Smart Cabinet

User Manual

Precautions for safe use

warn

- During the installation and use of the equipment, all electrical safety regulations of the country and the area of use must be strictly observed.
- The protective grounding of the equipment should be reliably connected to the protective grounding of the building equipment.
- The plug or socket of the equipment is the device to disconnect the power supply. Please do not block it and make it easy to plug and unplug.
- If the device contains a fan: The device contains a fan. Please keep your body away from the fan blades. Please disconnect the fan power supply when repairing. If the device contains a motor: The device contains an electric motor. Please keep your body away from the motor and disconnect the power supply during maintenance.
- The building installation to which this equipment is connected must have an all-pole mains switch .
- 1. Warning: There is a risk of explosion if the battery is replaced with an incorrect type.
  2. Replacing the battery with an incorrect model (such as certain types of lithium batteries) may cause the safety protection to fail.
  3. Do not throw the battery into fire or heating furnace. Do not squeeze, bend or cut the battery, as it may cause explosion.
  4. Do not place the battery in an extremely high temperature environment, as this may cause the battery to explode or leak flammable liquids or gases.
  5. Do not place the battery in an extremely low pressure environment, as this may cause the battery to explode or leak flammable liquids or gases.
  6. Discarded batteries will pollute the environment. Please dispose of used batteries according to the instructions.
- The apparatus shall not be exposed to dripping or splashing and no objects filled with liquids, such as vases, shall be placed on the apparatus.

Notice

- The terminals connected to the AC power grid must have the correct wiring sequence .
- IT power distribution system directly or with modifications if necessary .
- Identify the battery holder itself and identify the positioning of the battery within the holder.
- + identifies the positive terminal of a device that uses or generates direct current. - identifies the negative terminal of a device that uses or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The device is suitable for mounting on concrete or non- combustible surfaces only.
- USB port of the device can only be connected to a mouse, keyboard or USB flash drive, and is not allowed to be used for charging or other loads.
- Be careful not to pull the smart cabinet forward to prevent it from tipping over.
- Please prevent the device from tipping over and damaging it during transportation .
- If you need to move the cabinet, you must first disconnect the cabinet connection line to avoid pulling the wire and damaging the wiring harness or board.
- During installation and maintenance, please ensure that the device is powered off.

illustrate

Qualification requirements for installation and maintenance personnel

- Have basic knowledge and installation skills of access control systems and their components.

- Have basic knowledge and operational skills of low-voltage wiring and low-voltage electronic circuit wiring.
- Have basic network security knowledge and skills, and be able to understand the contents of this manual.

Order record

Chapter 1 Smart Cabinet Appearance Introduction

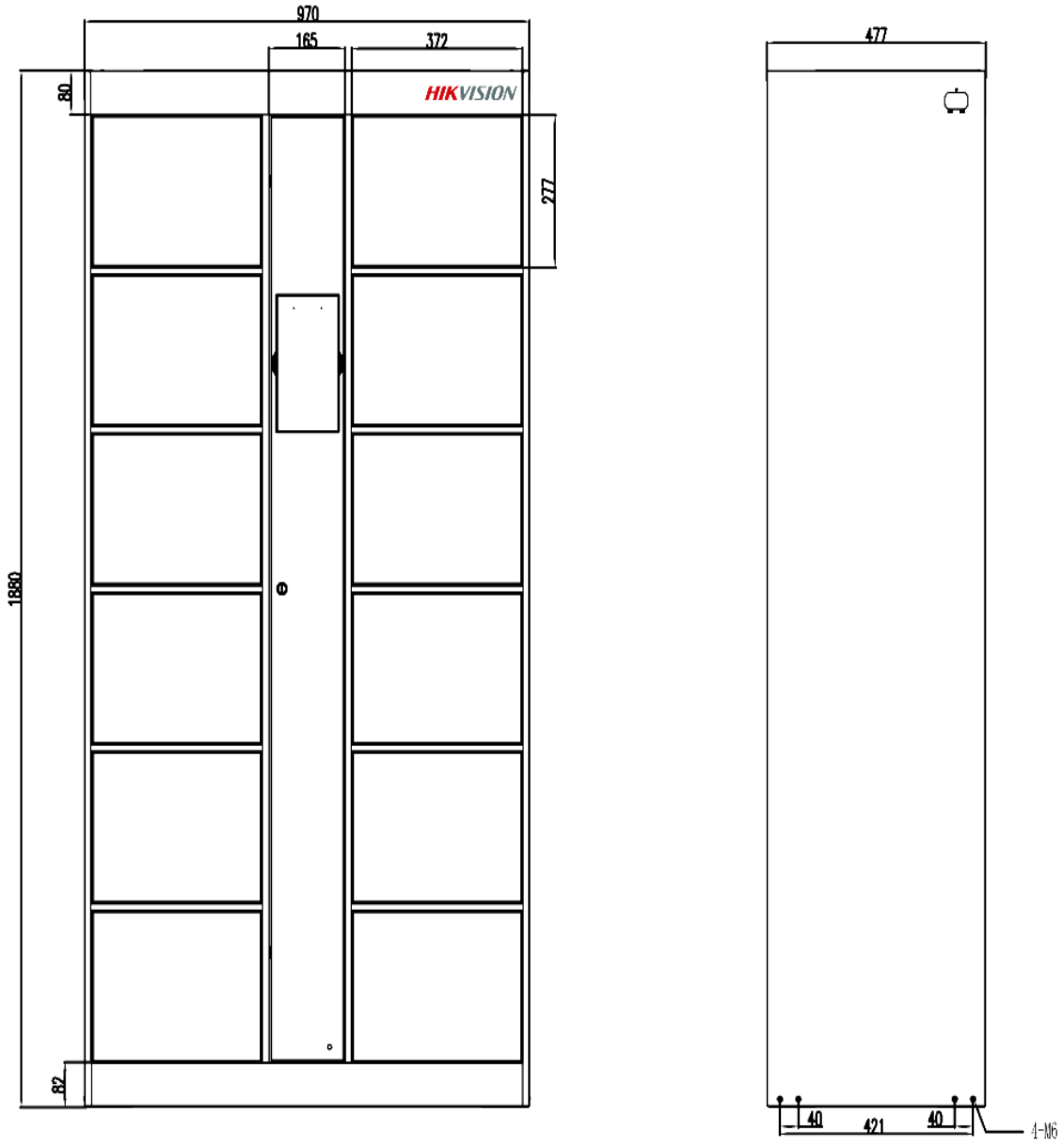


Figure 1-1 Main cabinet

illustrate

Only QR series models support the connection of barcode scanners .

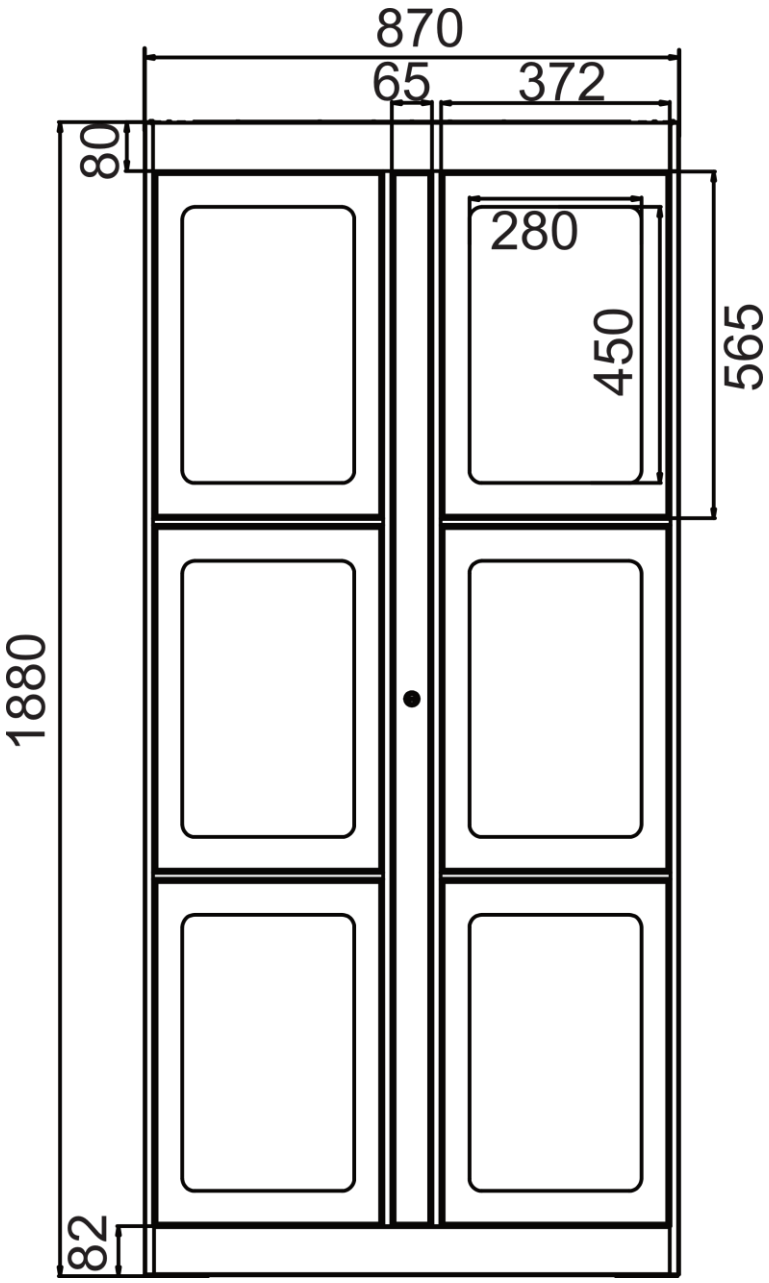


Figure 1-2 Sub-cabinet (6 compartments)

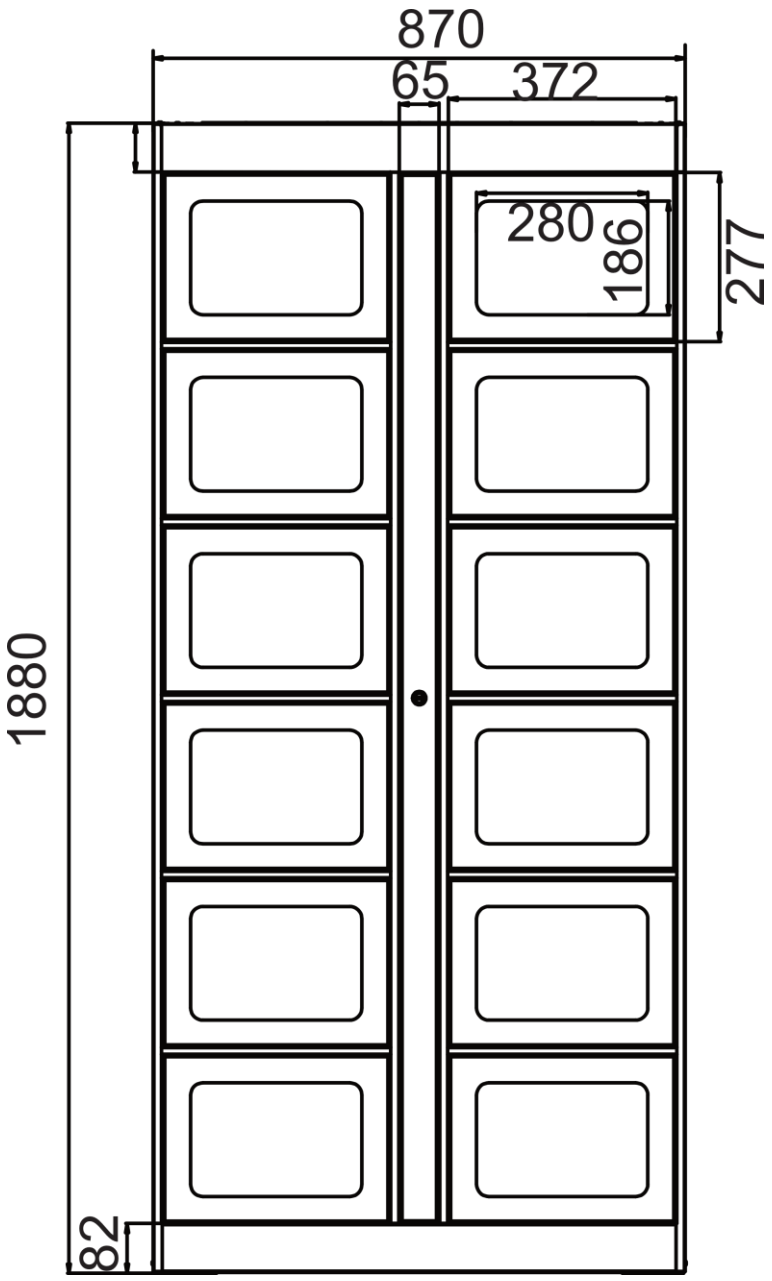


Figure 1-3 Auxiliary cabinet （ 12 compartments 1 ）

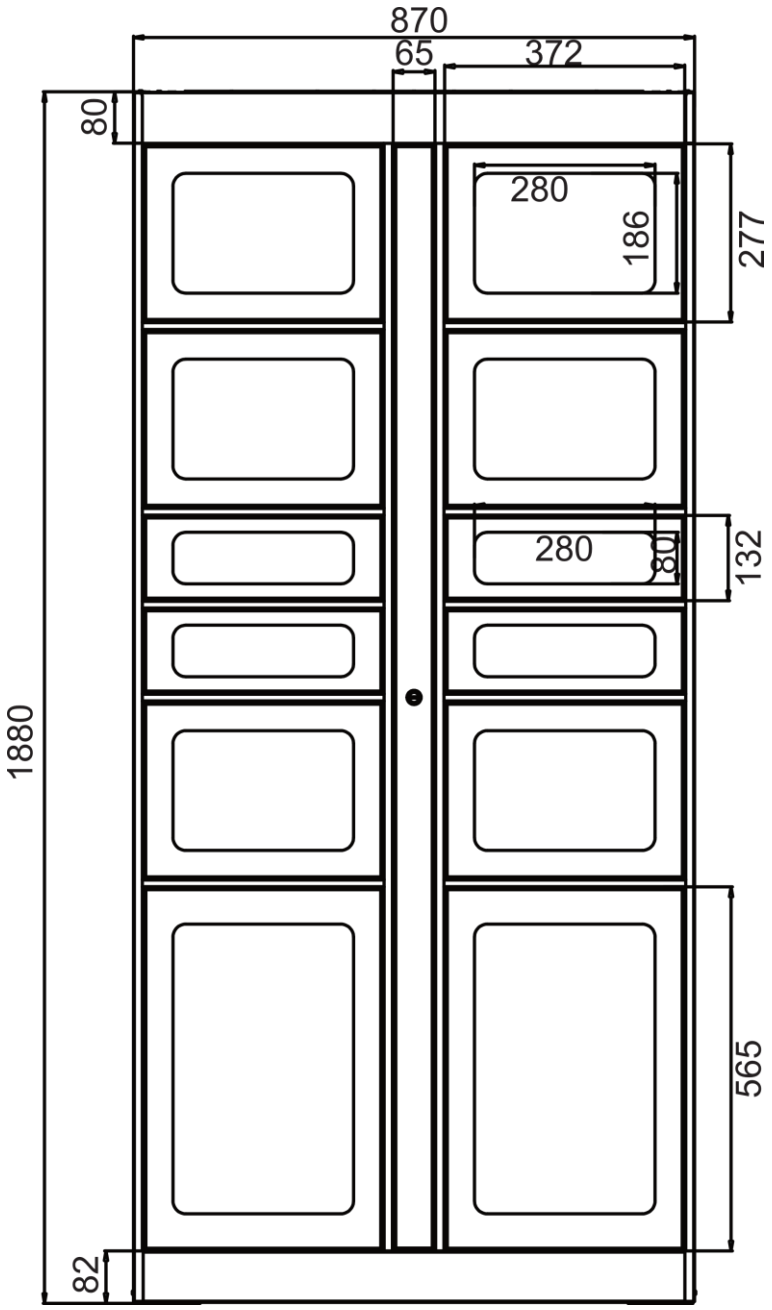


Figure 1-4 Sub-cabinet （ 12 compartments 2 ）

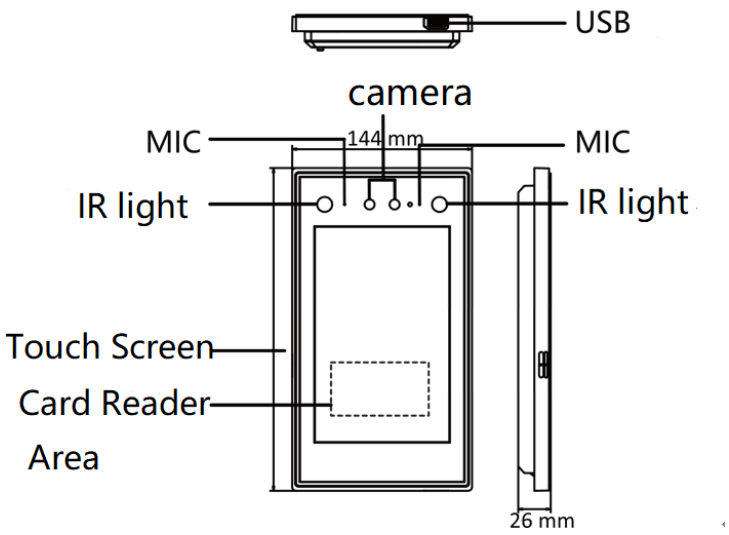


Figure 1-5 Appearance of face recognition device

Unit: mm .

Chapter 2 Installation Instructions

2.1 Installation Environment

The device can only be installed indoors. Avoid installing it in places where it may be exposed to rain, dripping water from the top, or in places where it is abnormally humid or has water on the ground.
The installation ground must be flat without slopes or inclinations, and avoid installing it on places where the surface vibrates or is susceptible to impact.
Avoid backlight, direct sunlight, oblique light or close exposure to light.
The PE ground wire of the Power supply socket must be grounded.
Try to stay away from interference environments (such as various motors, water pump rooms, etc.).

illustrate

For specific installation precautions, see the appendix *Installation Environment Precautions* .

2.2 Smart Cabinet Installation

Procedure

1. Unpacking and material inspection.
   1) Remove the hexagonal bolts that install the wooden bracket at the bottom of the cabinet, and remove the wooden tray of the smart cabinet. Check whether the cabinet is damaged, scratched, or deformed, and whether the cabinet and internal cables, power supply, etc. are loose.
   2) Remove the key reserved on the top of the main cabinet, use the key to open the bottom door of the main cabinet , take out the accessory box, and check whether all accessories are complete according to the packing list.
2. If the installation ground is uneven (within a 2 -meter length, the chord height of the ground unevenness exceeds plus or minus 3 mm), it is necessary to install anchors. The height of the four corners of the cabinet can be adjusted by adjusting the length of the anchor bolts. Specifically, the level gauge is used to ensure that all cabinets are placed horizontally and the main and auxiliary cabinets are tightly attached without gaps.
3. Connect the power supply: Open the middle compartment of the main cabinet, take out the power cord and accessories. Connect the power interface on the back of the main cabinet and power on, then you can use it.
4. Place the cabinets: Place the main and auxiliary cabinets close to each other , with the overall openings facing outwards in a straight line .

   illustrate

   - Place the main cabinet in the middle.
   - The device supports the installation of 6 -grid, 12- grid, and 24 -grid smart cabinets, which can be combined according to actual needs.

5. Wiring: Remove the wiring cover on the top of the auxiliary cabinet. 6/12/24 slots: Plug the cable connector reserved on the top of the main cabinet into the corresponding connector on the top of the auxiliary cabinet .

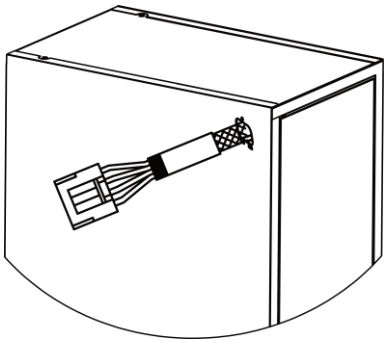


Figure 2-1 6/12/24 grid connection

illustrate

- When a main cabinet is used to tow multiple auxiliary cabinets , the top connectors of each auxiliary cabinet need to be connected. The wiring terminals reserved in the auxiliary cabinet can be connected to the main cabinet at one end and to other auxiliary cabinets at the other end .
- of the main cabinet and auxiliary cabinet support fool-proofing.

6. Combine cabinets: Adjust the positions of all cabinets to ensure they fit tightly without any gaps. Use M3 screws to fix the cabinet pieces on the top of the adjacent cabinets, and use M6*15 screws to fix the cabinet corner pieces on the top of the adjacent cabinets.

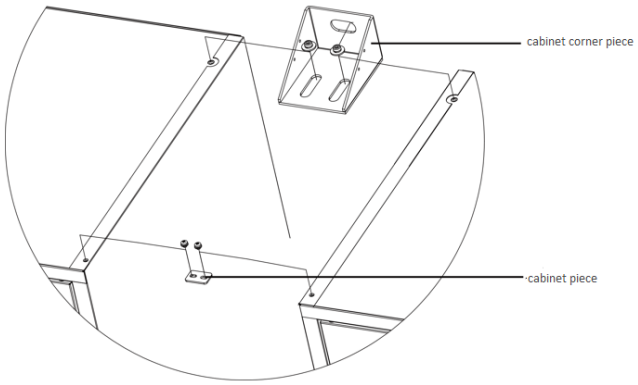


Figure 2-2 Cabinet combination

7. Cabinet fixing: The cabinet can be fixed at the bottom or at the top. You can choose the required installation method according to the actual scenario.
   - Bottom fixing: If the bottom is fixed to the ground, after all cabinets are adjusted, the cabinet must be connected to the ground with anchors. One end of the anchor is first fixed to the screw hole reserved on the side of the cabinet through the M6 combination bolt (note that the anchor should be placed in the corresponding position in advance, and the ground expansion bolts should be marked and punched). The other end is fixed to the ground through the M12 expansion bolt.

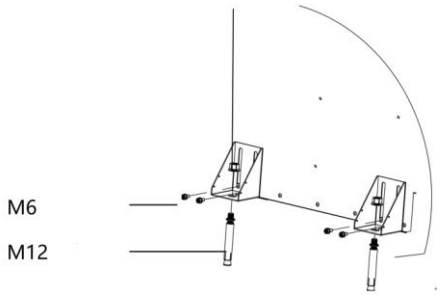


Figure 2-3 Bottom fixing

Illustrate

The anchor fixture can not only fix the cabinet to the ground, but also connect two adjacent cabinets.

– Top fixing: If the top and wall fixing is selected, after all cabinets are adjusted, the top fixing parts need to be used to fix the cabinets to the wall (note that the top fixing parts should be placed in the corresponding position in advance to mark and punch the wall expansion bolts). One end of the top fixing part is first fixed to the screw hole reserved on the top of the cabinet with an M6 combination bolt , and the other end is fixed to the wall with an M8 expansion bolt.

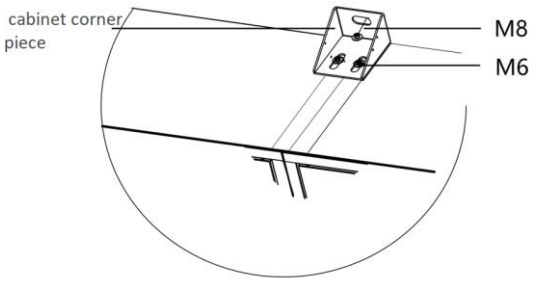


Figure 2-4 Top fixation

8. Fix the decorative panel: After the cabinet is installed and fixed, use M3 combination screws to fix the top decorative panel.

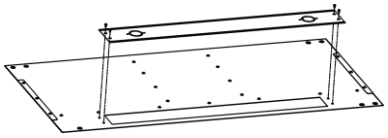


Figure 2-5 Fixing the decorative panel

9. 9 Seal the terminal wiring hole to prevent foreign matter from entering.

Chapter 3 Smart cabinet wiring

Wiring (smart cabinet)

After the device is installed, connect the power interface to the power source and it can be used.

illustrate

The factory power cord of the device is 2 m. If the cord is not long enough, it needs to be shortened.

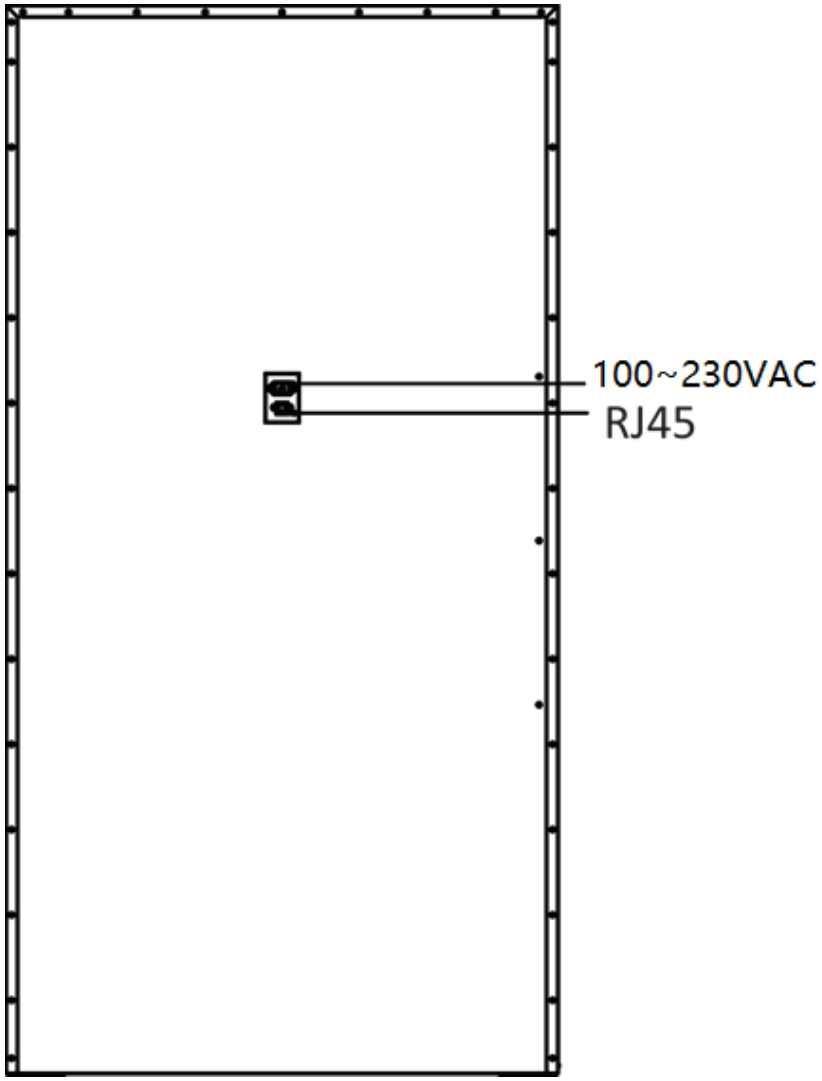


Figure 3-1 Wiring (intelligent cabinet)

Wiring (barcode scanner)

If necessary, open the middle cabinet door with the intelligent identification terminal device and connect the barcode scanner to the USB port of the intelligent identification terminal .

illustrate

Only some devices support the connection of barcode scanners . Please refer to the actual device.

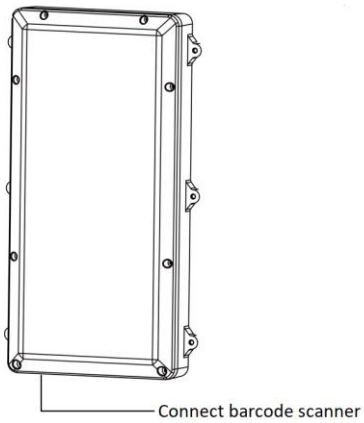


Figure 3-2 Wiring (barcode scanner)

Chapter 4 activation

When using the device for the first time, you need to activate it and set a password before you can log in and use it normally.
The factory default values of the device are as follows:

- The default IP is: 192.0.0.64 .
- The default ports are: 80 , 443 .
- Default user name (administrator): admin .

4.1 Activate locally on the device

If the device has not been activated before use, it will automatically enter the activation interface after power-on.

Procedure

1. Click the Enter Power-On Password edit box and create a password on the interface soft keyboard.
2. Click the Confirm Password edit box and repeat the password you just entered.
3. Click *Next* to complete the activation.

illustrate

The activation password cannot contain the characters admin and nimda .

Notice

- To better protect your privacy and improve product security, we strongly recommend that you set a more complex password according to the following rules: the password must be between 8 and 16 characters long and consist of two or more types of numbers, uppercase and lowercase letters, and special characters.
- Please understand that you are responsible for properly configuring all passwords and other related product security settings.

4.2 Activate the device through the web page

You can activate an unactivated device through the device web page.
IP address (192.0.0.64) on the web page and create a password in the pop-up window. After confirming the password, you can activate the device.

illustrate

- Please make sure that the device IP and computer IP are in the same network segment.
- The activation password cannot contain the characters admin and nimda .

Notice

- To better protect your privacy and improve product security, we strongly recommend that you set a more complex password according to the following rules: the password must be between 8 and 16 characters long and consist of two or more types of numbers, uppercase and lowercase letters, and special characters.
- Please understand that you are responsible for properly configuring all passwords and other related product security settings.

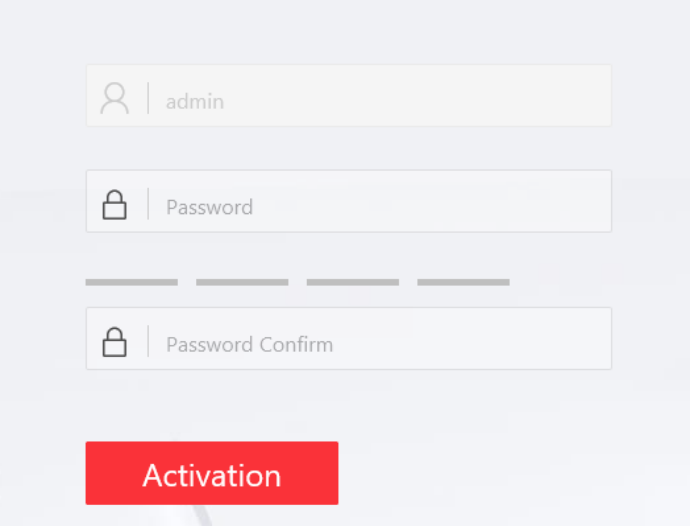


Figure 4-1 Activation page

IP address, gateway and other information can be modified through the SADP tool, the device local, or the client software .

4.3 Activate the device through SADP software

Download the SADP software and run it. The SADP software will automatically search for all online devices in the LAN, and the list will display information such as device type, IP address, security status, device serial number, etc. The SADP software can be used to activate unactivated devices.

Procedure

1. Download the SADP software from the official website and run it.
2. Select the device you want to activate, and the relevant information of the device will be displayed on the right side of the list.
3. Set the device password in the Activate Device field and click *OK* to complete the activation.

Notice

- To improve the security of product network use, the set password must be 8-16 characters long and must be composed of at least two or more of the following types: numbers, lowercase letters, uppercase letters, and special characters.
- The activation password cannot contain the characters admin and nimda .

After the device is successfully activated, the activation status in the list will be updated to **Activated** .

4. Modify the device IP address
   1) Select the activated device in the device list.
   2) Enter the IP address, subnet mask, gateway and other information in **the Modify Network Parameters** on the right .

> illustrate
>
> setting the IP address, please keep the device IP address and computer IP address in the same network segment.

   3) After the modification is completed, enter the password set when activating the device and click *Modify* .

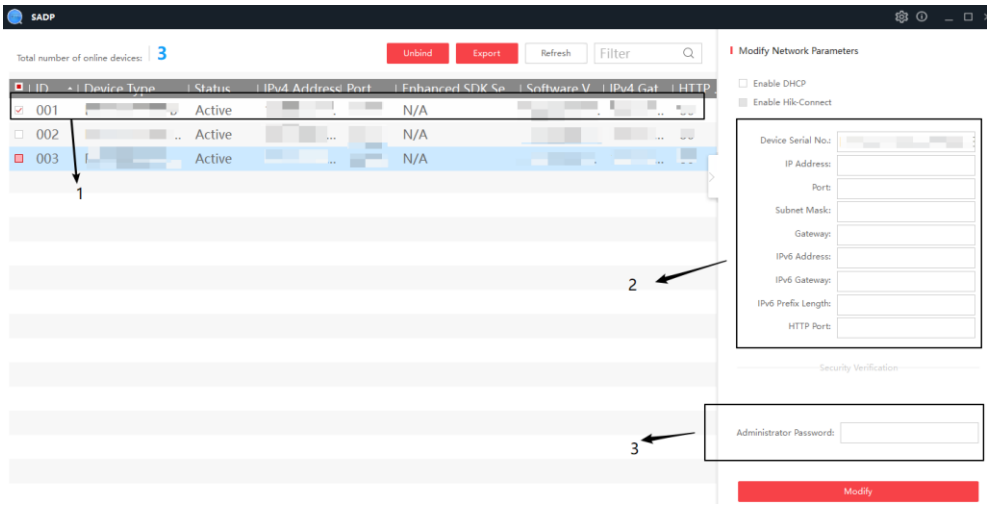


Figure 4-2 Modify the device IP address

If the prompt **"Parameter modification is successful" appears, it means that** the IP and other parameter settings are effective.

Chapter 5 Quick Setup

5.1 Set password reset method

After activating the device, you can set the password reset method. If you forget your password, you can reset your account password through identity verification.
You can choose to reset your password using the security question method or by clicking on the upper-right corner to switch to the security code method.

Security Question Method

Enter the answer to the security question. You can verify your identity through the security question later.

security code

Enter the reserved mobile phone number. You can reset your password later using the mobile phone security code .

5.2 Configure Network

After activating the device and selecting the usage environment, you need to configure the network before you can use the device normally.

wired

illustrate

Please make sure your device is connected to a wired network.

If *DHCP is turned on* , the system automatically assigns IP addresses and other network parameters.
If it is not enabled, you need to manually configure the IP address, subnet mask and gateway.

Wi-Fi

Wi-Fi from the list and enter the password.
Or click *Add Wi-Fi* and enter the Wi-Fi name and password to access the network.

Click *Next* .

5.3 Set the user groups of the cabinet group

According to the needs, the users of the cabinet group can be selected as *internal staff* , *visitors* or *mixed personnel* .

illustrate

Only some models support this function. Please refer to the actual device.

5.4 Configure Cloud Services

If you need to add a device to the APP , you need to access the cloud service.

illustrate

Some device models support cloud service functions.

Click the slider to enable *Cloud Services* . Or click *Skip* to skip this step.
You can choose to enable *video encryption* and configure **the video encryption password** . After adding the device to the APP , if you want to preview the device, you need to enter the set **video encryption password.** .
Click *Next* .
Bind your account. You can choose to scan the QR code to bind or bind manually. Or click *Skip to* skip this step.

Scan code to bind

Scan the QR code via the mobile app to bind your cloud account.

illustrate

Please follow the on-screen prompts and scan the QR code before it expires .

Manual Binding

Available in *my* mobile app → Check the account verification code in *the account , click Unable to scan the code* on the device page , please try to bind manually , and enter this verification code in **the user token , click** *Next* to bind.

Or click *Back* to return to the previous page.

5.5 Privacy Configuration

Configurable device privacy and security information.
Make selections as required.

illustrate

By default, all are unchecked.

Save the recognized captured image

The picture captured during authentication will be saved to the device.

Upload the captured image for identification

The pictures captured during authentication will be uploaded to the platform.

Save the face registration picture

The registration picture when adding a person will be saved to the device.

Automatic photo taking when visitor enters the account

After it is turned on, a facial picture will be automatically taken after the visitor enters their face.

Click *Next* to complete the configuration.

5.6 Configuring Administrators

After activating the device, you can add an administrator to manage the device background parameters.

Procedure

1. On the Add Administrator page, enter the administrator ID and **name** and click *Next* .
2. Select the credentials you want to add.
   - : Face your face to the device camera, make sure your face is within the face mark on the device interface, and perform face recognition. Click to enter. After successful entry, click to confirm entry.
   - : Enter the card number in the input box, or swipe the card in the device's card swiping area to obtain the card number. Click *Done* .

Chapter 6 Device local operation

6.1 Login

If you need to configure background parameters, you must log in to the background first.

Procedure

1. Enter the backend page.
   - If the cabinet user is configured as *an internal staff on the web page* , you need to press and hold the non-grid area at the top of the screen for 3 seconds on the selection grid interface and then slide left or right to enter the background management window.
   - If it is in other standby interfaces, press and hold the main display screen for 3 seconds and slide left or right to enter the background management window.
2. Enter the password in the pop-up box for entering the backend configuration. The password here is the activation password.
3. Click *OK* to enter the backend main menu interface.

illustrate

If you enter an incorrect password five times in a row, the device will be locked for 30 minutes.

6.2 Forgot your password

If you forget your password when logging in, you can reset a new account password by verifying your identity.

Procedure

1. On the password input interface, click *Forgot Password* .
2. In the pop-up verification identity interface, select the reset method to verify your identity.
   - Select *Reset by security question* , enter the answer to the security question, verify your identity with the security question, and click *OK* .
3. Set a new password and confirm it to complete the password change.
4. Optional operation : The user can pass the name and mobile phone number information to the administrator, and the administrator will reset the password in the personnel information.

6.3 Personnel Management

In the Personnel Management menu, you can add, edit, and delete personnel.

6.3.1 Administrator Login

If you need to configure background parameters, you must log in to the background first. If the device has an administrator, and the administrator has added faces and cards, you can log in to the background by authenticating your face or swiping your card.

Prerequisites

Add an administrator and add a face card for the administrator. For details on how to add an administrator, see

Add an administrator .

Procedure

1. On the authentication interface, press and hold the non-button area of the main display screen for 3 seconds , and slide left or right according to the gestures on the top of the interface to enter the administrator verification interface.
2. After verifying the administrator 's face or swiping the administrator card, enter the main menu interface.

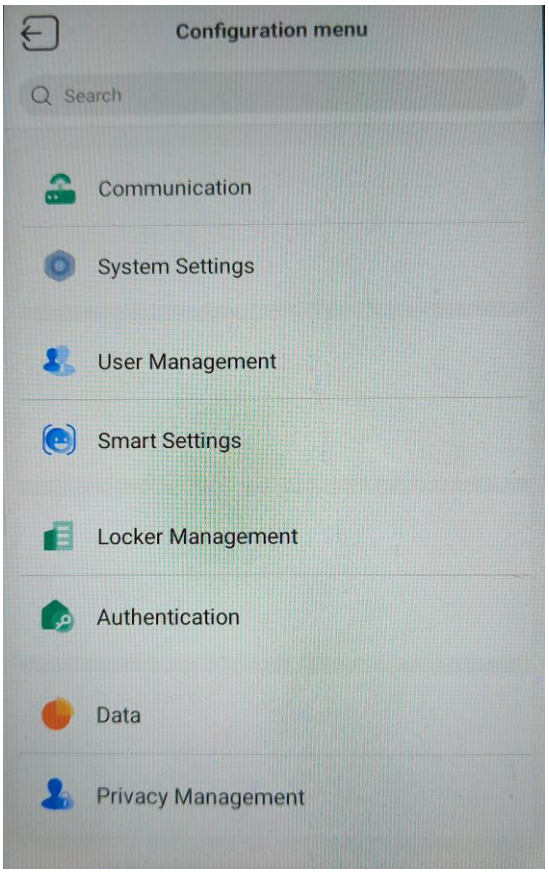


Figure 6-1 Main menu interface

illustrate

5 consecutive authentication errors, the device will be locked for 30 minutes.

3. Optional operation : Click to enter the device activation password to log in.
4. Optional operation : Click to exit the administrator verification page.

illustrate

no operation is performed for about 1 minute, the device will automatically log out of the backend and return to the authentication interface.

6.3.2 Adding Administrators

Procedure

1. Click *Personnel Management in the device menu interface* → + Enter the Add UI.
2. Click *the work number* to edit the user's work number.

illustrate

- The employee number cannot exceed 32 characters and can be a combination of uppercase and lowercase letters and numbers.
- To add an administrator user, you must first add the work number before adding other information items.

3. Click *Name* and enter a new name. You can enter the user name on the pop-up soft keyboard.

illustrate

Names support numbers, Chinese characters, uppercase and lowercase English characters, characters, and emoticons.

4. Configure the administrator face and card as needed.

illustrate

- Please *add person's face* and *add person's card* .

5. Click *Password* to set an administrator password.
6. Fill in your mobile phone number based on actual situation.
7. Select the user type.
8. Set the validity period of the permission.
9. Enable *Administrator* .
10. Configure the administrator's permission type.

illustrate

Different devices support different types of interfaces . Please refer to the actual device.

11. Click ✓ Save Settings.

6.3.3 Add Person Card

Procedure

illustrate

Each person can add up to 5 cards.

1. Click the *+ button* on the personnel list interface to enter the "Add Person" interface.
2. Click *the work number* to edit the work number of the newly added user.

illustrate

- The employee number cannot exceed 32 characters and can be a combination of uppercase and lowercase letters and numbers.
- To add an administrator user, you must first add the work number before adding other information items.

3. Click *Name* and enter a new name. You can enter the user name on the pop-up soft keyboard.

illustrate

The name supports numbers, Chinese characters, uppercase and lowercase English characters, and letters.

4. Click on *the mobile phone number* to add the user's mobile phone number.
5. Click on *the card* and add the card information.
   1) Click + and enter the card number or swipe the card on the device to read the card number.

illustrate

- Card number cannot be empty.
- The card number can be up to 20 digits long.
- Card numbers cannot be repeated.

   2) Click ✓ Save Settings.

6.3.4 Adding a Person's Face

Procedure

1. Click *Personnel Management in the device menu interface* → + Enter the Add Person interface.

2. Click *the work number* to edit the work number of the newly added user.

illustrate

- The employee number cannot exceed 32 characters and can be a combination of uppercase and lowercase letters and numbers.
- To add an administrator user, you must first add the work number before adding other information items.

3. Click *Name* and enter a new name. You can enter the user name on the pop-up soft keyboard.

illustrate

The name supports numbers, Chinese characters, uppercase and lowercase English characters, and letters.

4. Click on *the mobile phone number* to add the user's mobile phone number.
5. Click the face avatar to enter the face entry interface.
6. Align your face to the device camera, make sure your face is within the face icon on the interface, click , and click to confirm the entry.

7. Click ✓ Save Settings.

6.3.5 Adding personnel password

Procedure

illustrate

Before adding a password, please agree to *the password security statement* . For details, see *Configuring Privacy Parameters* .

1. Click *Personnel Management in the device menu interface* → + Enter the Add Person interface.
2. Click *the work number* to edit the work number of the newly added user.

illustrate

- The employee number cannot exceed 32 characters and can be a combination of uppercase and lowercase letters and numbers.
- To add an administrator user, you must first add the work number before adding other information items.

3. Click *Name* and enter a new name. You can enter the user name on the pop-up soft keyboard.

illustrate

The name supports numbers, Chinese characters, uppercase and lowercase English characters, and letters.

4. Click on *the mobile phone number* to add the user's mobile phone number.
5. Click *Password* to enter the password input interface. Create a password and confirm it.

illustrate

The system randomly assigns a 6 -digit letter + number combination. The password can be reset.

6. Click *Confirm* to save.
7. Click ✓ Save Settings.

6.3.6 Editor / Query Personnel

Search personnel

In the *personnel list* interface, click the search bar to enter the search page, where you can search for personnel in the list by employee number, card number or name. You can also search for personnel through the alphabetical navigation bar.

Editorial Staff

In *the personnel list* interface, click the person you want to edit and modify the added person information.

illustrate

The employee number cannot be edited.

6.3.7 Authority Allocation and Grid Selection

You can set personnel permissions and levels .

Procedure

1. Click the *+ button* on the personnel list interface to enter the "Add Person" interface.
2. Set the personnel's **slot permission type** and **number of available slots** according to actual needs .

illustrate

- Guests can only be assigned free slots. Guests can only view, but not configure permissions.
- The port permissions supported by different device models may vary. Please refer to the actual device.

6.4 Deposit / retrieve

illustrate

The access interface is different in different modes, please refer to the actual configuration. For the configuration of specific modes, please refer to *the access configuration* .

1. Visitor storage (non-barcode scanner model device)

1. Before making local deposits and withdrawals, go to *the smart locker* on the web → *Parameter configuration* → Configure **the location information** and **device number of the** *smart cabinet in the service information configuration* , and → *Parameter configuration* → In *the storage and retrieval configuration,* **the users of the cabinet group are set** to *visitors* or **mixed personnel** .
2. Click *Save (Guest)* on the Storage and Retrieval interface .
3. Perform face, card or password verification.
4. Click on the interface to select the green grid, click *OK* , and the relevant cabinet doors can be opened.
5. Store the relevant items and close the cabinet door.
6. Click *Done* .

2. Visitor Pickup (Non-Broadcasting Gun Model Device)

illustrate

If any problems occur during the deposit/retrieval process of the smart locker, you can click the call button on the deposit / retrieval interface to contact the management center for resolution.

1. Before making local deposits and withdrawals, log in to *the smart locker* on the web page. → *Parameter configuration* → In *the storage and retrieval configuration,* **the users of the cabinet group are set** to *visitors* or **mixed personnel** .
2. Click *on the main* interface .
3. Perform face, card or password verification.

4. On the pickup list interface, click *the pickup* code behind the relevant pickup code to open the cabinet door.
5. Take out relevant items and close the cabinet door.
6. Click *Done* .

3. Storage of internal personnel (non-barcode scanner model equipment)

1. Before making local deposits and withdrawals, go to *the smart locker* on the web → *Parameter configuration* → Configure **the location information** and **device number of the** *smart cabinet in the service information configuration* , and → *Parameter configuration* → In *the storage and retrieval configuration,* **the cabinet group users are set** to *internal personnel* or **mixed personnel** .
2. Click *Save (Internal)* on the Storage and Retrieval interface .
3. Perform face, card or password verification.
4. Click on the interface to select the green grid, click *OK* , and the relevant cabinet doors can be opened.
5. Store the relevant items and close the cabinet door.
6. Click *Done* .

4. Internal personnel pick up the package (non-scanning gun model equipment)

illustrate

If any problems occur during the deposit/retrieval process of the smart locker, you can click the call button on the deposit / retrieval interface to contact the management center for resolution.

1. Before making local deposits and withdrawals, log in to *the smart locker* on the web page. → *Parameter configuration* → In *the storage and retrieval configuration,* **the cabinet group users are set** to *internal personnel* or *mixed personnel* .
2. Click *on the main* interface .
3. Perform face, card or password verification.
4. On the pickup list interface, click *the pickup* code behind the relevant pickup code to open the cabinet door.
5. Take out relevant items and close the cabinet door.
6. Click *Done* .

5. Internal personnel storage (barcode scanner model equipment)

1. Before making local deposits and withdrawals, go to *the smart locker* on the web → *Parameter configuration* → Configure **the location information** and **device number of the** *smart cabinet in the service information configuration* , and → *Parameter configuration* → In *the storage and retrieval configuration,* set **the cabinet group users** to *internal personnel* .
2. Click Save on the Save and *Retrieve interface* .
3. Perform face, card or password verification.
4. Click on the interface to select the green grid and click *OK* .
5. Use a barcode scanner to scan the item barcode and confirm on the interface.
6. The relevant cabinet doors can be opened.
7. According to the voice prompts, store the items in the relevant compartment and close it.
8. Click *Done* .

6. Internal personnel pick up the package (barcode scanner model

equipment)

illustrate

If any problems occur during the deposit/retrieval process of the smart locker, you can click the call button on the deposit / retrieval interface to contact the management center for resolution.

1. Before making local deposits and withdrawals, log in to *the smart locker* on the web page. → *Parameter configuration* → In *the storage and retrieval configuration,* set **the cabinet group users** to *internal personnel* .
2. Click *on the main* interface .
3. Perform face, card or password verification.
4.1 If the user only has single-grid access rights, the smart cabinet interface will jump to the item list information. After taking out the item, select the taken out item on the pop-up interface and scan the item for verification.
4.2 If the user has permission to open multiple slots, after selecting the slot to be opened, the smart cabinet interface will jump to the item list information. After taking out the item, select the taken out item on the pop-up interface and scan the item for verification.
5. Click *Done* .

6.5 Communication Settings

Configurable wired network parameters.

6.5.1 Network Settings

Configure the device's network parameters, including IPv4 's IP address, subnet mask, gateway address, and DNS . After configuration is complete, the device can communicate with client software, platforms, etc.

Procedure

1. Click *Communication Settings* in the main menu interface → *Wired network* enters the communication setting interface.

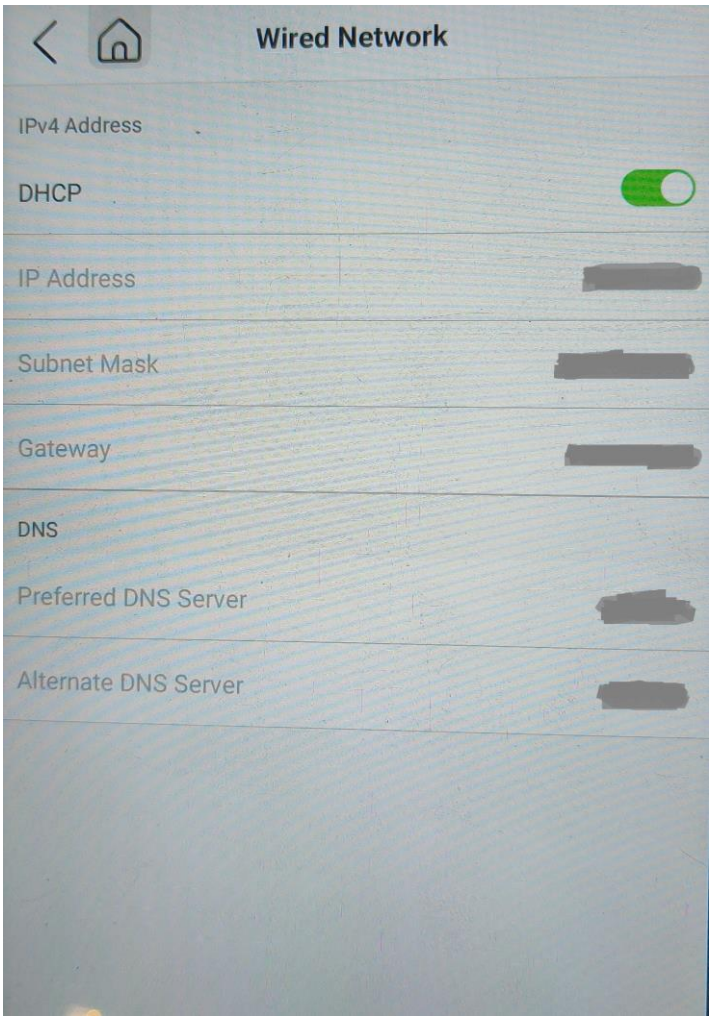


Figure 6-2 Wired network settings page

2. Configure **network parameters** , including DHCP , IPv4 address, gateway address, subnet mask, DNS , etc.

illustrate

- The device IP address and computer IP address must be in the same network segment.
- *DHCP* is enabled , the system automatically assigns an IP address, gateway, and subnet mask to the device.
- If you do not enable the *automatic DNS acquisition* function, you need to configure the preferred DNS server and the backup DNS server. If you enable the *automatic DNS acquisition function* , the system automatically assigns a DNS server.

6.5.2 Setting Wi-Fi parameters

Choose whether to enable Wi-Fi and configure the corresponding Wi-Fi parameters.

Procedure

illustrate

Some device models support Wi-Fi function.

1. Click *Communication Settings* in the menu interface → *Wi-Fi* Enter the Wi-Fi configuration interface.
2. Click the slider  to turn on Wi-Fi .
3. Configure Wi-Fi parameters.
   - Select an existing Wi-Fi in the list and enter the Wi-Fi password. Click *OK* to connect.
   - Wi-Fi in the list , click *Add Wi-Fi* , enter the Wi-Fi name and password, and click *OK* to connect.

illustrate

Passwords support numbers, uppercase and lowercase letters, and symbols.

4. Optional operation : Click the connected Wi-Fi and configure detailed parameters.
   - By default , *DHCP is enabled on the device* , and the system automatically assigns an IP address, subnet mask, and gateway address.
   - DHCP is not enabled , you need to set the IP address, subnet mask and gateway address.

6.6 System Settings

You can configure the device's sound, screen brightness, screen off time, date and time, application management and other functions.
In the menu interface, click *System Settings* to enter the configuration interface.

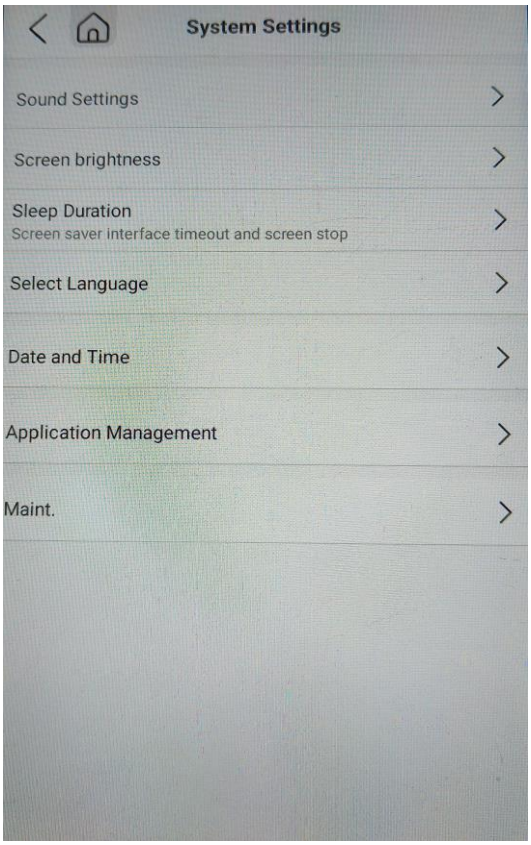


Figure 6-3 System Settings

Sound Settings

You can turn on the device's *voice prompts* and *key tones* , and slide the volume bar to adjust the device's media volume and voice volume.

Screen brightness

You can turn on the device's *adaptive screen brightness* and slide the volume bar to adjust the device's screen brightness.

Screen off time

You can set the device screen saver interface to time out. You can turn on *the screen to never go off* or set **a screen off time** .

Time and Date

The device time, date and date format can be set.

Application Management

You can set application management for the device.

illustrate

Different device models support different functions. Please refer to the actual device.

6.7 System Maintenance

You can view device system information and capacity, restore device factory / default settings, and upgrade or restart the device.

Long press the standby interface for 3 seconds , log in to the backend, and click *System Settings* on the backend management page. → *System maintenance* .

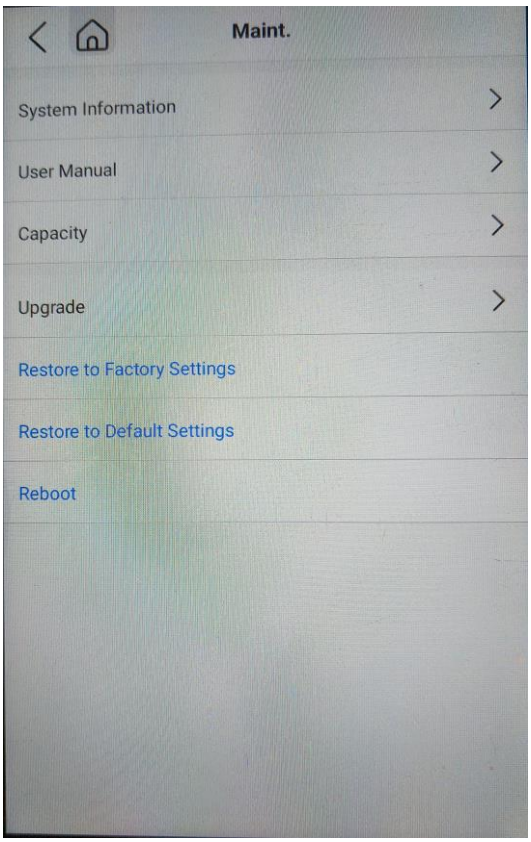


Figure 6-4 System maintenance

System Information

You can view information such as device model, serial number, version, MAC address, and open source code license.

Equipment capacity

You can view device capacity information.

Equipment Upgrade

Insert the USB flash drive into the USB port and click *Device Upgrade* on the interface . → *U disk upgrade* , click *?* , and change the name of the upgrade package according to the corresponding name of the upgrade package prompted on the interface. The device will read the upgrade file in the U disk to upgrade the system.

Restore factory settings

After restoring factory settings, the device will automatically restart.

Restore Default Settings

The system will retain the communication configuration and other parameters will be restored to default. After restoring the default parameters, the device will automatically restart.

Restart your device

The device will restart.

6.8 Face parameter configuration

Configurable face related parameters.
Log in to the backend and click *Smart Settings → Face recognition settings* , you can configure the corresponding parameters.

6.8.1 Locally configure the real person detection security level through the device

After turning on the real person detection function, you can set the face matching security level.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings* .
Enable *human detection* and select the human detection security level.
You can choose from three levels: General, Enhanced, and Professional. The higher the level, the lower the false recognition rate and the higher the false rejection rate.

6.8.2 Configuring the face recognition distance on the device

Configure the distance between the device camera and the face that can be effectively recognized.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings* .
Configure the recognition distance parameters.

6.8.3 Configuring the continuous face recognition interval on the device

Configure the interval between two face recognition attempts during authentication.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings* .
Configure the continuous identification interval.

illustrate

Please fill in a number between 1 and 10 .

6.8.4 Configuring the 1:N Face Matching Threshold on the

Device

1:N face matching.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings* .
Configure the face 1:N comparison threshold.
The larger the threshold, the lower the false recognition rate and the higher the rejection rate . The maximum value is 100 .

6.8.5 Configure the 1:1 face matching threshold on the device

1:1 face matching.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings* .
1:1 face comparison threshold.
The larger the threshold, the lower the false recognition rate and the higher the rejection rate . The maximum value is 100 .

6.8.6 Enable / disable low light mode via the device

enabling low-light mode, the device uses the infrared camera to perform face comparison in low-light or no-light environments.
Log in to the device backend. For details, see .
On the menu page, click *Smart Settings → Face recognition settings → Low light settings* .
enabling low light mode, the device uses the infrared camera to perform face matching in low light or no light environment. You can configure the switching threshold, 1:N threshold, and 1:1 threshold.

Switching threshold

enabling low-light mode, you need to configure the low-light switching threshold. The larger the threshold, the easier it is for the device to enter low-light mode; the smaller the threshold, the less likely it is to enter low-light mode. The threshold is related to light intensity.

1:1 Threshold

1:1 face matching through the camera in low-light mode . The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value that can be filled is 100 .

1:N Threshold

The matching threshold for 1:N face matching by the camera in low-light mode . The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces. The maximum value that can be filled is 100 .

6.9 Cabinet Management

The smart cabinet can be managed.

Procedure

1. Log in to the backend and click *Cabinet Management* .
2. Click on *the grid status* to check the grid status.
3. Select **the cabinet user role** .

illustrate

Different device models support different user roles. Please refer to the actual device for details.

Visitors and Internal Personnel

It is suitable for scenarios where temporary visitors and internal fixed staff use it together.

Visitors

Suitable for scenarios where visitors or temporary personnel temporarily use the entrance.

Insiders

It is suitable for scenarios where fixed personnel such as internal employees use the grid for a long time.

4. *Visitor input information supplement* can be enabled . After enabling, visitors can supplement the input information.
5. Click on *the stored items query* , select the stored items certificate , and verify the relevant certificates to query the stored items.
6. Click *one button to open the cabinet* , and all cabinets of the equipment will be opened with one button, and you can store items.

illustrate

The grid relationship of the one-click locker opening personnel will still be retained.

7. Click *one button to clear the boxes* , and all the cabinets in the equipment will be opened with one button, and you can take out the items.

illustrate

After clearing the box with one click , the corresponding slot permissions of the personnel will be cleared.

6.10 Configure host authentication method through the device

Set the authentication type and method for personnel authentication on this device . You can choose different combinations for authentication.
Log in to the device backend. For details, see .
Authentication Settings on the main menu interface. → *Host authentication settings* .
Select the personnel authentication type and method in Host Authentication Mode and save the parameters.

illustrate

Some device models do not support fingerprint-related authentication.

Notice

Biometric products cannot be 100% applicable to all anti-counterfeiting environments. For high-security locations, please use a combination of authentication methods.

6.11 Set password mode through the device

Before configuring a personnel password, you need to specify whether the password mode used is a local personal password or a platform personal password. If it is a local personal password, you can create and edit the password on the device and the Web , but not on the platform; if it is a platform personal password, you need to configure the personnel password on the platform, and it cannot be edited locally or on the Web .
Log in to the device backend. For details, see .
In the configuration menu interface, click *Authentication Settings* → *Password mode* .
Configure *the password mode* to **platform personal password** or **local personal password**

Platform personal password

You can create a password on the platform that the device is connected to and send it to the device for use. You cannot create or edit it locally on the device or on the web .

Local personal password

You can create or edit a personnel password locally on the device or on the web . You cannot set this password on other platforms.

6.12 Data Management

Import users, export user templates, export collected data, and clear collected data in the data management module.

6.12.1 Deleting Data

User data can be deleted in the data *management module.*
Data Management in the main menu interface. → *Delete data* and select the data to be deleted according to your needs.

6.12.2 Importing Data

Procedure

1. Insert the USB flash drive into the USB port of the device .
2. Click *Data Management* on the main menu interface to enter the data management page.
3. Click *Import Data* on the Data Management page .
4. Select the data you want to import.

5. Enter the password created when exporting data. If no password is configured, leave it blank and click *Confirm* . The data will be imported from the USB drive to the device.

illustrate

- import all user information in device A to device B , you need to first import the user data in device A to a USB flash drive, and then import the user data to device B via the USB flash drive .
- supported USB flash drive formats are FAT32 or exFat .
- If there are too many pictures to be imported manually and enroll_pic cannot store all of them, you can create folders enroll_pic1 , enroll_pic2 , enroll_pic3 , and enroll_pic4 in the root directory to store the pictures. The picture names must comply with the picture naming rules.

6.12.3 Exporting Data

Procedure

1. Insert the USB flash drive into the USB port of the device .
2. Click *Data Management* on the main menu interface to enter the *data management* interface.
3. Click *Export Data* on the Data Management page .
4. Select the data you want to export.
5. Create a password for exporting data. If you import this data into other devices, you must enter the same password to export successfully.

illustrate

- The created export password can be empty.
- supported USB flash drive formats are FAT32 or exFAT .
- USB supports 1G ~ 256G USB flash drives. Please ensure that the remaining space of the USB flash drive is more than 512M .
- The exported data is an encrypted file in DB format and cannot be edited.

6.13 Configuring Privacy Parameters

You can configure the parameters related to image upload .

illustrate

Different device models support different functions. Please refer to the specific device for details.

Log in to the device backend. For details, see .
Select *Privacy Management → Privacy settings* .

Set up image storage and upload

Save the recognized captured image

The picture captured during authentication will be saved to the device.

Upload the captured image for identification

The pictures captured during authentication will be uploaded to the platform.

Save the face registration picture

The registration picture when adding a person will be saved to the device.

Personnel Password Security Statement

Click on *the Personal Password Security Statement* . Read the security statement and choose to *not use a password yet* or *continue using a password* .

6.14 Device Password Management

You can modify the device password, or bind a mobile phone number to the device and reset the password via your mobile phone.

Privacy Management on the backend management page → *Device Password* Enter the device password management interface.

Change device password

Click *Change Password* , enter the old password, and click *Next* to modify it.

Enter a new password and confirm it, then click *OK* .

Notice

- To better protect your privacy and improve product security, we strongly recommend that you set a more complex password according to the following rules: the password must be between 8 and 16 characters long and consist of two or more types of numbers, uppercase and lowercase letters, and special characters.
- Please understand that you are responsible for properly configuring all passwords and other related product security settings.
- The password cannot contain the user name, 123 , admin , 4 or more consecutive increasing or decreasing numbers, or the same characters.
- The password cannot contain the phrases hik , hkws , hikvision and is not case sensitive.

Reserve mobile phone number

You can enter an 11- digit mobile phone number to bind the phone number to the device. You can then reset the password by verifying the phone number.

Chapter 7 Web page quick configuration

7.1 Web Wizard: Retrieve Password

If you forget your password, you can reset your device password using the security questions you set or your reserved mobile phone number.

Set security questions

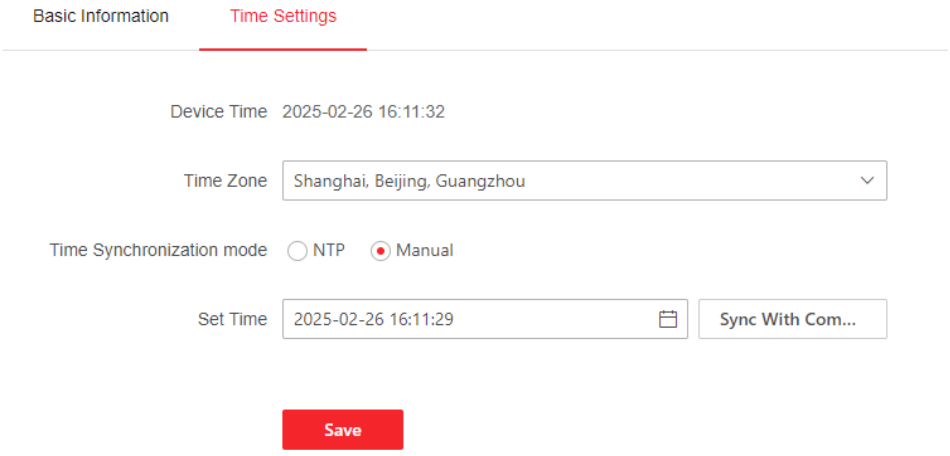
Click on the upper right corner of the web page to enter the password recovery interface. Set security questions and answers according to actual needs. Click *Next* .
Or click *Skip* .

Reserve mobile phone number (optional)

Click on the upper right corner of the web page to enter the password recovery interface. Configure your mobile phone number. Click *Next* .
Or click *Skip* .

7.2 Time Configuration

time calibration method and time displayed on the machine .
Click on the upper right corner of the web page to enter the time configuration interface. You can click *Skip* ; or after the configuration is completed, click *Next* .



Time Zone

Select the time zone where your device is located from the drop-down box.

Time adjustment method

Manual time adjustment

The default setting is manual time adjustment. You can manually configure the device time, or check Synchronize *with computer time* to have the device automatically synchronize with the computer time.

NTP time synchronization

You need to configure the NTP time synchronization server address, port, and time synchronization interval.

After the configuration is complete, click *Next step* .

7.3 Select the users of the cabinet group

According to the needs, **the users of the cabinet group can be selected** as *internal staff* , *visitors* or *mixed personnel* .

7.4 Privacy Configuration

Configurable image upload and storage related parameters.

illustrate

Different device models support different functions. Please refer to the specific device for details.

Click in the upper right corner of the web page to enter the configuration interface. You can click *Skip* or *Next to* continue configuration.

Image upload and storage configuration

Configurable image uploading and storage.

Save the recognized captured image

The picture captured during authentication will be saved to the device.

Upload the captured image for identification

The pictures captured during authentication will be uploaded to the platform.

Save the face registration picture

When enabled, face pictures will be saved to the device when people add faces.

Automatic photo taking when visitor enters the account

Once enabled, automatic photography may pose compliance risks , and visitors need to be informed in advance that their faces will be automatically captured.

Chapter 8 Web page operation instructions

8.1 Login

You can log in to the device through the web page to configure parameters.

illustrate

Please make sure that the device has been activated. For detailed activation configuration, see *Activation* .
http:// device IP address in the browser address bar and press Enter on the keyboard to enter the login interface. Enter the user name and password and click *Login* .

8.2 Overview

You can preview the smart cabinet configuration information, service information, real-time images, personnel information, network status, basic equipment information and equipment capacity.
After logging in, enter the *preview* page and preview the cabinet status, slot status, slot occupancy, configuration information, service information, real-time images, personnel information, network status, basic equipment information and equipment capacity.
Functional description:

illustrate

Different devices support different functions. Please refer to the actual interface.

Configuration Information

You can view the current cabinet operation mode, authentication method, and user.

Service Information

You can view the phone number, address and other information of the current ATM service provider.

Grid status

You can view the current free slots, allocated slots, stored slots, locked slots and abnormal slots.

Real-time picture

You can view the real-time status of the device.

Network Status

You can view the wired network and wireless network status.

Equipment capacity

You can view the device’s face and card information.

View basic device information

You can view the device model, serial number and main control version.

8.3 Adding People

Add basic information of personnel

Click *People Management → Add* to enter the Add Person page.
Create a personnel ID, name, and mobile phone number, and set the personnel type.
Click *Save* .

Setting up access control

Click *People Management → Add* to enter the Add Person page.
checking *whether to be a device administrator* in access control , the added personnel can log in to the device backend through authentication.
Enables *personnel to determine whether they are valid for a long period of time* or configures the start and end time of personnel permissions.
Click *Save* .

Add a card

Click *People Management → Add* to enter the Add Person page.
Click *Add Card* , enter the card number and select the card properties.
Click *Save* .

Add a photo of a face

Click *People Management → Add* to enter the Add Person page.
Click *Local Upload* or *Device Collection* and select photos to upload from your local computer.

illustrate

The image format should be JPG , JPEG or PNG and smaller than 200K .

Click *Save* .

Add a password

6 -digit alphanumeric password manually or click *Generate automatically* .

illustrate

- Before adding a password, please agree to *the password security statement* . For details, see *Configuring Privacy Parameters* .
- This operation must be performed by the user himself/herself. The administrator cannot set it on your behalf. Please make sure the surrounding environment is safe. Please keep the password properly after setting it.

Permission Configuration

Click *People Management → Add to → Permission configuration* , select the slot permissions for the person, and set **the number of free slots to be allocated** .

illustrate

- Internal personnel support configuration of free slots and corresponding quantities, designated slots and corresponding designated slots, and configuration as no permission.

- Guests only support free slots.

Click *Save* .

8.4 Check the status of smart cabinet

You can check the usage status of the smart cabinet .
Click *Smart Cabinet → Cabinet group management* enters the smart cabinet status viewing page.

locking

A cabinet in a locked state cannot be opened and can only be opened after recovery.

Allocated

The use rights of the cabinets have been assigned to the corresponding personnel. The rights can be issued through the web page or entered locally in the guest mode.

idle

Locker permissions have not been assigned and there are no items in the locker.

Storage

Locker permissions are assigned and there are items in the locker.

abnormal

The cabinet is in an abnormal state. Hovering the mouse over the cabinet will display its abnormal information.

One-click box clearing

Click *one button* to clear the cabinet to delete all cabinet permissions. You can check *whether to delete the personnel according to actual needs* . After checking, you need to verify the administrator password and the set personnel permissions will be cleared.

Batch rename cabinet groups and compartment names

Click *Batch Rename* to batch edit the cabinet group names or compartment names on the right.
Click a slot to open, lock, release, unlock, rename, or view the access history of the slot .

8.5 Access Record Query

Click *Smart Cabinet → Access records* to enter the query page.
Enter the search criteria, including employee number, name, card number, slot, search start time, and end time, and click *Search* .

illustrate

Supports searching for names within 128 characters.

The search results will be displayed on the right side of the interface.

8.6 Main cabinet configuration

8.6.1 Storage and Access Configuration

Configurable cabinet storage and retrieval components.

Procedure

1. Click *Smart Cabinet → Parameter configuration → Accessor configuration* .
2. Select **the user who will use the cabinet** .

illustrate

Different device models support different user types. Please refer to the actual device for details.

Cabinet users

Insiders

It is suitable for scenarios where fixed personnel such as internal employees use the grid for a long time.

Visitors

Suitable for scenarios where visitors or temporary personnel temporarily use the entrance.

Mixed staff

It is suitable for scenarios where temporary visitors and internal fixed staff use it together.

illustrate

To switch **the user group of the cabinet** , you need to verify the administrator password.

Grid opening timeout

When the timeout period arrives after the user opens the gate, the device will be locked.

Storage Selection Method

If you choose *manual selection* , the user needs to select the cabinet when depositing items . If you choose *system random* , the system will randomly assign a cabinet when depositing items .

Visitor storage validity period

If the user of the cabinet selects *visitor* or *employee and visitor* , the validity period of the visitor's storage must be configured . If the configured number of days is exceeded, the compartment permission will be cleared and the visitor will not be able to access the items in the compartment.

Number of visitor slots allocated

The number of slots reserved for visitors.

Countdown for deposit and withdrawal operations

You can set a countdown for the deposit and retrieval operation , and the operation will be unavailable after the timeout.

Grid closure confirmation

After opening, when the deposit or retrieval is completed, the smart cabinet will confirm the closure of the compartment.

Pickup code

Once turned on, the device will be able to pick up items using the pickup code.

Grid lock expired

When the timeout period expires after the user opens the port, the device will be locked.

Expiration Type

overdue type and **overdue duration** according to actual conditions.

.

3. Click *Save* .

8.6.2 Authentication parameter configuration

Configure authentication parameters.
Click *Smart Cabinet → Parameter configuration → Authentication Configuration* , enter the configuration page.
After configuring the parameters, click *Save* to save the configuration.

Enable Authentication Device

If this function is enabled, the authentication terminal can be used normally by swiping a card; if this function is disabled, the door entry authentication terminal cannot be used normally by swiping a card.

Single credential authentication timeout

The time for each credential authentication can be configured.

illustrate

The default password authentication mode is 20s and is not restricted by the above configuration.

Continuous face recognition interval

Please fill in a number between 1 and 10 .

Re-authentication interval

Configure the interval between two authentication attempts of the same person. During the configured time period, the same person can only be authenticated once.

Certification Program Configuration

You can select the **authentication plan** method. If you select *All Time Periods , you can select* **the authentication method** for all time periods . If you select *Custom* , you can click *Edit* , select the authentication method, and drag the time period in the plan list. Click *Save* .

8.6.3 Cabinet information configuration

When the user encounters problems when operating the cabinet, he can open the help to see the cabinet

information.

Procedure

1. Click *Smart Cabinet → Parameter configuration → Service information configuration* .
2. Enter **the contact number** , **device number** and **location information** .
3. Click *Save* to complete the configuration.

8.6.4 Configuring biometric parameters

Configure biometric related parameters.

Biometric parameter configuration

Click *Smart Cabinet → Parameter configuration → Smart Configuration* , enter the configuration page.

illustrate

The parameter items supported by different models are different. Please refer to the actual interface.

Configure face parameters.

Enable human detection

Choose whether to enable the real face detection function. After enabling this function, the device can determine whether it is a real face. If the detected face is not a real face, the authentication fails.

Real person detection safety level

The face matching security level after the real person detection function is turned on. You can choose from three levels: General, Enhanced, and Professional. The higher the level, the lower the false recognition rate and the higher the rejection rate .

Face duplication check

enabling face duplication check , when adding a person's face, the system will perform a face duplication check. If the system detects that the same face exists, a prompt will be given.

Identification distance

Select the distance for face recognition in the actual environment.

Face 1:N threshold

face 1:N matching. The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value is 100 .

Face recognition timeout

Configure the timeout period for face recognition. If the face recognition time exceeds the configured value, the device prompts "Face not registered".

Up and down pitch angle

The maximum angle at which the head can be raised or lowered during face detection. When matching or recording faces, the angle of raising or lowering the head must be less than the configured value.

Left and right horizontal angle

The maximum angle that can be rotated left or right during face detection. When matching or recording faces, the angle of rotation left or right must be less than the configured value.

The face scoring threshold for sending pictures

The score threshold for the face images sent. The higher the threshold, the higher the image quality requirement. If the image fails to be sent, you can adjust the threshold or image quality according to actual needs.

1 : 1 comparison face scoring threshold

The scoring threshold for face comparison. Keep the default value.

Face 1:1 threshold

1:1 face matching. The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value is 100 .

Face 1:N threshold

face 1:N matching. The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value is 100 .

Face recognition timeout

Configure the timeout period for face recognition. If the face recognition time exceeds the configured value, the device prompts "Face not registered".

Low light mode parameters

Low light mode

enabling low-light mode, the device uses the infrared camera to perform face comparison in low-light or no-light environments. You can configure low-light mode threshold, low-light mode (1:N), low-light mode (1:1), low-light mode mask face 1:1 threshold, and low-light mode mask face 1:N threshold.

Low light mode 1:1 threshold

1:1 face matching in low-light mode. The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value that can be filled is 100 .

Low light mode 1: N threshold

1:N face matching in low-light mode. The larger the threshold, the lower the false recognition rate and the higher the rejection rate when recognizing faces . The maximum value that can be filled is 100 .

Face recognition area configuration

Click *Configure → Intelligent configuration → Regional Configuration* , enter the configuration page.
Drag the outline of the yellow frame in the preview screen to adjust the effective area for face recognition to the left, right, top, and bottom.
Click *Save* to save the configuration.

8.6.5 Card Configuration

/ disable NFC protection via the web page

Once turned on, the device can recognize NFC cards.
Click *Smart Cabinet → Parameter configuration → Card Configuration* , enter the configuration page.
Click the slider *to enable NFC cards* , and click *Save* . After it is turned on, the device can recognize NFC

cards. To prevent mobile phones from obtaining access control device data and illegal access, you can disable the NFC function to protect access to access control devices.

/ disable M1 card via web interface

enabling the M1 card, the device can recognize the M1 card and users can swipe the M1 card on the device .
Click *Smart Cabinet → Parameter configuration → Card Configuration* , enter the configuration page.
Click the slider *to enable the M1 card* .

M1 card encryption verification

Enabling M1 card encryption verification can improve the security of access control cards , making them less likely to be copied.

Sector

enabling M1 card encryption verification, configure the encryption sector number.

illustrate

It is recommended to encrypt sector 13 .

Click *Save* .

/ disable CPU card through web page

the CPU card is enabled , the device can recognize the CPU card and the user can swipe the CPU card on the device .
Click *Smart Cabinet → Parameter configuration → Card Configuration* , enter the configuration page.
Click the slider *to enable the CPU card* .
Click the slider to enable *CPU card reading* . After enabling, the device can read the contents of the CPU card.
Click *Save* .

Enable / disable ID card

can be enabled / disabled.
Click *Smart Cabinet → Parameter configuration → Card Configuration* , enter the configuration page.
Click **to enable ID card** . After turning it on, the device can recognize the ID card.
Click *Save* .

Configure the card number authentication mode via the web page

Configure the card number content that the device reads when passing card number authentication.
Click *Smart Cabinet → Parameter configuration → Card configuration* .
Select Card Number Authentication Mode and click *Save* .

Full card number

The entire card number content will be read.

3 bytes

Only 3 bytes of card number are read.

4 bytes

Only 4 bytes of card number are read.

8.6.6 Privacy parameter configuration

Configure event storage via the web page

Configurable way of storing events.
Click *Smart Cabinet → Parameter configuration → Privacy configuration* .
You can choose **to delete old events regularly** , **delete old events according to specified events** , or **overwrite them cyclically in the event storage method** .

Periodically delete old events

Drag the slider to select or directly enter the cycle for deleting old events in the input box. All events will be deleted according to the set cycle.

Delete old events by specified time

Configure the time, all events before the specified time will be deleted.

Loop Coverage

the event storage is 95% full , the system automatically deletes the earliest 5% of stored events.

Click *Save* .

Configure the authentication result display content through the web page

Configure the content displayed in the authentication result, such as photo, name, work number, health information, etc.
Smart Locker on the web page → *Parameter configuration → Privacy configuration* .
In the authentication configuration module, you can check the authentication results to display relevant content, such as photo, name, work number, etc.
select *the name desensitization display* and *employee number desensitization display* according to actual needs . After desensitization, only part of the name and employee number will be displayed.
the authentication result display duration as required .
After configuration is complete, click *Save* .

Configure image upload and storage parameters through the web page

Configurable image uploading and storage.
Click *Smart Cabinet → Parameter configuration → Privacy Configuration* , enter the configuration page.
Click the slider to save and upload the image or voiceprint content.

Save the recognized captured image

The picture captured during authentication will be saved to the device.

Upload the captured image for identification

The pictures captured during authentication will be uploaded to the platform.

Automatic photo taking when visitor enters the account

Once enabled, automatic photography may pose compliance risks , and visitors need to be informed in advance that their faces will be automatically captured.

Click *Save* .

Clear device images via the web page

All registered, authenticated or captured face images in the device can be cleared.

Click *Smart Cabinet* → *Parameter configuration* → *Privacy Configuration* , enter the configuration page.

Click *Clear* to clear all registered, authenticated, or captured face images in the device.

Configuring Password Mode

Before configuring a personnel password, you need to specify whether the password mode used is a local personal password or a platform personal password. If it is a local personal password, you can create and edit the password on the device and the Web , but not on the platform; if it is a platform personal password, you need to configure the personnel password on the platform, and it cannot be edited locally or on the Web .

Click *Smart Cabinet* → *Parameter configuration* → *Privacy configuration* .

In the Password Mode module, you can configure the following parameters. After completing the configuration, click *Save* .

Platform personal password

You can create a password on the platform that the device is connected to and send it to the device for use. You cannot create or edit it locally on the device or on the web .

Local personal password

You can create or edit a personnel password locally on the device or on the web . You cannot set this password on other platforms.

Information entry

After it is turned on, visitors can enter and supplement their information.

Click *Smart Cabinet* → *Parameter configuration* → *Privacy configuration* .

Enable *the supplementary entry of visitor information* . After completing the configuration, click *Save* .

Configuring privacy parameters

You can configure the privacy protocol related parameters. You can enable the privacy protocol confirmation (informed confirmation) function according to the actual situation. After it is enabled, the user will be prompted to confirm the information before each collection.

Click *Smart Cabinet* → *Parameter configuration* → *Privacy configuration* .

Click the slider to enable *the privacy agreement confirmation* . Enter the privacy document title and file name.

Personnel Password Security Statement

You can view the personnel password security statement and decide whether to use the password.
Click *Smart Cabinet → Parameter configuration → Privacy configuration* .
View after the password security statement . You can choose *to agree* or *not use the password for now* .
After the configuration is complete, click *Save* .

8.7 System Maintenance

8.7.1 View basic device information

You can view the device name, device number, device language, device model, device serial number, version, number of channels, and local 485 number of the device.
Click *Smart Cabinet → System Management → system → System Configuration → Basic information* , enter the page.
You can view the device name, device number, device language, device model, device serial number, version, number of channels, and local 485 number of the device.

illustrate
The viewing items supported by different device models may vary. Please refer to the actual device.

8.7.2 Configuring device time

time calibration method and time displayed on the machine .
Click *System Maintenance → System Management → system → System Configuration → Time Configuration* , enter the configuration page.
After configuring the parameters, click *Save* to save the configuration.

Time Zone

Select the time zone where your device is located from the drop-down box.

Time adjustment method

Manual time adjustment

The default setting is manual time adjustment. You can manually configure the device time, or check Synchronize *with computer time* to have the device automatically synchronize with the computer time.

NTP time synchronization

You need to configure the NTP time synchronization server address, port, and time synchronization interval.

8.7.3 Change the administrator password

Change the administrator's login password

Procedure

1. Click *System Maintenance → System Management → system → User Management* , enter the configuration page.
2. Click admin under the User Operation column .
3. Enter your old password, create a new password, and confirm your password.

Notice

- To better protect your privacy and improve product security, we strongly recommend that you set a more complex password according to the following rules: the password must be between 8 and 16 characters long and consist of two or more types of numbers, uppercase and lowercase letters, and special characters.
- Please understand that you are responsible for properly configuring all passwords and other related product security settings.

4. Click *Confirm* .
   The device password will be changed and you will need to log in to the web page again.

8.7.4 Modify account security questions and answers

Set the device's account security questions and answers. If you forget your password, you can reset your account password through identity verification.

Procedure

1. Click *System Maintenance → System Management → system → User Management → Account security settings* .
2. Select security questions according to actual needs and enter the answers.
3. Click *OK* .

8.7.5 Check the deployment

View online users of the device.
Click *System Maintenance → System Management → system → User Management → Online users* , enter the configuration interface.
Users can view the online user information of the device.

8.7.6 Network Configuration

Configure TCP/IP , HTTP parameters, RTSP , platform, and SDK services.

Configure basic network parameters

Configure device TCP/IP information.
Click *System Maintenance* → *System Management* → *network* → *Network Configuration* → *TCP/IP* , enter the configuration page.

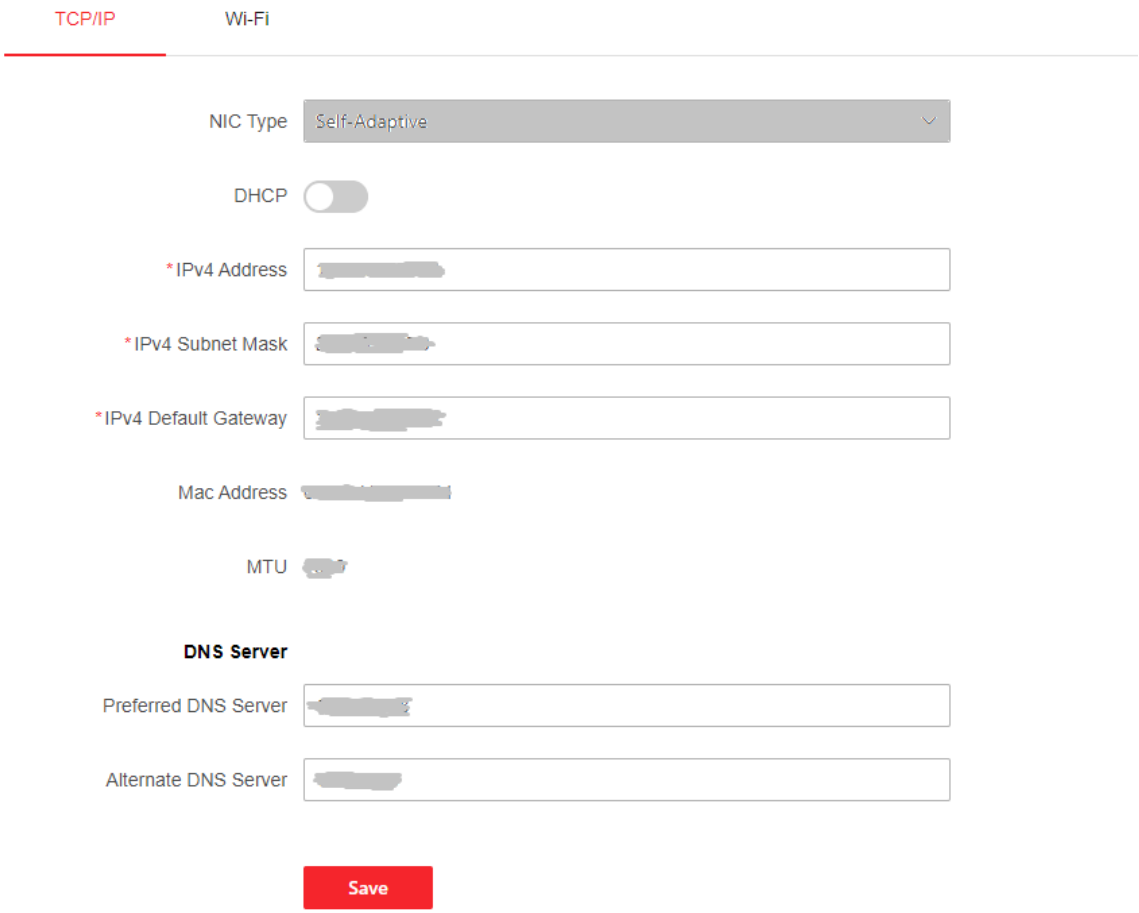


Figure 8-1 Basic network parameter configuration

After configuring the parameters, click *Save* to save the parameters.

Network card type

Select the network card type in the drop-down box. The default is adaptive.

Automatic acquisition

If this option is not checked , you need to manually configure the IPv4 address, IPv4 subnet mask, IPv4 default gateway, MTU and physical address.
If this option is checked , the system automatically assigns the IPv4 address, IPv4 subnet mask, IPv4 default

gateway and MTU .

Preferred DNS server and alternate DNS server

DNS server address as required .

Wi-Fi parameters via the web page

Configure the Wi-Fi parameters to which the device is connected.

Procedure

illustrate

Wi-Fi parameters can be configured only if the device supports it .

1. Click *System and Maintenance → System Management → network → Network Configuration → Wi-Fi* , enter the configuration interface.
2. Click the slider to enable *Wi-Fi* .
3. Add Wi-Fi .
   1) Click *Add Manually* .
   2) Enter the Wi-Fi SSID and select the security mode.
   3) Click *OK* .
4. The added Wi-Fi is displayed in the list. Click *Connect* , enter the Wi-Fi password and click *Connect* .
5. Click *Refresh* Wi-Fi List.
6. Configure WLAN parameters.
   1) Configure the IPV4 address, subnet mask and default gateway. Or click the slider to enable *automatic acquisition* , and the system will automatically assign the IPV4 address, subnet mask and default gateway.
   2) Configure the DNS server address. Or click the slider to enable *automatic acquisition* , and the system will automatically assign the server address.
7. Click *Save* .

Port Configuration

Enable / disable HTTP

You can enable the HTTP function to improve the security of browser access.

Click *System and Maintenance → System Management → network → Network Services → HTTP(S)* , enter the configuration interface.

After configuring the parameters, click *Save* .

HTTP Port

, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81 , when you log in using a browser, you need to enter http://192.0.0.65:81 .

HTTPS Port

Configure the device HTTPS port for browser access, but certificate verification is required.

HTTP Listener

The device sends alarm information to the destination IP or domain name through HTTP protocol , which

requires the destination IP address or domain name to support HTTP protocol transmission. Enter the destination IP or domain name, URL address and port, and select the protocol type.

RTSP port through the web page

Real-time Transport Protocol port.

Click *System and Maintenance* → *System Management* → *network* → *Network Services* → *RTSP* , enter the configuration interface.

Check the RTSP port.

WebSocket(s) via the web client

Websocket(s) are used for plugin-free preview, playback, and alarm display.

Click *System and Maintenance* → *System Management* → *network* → *Network Services* → *WebSocket(s)* , enter the configuration interface.

Enable WebSocket or WebSockets and configure the port number.

illustrate

If you do not need to use the plug-in-free preview, playback, and alarm display functions, it is recommended to close Websocket(s) to ensure the network security of the device.

Click *Save* .

8.7.7 Video and Audio Parameter Configuration

Configure video parameters via the web page

You can configure image parameters such as image quality and resolution of the device camera.

Click *System and Maintenance* → *System Management* → *Video and Audio* → *Video* , enter the

configuration interface.

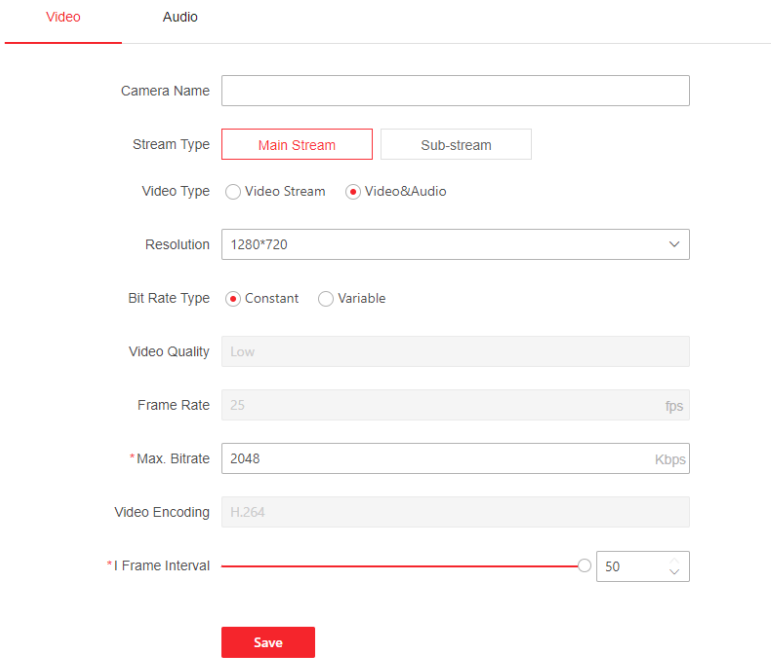


Figure 8-2 Video

Configure the channel name, stream type, video type, resolution, bitrate type, image quality, video frame rate, bitrate upper limit, video encoding , and I -frame interval.

After configuring the parameters, click *Save* to save the configuration.

Configure audio parameters via the web page

Configurable device volume.

Click *System and Maintenance* → *System Management* → *Video and Audio* → *Audio* , enter the configuration interface.

the stream type and audio encoding as needed . Use the sliders to configure the input and output volumes.

Enable *voice prompt* to turn on the voice prompt function of the device.

After configuring the parameters, click *Save* to save the configuration.

8.7.8 Image parameter configuration

/ contrast / saturation / sharpness via the web page

Configure image information such as image brightness, contrast, saturation, and sharpness on the device preview page .

Click *System and Maintenance* → *System Management* → *image* → *Display configuration* and enter

the configuration page.

Image Adjustment

Drag the sliders or enter values to configure Brightness, Contrast, Saturation, and Sharpness as required . Click *Restore Defaults* to restore default parameters.

Configure the fill light brightness via the web page

Configure the device fill light brightness.

Procedure

1. Click *System and Maintenance* → *System Management* → *image* → *Display configuration* and enter the configuration page.
2. Configure the fill light type, fill light mode and fill light brightness.
3. Optional operation : Click *Restore Defaults* to restore the default parameters.

Configure wide dynamic range via web page

Click *System and Maintenance* → *System Management* → *image* → *Display configuration* and enter the configuration page.

Turn on or off the wide dynamic range function. When wide dynamic range is turned on, both the brightest and darkest parts of the scene can be seen more clearly .

Click *Restore Defaults* to restore default parameters.

Configure the video format via the web page

Configure the video format of the device preview page.

Click *System and Maintenance* → *System Management* → *image* → *Display configuration* and enter the configuration page.

Video Adjustment

Set the frame rate of the video during remote preview. After changing the format, you need to restart the device for it to take effect.

PAL

25 frames per second , suitable for countries and regions such as mainland China, Hong Kong, China, the Middle East and Europe.

NTSC

30 frames per second , suitable for countries and regions such as the United States, Canada, Japan, Taiwan,China, South Korea, and the Philippines.

Click *Restore Defaults* to restore default parameters.

8.7.9 Configure RS-485 parameters via the web page

The device can be connected to an access control host, card reader or expansion module via the RS-485

interface. Set the RS-485 parameters here to connect to external devices.

Click *System and Maintenance → System Management → Access Configuration → RS-485* , enter the configuration page.

After configuring the parameters, click *Save* to save the configuration.

Enable

turning on RS-485 , you can enable the RS-485 function.

External device type

The external device type supports *the lock control panel* .

illustrate

After changing the external device and saving the parameters, the device will automatically restart.

RS-485 Address

Configure the RS-485 address according to actual conditions.

illustrate

When the external device selects **the access control host** , if the external device is an integrated device, the local RS-485 address corresponding to the external device needs to be set to 2 ; if the external device is a access control host, the RS-485 address needs to be configured according to the corresponding door number .

Baud rate / data bit / stop bit

Check the baud rate, data bits, and stop bits during RS-485 communication.

Verification / flow control / communication mode

Check the calibration, flow control and communication mode.

8.7.10 Personalized Configuration

Configure the standby screen via the web page

Configurable time to enter standby mode.

Click *System & Maintenance → Personalization → The screen displays* , entering the configuration page.

Configure the idle screen parameters and click *Save* .

Enter standby time

The device will enter the standby screen after the configured time.

Configure the screen off via the web page

When screen off is enabled, the device automatically turns off the screen after the configured screen off time .

This can reduce power consumption.

Click *System and Maintenance* → *Personalization* → *The screen displays* , entering the configuration page.

sliding **to enable the screen off function** , you can configure the screen off time.

After configuring the screen off parameters, click *Save* .

Configuring information publishing via the web page

Configure the device's main interface advertisement.

Procedure

1. Click *System and Maintenance* → *Personalization* → *Information release* , enter the configuration page.
2. Click *Add Program* , enter **the program name** and select **the program type** , then click *Save* .
   - If you select picture as the program type, you can click + to select a picture from the library and configure **the switching time** .
3. Click *Edit Name* to modify the program name, and click *Delete Program* to delete the added program.
4. Click *Media Library Management* → + You can upload materials.
5. Click *Download MP4 Format Conversion Tool* to download the tool for format conversion.
6. Set the playback schedule.
   1) Select the corresponding program and drag the time interval to be played on the timeline.
   2) Optional operation : Click the drawn area to manually modify the time.
   3) Click *Erase* to delete the selected interval. Click . . . → Clear and delete all drawn intervals *with one click* .
7. Click *Save* .

8.7.11 System Upgrade and Maintenance

You can restart the device, restore device parameters, upgrade the device, and back up device parameters.

Restart your device

Click *Maintenance and Security* → *System maintenance* → *Restart* and enter the configuration page.

Click *Restart* and the device starts restarting.

Upgrading Equipment

Click *Maintenance and Security* → *System maintenance* → *Upgrade* and enter the configuration page.

Select the upgrade type from the drop-down list, click Select an upgrade file from local, and click *Upgrade* .

The device automatically obtains the upgrade file for the upgrade.

illustrate

The upgrade process takes about 1 to 10 minutes. Please do not turn off the power during the upgrade process. The device will automatically restart after the upgrade is completed.

Restore Parameters

Click *Maintenance and Security → System maintenance → Backup and reset* , enter the configuration page.

Simple recovery

The device parameters will be restored to the default parameters, but the device IP address information will not be restored.

Full recovery

The device is restored to factory settings and needs to be reactivated before it can be used again.

Equipment parameter import and export

Click *Maintenance and Security → System maintenance → Backup and reset* , enter the configuration page.

Parameter export

Click *Export* to export the device parameters.

illustrate

The exported device parameters can be imported into another device via parameters.

Parameter import

Click to select the file to be imported from the local computer , and click *Import* to import parameters.

Restart your device

The device can be restarted.

Click *System and Maintenance → maintain → Restart* and enter the configuration page.

Click *Restart* and the device starts restarting.

Equipment Upgrade

Local upgrade via the web page

The device can be upgraded locally.

Click *System and Maintenance → maintain → Upgrade* and enter the configuration page.

Select the upgrade type from the drop-down box, click Select the upgrade file from local, and click *Upgrade* . The device automatically obtains the upgrade file for the upgrade. When the lock control board needs to be

upgraded, you can select the cabinet group for the upgrade.

Restore settings

Restore factory settings via the web interface

You can restore the device to factory settings.

Click *System and Maintenance → maintain → Backup and reset* , enter the configuration page.

Click *Full Restore* to restore the device to factory settings. The device needs to be reactivated before it can be used again.

Restore default settings via the web page

The device can be restored to default parameters.

Click *System and Maintenance → maintain → Backup and reset* , enter the configuration page.

Click *Simple Restore* to restore the device parameters to the default settings, but do not restore information such as the device IP address.

Export device parameters via the web page

Device parameters can be exported according to actual needs.

Click *System and Maintenance → maintain → Backup and reset* , enter the configuration page.

Parameter export

Click *Export* to export the device parameters.

illustrate

The exported device parameters can be imported into another device via parameters.

Import device parameters via the web page

parameters can be imported according to actual needs .

Click *System & Maintenance → maintain → Backup and reset* , enter the configuration page.

Parameter import

Click to select the file to be imported from the local computer , and click *Import* to import parameters.

Equipment debugging

/ disable SSH via the web client

You can enable the SSH function for remote debugging.

Click *System and Maintenance → maintain → Equipment debugging → Log debugging* , enter the configuration interface.

Enable SSH

SSH is generally used for remote debugging. When this service is not needed, it is recommended not to enable SSH to improve device security.

Exporting print logs via the web page

Printable device logs.

Click *System & Maintenance → maintain → Equipment debugging → Log debugging* , enter the configuration interface.

Click *Export* to print the device log.

network packet capture via the web page

You can set the packet capture duration and size, and view and debug logs based on the packet capture content .

Click *System and Maintenance → maintain → Equipment debugging → Log debugging* , enter the configuration page.

Configure **the packet capture duration** and **size** , and click *Start packet capture* to start packet capture.

Protocol testing via the web page

After entering the protocol address, perform a protocol test. The device protocol can be debugged through the returned response header and return value.

Click *System and Maintenance → maintain → Equipment debugging → Protocol test* , enter the configuration page.

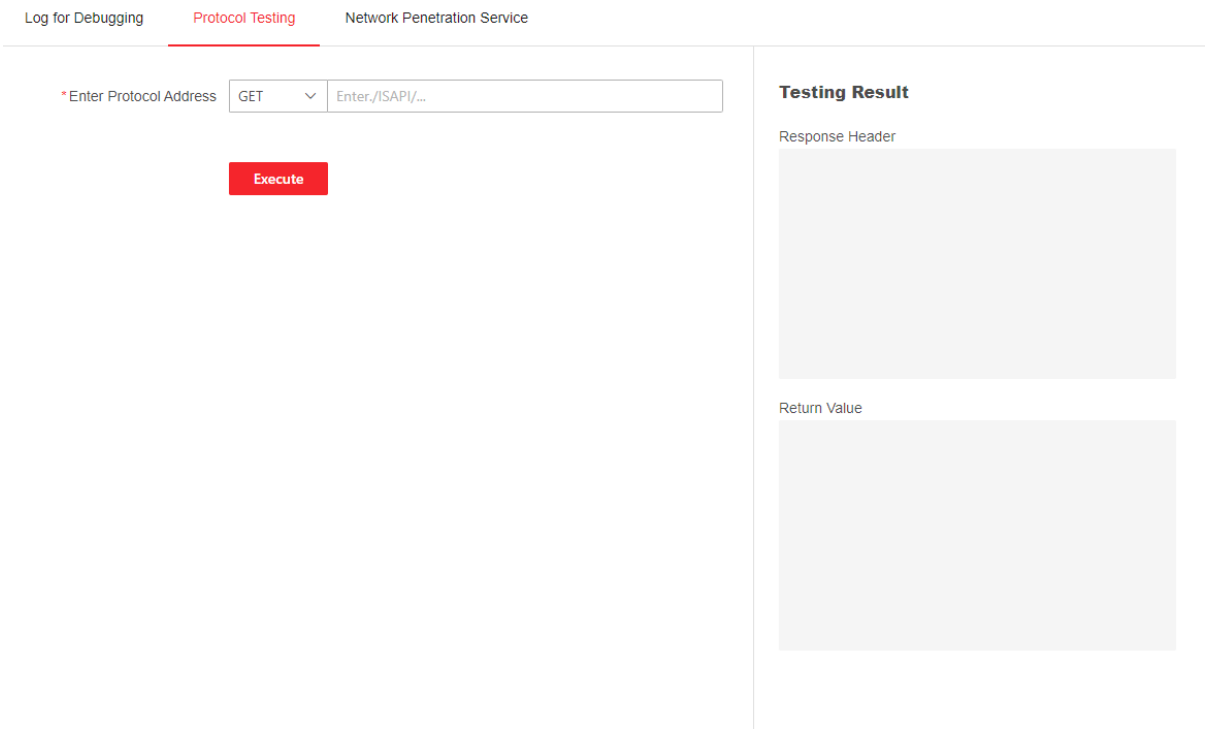


Figure 8-3 Protocol test

Select the protocol type, enter the protocol, and click *Execute* .

Perform protocol debugging based on the response header and return value.

Enable Developer Mode

After obtaining the license, you can enable developer mode, in which you can freely import third-party applications and perform adb debugging.

Click *System & Maintenance* → *maintain* → *Equipment debugging* → *Log debugging* , enter the configuration interface.

Obtain the license certificate and import it. Enable **developer mode** to enter developer mode for adb debugging.

View logs

Device logs can be searched and viewed.

Click *System and Maintenance* → *maintain* → *Log* , enter the configuration interface.

Select the main and sub-type of the log, select the start time and end time to be queried and exported, click *Search* , and the list will display the log information, including the sequence number, time, main type, sub-type, channel number, local / remote user, remote host address, parameters and information.

Advanced options configuration

Click *System and Maintenance* → *maintain* → *Advanced options* : Enter the administrator password to enter the configuration page.

Smart Parameters

Real person detection customization

After enabling, you can set **the real person detection security level** , **real person detection threshold** and **mask real person detection threshold** .

illustrate

The threshold can be set from 1 to 100. The smaller the threshold, the lower the accuracy and the higher the traffic efficiency. The larger the threshold, the higher the accuracy and the lower the traffic efficiency.

Attack Lock

When this function is enabled, the device will automatically lock after human detection fails. The lock time can be configured.

Lock Time

the attack lock function is enabled , the time it takes for the device to lock itself after a real person detection fails.

Version Information

You can view the device version information.

Certificate Management

Used to create and centrally manage all communication certificates, CA certificates, etc. of devices.

Creating a certificate request and installing the certificate

Used to import a certificate request generated by the device and signed by a trusted authority.

Prerequisites

A self-signed certificate has been created.

Procedure

1. Click *System and Maintenance → Safety → Certificate management* .
2. Click *Create Certificate Request* in the **HTTPS Certificate** or **SYSLOG Certificate module** .
3. Set the certificate request information.
4. Click *Save* .
   A pop-up window displays the certificate details. Swipe up or down to view the full text.
5. Copy the certificate details and save them in a local request file.
6. Send the request file to the certificate authority for signing.
7. Import the certificate sent back by the certification authority.
   1) In the **HTTPS Certificate** or **SYSLOG Certificate** module, select the key from the local computer and click *Import* .
   2) In the **HTTPS Certificate** or **SYSLOG Certificate** module, select the communication certificate (public key) from the local computer and click *Import* .

Install a third-party signed certificate

Used to import a signed certificate authenticated by a third-party organization.

Prerequisites

A third-party signed certificate has been obtained.

Procedure

1. Click *System and Maintenance → Safety → Certificate management* .
2. Upload the key certificate and communication certificate from the local computer in **the HTTPS certificate** or **SYSLOG certificate module.**
3. Click *Import* .

Install CA Certificate

certificates issued by an authoritative certificate authority (CA) (generally authoritative CA organizations require fees) to improve the security level of access.

Prerequisites

CA certificate has been obtained .

Procedure

1. Click *System and Maintenance → Safety → Certificate management* .
2. Customize and create CA certificate ID in **CA certificate import** in **SYSLOG certificate** module .
3. Upload the CA certificate from your local computer and click *Import* .

A. Legal Notice

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (*https://www.hikvision.com*). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS

IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

B. Symbol Conventions

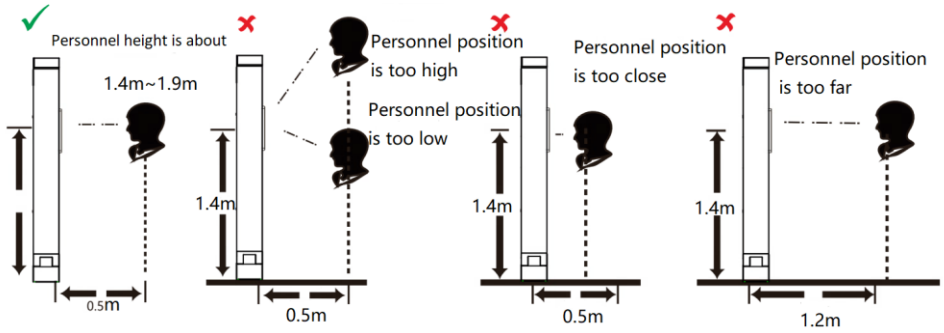
The symbols that appear in this document are described as follows.

Symbol	illustrate
 illustrate	Explanatory text is used to supplement and explain the main text.
 Notice	Caution texts are used to remind users of important operations or to prevent potential dangers of injury and property loss. If not avoided, it may cause injury accidents, equipment damage or business interruption.
 Danger	Dangerous words indicate a high potential risk which, if not avoided, could result in serious danger of loss of life.

C. Face Recognition Notes

Face entry / matching position

The face entry / matching position is shown in the following figure (taking the standing distance of 0.5 m as an example):



Face Entry / Position Comparison

Facial expressions

To ensure the quality of facial parameter entry and comparison accuracy, please be sure to maintain a natural expression during the entry / comparison process (as shown in the figure below).

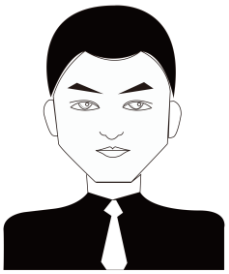


Figure C-1 Natural facial expressions

Face pose

To ensure the quality of facial parameter entry and comparison accuracy, please make sure that the face is facing the entry window during the entry / comparison process .
the face entry / comparison posture:

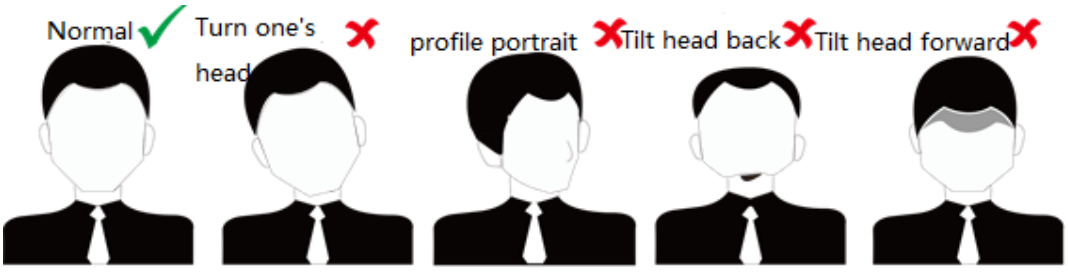


Figure C-2 Diagram of face input / comparison posture

Face resizing

During the registration process, please try to keep your face in the center of the window.
The schematic diagram of face resizing is as follows:

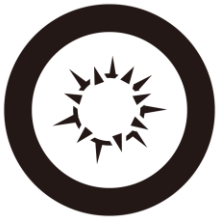
Figure C-3 Schematic diagram of face resizing

D. Installation Environment Notes

1. Installation environment light source reference value:

Candle: 10 Lux

Bulb: 100 ~ 850 Lux



Daylight: greater than 1200 Lux

2. Please install the device indoors.
3. Avoid backlight, direct sunlight, direct sunlight through windows, oblique sunlight through windows, and close-range lighting.
4. It is recommended to keep at least 1 m away from the window .
5. Avoid installing the equipment in humid areas, such as basements.

E. Smart cabinet dimensions

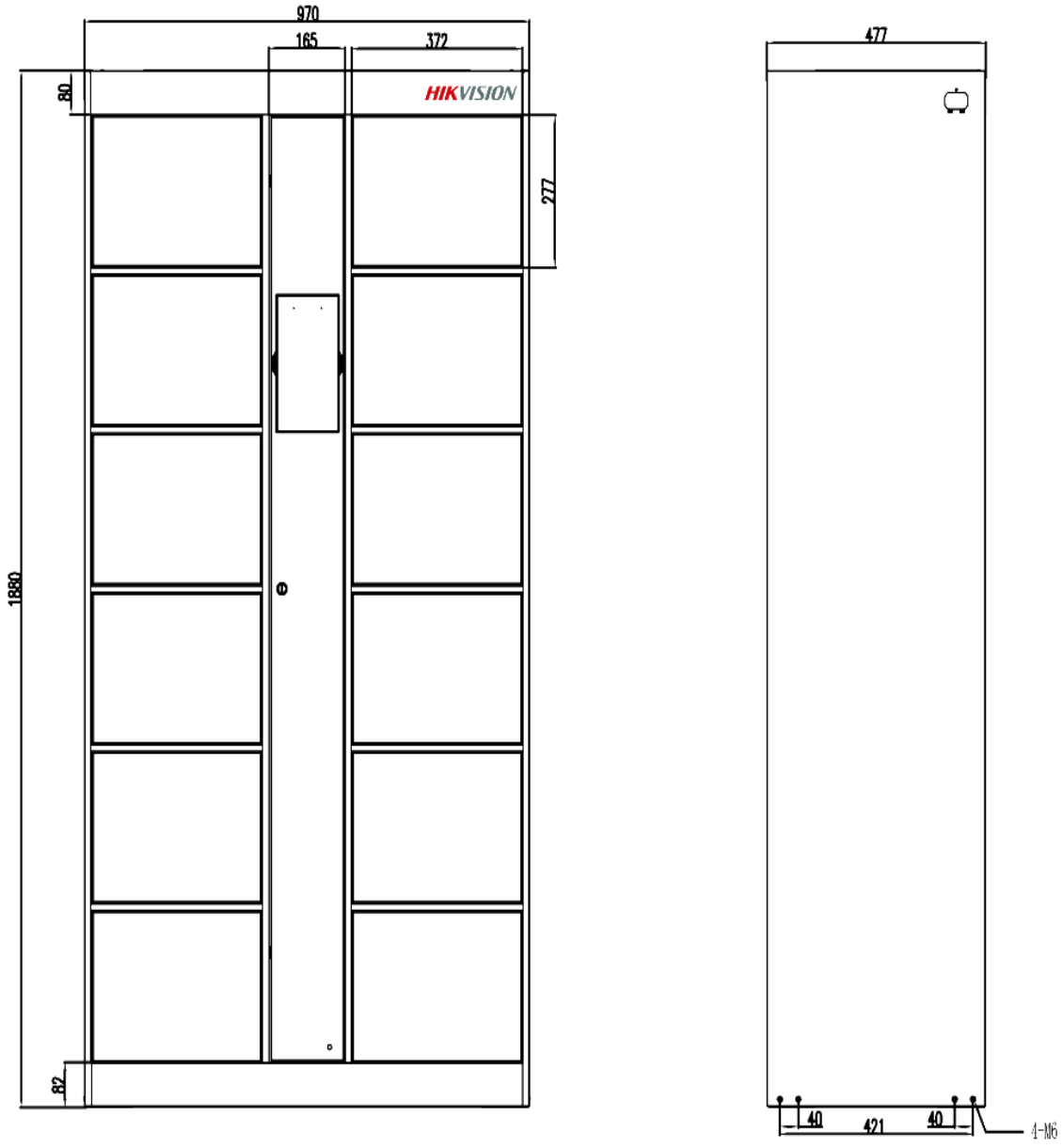


Figure E-1 Main cabinet

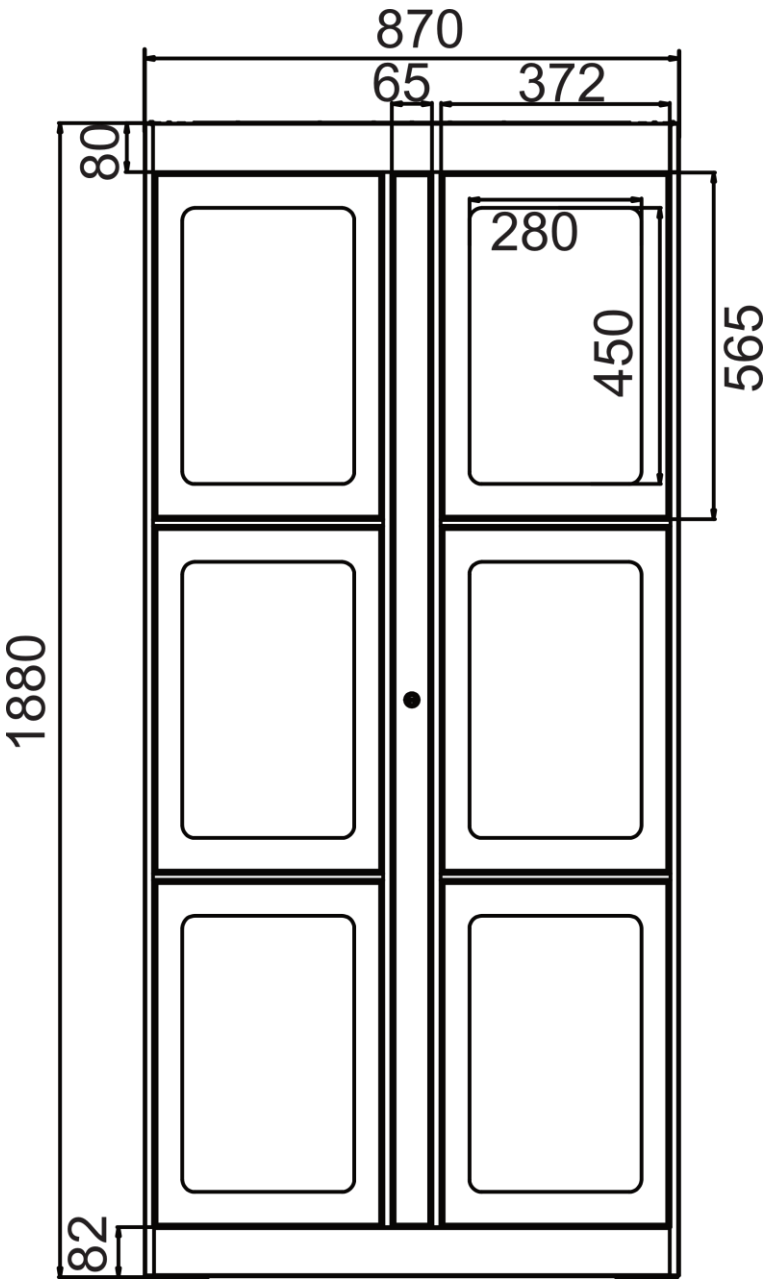


Figure E-2 Auxiliary cabinet （ 6 compartments）

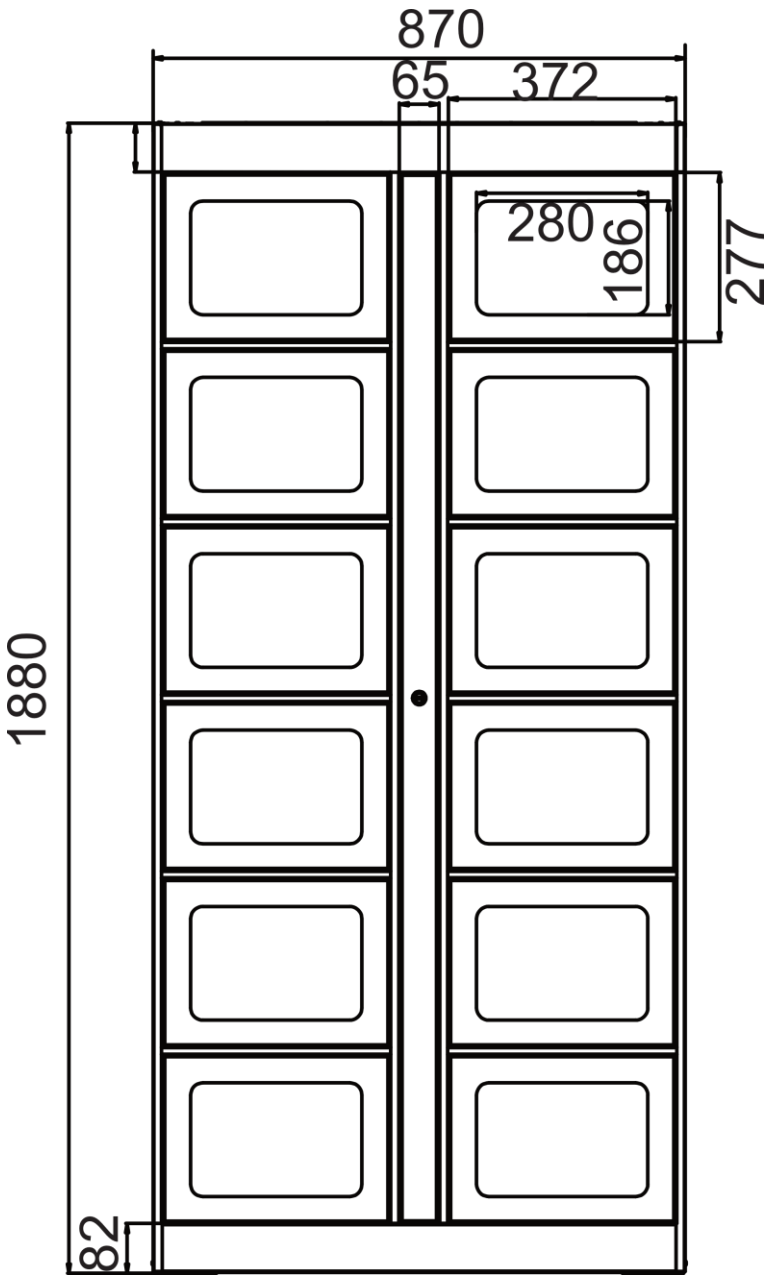


Figure E-3 Auxiliary cabinet （ 12 compartments 1 ）

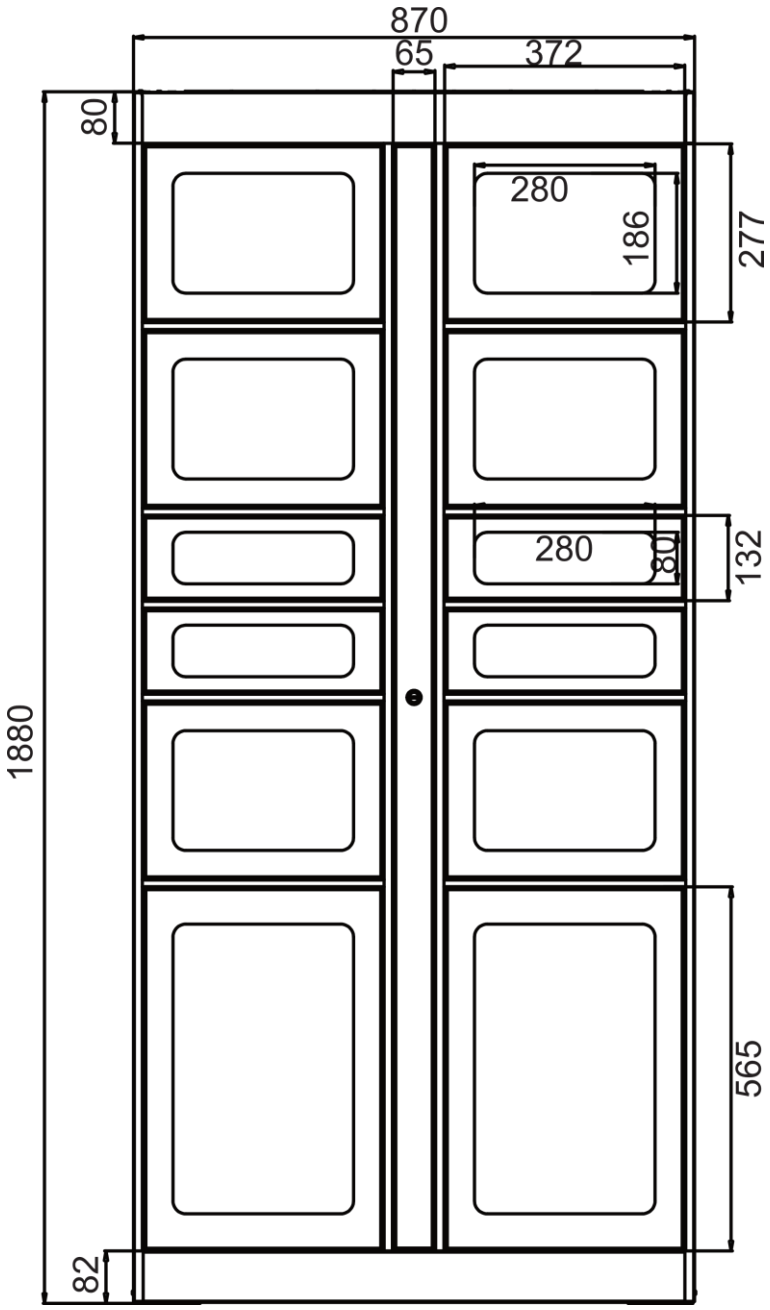


Figure E-4 Sub-cabinet (12 compartments 2)

Unit: mm .

见远 行更远

See Far, Go Further

杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.

总部：杭州市滨江区阡陌路555号（310051）
服务热线：400-800-5998（7×24小时）
www.hikvision.com

UD38703B-A