2M TECHNOLOGY

Face Recognition Access Control Terminal with Digital Temperature Measurement Module 2MTHFR-2M

User Manual

Version: 1.00

REV06042020

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 2M Technology.

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.

2M Technology shall not under any circumstances be liable for any special, consequential, incidental or indirect damages arising from the use of this manual or 2M Technology's 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.
- 2M Technology Co., Ltd. (hereinafter referred to as "2M Technology") reserves the right to modify the content in this manual without prior notice or prompt, but 2M Technology does 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 2M Technology.
- Follow operation instructions in this manual when using the product. 2M Technology is 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 2M Technology.
- Follow this manual when using the product. Professional guidance is recommended.
- Notational conventions used in this document are described as follows:

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

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

Symbol	Description
 **WARNING!**	Contains important safety instructions and indicates situations that could cause bodily injury.
 **CAUTION!**	Means reader be careful and improper operations may cause damage or malfunction to product.
 **NOTE!**	Means useful or supplemental information about the use of product.

Contents

1 Application Scope of the Manual

Table1-1 Application Scope of the Manual

Model	Name
2MTHFR-2M	Face Recognition Access Control Terminal

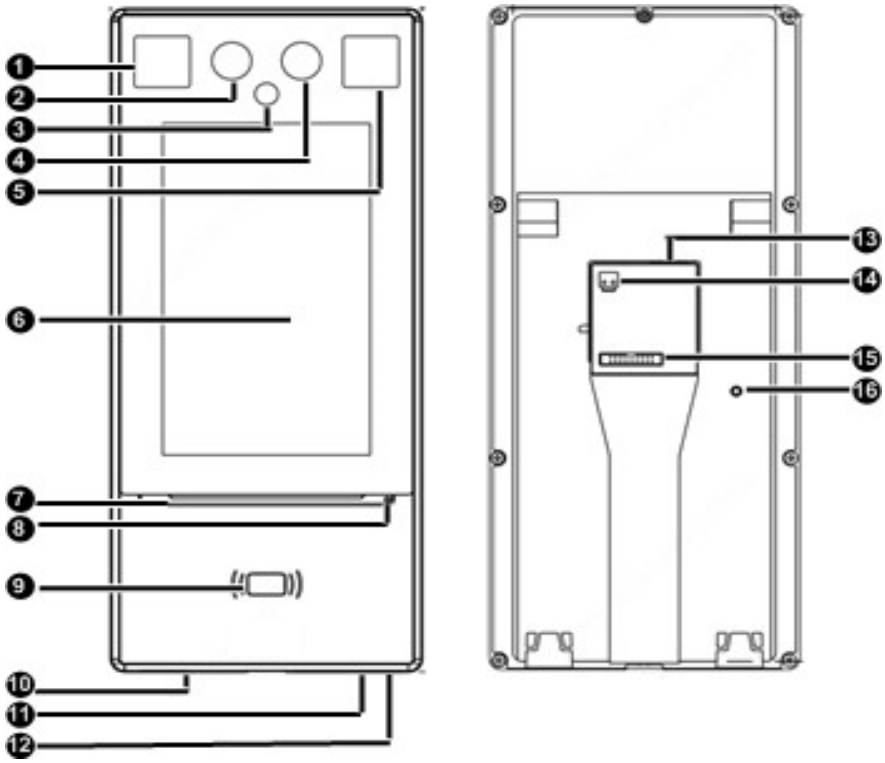
2 Product Overview

Visual intercom face recognition terminal ("the face recognition terminal" for short) is a face recognition access control product featuring high performance and high reliability. The 2M 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. Moreover, using remote control to open the door is also supported via indoor monitor. 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.

- 2MTHFR-2M
  Figure3-2 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.Reset	12.USB2.0
13.Network interface	14.Power input (DC 12V±25%)
15.20-pin interface	16.Tamper proof button

4 Product Installation

- Installation of 2MTHFR-2M

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

5 Local Operations

5.1 Initial Interface

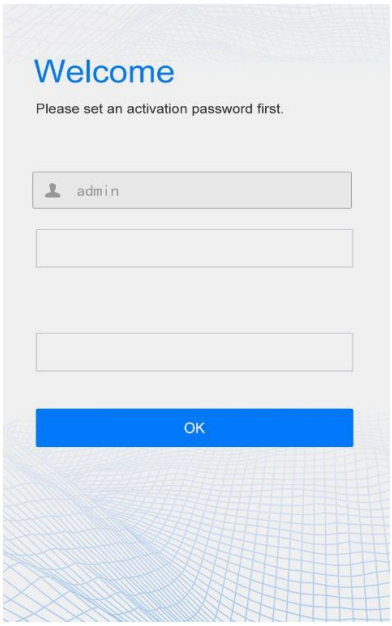
When the face recognition terminal is used for the first time or the factory defaults are restored, users need to set the activation password, which is used to log in to the Activation Config interface.

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 log in to the Web interface.

After the activation password is configured, the main interface of the visual intercom face recognition terminal is displayed. If the activation password needs to be changed later, refer to "Activation Password" to change the password.

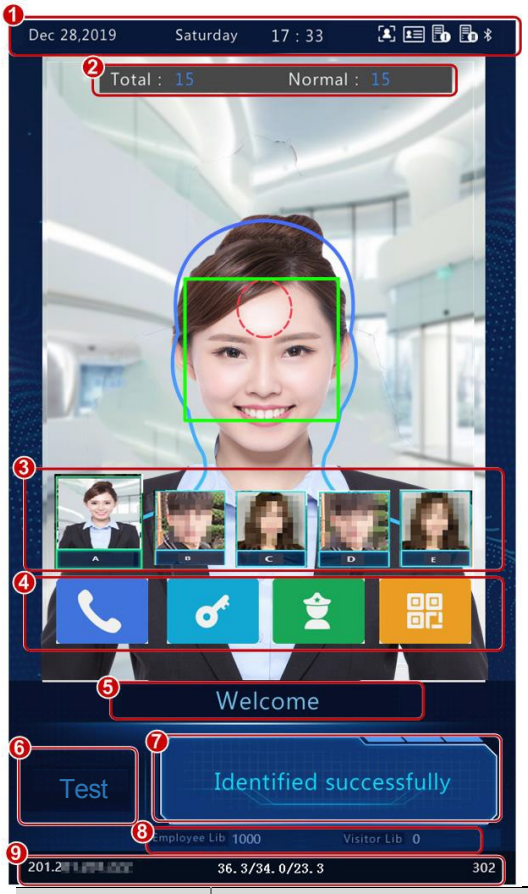
Figure5-1 Activation Password Configuration Interface



5.2 Main Interface

The main interface displayed on the face recognition terminal varies with the device type.

Figure5-2 Main Interface (Video Intercom Mode)



No.	Description
1	Displays the current date, time, and connection status of different services.  indicates the following items from left to right: • Whether to enable the face scan mode • Whether an ID card reader is connected properly • Whether server 1 is online • Whether server 2 is online **NOTE!** An icon marked with  indicates "No".
2	• Total：total number of detected people. • Normal：Number of people with normal temperature This interface is only displayed when the temperature measurement function is enabled. For detailed operation description, see "Advanced Setting".
3	Displays the photo and name of an identified person in the library. Refer to Recognition Result Display to enable the face recognition terminal to display one or more registered face pictures. When **Multiple Faces** 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.

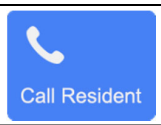
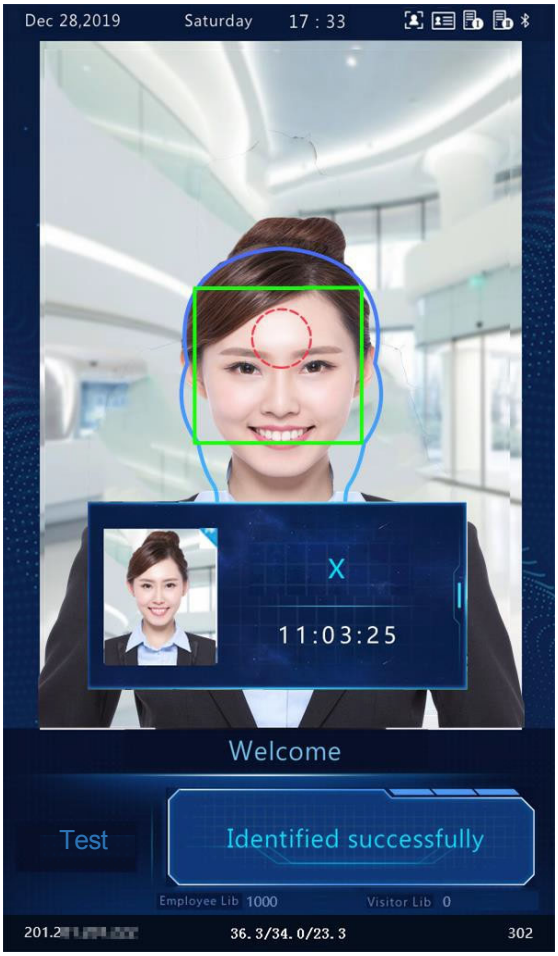
4		Calls a resident. For detailed operation description, see "Call Resident".
		Enters a password to open the door. For detailed operation description, see "Password-based Door Opening".
		Calls the management center. For detailed operation description, see "Call Management Center".
		QR code used for door opening. For detailed operations, see "QR Code-based Door Opening".
5	Title bar, which can be defined by users. For detailed operations, see "Custom Logo and Prompt".	
6	Logo bar, which can be defined by users. For detailed operations, see "Custom Logo and Prompt".	
7	Displays the identification result (such as identified successfully or unregistered person), authentication mode (such as face scan or card swiping), and other information.	
8	Displays the number of people in the employee library and that in the visitor library.	
9	Status bar at the bottom Displays the device IP address, real-time temperature, preset minimum temperature, ambient temperature, and match time.	

Figure5-3 Main Interface (Common Access Control Mode)

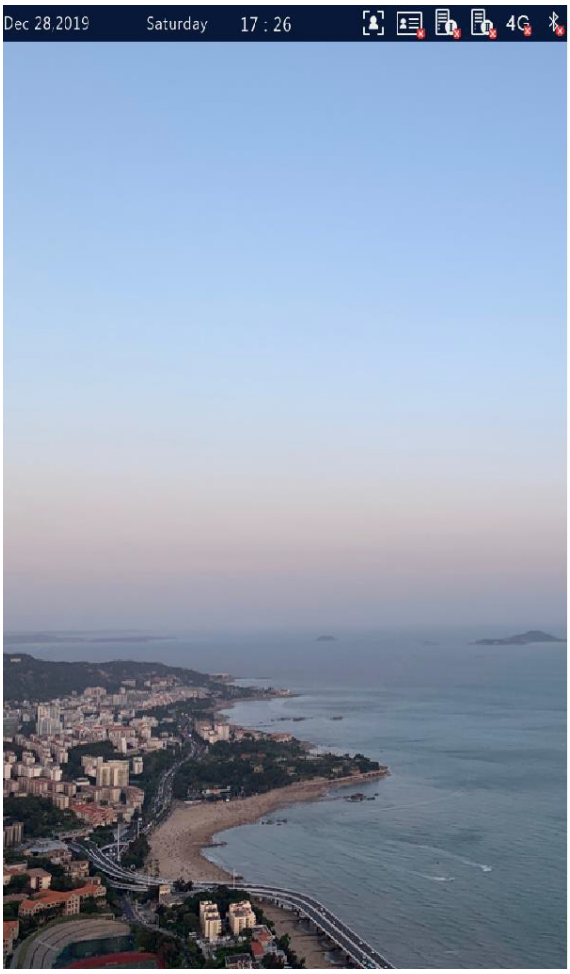


NOTE!
The main interface does not support call, QR code- and password-based door opening in common access control mode. The GUI displays the recognition result of only a single person.

5.3 Ad Mode

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

Figure5-4 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 Intelligent — 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 5-5. 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.
- 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 visual intercom 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.

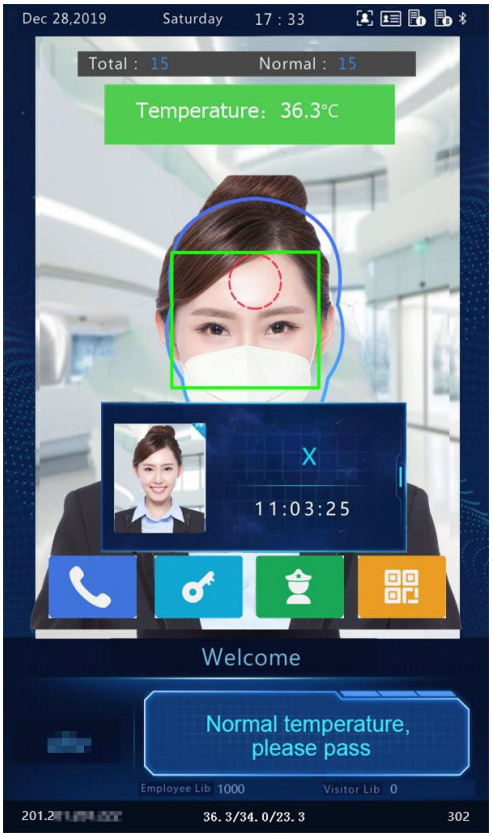
1. Mask detection and temperature measurement

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.

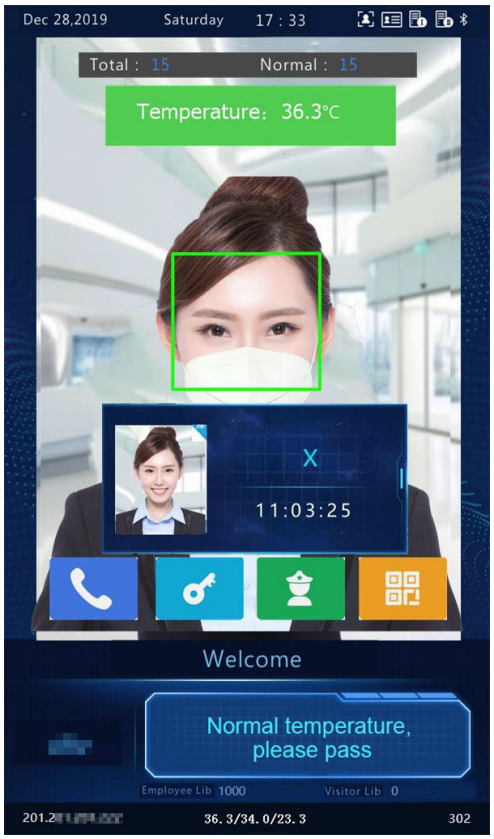
NOTE!

The following figures show interfaces of forehead temperature measurement. The interfaces of wrist temperature measurement are basically the same as those of forehead temperature measurement except that no human shape and red circle are displayed on the GUI. For the wrist temperature measurement interface, see Figure 5-8.

Figure5-5 Normal Temperature and Mask Worn

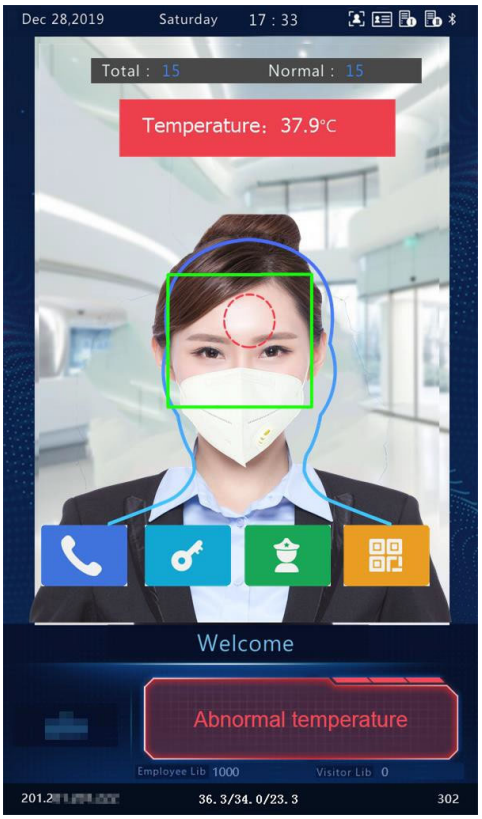


Measure Forehead Temperature

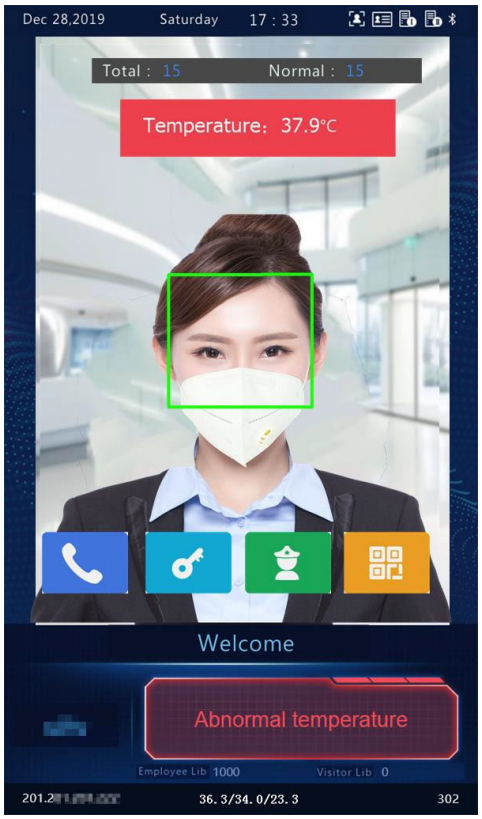


Measure Wrist Temperature

Figure5-6 Mask Worn but Abnormal Temperature



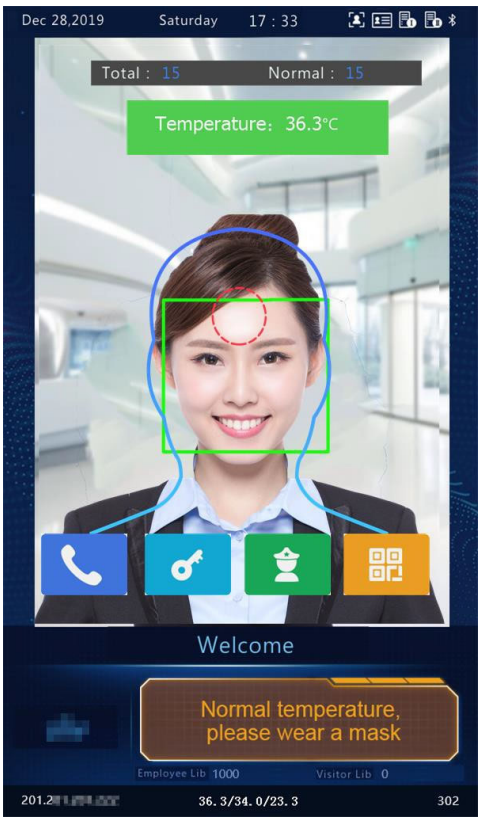
Measure Forehead Temperature



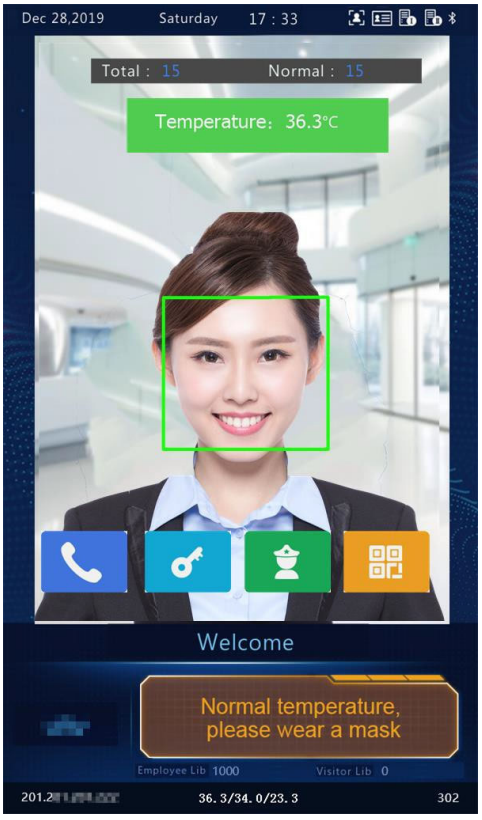
Measure Wrist Temperature

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 5-7 Normal Temperature but Mask Unworn



Measure Forehead Temperature

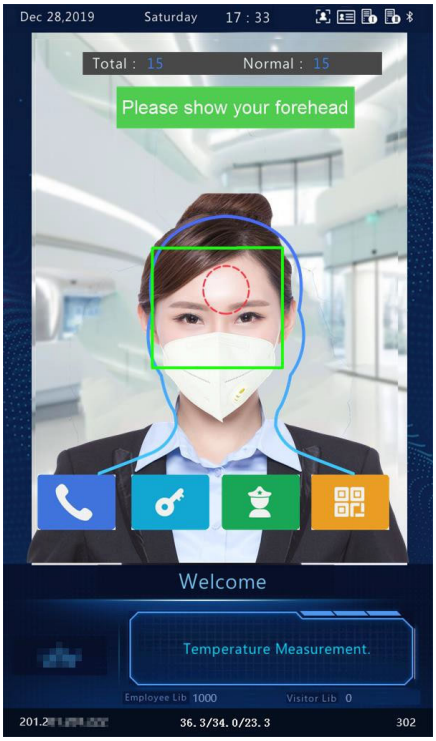


Measure Wrist Temperature

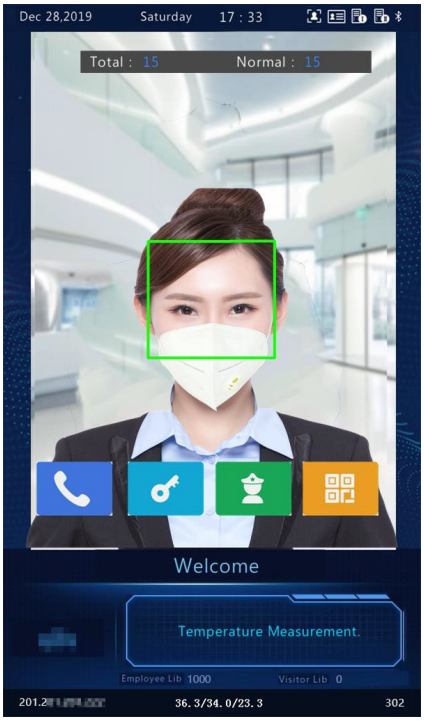
2. Temperature measurement mode

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 Intelligent — Advanced Setting.

Figure 5-8 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 5-5.
- Abnormal Temperature: The temperature of a detected person is abnormal. For the prompt on the GUI and voice prompt, see Figure 5-6.

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 Intelligent — Advanced Setting.

Figure5-9 Mask Worn

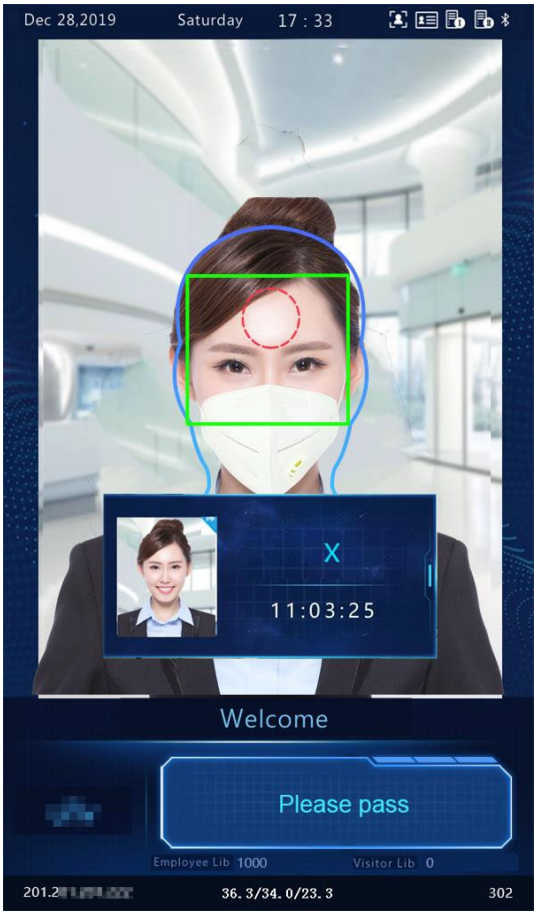
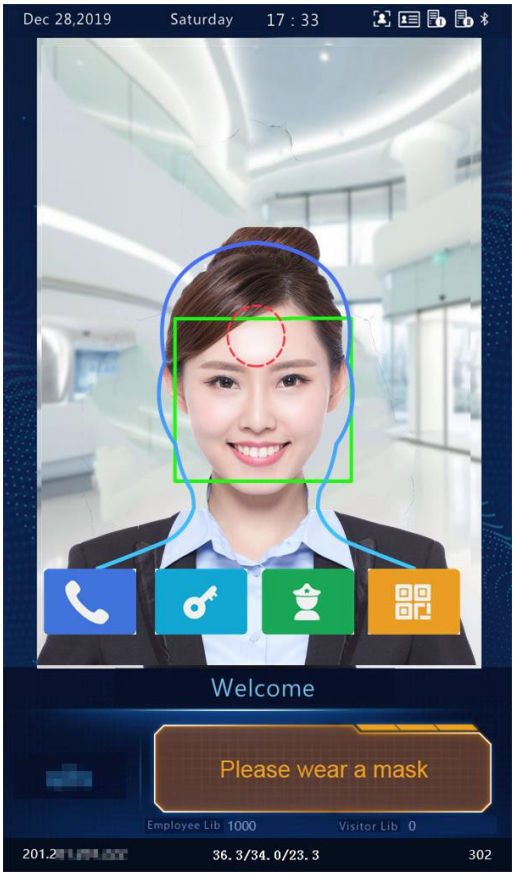


Figure5-10 Mask Unworn



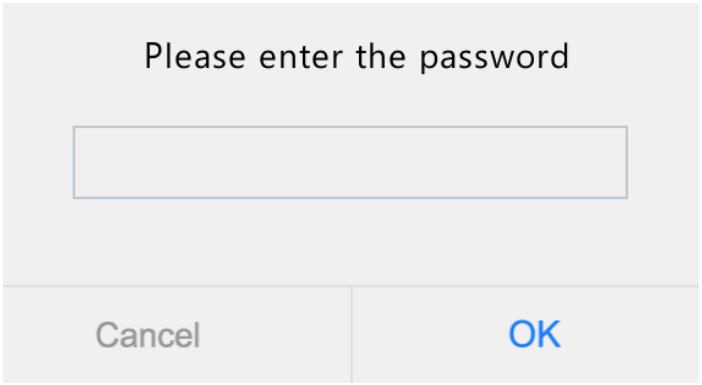
5.5 Activation Config

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 deale to seek help.

NOTE!

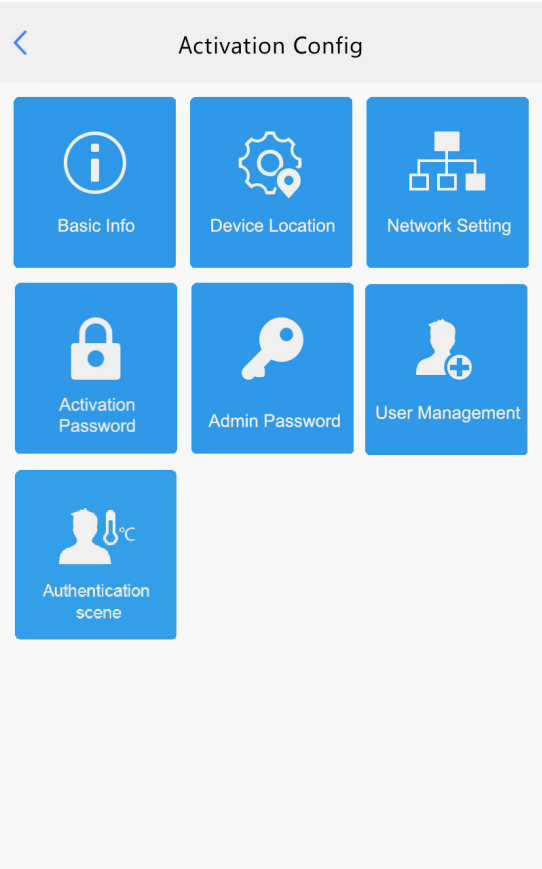
The initial activation password is configured on the initial interface. If it is changed (on the local device or on the Web interface), enter the new activation password.

Figure5-11 Activation Password Input Interface



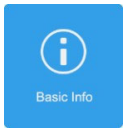
On the **Activation Config** interface, you can view basic information about the face recognition terminal, configure the device location, network, and password, input personnel information, and authentication scene.

Figure5-12 Activation Config Interface



5.5.1 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) On the **Activation Config** interface, tap 

to go to the **Basic Info** interface.

Figure5-13 Basic Info Interface

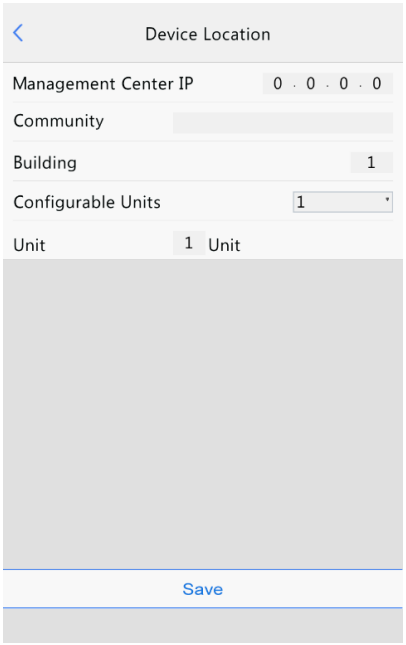
5.5.2 Device Location

On the **Device Location** interface, you can configure the community, unit, and management center to which the device belongs.

(1) On the **Activation Config** interface, tap 

to go to the **Device Location** interface.

Figure5-14 Device Location Interface



(2) Configure device location information by referring to the table below.

Table5-1 Parameter Description and Configuration

Parameter	Parameter Description and Configuration
Management Center IP	Enter the IP address of the management center. After configuration, a user can tap **Call Management Center** on the GUI to call the management center. **NOTE!** The management center IP address must be in the same network segment as the device and cannot begin with 127.
Community	Enter the name of the community to which the device belongs. A string of 1 to 35 characters (1 to 11 Chinese characters) can be entered.
Building	• Enter the No. of the building where the device is located. • The value must be an integer in the valid range of 1 to 99.
Configurable Units	Select the quantity of units that can be served by the device from the drop-down list. The options include **1**, **2**, and **3**.
Unit	Enter the No. of the unit where the device is located. The value is an integer in the valid range of 1 to 9.

(3) Tap **Save** to complete the device location information configuration.

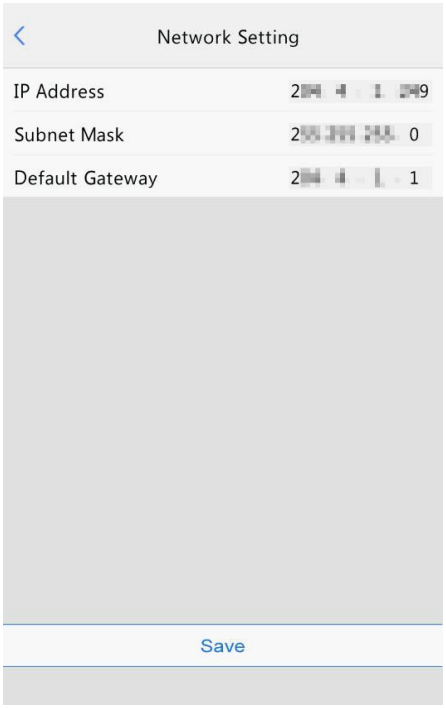
5.5.3 Network Setting

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.

Figure5-15 Network Setting Interface



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

Table5-2 Parameter Description and Configuration

Parameter	Parameter Description and Configuration
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:

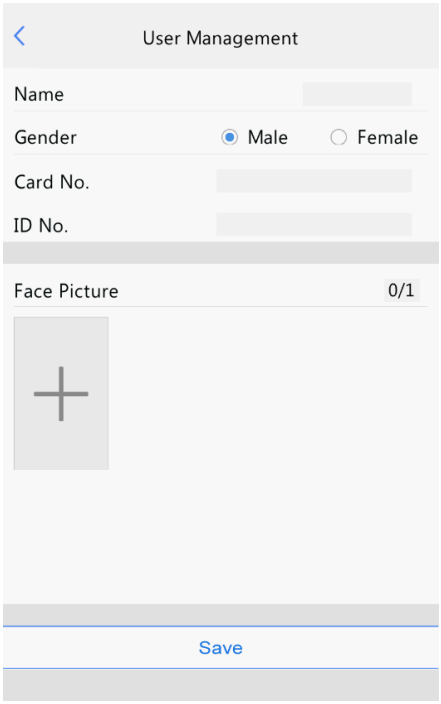
- General requirement: bareheaded full-face photo. Only the face photo of the person under collection is displayed on the screen of the terminal during collection and face photos of other people cannot be contained.
- Range requirement: The photo should show the outline of a person's both ears and cover 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.

Figure5-16 User Management Interface



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

Table5-3 Parameter Description and Configuration

Parameter	Parameter Description and Configuration	Remarks
Name	Mandatory. Enter the name of a person.	/
Gender	Enter the gender of the person. Select **Male** or **Female** from the drop-down list. The default value is **Male**.	/
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.
ID No.	Enter the ID card No. of the person. After successful input, the person can swipe the ID card for access.	
Face Picture	Collect and input face photos by referring to the face photo collection process. 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  tocollect the face snapshot. See the figure below.

 is the back button.

Figure5-17 Collecting and Inputting a Face Photo

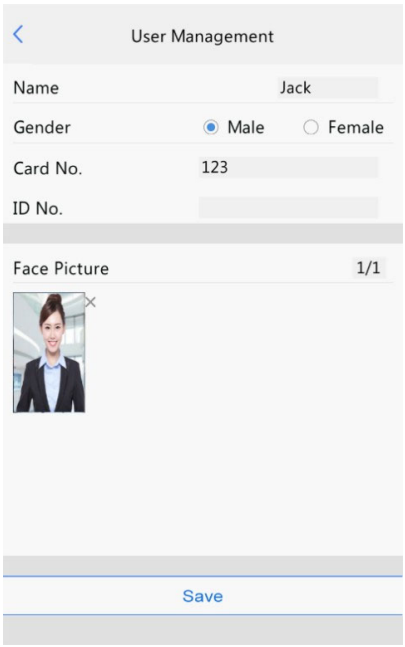
c On the photo confirmation interface, tap  to confirm the collected photo.

 is the back button.

Figure5-18 Photo Confirmation Interface

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

Figure5-19 Save Interface



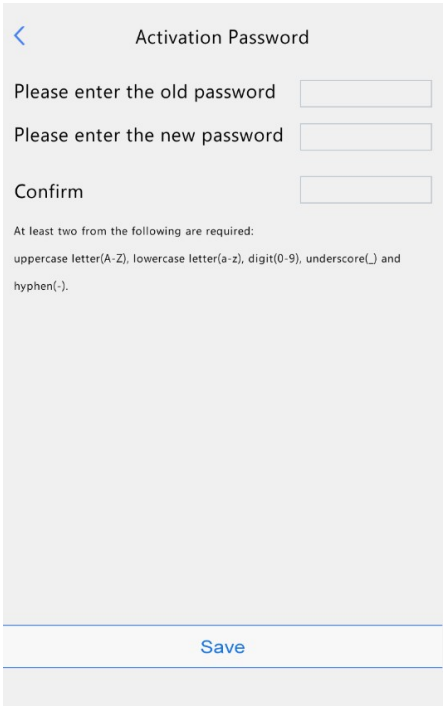
5.5.5 Activation Password

To change the configured activation password, do as follows:

(1) On the **Activation Config** interface, tap 

to go to the **Activation Password** interface.

Figure5-20 Activation Password Interface



(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: uppercase 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

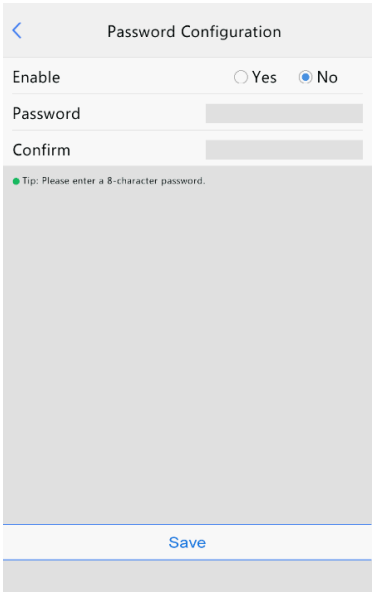
On the password-based door opening interface, users can enter an admin password to open the door. The admin password is applicable to device managerial personnel (such as people in the management center).

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.

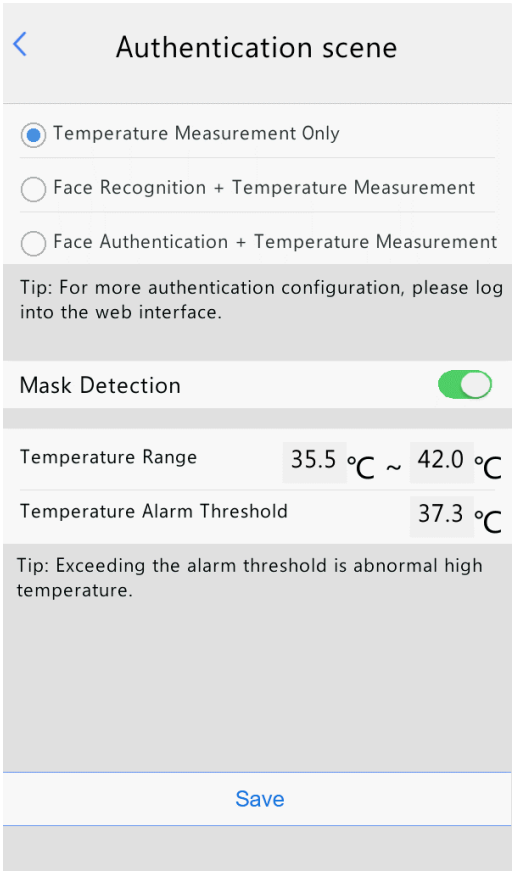
Figure5-21 Admin Password Configuration Interface



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.

Figure5-22 Authentication Scene Interface



Parameter		Description and Configuration
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 **Temperature measurement mode**. 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 Mask detection and temperature measurement.
	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 Mask detection and temperature measurement. Note: This scene can be configured only when the default employee library exists under Face Library Management.
Mask Detection		Enable or disable it based on actual application scenes.
Temperature Configuration	Temperature Measurement Range	Value range: [30–45]; default range: [34–42] Configure the range based on actual application scenes.
	Temperature Alarm Threshold	When the digital detection module detects a temperature higher than the threshold configured here, the "abnormal temperature" alarm is displayed on the GUI and the warning sound is played. Value range: [30–45]; default value: 37.3

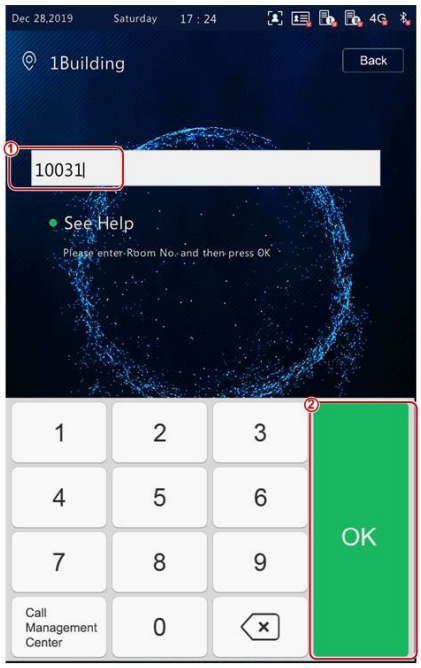
5.6 Call Operations on Visual Intercom Face Recognition Terminal

5.6.1 Call Resident

(1) Tap **Call Resident** on the main interface.

(2) On the displayed interface, enter the room No. as prompted and tap **OK**.

Figure5-23 Call Creation Interface



(3) The call waiting interface is displayed on the face recognition terminal, as shown in the figure below.

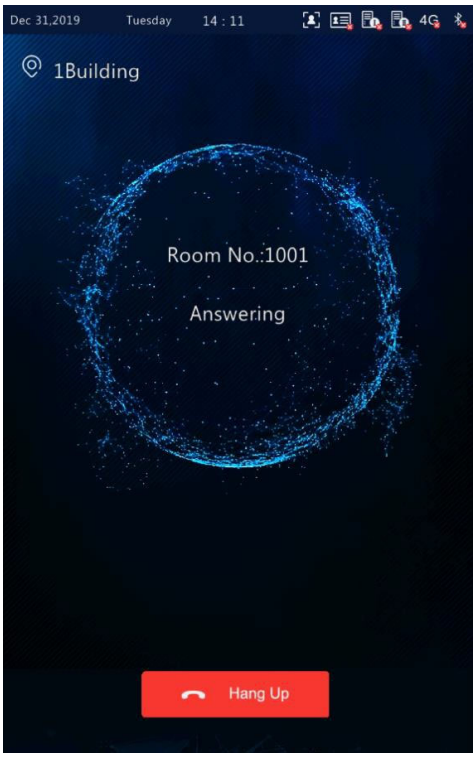
Figure5-24 Call Waiting Interface

(4) The face recognition terminal displays different interfaces, depending on whether the indoor monitor answers the call.

- Answer

When the indoor monitor answers the call from the face recognition terminal, an interface as shown in the figure below is displayed.

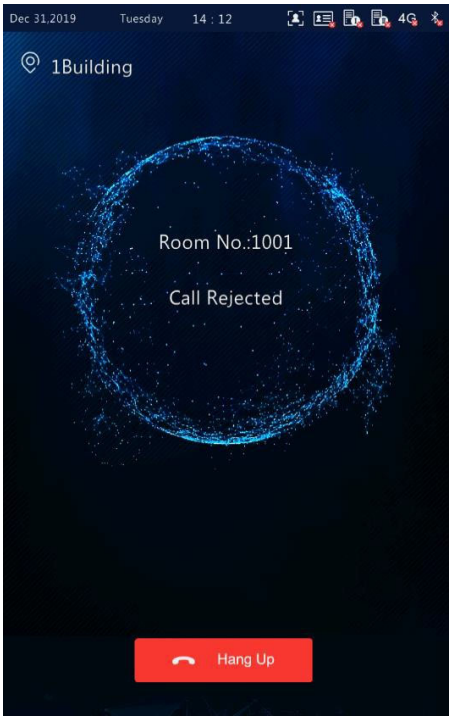
Figure5-25 Interface Displayed after the Indoor Monitor Answers the Call



- Rejection

When the indoor monitor rejects the call from the face recognition terminal, an interface as shown in the figure below is displayed and the terminal returns to the main interface.

Figure5-26 Interface Displayed after the Indoor Monitor Rejects the Call



- Call timeout

When the indoor monitor does not answer the call within the set call duration (60s), the face recognition terminal automatically ends the call and returns to the main interface.

- Other cases

When the face recognition terminal calls an indoor monitor, different prompts are provided on the interface of the terminal based on the configuration and operations. See the table below.

Table5-4 Description of Prompts Displayed on the Interface

Prompt Displayed on the Interface of the Face Recognition Terminal	Description
Hanging Up	When you tap **Hang up** on the interface of the face recognition terminal before the resident answers the call, "Hanging Up" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.
Unable to Connect	When the resident called by the face recognition terminal does not exist, "Unable to Connect" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.
The subscriber you dialed is busy	When the face recognition terminal calls an indoor monitor that is in Do Not Disturb mode, "The subscriber you dialed is busy" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.
No Answer	When the face recognition terminal calls an indoor monitor that is configured with auto answer, "No Answer" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.
Network Failure	If the network of the face recognition terminal or a called indoor monitor is disconnected, "Network Failure" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.
Incorrect password configured for the outdoor station.	If the called indoor monitor configures incorrect password for the outdoor monitor, "Incorrect password configured for the outdoor station" is displayed on the interface, and the terminal ends the call and returns to the main interface 2s later.

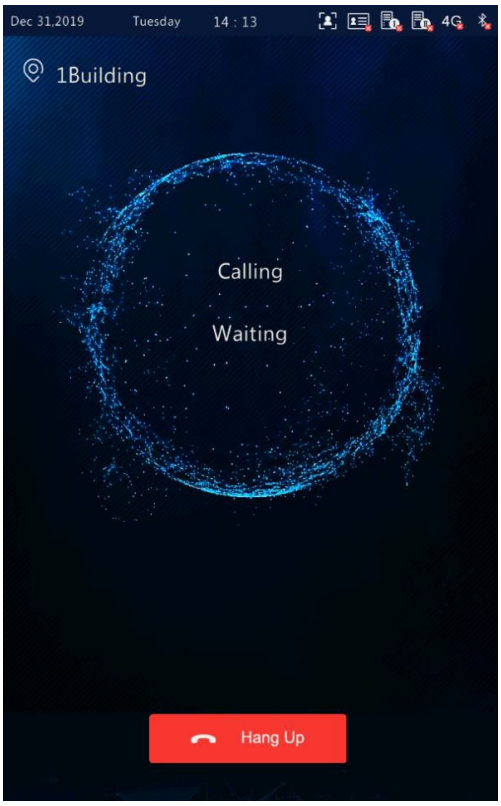
5.6.2 Call Management Center

(1) Tap **Call Management Center** on the main interface.

(2) The figure below shows the call interface displayed when the face recognition terminal calls the management center.

(3) For the configuration of management center, see management center configuration.

Figure 5-27 Management Center Calling Interface



(4) The face recognition terminal displays different interfaces based on whether the management center answers the call.

- Answer

A person in the management center answers the call from the face recognition terminal. For the interface display, see Answer.

- Rejection

A person in the management center rejects the call from the face recognition terminal. For the interface display, see Rejection.

- Call timeout

When no person in the management center answers the call within the set call duration (60s), the face recognition terminal automatically ends the call and returns to the main interface.

5.7 Door Opening Method

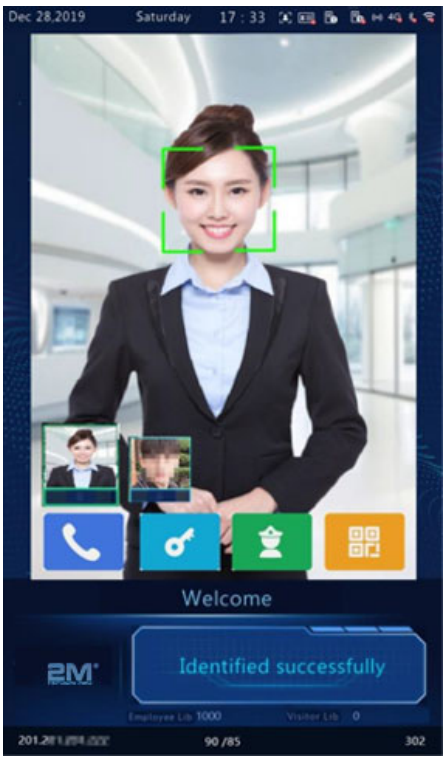
5.7.1 Face Scan-based Door Opening

The face recognition terminal matches a collected face photo with photos in the face photo library.

- If the match is successful, an interface as shown in the figure below is displayed, the audio "Recognized successfully" is played, and the door is successfully opened.

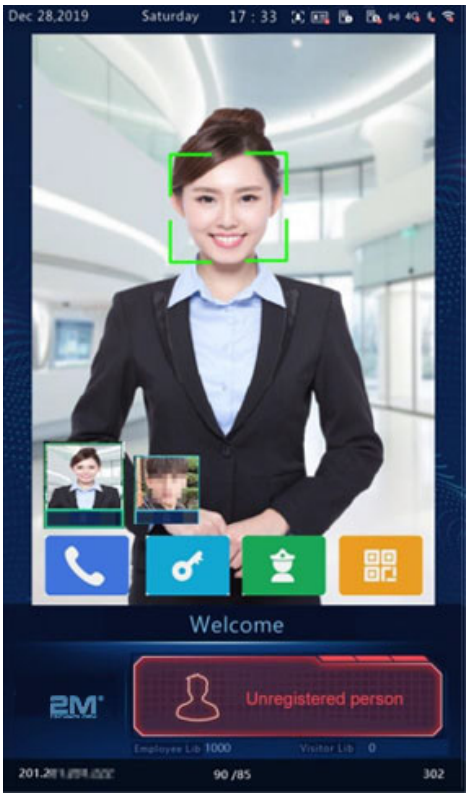
Figure5-28 Successful Recognition Interface

f



- If the match fails, an interface as shown in the figure below is displayed and the audio "Unregistered person" is played. You can try other methods to open the door.

Figure5-29 Unregistered Person Interface



- Other face scan-based door opening failures

Some failures may arise during face scan-based door opening. The prompts displayed on the interface are as follows and the effect is similar to the Unregistered Person interface.

- Not a real person.
- Unscheduled access.
- Please face the camera.

5.7.2 Password-based Door Opening

When password authentication is enabled on the outdoor monitor (for the configuration, see Check Template), a person can enter the room password or admin password to open the door.

1. Password-based door opening

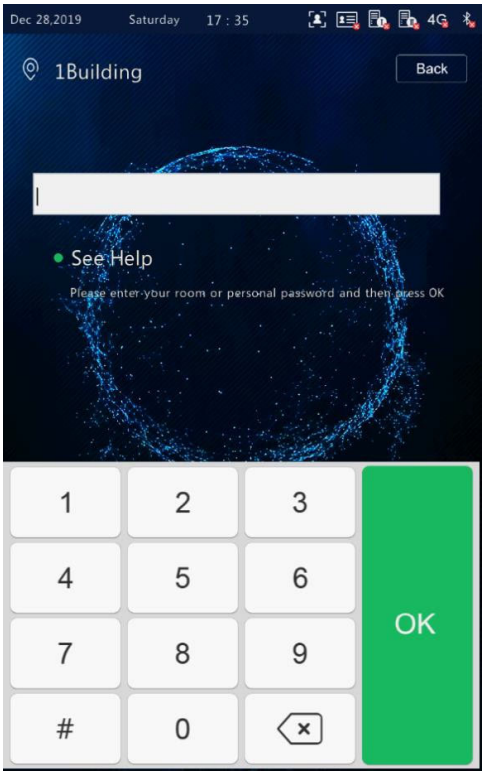
(1) Tap **Password** on the main interface.

(2) On the displayed interface, enter the password as prompted and then tap **OK**.

NOTE!

- Door opening passwords are configured on the indoor monitor. For details, see the *Wall-mounted Indoor Monitor User Manual*.

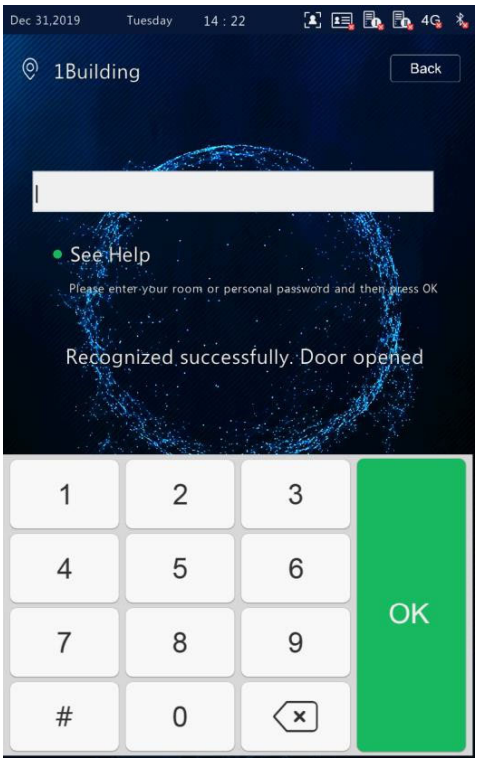
Figure5-30 Password-based Door Opening Interface



- The password is correct and the door is opened successfully.

  After a correct room password is entered, an interface as shown in the figure below is displayed and the audio "Recognized Successfully" is played.

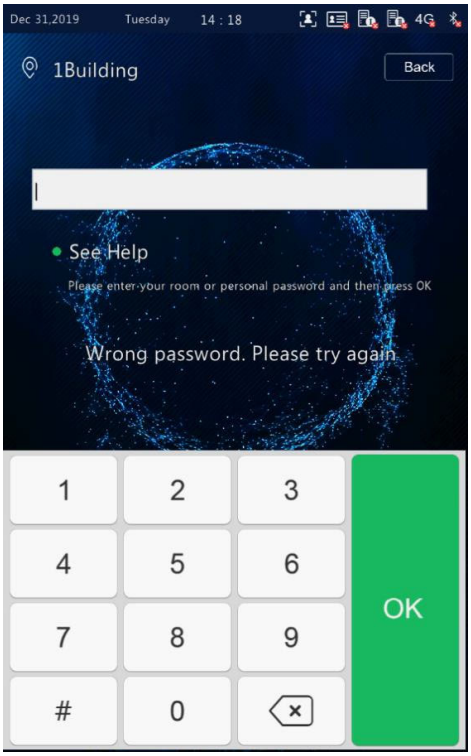
Figure5-31 Successful Recognition Interface



- The password is wrong and the door fails to be opened.

  After a wrong room password is entered, an interface as shown in the figure below is displayed and the audio "Password authentication failed" is played.

Figure5-32 Wrong Password Interface



2. Admin password-based door opening

(1) Tap **Password** on the main interface.

(2) On the displayed interface, enter the admin password and tap **OK**.

NOTE!

- For the setting of the admin password, see Admin Password.

- The admin password is correct and the door is opened successfully.

  For the interface and voice prompt, see The password is correct and the door is opened successfully.
- The admin password is wrong and the door fails to be opened.

  For the interface and voice prompt, see The password is wrong and the door fails to be opened.

5.7.3 Card Swiping-based Door Opening

- People can swipe their cards on the face recognition access control terminal to open the door.
- When a card reader is connected to the face recognition terminal, people can swipe their cards in the card scan area to open the door.

NOTE!

People's card information needs to be sent to the face recognition terminal in advance.

5.7.4 QR Code-based Door Opening

The face recognition terminal supports QR code-based door opening.

(1) Tap  on the main interface to go to the QR code interface.

(2) Aim the generated QR code towards the camera of the face recognition terminal or a connected QR code scan device. The recognition will be successful and the door will be open.

NOTE!

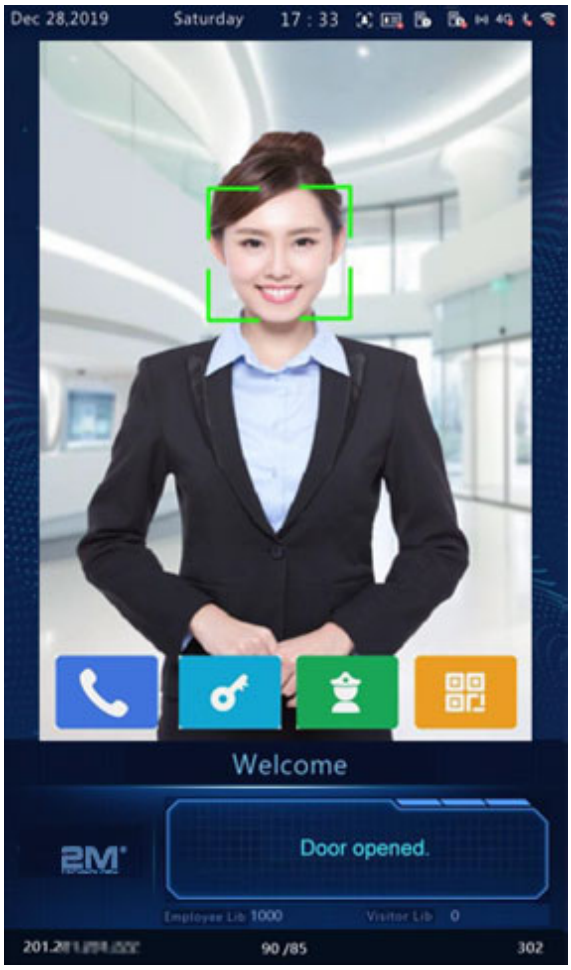
If no operation is performed on the QR code interface within 30s, the face recognition terminal automatically switches to the live viewinterface.

5.7.5 Remote Opening

After the door is opened remotely, the face recognition terminal notifies the user of the door opening by displaying and playing a prompt.

After the face recognition terminal is connected to an indoor monitor and the configuration is complete, operations can be performed on the indoor monitor to open the door remotely. For detailed operations, see the *Wall-mounted Indoor Monitor User Manual*.

Figure5-33 Door Opening Success Interface



6 Personnel Management

6.1 Personnel Information Input

The face recognition terminal supports multiple personnel information input methods. Users can select a proper method based on actual application scenes.

6.1.1 Information Import to the Terminal

You can import information by using the People Import Tool or input the information locally.

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. Import using the People Import Tool

Decompress **People Import Tool.7z** and import personnel information by referring to the *People Import Tool Operation Manual-Detailed Version* and *People Import Tool Operation Manual-Simplified Version*.

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 People Import Tool

For detailed operation process, see Import using the People Import Tool.

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

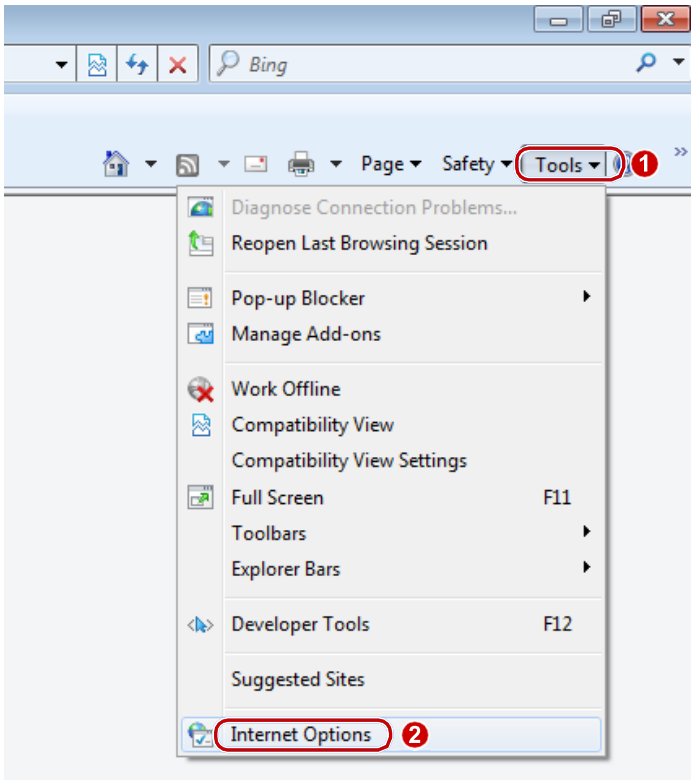
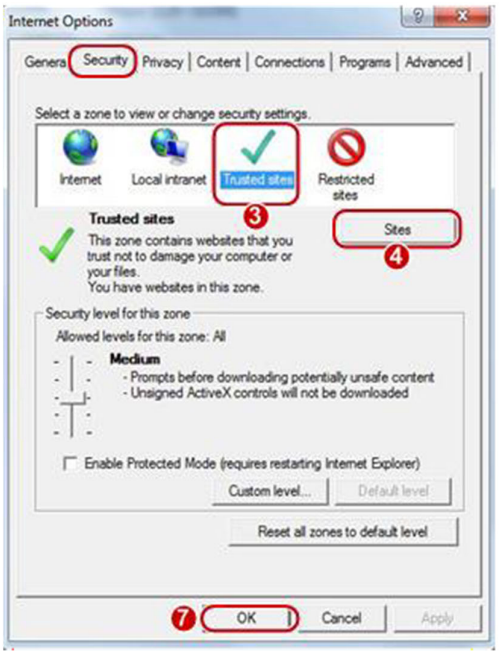
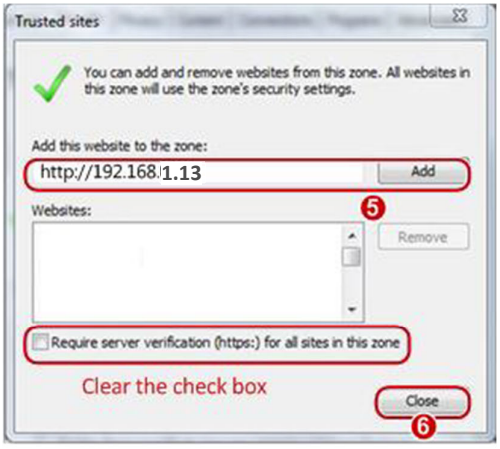


Figure 7-2 Adding the IP Address as a Trusted Site





NOTE!

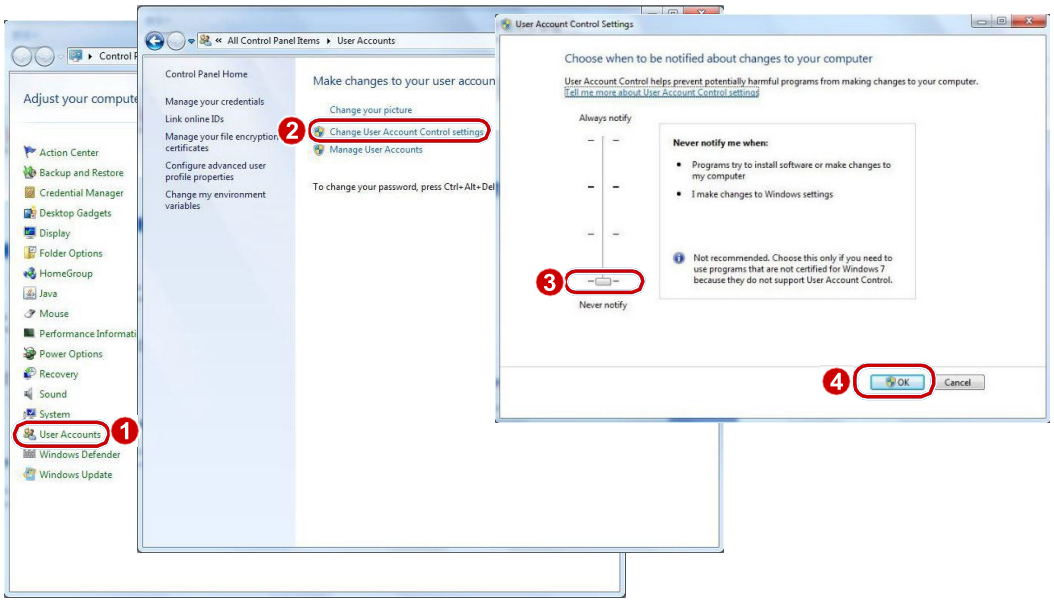
- The IP address 192.168.1.13 in this example is the default IP address. Please replace it with the actual address of your face recognition terminal if it has been changed.

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.

Figure7-3 Setting the Control Permission



7.1.2 Logging In to the Web Interface

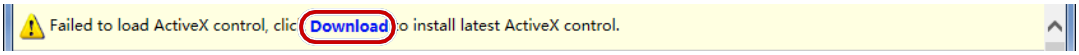
The default static IP address of the device is 192.168.1.13. The device also supports simple login using the IP address of 192.168.0.13 and subnet mask of 255.255.255.0.

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.

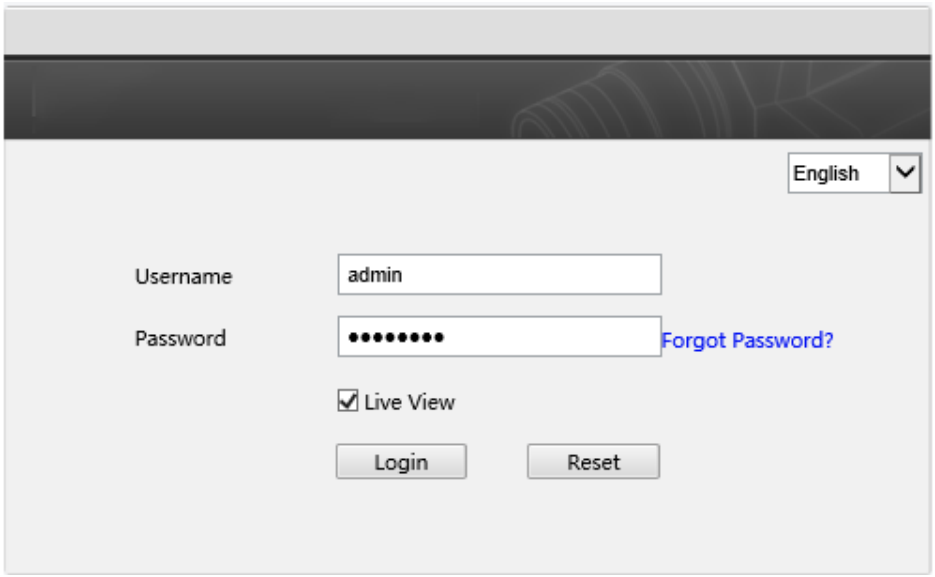


NOTE!

- 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 ten minutes.

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

Figure7-4 Login Interface



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

Table7-1 Parameter Description and Configuration

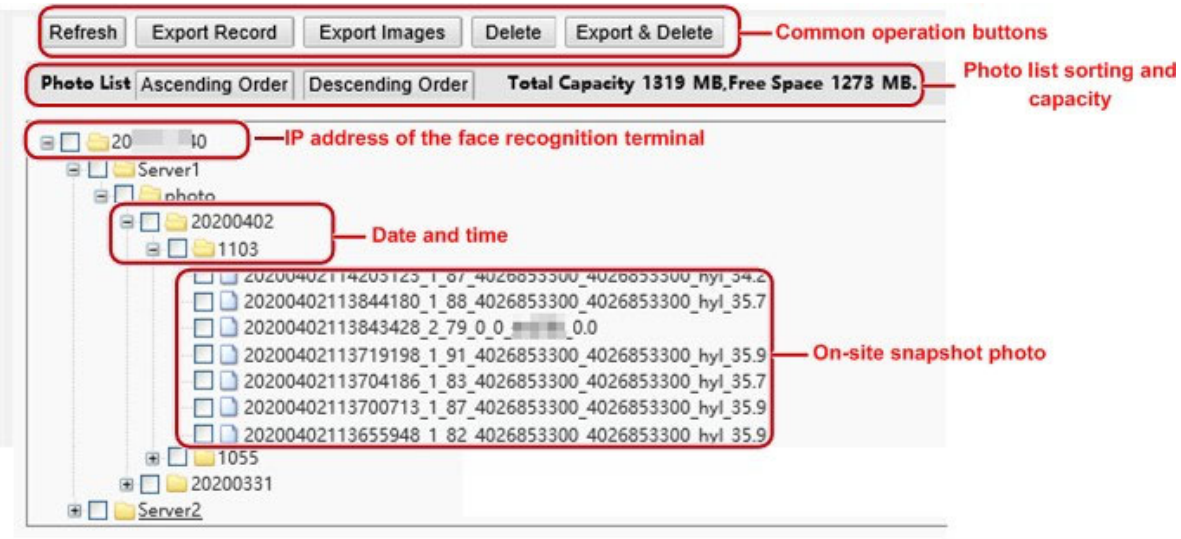
Parameter/Plug-in	Description	Configuration
Username/Password	Username and password for logging in to the Web interface. At initial login: The default username is **admin** and the default password is **123456**. The password for **admin** to log in to the Web interface is the same as the activation 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	● If it is selected, live view videos are displayed on all live view screens after login to the Web interface. ● If it is deselected, live view videos are displayed only after live view is enabled manually. For detailed operations, see Live View.	Set the parameter based on the actual conditions. It is selected in this example.
Forgot Password	/	/
Save Password	After it is selected, you can directly log in without entering the password at your next login. If your password is changed, you cannot log in without entering the password. It is not recommended to select it for the sake of security.	It is deselected in this example.
Reset	After **Reset** is clicked, the **Username**, **Password**, and **Save Password** boxes will be cleared. Other boxes such as the language and **Live View** 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.

Figure7-5 Photo Information



7.2.1 Photo List Sorting

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

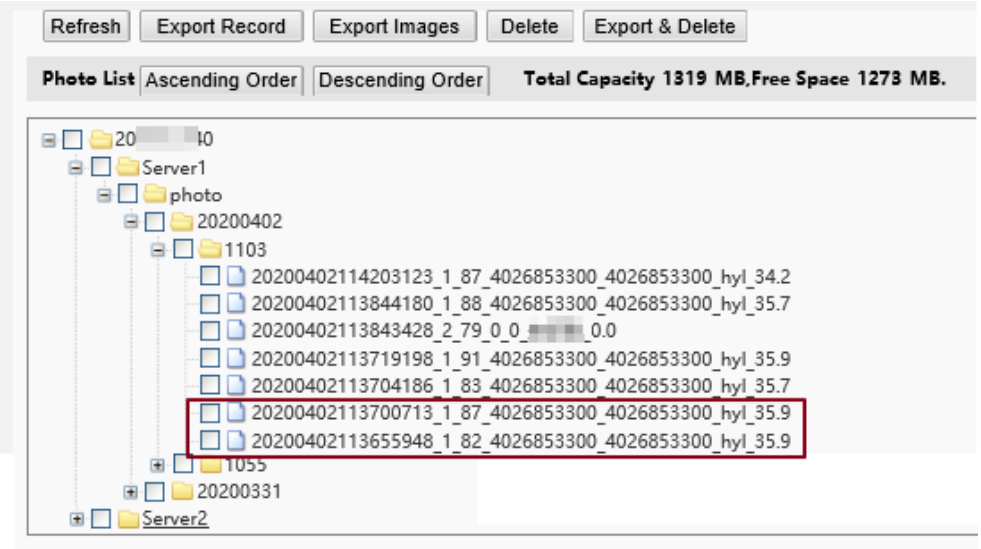
7.2.2 Total Capacity/Available Capacity

The total capacity and available capacity of TMS servers 1 and 2 are displayed.

7.2.1 Photo Naming Rules

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

Figure7-6 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".

7.2.2 Refreshing the Photo Library

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

7.2.3 Exporting Records

You can export some operation records from the database.

7.2.4 Exporting Photos

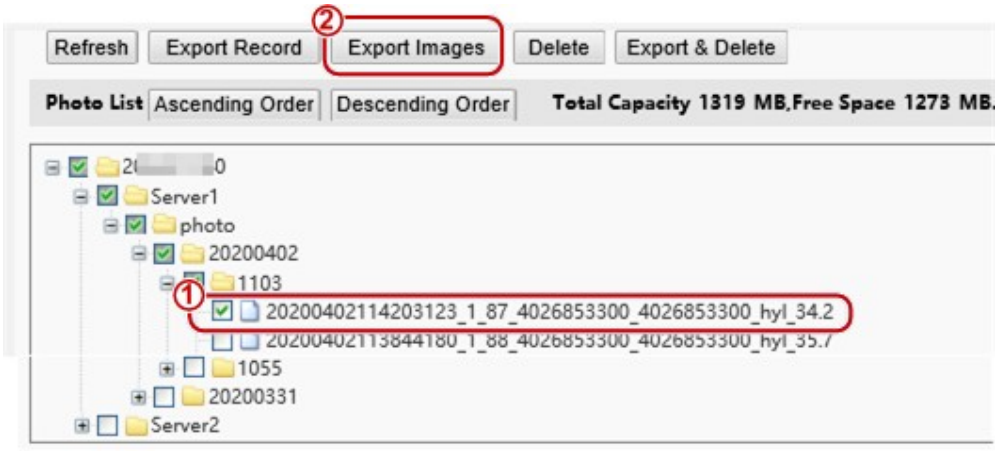
You can export all or some of the photos stored in the face recognition terminal.

(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.

Figure7-7 Export Operation Interface



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

7.2.5 Deleting a Photo

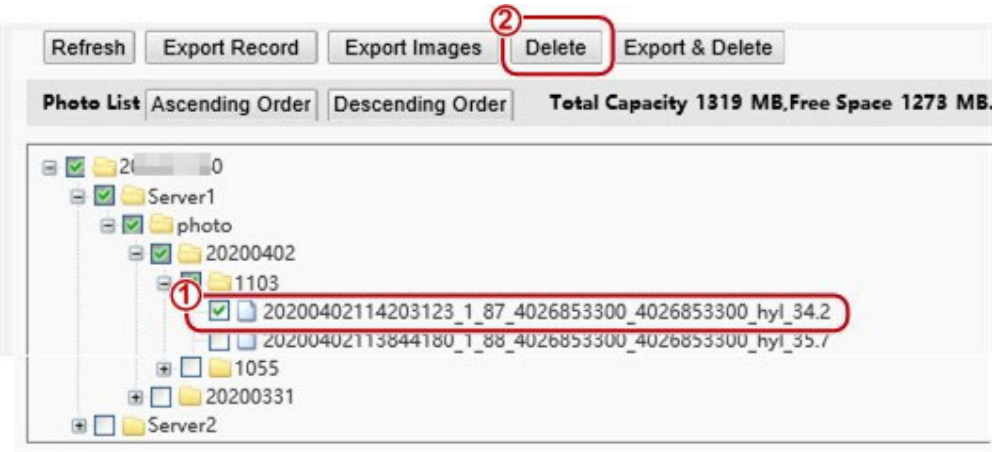
(1) Go to the **Photo List** interface.

(2) Select a photo to be deleted.

(3) Click **Delete**.

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

Figure7-8 Deletion Operation Interface



7.2.6 Exporting and Deleting Photos

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

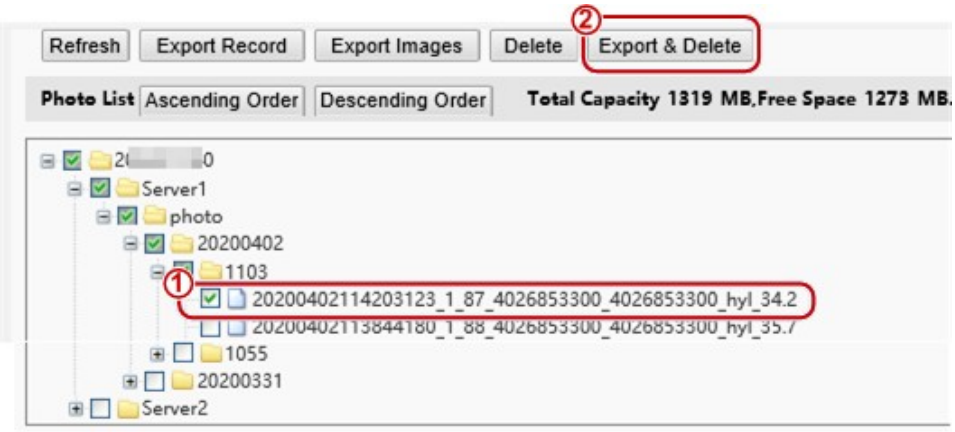
(1) Go to the **Photo List** interface.

(2) Select photos to be exported and deleted.

(3) Click **Export & Delete**.

(4) In the deletion confirmation box, click **OK**.

Figure7-9 Export and Deletion Operation Interface

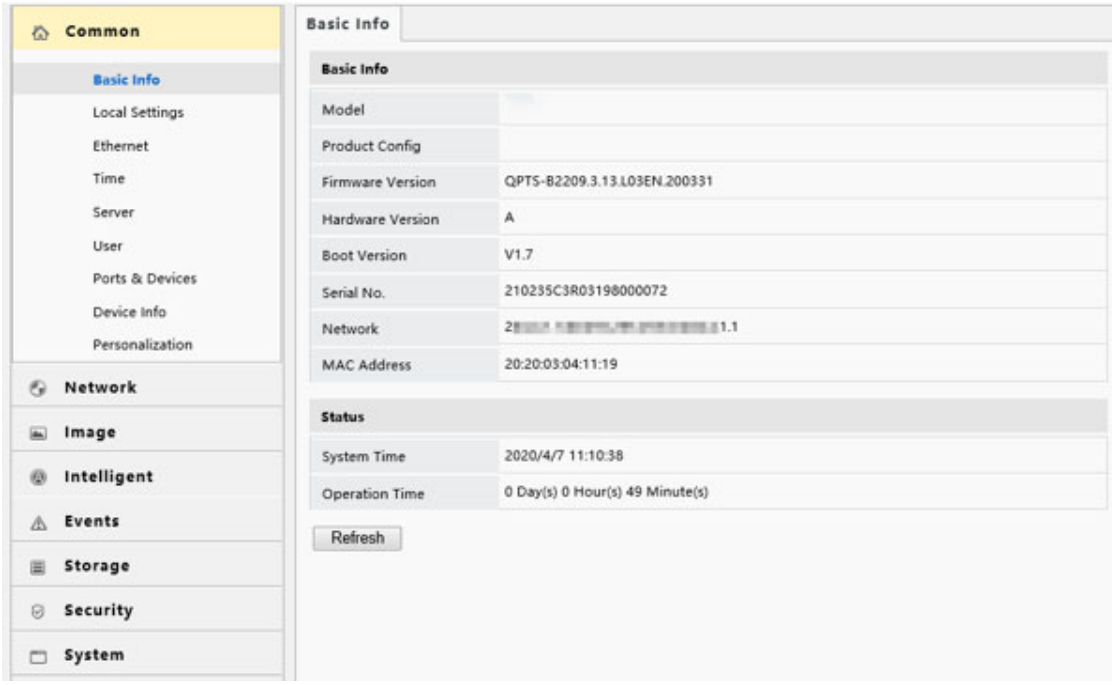


(5) Select the path for storing the photos and click **OK** to complete the export and deletion operation.

7.3 Parameter Configuration

7.3.1 Common

Figure7-10 Common Parameter Configuration Interface



1. 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** to go to the **Basic Info** interface.

Figure7-11 Basic Info Interface

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

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

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.

Figure7-12 Local Settings Interface

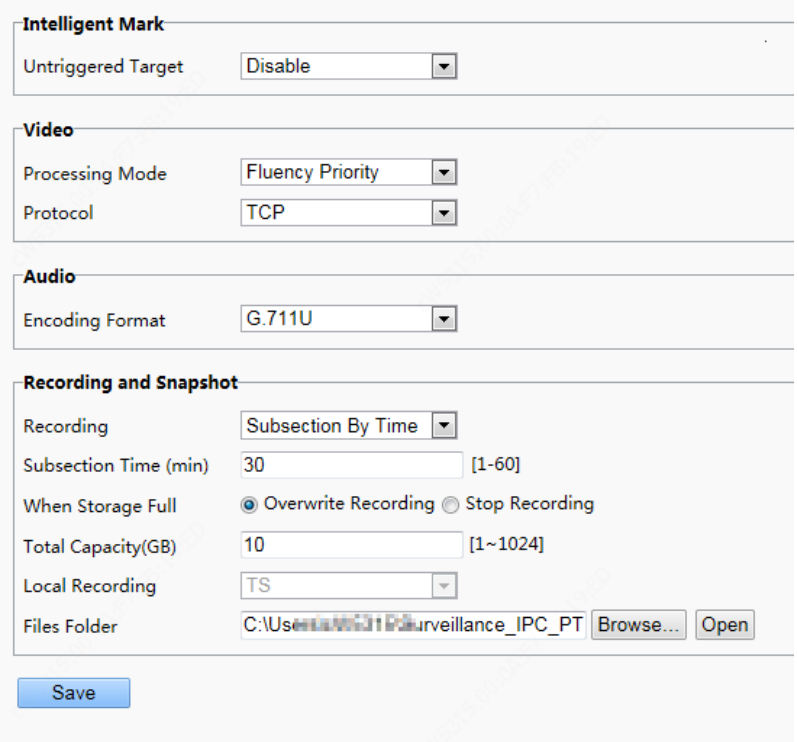


Table7-2 Parameter Description and Configuration

Area	Parameter	Description
Intelligent Mark	Untriggered Target	The options are as follows: ● Disable ● Enable When this function is enabled, the terminal will track and mark targets. If the face detection function is enabled, the device will track and mark faces.
Video	Processing Mode	The options are as follows: ● Real-Time Priority: Recommended if the network is in goodcondition. ● Fluency Priority: Recommended if you want short time lag for live video. ● Ultra-low Latency: Recommended if you want the minimum time lag for live video. When the network is in good condition, **Real Time Priority** is recommended. If delay exists on the network, **Fluency Priority** is recommended. If it is required that the live view delay should be lower than the real time priority, **Ultra-low Latency** is recommended.
	Protocol	Set the protocol used to transmit media streams to be decoded by the PC. The options are as follows: ● UDP ● TCP
Audio	Encoding Format	Audio encoding format on the client. The options are as follows: ● G.711 U ● AAC-LC
Recording and Snapshot	Recording	Type of local recording subsection. The options are as follows: ● Subsection by Time: Duration of recorded video for each recording file on the computer. For example, 2 minutes. ● Subsection by Size: Size of each recording file stored on the computer. For example, 5M.
	Subsection Time (min)	This parameter is displayed only when **Recording** is set to **Subsection by Time**.

		The value ranges from 1min to 60min. You can enter the value based on actual conditions.
	Subsection Size (MB)	This parameter is displayed only when **Recording** is set to **Subsection by Size**. The value ranges from 10MB to 1024MB. You can enter the value based on actual conditions.
	When Storage Full	The options are as follows: ● Overwrite Recording: When the assigned storage space on the computer is used up, The device deletes the existing recording filesto make room for the new recording file. ● Stop Recording: When the assigned storage space on the computer is full, recording stops automatically.
	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.

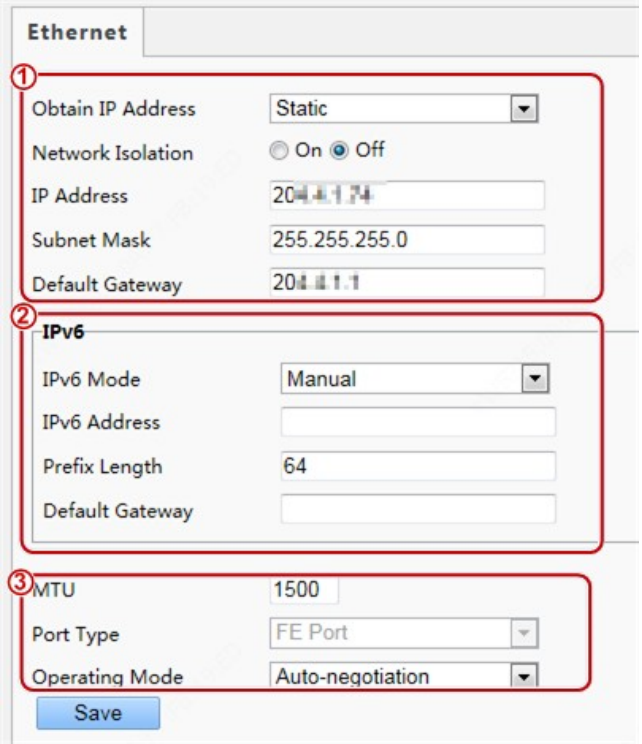
3. Ethernet

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.

Figure7-13 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.

Figure7-14 Static Address Configuration Interface

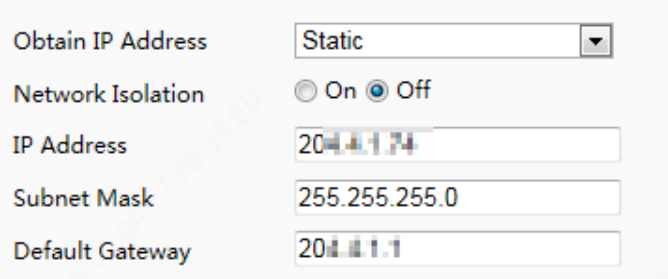


Table7-3 Parameter Description and Configuration

Parameter	Description and Configuration
Network Isolation	Keep the default value **Off**. 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.

Figure7-15 PPPoE Configuration Interface

Table7-4 Parameter Description and Configuration

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

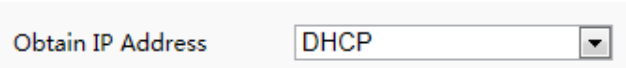
NOTE!

- 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.

Figure7-16 DHCP Configuration Interface



(3) Configure IPv6 settings as shown in ② in the figure above.

Table7-5 Parameter Description and Configuration

Parameter	Description and Configuration
IPv6 Mode	The default value is **Manual**. Keep the default value here.
IPv6 Address	Enter the IPv6 address of the device. The IP address of the device must be unique across the network.
Prefix Length	Enter the length of the subnet prefix of the device.
Default Gateway	Enter the default gateway of the device.

(4) Set parameters as shown in ③ in the figure above.

Table7-6 Parameter Description and Configuration

Parameter	Description and Configuration
MTU	The value ranges from 576 to 1500. This parameter is not displayed when **Obtain IP Address** is set to **PPPoE**.
Port Type	The default value is **FE Port**. 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

(5) 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.

Figure7-17 Time Configuration Interface

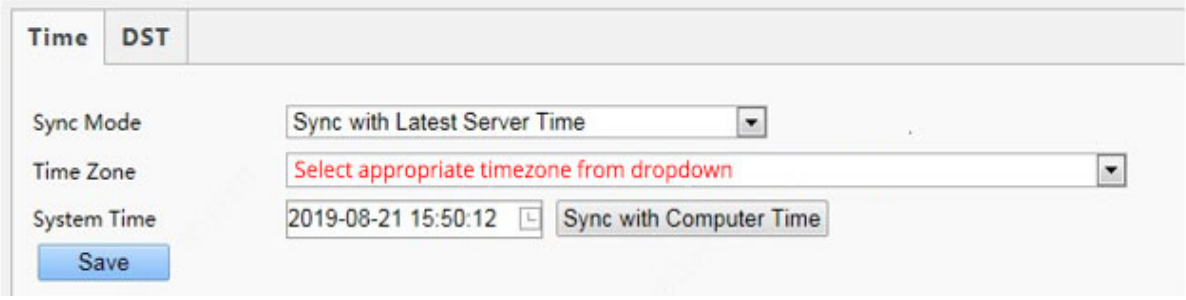


Table7-7 Parameter Description and Configuration

Parameter	Description and Configuration

Sync Mode	The options are as follows:

	● Sync with System Configuration: The time is synchronized with the initially configured time of the system. ● Sync with NTP Server: The time is synchronized with the time of the NTP server. ● Sync with Management Server(Non-ONVIF): The time is synchronized with the time of the management server. ● Sync with Management Server(ONVIF): The time is synchronized with the time of the management server. ● Sync with Latest Server Time: The time is synchronized with the latest time of all servers in the network.
Time Zone	Select the correct time zone.
System Time	This parameter is available only when **Sync Mode** is set to **Sync with System Configuration** or **Sync with Latest Server Time**. Configure the correct time.
Sync with Computer Time	This parameter is available only when **Sync Mode** is set to **Sync with System Configuration** or **Sync with Latest Server Time**. The system time for synchronization is the time of the local PC.
NTP Server Address	This parameter is displayed only when **Sync Mode** is set to **Sync with NTP Server**. Enter the IP address of the NTP server.
Update Interval(s)	This parameter is displayed only when **Sync Mode** is set to **Sync with NTP Server**. 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.

Figure7-18 DST Configuration Interface

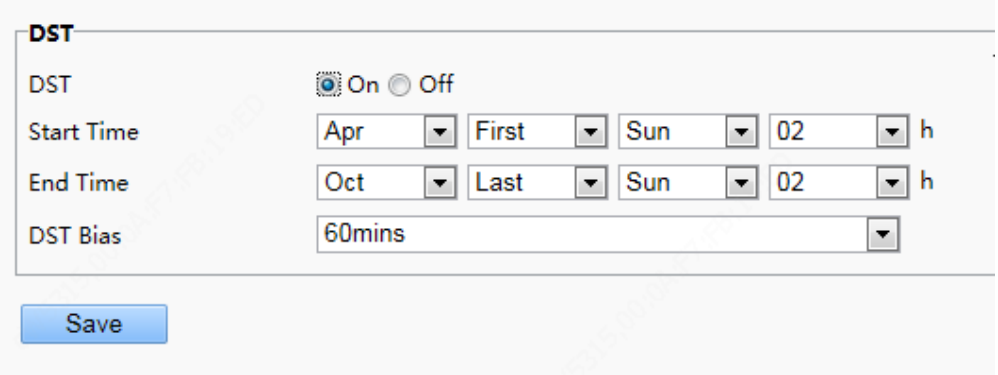


Table7-8 Parameter Description and Configuration

Parameter	Description and Configuration
DST	The options are as follows: ● On ● Off The following parameters are configurable only when **DST** is set to **On**.
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: ● 30mins ● 60mins ● 90mins ● 120mins 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 config server information.

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.

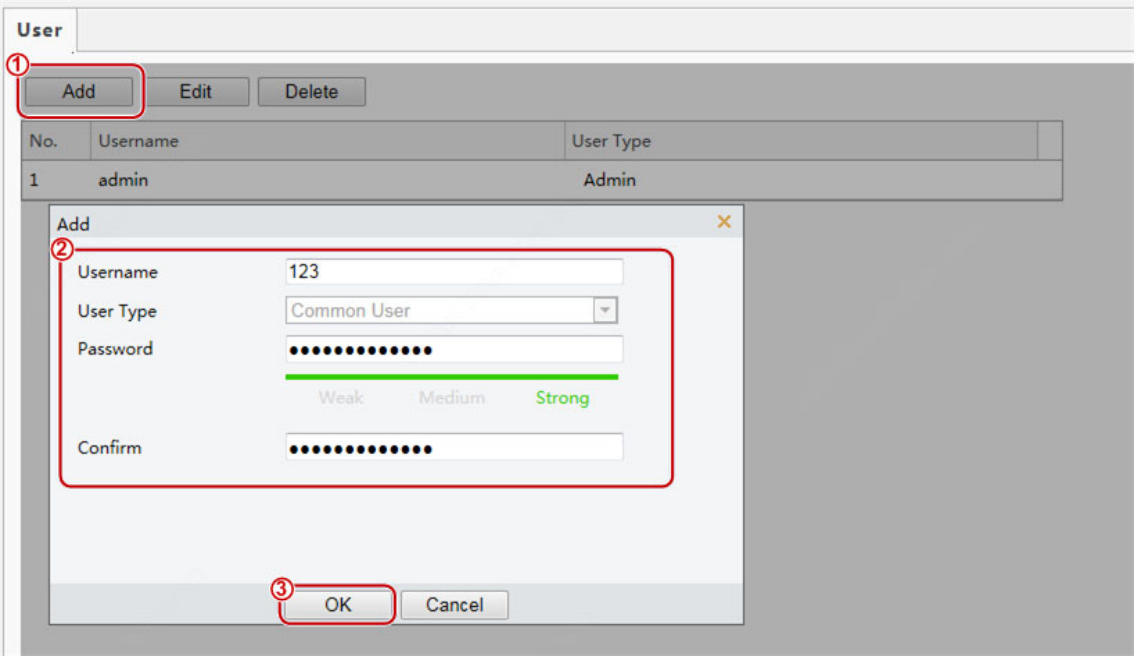
(1) Adding an ordinary user

(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.

Figure7-19 Ordinary User Adding Interface



(2) Editing an ordinary user

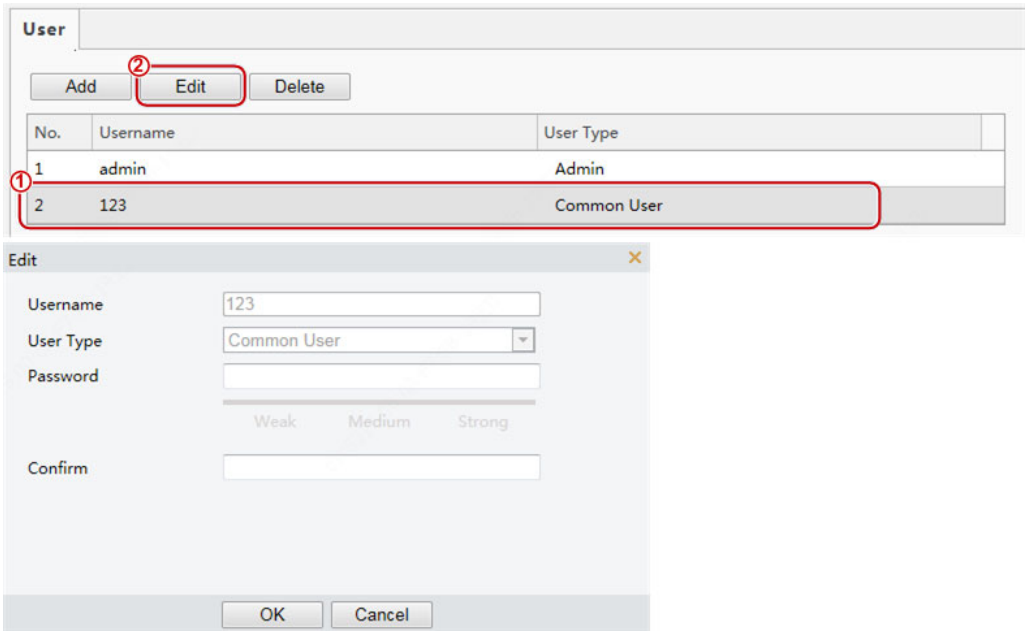
The following uses an ordinary user as an example. The steps of editing **admin** are the same as those of editing an ordinary user.

(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.

Figure7-20 Ordinary User Information Editing Interface



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

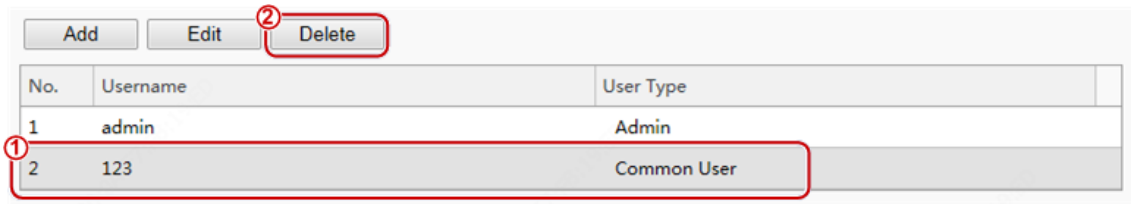
(3) Deleting an ordinary user

(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.

Figure7-21 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

(1) Serial Port

When the face recognition terminal conducts O&M management on a gate machine through a serial port or it connects to an ID 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.

Figure7-22 Serial Port Configuration Interface

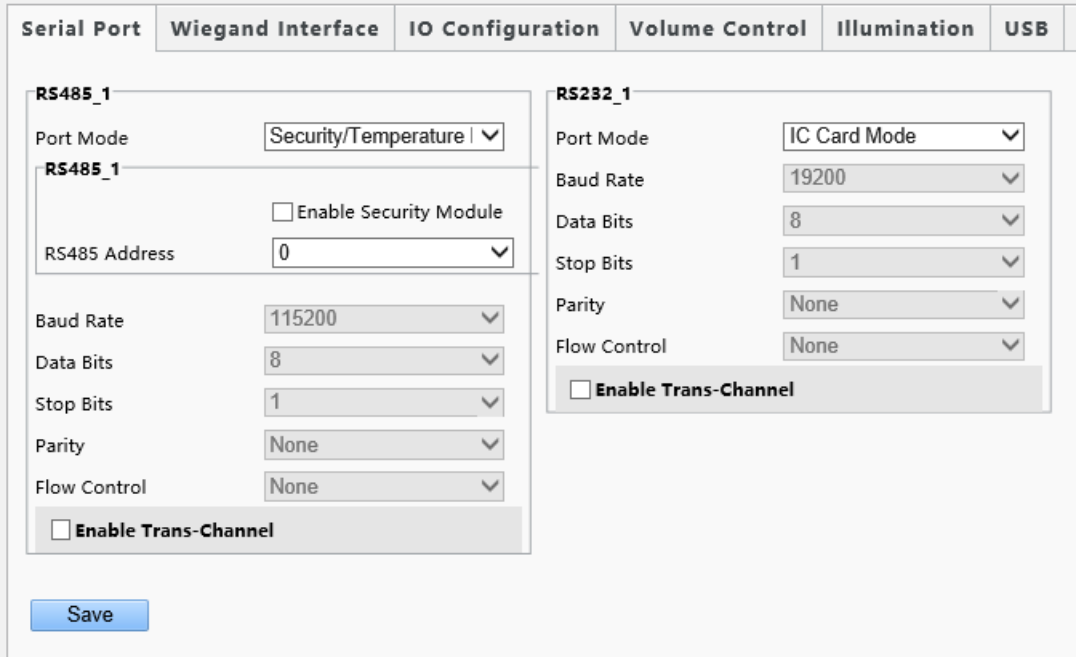


Table7-9 Parameter Description and Configuration

Parameter	RS485_1	RS232_1
Port Mode	• Security Module: Select this option when the face recognition terminal connects to a digital detection module through the RS485 serial port. • Gate Mode C: Select this option when O&M management is required for gate machines connected to the face recognition terminal through the RS485 serial port. Only the FG8223 gate machine supports this option. • Gate Mode B: The current gate machines do not support this option. • None: Select this option when no external device is connected or external devices do not need O&M management. • Door Magnet Mode: Select this option when the face recognition terminal connects to a door magnet through the RS485 serial port. Set this parameter based on actual scenes. Note: The security module function is not applicable currently.	• ID Card Mode: Select this option when the face recognition terminal connects to an ID card reader. • QR Code Mode: Select this option when the face recognition terminal connects to a QR code reader. • IC Card Mode: This option is displayed when the face recognition terminal has a built-in card reader. • Two-to-One Mode: Select this option when the face recognition terminal connects to an IC card reader (model: EG121@ID). • Gate Mode A: Select this option when O&M management is required for gate machines connected to the face recognition terminal through the RS232 serial port. The FG6221, FG8221, and FG8222 gate machines support this mode. • Gate Mode D: Select this option when O&M management is required for gate machines connected to the face recognition terminal through the RS232 serial port. (The EL-S802, EL-S801, EL-S601, EL-B602, EL-B501, DEL-811, DEL-611, and DEL-511 gate machines support this mode.) • Not Configured: Select this option when no

		external device isconnected or external devices do not need O&M management. • Bluetooth Mode: This option is displayed when the face recognition terminal is used with a smart lock via Bluetooth. • Wiegand IC Card Mode: Select this option when the face recognition terminal connects to a card reader through RS232. Set this parameter based on actual scenes.
	NOTE! For RS485 and RS232 serial ports, Port Mode cannot be set to a gate mode at the same time.	
Enable Security Module	The configuration is not supported.	/
RS485 Address	The configuration is not supported.	/
Baud Rate	The configuration is not supported. Use the default value.	
Data Bits/ Stop Bits/ Parity/ Flow Control	Keep the default values as follows: Data Bits: 8 Stop Bits: 1 Parity: None Flow Control: None NOTE! The parameters cannot be set when **Port Mode** is set to **IC Card Mode**.	
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.

(2) 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 with a built-in IC card reader.

Figure7-23 Wiegand Interface Configuration Window

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

Table7-10 Parameter Description and Configuration

Parameter	Configuration
Protocol	Set it to **Wiegand 26** or **Wiegand 34** based on actual scenes.
Format	The options are as follows: • Ascending Order The sequence of the card No. read by 2M card reader (EG121@IC)is the positive sequence. When the sequence is the same as the sequence of the card No. read by 2M card reader, select **Ascending Order** in the input/output. • Descending Order When the sequence is opposite to the sequence of the card No. read by 2M card reader, select **Descending Order** in the input/output. The default value is **Ascending Order**. Set this parameter based on actual scenes.

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

(3) IO Configuration

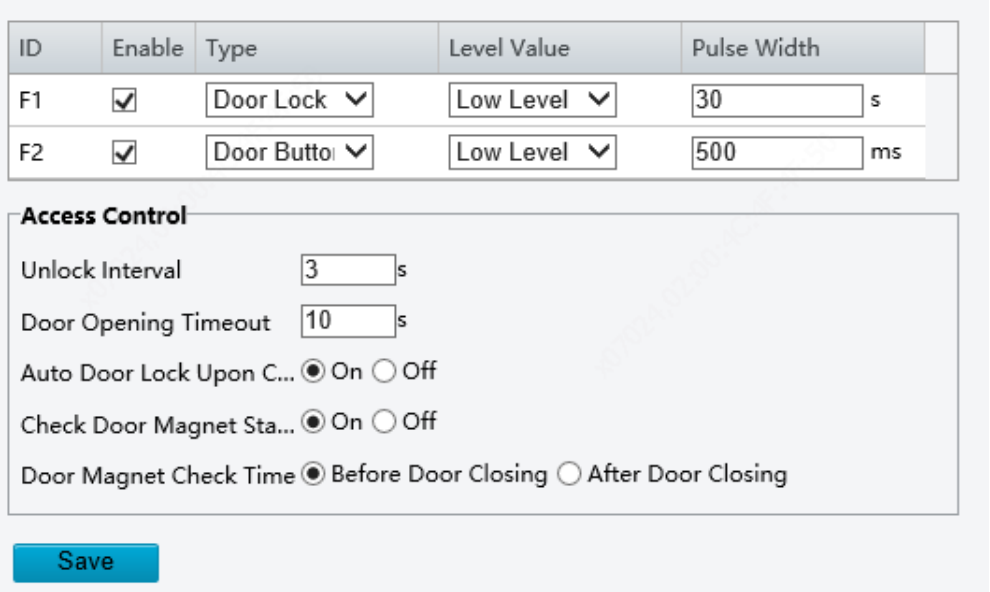
The face recognition terminal connects to gate machines, door locks, or access control buttons and sends the door opening signal to them. Perform the following operations to complete configuration:

(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.

Figure7-24 IO Configuration Interface



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

Table7-11 Parameter Description and Configuration

Parameter	Parameter Description and Configuration
F1/F2	F1/F2 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. IO ports support the following types of external devices: • Door lock: The face recognition terminal outputs door opening signals to door locks through an IO port. **Pulse Width** 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 • 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 **Level Value** can be set to **Low Level** or **High Level**. The value should be consistent with the input and output signal level supported by external devices.
Unlock Interval	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 **0**, door unlock will be triggered 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 Auto Door Lock Upon Closing 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 **NOTE!** • It is not recommended to set it to a very small value. Otherwise, normal door opening will be affected. • The generation of a door magnet alarm is related to door opening timeout.
Auto Door Lock Upon Closing	Select whether to enable auto door lock upon door closing. The options are as follows: • On: When the door magnet detects that the door is closed and the door closing time exceeds the value of Door Opening Timeout, the door will be locked automatically. • Off: The auto door lock upon closing is disabled and the door closing time is the door opening duration.
Check Door Magnet Status Before Closing	The options are as follows: • On: The door magnet status is checked before closing. • Off: The door magnet status is not checked before closing.
Door Magnet Check Time	This parameter is available only after Check Door Magnet Status Before Closing is set to **On**. Set this parameter based on the lock type. • Before Door Closing: Select this value for electronic locks. • After Door Closing: Select this value for electromagnetic locks.

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

(4) Audio

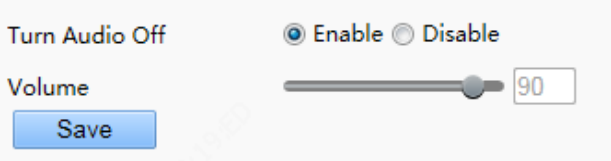
If the face recognition terminal connects to an audio device, configure audio information on the **Audio** tab page.

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

NOTE!

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

Figure7-25 Audio Configuration Interface



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

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

(5) Illumination

NOTE!

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

(1.1) LCD Light

Configure the LCD light for the face recognition terminal on the **Illumination** tab page.

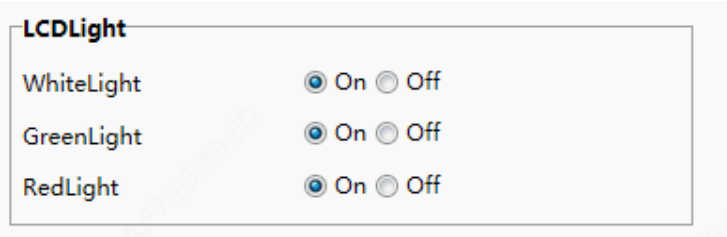
NOTE!

- Some devices do not support the LCD light configuration and the **LCDLight** area will not be displayed for them.

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

(2) Set the LCD light as required.

Figure7-26 LCD Light Configuration Interface



Status Light	Operation
WhiteLight	When the face recognition terminal is in standby mode, the LCD light shows white. • On: The LCD light shows white when the face recognition terminal is in normalstandby mode. • Off: The LCD light does not show white when the face recognition terminal is in normal standby mode.
GreenLight	The LCD light of the face recognition terminal shows green in the case of normal passage. • On: The LCD light of the face recognition terminal shows green in the case ofnormal passage. • Off: The LCD light of the face recognition terminal will not show green in the case of normal passage.

RedLight	The LCD light of the face recognition terminal shows red when an exception occurs during personnel passage. • On: The LCD light of the face recognition terminal shows red when an exception occurs during personnel passage. • Off: The LCD light of the face recognition terminal will not show red when anexception occurs during personnel passage.

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

(1.2) Energy Conservation

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.

Figure7-27 Energy Conservation Configuration Interface

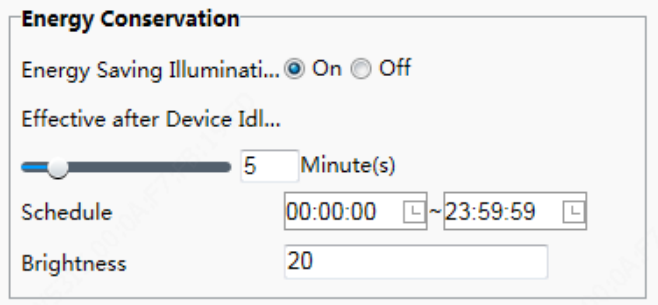


Table7-12 Parameter Description and Configuration

Parameter	Description	Configuration
Energy Saving Illumination	• On: When the face recognition terminal detects a face within the preset Schedule, 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 Effective after Device Idle For, 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 Schedule regardless of whether the face recognition terminal detects a face. • Off: Lights are steady on regardless of whether the face recognition terminal detects a face. Energy conservation is disabled on the lights. Energy saving illumination is disabled by default.	Set this parameter based on actual scenes.
Effective after Device Idle For	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. Value range: [1–30]min; default value: 5min	Set this parameter based on actual scenes.
Schedule	After Energy Saving Illumination 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. The value ranges from 00:00:00 to 23:59:59 and the unit can be accurate to seconds. **NOTE!** When Energy Saving Illumination is set to On, the default value of Schedule is [00:00:00~23:59:59]. When Energy Saving Illumination is set to Off, Schedule is unavailable.	Set this parameter based on actual scenes.

Brightness	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. Value range: [0–200]; default value: 20 If it is set to **0**, the light supplement lamp is turned off. The brightness can take effect only after the display screen becomes off again.	Set this parameter based on actual scenes.

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

(6) USB

The configuration is not supported.

(7) Card Reader

The configuration is not supported.

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.

Figure7-28 Device Info Configuration Interface

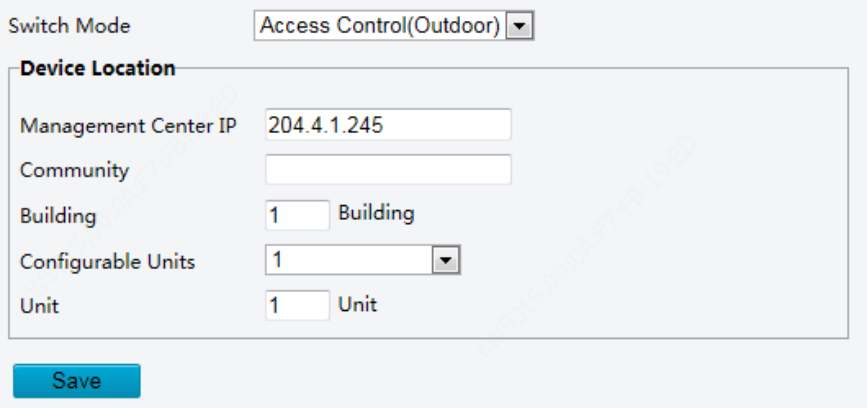


Table7-13 Parameter Description and Configuration

Parameter	Parameter Description and Configuration
Switch Mode	Set the work mode for the access control terminal. The options include the following: • Access Control (Outdoor): normal access control device, which has the call, password-based door opening, face scan-based door opening, and other functions. • Normal Access Control: The access control terminal is a common access control device which does not support call and password-based door opening functions. For detailed operations, see the *Face Recognition Terminal User Manual*. Set this parameter based on actual application scenes.
Management Center IP	Enter the IP address of the management center. After configuration, a user can tap **Call Management Center** on the GUI to call the management center. **NOTE!** The management center IP address must be in the same network segment as the device.

Community	Enter the name of the community to which the device belongs. A string of 1 to 36 characters (1 to 12 Chinese characters) can be entered.
Building	• Enter the No. of the building where the device is located. • The value must be an integer in the valid range of 1 to 99.
Configurable Units	Select the quantity of units that can be served by the device from the drop-down list. The options are 0, 1, 2, and 3.
Unit	Enter the No. of the unit where the device is located. The value is an integer in the valid range of 0 to 9.

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

9. Personalization

(1) 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.

Figure7-29 Ad Mode Setting Interface

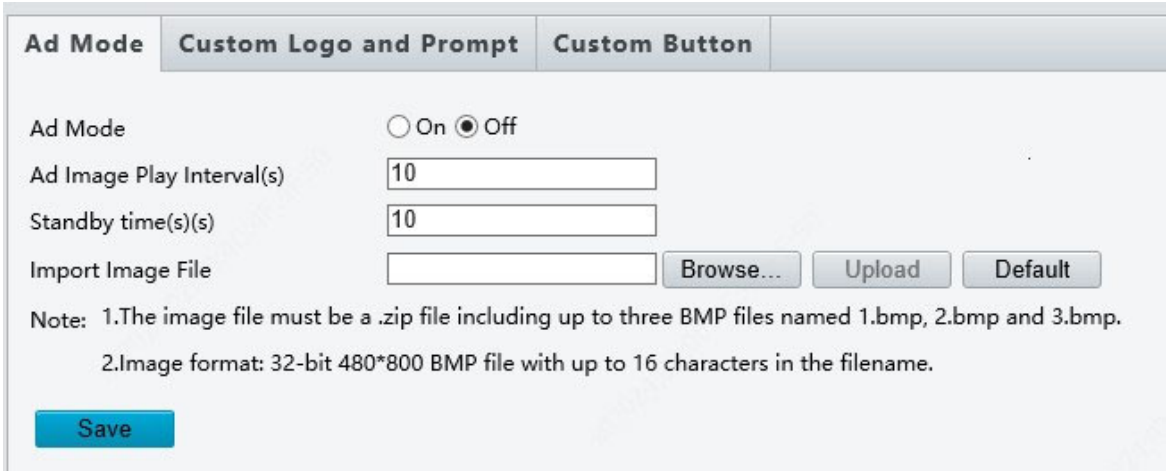


Table7-14 Parameter Configuration

Parameter	Description and Configuration
Ad Mode	• On • Off Select whether to enable the ad mode based on actual conditions.
Ad Image Play Internal(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. The value is an integer in the range of 10s to 3600s. The default value is 10s. The face recognition terminal exits the ad mode when the face scan fails or a user taps the

	screen.
Import Image File	Users can define ad images. The requirements for ad images are as follows: • The file to be imported must be a .zip file. The file can contain three .bmp pictures at most, which are named 1.bmp, 2.bmp, and 3.bmp, respectively. • Image format: The image must be a 32-bit .bmp file with the size of 480x800.

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

(2) 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.

Figure7-30 Custom Logo and Prompt Interface

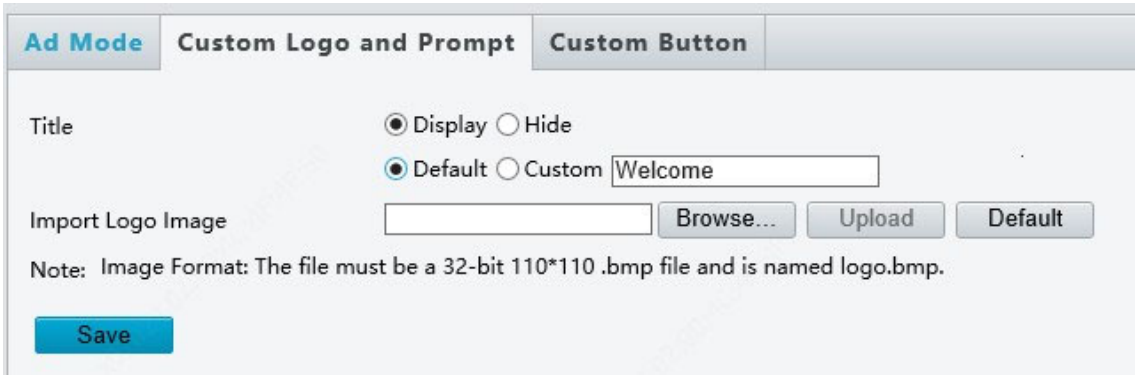


Table7-15 Parameter Configuration

Parameter	Description and Configuration
Title	• Display: The title bar is displayed. The title content can be set as follows: ➢ Default: "Welcome" is displayed on the title bar. ➢ Custom: You can define the title content. A string of 0–14 characters can be entered. • Hide: The title bar is not displayed.
Import Logo Image	Users can define a logo image. The requirements for a logo image are as follows: The image must be a 32-bit .bmp file with the size of 110x110 and named logo.bmp.

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

(3) Custom Button

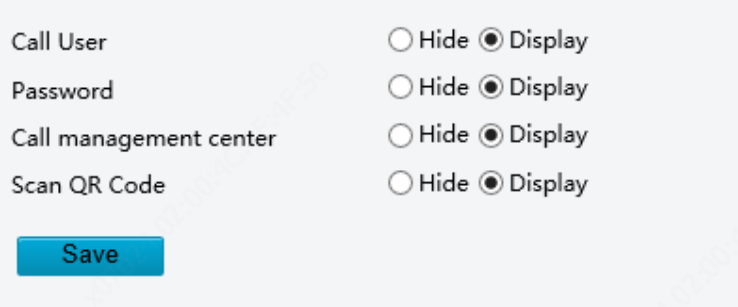
The face recognition terminal supports custom buttons. The configuration is as follows:

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

(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.

Figure7-31 Custom Button Interface



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

7.3.2 Network

1. Network

For the Ethernet configuration interface, see Ethernet.

2. UNP

The configuration is not supported.

3. DNS

The configuration is not supported.

4. Port

The configuration is not supported.

5. DDNS

The configuration is not supported.

6. EZCloud

The configuration is not supported.

7. E-mail

The configuration is not supported.

8. SNMP

The configuration is not supported.

9. 802.1x

The configuration is not supported.

7.3.3 Image

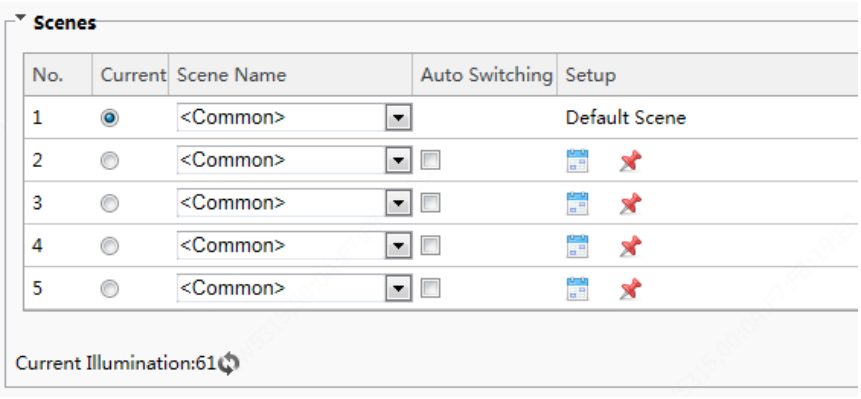
1. Image

(1) 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**.

Figure7-32 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.
- Standard: standard image parameter, which is the default image style.
- Bright: The image brightness is improved based on the standard mode.
- Vivid: The image saturation is improved based on the standard mode.
- Road Highlight Compensation(HLC): The road highlight can be suppressed so that clear images can be obtained. It is applicable to road scenes.
- Park Highlight Compensation(HLC): The park highlight can be suppressed so that clear images can be obtained. It is applicable to park scenes.
- WDR: recommeded for scenes with high-contrast lighting, such as window, corridor, front door or other scenes that are bright outside but dim inside.
- 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).

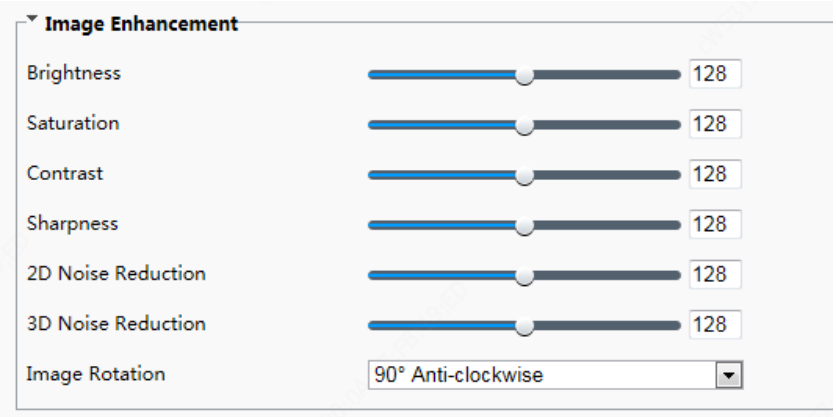
(2) Image Enhancement

NOTE!

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

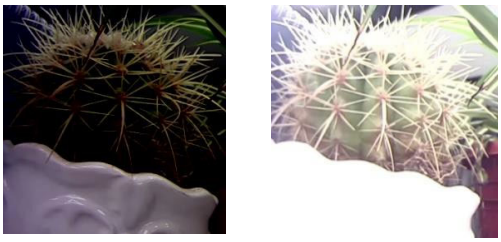
(1) Click **Setup** > **Image** > **Image** and then click **Image Enhancement**.

Figure7-33 Image Enhancement Interface



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

Table7-16 Parameter Description

Item	Description
Brightness	Set the degree of brightness of images.  Low brightness High brightness
Saturation	The amount of a hue contained in a color.  Low saturation High saturation
Contrast	Set the degree of difference between the blackest pixel and the whitest pixel.  Low contrast High contrast
Sharpness	Contrast of boundaries of objects in an image.

Item	Description
	  Low sharpness High sharpness
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	Rotation of the image.   Normal Flip Vertical   Flip Horizontal 180   90°Clockwise 90°Anti- clockwise

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

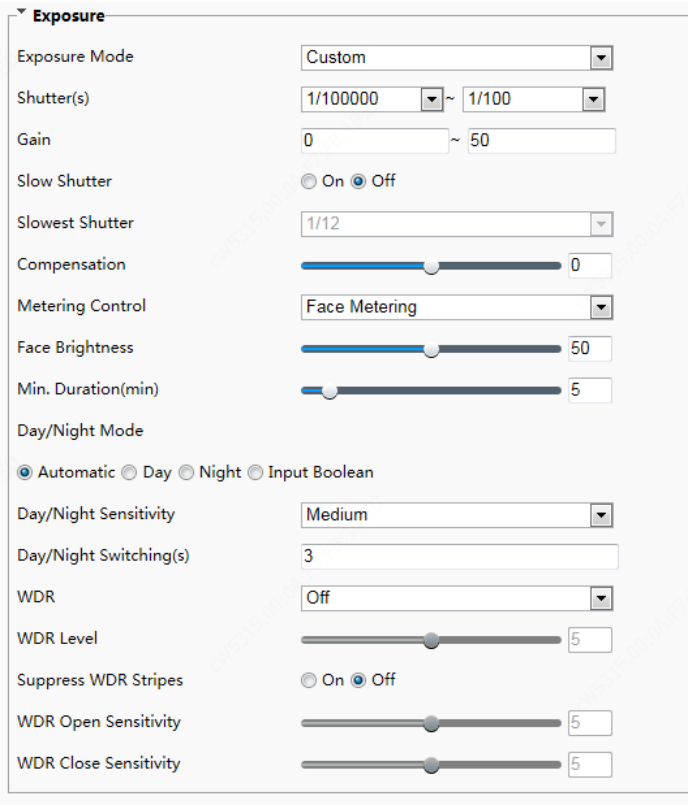
(3) Exposure

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**.

Figure7-34 Exposure Configuration Interface



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

Table7-17 Parameter Description and Configuration

Item	Description
Exposure Mode	Select a mode to achieve the desired exposure effect. • Automatic: The device automatically adjusts exposure based on the environment. • Custom: The user sets exposure as needed. • Shutter Priority: The device prefers to adjust the shutter to control the image quality. • Indoor 50Hz: The device reduces stripes by limiting shutter frequency. • Indoor 60Hz: The device reduces stripes by limiting shutter frequency. • Manual: The device allows fine-tuning image quality by setting shutter, gain and iris manually. Low Motion Blur: The device controls the minimum shutter to reduce motion blur in face photos captured in motion.
Shutter(s)	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. **NOTE!** • You can set a shutter speed when **Exposure Mode** is set to **Manual** or **Shutter Priority**. • If **Slow Shutter** is set to **Off**, the reciprocal of the shutter speed must be greater than the frame rate.
Gain	Control image signals so that the device outputs standard video signals according to the light condition. **NOTE!** You can set this parameter only when **Exposure Mode** is set to **Manual** or **Gain Priority**.
Slow Shutter	Improves image brightness in low light conditions.

	NOTE! You can set this parameter only when **Exposure Mode** is not set to **Shutter Priority** and when **Image Stabilizer** is disabled.
Slowest Shutter	Set the slowest shutter speed that the device can use during exposure. **NOTE!** You can set this parameter only when **Slow Shutter** is set to **On**.
Compensation	Adjust the compensation value as required to achieve the desired effects. **NOTE!** You can set this parameter only when **Exposure Mode** is not set to **Manual**.
Metering Control	Set the way the device measures the intensity of light. ● Center-Weighted Average Metering: The device measures light mainly in the central part of images. ● Evaluative Metering: The device measures light in the customized area of images. ● Spot Metering: It is similar to **Evaluative Metering** but the difference is that the image brightness cannot be improved. ● Face Metering: The device adjusts the image quality in poor lighting conditions by controlling the brightness of captured face photos in Face scene. ● Interlligent Metering: In case of poor illumination or backlight in the "face" scene, when someone passes through the terminal the terminal controls the brightness of the captured person photo or face photo to improve the snapshot quality. **NOTE!** You can set this parameter only when **Exposure Mode** is not set to **Manual**. The default value is **Face Metering**.
Face Brightness	This parameter is displayed only when Metering Control is set to **Face Metering**. In **Face Metering** mode, the system adjusts the exposure based on the value of **Face Brightness** 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 **Face Brightness** value indicates higher image brightness on the device and brighter face snapshot photos.
Min. Duration(min)	This parameter is displayed only when Metering Control is set to **Face Metering**. 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	● 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. ● Day: The device provides high-quality color images using the existing light. ● Night: The device provides high-quality black and white images using the existing light. Input Boolean: The device provides high-quality images by using external light.
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. **NOTE!** You can set this parameter only when **Day/Night Mode** is set to **Automatic**.
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. **NOTE!** You can set this parameter only when **Day/Night Mode** is set to **Automatic**.

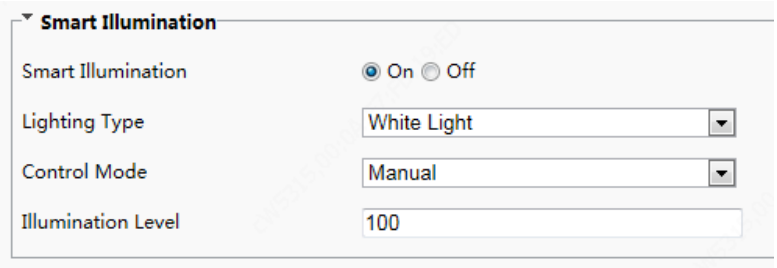
WDR	Enable WDR to distinguish the bright and dark areas in the same image. **NOTE!** This parameter is available only when **Exposure Mode** is set to **Automatic**, **Custom**, **Shutter Priority**, **Indoor 50Hz**, or **Indoor 60Hz** and electronic image stabilization and defog are disabled. You can set this parameter only when **Exposure Mode** is neither **Customize** nor **Manual** and when **Image Stabilizer** is disabled.
WDR Level	After enabling the WDR function, you can improve the image by adjusting the WDR level. **NOTE!** 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.
Suppress WDR Stripes	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 Open Sensitivity	Enable the WDR sensitivity. **NOTE!** This parameter is available only when **WDR** is set to **Automatic**.
WDR Close Sensitivity	Disable the WDR sensitivity. **NOTE!** This parameter is available only when **WDR** is set to **Automatic**.

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

(4) Smart Illumination

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

Figure7-35 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 **White Light** only currently.
Control Mode	• Manual: After smart illumination is enabled, the light supplement lamp automatically controls illumination. • Manual –Always on: After smart illumination is enabled, the light supplement lamp will always supplement illumination.
Illumination Level	Set the intensity level of the IR light. The greater the value, the higher the intensity. **0** means that the IR light is turned off.

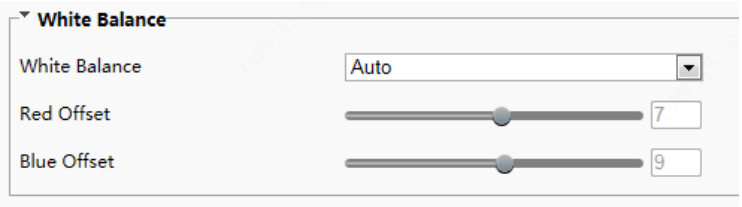
(3) To restore the default settings, click **Default**.

(5) 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**.

Figure7-36 White Balance Configuration Interface



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

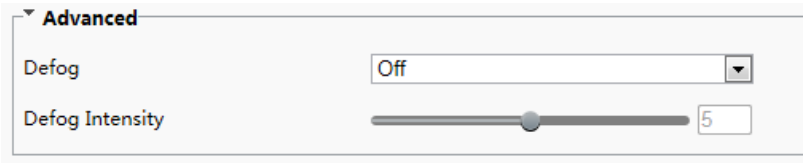
Item	Description
White Balance	Adjust the red or blue offset of the image: ● Auto/ Auto 2: The device adjusts the red and blue offset automatically according to the light condition (the color tends to be blue).If the images are still unnaturally red or blue in Auto mode, please try Auto2. ● Fine Tune/ Fine Tune(Base on night mode): Allow you to adjust the red and blue offset manually. ● Sodium Lamp: The camera adjusts red and blue offset automatically according to the light condition (the color tends to be red). ● Outdoor: Suitable for outdoor environment with a relatively greater color temperature range. ● Locked: Lock the current color temperature without change.
Red Offset	Adjust the red offset manually. **NOTE!** You can set this parameter only when **White Balance** is set to **Fine Tune**.
Blue Offset	Adjust the blue offset manually. **NOTE!** You can set this parameter only when **White Balance** is set to **Fine Tune**.

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

(6) 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 **Auto** 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.

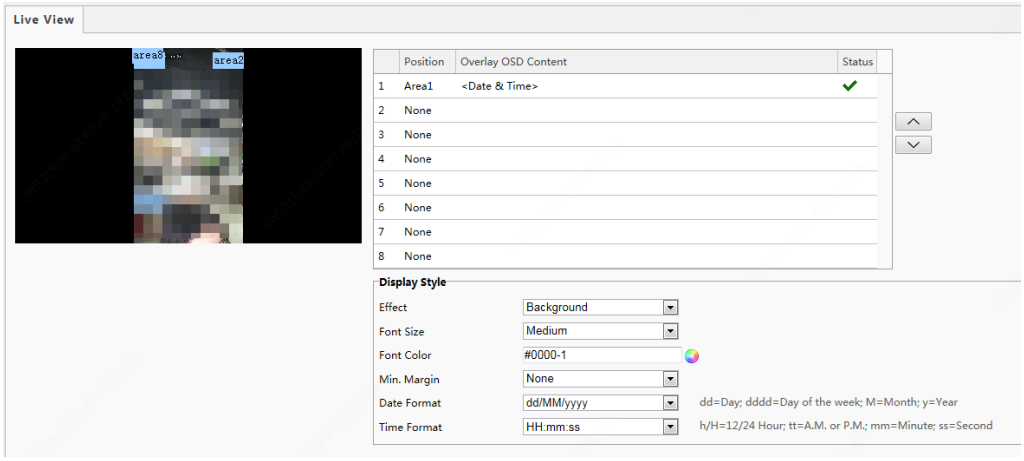
(2) Enable the defog function and then select a level for the scene. Level 9 achieves the maximum defog effects, and level 1 achieves the minimum.

(3) 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.

(1) Click **Setup** > **Image** > **OSD**.



(2) 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 to adjust the sequence of display.

(3) 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.

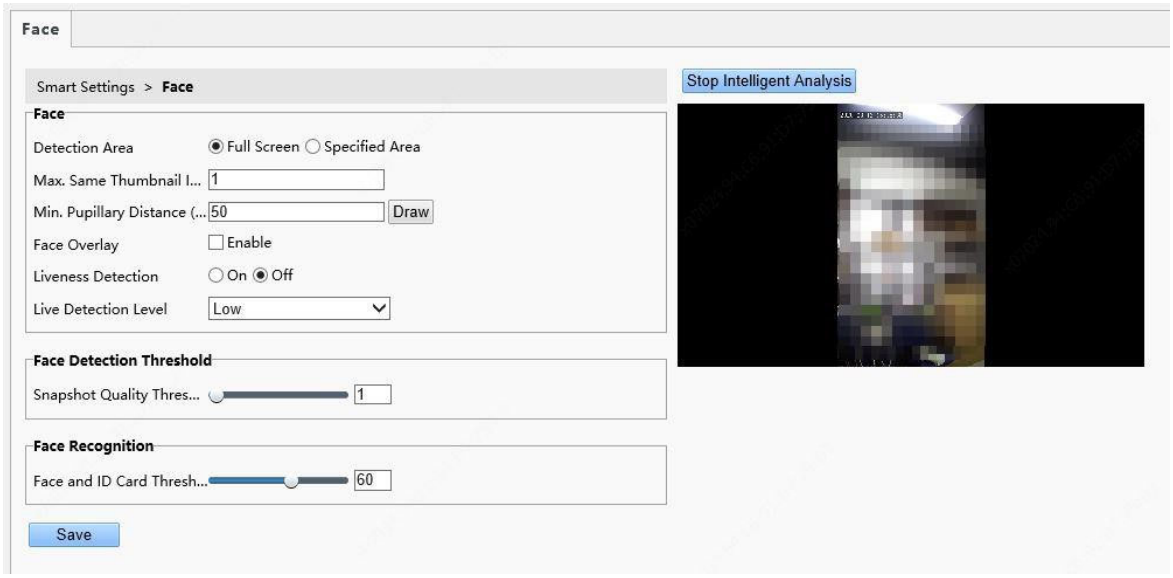
7.3.4 Intelligent

1. Face Snapshot

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 andmatch.

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

Figure7-37 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.

Table7-18 Parameter Description and Configuration

Pane	Parameter	Description and Configuration
Face	Detection Area	● Click **Full Screen**, indicating that the full-screen face photo will be detected. ● Click **Specified Area**, indicating that face photo of a specified area willbe detected.

	Max. Same	It is unavailable currently.
	Min. Pupillary Distance (px)	You can draw the pupillary distance by using the mouse in the live view on the right side of the interface. A photo will be collected when the value of **Min. Pupillary Distance(px)** is within the preset valid range. The value range is 20 px to 150 px.
	Face Ovelay	The configuration is not supported.
	Liveness Detection	Click **On** 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: **High**, **Medium**, and **Low**. A higher liveness detection level indicates a higher accuracy that non-real people can be detected. The default value is **Low**.
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. Value range: [1–100]; default value: 1 Note: After mask detection is enabled, **Snapshot Quality Threshold** must be set to **1**.
Face Recognition	Face and ID Card Threshold	Threshold for 1:1 match on ID cards. When the similarity between a face snapshot photo and the photo on the ID card reaches the preset quality threshold, the match is successful. Value range: [1–100]; default value: 60

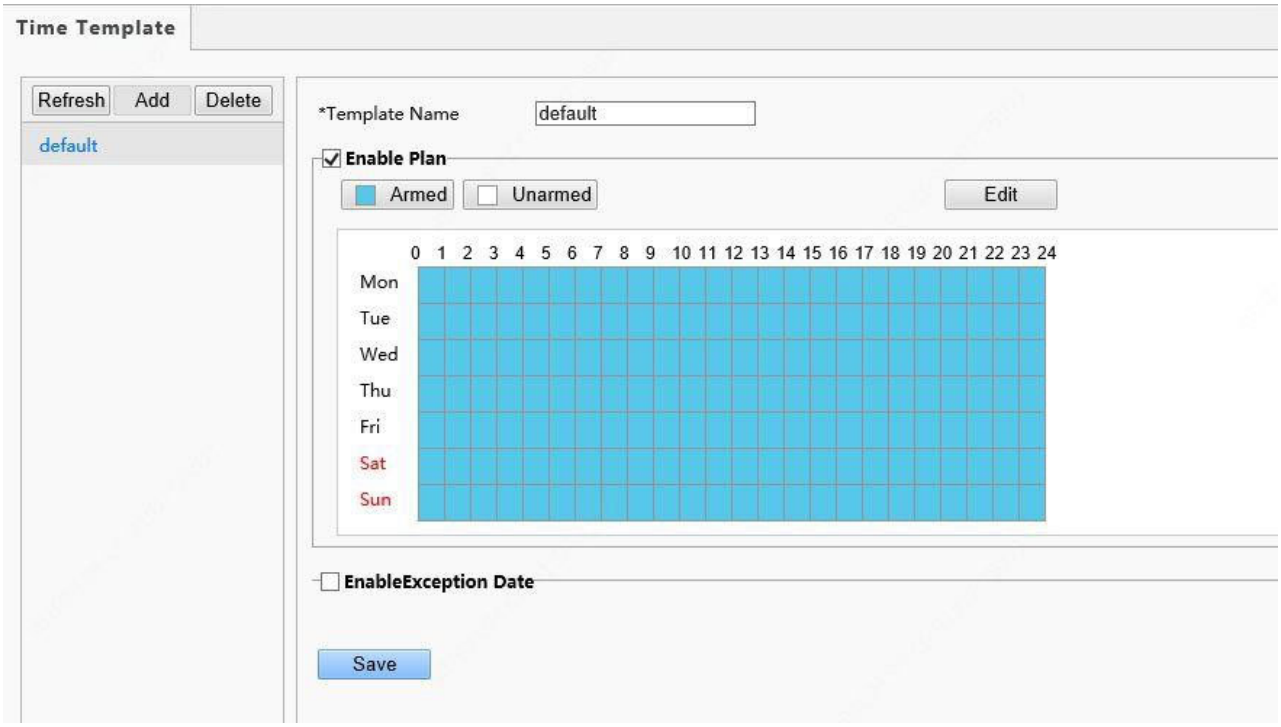
(1) Click **Save** to complete the configuration.

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

2. 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.

Figure7-38 Time Template



- Adding a time template

NOTE!
A maximum of 16 time templates can be set.

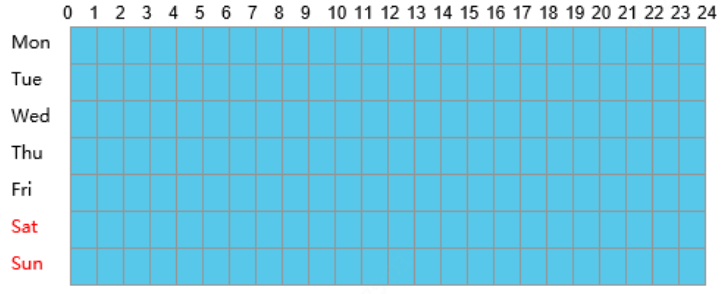
(1) Choose **Setup** > **Intelligent** > **Time Template** and click **Add**.

(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 

and drag the mouse on the time table to set the arming time range. The time accuracy is 1 hour.

Figure7-39 Time Table for Dragging the Mouse to Set the Arming Time Range



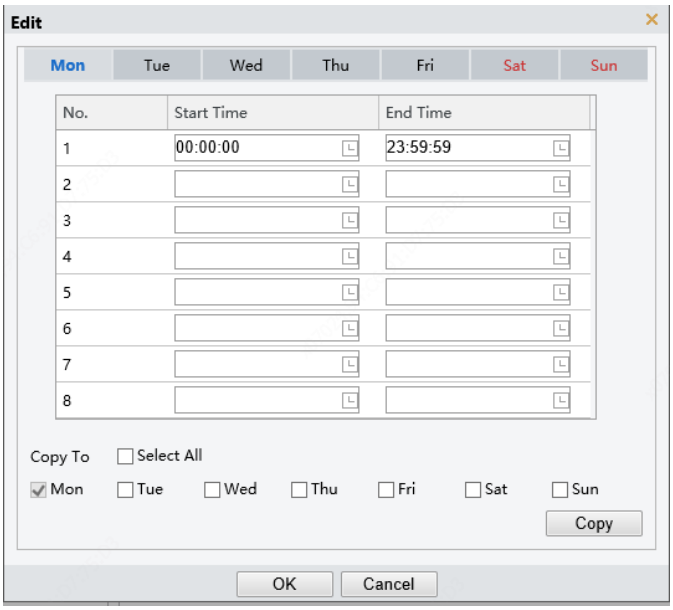
  - You can also click 

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.

Figure7-40 Edit Interface

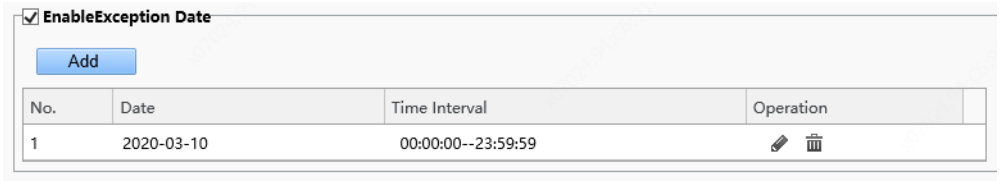


- **EnableException Date**: Select the check box to enable exception dates.
- Set an exception date.

  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.

Figure7-41 EnableException Date



(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.

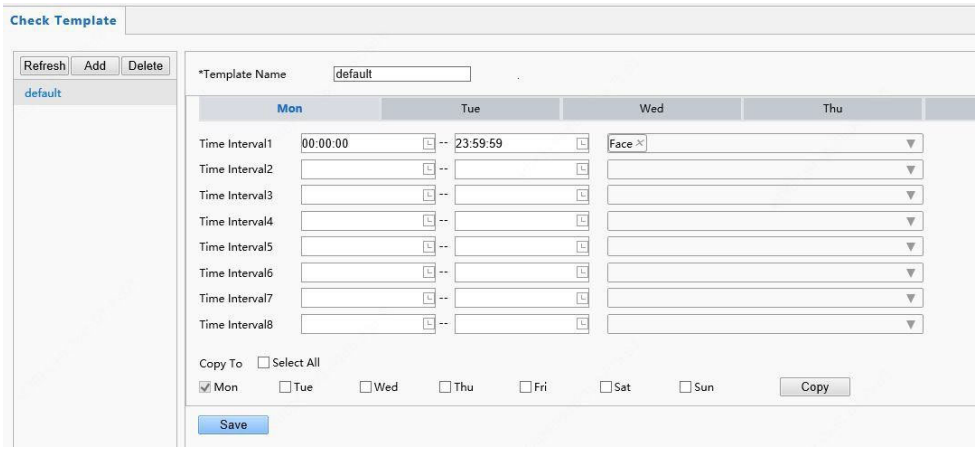
NOTE!

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.

3. 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.

Figure7-42 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. The value is a string of 1–63 characters.
- 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:

  - IC Card: The face recognition terminal conducts 1:N match on the acquired card number (IC card number or ID 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.
  - IC Card+Face: The face recognition terminal conducts 1:N match on the acquired card number (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 five 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.

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.

Figure7-43 Face Library Interface

(1) 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.

Figure7-44 Add Face Library Interface

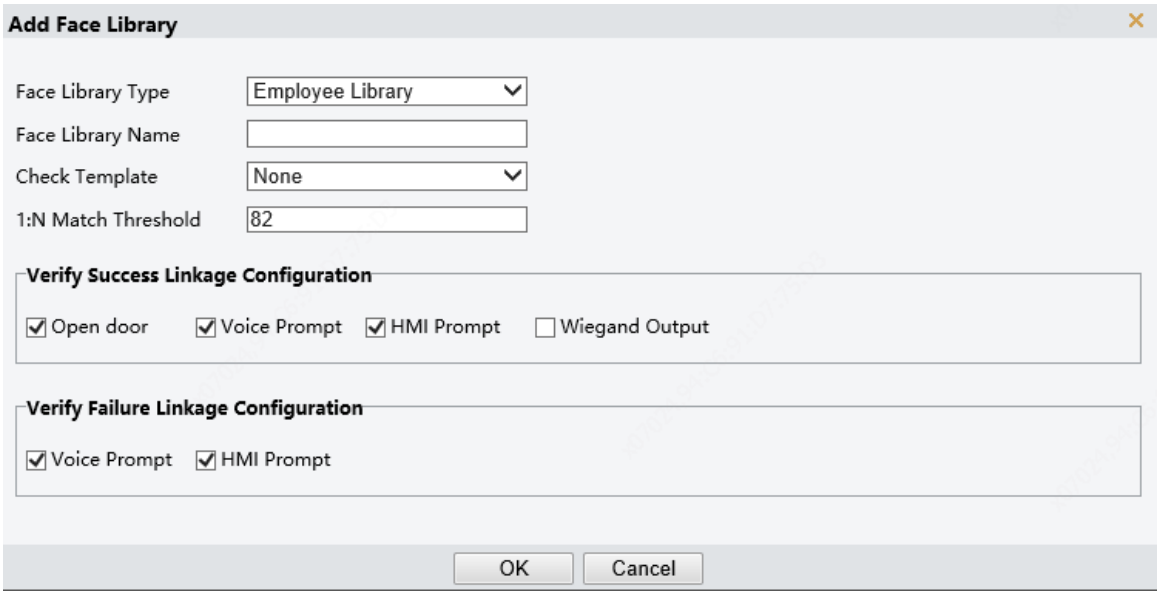


Table7-19 Parameter Configuration

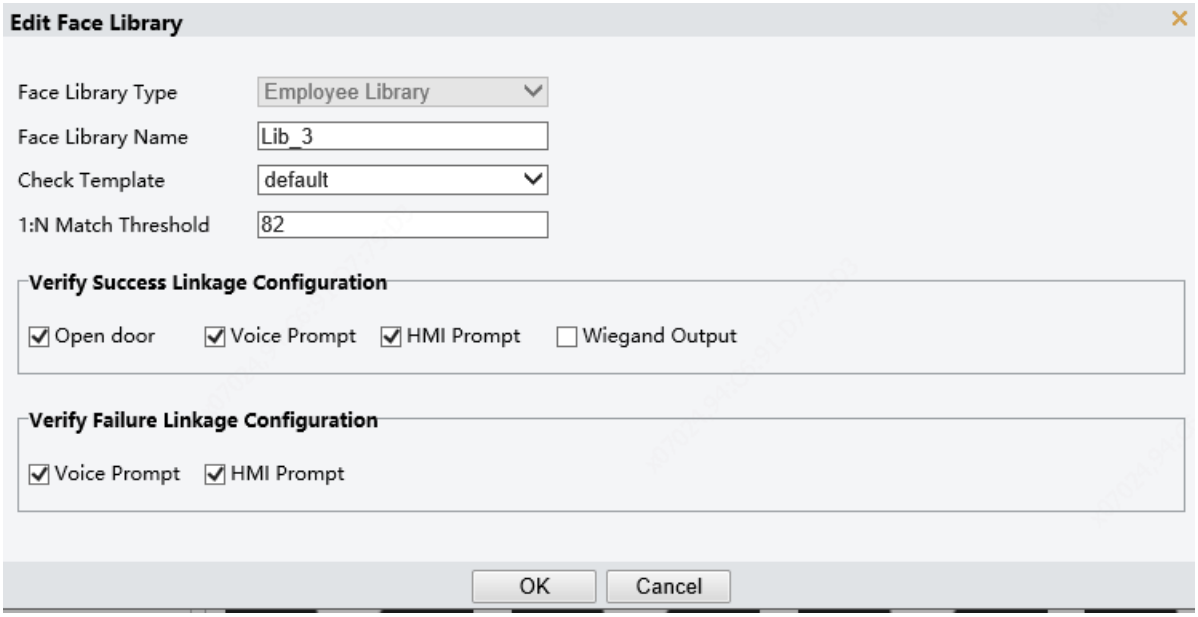
Parameter	Description and Configuration
Face Library Type	Set the parameter to either of the following options based on the actual conditions: • Employee Library • Visitor Library
Face Library Name	Enter a library name. A string of 1 to 63 characters can be entered.
Check Template	Select a check template from the drop-down list. Check templates are added on the Check Template 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	The options are as follows: • **Open door**: After the authentication succeeds, a door opening signal is sent totrigger door opening. • **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 theauthentication succeeds.
Verify Failure Linkage Configuration	The options are as follows: • **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

(1) Select a required face library and click **Edit**.

(2) In the displayed **Edit Face Library** interface, modify parameters by referring to the description in Adding a face library.

Figure7-45 Edit Face Library Interface



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

- Deleting a face library

(1) Select a required face library and click **Delete**.

(2) In the displayed confirmation box, click **OK** to delete the face library.

Deleting a face library will delete people in the face library.

(1) 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.

Figure7-46 Add Face Info Interface

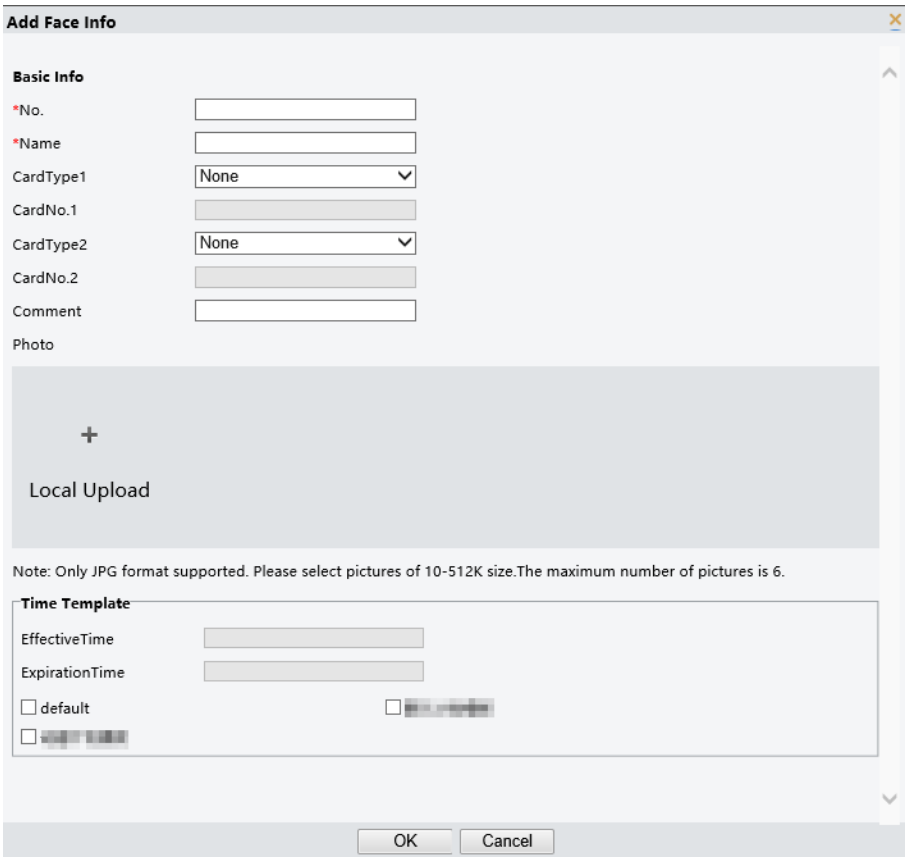


Table7-20 Parameter Configuration

Pane	Parameter	Description and Configuration
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. Requirements: a string of 1 to 63 characters.
	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. Card No. requirements: 1–20 characters, with upper- and lower-case English letters and digits supported.
	Comment	Enter remarks for the person.
Photo	/	Click **Local Upload**. On the displayed interface, select a local face photo for uploading. Allows for uploading up to six photos for a person and supports three photos at most for a person. 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. Select the check box in front of a time template based on the actual situation. NOTE!
	ExpirationTime	
	Time Template	

		• When multiple time templates are bound, the union of the time templates is taken during authentication. • 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.

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

➢ Importing personnel information in batches

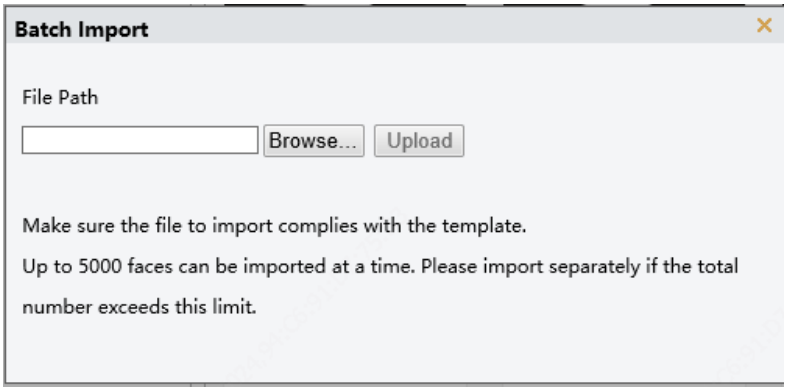
(1) Choose **Setup** > **Intelligent** > **Face Library** and select the face library to which persons are to be added.

(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.

Figure7-47 Batch Import



The figure below shows the import status.

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.

NOTE!

- OET-515H can store information about a maximum of 50,000 persons.
- 2MTHFR-2M can store information about a maximum of 10,000 persons.

- 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.

Figure7-48 Edit Interface

(3) On the displayed edit interface, modify person information by referring to Adding a person.

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

- Deleting persons

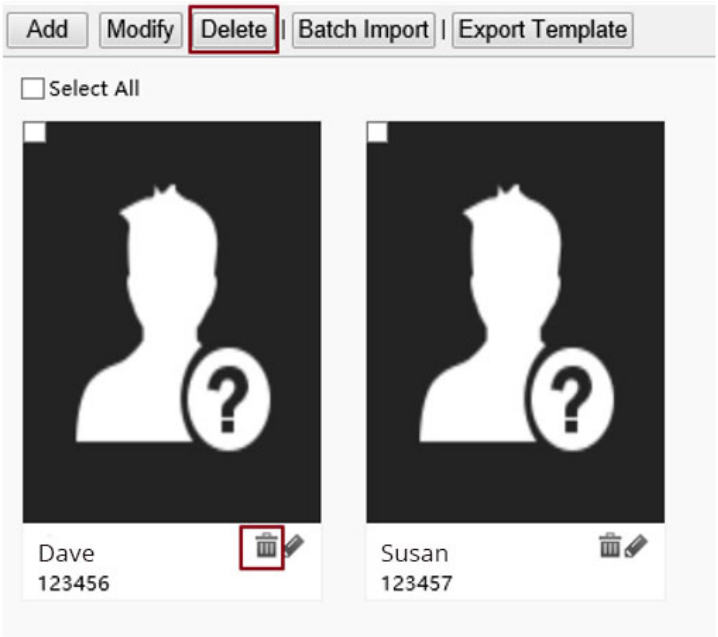
  Persons can be deleted one by one or together.

  ➢ 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.

Figure7-49 Delete Interface

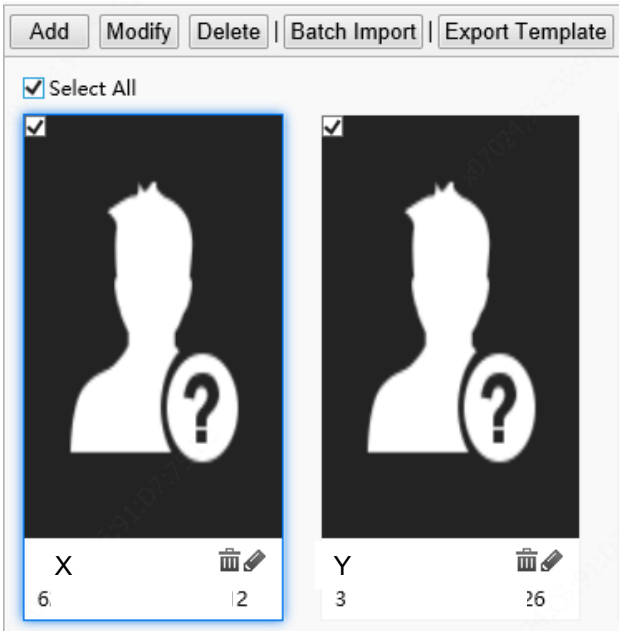


(3) In the displayed deletion confirmation box, click **OK** to complete the deletion.

➢ Deleting all persons

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

Figure7-50 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., name, or ID card No.

Figure7-51 Search Box

5. Advanced Setting

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

Set parameters by referring to the table below.

Figure7-52 Advanced Setting Interface

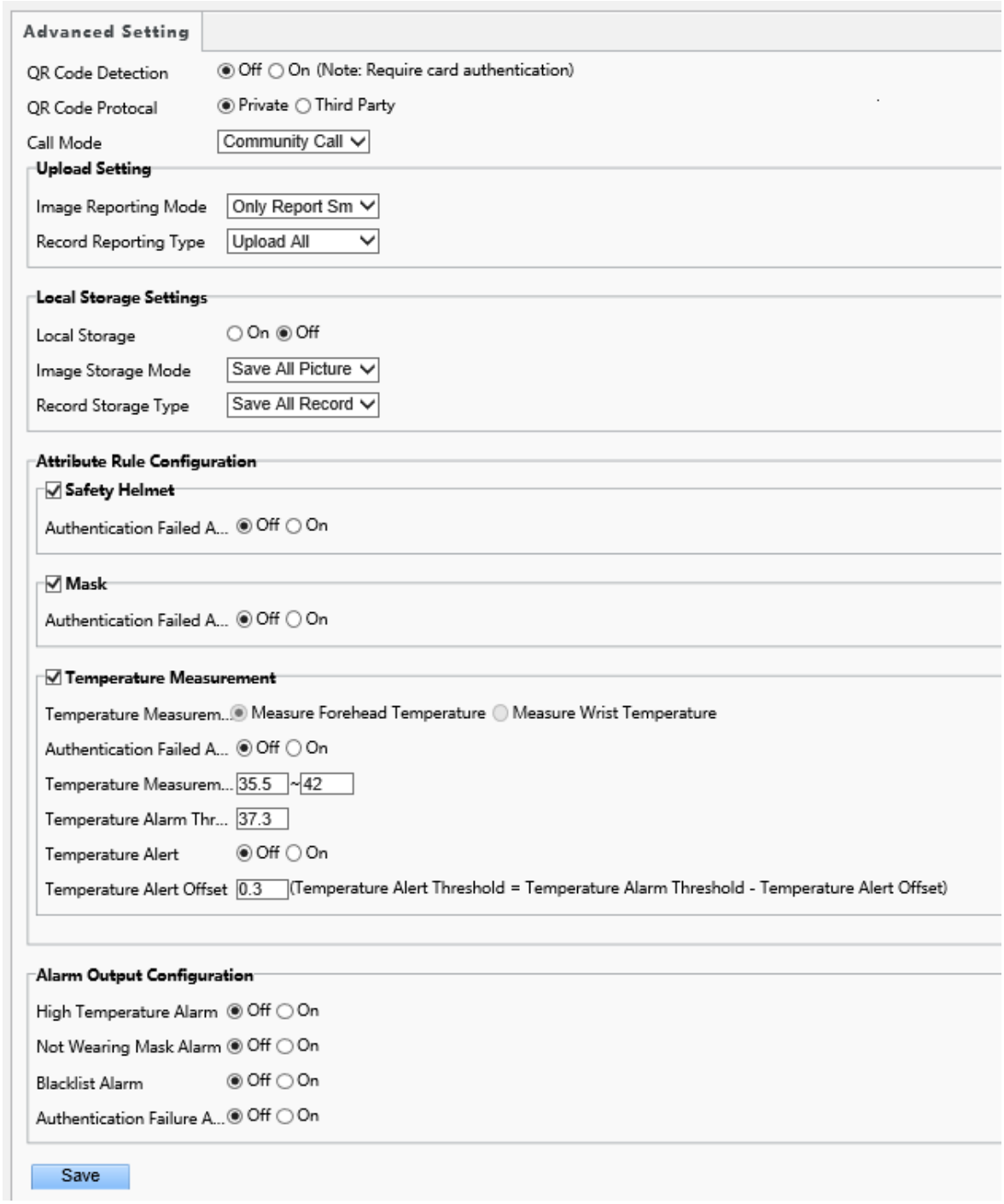


Table7-21 Parameter Description and Configuration

Item	Description
Door Opening Mode	• Authentication: After **Door Opening Mode** is set to **Authentication**, the terminal generates the door opening signal only after a person passes the authentication in Check Template. • Face: After **Door Opening Mode** is set to **Face**, the face recognition 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.

			Set this parameter based on actual application scenes.
QR Code Detection			• Off: When it is set to **Off**, the camera of the face recognition terminal will not collect QR code data. • On: When it is set to **On** and IC card is contained in Check Template, the camera of the face recognition terminal will collect QR code data and authentication will be conducted. For detailed operations, see QR Code-based Door Opening. Set this parameter based on actual application scenes.
QR Code Protocal			• Private When it is set to **Private**, 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). • Third Party The configuration is not supported.
Call Mode			• Community Call: When **Call Mode** is set as **Community Call**, the call created on the visual intercom face recognition terminal is a normal call (calling the indoor monitor). • Cloud Call: When **Call Mode** is set as **Cloud Call**, the call created on the visual intercom face recognition terminal is a cloud call (calling the mobile APP). Set this parameter based on actual application scenes.
Upload Setting	Image Reporting Mode		• Report No Image: When access records are reported to the upper-level platform, no image is reported. • Only Report Large: When access records are reported to the upper-level platform, only large images (that is, panoramic images) are reported. • Only Report Small: When access records are reported to the upper-level platform, only small images (that is, fact cutout images) are reported. • Report All: When access records are reported, both large and small images are reported The default value is **Report All**.
	Record Reporting Mode		• Upload All: The face recognition terminal uploads all personnel pass-through records. • Upload success Record: The face recognition terminal uploads only authentication success pass-through records. Set this parameter based on actual application scenes.
Local Storage settings	Local Storage		The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**.
	Images Storage Mode		**Save All Pictures**: All pictures will be stored, including large pictures and small pictures.
	Record Storage Typpe		**Save All Records**: All access records (including authentication success and authentication failure) will be stored.
Attribute Rule Cofiguration	Safety Helmet	Open Door If Detection Failed	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After **On** is clicked, when the face recognition terminal detects that a person does not wear a safety helmet, a prompt is displayed on the GUI and a voice prompt (please wear a safety helmet) is played but the authentication (face scan, IC card, ID card) and door opening result will not be affected. After **Off** is clicked, when the face recognition terminal detects that a person does not wear a safety helmet, a prompt is displayed on the GUI and a voice prompt (please wear a safety helmet) is played, and the door will not open.

	Mask	Open Door If Detection Failed	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After **On** is clicked, when the face recognition terminal detects that a person does not wear a mask, a prompt is displayed on the GUI and a voice prompt (please wear a mask) is played but the authentication (face scan, IC card, ID card) and door opening result will not be affected. After **Off** is clicked, when the face recognition terminal detects that a person does not wear a mask, a prompt is displayed on the GUI and a voice prompt (please wear a mask) is played, and the door will not open.
	Temperature Measurement	Temperature Measurement	• Measure Forehead Temperature: The forehead temperature will be measured. • Measure Wrist Temperature: The wrist temperature will be measured. Do not need configuration. Terminal will automatically match the temperature measurement mode when it is connected to the digital detection module.
		Authentication Failed And Open The Door	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After **On** is clicked, when the digital detection module detects that a person's temperature exceeds the preset temperature alarm threshold, a prompt is displayed on the GUI and a voice prompt (abnormal temperature) is played but the authentication (face scan, IC card, ID card) and door opening result will not be affected. After **Off** is clicked, when the digital detection module detects that a person's temperature exceeds the preset temperature alarm threshold, a prompt is displayed on the GUI and a voice prompt (abnormal temperature) is played and the door will not open.
		Temperature Measurement Range	Value range: [30–45]; default range: [34–42] Configure the range based on actual application scenes.
		Temperature Alarm Threshold	When the digital detection module detects a temperature higher than the threshold configured here, the "abnormal temperature" alarm is displayed on the GUI and the warning sound is played. Value range: [30–45]; default value: 37.3
		Temperature Alert	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After turning on the temperature alert, 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.
		Temperature Alert Offset	Temperature Alert Threshold = Temperature Alarm Threshold - Temperature Alert Offse
Alarm Output Configuration		High Temperature Alarm	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After turning on the high temperature alarm, terminal will output a high temperature alarm when digital detection module detects high temperature.
		Not Wearing Mask Alarm	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After turning on the not wearing mask alarm, terminal will output a not wearing mask alarm when it detects people who not wearing a mask.
		Blacklist Alarm	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After turning on the blacklist alarm, terminal will output a blacklist

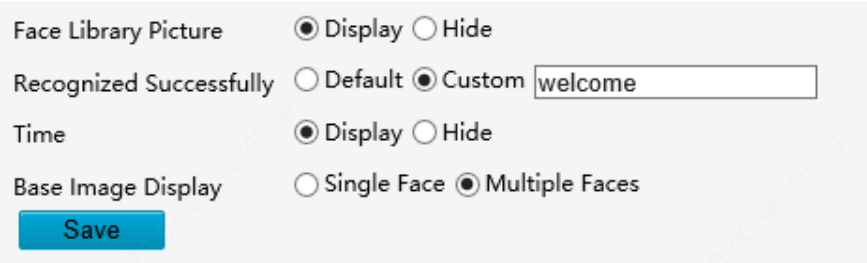
		alarm when blacklist person is detected.
	Authentication Failure Alarm	The options are **On** and **Off**. Set the parameter based on the actual conditions. The default value is **Off**. After turning on the authentication failure alarm, terminal will output an authentication failure alarm when face and card authentication failed.

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** > **Common** > **Smart Snapshot** and click the **Recognition Result Display** tab.

Figure7-53 Recognition Result Display Interface



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

Table7-22 Parameter Description and Configuration

Parameter	Description and Configuration
Face Library Picture	• Display: The face recognition terminal displays a person's registered picture after face recognition succeeds. • Hide: The face recognition terminal does not display a person's registered picture after face recognition succeeds. Set this parameter based on actual requirements.
Recognized Successfully	• Default: The face recognition terminal displays "Recognized Successfully" after face recognition succeeds. • Custom: The face recognition terminal displays information defined here rather thana person's name after face recognition succeeds. A string of 0–10 characters can be entered in the custom box. Set this parameter based on actual requirements.
Time	• Display: The face recognition terminal displays the current system time. • Hide: The face recognition terminal does not display the current system time. Set this parameter based on actual requirements. Note: This parameter is available only when **Base Image Display** is set to **Single Face**.
Base Image Display	• Single Face: The GUI displays only information about the identified person after face recognition succeeds. • 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. Set this parameter based on actual requirements. It is set to **Single Face** by default.

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

7. Sensing

The configuration is not supported.

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.

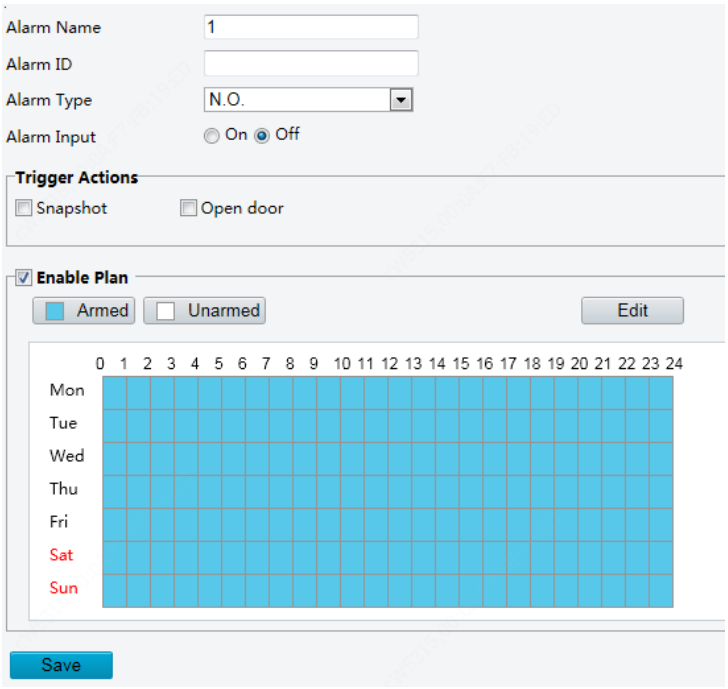
Alarm arming includes fire alarms, anti-disassembly alarms, and door magnet alarms.

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**.

Figure7-54 Fire Alarm Configuration Interface



(2) Set fire alarm information.

1) Select alarm and set the alarm name.

2) 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.

3) 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.

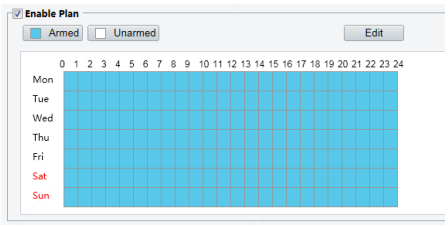
(3) Set actions to be associated with fire alarms.

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

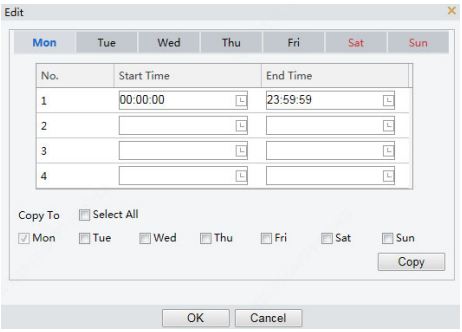
(4) Set whether to enable the arming schedule.

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

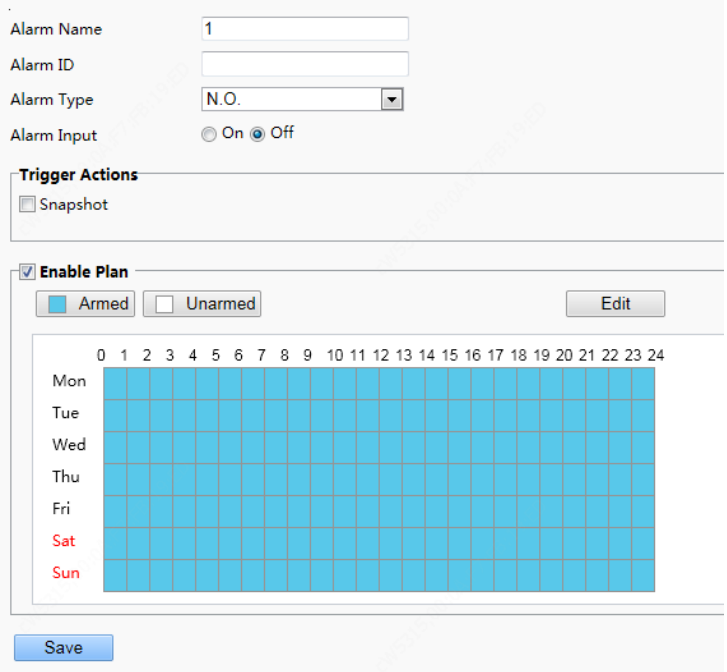
(5) Click **Save**.

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**.

Figure7-55 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.

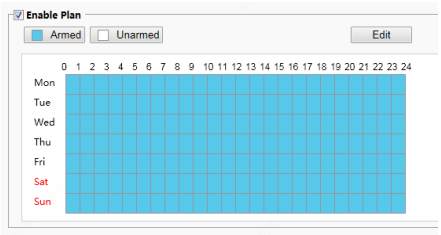
(3) Set actions to be associated with tamper alarms.

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

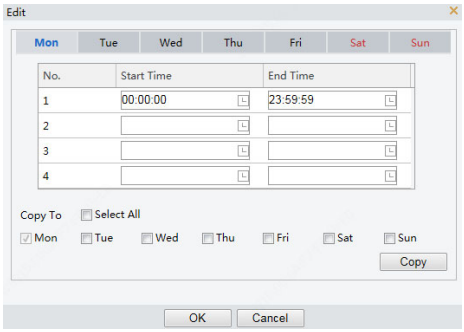
Set whether to enable the arming schedule.

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

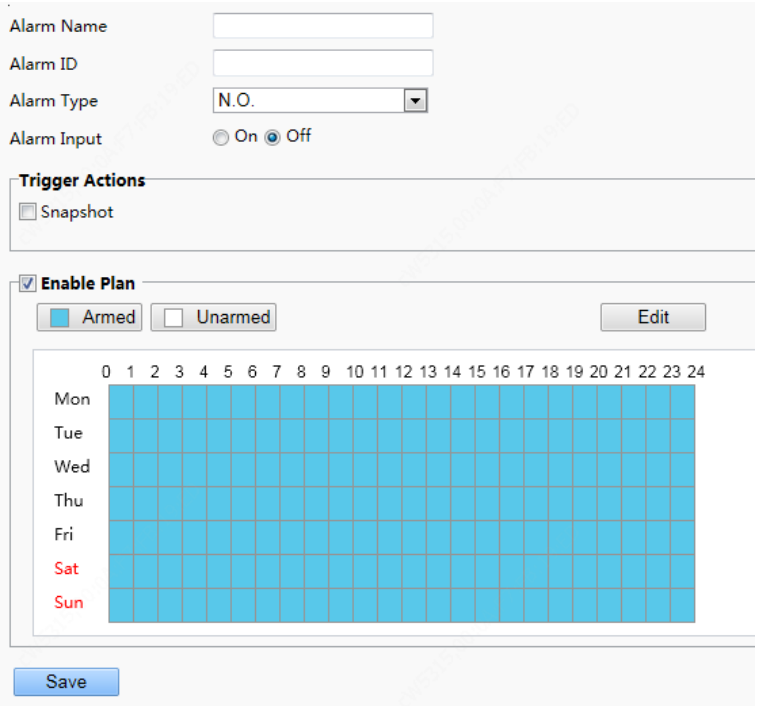
(5) Click **Save**.

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**.

Figure7-56 Door Magnet Alarm Configuration Interface



(2) Set basic information about door magnet 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 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.

3) 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.

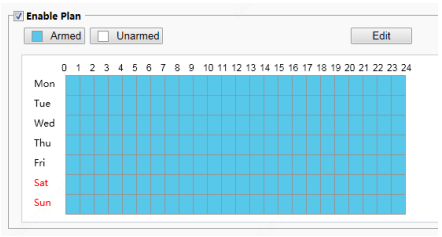
(3) Set actions to be associated with door magnet alarms.

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

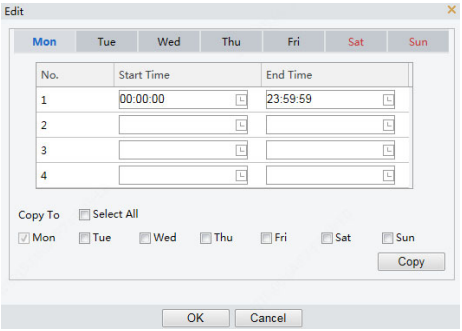
(4) Set whether to enable the arming schedule.

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**.

7.3.6 Storage

1. Storage

(1) Click **Setup** > **Storage** > **Storage**.

NOTE!

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

2. FTP

The configuration is not supported.

7.3.7 Security

1. User

For user configuration, see User.

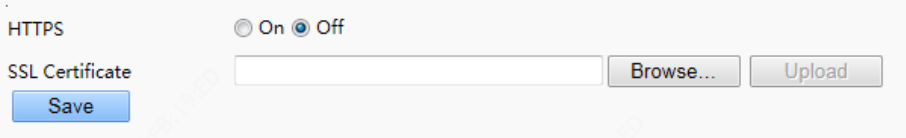
2. Network Security

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

(1) HTTPS

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

Figure7-57 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.

(2) 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.

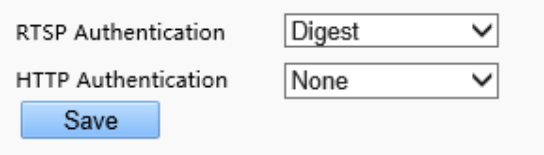
(1) Click Setup > Security > Network Security > RTSP Authentication.

(2) Select an authentication mode.

Table7-23 Parameter Description and Configuration

Parameter	Description and Configuration
RSTP Authentication	The options are **Basic**, **Digest**, and **None**. The default value is **Digest**.
HTTP Authentication	The options are **Digest** and **None**. The default value is **None**.

Figure7-58 RTSP Authentication Setting Interface



(3) Click **Save**.

NOTE!

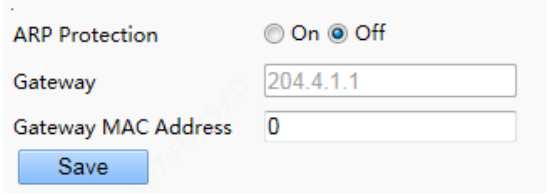
When the visual intercom face recognition terminal is used in combination with indoor monitors, the authentication mode needs to be set to **None**.

(3) 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**.

Figure7-59 ARP Protection Setting Interface



(2) Select the check box to enable the ARP binding function and set the gateway MAC address.

(3) Click **Save**.

(4) IP Address Filtering

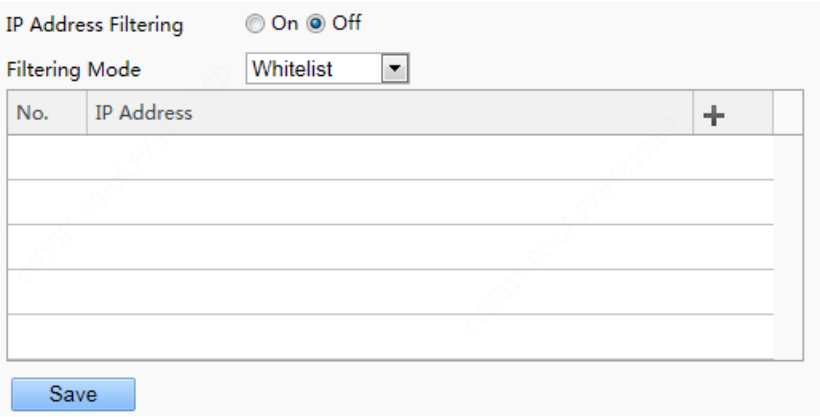
Use IP address filtering to allow or forbid access from specified IP address(es).

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**.

Figure7-60 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.

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

The configuration is not supported.

3. Ports & Devices

For the configuration of ports and devices, see Ports & Devices.

(1) Maintenance

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

Figure7-61 Local Upgrade Interface

(2) Under **Software Upgrade**, click **Browse** and select the correct upgrade file.

(3) Click **Upgrade** and then confirm to start. The camera will restart automatically after the upgrade is completed.

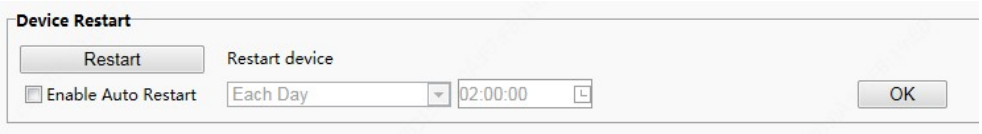
NOTE!

- You must use the correct upgrade file for you camera. 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.

(2) Device Restart

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

Figure7-62 Restart Configuration Interface



(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.

(3) System Configuration

(1.1) Restoring Factory Defaults

- 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. Refer to the password change operation.

- 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.

(1.2) Importing and Exporting System Configuration File

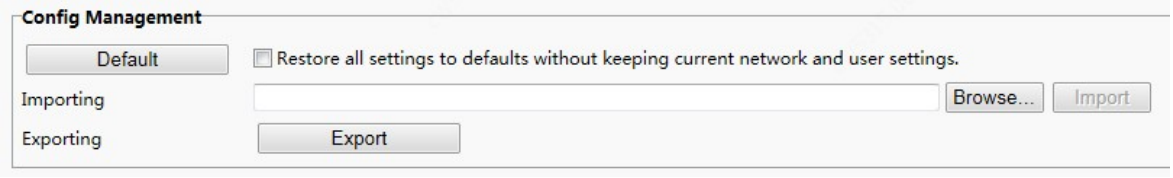
Export the current configurations of the camera and save them to the PC or an external storage medium. You can also quickly restore configurations by importing backup configurations stored on the PC or an external storage medium back to the camera.

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**.

Figure7-63 Import/Export Configuration Interface



(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**.

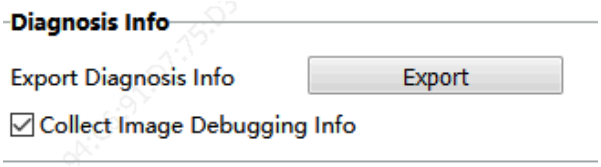
(4) To restore default configurations, click **Default** and then confirm the operation. The device will restart and restore the default configurations. Clicking **Default** with the check box selected will completely restore the device to factory default settings.

(4) Collecting Diagnosis Information

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

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

Figure7-64 Diagnosis Information Collection Interface



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

NOTE!

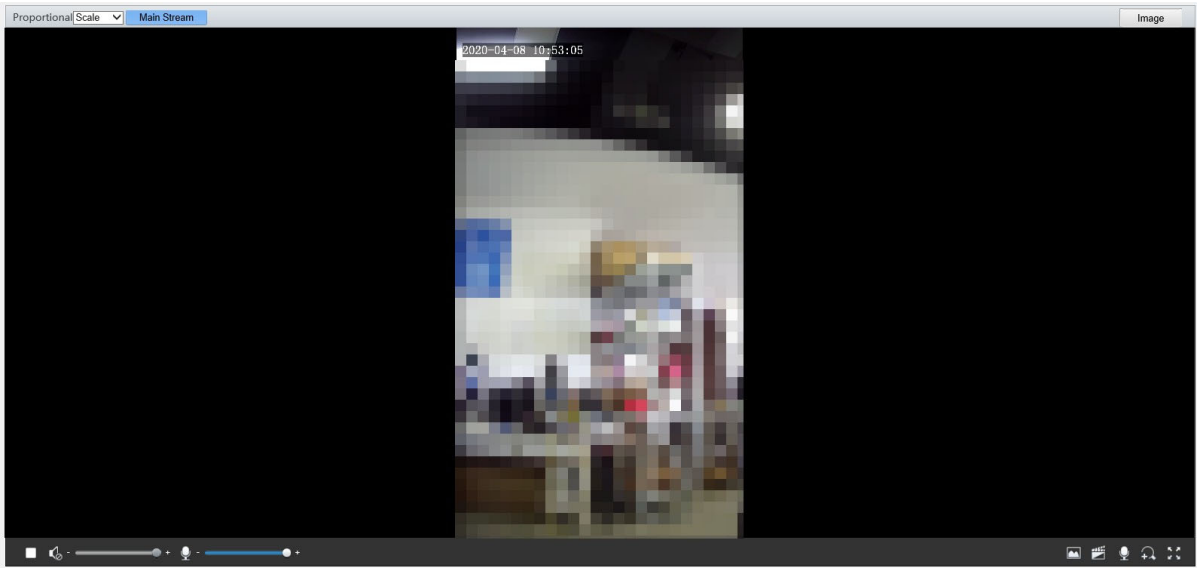
- Diagnosis information is exported to the local folder in form of a compressed file. You need to decompress the file using a tool such as WinRAR and then open the file using a text editor.
- By selecting **Collect Image Debugging Info**, you can display video with debugging information at the same time,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

8 Live View

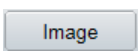
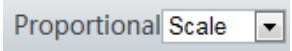
Live view means playing live video (real-time audio and video) received from a camera in a window through the Web interface.

If you log in with the **Live View** check box selected, live video appears by default when you are logged in. You may double-click the window to enter or exit full screen mode.

Figure8-1 Live View



Description of the Live View Toolbar

Configuration Item	Description
	Play/stop live video.
	Adjust the output volume for the media player on the PC.(not supported)
	Adjust the microphone volume on the PC during audio communication between the PC and the camera.(not supported)
	Take a snapshot of the current image displayed on the PC. **NOTE!** You can set the path for saving images in Local Settings.
	Start/stop local recording. **NOTE!** You can set the path for saving snapshot photos in Local Settings.
	tart/stop audio communication between the PC and the camera.(not supported)
	Start/stop digital zoom.(not supported)
	Rapidly link to the image setting interface of the device.
	Display in full screen mode.
	Set image display ratio in the window. For example, to display high-definition images at original 16:9, select **Scale**; to display according to window size, select **Stretch**; to display

Configuration Item	Description
	with the original image size, select **Original**.
Main Stream	The main stream is played in the live view of the device.

9 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:

1. Click the **Start** button, and then click **Control Panel**.
2. In the search box, type uac, and then click **Change User Account Control Settings**.
3. Move the slider to the **Never Notify** position, and then click **OK**.
4. 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.

2M® TECHNOLOGY
802 Greenview Dr.
Grand Prairie TX. 75050 USA
Toll Free: 1-866-708-5401
Fax: (+1) 972-999-4113
sales@2MTechnology.net