Trusted Site





## NOTE!

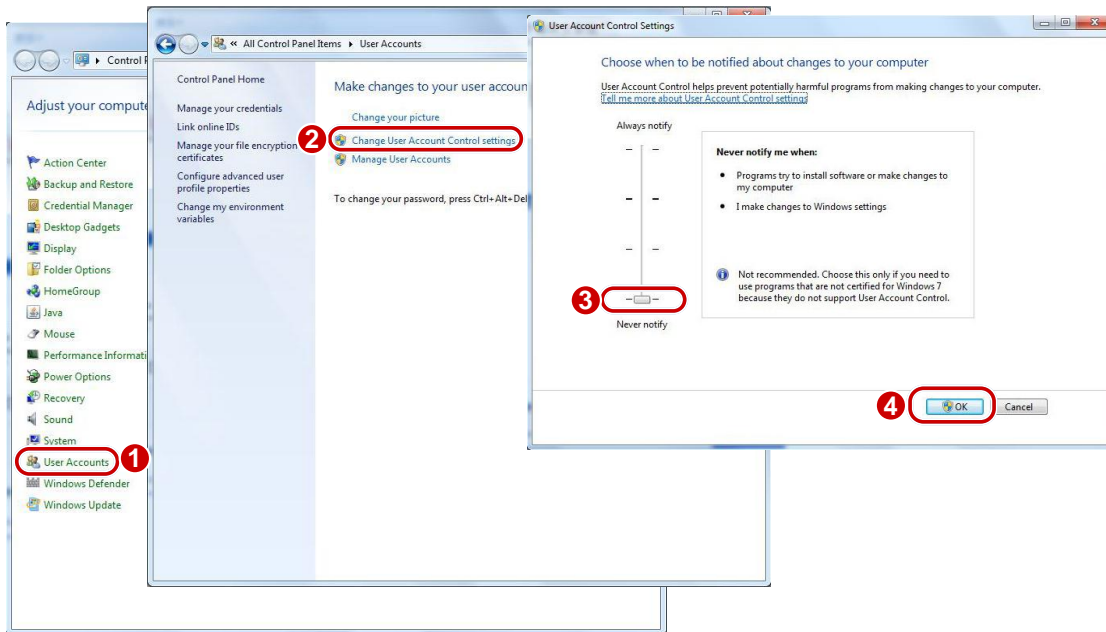
The IP address 192.168.1.13 in this example is the default IP address. Please replace it with the actual address of your face recognition terminal if it has been changed.

### 3. (Optional) Modify user access control settings

You are recommended to set the user control permission to minimum before accessing the device.

Choose **Start > Control Panel**. In the **Control Panel** window, follow the steps below to set the user control permission to minimum.

Figure 7-3 Setting the Control Permission



### 7.1.2 Logging In to the Web Interface

The default static IP address of the device is 192.168.1.13. The device also supports simple login using the IP address of 192.168.0.13 and subnet mask of 255.255.255.0.

The Dynamic Host Configuration Protocol (DHCP) is enabled on the device by default. If a DHCP server is used in the network, the IP address may be assigned dynamically. In this case, use the actual IP address for login. For operations to be performed when a dynamic IP address is assigned, click [Here](#) for a reference.

The steps of logging in to the Web interface (Internet Explorer 10 as an example) are as follows:

- (1) Enter the IP address in the address bar of the browser and press **Enter**.
- (2) A plug-in installation prompt as shown in the figure below is displayed when you log in to the Web interface for the first time. Follow instructions on the interface to complete the plug-in installation (all browsers need to be closed for the installation), restart the Internet Explorer, and log in to the system again.



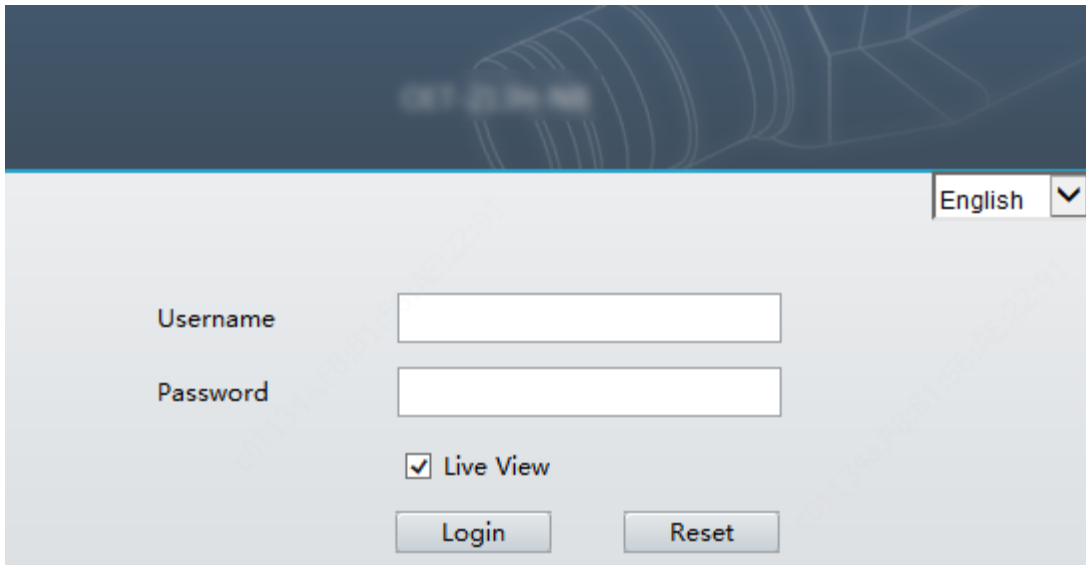


**NOTE!**

- To manually load the ActiveX, enter *http://IP address/ActiveX/Setup.exe* in the address bar and press **Enter**.
- The default password is used for your first login. To ensure account security, please change the password after your first login. You are recommended to set a strong password (no less than eight characters).
- The device protects itself from illegal access by limiting the number of failed login attempts. If login fails six times consecutively, the device locks automatically for five minutes.

(3) Enter the username and password, and then click **Login**.

Figure 7-4 Login Interface



The table below describes parameters and plug-ins on the interface and their configuration.

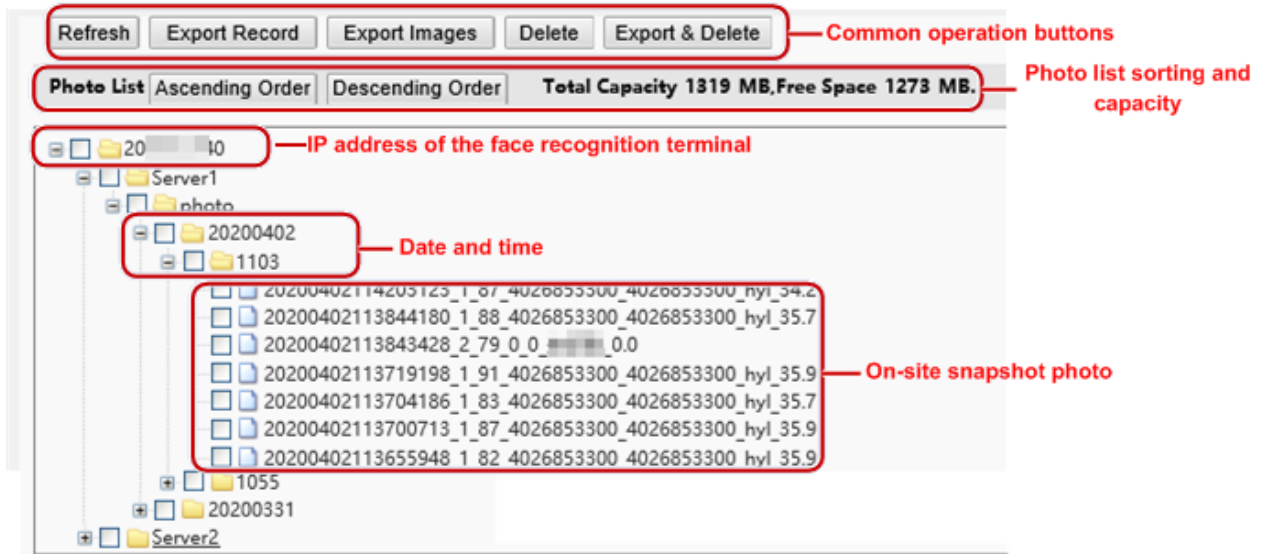
Table 7-1 Parameter Description

Parameter/Plug-in	Description	Remarks
Username/Password	Username and password for logging in to the Web interface. At initial login: The default username is <b>admin</b> and the default password is <b>123456</b> . The password for <b>admin</b> to log in to the Web interface is the same as the activation password. If the activation password has been changed, enter the new password here.	Enter the username and password based on the actual conditions.
Live View	<ul style="list-style-type: none"> <li>• If it is selected, live view videos are displayed on all live view screens after login to the Web interface.</li> <li>• If it is deselected, live view videos are displayed only after live view is enabled manually. For detailed operations.</li> </ul>	Set the parameter based on the actual conditions. It is selected in this example.
Reset	After <b>Reset</b> is clicked, the <b>Username</b> , <b>Password</b> , and <b>Save Password</b> boxes will be cleared. Other boxes such as the language and <b>Live View</b> will not be reset or cleared.	/

## 7.2 Photo

Face photos captured by the terminal are stored in the **Photo** menu bar. Click **Photo** in the menu bar. The current photo storage status is displayed.

Figure 7-5 Photo Information



### 7.2.1 Photo List Sorting

You can click **Ascending Order** or **Descending Order** to sort the photo list.

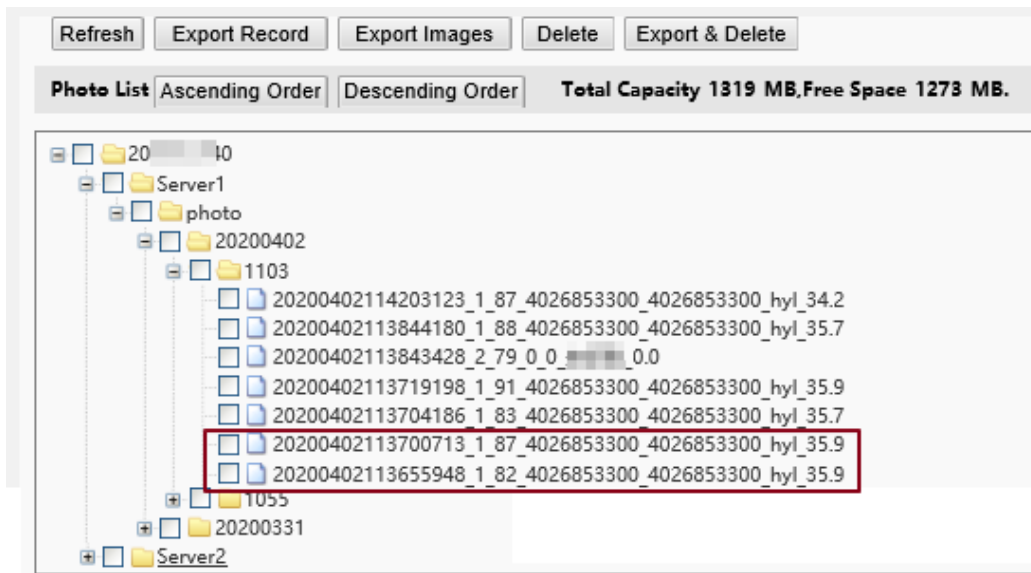
### 7.2.2 Total Capacity/Available Capacity

The total capacity and the available capacity of the local storage resource are displayed.

### 7.2.3 Photo Naming Rules

In the photo list, photos are named in a format as shown in the figure below for storage.

Figure 7-6 Photo Name



The naming rule is described as follows:

Snapshot time + match result code + highest similarity value (one value) + information about the person corresponding to the highest similarity (person ID + face ID + name) + detected temperature

Possible match results include the following:

- 1: authentication succeeded
- 2: authentication failed
- 3: authentication succeeded but not within arming time period
- 10: Abnormal temperature or mask unworn
- 21: person creation succeeded
- 22: person modification succeeded
- 23: face collection succeeded
- 24: invalid value

If a stranger is scanned, the match result shows "0\_0\_unidentified".

### 7.2.4 Refreshing the Photo Library

Click **Refresh** to refresh the stored content to the latest state.

### 7.2.5 Exporting Records

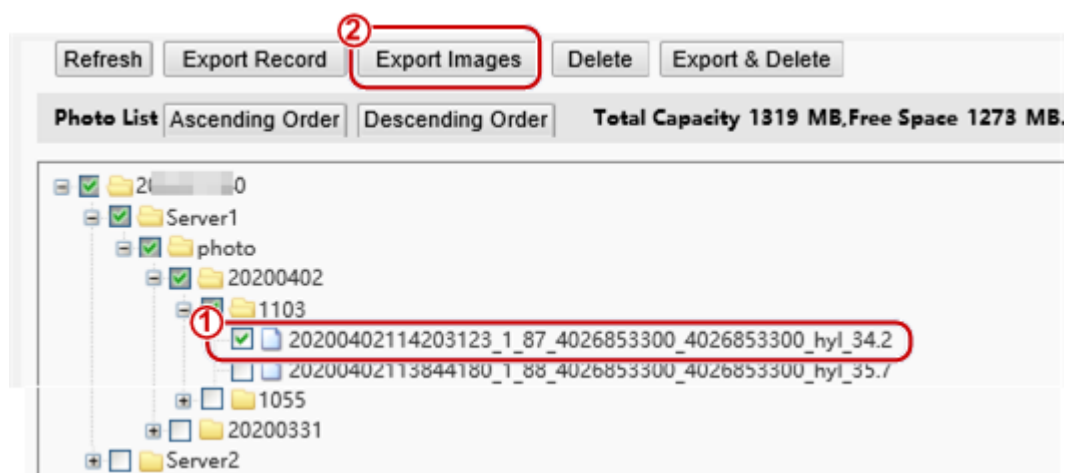
You can export some operation records from the database.

### 7.2.6 Exporting Photos

You can export all or some of the photos stored in the face recognition terminal.

- (1) Go to the **Photo List** interface.
- (2) Select photos to be exported.
- (3) Click **Export** and select the storage path to export the photos.

Figure 7-7 Export Operation Interface



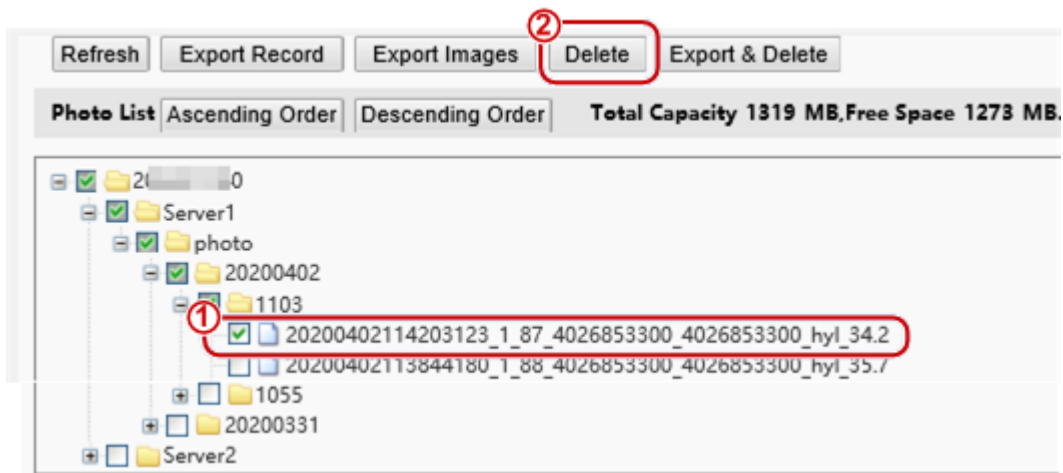
- (4) Access the folder that stores the exported photos to view the exported photos.

### 7.2.7 Deleting a Photo

- (1) Go to the **Photo List** interface.
- (2) Select a photo to be deleted.
- (3) Click **Delete**.

- (4) In the deletion confirmation box, click **OK** to complete the deletion operation.

Figure 7-8 Deletion Operation Interface

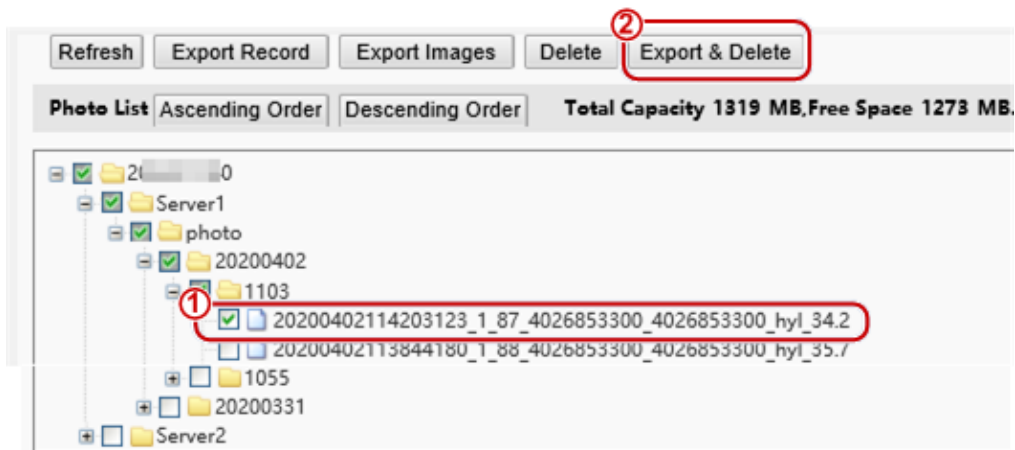


### 7.2.8 Exporting and Deleting Photos

When **Export & Delete** is clicked, selected photos will be exported and deleted from the face recognition terminal.

- (1) Go to the **Photo List** interface.
- (2) Select photos to be exported and deleted.
- (3) Click **Export & Delete**.
- (4) In the deletion confirmation box, click **OK**.

Figure 7-9 Export and Deletion Operation Interface



- (5) Select the path for storing the photos and click **OK** to complete the export and deletion operation.

## 7.3 Parameter Configuration

### 7.3.1 Common

#### 1. Basic Info

- Basic Info

The **Basic Info** interface allows you to view the status of the current device in real time, so as to rapidly know about the device condition and better maintain the device.

- (1) Choose **Setup > Common > Basic Info** and click the **Basic Info** tab.

Figure 7-10 Basic Info Interface

Basic Info	
Model	OET-XXXX-NB
Firmware Version	XXXX-XXXX-XXXX-XXXX-XXXX
Hardware Version	A
Boot Version	V1.15
Serial No.	XXXXXXXXXXXXXXXXXXXX
Network	XXXX.XXXXX.XXXXX.XXXXX
MAC Address	00:41:52:73:94:15
Status	
System Time	2020/7/31 10:33:01
Operation Time	0 Day(s) 0 Hour(s) 2 Minute(s)
Refresh	

(2) Click **Refresh** to update the device to the latest state.

On the refreshed interface, you can view status information about the current device.

- External Device

External device interface can view related information of temperature measurement module.

Choose **Setup > Common > Basic Info** and click the **External Device** tab.

Figure 7-11 External Device

Basic Info		External Device
Temperature Measurement Module		
Model	2	
Firmware Version	F7	
Hardware Version	F7	



**NOTE!**

Only if Fireware Version and Hardware Version information are consistent, the temperature measurement function can be used normally.

**2. Local Settings**

Set local parameters for your PC.



- (1) Choose Setup > Common > Local Settings to go to the Local Settings interface.
- (2) The figure below shows the **Local Settings** interface. Modify parameters based on actual requirements by referring to the table below.

Figure 7-12 Local Settings Interface

The screenshot shows the 'Local Settings' interface with the following sections and parameters:

- Intelligent Mark:** Untriggered Target: Disable
- Video:** Processing Mode: Fluency Priority; Protocol: TCP
- Audio:** Encoding Format: G.711U
- Recording and Snapshot:**
  - Recording: Subsection By Time
  - Subsection Time (min): 30 [1-60]
  - When Storage Full:  Overwrite Recording  Stop Recording
  - Total Capacity(GB): 10 [1~1024]
  - Local Recording: TS
  - Files Folder: C:\Users\user\AppData\Local\Surveillance\_IPC\_PT [Browse... Open]

A 'Save' button is located at the bottom left of the interface.

Table 7-2 Parameter Description

Area	Parameter	Description
Intelligent Mark	Untriggered Target	The configuration is not supported.
Video	Processing Mode	<p>The options are as follows:</p> <ul style="list-style-type: none"> <li>Real-Time Priority: Recommended if the network is in good condition.</li> <li>Fluency Priority: Recommended if you want short time lag for live video.</li> <li>Ultra-low Latency: Recommended if you want the minimum time lag for live video.</li> </ul> <p>When the network is in good condition, <b>Real Time Priority</b> is recommended. If delay exists on the network, <b>Fluency Priority</b> is recommended. If it is required that the live view delay should be lower than the real time priority, <b>Ultra-low Latency</b> is recommended.</p>
	Protocol	<p>Set the protocol used to transmit media streams to be decoded by the PC.</p> <p>The options are as follows:</p> <ul style="list-style-type: none"> <li>UDP</li> <li>TCP</li> </ul>
Audio	Encoding Format	Audio encoding format on the client.
Recording and Snapshot	Recording	<p>Type of local recording subsection. The options are as follows:</p> <ul style="list-style-type: none"> <li>Subsection by Time: Duration of recorded video for each recording file on the computer. For example, 2 minutes.</li> <li>Subsection by Size: Size of each recording file stored on the computer. For example, 5M.</li> </ul>
	Subsection Time (min)	<p>This parameter is displayed only when <b>Recording</b> is set to <b>Subsection by Time</b>.</p> <p>The value ranges from 1min to 60min.</p>

Area	Parameter	Description
		You can enter the value based on actual conditions.
	Subsection Size (MB)	This parameter is displayed only when <b>Recording</b> is set to <b>Subsection by Size</b> . The value ranges from 10MB to 1024MB. You can enter the value based on actual conditions.
	When Storage Full	The options are as follows: <ul style="list-style-type: none"> <li>• Overwrite Recording: When the assigned storage space on the computer is used up, the device deletes the existing recording files to make room for the new recording file.</li> <li>• Stop Recording: When the assigned storage space on the computer is full, recording stops automatically.</li> </ul>
	Total Capacity(GB)	Total capacity assigned for local recording. The value ranges from 10GB to 1024GB. You can enter the value based on actual conditions.
	Files Folder	Path for storing snapshot photos.

(3) Click **Save** to complete the configuration.

### 3. Ethernet

Modify communication settings such as the IP address for the face recognition terminal so that the face recognition terminal can communicate with other devices.



#### NOTE!

After you have changed the IP address, you need to use the new IP address to log in.

(1) Choose **Setup > Common > Ethernet** to go to the **Ethernet** interface.

Figure 7-13 Ethernet Configuration Interface

(2) Set **Obtain IP Address** as shown in ① in the figure above.

- When **Obtain IP Address** is set to **Static**, complete the configuration by referring to the figure below.

Figure 7-14 Static Address Configuration Interface

Table 7-3 Parameter Description

Parameter	Description
Network Isolation	Keep the default value <b>Off</b> . It cannot be configured.
IP Address	Enter the IP address of the device. The IP address of the device must be unique across the network and cannot begin with 127.
Subnet Mask	Enter the subnet mask of the device.
Default Gateway	Enter the default gateway of the device.

- When **Obtain IP Address** is set to **PPPoE**, complete the configuration by referring to the figure below. If the face recognition terminal is connected to the network through Point to Point over Ethernet (PPPoE), you need to select PPPoE as the IP obtainment mode.

Figure 7-15 PPPoE Configuration Interface

Table 7-4 Parameter Description

Parameter	Description
Username	Enter the username and password provided by your internet Service Provider (ISP).
Password	



**NOTE!**

This function is not supported by some models. Please see the actual model for details.

- When **Obtain IP Address** is set to **DHCP**, complete the configuration by referring to the figure below. The Dynamic Host Configuration Protocol (DHCP) is enabled by default when the face recognition terminal is delivered. If a DHCP server is deployed in the network, the face recognition terminal can automatically obtain an IP address from the DHCP server.

Figure 7-16 DHCP Configuration Interface

- (1) The IPv6 configuration is not supported as shown in ② in the figure above.
- (2) Set parameters as shown in ③ in the figure above.

Table 7-5 Parameter Description

Parameter	Description
MTU	The value ranges from 576 to 1500. This parameter is not displayed when <b>Obtain IP Address</b> is set to <b>PPPoE</b> .
Port Type	The default value is <b>FE Port</b> . Keep the default value.
Operating Mode	The options are as follows: 10M Half Duplex 10M Full Duplex 10M Auto-Negotiation 100M Half Duplex 100M Full Duplex 100M Auto-Negotiation Auto-Negotiation

- (3) Click **Save** to complete the configuration.

#### 4. Time

Users can try the following methods to adjust the system time of the face recognition terminal to correct time.

- (1) Choose **Setup > Common > Time** to go to the **Time** interface.

Figure 7-17 Time Configuration Interface

Table 7-6 Parameter Description

Parameter	Description
Sync Mode	The options are as follows: <ul style="list-style-type: none"> <li>• Sync with System Configuration: The time is synchronized with the initially configured time of the system.</li> <li>• Sync with NTP Server: The time is synchronized with the time of the NTP server.</li> <li>• Sync with Management Server (ONVIF): The time is synchronized with the time of the management server.</li> <li>• Sync with Latest Server Time: The time is synchronized with the latest time of all servers in the network.</li> </ul>
Time Zone	Select the correct time zone.
System Time	This parameter is available only when <b>Sync Mode</b> is set to <b>Sync with System Configuration</b> or <b>Sync with Latest Server Time</b> . Configure the correct time.

Parameter	Description
Sync with Computer Time	This parameter is available only when <b>Sync Mode</b> is set to <b>Sync with System Configuration</b> or <b>Sync with Latest Server Time</b> . The system time for synchronization is the time of the local PC.
NTP Server Address	This parameter is displayed only when <b>Sync Mode</b> is set to <b>Sync with NTP Server</b> . Enter the IP address of the NTP server.
Update Interval(s)	This parameter is displayed only when <b>Sync Mode</b> is set to <b>Sync with NTP Server</b> . It indicates the interval for synchronizing time with the NTP server. The value ranges from 30s to 3600s.

(2) Choose **Setup > Common > Time** and click the **DST** tab to go to the **DST** tab page.

Figure 7-18 DST Configuration Interface

Table 7-7 Parameter Description

Parameter	Description
DST	The options are as follows: <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> </ul> The following parameters are configurable only when <b>DST</b> is set to <b>On</b> .
Start Time	Set the parameter based on actual conditions.
End Time	Set the parameter based on actual conditions.
DST Bias	The options are as follows: <ul style="list-style-type: none"> <li>• 30mins</li> <li>• 60mins</li> <li>• 90mins</li> <li>• 120mins</li> </ul> Set the parameter based on actual conditions.

(3) Click **Save** to complete the configuration.

## 5. Server

If the face recognition terminal is used in standalone mode, you do not need to configure server information. When connected to the intelligent server, the face recognition terminal can upload data including entry/exit records and captured images to the intelligent server in real time. Follow the steps to configure the intelligent server:

(1) Choose **Setup > Common > Server** and click the **Intelligent Server** tab.

(2) Under **Intelligent Server 1**, complete the configuration by referring to the table below.

### Intelligent Server

#### Intelligent Server 1

Server IP

Server Port

Platform Communication Type

Device No.

Keepalive interval(s)  s

Record Upload Response  On  Off

**Enable Intelligent Server 2**

#### Subscription List

No.	Subscription ID	Server IP	Port No.	Type	Remaining Time(s)	
1	0	<a href="#">202.8.20.11</a>	62732	Alarm Subscription	Permanent Subscription	

**Note:**To transfer images by FTP, you need to add server information on the FTP setting page.

Table 7-8 Parameter Description

Parameter	Description
Server IP	IP address of the server
Server Port	Port number on the server. Default: 5196
Platform Communication Type	Choose a communication protocol according to the actual connection method: <ul style="list-style-type: none"> <li>UV-V2: Choose this option if the terminal is to be connected with Guard Station.</li> <li>FTP: To transfer images by FTP, you need to add server information on the <a href="#">FTP</a> setting page</li> <li>LAPI V2: Choose this option if the communication between the terminal and the platform requires Network Address Translation (NAT).</li> </ul>
Device No	A device number is an identifier that the face recognition terminal uses to connect to the platform server. The device number must be unique on the network. <b>Note:</b> Configuration is required only when <b>Platform Communication Type</b> is set to <b>UV-V2</b> . Use the default setting.
Keepalive interval(s)	A new persistent LAPI connection is required if the length of time that there's no communication between the terminal and the platform exceeds the keepalive interval. <b>Note:</b> Configuration is required only when <b>Platform Communication Type</b> is to <b>LAPI V2</b> .
Record Upload Response	<ul style="list-style-type: none"> <li>On: The terminal verifies whether a record has been uploaded successfully to the platform in accordance with the response from the platform.</li> <li>Off: The terminal uploads records to the platform without performing the above-mentioned verification.</li> </ul> <b>Note:</b> Configuration is required only when <b>Platform Communication Type</b> is to <b>LAPI V2</b> .

(3) Under **Subscription List**, you can see detailed subscription information.



## NOTE!

If the terminal is to be connected to two Guard Station servers, select the check box for **Enable Intelligent Server 2** and then complete the configuration by referring to this above table.

### 6. User

The device supports no more than one administrator and a maximum of 32 ordinary users. The administrator is **admin** (the administrator name cannot be modified) by default and has all management and operation permissions for the device and users. Ordinary users only have the live view permission for the device.

#### 6A. Adding an ordinary user

- (1) Log in to the terminal interface as **admin**.
- (2) Choose **Setup > Common > User** to go to the **User** interface.
- (3) Follow the steps shown in the figure below to add an ordinary user.

Figure 7-19 Ordinary User Adding Interface

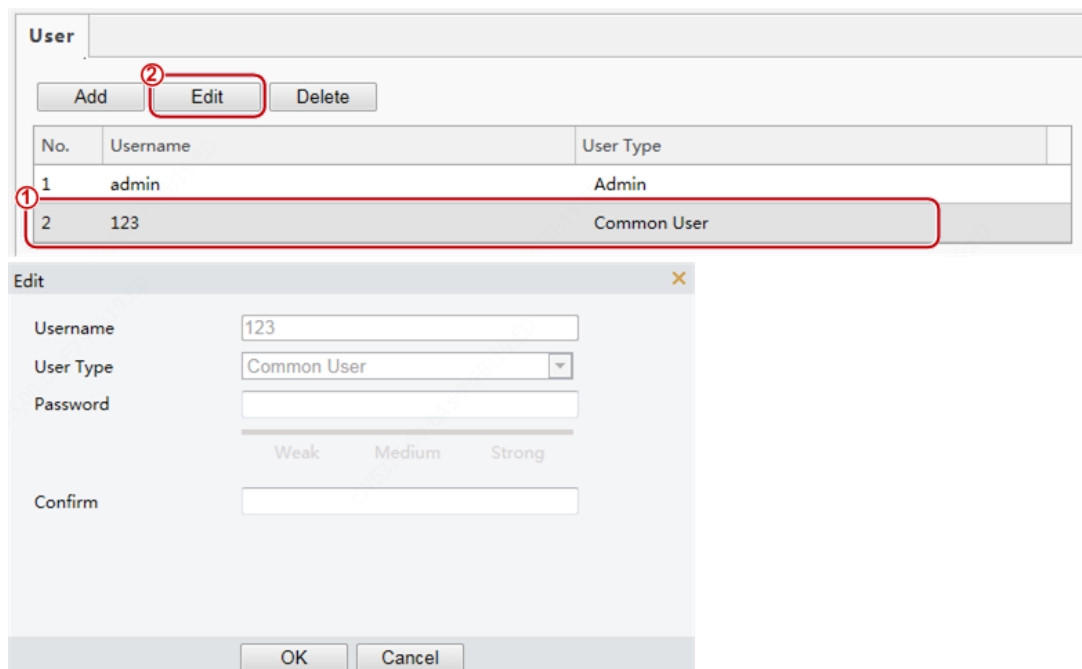
The screenshot shows the 'User' management interface. At the top, there are three buttons: 'Add', 'Edit', and 'Delete'. The 'Add' button is circled in red and labeled with a circled '1'. Below the buttons is a table with columns 'No.', 'Username', and 'User Type'. The table contains one row with '1' in the 'No.' column, 'admin' in the 'Username' column, and 'Admin' in the 'User Type' column. An 'Add' dialog box is open in the foreground, also circled in red and labeled with a circled '2'. The dialog box has the following fields: 'Username' (containing '123'), 'User Type' (a dropdown menu set to 'Common User'), 'Password' (a masked field with 10 dots), and 'Confirm' (a masked field with 10 dots). Below the password field, there is a strength indicator with three bars: 'Weak' (grey), 'Medium' (yellow), and 'Strong' (green). The 'OK' button is circled in red and labeled with a circled '3', and the 'Cancel' button is also visible.

#### 6B. Editing an ordinary user

The following uses an ordinary user as an example. The steps of editing **admin** are the same as those of editing an ordinary user.

- (1) Log in to the terminal interface as **admin**.
- (2) Choose **Setup > Common > User** to go to the **User** interface.
- (3) Select the ordinary user to be edited and follow the steps as shown in the figure below to edit the user information.

Figure 7-20 Ordinary User Information Editing Interface

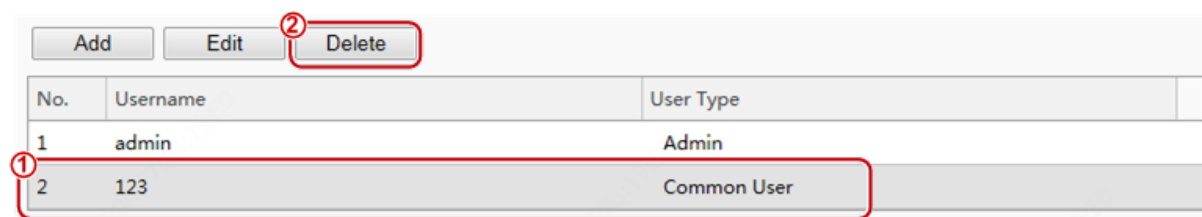


(4) After editing information, click **OK** to save the user information.

#### 6C. Deleting an ordinary user

- (1) Log in to the terminal interface as **admin**.
- (2) Choose **Setup > Common > User** to go to the **User** interface.
- (3) Select the ordinary user to be deleted and follow the steps as shown in the figure below to delete the user.

Figure 7-21 Ordinary User Deletion Interface



#### NOTE!

- Only **admin** can modify passwords. When the name or password of a user is modified, if the user has logged in to the system, the user will be forced to log out and needs to enter the new name or password for login next time.
- Only **admin** can delete existing users. After a user is deleted, the user cannot log in. If the user has logged in to the system before deletion, the user will be forced to log out.
- The Web interface login password of **admin** is the same as the activation password. If the login password of **admin** has been changed, use the new password to log in to the [Activation Config](#) interface.

## 7. Ports & Devices

### 7A. Serial Port



When the face recognition terminal conducts O&M management on a gate machine through a serial port or it connects to an IC card reader, serial port information needs to be configured. Perform the following operations to configure a serial port:



**NOTE!**

The serial port configuration interface varies with the device type.


- (1) Choose **Setup > Common > Ports & Devices** and click the **Serial Port** tab.

Figure 7-22 Serial Port Configuration Interface

The screenshot shows two configuration panels side-by-side. The left panel is for 'RS485\_1' and the right panel is for 'RS232\_1'. Both panels have a 'Port Mode' dropdown menu. The RS485\_1 panel includes checkboxes for 'Enable QR code reader' and 'Enable Security Module', an 'RS485 Address' dropdown, and standard serial port settings (Baud Rate, Data Bits, Stop Bits, Parity, Flow Control). The RS232\_1 panel includes a 'Format' dropdown, standard serial port settings, and an 'Enable Trans-Channel' checkbox. A 'Save' button is located at the bottom left of the RS485\_1 panel.

Table 7-9 Parameter Description

Parameter	RS485_1	RS232_1
Port Mode	Security/Temperature Module: Select this option when the face recognition terminal connects to a digital detection module through the RS485 serial port.	IC Card Mode: This option is displayed when the face recognition terminal has a built-in card reader.
Enable QR code reader /Enable Security Module	The configuration is not supported.	/
RS485 Address	The configuration is not supported.	/
Format	/	Card number reading and storage mode. For example, the card number 4204783027 is stored with binary in different ways as follows. Ascending Order: 1111 1010 1001 1111 1110 0101 1011 0011 Descending Order: 1011 0011 1110 0101 1001 1111 1111 1010
Baud Rate	The configuration is not supported. Use the default value.	
Data Bits/ Stop Bits/ Parity/	Keep the default values as follows: Data Bits: 8	

Parameter	RS485_1	RS232_1
Flow Control	Stop Bits: 1 Parity: None Flow Control: None  <b>NOTE!</b> The parameters cannot be set when <b>Port Mode</b> is set to <b>IC Card Mode</b> .	
Enable Trans-Channel	It is used for internal debugging. Ignore it.	

- (2) Configure serial port information based on actual scene configuration.
- (3) Click **Save** to complete the serial port configuration.

### 7B. Wiegand Interface

When the face recognition terminal connects to an IC card reader, Wiegand interface information needs to be configured. Perform the following operations to complete the configuration:

- (1) Choose **Setup > Common > Ports & Devices** and click the **Wiegand Interface** tab.



#### NOTE!

- Some devices support the input through only one or zero Wiegand interfaces and the configuration window for the Wiegand input interface is different for the devices.
- Some devices do not support the output through the Wiegand interface. In this case, the configuration window for the Wiegand output interface will not be displayed.
- The Wiegand interface configuration window is unavailable to OET-213H with a built-in IC card reader.

Figure 7-23 Wiegand Interface Configuration Window

The screenshot shows two configuration panels. The left panel, titled 'Wiegand Input\_1', has 'Protocol' set to 'Wiegand 26' and 'Format' set to 'Ascending O'. The right panel, titled 'Wiegand Output\_1', has 'Protocol' set to 'None' and 'Format' set to 'Ascending O'.

- (2) Configure Wiegand interface information by referring to the table below.

Table 7-10 Parameter Description

Parameter	Description
Protocol	Set it based on actual scenes. <ul style="list-style-type: none"> <li>• Wiegand 26</li> <li>• Wiegand 32</li> <li>• Wiegand 34</li> <li>• Wiegand 36</li> <li>• Wiegand 37</li> <li>• Wiegand 50</li> </ul>
Format	The default value is <b>Ascending Order</b> . Set this parameter based on actual scenes. The parameter description is the same as <a href="#">Table 7-9 Format</a> .

- (3) Click **Save** to complete the Wiegand interface configuration.

## 7C. IO Configuration

The face recognition terminal connects to gate machines, door locks, or access control buttons and sends the door opening signal to them. Perform the following operations to complete configuration:

- (1) Choose **Setup > Common > Ports & Devices** and click the **IO Configuration** tab.



### NOTE!

- Some devices support the output from only one or zero IO ports and the IO port configuration interface is different for the devices.
- Some devices does not support door locks or access control buttons and the IO port configuration interface is different for the devices.

Figure 7-24 IO Configuration Interface

ID	Enable	Type	Level Value	Pulse Width
F1	<input checked="" type="checkbox"/>	Door Lock	Low Level	5 s
F2	<input checked="" type="checkbox"/>	Door Button	Low Level	100 ms
F3	<input checked="" type="checkbox"/>	Alarm Output	Low Level	100 ms

**Access Control**

Unlock Interval  s

Door Opening Timeout  s


Auto Door Lock Upon C...  On  Off

Check Door Magnet Sta...  On  Off

- (2) Configure IO port information by referring to the table below.

Table 7-11 Parameter Description

Parameter	Description
F1/F2/F3	<p>F1/F2/F3 indicates the IO port of the face recognition terminal. Select the check box in the front. Then, the configuration of the IO port will take effect.</p> <p>IO ports support the following types of external devices:</p> <ul style="list-style-type: none"> <li>• Door lock: The face recognition terminal outputs door opening signals to door locks through an IO port. <b>Pulse Width</b> here refers to one door opening duration. When the door opening duration exceeds this time, the door magnet will generate an alarm. Value range: [1–300]s; Default value: 5s</li> <li>• Door button: The face recognition terminal can receive the door opening signal from the access control button through an IO port and sends the door opening signal to the door lock. The pulse width value here indicates that a valid door opening signal is generated only when the duration in which the door opening button is held down reaches the value here. Value range: [0–20000]ms; Default value: 100ms</li> <li>• Alarm output: The face recognition terminal outputs alarms through an IO port. Value range: [0–20000]ms; Default value: 100ms</li> </ul> <p><b>Level Value</b> can be set to <b>Low Level</b> or <b>High Level</b>. The value should be consistent with the input and output signal level supported by external devices.</p>
Unlock Interval	<p>It indicates the interval between two unlock operations. After the door is unlocked, it will not be re-unlocked within the unlock interval even if a new unlock signal is received. In addition, the door opening duration of the door lock will not be re-timed. If it is set to <b>0</b>, door unlock will be triggered</p>

Parameter	Description
	each time the unlock signal is received, and the door opening duration of the door lock will be re-timed. Value range: [0–300]s; Default value: 0s
Door Opening Timeout	After <b>Auto Door Lock Upon Closing</b> is enabled, if the door closing time exceeds the value here and the door magnet detects that the door is in the closed position, the face recognition terminal automatically locks the door. Value range: [1–300]s; Default value: 10s  <b>NOTE!</b> <ul style="list-style-type: none"> <li>It is not recommended to set it to a very small value. Otherwise, normal door opening will be affected.</li> <li>The generation of a door magnet alarm is related to door opening timeout.</li> </ul>
Auto Door Lock Upon Closing	Select whether to enable auto door lock upon door closing. <ul style="list-style-type: none"> <li>On: When the door magnet detects that the door is closed and the door closing time exceeds the value of <b>Door Opening Timeout</b>, the door will be locked automatically.</li> <li>Off: The auto door lock upon closing is disabled and the door closing time is the door opening duration.</li> </ul>
Check Door Magnet Status Before Closing	<ul style="list-style-type: none"> <li>On: The door magnet status is checked before closing.</li> <li>Off: The door magnet status is not checked before closing.</li> </ul>

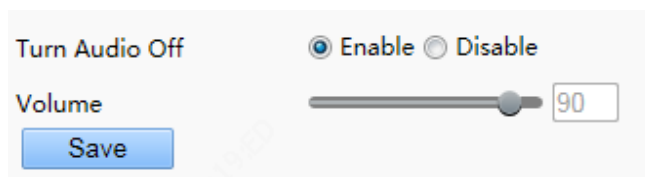
(3) Click **Save** to complete the IO port configuration.

#### 7D. Volume Control

If the face recognition terminal connects to an audio device, configure audio information on the **Volume Control** tab page.

(1) Choose **Setup > Common > Ports & Devices** and click the **Volume Control** tab.

Figure 7-25 Audio Configuration Interface



(2) Set whether to mute the audio. If no, set the play volume.

(3) Click **Save** to complete the audio configuration.

#### 7E. Illumination

The face recognition terminal supports light energy conservation configuration.

(1) Choose **Setup > Common > Ports & Devices** and click the **Illumination** tab.

(2) Set energy conservation parameters based on actual requirements.

Figure 7-26 Energy Conservation Configuration Interface

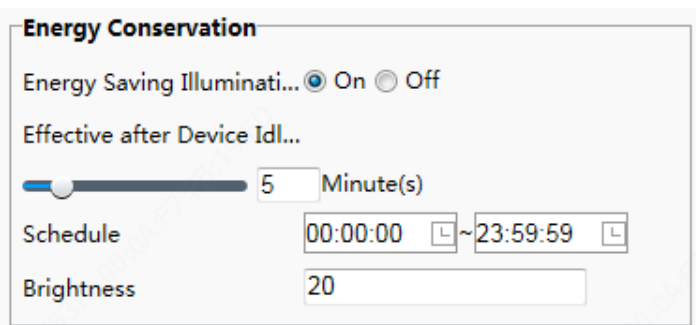



Table 7-12 Parameter Description

Parameter	Description
Energy Saving Illumination	<ul style="list-style-type: none"> <li>On: When the face recognition terminal detects a face within the preset <b>Schedule</b>, all lights (including the LCD light, display screen, and light supplement lamp) are on (only when the brightness of the current ambient light does not reach the minimum brightness threshold of the device). When no face is detected within the preset <b>Effective after Device Idle For</b>, the lights become off gradually (only when the brightness of the current ambient light exceeds the maximum brightness threshold of the device). Lights are steady on out of the <b>Schedule</b> regardless of whether the face recognition terminal detects a face.</li> <li>Off: Lights are steady on regardless of whether the face recognition terminal detects a face. Energy conservation is disabled on the lights.</li> </ul> <p>Energy saving illumination is disabled by default.</p>
Effective after Device Idle For	<p>Duration in which the face recognition terminal does not detect a face. If the duration exceeds this value, the lights of the face recognition terminal will be off gradually.</p> <p>Value range: [1–30]min; default value: 5min</p>
Schedule	<p>After <b>Energy Saving Illumination</b> is set to On, the face recognition terminal applies energy saving illumination within the schedule. Energy saving illumination is not performed out of the schedule.</p> <p>The value ranges from 00:00:00 to 23:59:59 and the unit can be accurate to seconds.</p> <p> <b>NOTE!</b></p> <p>When <b>Energy Saving Illumination</b> is set to On, the default value of Schedule is [00:00:00~23:59:59]. When <b>Energy Saving Illumination</b> is set to Off, Schedule is unavailable.</p>
Brightness	<p>This parameter is used to adjust the brightness of the light supplement lamp when the display screen is off. A larger parameter value indicates brighter light supplement lamp and vice versa.</p> <p>Value range: [0–200]; default value: 20</p> <p>If it is set to <b>0</b>, the light supplement lamp is turned off.</p> <p>The brightness can take effect only after the display screen becomes off again.</p>

(3) Click **Save** to complete the energy conservation configuration.

## 7F. USB

Storage information will be displayed when a USB flash drive is plugged into the terminal. See [Device Maintenance](#) and [Data Management](#) for the use of USB function.

## 8. Device Info

The **Device Info** interface allows you to configure the current location of the device.

- (1) Log in to the terminal interface as **admin**.
- (2) Choose **Setup > Common > Device Info** to go to the **Device Info** interface.

Figure 7-27 Device Info Configuration Interface

**Device Info**

**Device Location**

Management Center IP

Community

Building  Building

Configurable Units

Unit  Unit

**Save**

Table 7-13 Parameter Description

Parameter	Description
Device Location	The configuration is not supported.



**NOTE!**

Changing the device type will restart the device and restore the authentication mode to the default configuration.

**9. Personalization**

**9A. Ad Mode**

The face recognition terminal supports ads (pictures only). The configuration is as follows:

- (1) Choose **Setup > Common > Personalization** and click the **Ad Mode** tab.
- (2) Set the ad mode by referring to the table below.

Figure 7-28 Ad Mode Setting Interface

Ad Mode  On  Off

Ad Image Play Interval(s)

Standby time(s)

Import Image File  **Browse...** **Upload** **Default**

Note: 1.The imported must be a .zip file including no more than 3 JPG images named 1.jpg, 2.jpg and 3.jpg.  
 2.JPG only. Recommended sizes: 800\*1280 for 10 inches , 600\*1024 for 7 inches, 480\*800 for 4 inches.

**Save**

Table 7-14 Parameter Description

Parameter	Description
Ad Mode	Select whether to enable the ad mode based on actual conditions.
Ad Image Play Interval(s)	Set the interval for playing ad images. The value is an integer in the range of 1s to 3600s. The default value is 10s.
Standby Time(s)	When the duration in which the face recognition terminal does not detect a face reaches the time set here, the face recognition terminal enters the ad mode.

Parameter	Description
	<p>The value is an integer in the range of 10s to 3600s. The default value is 10s.</p> <p>The face recognition terminal exits the ad mode when the face scan fails or a user taps the screen.</p>
Import Image File	<p>Users can define ad images. The requirements for ad images are as follows:</p> <ul style="list-style-type: none"> <li>• The imported must be a .zip file including no more than 3 JPG images named 1.jpg, 2.jpg and 3.jpg.</li> <li>• JPG only. Recommended sizes: 800*1280 for 10 inches, 600*1024 for 7 inches, 480*800 for 4 inches.</li> </ul>

(3) Click **Save** to complete the ad mode configuration.

### 9B. Custom Logo and Prompt

The face recognition terminal supports custom logos and prompts. The configuration is as follows:

- (1) Choose **Setup > Common > Personalization** and click the **Custom Logo and Prompt** tab.
- (2) Set the custom logo and prompt by referring to the table below.

Figure 7-29 Custom Logo and Prompt Interface

Table 7-15 Parameter Description

Parameter	Description
Title	<ul style="list-style-type: none"> <li>• Display: The title bar is displayed. The title content can be set as follows: <ul style="list-style-type: none"> <li>➤ Default: "Welcome" is displayed on the title bar.</li> <li>➤ Custom: You can define the title content. A string of 0–14 characters can be entered.</li> </ul> </li> <li>• Hide: The title bar is not displayed.</li> </ul>
Import Logo Image	<p>Users can define a logo image. The requirements for a logo image are as follows: JGP only, no more than 16 characters in file name. Recommended size: 220*180.</p>

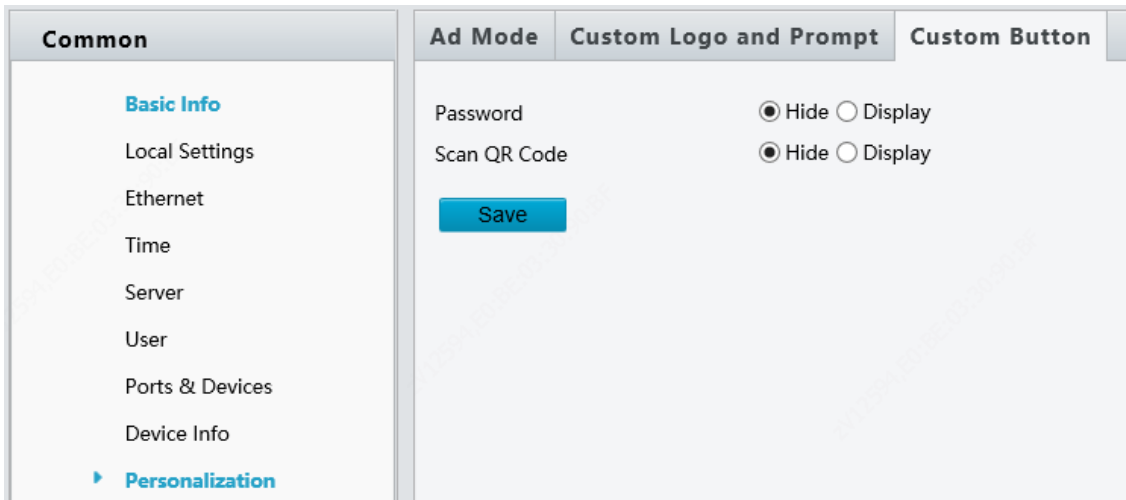
(3) Click **Save** to complete the custom logo and prompt configuration.

### 9C. Custom Button

The face recognition terminal supports custom buttons. The configuration is as follows:

- (1) Choose **Setup > Common > Personalization** and click the **Custom Button** tab.

Figure 7-30 Custom Button Interface



- (2) Define buttons based on application scenes.
  - Display: The corresponding button is displayed on the GUI.
  - Hide: The corresponding button is not displayed on the GUI.
- (3) Click **Save** to complete the custom button configuration.

### 7.3.2 Network

#### 1. Network

For the Ethernet configuration interface, see [Ethernet](#).

#### 2. DNS

The configuration is not supported.

#### 3. Port

The configuration is not supported.

#### 4. DDNS

The configuration is not supported.

#### 5. P2P

Add the device to a cloud server to achieve remote management.

Log in to [www.star4live.com](http://www.star4live.com) and add the device by scanning the QR code. For detailed operations, see the online documentation at the website





## 6. E-mail

The system can send captured images (snapshots) to user-specified email addresses according to the configured parameters.

- (1) Choose **Setup > Network > E-mail**
- (2) Set parameters by referring to the table below. Click **Save** to complete the configuration.

Parameter	Description
Name	Set a name as needed.
Address	Sender's email address.
SMTP Server	Address of a server that sends emails using SMTP. For example, smtp.163.com. Configure based on the actual condition. You can find the required information by accessing the sender's mailbox on the web or by contacting the email service provider.
SMTP Port	Configure the corresponding transport port based on whether TLS/SSL is enabled. Access the sender's mailbox on the web or contact the email service provider for the port number.
TLS/SSL	When enabled, emails will be sent through a secure channel encrypted using TLS or SSL.
Snapshot Interval(s)	Reserved. The configuration is not supported.
Attach Image	When enabled, emails will be attached with snapshots.
Username	Sender's email address.
Password	Login password, provided by third-party email service provider. To get the login password: access the sender's mailbox, enable SMTP on the service setup page to request for the password.
Name	Set a name that can easily identify the recipient.
Address	Recipient's email address. Clicking Test will immediately send the recipient a test email.

## 7. SNMP

The configuration is not supported.

## 8. 802.1x

The configuration is not supported.

### 7.3.3 Image

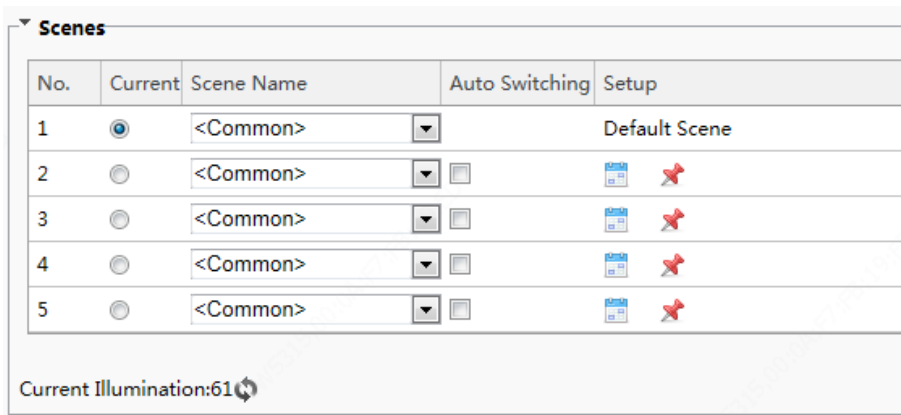
#### 1. Image

##### 1A. Scenes

Set image parameters to achieve the desired image effects based on live video in different scenes.

- (1) Click **Setup > Image > Image** and then click **Scenes**.

Figure 7-31 Scene Configuration Interface



- (2) Scene Name: name of the current scene. Several scene modes have been preset in the device. After a scene mode is selected, image parameters are automatically switched (you can adjust image parameters as required).
  - Common: recommended for outdoor scenes.
  - Custom: set a scene name as needed.
- (3) Select a scene and then click to set it as the default scene.
- (4) If auto-switching is enabled, the device can switch to the scene automatically when the condition for switching to a non-default scene is met. Otherwise, the device remains in the default scene. When auto-switching is not enabled, the device remains in the current scene.



**NOTE!**

- If **Auto Switching** is enabled (scene settings will be unavailable), the device will switch between the set scenes. If not, the device will stay at the current scene. The device will stay at default scenes unless the non-default scenes are triggered.
- If multiple non-default scenes are triggered, then the device will switch to the scene with the minimum number (starting from 1 to 5).

1B. Image Enhancement

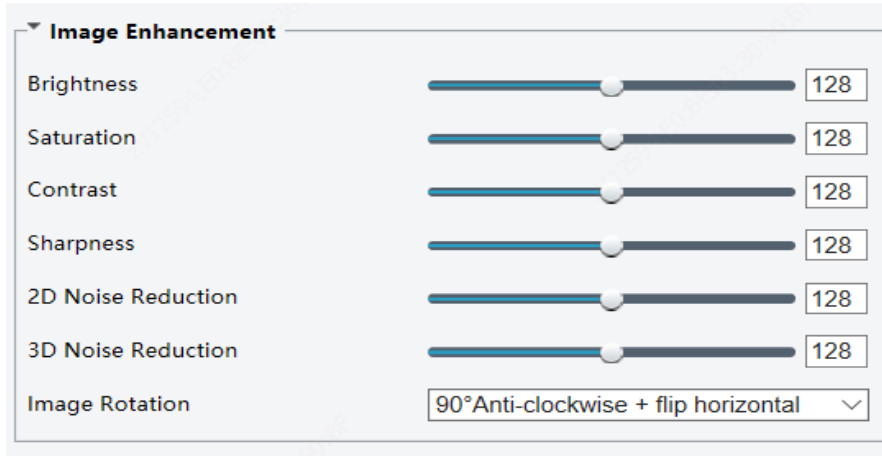


**NOTE!**

All parameters on the **Image Enhancement** interface use default values and cannot be configured.







- (1) Click **Setup > Image > Image** and then click **Image Enhancement**.









Figure 7-32 Image Enhancement Interface



(2) Use the sliders to change the settings. You may also enter values directly. The following table describes some major parameters.

Table 7-16 Parameter Description

Item	Description
<p>Brightness</p>	<p>Set the degree of brightness of images.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="579 1218 730 1245">Low brightness</span> <span data-bbox="855 1218 1007 1245">High brightness</span> </div>
<p>Saturation</p>	<p>The amount of a hue contained in a color.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="579 1585 730 1612">Low saturation</span> <span data-bbox="855 1585 1007 1612">High saturation</span> </div>
<p>Contrast</p>	<p>Set the degree of difference between the blackest pixel and the whitest pixel.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="579 1957 730 1984">Low contrast</span> <span data-bbox="855 1957 1007 1984">High contrast</span> </div>
<p>Sharpness</p>	<p>Contrast of boundaries of objects in an image.</p>

Item	Description
	<div style="display: flex; justify-content: space-around; align-items: center;">   </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span data-bbox="580 483 729 510">Low sharpness</span> <span data-bbox="860 483 1008 510">High sharpness</span> </div>
2D Noise Reduction	Reduce the noise of images. The function may cause image blurring.
3D Noise Reduction	Reduce the noise of images. The function may cause motion blur (or ghosting in some applications).
Image Rotation	<p data-bbox="424 696 644 723">Rotation of the image.</p> <div style="display: flex; flex-wrap: wrap; justify-content: space-around; align-items: center;"> <div style="text-align: center; margin: 5px;">  <p data-bbox="619 1032 695 1059">Normal</p> </div> <div style="text-align: center; margin: 5px;">  <p data-bbox="884 1032 1000 1059">Flip Vertical</p> </div> <div style="text-align: center; margin: 5px;">  <p data-bbox="584 1375 730 1402">Flip Horizontal</p> </div> <div style="text-align: center; margin: 5px;">  <p data-bbox="922 1375 963 1402">180</p> </div> <div style="text-align: center; margin: 5px;">  <p data-bbox="596 1700 729 1727">90°Clockwise</p> </div> <div style="text-align: center; margin: 5px;">  <p data-bbox="873 1700 1054 1727">90°Anti- clockwise</p> </div> </div>

(3) To restore default settings in this area, click **Default**.

### 1C. Exposure

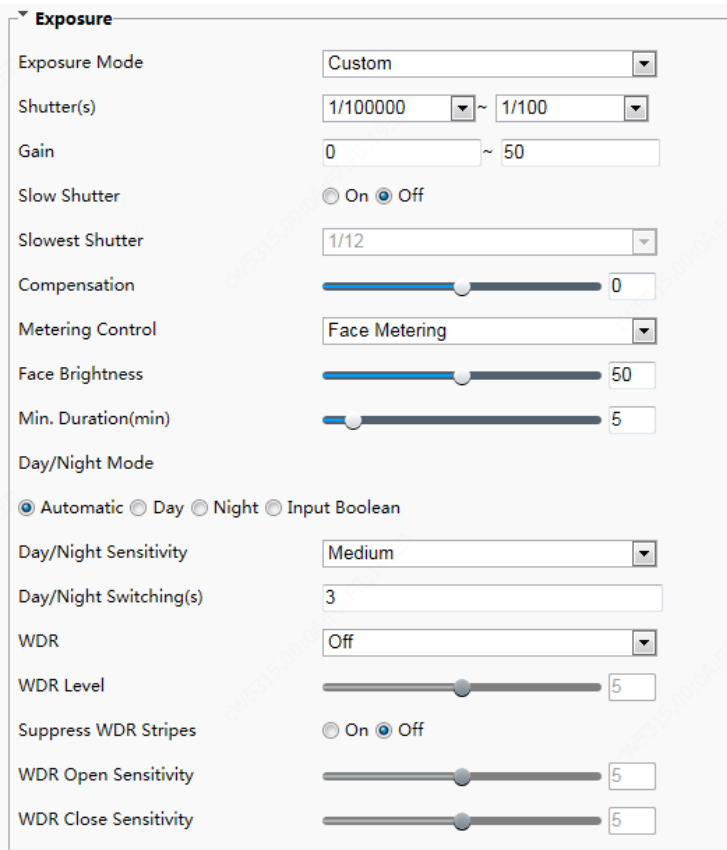


**NOTE!**

- This function may vary with models. Please see actual Web interface for details.
- The default settings are scene-adaptive. Use default settings unless modification is necessary.



(1) Click **Setup > Image > Image** and then click **Exposure**.







Figure 7-33 Exposure Configuration Interface







(2) Set parameters as required. The table below describes the exposure parameters.

Table 7-17 Parameter Description

Item	Description
Exposure Mode	<p>Select a mode to achieve the desired exposure effect.</p> <ul style="list-style-type: none"> <li>Automatic: The device automatically adjusts exposure based on the environment.</li> <li>Custom: The user sets exposure as needed.</li> <li>Indoor 50Hz: The device reduces stripes by limiting shutter frequency.</li> <li>Indoor 60Hz: The device reduces stripes by limiting shutter frequency.</li> <li>Manual: The device allows fine-tuning image quality by setting shutter, gain and iris manually.</li> <li>Low Motion Blur: The device controls the minimum shutter to reduce motion blur in face photos captured in motion.</li> </ul>
Shutter(s)	<p>Shutter is used to control the light that comes into the lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly.</p> <p> <b>NOTE!</b></p> <ul style="list-style-type: none"> <li>You can set a shutter speed when <b>Exposure Mode</b> is set to <b>Manual</b> or <b>Shutter Priority</b>.</li> <li>If <b>Slow Shutter</b> is set to <b>Off</b>, the reciprocal of the shutter speed must be greater than the frame rate.</li> </ul>
Gain	<p>Control image signals so that the device outputs standard video signals according to the light condition.</p> <p> <b>NOTE!</b></p> <p>You can set this parameter only when <b>Exposure Mode</b> is set to <b>Manual</b> or <b>Gain Priority</b>.</p>
Slow Shutter	Improves image brightness in low light conditions.

Item	Description
	 <b>NOTE!</b> You can set this parameter only when <b>Exposure Mode</b> is not set to <b>Shutter Priority</b> and when <b>Image Stabilizer</b> is disabled.
Slowest Shutter	Set the slowest shutter speed that the device can use during exposure.  <b>NOTE!</b> You can set this parameter only when <b>Slow Shutter</b> is set to <b>On</b> .
Compensation	Adjust the compensation value as required to achieve the desired effects.  <b>NOTE!</b> You can set this parameter only when <b>Exposure Mode</b> is not set to <b>Manual</b> .
Metering Control	Set the way the device measures the intensity of light. <ul style="list-style-type: none"> <li>• Center-Weighted Average Metering: The device measures light mainly in the central part of images.</li> <li>• Evaluative Metering: The device measures light in the customized area of images.</li> <li>• Spot Metering: It is similar to <b>Evaluative Metering</b> but the difference is that the image brightness cannot be improved.</li> <li>• Face Metering: The device adjusts the image quality in poor lighting conditions by controlling the brightness of captured face photos in Face scene.</li> </ul>  <b>NOTE!</b> You can set this parameter only when <b>Exposure Mode</b> is not set to <b>Manual</b> . The default value is <b>Face Metering</b> .
Face Brightness	This parameter is displayed only when <b>Metering Control</b> is set to <b>Face Metering</b> . In <b>Face Metering</b> mode, the system adjusts the exposure based on the value of <b>Face Brightness</b> and the face brightness in the live view so that the face brightness in the live view is within the appropriate range (over-exposure or under-exposure may be incurred to surroundings on the images). The value ranges from 0 to 100 and the default value is 50. A larger <b>Face Brightness</b> value indicates higher image brightness on the device and brighter face snapshot photos.
Min. Duration(min)	This parameter is displayed only when <b>Metering Control</b> is set to <b>Face Metering</b> . It refers to the maximum duration that the screen brightness of the device (applicable to the previous face) can be retained after the face detection of the previous person ends and the face of the next person is not detected. The timer is restarted each time the face detection of a person ends. After the time expires, the device adapts to the average brightness of the current environment till the face of the next person is detected. The value ranges from 0 to 60 and the default value is 5.
Day/Night Mode	Keep the default value <b>Automatic</b> . <ul style="list-style-type: none"> <li>• Automatic: The device outputs the optimum images according to the light condition. In this mode, the device can switch between night mode and day mode automatically.</li> <li>• Day: The device provides high-quality color images using the existing light.</li> <li>• Night: The device provides high-quality black and white images using the existing light.</li> <li>• Input Boolean: The device provides high-quality images by using external light.</li> </ul>
Day/Night Sensitivity	Light threshold for switching between day mode and night mode. A higher sensitivity means that The device is more sensitive to the change of light and becomes more easily to switch between day mode and night mode.  <b>NOTE!</b> You can set this parameter only when <b>Day/Night Mode</b> is set to <b>Automatic</b> .
Day/Night Switching(s)	Set the length of time before The device switches between day mode and night mode after the conditions for switching are met.  <b>NOTE!</b> You can set this parameter only when <b>Day/Night Mode</b> is set to <b>Automatic</b> .

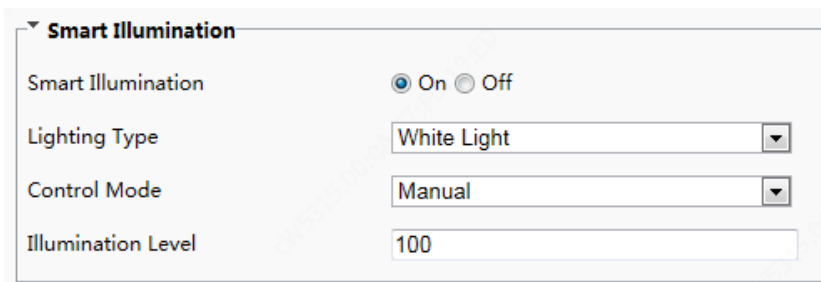
Item	Description	
WDR		<p>Enable WDR to distinguish the bright and dark areas in the same image.</p> <p> <b>NOTE!</b></p> <p>This parameter is available only when <b>Exposure Mode</b> is set to <b>Automatic, Custom, Shutter Priority, Indoor 50Hz, or Indoor 60Hz</b> and electronic image stabilization and defog are disabled.</p> <p>You can set this parameter only when <b>Exposure Mode</b> is neither <b>Customize</b> nor <b>Manual</b> and when <b>Image Stabilizer</b> is disabled.</p>
WDR Level		<p>After enabling the WDR function, you can improve the image by adjusting the WDR level.</p> <p> <b>NOTE!</b></p> <p>Use level 7 or higher when there is a high contrast between the bright and dark areas of the scene. In the case of low contrast, it is recommended to disable WDR or use level 1-6.</p>
Suppress Stripes	WDR	When enabled, The device can automatically adjust slow shutter frequency according to the frequency of light to minimize stripes that may appear in images.
WDR Sensitivity	Open	<p>Enable the WDR sensitivity.</p> <p> <b>NOTE!</b></p> <p>This parameter is available only when <b>WDR</b> is set to <b>Automatic</b>.</p>
WDR Sensitivity	Close	<p>Disable the WDR sensitivity.</p> <p> <b>NOTE!</b></p> <p>This parameter is available only when <b>WDR</b> is set to <b>Automatic</b>.</p>

(3) To restore the default settings, click **Default**.

#### 1D. Smart Illumination

(1) Click **Setup > Image > Image** and then click **Smart Illumination**.

Figure 7-34 Smart Illumination Interface



(2) Set smart illumination parameters by referring to the table below based on actual scenes.

Item	Description
Smart Illumination	Select whether to enable smart illumination based on actual conditions.
Lighting Type	It can be set to <b>White Light</b> only currently.
Control Mode	<ul style="list-style-type: none"> <li>Manual: After smart illumination is enabled, the light supplement lamp automatically controls illumination.</li> <li>Manual –Always on: After smart illumination is enabled, the light supplement lamp will always supplement illumination.</li> </ul>
Illumination Level	Set the intensity level of the IR light. The greater the value, the higher the intensity. <b>0</b> means that the IR light is turned off.

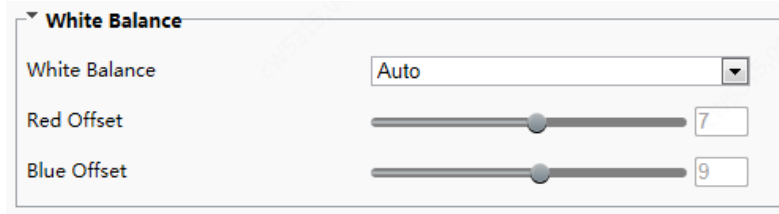
(3) To restore the default settings, click **Default**.

### 1E. White Balance



White balance is the process of offsetting unnatural color cast in images under different color temperatures so as to output images that best suit human eyes.

(1) Click **Setup > Image > Image** and then click **White Balance**.

Figure 7-35 White Balance Configuration Interface



(2) Select a white balance mode as required. The following table describes some major parameters.

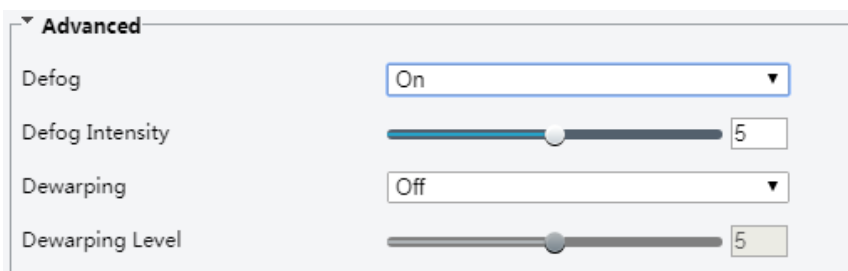
Item	Description
White Balance	<p>Adjust the red or blue offset of the image:</p> <ul style="list-style-type: none"> <li>• Auto/ Auto 2: The device adjusts the red and blue offset automatically according to the light condition (the color tends to be blue).If the images are still unnaturally red or blue in Auto mode, please try Auto2.</li> <li>• Fine Tune/ Fine Tune(Base on night mode): Allow you to adjust the red and blue offset manually.</li> <li>• Sodium Lamp: The camera adjusts red and blue offset automatically according to the light condition (the color tends to be red).</li> <li>• Outdoor: Suitable for outdoor environment with a relatively greater color temperature range.</li> <li>• Locked: Lock the current color temperature without change.</li> </ul>
Red Offset	<p>Adjust the red offset manually.</p> <p> <b>NOTE!</b> You can set this parameter only when <b>White Balance</b> is set to <b>Fine Tune</b>.</p>
Blue Offset	<p>Adjust the blue offset manually.</p> <p> <b>NOTE!</b> You can set this parameter only when <b>White Balance</b> is set to <b>Fine Tune</b>.</p>

(3) To restore the default settings, click **Default**.

### 1F. Advanced

Use the defog function to adjust the clarity of images captured in fog or haze conditions.

(1) Click **Setup > Image > Image** and then click **Advanced**.







## NOTE!

- You can set this parameter only when WDR is turned off.
- Only some camera models support optical defog. When **Defog** is set to **On**, defog intensity level 6-9 represent optical defog, and images change from color to black/white when defog intensity is set from level 5 to 6; if **Defog** is set to Automatic and defog intensity level is somewhere between 6-9, images do not automatically change to black/white in light fog conditions; the camera automatically switches to optical defog only in heavy fog conditions.

- Enable the defog function and then select a level for the scene. Level 9 achieves the maximum defog effects, and level 1 achieves the minimum.
- To restore the default settings, click **Default**.

## 2. OSD

On Screen Display (OSD) is the text displayed on the screen with video images and may include time and other customized contents.

- Click **Setup > Image > OSD**.

	Position	Overlay OSD Content	Status
1	Area1	<Date & Time>	✓
2	None		
3	None		
4	None		
5	None		
6	None		
7	None		
8	None		

**Display Style**

Effect: Background

Font Size: Medium

Font Color: #0000-1

Min. Margin: None

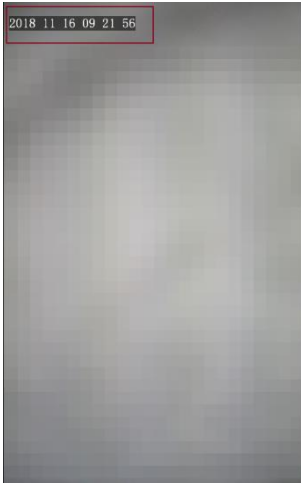
Date Format: dd/MM/yyyy (Legend: dd=Day; dddd=Day of the week; M=Month; y=Year)

Time Format: HH:mm:ss (Legend: h/H=12/24 Hour; tt=A.M. or P.M.; mm=Minute; ss=Second)

- Select the position and content of the OSD.
  - Position: Click the box of an area on the preview screen. After the cursor changes to a movable status icon, hold down and drag the mouse to select the position.
  - Overlay OSD Content: The drop-down list provides **Time**, **Preset** and **Serial Info**. You may also select **Custom** and enter the content you want.
  - After you have set the position and OSD content, the ✓ symbol appears in the **Status** column, which means that the OSD is set successfully. You may set multiple lines of contents for each area and use ^ and v to adjust the sequence of display.
- After you have completed the settings, a message appears to indicate the successful settings.

To cancel OSD for an area, clear the OSD content in the **Overlay OSD Content** column or select **None** in the **Position** column.

The following shows an example time OSD.





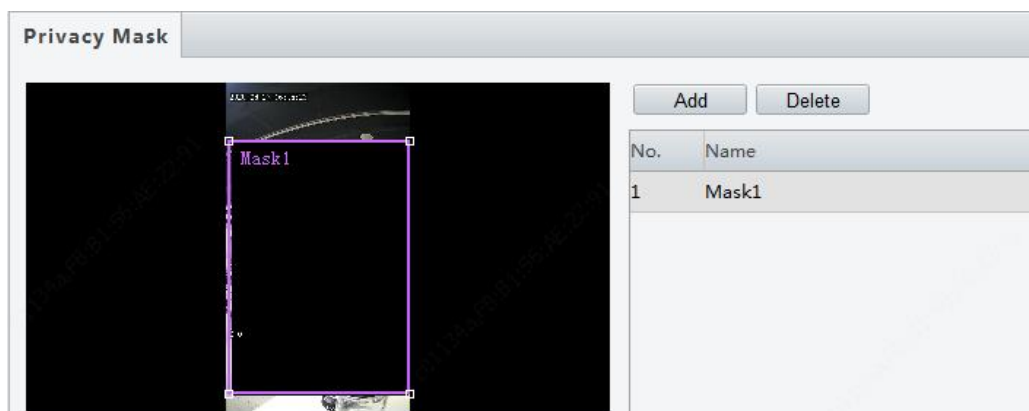
**NOTE!**

Currently, the OSD configuration is not displayed on the GUI of the face recognition terminal.

### 3. Privacy Mask

The device supports privacy mask and allows user to cover certain areas (such as sensitive or private areas) on the image for privacy protection.

- Add a mask area
  - (1) Choose **Setup > Image > Privacy Mask**, click **Add**. A solid black box appears on the left-side preview image.
  - (2) You can adjust the mask area by dragging or resizing the box:
    - On the preview image, drag the mask area to the desired location on the image.
    - To resize the mask area, place the mouse cursor on a border of the box, and when the cursor shape changes to  , drag the border to resize the mask area, or place the cursor on a corner of the box, and when the cursor shape changes to  , drag to resize the box.



- Delete a mask area

Choose a mask area on the left-side preview image, or select a row from the right-side list, and then click **Delete**. The corresponding mask area is deleted.

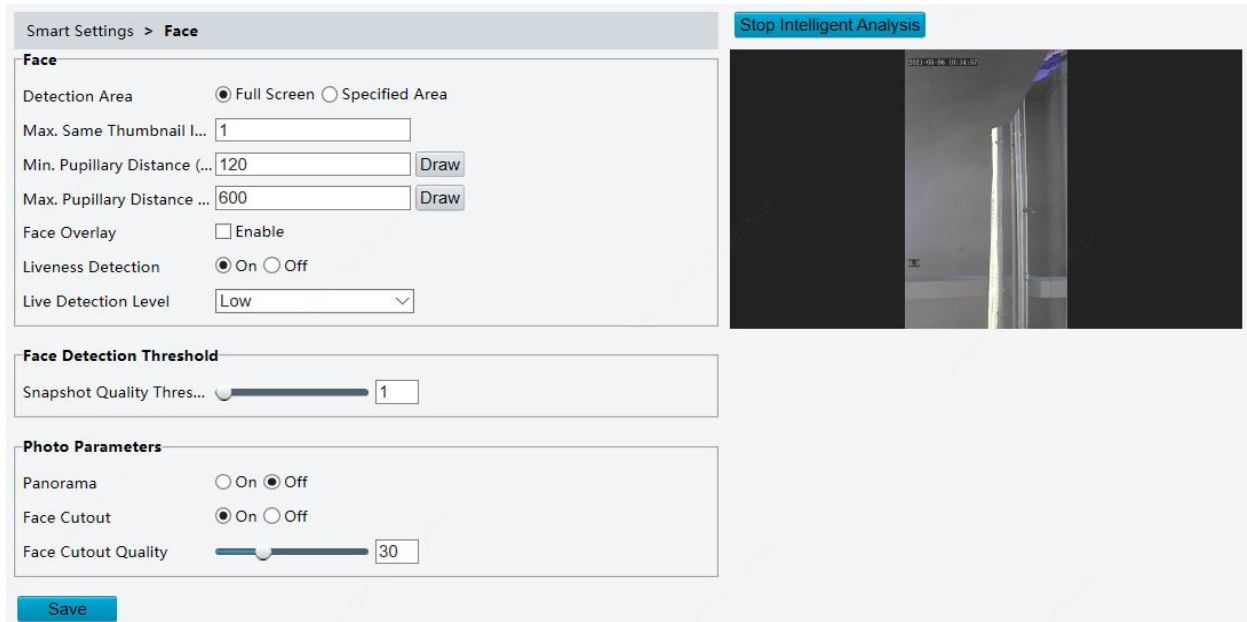
## 7.3.4 Intelligent

### 1. Face

Face snapshot configuration includes the configuration of face detection, face detection threshold, filter by object size (px), and other parameters. Proper parameter configuration is conducive to face detection and match.

(1) Choose **Setup > Intelligent > Face** and click the **Face** tab.

Figure 7-36 Face Snapshot Configuration Interface



(2) Set parameters by referring to the table below.

Intelligent analysis is enabled on the system by default. To modify parameters on the interface, click **Stop Intelligent Analysis** to stop intelligent analysis and then set parameters.

Table 7-18 Parameter Description

Pane	Parameter	Description
Face	Detection Area	<ul style="list-style-type: none"> <li>Click <b>Full Screen</b>, indicating that the full-screen face photo will be detected.</li> <li>Click <b>Specified Area</b>, indicating that face photo of a specified area will be detected.</li> </ul>
	Max. Same Thumbnail Images	The configuration is not supported.
	Min. Pupillary Distance (px)/ Max. Pupillary Distance (px)	You can draw the pupillary distances by using the mouse in the live view on the right side of the interface. A photo will be collected when the quantity of pupillary distance pixels is within these two preset values. The value range is 20 px to 650 px.
	Face Overlay	The configuration is not supported.
	Liveness Detection	Click <b>On</b> to enable the liveness detection function. Liveness detection can effectively prevent video and photo counterfeits. It is enabled by default.
	Live Detection Level	There are three liveness detection levels: <b>High</b> , <b>Medium</b> , and <b>Low</b> . A higher liveness detection level indicates a higher accuracy that non-real people can be detected. The default value is <b>Low</b> .
Face Detection Threshold	Snapshot Quality Threshold	Threshold for 1:N match on face snapshots. When the face match similarity reaches the preset similarity threshold, the match is successful.

Pane	Parameter	Description
		Value range: [1–100]; default value: 1 Note: After mask detection is enabled, <b>Snapshot Quality Threshold</b> must be set to 1.
Photo Parameters		<ul style="list-style-type: none"> <li>When <b>Panorama</b> is set to <b>On</b>, the face recognition terminal will save snapshot panorama photos. When <b>Panorama</b> is set to <b>Off</b>, the terminal will not save such photos. It is set to <b>On</b> by default.</li> <li>When <b>Face Cutout</b> is set to <b>On</b>, face photos will be cut out from snapshot photos. When <b>Face Cutout</b> is set to <b>Off</b>, face photos will not be cut out from snapshot photos. It is set to <b>On</b> by default.</li> <li>Snapshot Quality: The value determines the quality of snapshot photos. A larger value indicates that snapshot photos are clearer and vice versa.</li> <li>Face Cutout Quality: This parameter is displayed only when <b>Face Cutout</b> is set to <b>On</b>. The value determines the quality of face cutouts. A larger value indicates that face cutouts are clearer and vice versa.</li> </ul>

(3) Click **Save** to complete the configuration.

(4) Click **Start Intelligent Analysis** to enable intelligent analysis.

## 2. Check Template

A check template supports time range-based authentication modes and a maximum of eight time ranges can be set for a day (the time ranges cannot be overlapped). The authentication mode can be separately set for each day or copied to all days.

Figure 7-37 Check Template

- Adding a check template



### NOTE!

A maximum of 16 check templates can be set.

(1) Choose **Setup > Intelligent > Check Template** and click **Add**.

(2) Set parameters in the right pane of the interface.

- **Template Name:** Enter the name of a check template.
- Time range and authentication mode

Set the authentication mode for each time range in a week based on actual conditions. There are four authentication modes available:

- ◆ Card: The face recognition terminal conducts 1:N match on the acquired IC card number and the card numbers in the library.
- ◆ Face: The face recognition terminal conducts 1:N match on the face snapshot photo and face photos in the library.
- ◆ Card+Face: The face recognition terminal conducts 1:N match on the acquired IC card number and the card numbers in the library, and then conducts 1:1 match on the face photo corresponding to the card number and the snapshot photo.
- ◆ Password: The terminal allows users to enter correct "unit No.#room No.#room password" to open the door.

An authentication mode is used to configure the method for people to pass through the terminal. There are four authentication modes available in total. Users can select at least one but no more than three authentication modes based on actual requirements. When multiple authentication modes are adopted, the authentication modes are in an "OR" relationship, that is, the door is open when a person passes the authentication in any of the modes.

➤ Copying time ranges and authentication modes

- ◆ After setting time ranges and authentication modes for Monday, if the same time ranges and authentication modes are required for Tuesday to Sunday, select the check box in front of **Select All** to copy them to all days.
- ◆ If the same time ranges and authentication modes are required only for some days, select specific days and click **Copy**.

(3) Click **Save** to save the added check template.

- Modifying a check template

To modify an existing check template, select it, modify desired parameters, and click **Save** to complete the modification of the check template.

- Deleting a check template

(1) Choose **Setup > Intelligent > Check Template** and select the check template to be deleted.

(2) Click **Delete**.

(3) In the displayed confirmation box, click **OK** to delete it.

### 3. Time Template

You can set a time template to limit the time for people to go inside or outside. When a person is authenticated outside the time template (arming time), "non-specified time" will be reported. The time template can be set by week and a maximum of eight arming time ranges can be set for a day. Exception dates can be set separately but only by day.

Figure 7-38 Time Template

- Adding a time template



**NOTE!**

A maximum of 16 time templates can be set.

- (1) Choose **Setup > Intelligent > Time Template** and click **Add**.
- (2) Set parameters in the right pane of the interface.
  - **Template Name:** Enter the name of a time template. Requirements: 1–20 characters, with upper- and lower-case English letters, digits, hyphens, and underscores supported.
  - **Enable Plan:** Select the check box to enable the arming plan.
  - Set the arming time range.

- ◆ Click  Armed  Unarmed and drag the mouse on the time table to set the arming time range. The time accuracy is 1 hour.

Figure 7-39 Time Table for Dragging the Mouse to Set the Arming Time Range

	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
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

- ◆ You can also click  to go to the **Edit** interface, on which you can set arming time for a week.

A maximum of eight arming time ranges can be set for a day. The time ranges cannot be overlapped. A recognition success prompt is displayed only when the authentication succeeds in the preset arming time ranges. The prompt "non-specified time" is displayed when the authentication is successful out of the arming time ranges.

After setting arming time for a day, you can copy the arming time to other days.

Figure 7-40 Edit Interface

No.	Start Time	End Time
1	00:00:00	23:59:59
2		
3		
4		
5		
6		
7		
8		

Copy To  Select All  
 Mon  Tue  Wed  Thu  Fri  Sat  Sun

Copy OK Cancel

- **EnableException Date:** Select the check box to enable exception dates.
- Set an exception date.

Exception dates must be set based on dates and not time ranges on a day.

An exception date can be added, deleted, or modified. The prompt "non-specified time" is displayed when the authentication is successful on an exception date.

Figure 7-41 EnableException Date

EnableException Date

Add

No.	Date	Time Interval	Operation
1	2020-03-10	00:00:00--23:59:59	

(3) Click **Save** to save the added time template.

- Modifying a time template

To modify an existing time template, select it, modify desired parameters, and click **Save** to complete the modification of the time template.

- Deleting a time template

(1) Choose **Setup > Intelligent > Time Template** and select the time template to be deleted.

(2) Click **Delete**.

(3) In the displayed confirmation box, click **OK** to delete it.



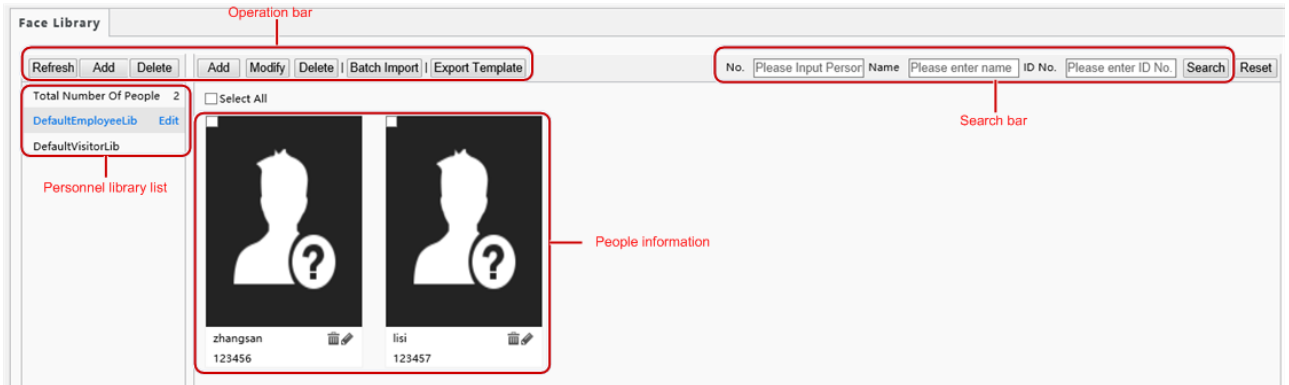
**NOTE!**

If a person is bound to a time template, you need to unbind the person before deleting the time template. Otherwise, a prompt, indicating that deletion failed and you are required to unbind the person first, is displayed when you delete it.

**4. Face Library**

Choose **Setup > Intelligent > Face Library**. On the **Face Library** interface, you can add a face library and add people to a face library.

Figure 7-42 Face Library Interface



**4B. Face library management**

- Adding a face library



**NOTE!**

A maximum of 16 face libraries can be set.

- (1) Above the personnel library list, click **Add**.
- (2) On the displayed **Add Face Library** interface, configure face library information by referring to the table below.

Figure 7-43 Add Face Library Interface

**Add Face Library** ✕

Face Library Type:

Face Library Name:

Check Template:

1:N Match Threshold:

**Verify Success Linkage Configuration**

Open door  
  Light Prompt  
  Voice Prompt  
  HMI Prompt  
  Wiegand Output

**Verify Failure Linkage Configuration**

Light Prompt  
  Voice Prompt  
  HMI Prompt



Table 7-19 Parameter Description

Parameter	Description
Face Library Type	Set the parameter to either of the following options based on actual conditions: <ul style="list-style-type: none"> <li>Employee Library</li> <li>Visitor Library</li> </ul>
Face Library Name	Enter a library name of 1 to 63 characters.
Check Template	Select a check template from the drop-down list. Check templates are added on the <a href="#">Check Template</a> interface.
1:N Match Threshold	The 1:N match is adopted in face recognition. When the match similarity reaches the threshold set here, the authentication succeeds.
Verify Success Linkage Configuration	Open door: After the authentication succeeds, a door opening signal is sent to trigger door opening. Light Prompt: A light prompt is played after the authentication succeeds. Voice Prompt: A voice prompt is played after the authentication succeeds. HMI Prompt: A prompt is displayed on the GUI after the authentication succeeds. Wiegand Output: Data is output through the Wiegand interface after the authentication succeeds.
Verify Failure Linkage Configuration	Light Prompt: A light prompt is played after the authentication fails. Voice Prompt: A voice prompt is played after the authentication fails. HMI Prompt: A prompt is displayed on the GUI after the authentication fails.

- Modifying a face library
  - Select a required face library and click **Edit**.
  - In the displayed **Edit Face Library** interface, modify parameters by referring to the description in [Face library management](#).

Figure 7-44 Edit Face Library Interface

- Click **OK** to complete the modification.
- Deleting a face library
    - Select a required face library and click **Delete**.
    - In the displayed confirmation box, click **OK** to delete the face library.  
 Deleting a face library will delete people in the face library.

#### 4C. Personnel management

- Adding persons

Persons can be added one by one or be imported in batches.


- Adding a person

- (1) Choose **Setup > Intelligent > Face Library** and select the face library to which persons are to be added.
- (2) On the personnel list bar, click **Add**.
- (3) On the displayed **Add Face Info** interface, configure person information by referring to the table below.

Figure 7-45 Add Face Info Interface

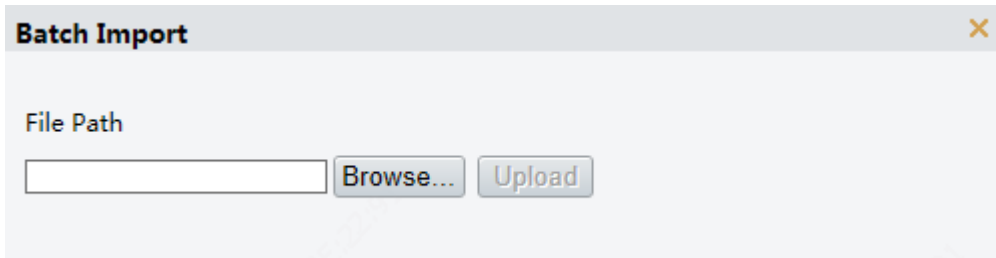
Table 7-20 Parameter Description

Pane	Parameter	Description
Basic Info	No.	It is required. Enter the No. of a person. Requirements: 1–15 characters, with upper- and lower-case English letters, digits, hyphens, and underscores supported.
	Name	It is required. Enter the name of the person.
	CardType1/CardType2 CardNo.1/CardNo.2	Select a card type and then enter the card No. The options of the card type include IC card, ID card, and none.
	Comment	Enter remarks for the person.
Photo	/	Click <b>Local Upload</b> . On the displayed interface, select a local face photo for uploading.

Pane	Parameter	Description
		Photo requirements: Only .jpg photos with the size of 10 KB to 512 KB are supported.
Time Template	EffectiveTime	Select a time template and then set the effective time and expiration time of the time template.
	ExpirationTime	Select the check box in front of a time template based on the actual situation.
	Time Template	 <b>NOTE!</b> <ul style="list-style-type: none"> <li>When multiple time templates are bound, the union of the time templates is taken during authentication.</li> <li>If a bound time template is not within the range of effective time to expiration time, the prompt "non-specified time" is displayed after successful authentication.</li> </ul>

- (4) Click **OK** to complete the adding.
- o Importing personnel information in batches
  - (1) Choose **Setup > Intelligent > Face Library** and select the face library to which persons are to be added.
  - (2) Click **Export Template** to download an import template to the local device.
  - (3) Decompress the template. In the import table, enter information according to requirements.
  - (4) Click **Batch Import** to upload the import table.

Figure 7-46 Batch Import



If information about a person fails to be imported, check the failure cause in the description column, modify information, and then import the person information again.

- Modifying person information
  - (1) Select the check box in the upper left corner of a person whose information need to be modified.
  - (2) Click the edit button as shown in the figure below.

Figure 7-47 Edit Interface



(3) On the displayed edit interface, modify person information by referring to [Personnel management](#).

(4) Click **OK** to complete the modification.

- Deleting persons

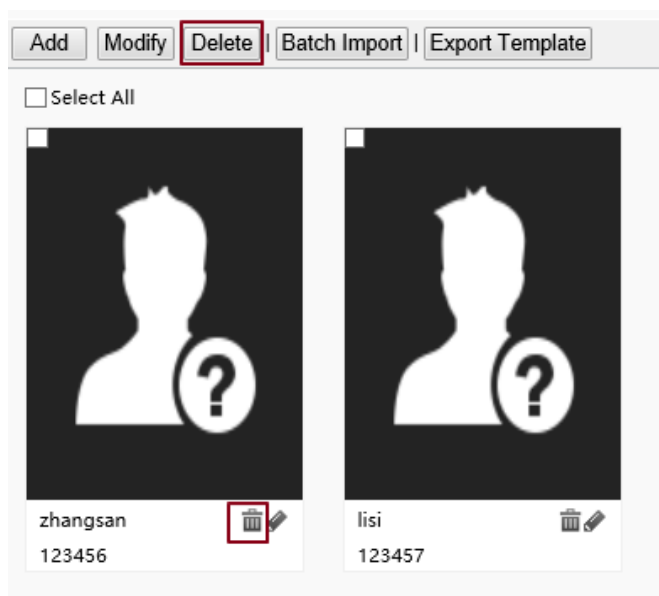
Persons can be deleted one by one or together.

- Deleting a person

(1) Select the check box in the upper left corner of a person to be deleted.

(2) Click the **Delete** button as shown in the figure below.

Figure 7-48 Delete Interface

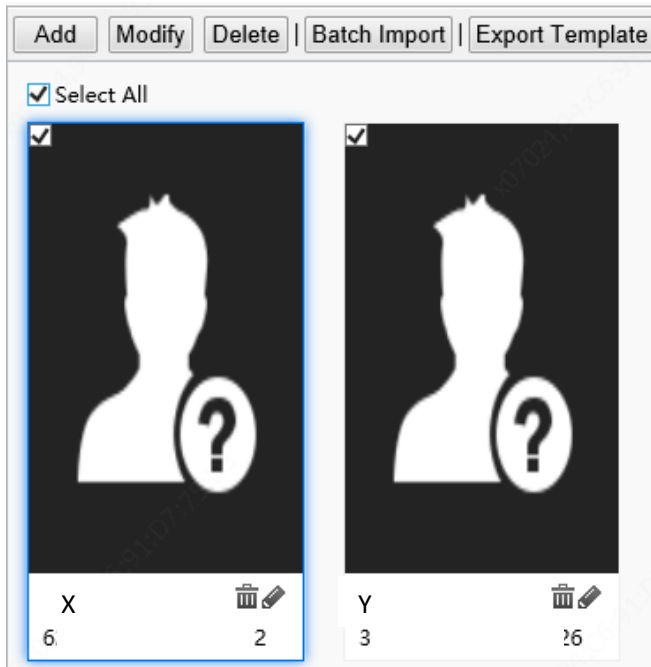


(3) In the displayed deletion confirmation box, click **OK** to complete the deletion.

- Deleting all persons

(1) Select the check box in front of **Select All**.

Figure 7-49 Selecting All Persons



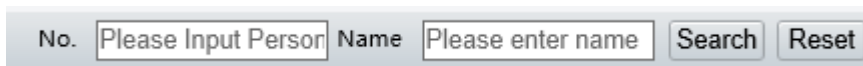
(2) Click **Delete** or .

(3) In the displayed confirmation box, click **OK** to complete the deletion.

- Searching for a person

You can search for personnel information by No.or name.

Figure 7-50 Search Box



### 5. Advanced Setting

Choose **Setup > Intelligent > Advanced Setting**.

Set parameters by referring to the table below.

Figure 7-51 Advanced Setting Interface

**Advanced Setting**

Door Opening Mode  Authentication  Face  Remote

QR Code Detection  Off  On (Note: Require card authentication)

QR Code Protocol  Private  Third Party

Call Mode

---

**Record Upload Settings**

Reporting Type

---

**Record Storage Settings**

Backup Storage  On  Off

Record Maintenance

---

**Attribute Rule Configuration**

**Safety Helmet**

Authentication Failed A...  Off  On

---

**Mask**

Authentication Failed A...  Off  On

---

**Temperature Measurement**

Temperature Measur...  Measure Forehead Temperature  Measure Wrist Temperature  Measure Forehead / Wrist Temperature

Authentication Failed A...  Off  On

Authentication success ...  Off  On

Temperature Unit

Temperature Measur...  ~

Temperature Alarm Thr...

Temperature Alert  Off  On

---

Temperature Alert Offset  (Temperature Alert Threshold = Temperature Alarm Threshold - Temperature Alert Offset)

Detection interval time  s

---

**Health question**

Open the door even wh...  Off  On

Trigger alarm when une...  Off  On

Visitor's name&snapshot  Disable  Enable

Title

Question set

Question1	<input type="text"/>	Expected answer <input checked="" type="radio"/> Yes <input type="radio"/> No
Question2	<input type="text"/>	Expected answer <input checked="" type="radio"/> Yes <input type="radio"/> No
Question3	<input type="text"/>	Expected answer <input checked="" type="radio"/> Yes <input type="radio"/> No
Question4	<input type="text"/>	Expected answer <input checked="" type="radio"/> Yes <input type="radio"/> No
Question5	<input type="text"/>	Expected answer <input checked="" type="radio"/> Yes <input type="radio"/> No

Pop up message when ...  Off  On

---

Temperature Measur...  Off  On

---

**Alarm Output Configuration**

High Temperature Alarm  Off  On

Not Wearing Mask Alarm  Off  On

Authentication Failure A...  Off  On

---

**Mail Linkage Configuration**

High Temperature  Off  On

Not Wearing Mask  Off  On

Not Wearing Helmet  Off  On

Authentication Failure  Off  On

[Save](#)

Table 7-21 Parameter Description

Parameter		Description
Door Opening Mode		<ul style="list-style-type: none"> <li>Authentication: After <b>Door Opening Mode</b> is set to <b>Authentication</b>, the terminal generates the door opening signal only after a person passes the authentication in <a href="#">Check Template</a>.</li> <li>Face: After <b>Door Opening Mode</b> is set to <b>Face</b>, the terminal generates the door opening signal when detecting a face snapshot photo. If a whitelist library is configured, face match will be conducted on whitelisted personnel and success prompts will be provided. No prompt will be given on the GUI when non-whitelisted personnel have their faces scanned.</li> <li>远程: 当配置为远程时, 终端不进行本地核验开门, 统一将抓拍图片上报人脸速通门管理平台或第三方平台, 平台根据核验结果, 远程控制终端开门。</li> </ul> <p>Set this parameter based on actual application scenes.</p>
QR Code Detection		<ul style="list-style-type: none"> <li>On: When it is set to <b>On</b> and IC card is contained in <a href="#">Check Template</a>, the camera of the terminal will collect QR code data and authentication will be conducted.</li> <li>Off: When it is set to <b>Off</b>, the camera of the terminal will not collect QR code data.</li> </ul> <p>Set this parameter based on actual application scenes.</p>
QR Code Protocol		<ul style="list-style-type: none"> <li>Private When it is set to <b>Private</b>, the face recognition terminal will parse QR code data locally (this protocol is applicable when a camera or QR code scanner is used for collection).</li> <li>Third Party The configuration is not supported.</li> </ul>
Call Mode		The configuration is not supported.
Record Upload Settings	Reporting Type	<ul style="list-style-type: none"> <li>Upload All: Upload local authentication records to EZStation in real time.</li> <li>Upload Success Record: Upload local authentication success records to EZStation in real time.</li> </ul> <p>For detailed operation instructions of EZStation, see EZStation user manual.</p>
Record Storage Settings	Backup Storage	<p>When it is set to <b>On</b>, the terminal will store records on the local memory card.</p> <p>When the option is switched, the terminal will clear local storage and restart.</p> <p>The default value is <b>Off</b>.</p>
Attribute Rule Configuration	Safety Helmet	<p>Authentication Failed And Open The Door</p> <p>On: When a person without a safety helmet is detected, the terminal will display a message “please wear a safety helmet” on the screen and play this message in audio, and the door will open.</p> <p>Off: When a person without a safety helmet is detected, the terminal will display a message “please wear a safety helmet” on the screen and play this message in audio, and the door will not open.</p> <p>The default value is <b>Off</b>.</p>

Parameter		Description
Mask	Authentication Failed And Open The Door	<p>On: When a person without a mask is detected, the terminal will display a message “please wear a mask” on the screen and play this message in audio, and the door will open.</p> <p>Off: When a person without a mask is detected, the terminal will display a message “please wear a mask” on the screen and play this message in audio, and the door will not open.</p> <p>The default value is <b>Off</b>.</p>
	Temperature Measurement	<ul style="list-style-type: none"> <li>• Measure Forehead Temperature: The forehead temperature will be measured.</li> <li>• Measure Wrist Temperature: The wrist temperature will be measured.</li> <li>• Measure Forehead / Wrist Temperature: The terminal can measure either forehead temperature or wrist temperature.</li> </ul> <p>Do not need configuration. Terminal will automatically match the temperature measurement mode when it is connected to the digital detection module.</p>
Temperature Measurement	Authentication Failed And Open The Door	<p>On: When a temperature over the preset temperature alarm threshold is detected, the terminal will display a message “abnormal temperature” on the screen and play this message in audio, and the door will open.</p> <p>Off: When a temperature over the preset temperature alarm threshold is detected, the terminal will display a message “abnormal temperature” on the screen and play this message in audio, and the door will not open.</p> <p>The default value is <b>Off</b>.</p>
	Authentication Success At Low Temperature	<p>On: When a temperature below the minimum temperature of the measurement range is detected, the terminal will display a message “low temperature” on the screen and play this message in audio, and the door will open.</p> <p>Off: When a temperature below the minimum temperature of the measurement range is detected, the terminal will display a message “low temperature” on the screen and play this message in audio, and the door will not open.</p> <p>The default value is <b>Off</b>.</p>
	Temperature Unit	<p>The options are as follows:</p> <ul style="list-style-type: none"> <li>• °C</li> <li>• °F</li> </ul> <p>Set the temperature unit based on actual conditions.</p>
	Temperature Measurement Range	<p>Value range: [30–45]; default range: [35.5–42]</p> <p>Set the range based on actual conditions.</p>
	Temperature Alarm Threshold	<p>When a temperature over the threshold configured here is detected, the terminal will display a message “abnormal temperature” on the screen and play this message in audio.</p> <p>Value range: [30–45]; default value: 37.3</p>
	Temperature Alert	<p>After this function is turned on, when body temperature is within the range of temperature alert threshold and temperature alarm threshold, high temperature alarm will be given to remind people to re-detect.</p> <p>The default value is <b>Off</b>.</p>
	Temperature Alert Offset	<p>Temperature Alert Threshold = Temperature Alarm Threshold = Temperature Alert Offset</p>



Parameter		Description
	Detection Interval Time	The digital detection module detects temperatures at intervals, the detection results within the interval time will be filtered. The default value is <b>7s</b> .
Health question	Open The Door Even When Unexpected Answer Detected	On: When the face recognition terminal detects an unexpected answer, the door will open. Off: When the face recognition terminal detects an unexpected answer, the door will not open, and the visitor need to perform face recognition and answer questions again or contact relevant personnel on site. The default value is <b>Off</b> .
	Trigger Alarm When Unexpected Answer Detected	On: The terminal will sound an alarm when it detects an unexpected answer. Off: The terminal will not sound an alarm when it detects an unexpected answer. The default value is <b>On</b> .
	Visitor's Name & Snapshot	After this function is turned on, when a person has his face scanned, his name and snapshot will be displayed on the GUI. If the person's information is not stored in the library, the GUI will only show his snapshot. The default value is <b>Disable</b> .
	Question Set	Set health questions displayed on the screen when the face recognition terminal performs face recognition and temperature detection and your expected answer of Yes or No. Up to 5 questions are allowed. Please set the questions based on actual conditions.
	Pop up Message When Unexpected Answer Detected	After this function is turned on, when an unexpected answer is detected, the terminal will display a pop-up message on the screen, please wait for a few seconds to close it. The default value is <b>Off</b> .
Temperature Measurement Timeout Strategy		After this function is turned on, when a person has the face scanned and remained in the live view but not the temperature taken for 10s, the GUI and the warning sound prompt temperature measurement timeout. The default value is <b>On</b> .
Alarm Output Configuration	High Temperature Alarm	After this function is turned on, the terminal will output a high temperature alarm when it detects a high temperature. The default value is <b>Off</b> .
	Not Wearing Mask Alarm	After this function is turned on, the terminal will output a not wearing mask alarm when it detects a person not wearing mask. The default value is <b>Off</b> .
	Authentication Failure Alarm	After this function is turned on, the terminal will output an authentication failure alarm when face and card authentication failed. The default value is <b>Off</b> .
Mail Linkage Configuration Please configure the email first before using this function (see <a href="#">E-mail</a> )	High Temperature	After this function is turned on, the terminal will send a high temperature alarm to the specified email address when it detects a high temperature. The default value is <b>Off</b> .
	Not Wearing Mask	After this function is turned on, the terminal will send a not wearing mask alarm to the specified email address when it detects a person not wearing mask.

Parameter		Description
		The default value is <b>Off</b> .
	Not Wearing Helmet	After this function is turned on, the terminal will send a not wearing helmet alarm to the specified email address when it detects a person not wearing helmet. The default value is <b>Off</b> .
	Authentication Failure	After this function is turned on, the terminal will send an authentication failure alarm to the specified email address when face and card authentication failed. The default value is <b>Off</b> .

## 6. Recognition Result Display

The **Recognition Result Display** interface allows you to configure whether a person's registered picture and name need to be displayed on the terminal interface after face recognition succeeds.

(1) Choose **Setup > Intelligent > Recognition Result Display** and click the **Display Recognition Result** tab.

Figure 7-52 Recognition Result Display Interface

(2) Configure recognition result display by referring to the table below.

Table 7-22 Parameter Description

Parameter		Description
Display Recognition Result	Display Image	<ul style="list-style-type: none"> <li>Images: The face recognition terminal displays a person's registered picture after face recognition succeeds.</li> <li>Snapshot: The face recognition terminal displays a person's captured snapshot after face recognition succeeds.</li> <li>Hide: The face recognition terminal does not display a person's registered picture after face recognition succeeds.</li> </ul>
	Display Image County	<ul style="list-style-type: none"> <li>Single Face: The GUI displays only information about the identified person after face recognition succeeds.</li> </ul>

Parameter		Description
		<ul style="list-style-type: none"> <li>Multiple Faces: The GUI displays information about multiple identified persons after face recognition succeeds. Information about recent five persons identified successfully can be displayed at most. Information about the latest person identified successfully is displayed on the left of the screen.</li> </ul> <p>It is set to <b>Single Face</b> by default.</p>
	Name	<ul style="list-style-type: none"> <li>Default: The face recognition terminal displays a person's name after face recognition succeeds.</li> <li>Encrypt Display: The face recognition terminal encrypts a person's name and displays only partial information after face recognition succeeds.</li> <li>Custom: The face recognition terminal displays information defined here rather than a person's name after face recognition succeeds. A string of 0–10 characters can be entered in the custom box.</li> </ul>
	Extended Info	<ul style="list-style-type: none"> <li>Display Time: The face recognition terminal displays the current system time.</li> <li>Remarks: The face recognition terminal displays a person's remarks after face recognition succeeds.</li> <li>Hide: The face recognition terminal displays neither time nor a person's remarks after face recognition succeeds.</li> </ul>
Recognition Result Message		<ul style="list-style-type: none"> <li>Default: The face recognition terminal displays "Identified successfully" after face recognition succeeds.</li> <li>Custom: The face recognition terminal displays information defined here after face recognition succeeds.</li> </ul>
Temperature Measurement Count		<ul style="list-style-type: none"> <li>Display: The face recognition terminal displays the total number of people with temperature taken and the number of people with normal temperature.</li> <li>Hide: The face recognition terminal does not display the total number of people with temperature taken and the number of people with normal temperature.</li> </ul>
IP Address		<ul style="list-style-type: none"> <li>Display: The face recognition terminal displays the IP address of the terminal.</li> <li>Hide: The face recognition terminal does not display the IP address of the terminal.</li> </ul>
Measurement Illustration		<ul style="list-style-type: none"> <li>Display: When the temperature measurement function is enabled, the face recognition terminal guides wrist temperature measurement.</li> <li>Hide: When the temperature measurement function is enabled, the face recognition terminal does not guide wrist temperature measurement.</li> </ul>
Temperature reminder		<ul style="list-style-type: none"> <li>Display: The GUI shows the measured temperature.</li> <li>Hide: The GUI does not show the measured temperature.</li> </ul>
Temperature parameter		<ul style="list-style-type: none"> <li>Display: The bottom status bar on the GUI shows the measured temperature and the time when the temperature is measured.</li> <li>Hide: The bottom status bar on the GUI does not show the measured temperature and the time when the temperature is measured.</li> </ul>
Temperature result font size		<ul style="list-style-type: none"> <li>Small: The GUI shows temperature results in small fonts.</li> <li>Medium: The GUI shows temperature results in medium fonts.</li> <li>Large: The GUI shows temperature results in large fonts.</li> </ul>

(3) Click **Save** to complete the configuration.

### 7.3.5 Events

You can set alarm arming to implement alarm reporting. By configuring triggered actions of other devices, an alarm can trigger one or more types of actions, so that the users handle the alarm and the corresponding actions in time.

Alarm arming includes fire alarms, anti-disassembly alarms, and door magnet alarms.

#### 1. Fire alarms

When the face recognition terminal connects to a fire alarm device, the terminal will generate a fire alarm record when a fire alarm occurs.

- (1) Choose **Setup > Events > Events** and then click **Fire Alarm**.

Figure 7-53 Fire Alarm Configuration Interface

Alarm Name: 1

Alarm ID:

Alarm Type: N.O.

Alarm Input:  On  Off

**Trigger Actions**

Trigger E-mail  Snapshot  Open door

**Enable Plan**

Armed  Unarmed

	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
Mon																									
Tue																									
Wed																									
Thu																									
Fri																									
Sat																									
Sun																									

- (2) Set fire alarm information.
  - a. Select alarm and set the alarm name.
  - b. Select **N.O.** or **N.C.** according to the type of the third-party alarm input device. For example, if the third-party alarm input device is normally open, you need to select **N.O.** here, so that the camera can receive alarm information from the third-party alarm input device.
  - c. Select whether to enable Alarm Input. If **Alarm Input** is set to **On**, the terminal will receive alarms from the fire alarm device. If it is set to **Off**, the terminal will not receive alarms from the fire alarm device.

- (3) Set actions to be associated with fire alarms.

Fire alarms can be associated with terminal snapshot and door opening actions. Select whether to enable the two functions based on actual scenes.

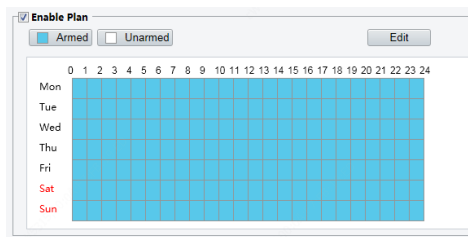
火灾警报可以与邮件触发、终端抓拍和开门功能相联动，根据实际场景选择这三项功能是否开启。

- (4) Set whether to enable the arming schedule.

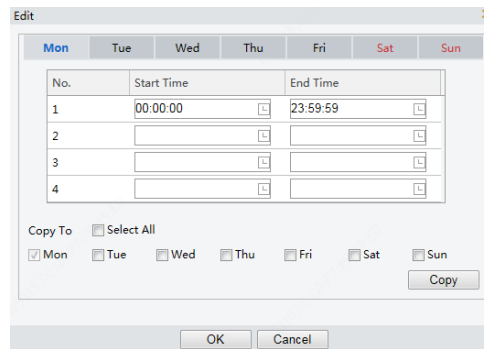
Select the **Enable Plan** check box and set the start time and end time of alarms (click **Edit**). The time ranges cannot be overlapped. The device outputs alarm signals only within the preset valid time ranges.

The options of day include Monday to Sunday and the time of each day is defined using four time ranges.

After setting the plan time for one day, you can click **Copy** and then click **Paste** on another day to copy the plan time to other days.



Drawing Arming Time by Using the Mouse



Editing Tables to Set Arming Time

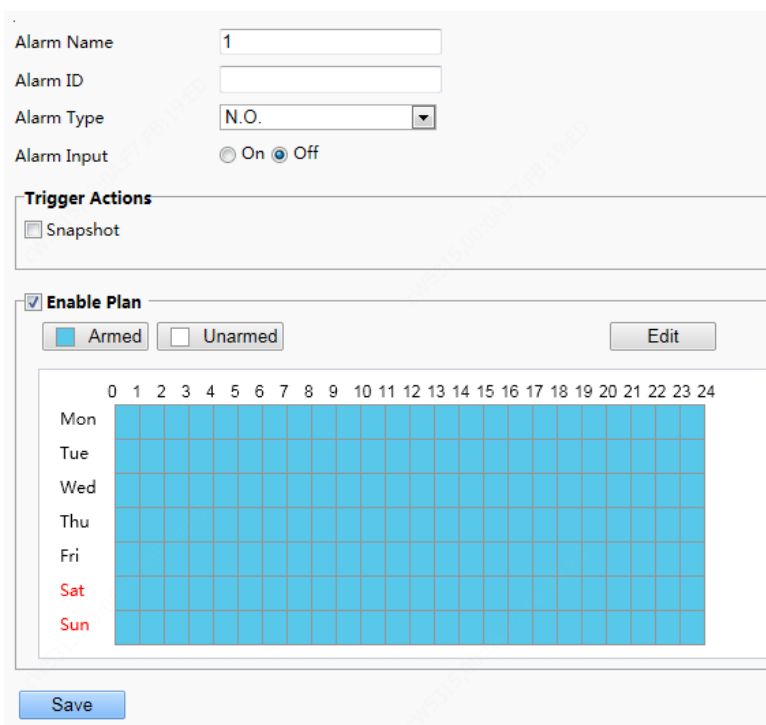
(5) Click **Save**.

## 2. Tamper Alarm

The face recognition terminal has a tamper button, which can input the tamper alarm to the terminal.

(1) Choose **Setup > Events > Events** and then click **Tamper Alarm**.

Figure 7-54 Tamper Alarm Configuration Interface



(2) Set basic information about tamper alarms.

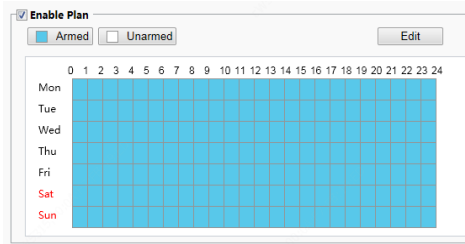
- 1) Select alarm and set the alarm name.
- 2) Select the alarm type. Set **Alarm Type** to **N.O.** or **N.C.** based on whether the tamper alarm input is of the normally open or normally closed type.
- 3) Select whether to enable alarm input. If **Alarm Input** is set to **On**, the terminal will receive anti-disassembly alarms. If it is set to **Off**, the terminal will not receive tamper alarms.

(3) Set actions to be associated with tamper alarms.

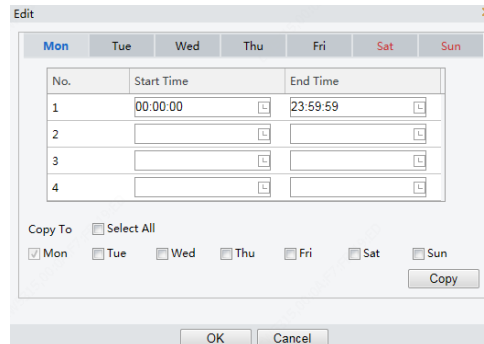
(4) Tamper alarms can be associated with the terminal snapshot action. Select whether to enable the function based on actual scenes.

Set whether to enable the arming schedule.

Select the **Enable Plan** check box and set the start time and end time of alarms (click **Edit**). The time ranges cannot be overlapped. The device outputs alarm signals only within the preset valid time ranges. The options of day include Monday to Sunday and the time of each day is defined using four time ranges. After setting the plan time for one day, you can click Copy and then click Paste on another day to copy the plan time to other days.



Drawing Arming Time by Using the Mouse



Editing Tables to Set Arming Time

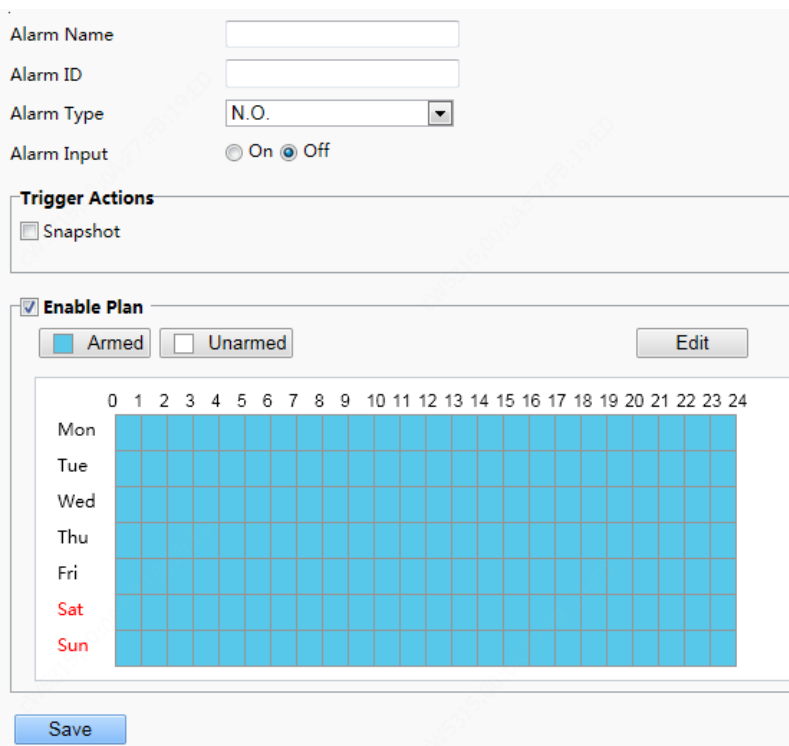
(5) Click **Save**.

### 3. Door magnet alarms

When the face recognition terminal connects to a door magnet, it can receive door magnet alarms.

(1) Choose **Setup > Events > Events** and then click **Door Magnet Alarm**.

Figure 7-55 Door Magnet Alarm Configuration Interface



(2) Set basic information about door magnet alarms.

- a. Select alarm and set the alarm name.
- b. Select the alarm type. Set **Alarm Type** to **N.O.** or **N.C.** based on whether the connected alarm input device is of the normally open or normally closed type. For example, for normally open alarm input devices, **Alarm Type** must be set to **N.O.** so that the face recognition terminal normally receives alarms from the connected device.

c. Select whether to enable alarm input. If **Alarm Input** is set to **On**, the terminal will receive door magnet alarms. If it is set to **Off**, the terminal will not receive door magnet alarms.

(3) Set actions to be associated with door magnet alarms.

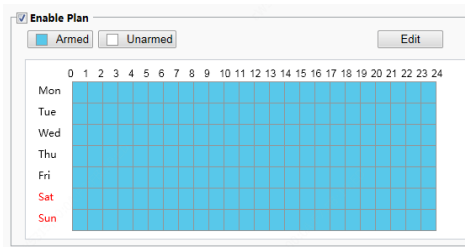
Door magnet alarms can be associated with the terminal snapshot action. Select whether to enable the function based on actual scenes.

(4) Set whether to enable the arming schedule.

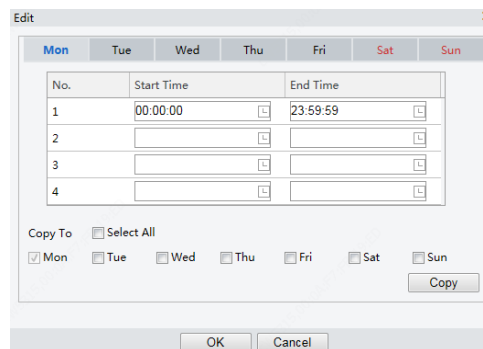
Select the **Enable Plan** check box and set the start time and end time of alarms (click **Edit**). The time ranges cannot be overlapped. The device outputs alarm signals only within the preset valid time ranges.

The options of day include Monday to Sunday and the time of each day is defined using four time ranges.

After setting the plan time for one day, you can click Copy and then click Paste on another day to copy the plan time to other days.



Drawing Arming Time by Using the Mouse



Editing Tables to Set Arming Time

(5) Click **Save**.

#### 4. Security Gate Alarm

When the face recognition terminal connects to a door magnet, it can receive security gate alarms.

(1) Choose **Setup > Events > Events** and then click **Security Gate Alarm**.

(2) Set basic information about security gate alarms.

a. Select alarm and set the alarm name.

b. Select the alarm type. Set **Alarm Type** to **N.O.** or **N.C.** based on whether the connected alarm input device is of the normally open or normally closed type. For example, for normally open alarm input devices, **Alarm Type** must be set to **N.O.** so that the face recognition terminal normally receives alarms from the connected device.

- c. Select whether to enable alarm input. If **Alarm Input** is set to **On**, the terminal will receive door magnet alarms. If it is set to **Off**, the terminal will not receive security gate alarms.
- (3) Set whether to send alarm emails when security gate alarms occur.
- (4) Click **Save**.

### 7.3.6 Storage

#### 1. Storage

Click **Setup > Storage > Storage**.



#### NOTE!

- Keep default values on the **Storage** interface. Configuration is forbidden.
- Formatting is forbidden.

**Storage**

Storage Medium    Enable

Storage Medium Status: Normal

Total Capacity 2839 MB, Free Space 1514 MB.

**Allocate Capacity**

Video(MB)  (The remaining capacity is used for image storage.)

Common Snapshot(MB)  (The remaining capacity is used for smart snapshot storage.)

Smart Snapshot(MB)

**Video Storage Info**

Storage Policy  Manual Storage  Off

Stream

When Storage Full  Overwrite  Stop

Post-Record(s)

#### 2. FTP

Use FTP to upload images to the FTP server in accordance with the set rules.

##### 2A. Smart

- (1) Choose **Setup > Storage > FTP** and then click **Smart**.
  - (2) Set parameters by referring to the table below
- Server Parameter

Parameter	Description
Server IP	Address of the FTP server for receiving images.
Port No	The default value is 21. Modify the value as needed.
Username	Username used to connect the FTP server.
Password	Password used to connect the FTP server.
Direction ID	Use the default setting.



Parameter	Description
Not Upload Pictures	No need to select
Custom Naming Rules	The filename allows custom fields when this option is selected.
Convert Path into UTF8 Format	No need to select.

- Snapshot Image

- Save To Root Directory

- Up to 4 directory levels are allowed.
    - The following naming elements can be configured for each level of directory.

Parameter	Description
IP Address	Use the face recognition device's IP address to name the folder.
Date	Use a short date (yyyyMMdd) to name the folder.
Device ID	Use the face recognition device's ID to name the folder.
Date+Hour	Use a long date (yyyyMMddhh) to name the folder.
Date-YYYY	Use year (yyyy) to name the folder.
Date-MM	Use month (MM) to name the folder.
Date-DD	Use date (dd) to name the folder.
Time-HourMin	Use time (hhmm) to name the folder.
Time-Hour	Use hour (hh) to name the folder.
Time-Min	Use minute (mm) to name the folder.
Custom	Customize a field. Choose Custom and then enter the desired content.

- Filename configuration

- Separator: used to connect the configured naming elements
    - The naming elements are described in the table below.

Parameter	Description
IP Address	Show the face recognition device's IP address.
Time	Show the time, including year, month, day, hour, minute and second.
Date	Show the date (yyyyMMdd).
ID Device ID	Show the face recognition device's ID.
Direction ID	Configuration is not supported.
Photo No	Auto-increment image sequence number.
Date+Hour	Show the year, month, day and hour (yyyyMMddhh).
Date-YYYY	Show the year (yyyy)
Date-MM	Show the month (MM).
Date-DD	Show the day (dd).
Time-HourMin	Show the hour and minute (hhmm).
Time-Hour	Show the hour (hh).

Parameter	Description
Time-Min	Show the minute (mm).
Time Sec	Show the second (ss)
Frame ID	Configuration is not supported.
4-Digit Random Number	A 4-digit number that is generated randomly.
Photo Total	Configuration is not supported.
Custom	Customize a field. Choose Custom and then enter the desired content. Please select <b>Custom Naming Rules</b> and then configure this parameter.

## 2B. General

The configuration is not supported.

## 7.3.7 Security

### 1. User

For user configuration, see [User](#).

### 2. Network Security

After security information transmission is set, you can establish an information security channel to ensure data transmission security.

#### 2A. HTTPS

Some interfaces support HTTPS, which can secure data transmission.

- (1) Click **Setup > Security > Network Security > HTTPS**.

Figure 7-56 HTTPS Setting Interface

- (2) Select **On** for **HTTPS**. You may import a custom SSL certificate as needed.
- (3) Click **Save**.

Next time you log in, enter the address in https://IP:HTTPS port number format, for example, https://192.168.1.13:443 to enter secure channel mode. If you use the default HTTPS port, enter https://IP.

#### 2B. RTSP Authentication

RTSP (Real Time Streaming Protocol) is an application layer protocol. To transmit and control the audio and video, set RTSP authentication on the Web interface.

- (1) Click **Setup > Security > Network Security > RTSP Authentication**.
- (2) Select an authentication mode.

Table 7-23 Parameter Description

Parameter	Description
RTSP Authentication	The options are <b>Basic</b> , <b>Digest</b> , and <b>None</b> . The default value is <b>Digest</b> .

Parameter	Description
HTTP Authentication	The options are <b>Digest</b> and <b>None</b> . The default value is <b>None</b> .

Figure 7-57 RTSP Authentication Setting Interface

- (3) Click **Save**.

## 2C. ARP Protection

This function protects a camera from ARP attacks. The gateway and the MAC address must be set properly before a PC can access the camera from another network; if an incorrect MAC is set, only PCs on the same LAN can access.

- (1) Click **Setup > Security > Network Security > ARP Protection**.

Figure 7-58 ARP Protection Setting Interface

- (2) Select the check box to enable the ARP binding function and set the gateway MAC address.
- (3) Click **Save**.

## 2D. IP Address Filtering

Use IP address filtering to allow or forbid access from specified IP address(es).



### NOTE!

This function is not supported by some models. Please see the actual model for details.

- (1) Click **Setup > Security > Network Security > IP Address Filtering**.

Figure 7-59 IP Address Filtering Setting Interface

- (2) Select **On** to enable IP address filtering.
- (3) Select a filtering mode, and then add IP address(es).

(4) Click **Save**.



**NOTE!**

- If Filtering Mode is set to Whitelist, then only the added IP address(es) are allowed to access the camera. If Filtering Mode is set to Deny Access, then only the added IP address(es) are not allowed to access the camera.
- Up to 32 IP addresses are allowed. Each IP address can be added once only.
- The first byte of each IP address must be 1-223, and the fourth cannot be 0. For example, the following IP addresses are illegal and cannot be added: 0.0.0.0, 127.0.0.1, 255.255.255.255, 224.0.0.1.

## 2E. Access Policy

(1) Click **Setup > Security > Network Security > Access Policy**.

(2) Select **On** to enable friendly password.

- Friendly Password: Login with a weak password is allowed when friendly password is enabled. When friendly password is disabled, login with a weak password is not allowed, and a strong password must be set before login is allowed.
- MAC Authentication: the configuration is not supported.

Figure 7-60 Access Policy Setting Interface

Friendly Password  On  Off

MAC Authentication  On  Off

**Save**

(3) Click **Save**.



**NOTE!**

Enabling friendly password does not affect use. If you turn it off and log in with a weak password, a page will pop up, prompting you to change the password. There is no Cancel or Close button on this page. The default password is treated as weak.

## 3. Registration Info

The configuration is not supported.

## 4. Watermark

The configuration is not supported.

## 7.3.8 System

### 1. Time

For time configuration, see [Time](#).

### 2. Server

For time configuration, see [Server](#).

### 3. Ports & Devices

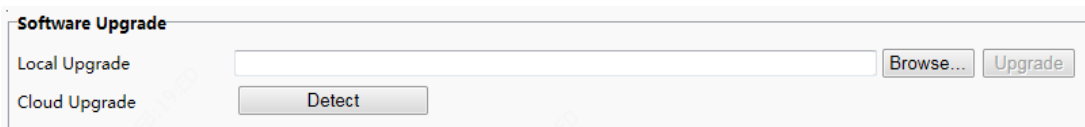
For the configuration of ports and devices, see [Ports & Devices](#).

### 4. Maintenance

#### 4A. Software Upgrade

- (1) Click **Setup > System > Maintenance**.

Figure 7-61 Local Upgrade Interface



The screenshot shows a 'Software Upgrade' window. Under 'Local Upgrade', there is a text input field, a 'Browse...' button, and an 'Upgrade' button. Under 'Cloud Upgrade', there is a 'Detect' button.

- (2) Under **Software Upgrade**, click **Browse** and select the correct upgrade file.
- (3) Click **Upgrade** and then confirm to start. The terminal will restart automatically after the upgrade is completed.



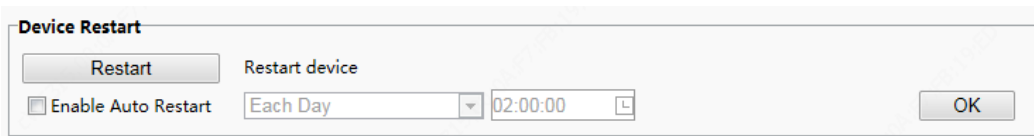
**NOTE!**

- You must use the correct upgrade file for you device. Otherwise, unexpected results may occur.
- The upgrade file is a ZIP file and must include all the necessary files.
- Ensure that the power supply is normal during upgrade. The device will restart after the upgrade is completed.

#### 4B. Device Restart

- (1) Click **Setup > System > Maintenance**.

Figure 7-62 Restart Configuration Interface



The screenshot shows a 'Device Restart' window. It contains a 'Restart' button, a 'Restart device' label, an 'Enable Auto Restart' checkbox, a dropdown menu set to 'Each Day', a time input field set to '02:00:00', and an 'OK' button.

- (2) Under **Device Restart**, click **Restart**. The device will restart after you confirm the operation.
- (3) You can select **Enable Auto Restart** and set the restart time point. Then, the device will automatically restart at the time point.



**CAUTION!**

Perform this operation with caution because restarting the system interrupts the ongoing service. It is recommended that the automatic restart time point of the device be set to idle time without ongoing services.

#### 4C. System Configuration

- Restoring factory defaults

When **Default** is clicked, all parameters are restored to factory defaults except the administrator login password, network port parameters, system time, admin password, and activation password.



**NOTE!**

After factory defaults are restored, a prompt asking you to change the activation password is displayed on the GUI.

- Restoring factory defaults completely

When **Restore all settings to defaults without keeping current network and user settings** is selected, all parameters are restored to factory defaults.

- Importing and Exporting System Configuration File

Export the current configurations of the camera and save them to the PC or an external storage medium. You can also quickly restore configurations by importing backup configurations stored on the PC or an external storage medium back to the camera.



### CAUTION!

- After you perform the Default operation, all settings are restored to factory defaults, except the following: login password of the system administrator, network settings, and system time.
- Make sure you import the correct configuration file for your camera. Otherwise, unexpected results may occur.
- The camera will restart when the configuration file is imported successfully.

- (1) Click **Setup > System > Maintenance**.

Figure 7-63 Import/Export Configuration Interface

**Config Management**

Restore all settings to defaults without keeping current network and user settings.

Importing

Exporting

- (2) To import configurations that you have backed up, click **Browse** next to the **Import** button and select the configurations you want to import, and then click **Import**. The result will be displayed.
- (3) To export current system configurations, click **Browse** (next to the **Exporting** field), set the destination and then click **Export**.
- (4) To restore default configurations, click **Default** and then confirm the operation. The device will restart and restore the default configurations. Clicking **Default** with the check box selected will completely restore the device to factory default settings.

#### 4D. Collecting Diagnosis Information

Diagnosis information includes logs and system configurations. You can export diagnosis information to your PC.

- (1) Click **Setup > System > Maintenance**.

Figure 7-64 Diagnosis Information Collection Interface

**Diagnosis Info**

Export Diagnosis Info

Collect Image Debugging Info

- (2) Click **Export**. In the displayed dialog box, select the local directory for storing the information.



### NOTE!

- Diagnosis information is exported to the local folder in form of a compressed file. You need to decompress the file using a tool such as WinRAR and then open the file using a text editor.
- By selecting **Collect Image Debugging Info**, you can display video with debugging information at the same time, which makes troubleshooting easier.

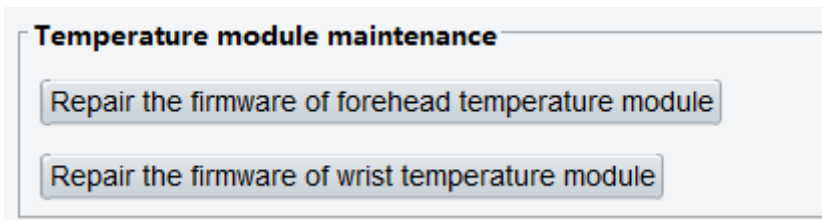
#### 4E. Temperature module maintenance

You can repair temperature measurement modules under **Temperature module maintenance**.

- (1) Click **Setup > System > Maintenance**.

- (2) Under **Temperature module maintenance**, click the corresponding button for the module you want to repair, forehead temperature module or wrist temperature module.
- (3) In the dialog box displayed, click **OK** to complete the maintenance.

Figure 7-65 Temperature module maintenance



## 8 FAQs

---

- (1) What to do if no message prompts me to install ActiveX when I log in on a Windows 7 PC the first time

Answer: Follow these steps to turn off UAC and then log in again:

- a. Click the **Start** button, and then click **Control Panel**.
- b. In the search box, type uac, and then click **Change User Account Control Settings**.
- c. Move the slider to the **Never Notify** position, and then click **OK**.
- d. After UAC is turned off, log in again.

- (2) What to do if the installation of ActiveX failed

Answer: If the installation failed, add the IP address of the camera as a trusted site: open **Internet Option** in IE, click the **Security** tab, click **Trusted sites**, and then click **Sites** to add the website.

If you use Windows 7, you need to save the **setup.exe** to your PC first, right-click the file, select **Run as administrator**, and then install it according to instructions.

- (3) What to do if live video fails when I log in for the first time

Answer: Close the firewall on your PC and then log in to the Web interface again.