



Video Intercom Villa Door Station

User Manual

Legal Information

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.

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.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction



Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

Video Intercom Villa Door Station User Manual

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Input voltage should meet both the SELV and the Limited Power Source according to 60950-1 standard.
- The power supply must conform to LPS. The recommended adaptor models and manufacturers are shown as below. Use the attached adapter, and do not change the adaptor randomly.

Model	Manufacturer	Standard
ADS-24S-12 1224GPCN	SHENZHEN HONOR ELECTRONIC CO.,LTD	CEE
G0549-240-050	SHENZHEN GOSPELL DIGITAL TECHNOLOGY CO.,LTD	CEE
TS-A018-120015Ec	SHENZHEN TRANSIN TECHNOLOGIES CO., LTD	CEE

Battery:

Do not ingest battery. Chemical burn hazard! This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death. Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

CAUTION: Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example,in the case of some lithium battery types). Do not dispose of the battery into fire or a hot oven,or mechanically crush or cut the battery,which may result in an explosion. Do not leave the battery in an extremely high temperature surrounding environment,which may result in an explosion or the leakage of flammable liquid or gas. Do not subject the battery to extremely low air pressure,which may result in an explosion or the leakage of flammable liquid or gas.+ identifies the positive terminal(s) of equipment which is used with, or generates direct current.- identifies the negative terminal(s) of equipment which is used with, or generates direct current.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope

rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

About this Manual

Get the manual and related software from or the official website (<http://www.hikvision.com>).

Product	Model
Villa Door Station	DS-KV8114 Series

Contents

Chapter 1 Appearance	1
Chapter 2 Terminal and Wiring Description	7
2.1 Terminal Description	7
2.2 Wiring Description	8
2.2.1 Door Lock Wiring	9
2.2.2 Alarm Input Device Wiring	10
Chapter 3 Installation	11
3.1 Accessory Introduction	11
3.2 Surface Mounting	15
3.3 Mounting with Gang Box	16
3.4 How to Install Rain Shield for Surface Mounting	19
3.5 How to Install Rain Shield for Flush Mounting	21
3.6 Nametag Paper Replacement Steps	23
3.7 How to Install Bracket without Rainshield	24
3.8 How to Install Bracket with Rainshield	27
Chapter 4 Activation	32
4.1 Activate via SADP	32
4.2 Activate via Web Browser	33
4.3 Activate Device via Client Software	33
4.4 Edit Network Parameters	34
Chapter 5 Quick Operation via Web Browser	35
5.1 Select Language	35
5.2 Time Settings	35
5.3 Privacy Settings	35
5.4 Administrator Settings	36
5.5 No. and System Network	36

Chapter 6 Operation via PC Web	38
6.1 Login Web Browser	38
6.2 Forget Password	38
6.3 Overview	38
6.4 Person Management	40
6.5 Device Management	43
6.6 Maintenance and Security	45
6.6.1 Set Protocol Testing	45
6.6.2 Set Network Diagnosis	45
6.6.3 Upgrade and Maintenance	45
6.6.4 Device Debugging	47
6.6.5 View Log via PC Web	48
6.6.6 Advanced Settings	48
6.6.7 Security Mode Settings	51
6.6.8 Certificate Management	52
6.7 Preference	53
6.8 Configuration	54
6.8.1 System Settings	54
6.8.2 User Management	56
6.8.3 Network Settings	58
6.8.4 TF Card Management	65
6.8.5 View Device Arming/Disarming Information	65
6.8.6 Set Video and Audio Parameters	65
6.8.7 Adjust Display Settings	67
6.8.8 Event Settings	70
6.8.9 Perimeter Protection	73
6.8.10 Event Linkage	81
6.8.11 Access Control Settings	82

6.8.12 Video Intercom Settings	94
Chapter 7 Configuration via Client Software	102
7.1 Device Management	102
7.1.1 Add Online Device	102
7.1.2 Add Device by IP Address	104
7.1.3 Add Device by IP Segment	104
7.2 Live View via Door Station	104
7.3 Organization Management	104
7.3.1 Add Organization	104
7.3.2 Modify and Delete Organization	105
7.4 Person Management	105
7.4.1 Add Person	105
7.4.2 Modify and Delete Person	106
7.4.3 Change Person to Other Organization	106
7.4.4 Import and Export Person Information	107
7.4.5 Get Person Information from Device	107
7.4.6 Issue Card in Batch	108
7.5 Video Intercom Settings	110
7.5.1 Receive Call from Door Station	111
7.5.2 Release Notice	111
7.5.3 Search Video Intercom Information	112
7.5.4 Upload Armed Information	114
Chapter 8 Video Intercom Operation	115
8.1 Call Resident	115
8.2 Unlock Door	115

Chapter 1 Appearance

Different models may have different ports, please refer to the specific device.

1 Lens with Nametag

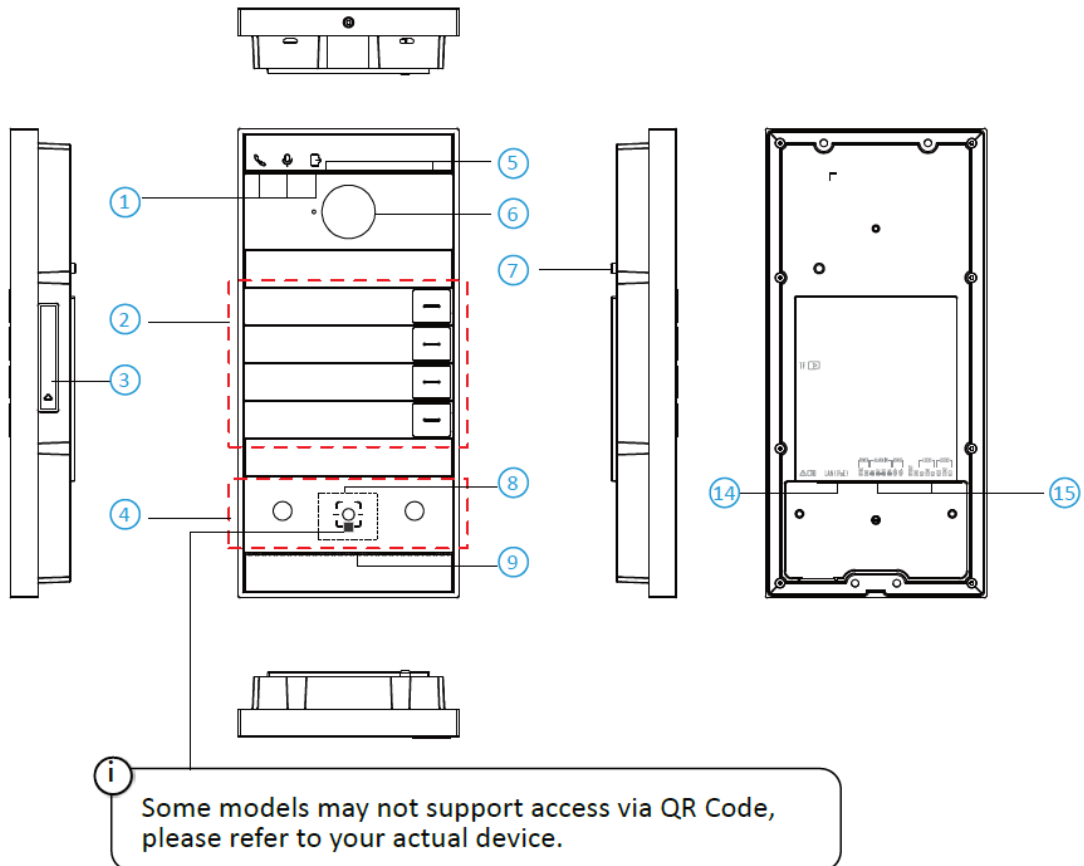


Figure 1-1 1 Lens with Nametag Appearance

1 Lens with Keypad

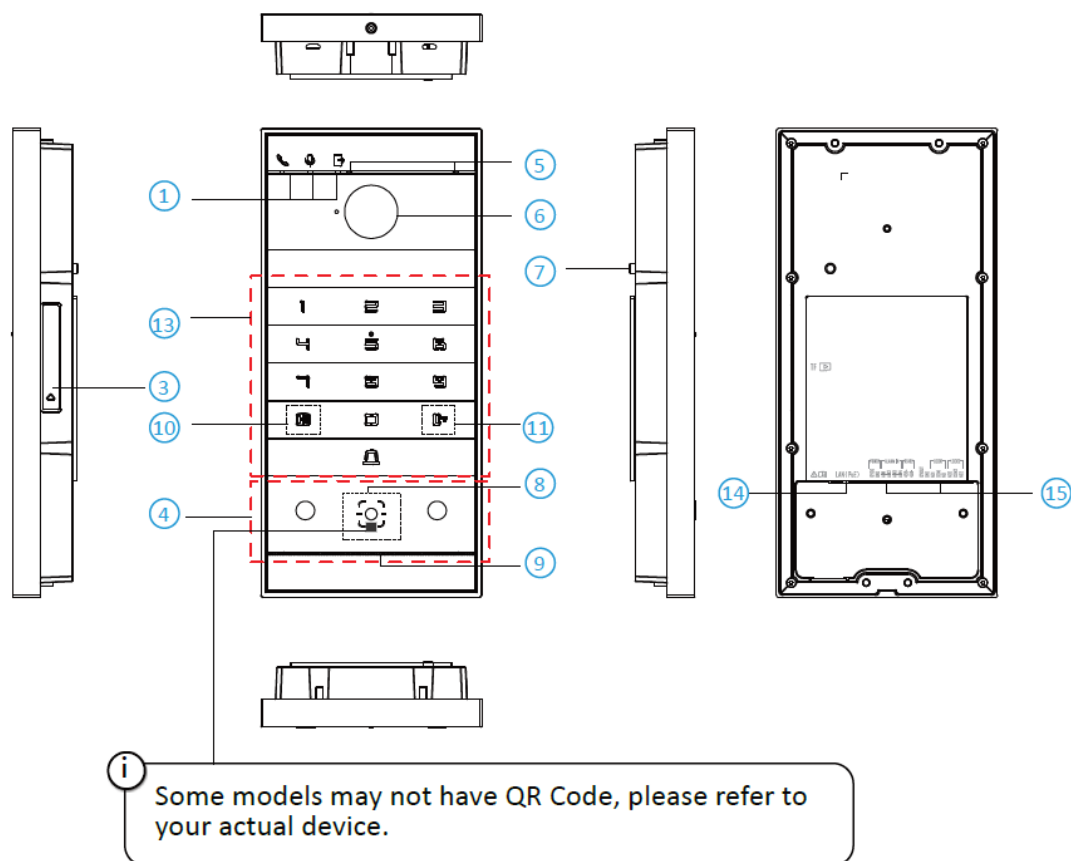


Figure 1-2 1 Lens with Keypad Appearance

3 Lenses with Nametag

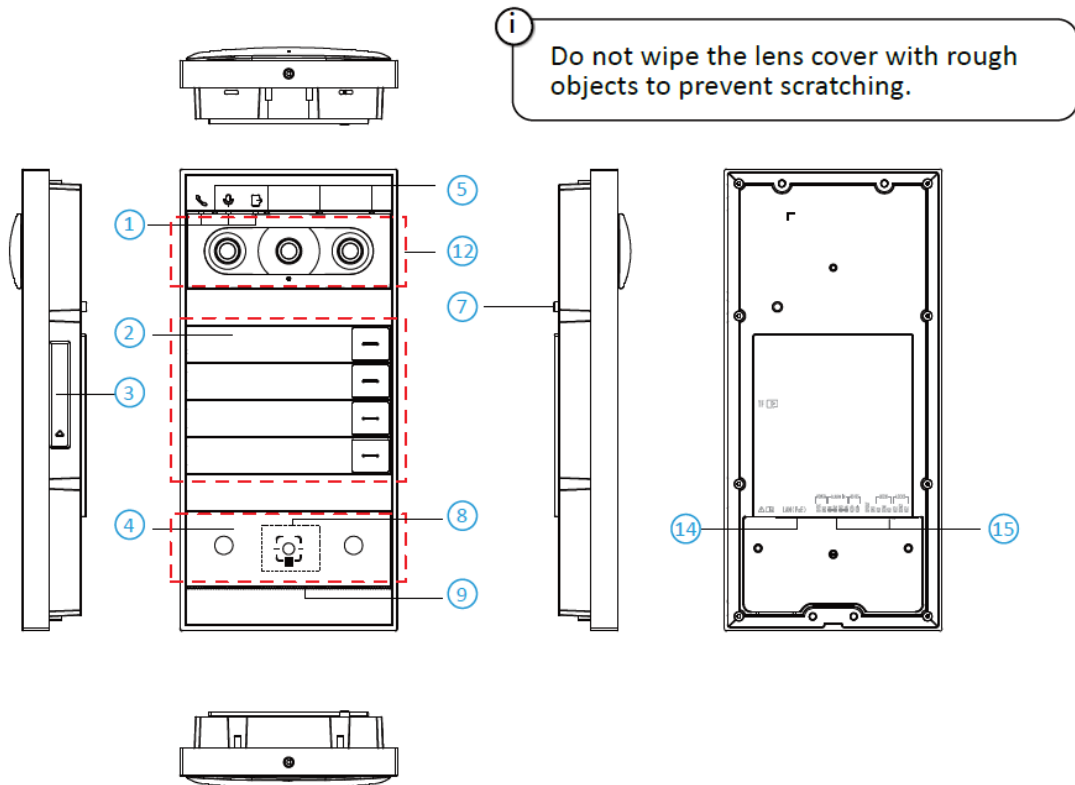


Figure 1-3 3 Lenses with Nametag Appearance

3 Lenses with Keypad

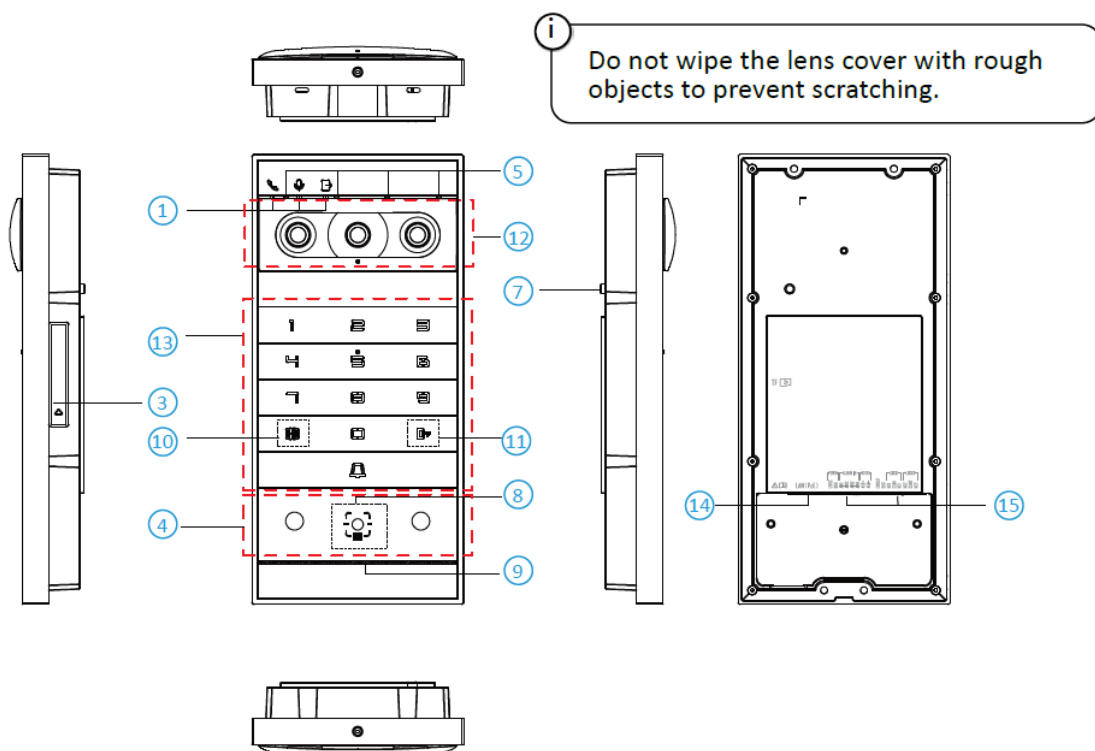


Figure 1-4 3 Lenses with Keypad Appearance

Table 1-1 Description

No.	Description
1	Indicators Call (Orange)/ Communicate (White)/ Unlock (Green)
2	Nametag Module
3	TF Card Slot
4	Card Reading Area
5	Microphones
6	1 Lens
7	Tamper

No.	Description
8	QR Code Module
9	Speaker
10	Lock 2
11	Lock 1
12	3 Lenses
13	Keypad Module
14	Network Interface
15	Terminals

Below the keypad panel and speaker, there are ambient lights.

Table 1-2 Light Description For 3 Lenses Models

Status	Light
Standby	Default: Breathing White You can change it to solid white/ disable.
Successful-Auth.	Default: Flash Green You can change it to flowing white/ disable.
Failed Auth.	Default: Flash Red You can change it to disable.
Calling	Default: Flowing White
Intercom	Default: Solid White
AP Mode	Orange light blinks for 10s. (Fast blinking when on, slow blinking when off.)

Table 1-3 Light Description For 1 Lens Models

Status	Light
Standby	Default: Breathing White You can change it to solid white/ disable.
Successful-Auth.	Default: Flash Green You can change it to flash white/ disable.
Failed Auth.	Default: Flash Red

Status	Light
	You can change it to disable.
Calling	Default: Flash White
Intercom	Default: Solid White
AP Mode	Orange light blinks for 10s. (Fast blinking when on, slow blinking when off.)

You can configure decoration light on web. For details, please go to **3.7 Preference**.

Chapter 2 Terminal and Wiring Description

2.1 Terminal Description

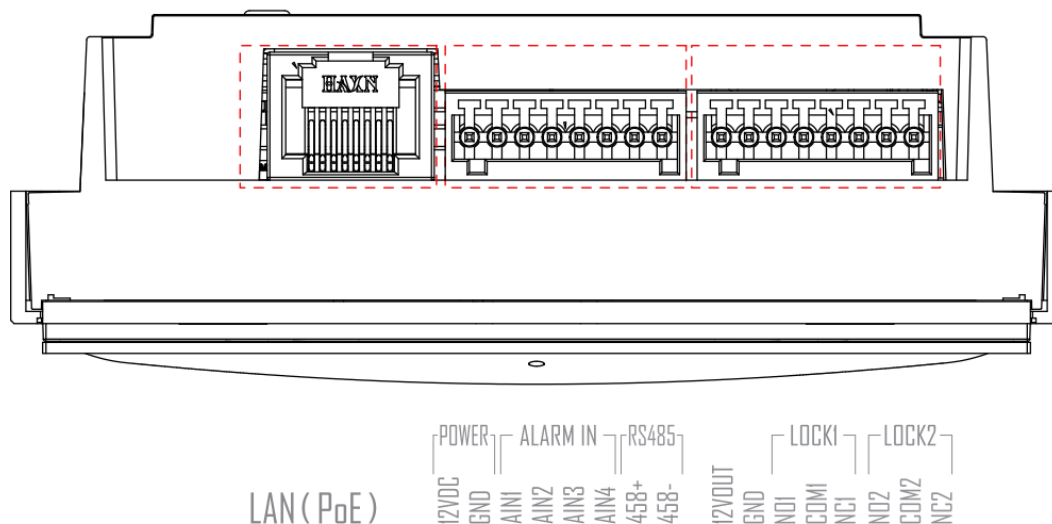


Figure 2-1 Terminal Description

Table 2-1 Description of Terminal and Interfaces

Name	Interface	Description
Lock 1	NO1	Door Lock Relay Output 1 (NO)
	COM1	Common Interface
	NC1	Door Lock Relay Output 1 (NO)
Lock 2	NO2	Door Lock Relay Output 2 (NO)
	COM2	Common Interface
	NC2	Door Lock Relay Output 2 (NC)
	12VOUT	12 V Output
	GND	Grounding
ALARM IN	AI1	Alarm Input 1 (For the access of Door Contact)
	AI2	Alarm Input 2 (For the access of Door Contact)

Name	Interface	Description
		 Note Before accessing to the Door Contact, select Input as Door Status in I/O Settings page first.
	AI3	Alarm Input 3 (For the access of Exit Button)
	AI4	Alarm Input 4 (For the access of Exit Button)  Note Before accessing to the Exit Button, select Input as Exit Button in I/O Settings page first.
RS-485	485+	RS-485 Communication Interface
	485-	
Power Input	12 VDC	12 VDC Input
	GND	
Network	LAN(PoE)	Standard PoE Power Supply

2.2 Wiring Description

Follow the instructions below to see how to connect the alarm input devices and door locks.

Note

- Do not wire the device to the 220V electric supply directly.
- The device supports 12V DC, 1.5A power supply or standard PoE power supply. After connecting to standard PoE cable, there is no need to connect other power cord. If the cable connected is not standard PoE cable, you need to connect power cord to the device for power supply.

Note

- If the cable size is 14 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 50 m.
- If the cable size is 16 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 30 m.
- If the cable size is 18 AWG, you should use a 12 V switched-mode power supply. And the distance between the power supply and the device should be no more than 20 m.

2.2.1 Door Lock Wiring

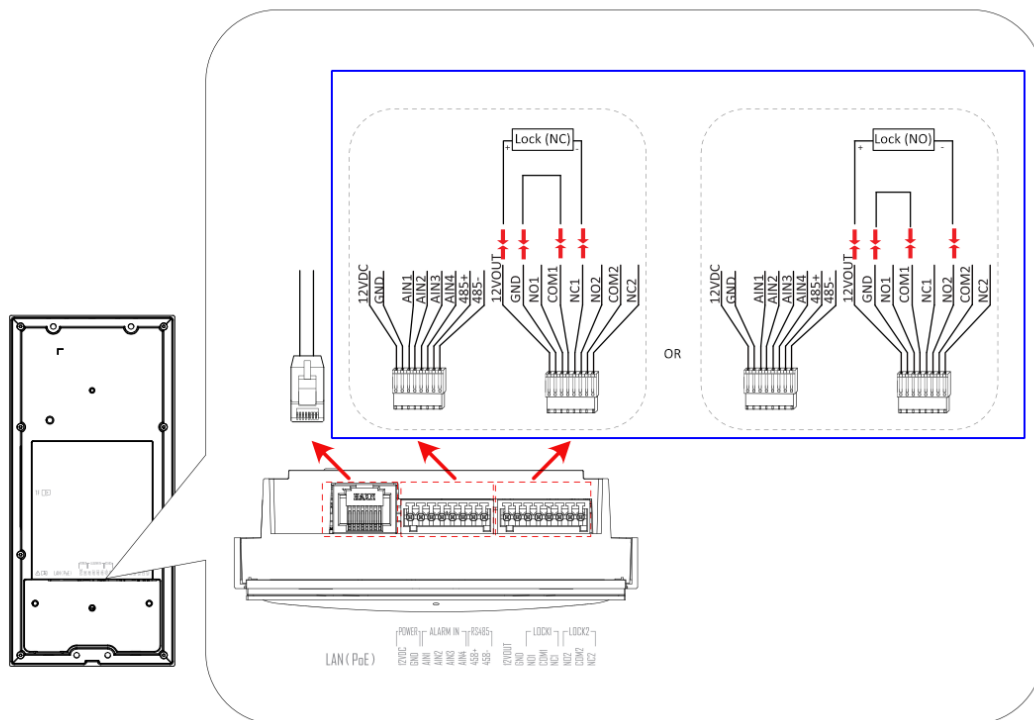


Figure 2-2 Door Lock Wiring

Note

- Terminal NC1/COM1 is set as default for accessing magnetic lock/electric bolt; terminal NO1/COM1 is set as default for accessing electric strike.
- To connect electric lock in terminal NO2/COM2/NC2, it is required to set the output of terminal NO2/COM2/NC2 to be electric lock with iVMS-4200 client software.

2.2.2 Alarm Input Device Wiring

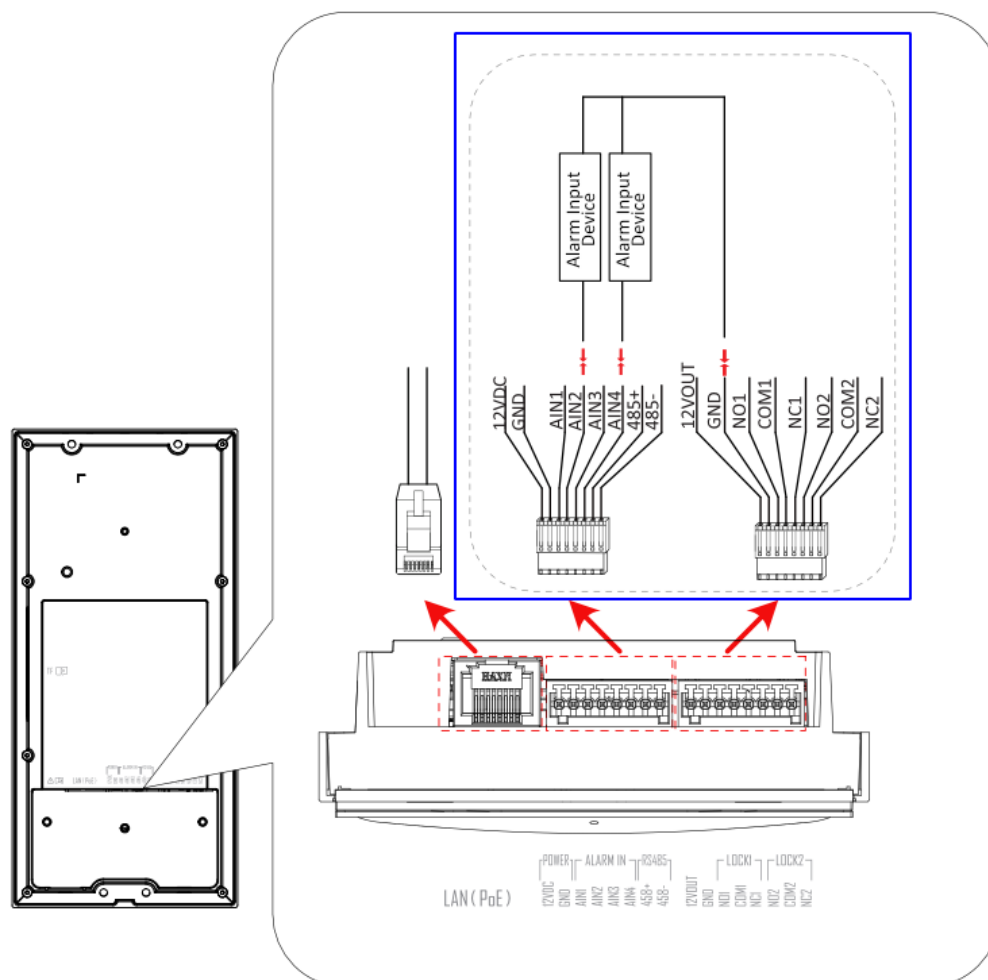


Figure 2-3 Alarm Input Device Wiring

Chapter 3 Installation

Note

- Make sure the device in the package is in good condition and all the assembly parts are included.
- Make sure your power supply matches your door station.
- Make sure all the related equipment is power-off during the installation.
- Check the product specification for the installation environment.

3.1 Accessory Introduction

The installation accessories are shown below. (Unit: mm)

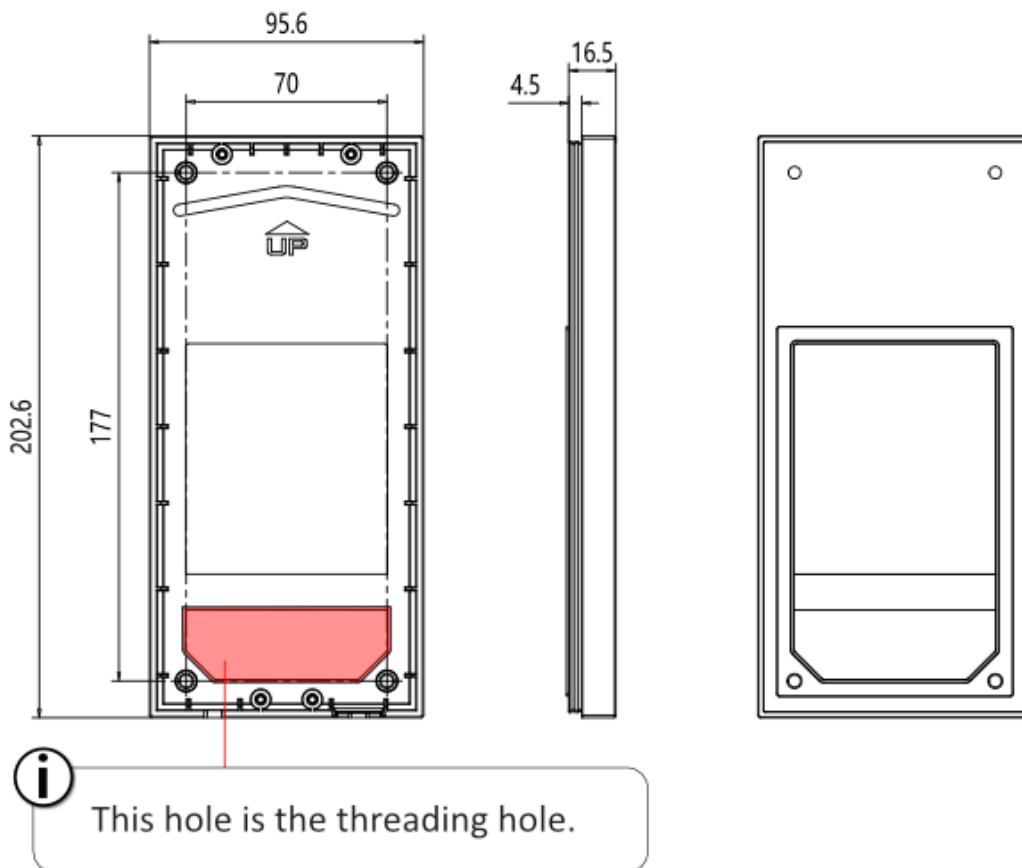


Figure 3-1 Mounting Plate

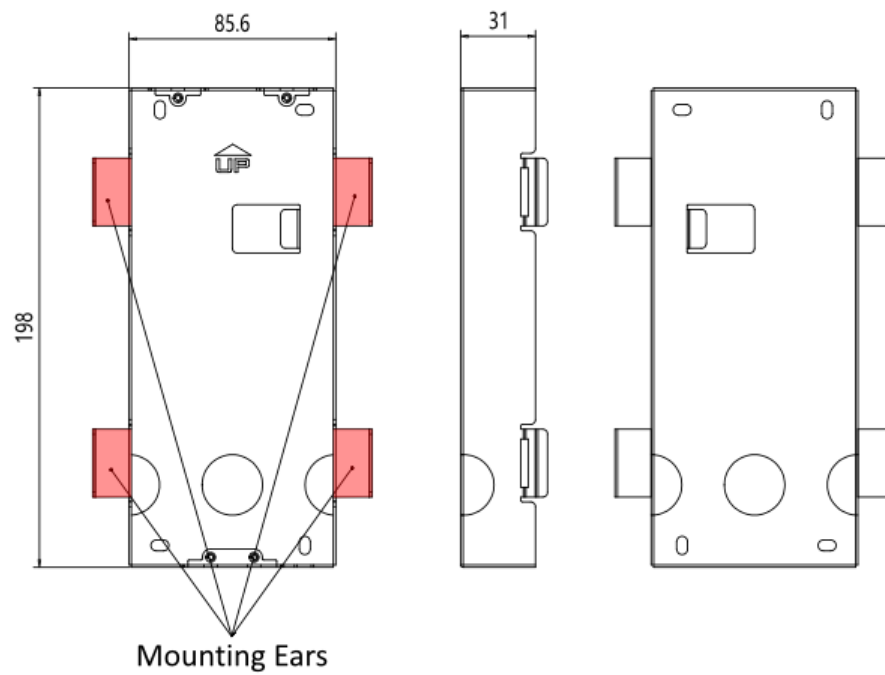


Figure 3-2 Flush-Mounting Gang Box

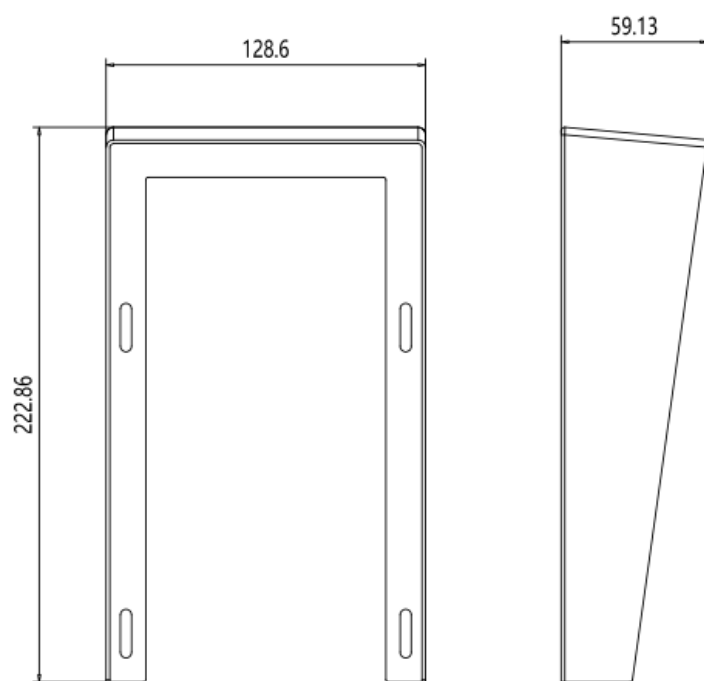


Figure 3-3 Surface-Mounting Rain Shield

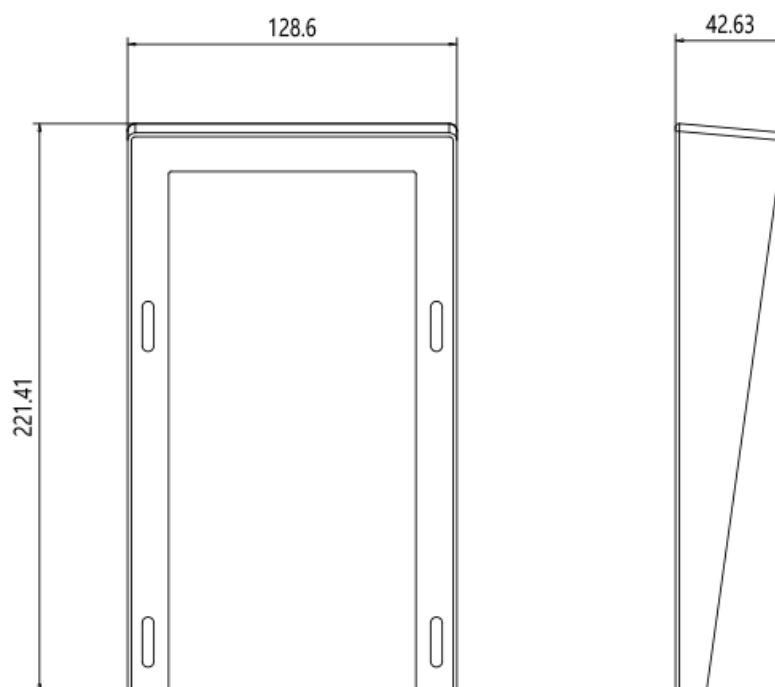


Figure 3-4 Flush-Mounting Rain Shield

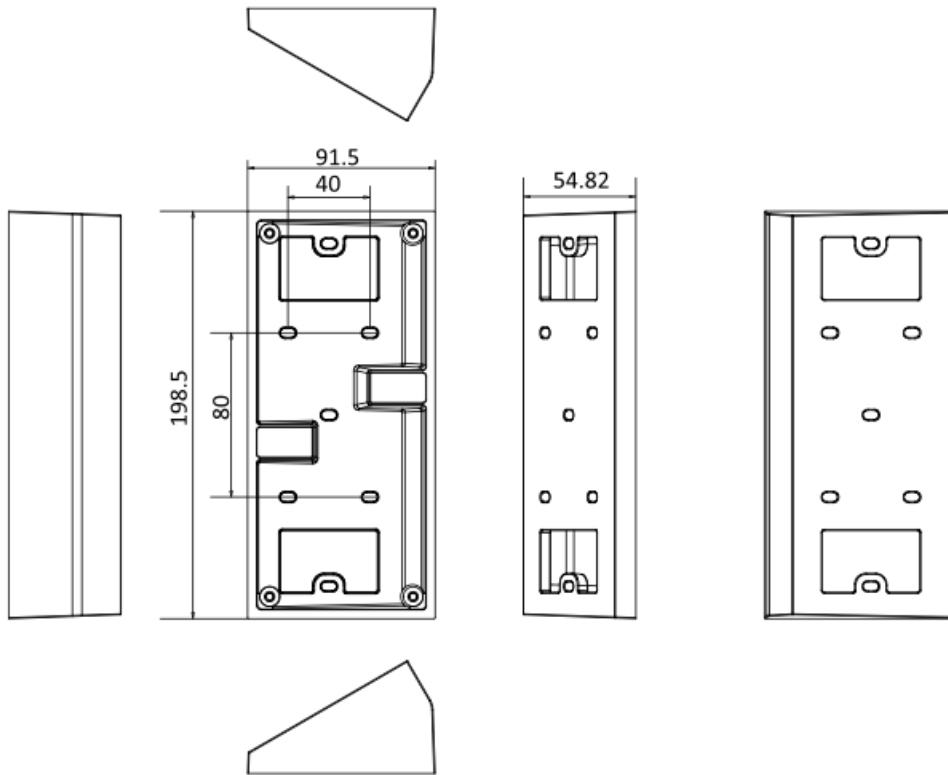


Figure 3-5 Diagonal Mounting Bracket

3.2 Surface Mounting

The mounting methods and procedures are basically the same for the models above. Here uses one as an example.

Steps

1. Attach the installation template to the wall, drill screw holes according to the template, then remove the installation template.

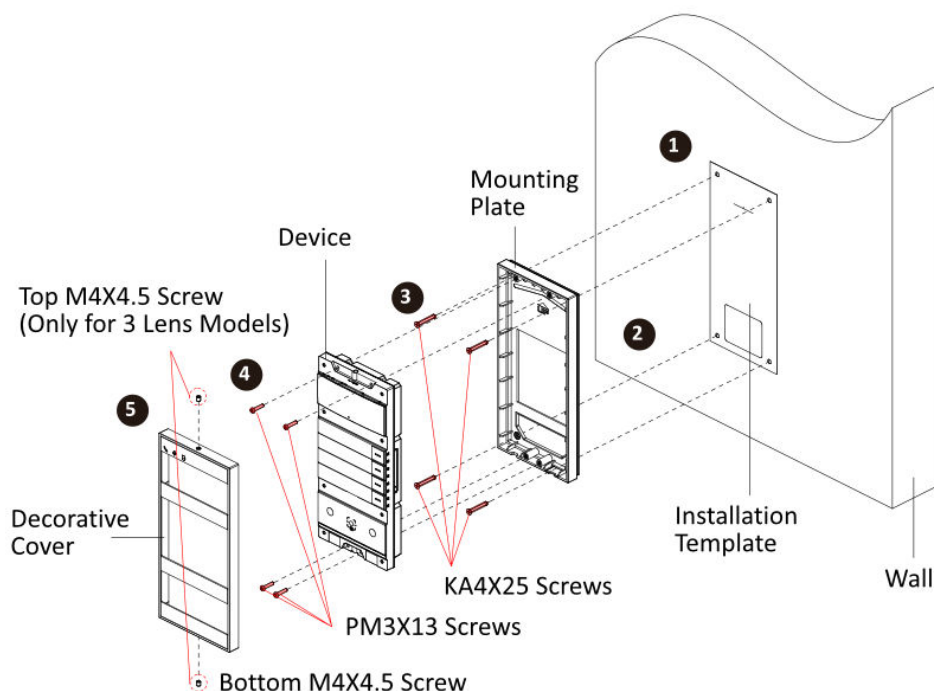


Figure 3-6 Surface Mounting

2. Insert expansion bolts into the holes then secure the mounting plate to the wall using 4 PCS KA4X25 screws.
3. After completing wiring, fix the device to the mounting plate using 4 PCS PM3X13 screws.
4. Assemble the decorative cover onto the device.
5. First, tighten the top M4X4.5 screw until it is flush with the cover, then tighten the bottom M4X4.5 screw to the appropriate position.



Note

- To ensure waterproof performance, it is recommended to apply silicone sealant to the top and both sides of the mounting plate.
- For device with one lens, the installation procedures are the same, except in step 5, you only need to tighten the bottom M4X4.5 screw to appropriate position to fix the decorative cover.

3.3 Mounting with Gang Box

Before You Start

- You should know the recommended installation hole size is 87.6 mm(W) × 200 mm(H) × 30.5 mm(D).

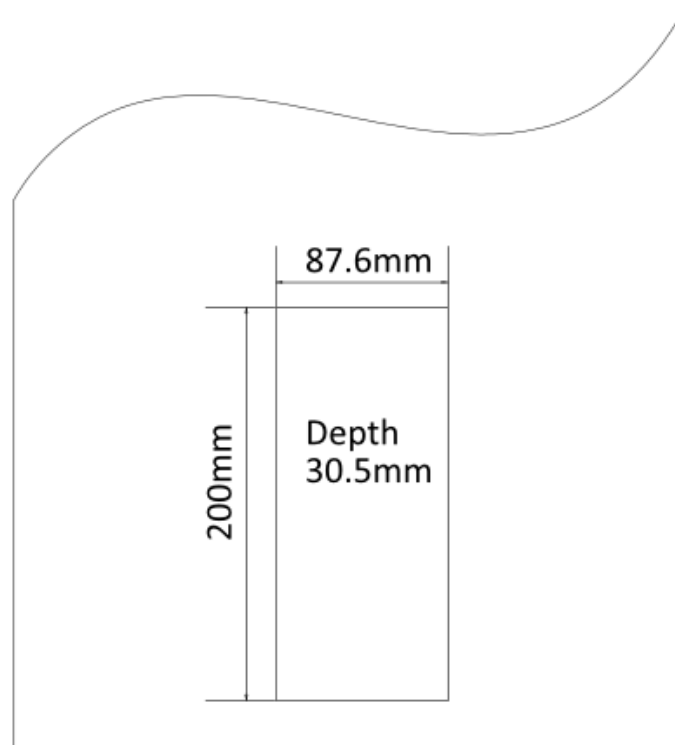


Figure 3-7 Recommended Installation Hole Size

- Before installing the device, you need to bury the gang box into the wall and break off the mounting ears.

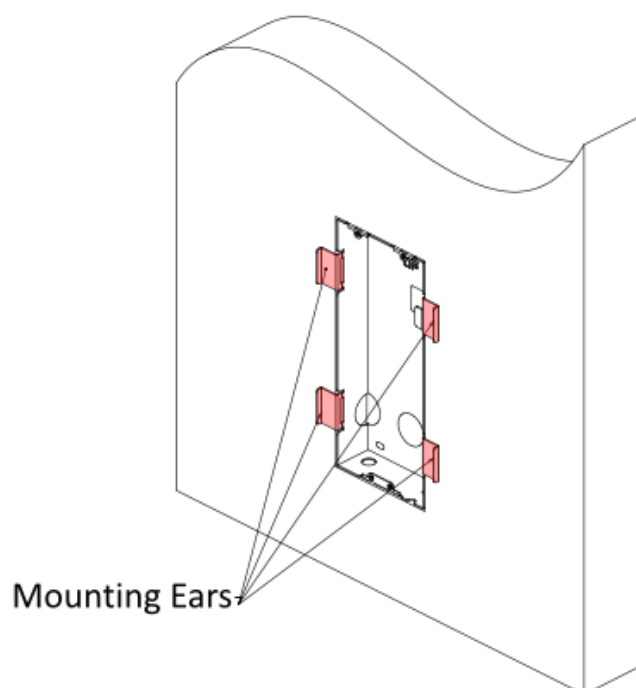


Figure 3-8 Break Off the Mounting Ears

Steps

1. Drill a 200mm × 87.6mm × 30.5mm hole in the wall. Pull the cables through the hole on the wall and place them into the gang box. Use a marker to mark the positions according to the holes on the gang box.

Note

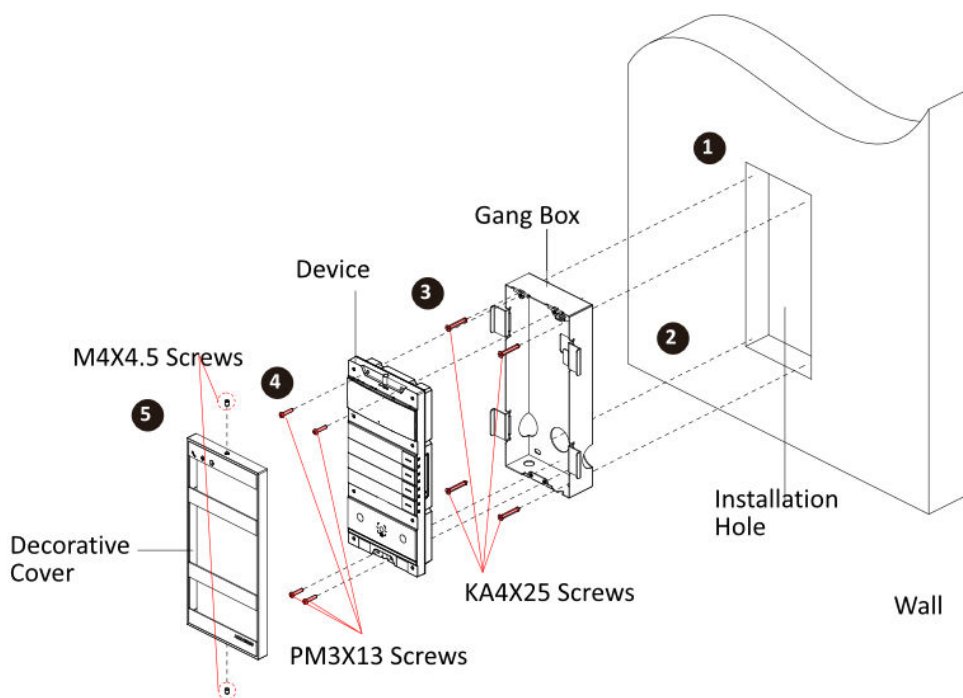


Figure 3-9 Mounting with Gang Box

2. Remove the gang box and drill holes at the marked positions using a drill. Insert expansion bolts into the holes. Place the gang box back into the wall and secure it with 4PCS KA4X25 screws. Fill the gaps between the gang box and the holes with concrete, and break off all mounting ears.
3. After wiring is completed, fix the device to the gang box using 4PCS PM3X13 screws.
4. Assemble the decorative cover onto the device.
5. First, tighten the top M4X4.5 screw until it is flush with the cover, then tighten the bottom M4X4.5 screw to the appropriate position.

3.4 How to Install Rain Shield for Surface Mounting

Follow the instructions below to install rain shield for surface mounting.

Before You Start

- Read the surface mounting steps shown at Quick Start Guide.
- Get the installation equipments including a drill bit, a marker, a screwdriver and so on.
- Check whether the device, rain shield and other spare parts are complete.

Steps

1. Install the door station into the wall following surface mounting steps shown at Quick Start Guide.

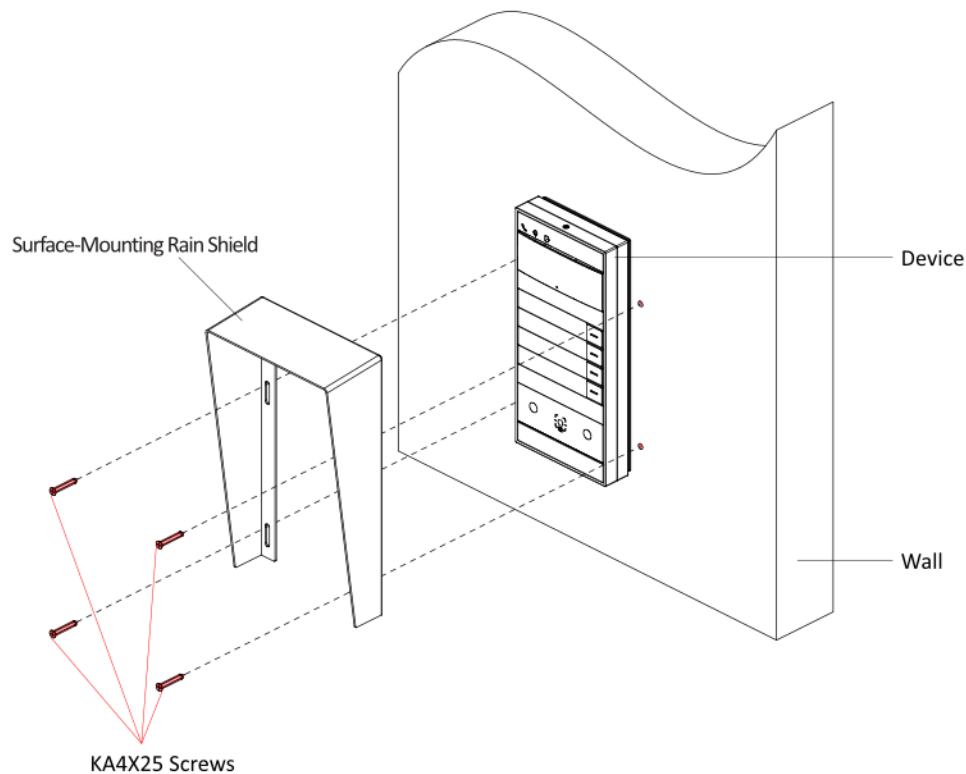


Figure 3-10 How to Install Rain Shield for Surface Mounting

2. Align the inner wall of the rain shield with the top of the device, pressing it flush against the wall. Mark the mounting hole positions of the rain shield with a marker.
3. Remove the rain shield, drill holes using a drill bit, and insert expansion bolts into the holes. Secure the rain shield to the wall using 4 pcs of KA4X25 screws. If necessary, remove the device before drilling.
4. Adjust the rain shield upward according to the required field of view, setting it to the appropriate installation height.

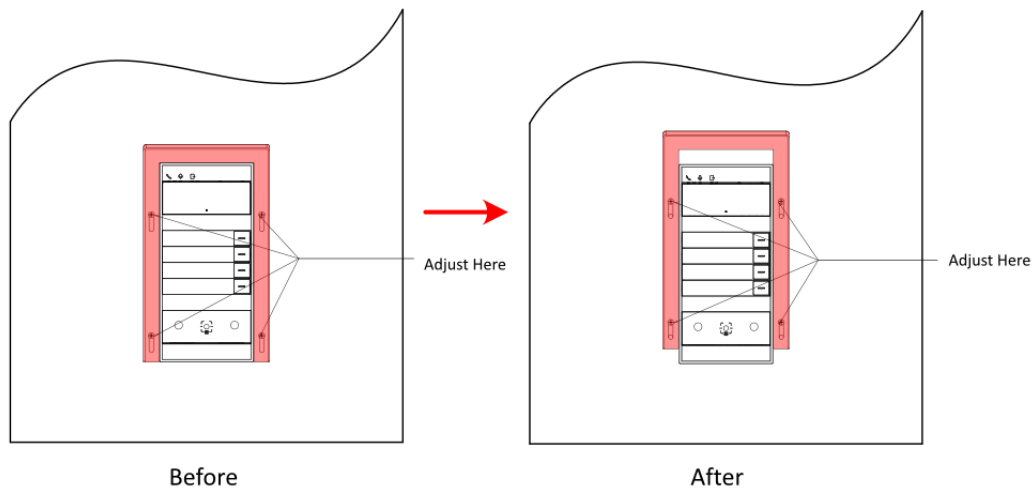


Figure 3-11 How to Adjust Rain Shield Upward

What to do next

To ensure waterproof effectiveness, it is recommended to apply silicone sealant to the top and sides of the rain shield.

3.5 How to Intall Rain Shield for Flush Mounting

Follow the instructions below to install rain shield for flush mounting.

Before You Start

- Read the flush mounting steps shown at Quick Start Guide.
- Get the installation equipments including a drill bit, a marker, a screwdriver and so on.
- Check whether the device, rain shield and other spare parts are complete.

Steps

1. Install the door station into the wall following flush mounting steps shown at Quick Start Guide.

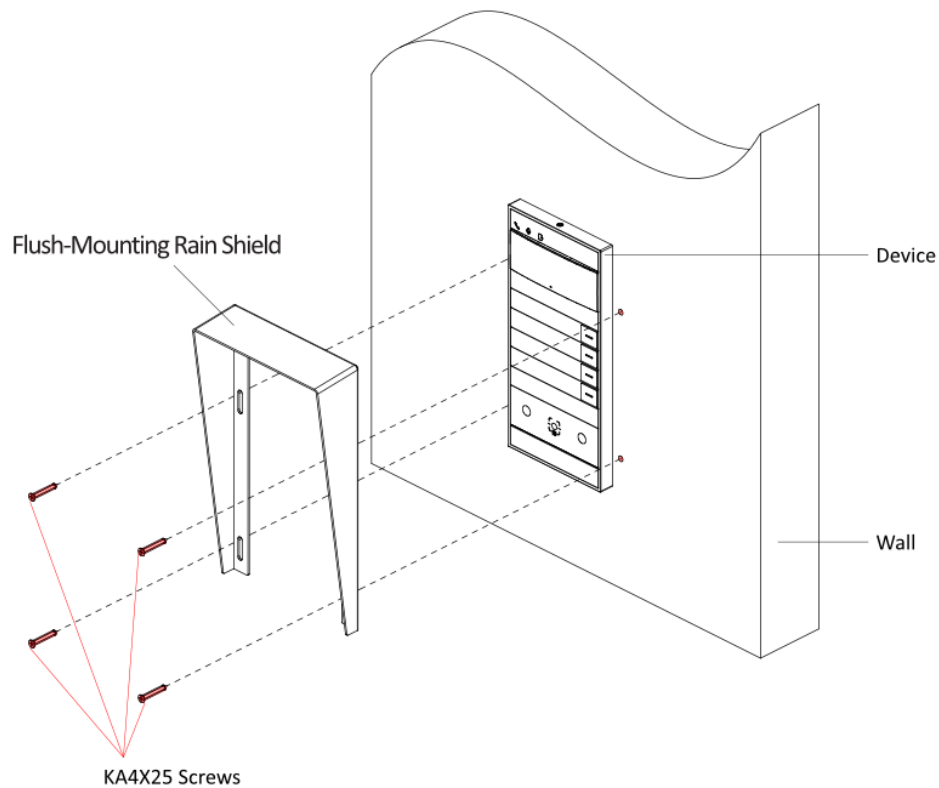


Figure 3-12 How to Install Rain Shield for Flush Mounting

2. Align the inner wall of the rain shield with the top of the device, pressing it flush against the wall. Mark the mounting hole positions of the rain shield with a marker.
3. Remove the rain shield, drill holes using a drill bit, and insert expansion bolts into the holes. Secure the rain shield to the wall using 4 pcs of KA4X25 screws. If necessary, remove the device before drilling.
4. Adjust the rain shield upward according to the required field of view, setting it to the appropriate installation height.

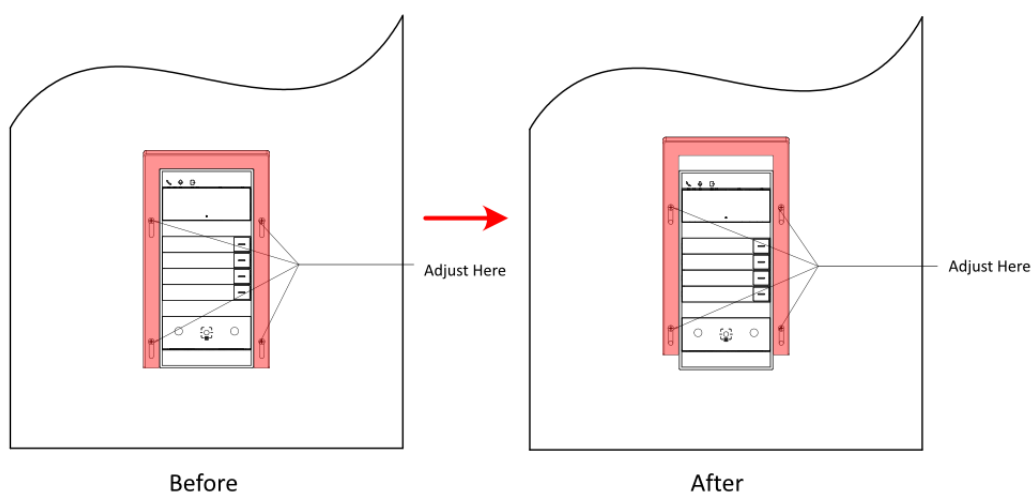


Figure 3-13 How to Adjust Rain Shield Upward

What to do next

To ensure waterproof effectiveness, it is recommended to apply silicone sealant to the top and sides of the rain shield.

3.6 Nametag Paper Replacement Steps

If you want to change nametag paper, just follow the steps below.

Before You Start

- Read **Nametag Key Replacement** first
- Know the recommended nametag paper dimensions are 350 mm × 54 mm.



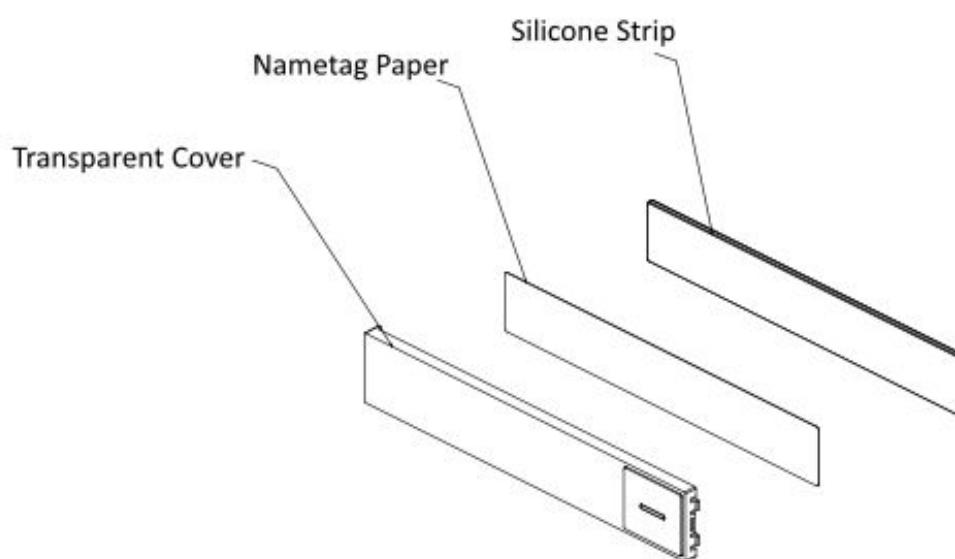
Recommended Nametag Paper Dimensions (mm)

Figure 3-14 Recommended Nametag Paper Dimensions

Steps

1. Print and cut the nametag paper according to the illustrated dimensions above.
2. Remove the nametag keys according to nametag keys' disassembly method.

3. Align the numbered side of the cut nametag paper with the transparent cover, place it between the transparent cover and the silicone strip, and ensure the number orientation is correct.



4. Reassemble all parts in the specified order to complete nametag paper replacement.

3.7 How to Intall Bracket without Rainshield

Follow the instructions below to install bracket without rain shield.

Before You Start

- Read the surface mounting steps shown at Quick Start Guide.
- Get the installation equipments including a drill bit, a marker, a screwdriver and so on.
- Check whether the device, bracket and other spare parts are compelete.

Steps

1. Align the bracket with the wall at a suitable height (ensure a minimum distance of 5mm between the bracket and any non-installation wall surface), mark the mounting hole positions for the diagonal bracket on the wall, then drill holes using a drill bit and insert expansion bolts into the holes. Secure the bracket to the wall using 4 pieces of KA4X25 screws.

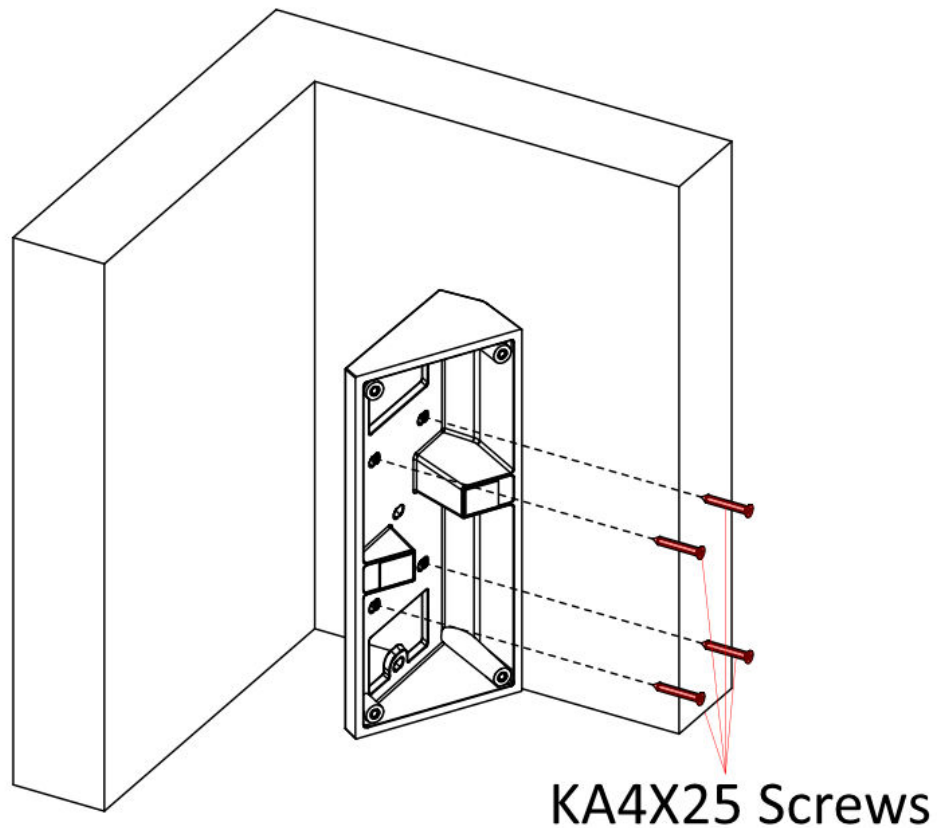


Figure 3-15 Step 1



Note

To ensure waterproof performance, it is recommended to apply sealant to the top and sides of the diagonal bracket.

2. Install the surface mounting junction box onto the diagonal bracket using 4 pieces of KM4X8 screws as shown. Route the wiring harness through the threading hole at the the surface mounting junction box.

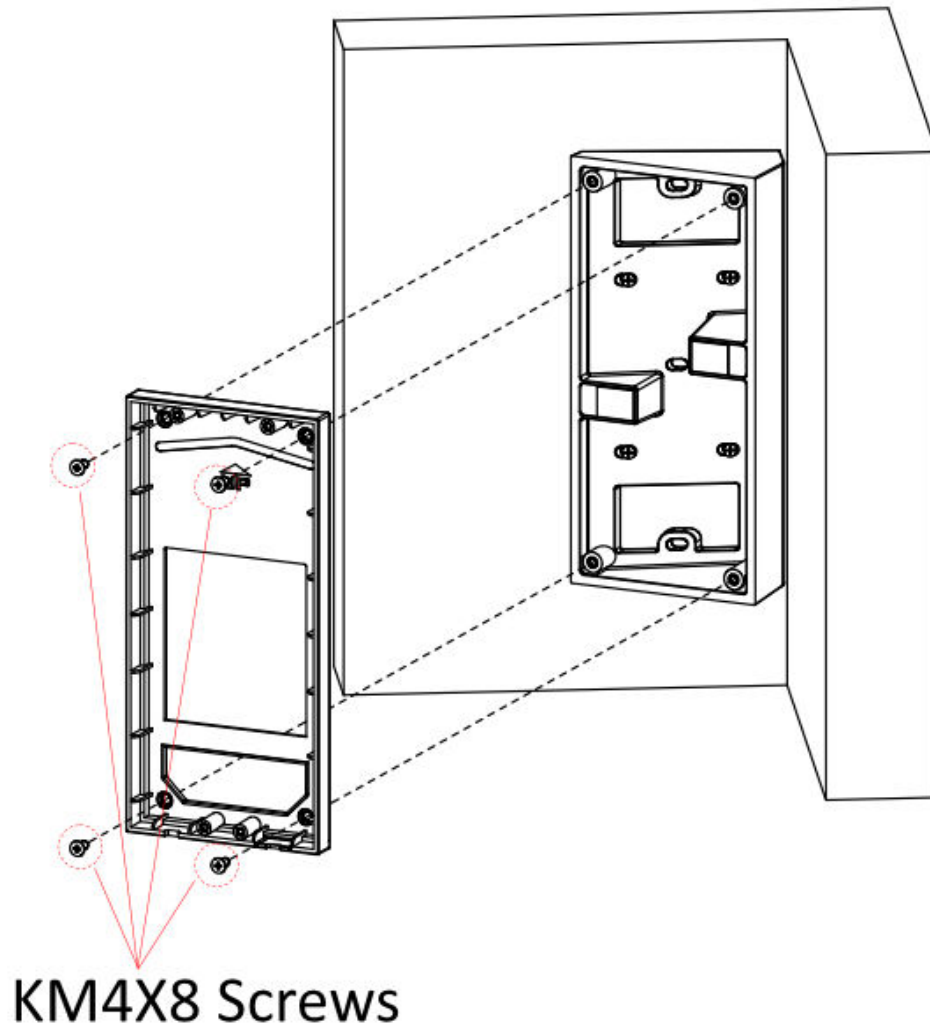


Figure 3-16 Step 2

3. After completing the wiring, assemble the main body of the device and the decorative cover onto the surface-mounting junction box in sequence according to the surface mounting method.

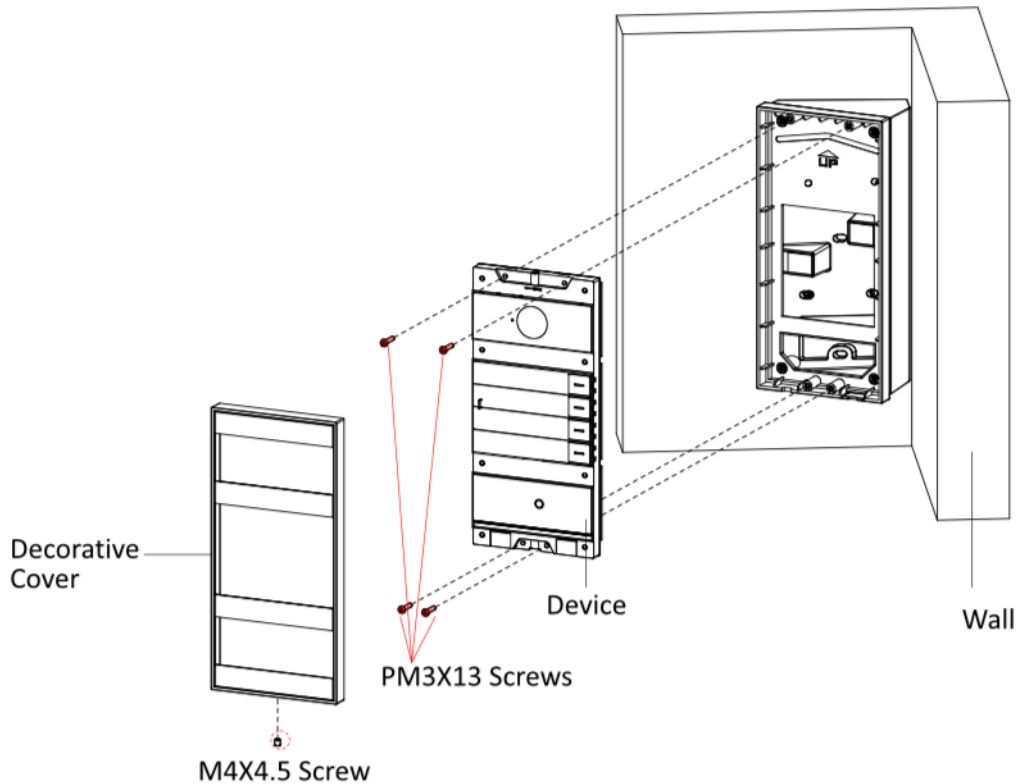


Figure 3-17 Step 3

- 1) Assemble the decorative cover onto the device.
- 2) Tighten the bottom M4X4.5 screw to the appropriate position.



Note

To ensure waterproof performance, it is recommended to apply silicone sealant to the top and both sides of the mounting plate.

For device with 3 lens, the installation procedures are the same, except in step 3, you need to tighten the top and bottom M4X4.5 screws to appropriate position to fix the decorative cover.

3.8 How to Install Bracket with Rainshield

Follow the instructions below to install bracket with rain shield.

Before You Start

- Read the surface mounting steps shown at Quick Start Guide.
- Get the installation equipments including a drill bit, a marker, a screwdriver and so on.
- Check whether the device, bracket, rain shield and other spare parts are complete.

Steps

1. Align the bracket with the wall at a suitable height (ensure a minimum distance of 5mm between the bracket and any non-installation wall surface), mark the mounting hole positions for the diagonal bracket on the wall, then drill holes using a drill bit and insert expansion bolts into the holes. Secure the bracket to the wall using 4 pieces of KA4X25 screws.

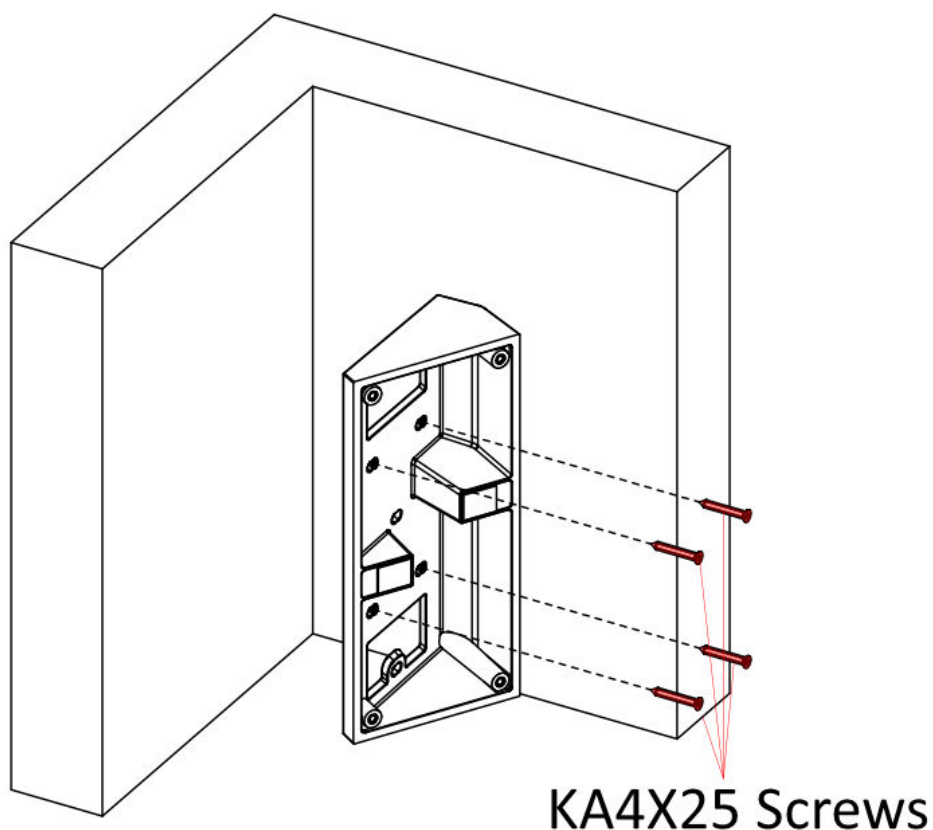


Figure 3-18 Step 1



Note

To ensure waterproof performance, it is recommended to apply sealant to the top and sides of the diagonal bracket.

2. Install the rain shield adapter plate and surface mounting junction box onto the diagonal bracket using 4 pieces of KM4X8 screws as shown. Route the wiring harness through the threading hole at the the junction box.

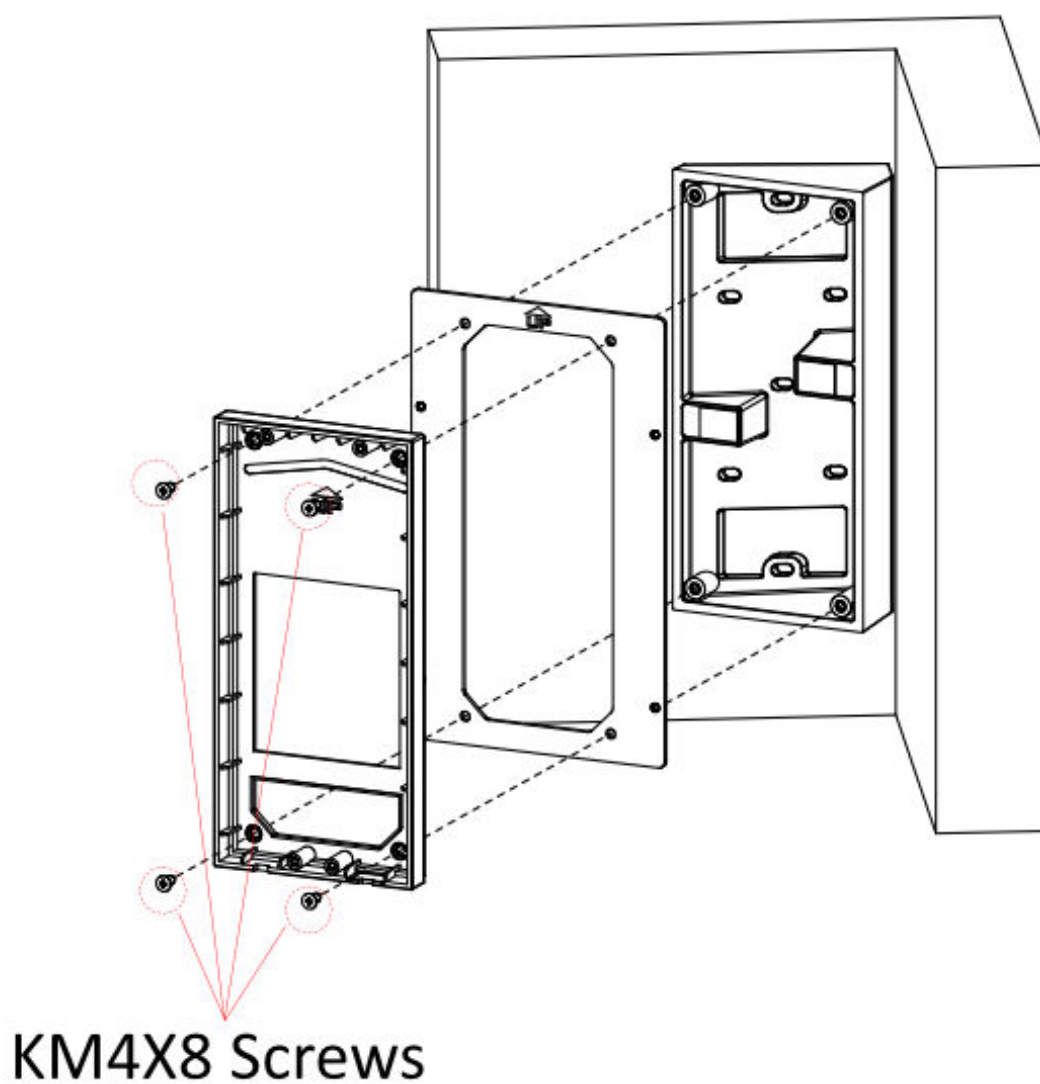


Figure 3-19 Step 2

3. After completing the wiring, assemble the main device body and decorative cover onto the surface mounting junction box in sequence following the surface-mounted installation method.

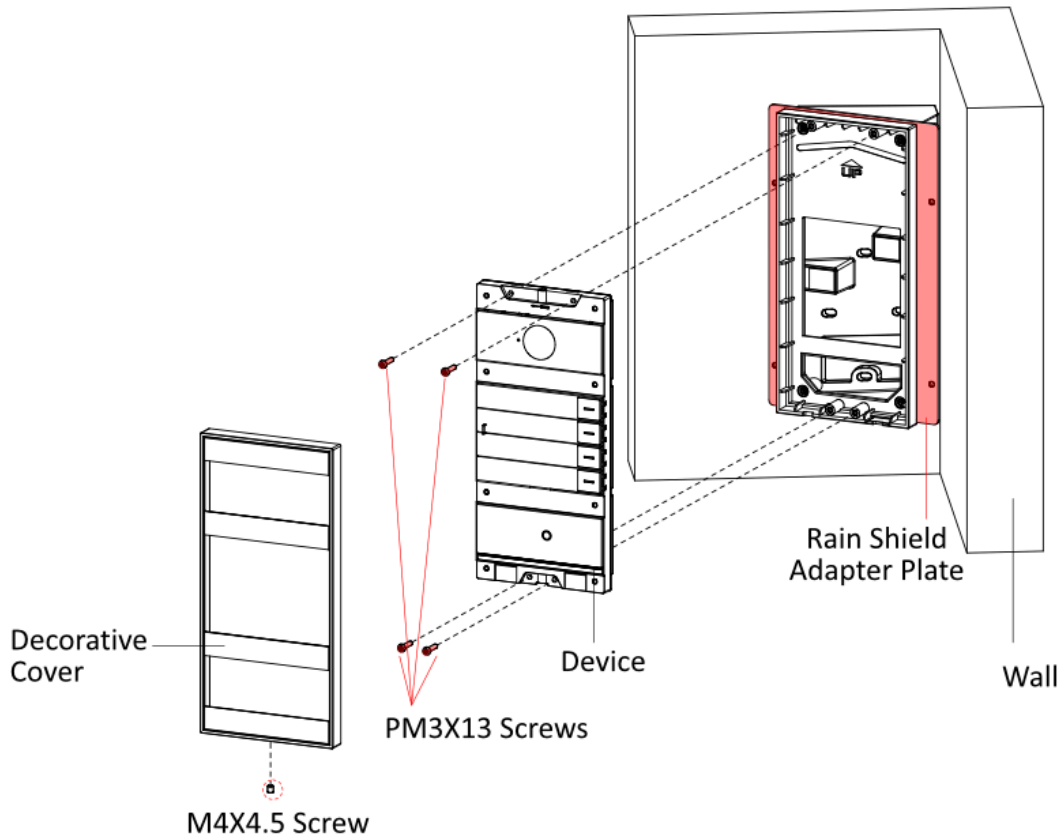


Figure 3-20 Step 3

- 1) Assemble the decorative cover onto the device.
- 2) Tighten the bottom M4X4.5 screw to the appropriate position.
4. Install the surface mounting rain shield onto the rain shield adapter using 4PCS KM4X8 screws. Adjust the rain shield upward according to the field of view requirements, and set it to the appropriate installation height.

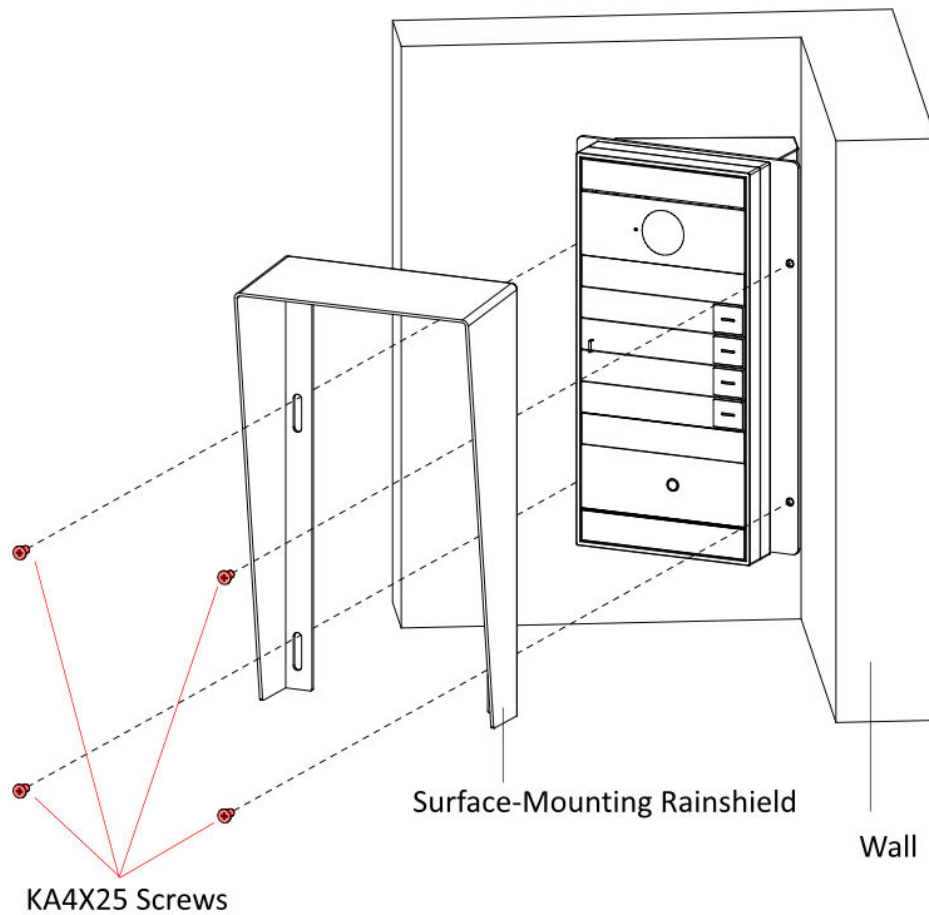


Figure 3-21 Step 4

Note

To ensure waterproof effectiveness, it is recommended to apply silicone sealant to the top and sides of the rain shield.

For device with 3 lens, the intallation procedures are the same, except in step 3, you need to tighten the top and bottom M4X4.5 screws to appropriate position to fix the decorative cover.

Chapter 4 Activation

4.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website <http://www.hikvision.com/en/>, and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

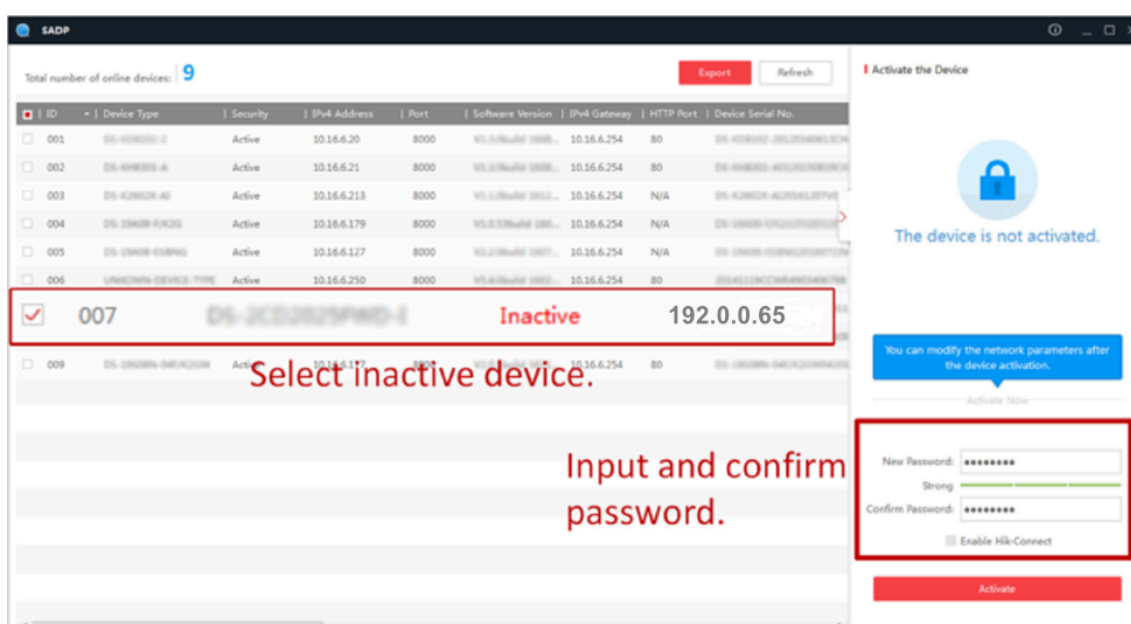
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

4.2 Activate via Web Browser

You can activate the device via the web browser.

Steps

- 1. Enter the device default IP address (192.0.0.65) in the address bar of the web browser, and press Enter.**



Note

Make sure the device IP address and the computer's should be in the same IP segment.

- 2. Create a new password (admin password) and confirm the password.**



Note

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- The username cannot be the same as the password. Password cannot be inverted write of user name.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

-
- 3. Click **Activate**.**

- 4. Edit the device IP address.** You can edit the IP address via the SADP tool, the device, and the client software.

4.3 Activate Device via Client Software

You can only configure and operate the door station after creating a password for the device activation.

Default parameters of door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Run the client software, click **Maintenance and Management** → **Device Management** → **Device** to enter the page.
2. Click **Online Device**.
3. Select an inactivated device and click **Activate**.
4. Create a password, and confirm the password.

Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

5. Click **OK** to activate the device.

Note

- When the device is not activated, the basic operation and remote operation of device cannot be performed.
- You can hold the **Ctrl** or **Shift** key to select multiple devices in the online devices, and click the **Activate** button to activate devices in batch.

4.4 Edit Network Parameters

To operate and configure the device via LAN (Local Area Network), you need connect the device in the same subnet with your PC. You can edit network parameters via **iVMS-4200** client software.

Steps

1. Select an online activated device and click the **Modify Netinfo**.
2. Edit the device IP address and gateway address to the same subnet with your computer.
3. Enter the password and click **OK** to save the network parameters modification.

Note

- The default port No. is 8000.
- The default IP address of the door station is 192.0.0.65.
- After editing the network parameters of device, you should add the devices to the device list again.

Chapter 5 Quick Operation via Web Browser

5.1 Select Language

You can select a language for the device system.

Click  in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.



Note

After you change the system language, the device will reboot automatically.

5.2 Time Settings

Click  in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

5.3 Privacy Settings

Set the picture uploading and storage parameters.

Click  in the top right of the web page to enter the wizard page.

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

5.4 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

- 1) Click **Add Face** to upload a face picture from local storage.
-

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

- 2) Click **Add Card** to enter the Card No. and select the property of the card.
-

Note

Up to 5 cards can be supported.

5.5 No. and System Network

Steps

1. Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

If set the device type as **Door Station**, you can set the **Community No.**, **Building No.**, **Unit No.**, **Floor No.** and **Door Station No.**.

Device Type

The device can be used as a door station or doorphone. Select a device type from the drop-down list.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.



Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 99.

3. Set the video intercom network parameters.



Note

The device type is selected as **Door Station** by default. If you select another type, you can reboot device and go to **Configuration → Intercom** for intercom settings.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete to save the settings after the configuration.**

Chapter 6 Operation via PC Web

6.1 Login Web Browser

You can log into the Web browser for device configuration.

Steps

1. Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
2. Enter the device user name and the password. Click **Login** to login to the page.

6.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

6.3 Overview

You can view the live video of the device, real-time event, linked devices, person information, network status, basic information, and device capacity.

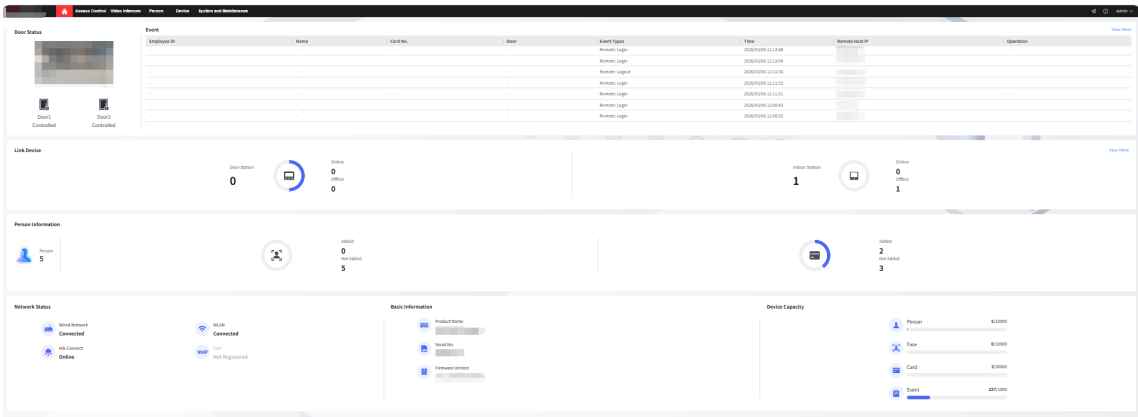


Figure 6-1 Overview Page

Function Descriptions:

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.



You can capture image when starting live view.



Select the streaming type when starting live view. You can select from the main stream and the sub stream.



Full screen view.



The door status is open/closed/remaining open/remaining closed.

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the time, the unit. Click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person face, fingerprint and card.

Network Status

You can view the connected and registered status of wired network, VoIP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the Person, Face, Card, and Event capacity.

6.4 Person Management

Click **Person** → **+Add** to enter the Add Person page. You can add the person's information, including the basic information, certificate, authentication and settings at this page.

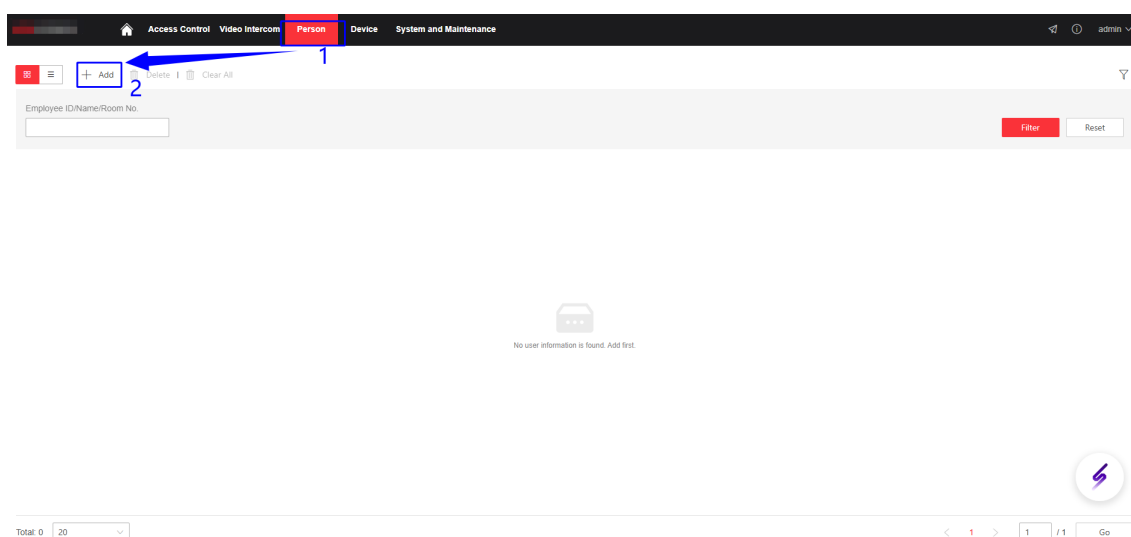


Figure 6-2 Person Page Overview

Add Basic Information

Add the person's basic information, including the employee ID, the person's name, floor No., room No., etc.



The 'Basic Information' form contains the following fields and controls:

- Employee ID:** A text input field with an asterisk indicating it is required.
- Name:** A text input field.
- Person Type:** A radio button selection with 'Normal User' selected.
- Administrator:** A toggle switch, currently turned off.
- Long-Term Effective User:** A toggle switch, currently turned off.
- Validity Period:** A date range selector showing '2026/03/06 00:00:00' to '2036/03/05 23:59:59' with a calendar icon on the right.

Figure 6-3 Basic Information

Click **Save** to save the settings.

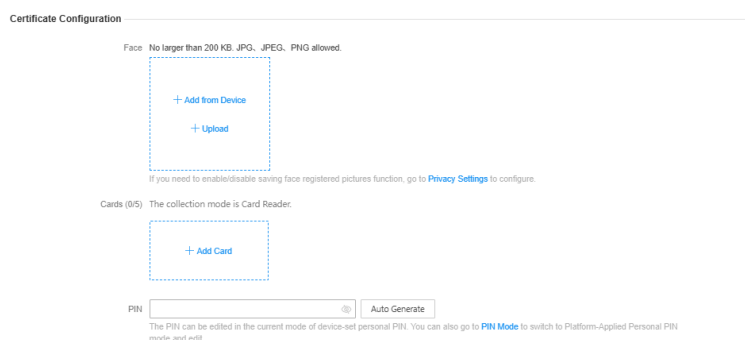
Set Validity Period

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Authentication Settings

Set the authentication type. You can choose from face, cards, and pin configuration.



The 'Certificate Configuration' form includes the following sections:

- Face:** A dashed box containing '+ Add from Device' and '+ Upload' buttons. A note above states 'No larger than 200 KB, JPG, JPEG, PNG allowed.' A note below states 'If you need to enable/disable saving face registered pictures function, go to [Privacy Settings](#) to configure.'
- Cards (0/5):** A dashed box containing '+ Add Card' button. A note above states 'The collection mode is Card Reader.'
- PIN:** A text input field with an 'Auto Generate' button. A note below states 'The PIN can be edited in the current mode of device-set personal PIN. You can also go to [PIN Mode](#) to switch to Platform-Applied Personal PIN mode and edit.'

Figure 6-4 Certificate Configuration

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

Add Face Picture

Click + to upload a face picture from the local PC or from device.

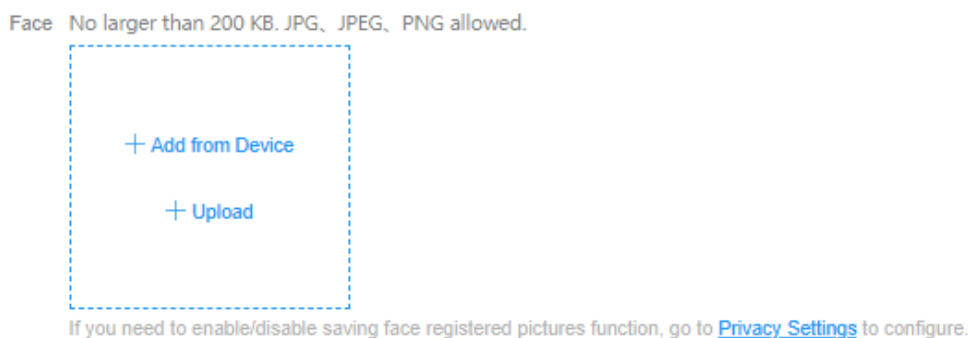


Figure 6-5 Add Face Picture



Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 K.

Add Card

Click **+ Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.



Note

Up to 5 cards can be added.

Generate PIN

You can click **Auto Generate** to get a random pin.

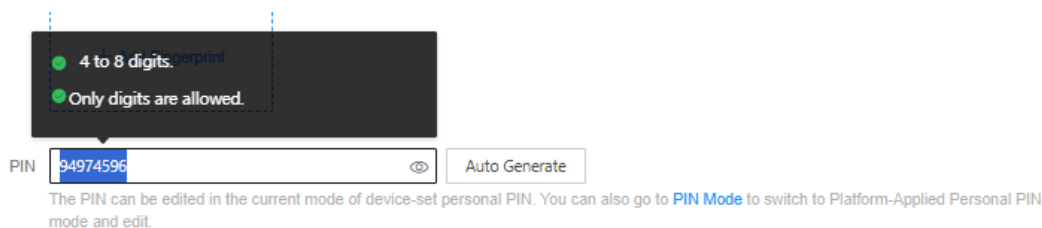


Figure 6-6 PIN

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

No. Settings

Click **+ Add**. Then you can configure the Room No. and Floor No. for this newly-added person.

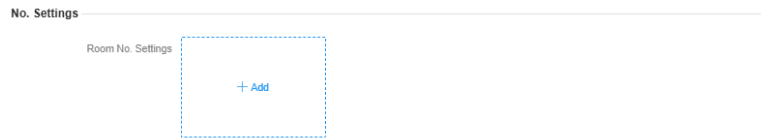
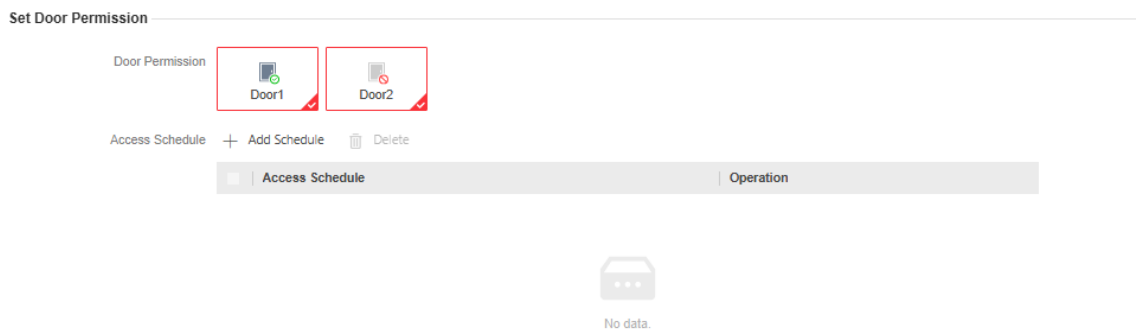


Figure 6-7 No. Settings

You can set the room No. and Floor No. for the added person here. This helps to record visitor entrance information and can help the property management team to contact the visitor.

Set Door Permission

You can add schedule and door permission for each person.



Note

Just select an access schedule from your saved template and click **OK**.

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

6.5 Device Management

You can manage the linked device on the page.

Click **Device** to enter the settings page.

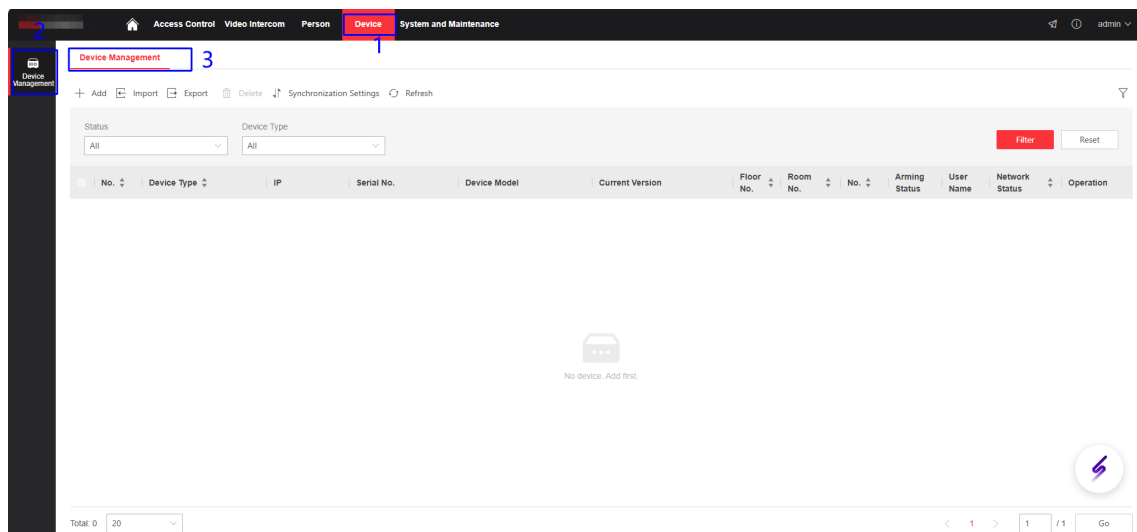


Figure 6-8 Device Management

Add Device

- Click **+Add** to add the indoor station or sub door station. Enter the parameters and click **Add** to add.
- Click **Import**. Enter the information of the device in the template to import devices in batch.

Export

Click **Export** to export the information to the PC.

Delete

Select the device and click **Delete** to remove the selected device from the list.

Synchronization Settings

Click **Synchronization Settings** and enable **Synchronize**. If enabled, the current device's settings will be synchronized to other devices.

Refresh

Click **Refresh** to get the device information.

Optional: Set Device Information.

- Click  to edit device information.
- Click  to delete device information from the list.
- Select **Status** and **Device Type** to search devices.

6.6 Maintenance and Security

6.6.1 Set Protocol Testing

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Protocol Testing** .

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

6.6.2 Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security → Maintenance → Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

6.6.3 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **System and Maintenance → Maintenance → Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .

Select an upgrade type from the drop-down list. Click  and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.



Note

Do not power off during the upgrading.

Sub Device Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .

Set Upgrade Settings as **RS-485 Card Reader**, and select a card reader.
Select an upgrade type from the drop-down list. Click  and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Backup

Device Parameters

Export

 Data Migration

Export

Default

Restore to Default Settings

Restore

All data except network parameters and user accounts will be cleared.

Restore to Factory Settings

Restore All

All functions and parameters will be restored to factory settings.

Import Config File

Device Parameters



Import

Data Migration



Import

Figure 6-9 Back up and Reset

Device Parameters

Click **Export** to export the device parameters.

 Note

You can import the exported device parameters to another device.

Data Migration

Click **Export** to migrate user information and configuration details to other devices.

The information and data include door station configuration data, advertisement information, ringtone and etc.

Import

Click  and select the file to import. Click **Import** to start import configuration file.

6.6.4 Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance** → **Maintenance** → **Device Debugging** .
2. You can set the following parameters.

Enable SSH

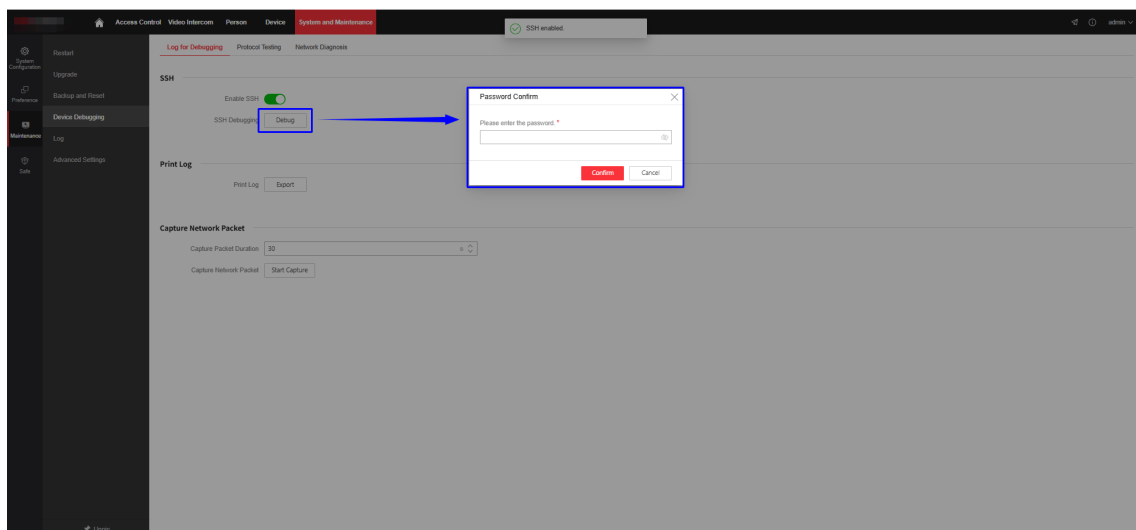


Figure 6-10 SSH Debugging

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.



Note

You need to enter admin password if you want to enable SSH debugging.

The SSH protocol provides encrypted communication, ensuring data security during the debugging process and preventing the leakage of sensitive information.

Print Log

You can click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, and click **Start Capture** to capture.

6.6.5 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log**.

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

6.6.6 Advanced Settings

View Version Information

Click **System and Maintenance → Maintenance → Advanced Settings →**, then enter admin password to visit the page.

Advanced Configuration

Biometrics

Custom Anti-Spoofing Detection ☐

 Lock Face for Anti-Spoofing Protection ☒

Lock Duration min  

Cancel Locking Face for Anti-Spoofing Protection

Unlock

If the device is locked, click the button to unlock.

Version Information

BSP Version V1.1.0 build20260811

DSP Version V2.10.1 build 20260818

Engine Version V9.2.0 build20251128

Face Algorithm Version V9.0.212 build20251113

Save

Figure 6-11 Version Information in Advanced Configuration

Here you can view version information including BSP Version, DSP Version, Engine Version and Face Algorithm Version.

Biometrics Settings

Steps

1. Click **System and Maintenance** → **Maintenance** → **Advanced Settings** → , then enter admin password to visit the page.

Advanced Configuration

Biometrics

Custom Anti-Spoofing Detection

i

 Lock Face for Anti-Spoofing Protection

Lock Duration

2

min

Cancel Locking Face for Anti-Spoofing Protection

Unlock

If the device is locked, click the button to unlock.

Version Information

BSP Version

V1.1.0 build20260811

DSP Version

V2.10.1 build 20260818

Engine Version

V9.2.0 build20251128

Face Algorithm Version

V9.0.212 build20251113

Save

Figure 6-12 Biometrics Settings in Advanced Configuration

2. Slide to enable **Custom Anti-spoofing Detection**, and set **Anti-Spoofing Detection Threshold** and **Anti-Spoofing Detection Threshold of Face with Mask**.

Biometrics

Custom Anti-Spoofing Detection ☒

Anti-Spoofing Detection Level General

① Anti-Spoofing Detection Threshold 90

① Anti-Spoofing Detection Threshold of Face with Mask 90

① Lock Face for Anti-Spoofing Protection ☒

Lock Duration min

Cancel Locking Face for Anti-Spoofing Protection

If the device is locked, click the button to unlock.

Figure 6-13 Biometrics Details



Note

Anti-Spoofing Detection Threshold

Range: 1 to 100. When you select a smaller value, the detection result will be less accurate and the passing efficiency will be higher.

Anti-Spoofing Detection Threshold of Face with Mask

Range: 1 to 100. When you select a smaller value, the detection result will be less accurate and the passing efficiency will be higher.

- 3. Lock Face for Anti-Spoofing** is enabled by default. If enabled, the face will be locked for anti-spoofing protection after the failed attempt limit of anti-spoofing detection has been reached.
- 4. Set Lock Duration.** (Range: 1 ~ 240 min)
- 5. Optional:** If the device is locked, you can click **Unlock** to cancel locking face for anti-spoofing protection.
- 6. Click Save** to enable the settings.

6.6.7 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **System and Maintenance** → **Safe** → **Security Service** to enter the page.

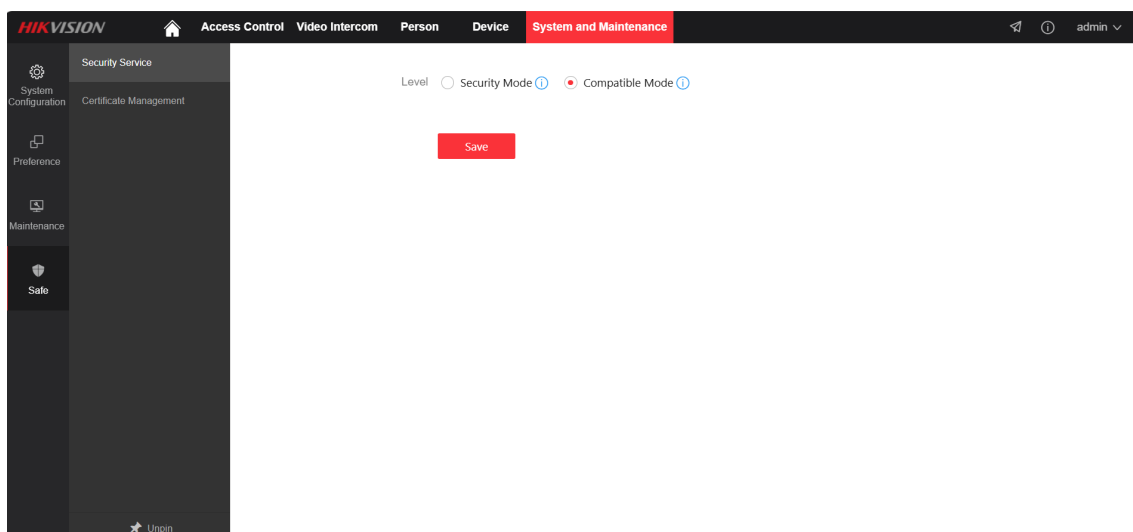


Figure 6-14 Security Service

Click to select a security mode and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

6.6.8 Certificate Management

It helps to manage the server/client certificates and CA certificate.



Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

1. Go to **System and Maintenance** → **Safe** → **Certificate Management**.
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

The created certificate is displayed in the **Certificate Details** area.

The certificate will be saved automatically.

6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
 - 1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
 - 2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.



Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

6.7 Preference

You can set decorate light at this page.

Steps

1. Tap **System and Maintenance → Preference** to enter the preference settings page.

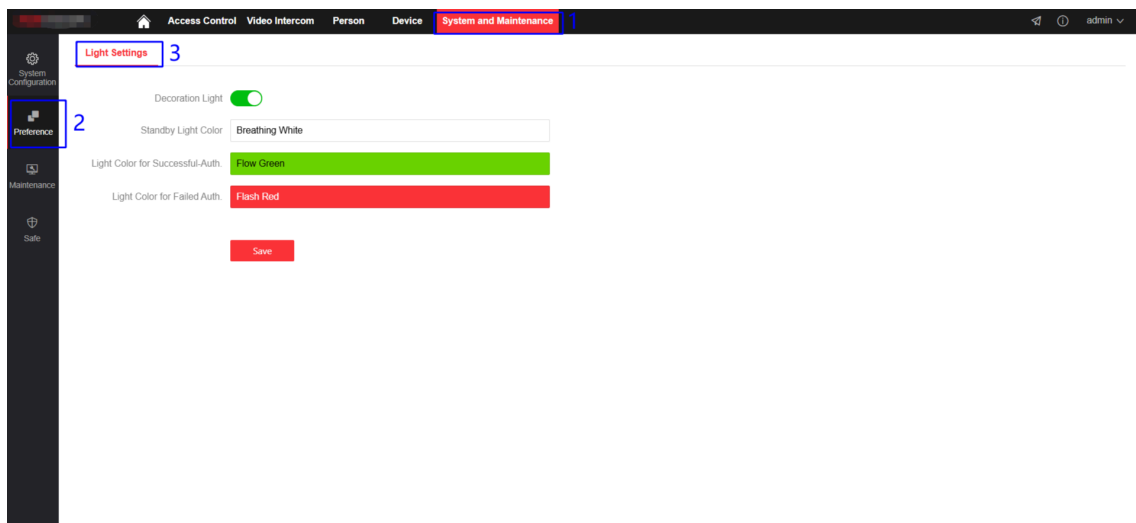


Figure 6-15 Preference

2. You can set the decoration light. Slide to enable **Decoration Light**. Then you can choose **Standby Light Color**, **Light Color for Successful-Auth** and **Light Color for Failed Auth**.

6.8 Configuration

6.8.1 System Settings

View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

Click **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Basic Information** to enter the configuration page.

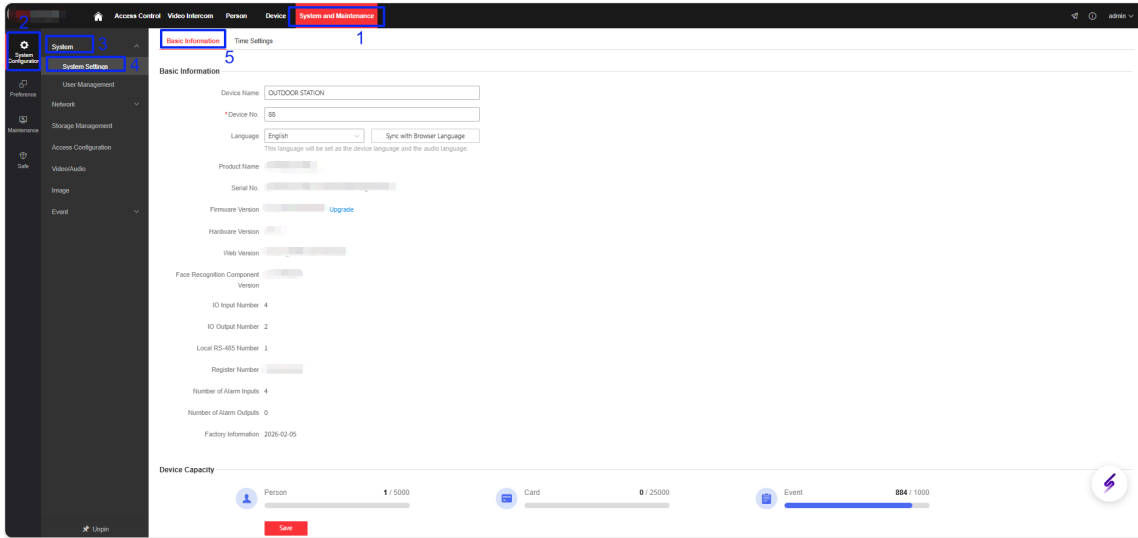


Figure 6-16 Basic Information

You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc. Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings** .

Device Time 2023-05-05 19:46:20

Time Zone (GMT+00:00) Dublin, Edinburgh, London

Time Synchronization mode ☒ Manual

Set Time 2023-05-05 19:46:16 Sync With Com...

DST

DST ☒

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias ☒ 30minute(s) ☐ 60minute(s) ☐ 90minute(s) ☐ 120minute(s)

Save

Figure 6-17 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

Set DST

Steps

1. Click **System Configuration → System → System Settings → Time Settings** .
2. Slide to enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

6.8.2 User Management

Change Administrator's Password

Steps

1. Click **System and Maintenance → System Configuration → System → User Management → User Management** .

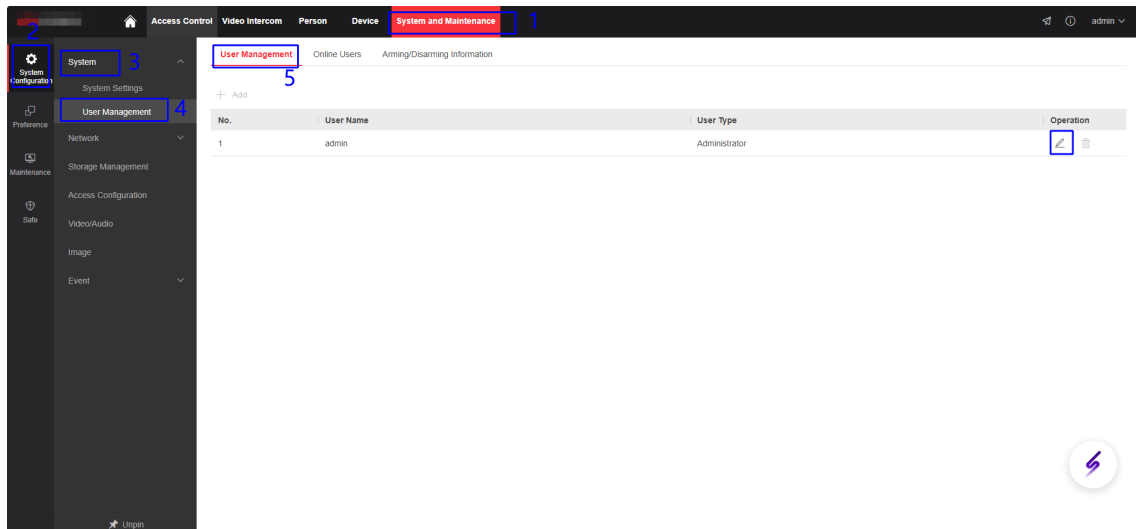


Figure 6-18 User Management

2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Note

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- The username cannot be the same as the password. Password cannot be inverted write of user name.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

Online Users

The information of users logging into the device is shown.

Go to **System and Maintenance** → **System Configuration** → **System** → **User Management** → **Online Users** to view the list of online users.

View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **System Configuration** → **System** → **User Management** → **Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.8.3 Network Settings

Set Basic Network Parameters

Click **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **TCP/IP** .

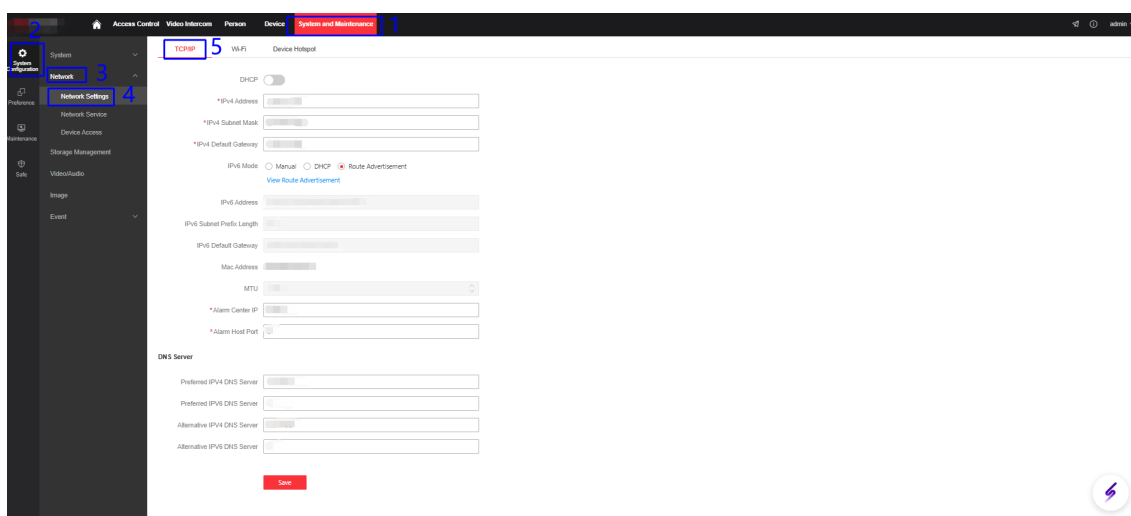


Figure 6-19 TCP/IP Settings

Set the parameters and click **Save** to save the settings.

DHCP

If disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server and the Alternate DNS server.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, preferred DNS server and the Alternate DNS server automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

Wi-Fi Settings

Some models support Wi-Fi function.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Wi-Fi** to enter the settings page.

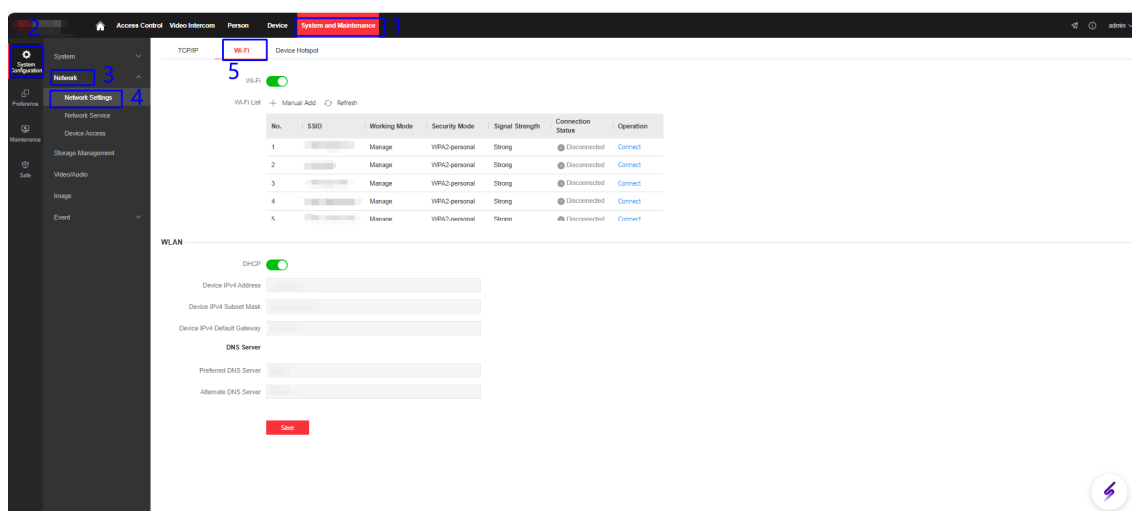


Figure 6-20 Wi-Fi

2. Enable **Wi-Fi**.
3. Click **+ Manual Add**, and set corresponding parameters and **Password** of the Wi-Fi.
 - 1) Enter the **SSID**.
 - 2) Select **Security Mode**.
 - 3) Click **Save**.
 - 4) **Optional**: Click **Refresh** to get the present information.

5) Click **Connect**.

4. **Optional:** Set WLAN.

1) Set the WLAN parameters.

Enable DHCP

Enable **DHCP** to **Auto DNS**, the device will allocate the IP and DNS automatically.

Disable DHCP

Manually set the IP and DNS server.

2) Tap **Save**.

Device Hotspot

Only some models support this function.

Steps

1. Click **Network → Network Settings → Device Hotspot** .

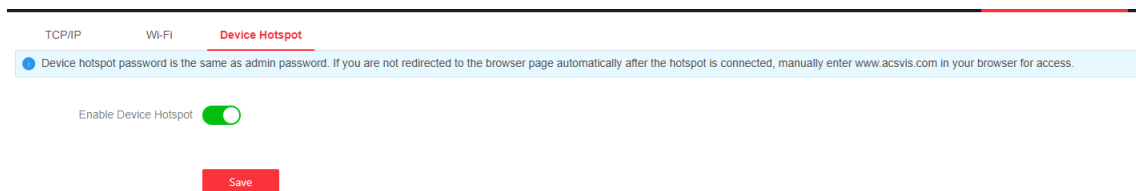


Figure 6-21 Device Hotspot

2. Slide to enable/disable device hotspot.



Note

Device hotspot password is the same as admin password. If you are not redirected to the browser page automatically after the hotspot is connected, manually enter www.acsvs.com in your browser for access.

3. Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, RTSP and Server port parameters.

Click **System Configuration → Network → Network Service → HTTP(S)** .

HTTP(S)

RTSP

FTP

WebSocket(s)

HTTP

Enable ☒

Enabling HTTP may cause security problems.

HTTP Port

HTTPS

Enable ☒

HTTPS Port

Web Authentication

Digest Algorithm ☐ MD5 ☐ SHA256 ☒ MD5/SHA256

Digest algorithm applies to both HTTP and HTTPS.

Save

Figure 6-22 HTTP(S)

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter **http://192.0.0.65:81** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Web Authentication

You can select **Digest Algorithm** as **MD5**, **SHA256** or **MD5/SHA256**.

Digest algorithm applies to both HTTP and HTTPS.

 Note

- MD5: A widely used cryptographic hash function that produces a 128-bit hash value. It is fast but considered less secure compared to SHA256.
- SHA256: A more secure cryptographic hash function that produces a 256-bit hash value. It offers stronger protection against collisions and brute-force attacks.
- MD5/SHA256: A combined mode that supports both algorithms, allowing the device to accept authentication requests using either MD5 or SHA256. This ensures compatibility with older clients while still enabling stronger security when supported.

Click **System Configuration** → **Network** → **Network Service** → **RTSP** .

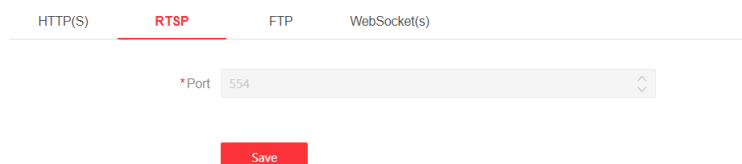


Figure 6-23 RSTP

RTSP

It refers to the port of real-time streaming protocol.

Click **System Configuration** → **Network** → **Device Access** → **SDK Server** .

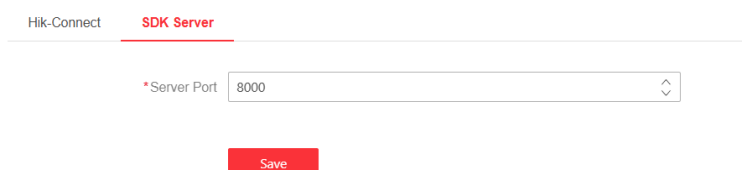


Figure 6-24 SDK Server

SDK Server

It refers to the port through which the client adds the device.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System Configuration** → **Network** → **Device Access** → **Hik-Connect** to enter the settings page.



Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and verification code.



Note

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

5. Enter the verification code.
6. You can also click **More Configure** to adjust **Network Connection Priority**.

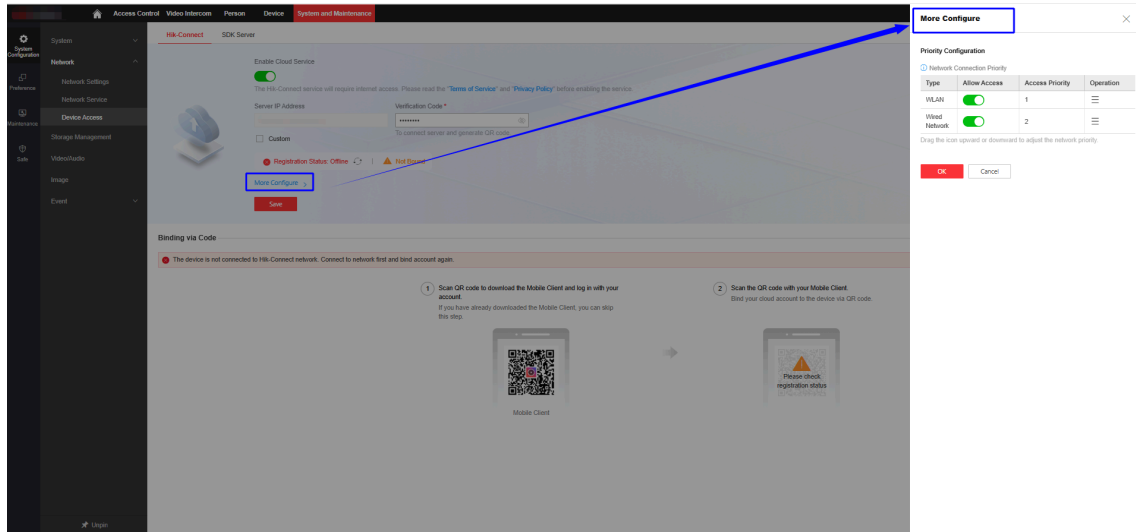


Figure 6-25 More Configure

7. Bind an account.
Binding via Code: Take your phone, open the app, then scan the QR code at the back of your device to bind the account.
8. Click **Save** to enable the settings.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)**.

View WebSocket and WebSockets port.

FTP Settings

You can configure FTP (File Transfer Protocol) parameters.

Steps

1. Click **Network** → **Network Service** → **FTP** to enter the settings page.

HTTP(S)

RTSP

FTP

WebSocket(s)

Enable FTP

Server Type

Server IP Address

* Server IP Address

* Port

Anonymous

* User Name

* Password

* Password Confirm

Directory Structure

Save in the child directory

Parent Directory

Building No. & Unit No.

Child Directory

Time

* Delimiter

-

Named Item

Option1

Option2

Option3

Option4

Option5

Option6

Named Item

Option1

Named Element

Time

Save

Figure 6-26 FTP Settings

- 2. EnableFTP.
- 3. Select **Server Type**.
- 4. Enter **Server IP Address** and **Port**.
- 5. Configure the FTP Settings, and the user name and password are required for the server login.



Note

If you enable **Anonymous**, you will not need to set user name and password.

- 6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
- 7. Set naming rules.
- 8. Click **Save** to enable the settings.

6.8.4 TF Card Management

You can check detailed TF card information.

Before You Start

Install the TF card to the device.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Storage Management** → **TF Card Management** .
2. The you can view **Current Status** of the TF card and check **TF Card Capacity**.



Note

You can also check TF card's used capacity and remaining capacity on this page.

3. Click **Format**.



Note

After formatting, the status of the TF card is changed from unformatted to normal. It means that the TF card can be used normally, and the disk capacity and remaining space can be viewed.

6.8.5 View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **System Configuration** → **System** → **User Management** → **Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

6.8.6 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **System and Maintenance** → **System Configuration** → **Video/Audio** → **Video** .

The screenshot shows the 'Video' settings page for 'Camera 01'. The left sidebar contains 'System Configuration' with sub-items: System, System Settings, User Management, Network, Storage Management, Video/Audio (selected), Image, and Event. The main content area has tabs for 'Video' and 'Audio'. Under the 'Video' tab, the following settings are visible: Camera Name (Camera 01), Stream Type (Main Stream), Video Type (Video Stream), Resolution (1280*720), Bit Rate Type (Constant), Video Quality (Medium), Frame Rate (30 fps), Max. Bitrate (4096 Kbps), Video Encoding (H.265), I Frame Interval (60), and a toggle for 'Enable Custom Payload' which is turned on. Below the toggle, a note states: 'After enabling, you can adjust the Payload value of the video stream. For example, H.264 corresponds to 96.' The 'Custom Video Stream Payload Value' is set to 96. A red 'Save' button is at the bottom.

Figure 6-27 Video Settings Page

Set the stream type, the video type, the resolution, the Bit Rate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

You can also slide to **Enable Custom Payload** and set **Custom Video Stream Payload Value**.



Note

After enabling Custom Payload, you can adjust the Payload value of the video stream. For example, H.264 corresponds to 96.

Click **Save** to save the settings.



Note

The functions vary according to different models. Refers to the actual device for details.

Set Audio Parameters

Click **System and Maintenance** → **System Configuration** → **Video/Audio** → **Audio** .

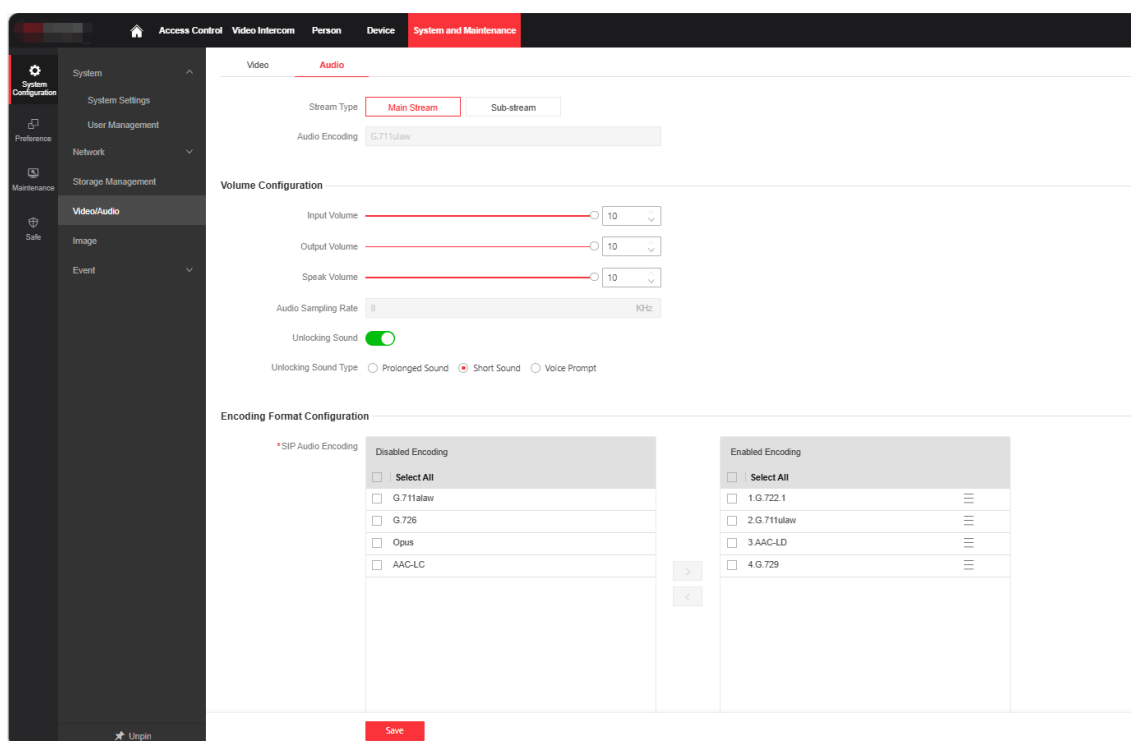


Figure 6-28 Audio Settings Page

Set the stream type, audio encoding, input volume, output volume, speak volume and audio sampling rate.

Slide to enable **Unlocking Sound** according to your actual need.

Check then click < or > to enable or disable **SIP Audio Encoding**.



Note

You can drag icon ≡ to adjust the order of the encoding.

Click **Save** to save the settings.

6.8.7 Adjust Display Settings

You can adjust image parameters, video parameters, supplement parameters, backlight, beauty etc..

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **Display Settings** .
2. Configure the parameters to adjust the image.

Video Adjustment

Set the video frame rate when performing live view remotely. After changing the video standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Backlight

- You can enable or disable the BLC function.
If enabled, you can choose BLC as **Center**, **UP**, **Down**, **Left** or **Right**.
- You can enable or disable the WDR function.
When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

Day/Night Switch

You can choose Day/Night Switch as Auto, Schedule Switch, Night or Daytime mode.

When choose Day/Night Switch as Auto, you also need to select **Sensitivity** range from 1 to 7.

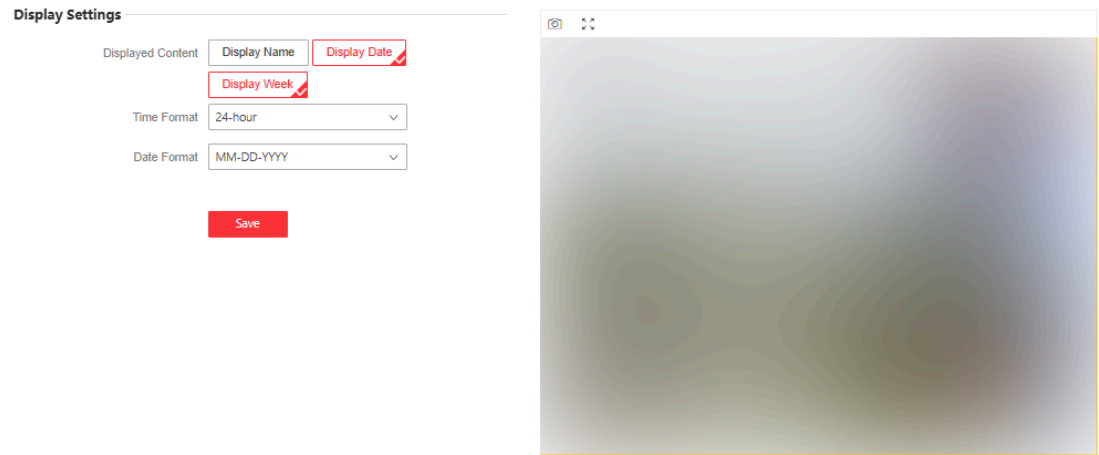
3. Click **Restore Default Settings** to restore the parameters to the default settings.

OSD Configuration

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **OSD Configuration** .

2. At **Displayed Content**, you can click to choose what to display.

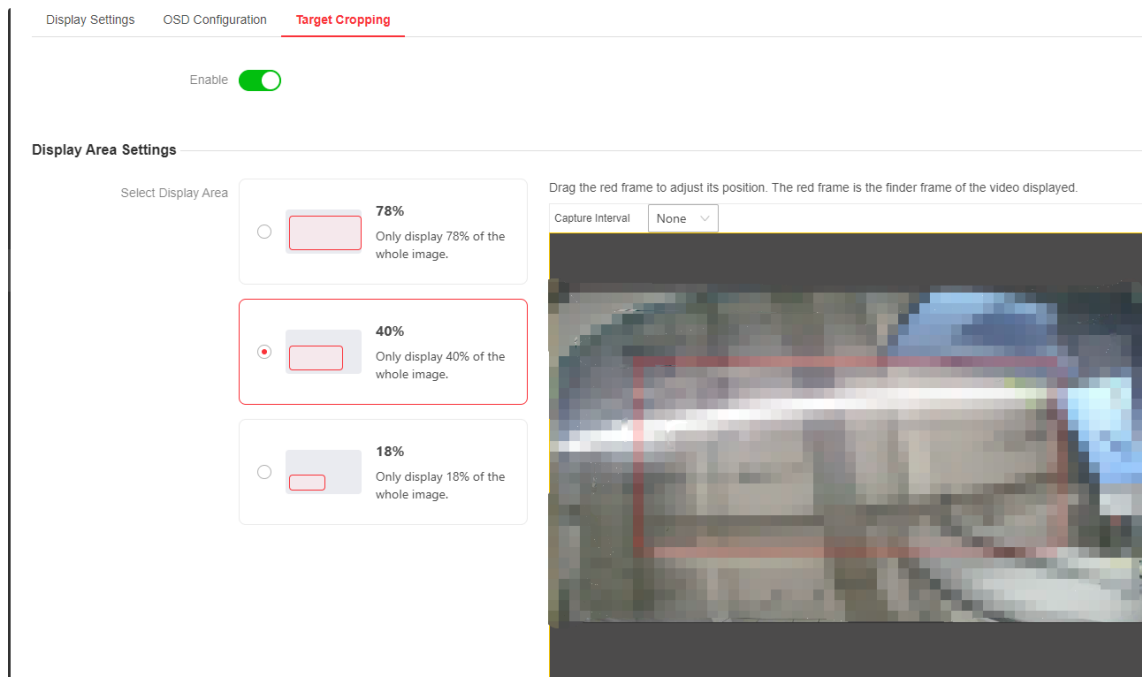


3. You can also choose **Time Format** and **Date Format** according to your actual needs.

Target Cropping

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **Target Cropping**.
2. Slide to enable this function.



3. Select a **Select a Cropping Resolution**.



Note

Cropping resolution is the main stream resolution after target cropping.

4. Click **Save**.



Note

Some models support target cropping. Refer to the actual device for details.

This function is mutually exclusive with some functions. After enabling target cropping, some functions will fail. Refer to the actual device for details.

6.8.8 Event Settings

Set Motion Detection

After enable the function of motion detection, people or stuff enter the configured area will trigger alarm.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Event** → **Event Detection** → **Motion** .

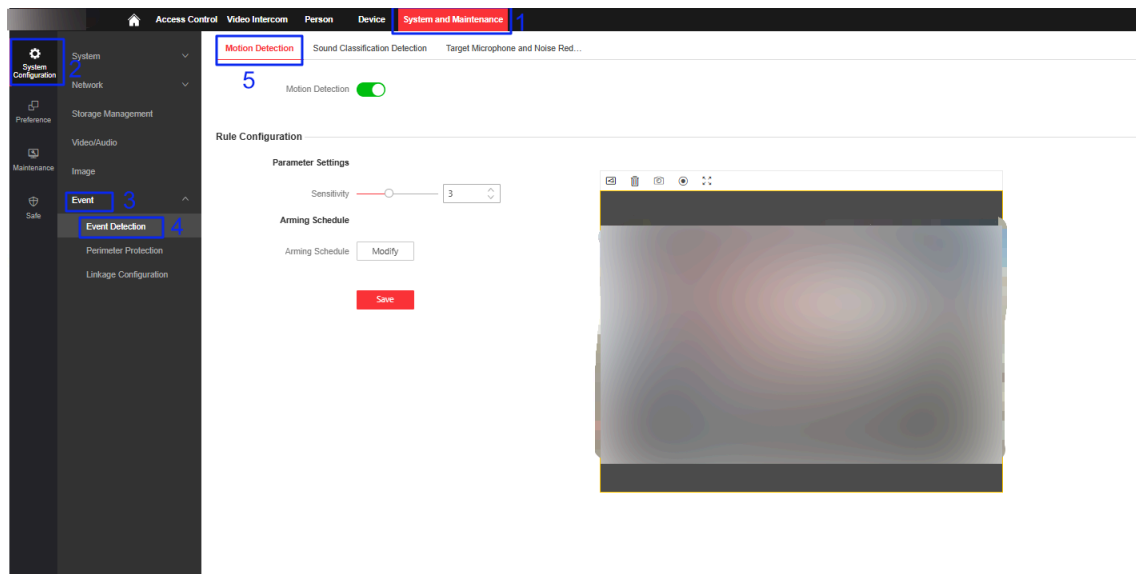


Figure 6-29 Motion Detection

2. Enable **Motion Detection**.
3. Drag the process bar to adjust the **Sensitivity** parameter.
4. Click **Save**.



Note

The arming schedule is defaulted as all-day.

Target Microphone and Noise Reduction

You can set the microphone's pickup direction and background noise reduction on this page.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Event** → **Event Detection** → **Target Microphone and Noise Reduction** to enter this page.

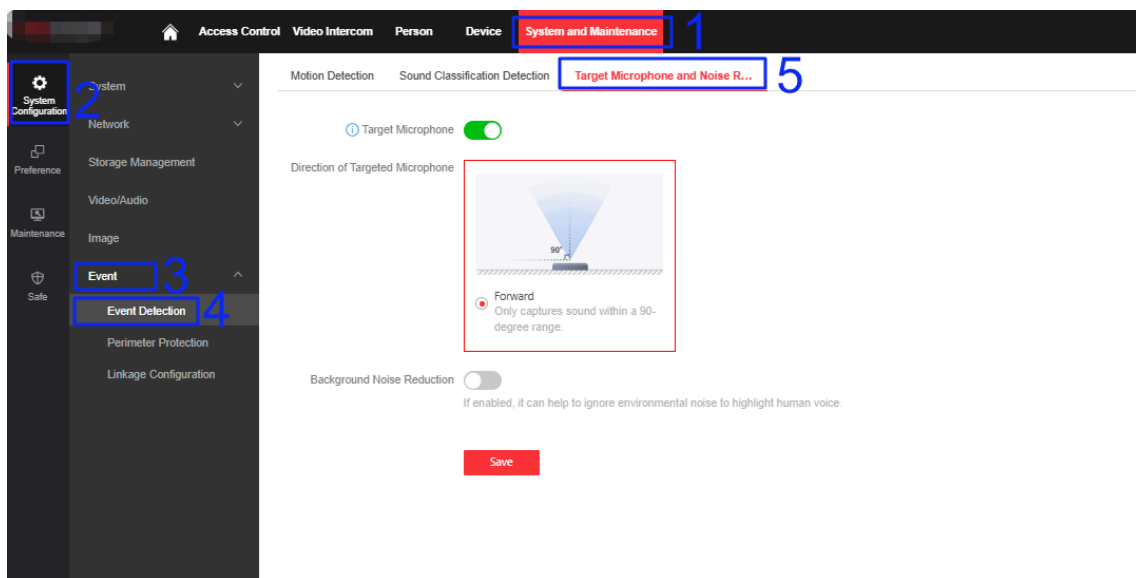


Figure 6-30 Target Microphone and Noise Reduction Page Overview

2. Slide to enable **Target Microphone**. If enabled, the mic will capture sound in the specific direction.
3. Then you can see the default **Direction of Targeted Microphone** is forward. The microphone will only capture sound within a 90-degree range.
4. You can also slide to enable **Background Noise Reduction**. If enabled, it can help to ignore environment noise to highlight human voice.



Note

If you enable **Background Noise Reduction**, **Target Microphone** will be disabled. You can also see a prompt at the screen.

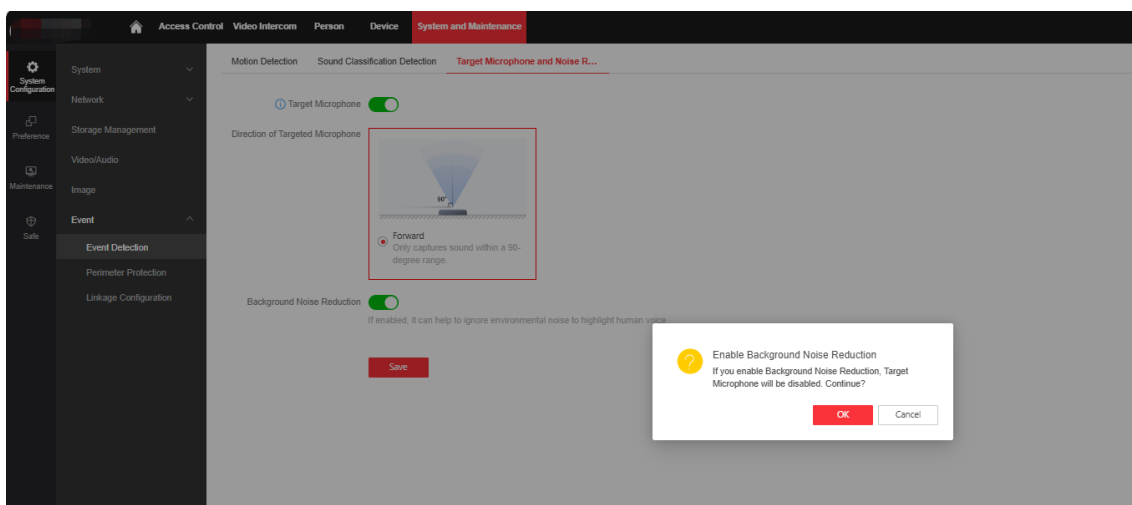


Figure 6-31 Note

Sound Classification Detection

Steps

1. Click **System and Maintenance** → **System Configuration** → **Event** → **Event Detection** → **Sound Classification Detection** to enter the settings page.

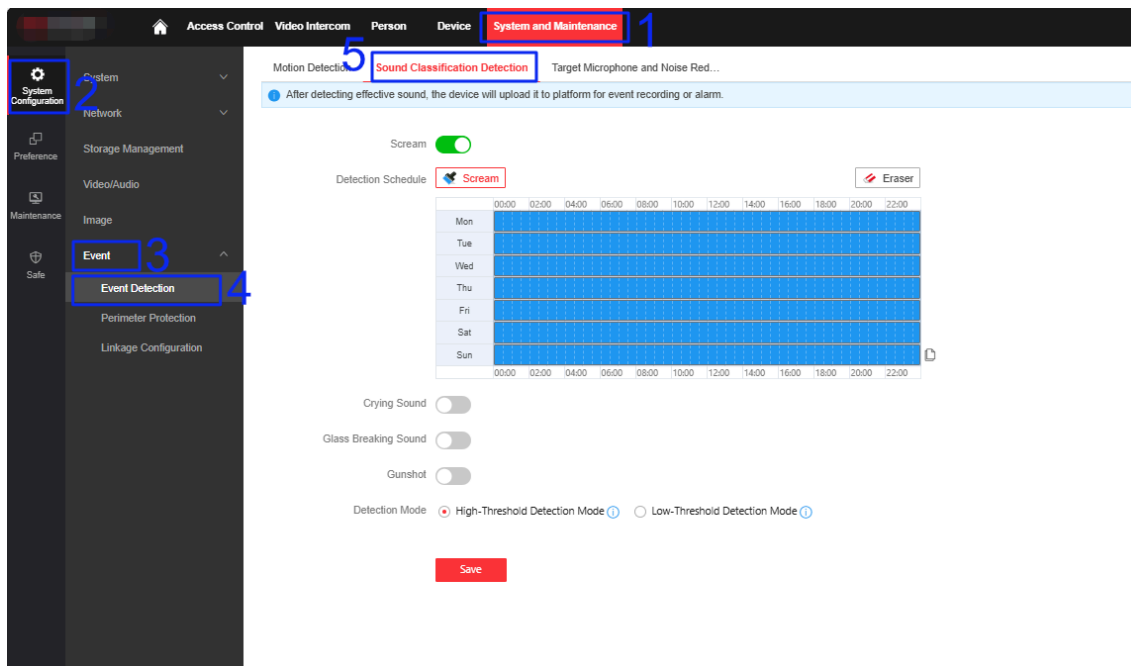


Figure 6-32 Sound Classification Detection

2. Slide to enable the detection of **Scream**, **Crying Sound**, **Glass Breaking Sound** or **Gunshot**.

3. Then you can drag on the diagram to edit the detection schedule. The edit method for three types of sounds is the same.
4. For the selection of **Detection Mode**
 - **High-Threshold Detection Mode**

Threshold greater than 50%: the false negative rate is low.
 - **Low-Threshold Detection Mode**

Threshold greater than 80%: the false positive rate is low.
5. Click **Save** to enable the settings.

6.8.9 Perimeter Protection

Configure Arming Schedule

In **Perimeter Protection** page, you will need to configure arming schedule.

Steps

1. Select **Arming Schedule**.

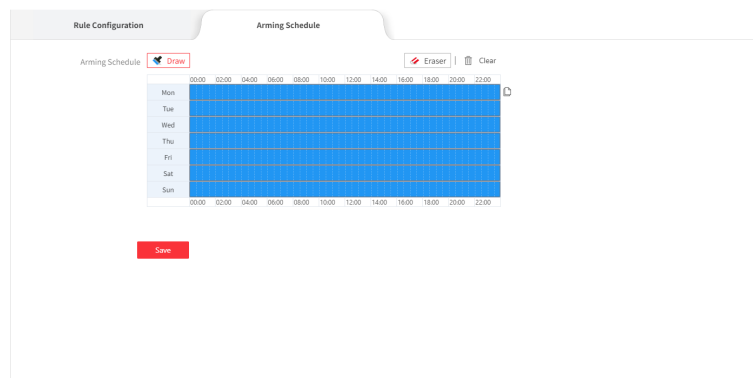


Figure 6-33 Arming Schedule

2. Click **Draw** or **Eraser** and slide on the chart to set arming schedule.



Note

Time periods shall not be repeated or overlapped.
You can click **Clear** to clear the drawn period..

3. Click **Save**.

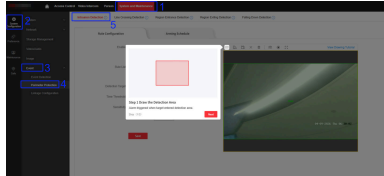
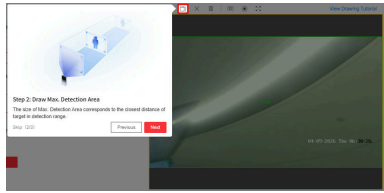
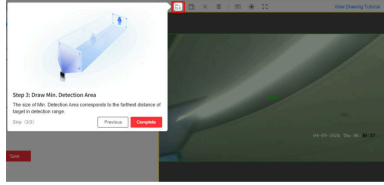
Intrusion Detection

Intrusion detection detects people, vehicles, or objects that enter and loiter in a pre-defined virtual region.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Event** → **Perimeter Protection** → **Intrusion Detection**.
2. When first enter this page, a notice will be displayed at the center. You can follow its instruction as it can tell you how to draw and adjust the detection area, how to draw the maximum and minimum drawing size. Click **Next** or **Previous** to read the instruction. Click **Complete** when finishing reading all four steps.

Table 6-1 Three Steps

Step	Tutorial Image
Step 1	
Step 2	
Step 3	

If you want to re-watch the drawing tutorial, you can click **View Drawing Tutorial** at the upper-right corner of the live-view window.

3. Slide to **Enable** or disable.
4. Set detection rules and detection areas.

Table 6-2 Icon Chart

Icon Image	Function
	Draw Detection Region
	Draw Max. Size
	Draw Min. Size
	Select the Area to Delete
	Clear All Drawn Areas

- 1) Set **Detection Area**, **Draw Min. Size** and **Draw Min. Size**.

- 2) Set **Time Threshold**. The time an object loitering in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm. Its range is [0-60s].
- 3) Set **Sensitivity**. The size of the object that can trigger the alarm. The higher the value is, the easier the detection alarm can be triggered. Its range is [1-100s].
- 4) **Optional**: Set **Detection Target** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
- 5) Set **Alarm Interval**. Range: 1 to 5s.
5. Set the arming schedule. Refer to for **Configure Arming Schedule** for details.
6. Click **Save**.

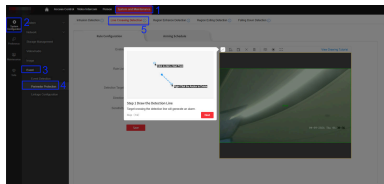
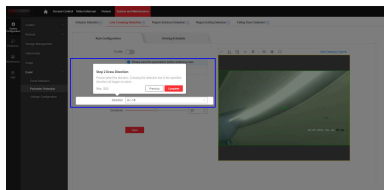
Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Steps

1. Go to **System and Maintenance → System Configuration → Event → Perimeter Protection → Line Crossing Detection**.
2. When first enter this page, a notice will be displayed at the center. You can follow its instruction as it can tell you how to draw and adjust the detection line, how to draw the direction. Click **Next** or **Previous** to read the instruction. Click **Complete** when finishing reading all four steps.

Table 6-3 Two Steps

Step	Tutorial Image
Step 1	
Step 2	

If you want to re-watch the drawing tutorial, you can click **View Drawing Tutorial** at the upper-right corner of the live-view window.

3. Slide to enable.
4. Set line crossing detection rules and detection direction.

Table 6-4 Icon Chart

Icon Image	Function
	Draw Detection Line
	Draw Max. Size
	Draw Min. Size
	Select the Area to Delete
	Clear All Drawn Areas

1) Draw **Detection Line**.

2) Select **Direction** as **A<->B**, **A->B**, or **A<-B**.

A<->B

Only the arrow on the B side shows. An object crossing a configured line in both directions can be detected and trigger alarms.

A->B

Only an object crossing the configured line from the A side to the B side can be detected.

B->A

Only an object crossing the configured line from the B side to the A side can be detected.

3) Set **Sensitivity**. The higher the value is, the easier the detection alarm will be triggered.
Range: 1~100.

4) **Optional**: Set **Detection Target** as **Human Body** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.

5) Click **Draw Area**, and set two points in the preview window to draw a virtual line.

5. Set the arming schedule. Refer to for **Configure Arming Schedule** for details.

6. Click **Save**.

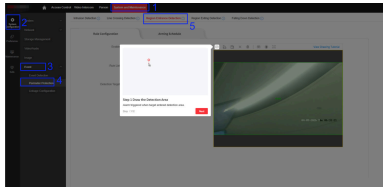
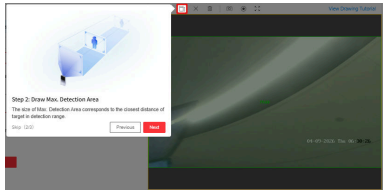
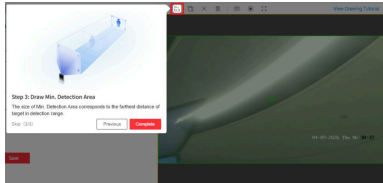
Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Event** → **Perimeter Protection** → **Region Entrance Detection**.
2. When first enter this page, a notice will be displayed at the center. You can follow its instruction as it can tell you how to draw and adjust the detection region, how to draw the maximum and minimum drawing size. Click **Next** or **Previous** to read the instruction. Click **Complete** when finishing reading all four steps.

Table 6-5 Three Steps

Step	Tutorial Image
Step 1	
Step 2	
Step 3	

If you want to re-watch the drawing tutorial, you can click **View Drawing Tutorial** at the upper-right corner of the live-view window.

3. Slide to **Enable** or disable.

4. Set detection rules and detection areas.

Table 6-6 Icon Chart

Icon Image	Function
	Draw Detection Region
	Draw Max. Size
	Draw Min. Size
	Select the Area to Delete
	Clear All Drawn Areas

1) Set **Detection Area**, **Draw Min. Size** and **Draw Min. Size**.

2) Optional: Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.

5. Set the arming schedule. Refer to for **Configure Arming Schedule** for details.

6. Click **Save**.

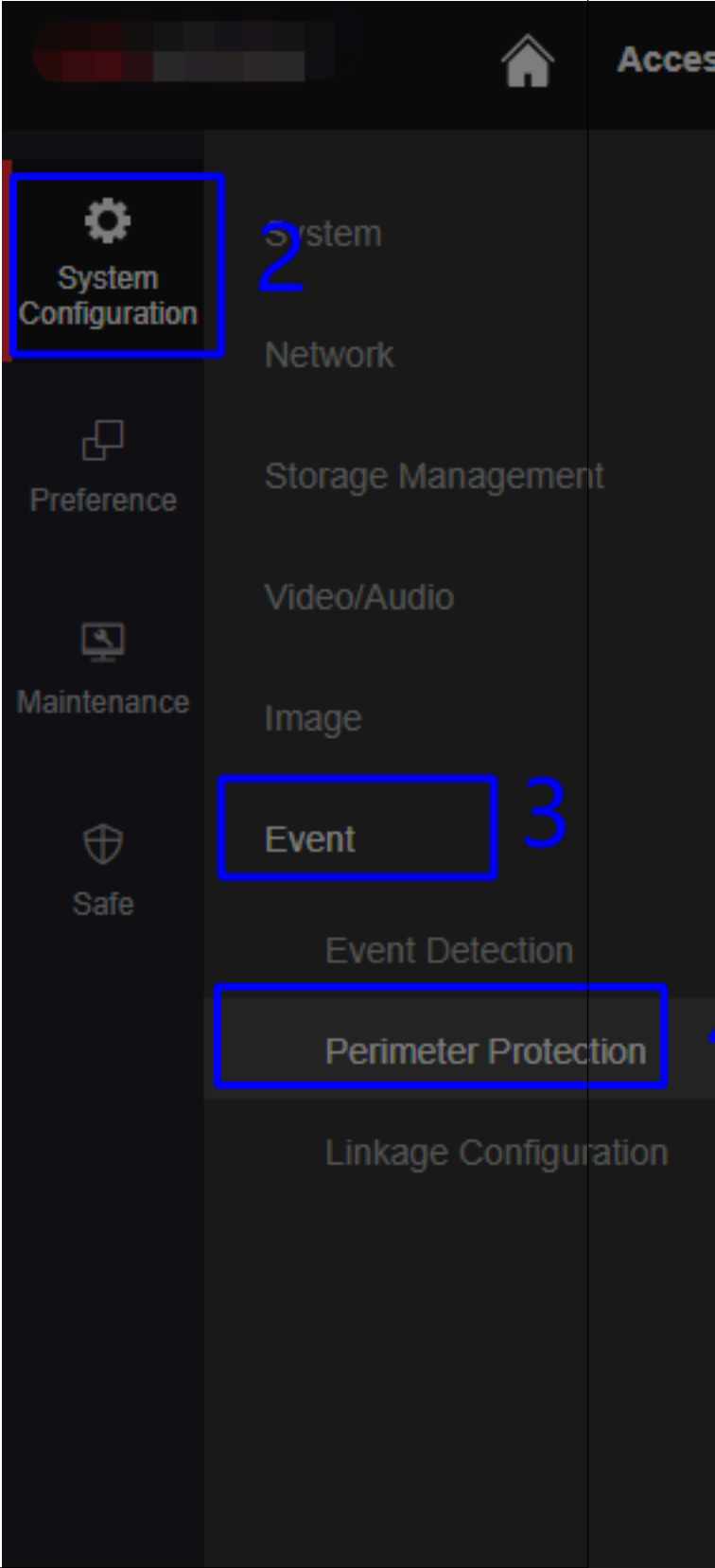
Region Exiting Detection

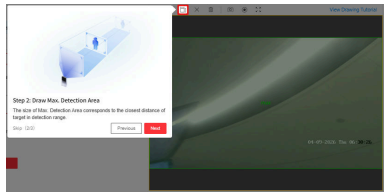
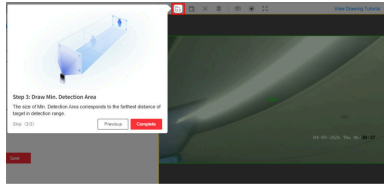
Region exiting detection detects objects that exit from a predefined virtual region.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Event** → **Perimeter Protection** → **Region Exiting Detection** .
2. When first enter this page, a notice will be displayed at the center. You can follow its instruction as it can tell you how to draw and adjust the detection region, how to draw the maximum and minimum drawing size. Click **Next** or **Previous** to read the instruction. Click **Complete** when finishing reading all four steps.

Table 6-7 Three Steps

Step	Tutorial Image
Step 1	 A screenshot of a dark-themed user interface for a video intercom system. The interface shows a sidebar menu on the left with icons for 'System Configuration' (gear), 'Preference' (two squares), 'Maintenance' (laptop), and 'Safe' (shield). The main area on the right lists options under 'System Configuration': 'System', 'Network', 'Storage Management', 'Video/Audio', 'Image', 'Event', 'Event Detection', 'Perimeter Protection', and 'Linkage Configuration'. Three blue boxes highlight the steps: 'System Configuration' (labeled with a large blue '2'), 'Event' (labeled with a large blue '3'), and 'Perimeter Protection' (labeled with a large blue '4').

Step	Tutorial Image
Step 2	
Step 3	

If you want to re-watch the drawing tutorial, you can click **View Drawing Tutorial** at the upper-right corner of the live-view window.

3. Slide to **Enable** or disable.
4. Set detection rules and detection areas.

Table 6-8 Icon Chart

Icon Image	Function
	Draw Detection Region
	Draw Max. Size
	Draw Min. Size
	Select the Area to Delete
	Clear All Drawn Areas

- 1) Set **Detection Area**, **Draw Min. Size** and **Draw Min. Size**.
- 2) **Optional**: Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
5. Set the arming schedule. Refer to for **Configure Arming Schedule** for details.
6. Click **Save**.

Falling-down Detection

Detect people in the area who falls down suddenly.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Event** → **Perimeter Protection** → **Falling Down Detection**.

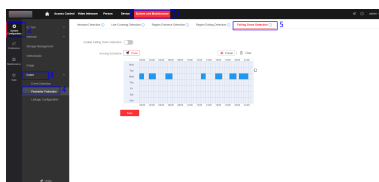


Figure 6-34 Falling Down Detection

2. Slide to enable or disable.
3. Set the arming schedule. Refer to for **Configure Arming Schedule** for details.
4. Click **Save**.

6.8.10 Event Linkage

Set linked actions for events.

Steps

1. Go to **System and Maintenance** → **System Configuration** → **Event** → **Linkage Configuration** → **Intrusion Detection**.

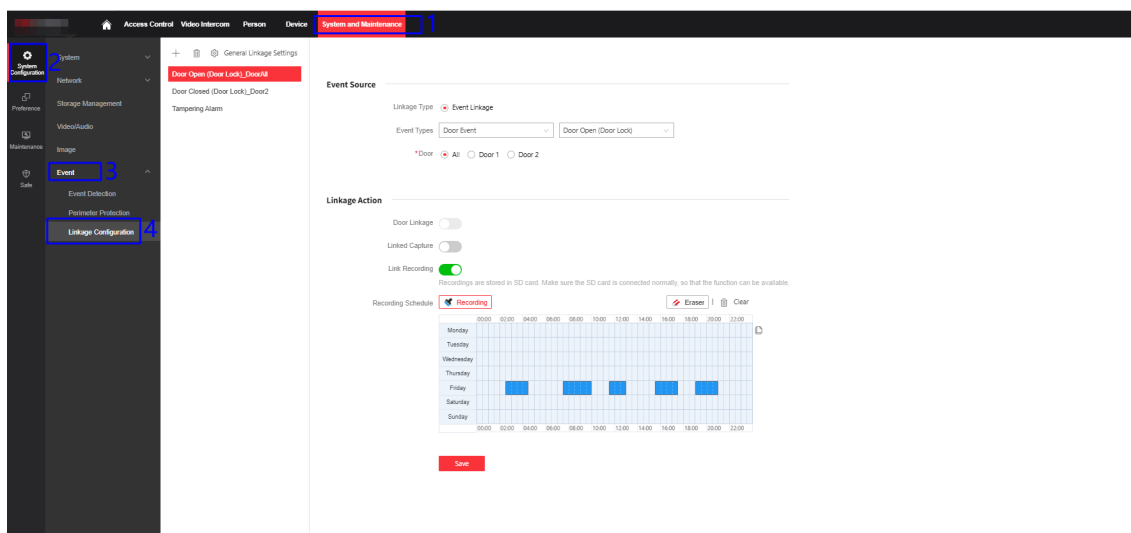


Figure 6-35 Linkage Configuration Overview

2. Click + to set event source. The default **Linkage Type** is **Event Linkage**, you need to select event types from the drop-down list.
 - **Device Event:** you need to select event types from the drop-down list. Tampering Alarm, Network Disconnected/ Recovered, Intrusion Detection, Line Crossing Detection, Region Entrance/ Exiting Detection, Falling Down Detection etc. are all included.
 - **Door Event:** you need to select event types from the drop-down list. Door Open/ Closed (Door Lock), Door Open/ Closed (Door Contact), Remote Unlock, Secure Door Control Unit Tampering Alarm etc. are all included.

- **Card Reader Event:** you need to select event types from the drop-down list. Duress Alarm, Authenticated via Valid Card, Card Invalid Currently, Expired Card, No Card No. Found etc. are all included.

3. Set linkage action.

Door Linkage

Enable **Door Linkage**, and select **Access Point 1** and **Access Point 2** for the target event. (Unlock/ Close/ Remain Open)

Linked Recording

Enable **Linked Recording** and set recording schedule.



Note

Recording schedule setting method is the same as arming schedule, refer to for **Configure Arming Schedule** for details.

Recordings are stored in SD card. Make sure the SD card is connected normally, so that the function can be available.

Linked Capture

Enable **Linked Capture** and select entrance or exit to capture for the target event.

6.8.11 Access Control Settings

Search Event

Click **Access Control** → **Event Search** to enter the page.

No.	Employee ID	Name	Card No.	Event Types	Time	Operation
1	--	-	--	Device Powering On	2022-07-06 09:32:04 08:00	-
2	--	-	--	Door Locked	2022-07-06 09:32:04 08:00	-
3	--	-	--	Device Tampered	2022-07-06 09:32:07 08:00	-
4	--	-	--	Authentication via Fingerprint Failed	2022-07-06 09:32:21 08:00	-
5	--	-	--	The password mismatches.	2022-07-06 09:54:24 08:00	-
6	--	-	--	The password mismatches.	2022-07-06 10:04:54 08:00	-
7	--	-	--	Network Disconnected	2022-07-06 10:05:05 08:00	-
8	--	-	--	Network Recovered	2022-07-06 10:05:08 08:00	-
9	--	-	--	Local Login	2022-07-06 10:06:06 08:00	-
10	--	-	--	Remote Login	2022-07-06 10:07:21 08:00	-
11	--	-	--	Remote Login	2022-07-06 10:12:50 08:00	-
12	--	-	--	Remote Login	2022-07-06 10:14:59 08:00	-
13	--	-	--	Remote Login	2022-07-06 10:20:46 08:00	-
14	--	-	--	Remote Login	2022-07-06 10:25:30 08:00	-
15	--	-	--	Remote Login	2022-07-06 10:37:30 08:00	-
16	--	-	--	Local Login	2022-07-06 10:40:55 08:00	-
17	--	-	--	Remote Login	2022-07-06 10:47:01 08:00	-
18	--	-	--	Remote Login	2022-07-06 11:05:29 08:00	-

Figure 6-36 Search Event

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

Set Access Schedule

You can name and add new access template on this page.

Steps

1. Click **Access Control** → **Time Schedule** → **Access Schedule** to enter this page.

	00:00	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00
Sun	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Mon	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Tue	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Wed	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Thu	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Fri	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period
Sat	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period	Access Time Period

Figure 6-37 Access Schedule

2. Click **+Add**. Then you can edit the name of the schedule.
3. Drag cursor on corresponding timestamp to map valid access period.
4. You can also click **Quick Operation** to apply existing template.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save** to save your settings.

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Access control** → **Time Schedule** → **Holiday Schedule** → **+Add** .

No.	Holiday Name	Holiday Time Period	Operation
1		2025/03/03 - 2025/03/03	

Figure 6-38 Holiday Schedule Template

2. Enter holiday name in the right column.
3. Set Start Date and End Date.
4. Drag cursor on corresponding timestamp to map valid holiday period.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save**.

Access Control

Set Door Parameters

Click **Access Control** → **Door Parameters** .

Door No.

*Door Name

Open Duration s

Relay Reverse ☒ Open ☐ Disable

Enable DTMF Custom ☒

If enabled, you can enter a custom value when making VoIP calls to unlock Lock 1 or Lock 2.

Lock 1

If enabled, you can enter 100 when making VoIP calls to unlock 1.

Lock 2

If enabled, you can enter 96 when making VoIP calls to unlock 2.

Figure 6-39 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Relay Reverse

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Enable DTMF Custom

DTMP: Dual-Tone Multi-Frequency, allows you to trigger predefined tasks on the device using buttons.

If enabled, you can enter a custom value when making VoIP calls to unlock Lock 1 or Lock 2.

Then you need to set the value for **Lock 1** and **Lock 2**, with which you can unlock lock 1 and lock 2 when making VoIP calls

Set Authentication Parameters

Set authentication related parameters, such as face recognition interval, bluetooth parameter, password settings etc.

Card Reader Parameter Configuration

Enable Face Authentication

Recognition Interval3

Bluetooth Parameter Configuration

Enable Bluetooth

*Device NameHIKDOOR_G05870380

Open Door via Bluetooth

To use the function, enable device Bluetooth first.

Password Settings

Person PIN

Person PIN ModePlatform-Applied Personal PINDevice-Set Personal PIN

Public Password

Public PINAddDelete

Password No.	Password Type	Enable Electric Lock	Remarks	Operation
No data.				

Save

Figure 6-40 Authentication Settings

Enable/Disable Bluetooth via PC Web

You can set to enable device bluetooth via PC Web.

Before You Start

You should add the device to mobile App before operation.

Steps

1. Click **Access Control** → **Access Control** → **Authentication Settings** to enter the settings page.
2. In the bluetooth parameter configuration section, slide to **Enable Bluetooth**.
3. Enter **Device Name**. After the bluetooth is connected, click **Save**. Enable **Open Door via Bluetooth**, you can control the door remotely.

Set Password on PC Web

You can configure personal PIN and public PIN on this page.

Steps

1. Click **Access Control** → **Access Control** → **Authentication Settings** .
2. If you want to set **Personal PIN**, select from **Platform-Applied Personal PIN** and **Device-Set Personal PIN**.
3. If you want to configure **Public Password**, click **+ Add** to add public password.
 - 1) Select **Password Type**.
 - 2) Enter the password and confirm the password.
 - 3) **Optional**: Add remarks for the password.
 - 4) Select Electric Lock.
4. Click **Save** to save the settings.

Set Face Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication.

Steps

1. Click **Access Control** → **Access Control** → **Authentication Settings** .



Note

The functions vary according to different models. Refers to the actual device for details.

2. Slide to enable **Enable Face Authentication**.
3. Set **Recognition Interval**. You can set the interval between 2 continuous recognition of a same person during the authentication. Range: 1 ~ 10 s.
4. Click **Save**.

Smart Settings

Enable/Disable Face with Mask Detection via PC Web

After enabling the face with mask detection, the system will recognize the captured face with mask picture or not.

Click **Access Control** → **Access Control** → **Smart** to enter the settings page.

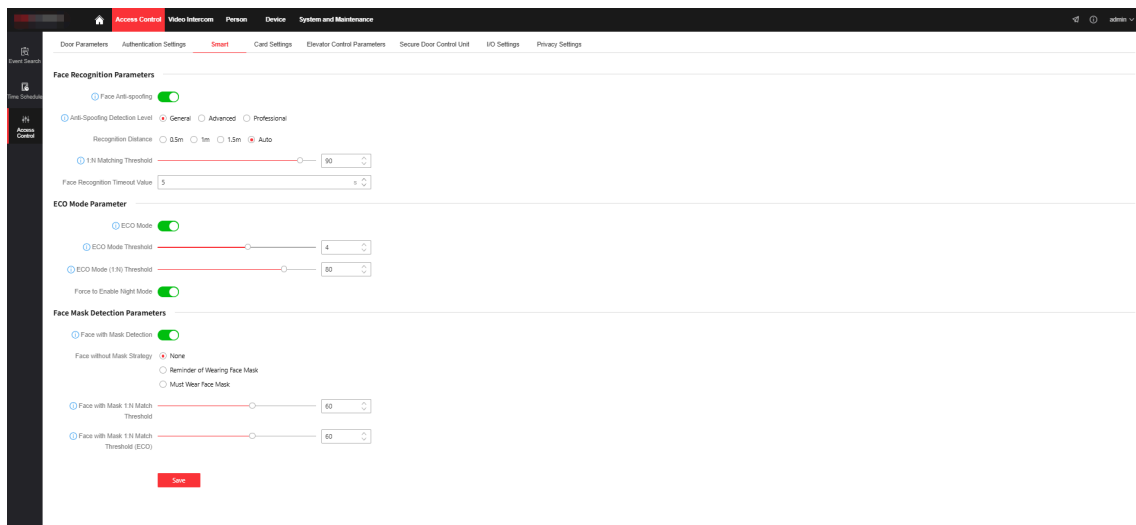


Figure 6-41 Smart Overview

After enabling the face with mask detection, you can set **Face without Mask Strategy**, **Face with Mask 1:N Match Threshold (ECO)**, and **Face with Mask 1:N Match Threshold (ECO)**.

Face without Mask Strategy

You can select **None**, **Reminder of Wearing Face Mask** and **Must Wear Face Mask** at the bottom of this page.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask&Face (1:N)

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:N matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

ECO Mode

To configure **ECO Mode Parameters**, you need to enable **ECO Mode** first.

After the ECO mode is enabled, the device will use the IR camera to authenticate faces in the low light or dark environment. After the ECO mode is disabled, the effect of face comparison will be lower in the low light or dark environment.

Force to Enable Night Mode

If enabled, the device automatically switches to night mode under specific conditions to optimize image quality in low-light environments.

ECO Mode Threshold

You can drag the bar or input a certain value in the right box to adjust the threshold. If you select a smaller value, it is harder for the device to enter the eco mode.

ECO Mode (1:N) Threshold

You can drag the bar or input a certain value in the right box to adjust the threshold. It's suggested to keep the device default value. Adjusting the value will affect the false acceptance rate and false rejection rate of face recognition.

Click **Save**.

Set Face Parameters

Tap **Access Control** → **Access Control** → **Smart** to enter the configuration page.



Note

The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Face Anti-spoofing

You can configure the parameters below at the top of this page, in **Face Recognition Parameters** section.

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.



Note

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Anti-Spoofing Detection Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Detection accuracy rankings: General < Advanced < Professional. When you select a mode with a higher detection accuracy, the passing efficiency will be lower.

Recognition Distance

Select the distance between the authenticating user and the device camera.

1:N Matching Threshold

Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Card Settings

Choose card types to enable.

Go to **Access Control** → **Access Control** → **Card Settings** .

Slide to enable card types and click **Save** to save the settings.

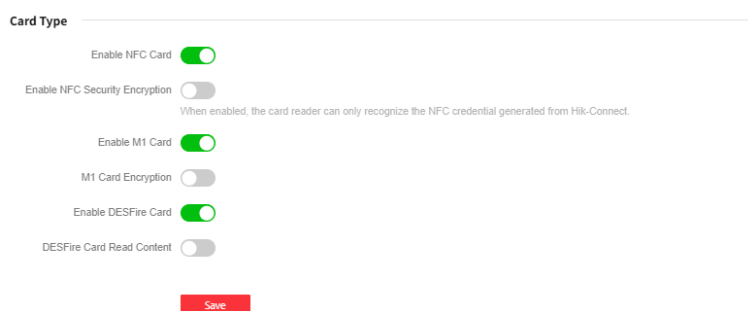


Figure 6-42 Card Type

Enable NFC Card

Enable the function and you can present the NFC card to authenticate. In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.



Note

Disable NFC card cannot completely avoid presenting NFC card.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Enable DESFire Card

DESFire Card Read Content: After enabling, the device can read DESFire card.



Note

Different models support different card types.

Only 3 lenses models support DESFire Card.

Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Click **Access Control** → **Privacy Settings** to enter this page.

Event Storage Settings

Event Storage Type

- ☐ Delete Old Events Periodically
- ☐ Delete Old Events by Specified Time
- ☒ Overwrite

Picture Uploading and Storage

Save Picture When Auth. ☒
If enabled, the captured picture when authentication will be saved to the device automatically.

Upload Picture When Auth. ☒
If enabled, the captured picture when authentication will be uploaded to the platform automatically.

Save Registered Picture ☒
If enabled, the captured face picture when registered will be saved to the device.

Clear All Pictures in Device

Clear Registered Face Pictures

Clear Captured Pictures

Figure 6-43 Privacy Settings

Upload Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Pic. When Auth. (Save Captured Picture When Authenticating)

If you enable this function, you can save the picture when Authenticating to the device.

Save Registered Pic. (Save Registered Picture)

The registered face picture will be saved to the system if you enable the function.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform. Tap **Save** to complete the settings.

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 10% events will be deleted when the system detects the stored events have taken the full space.

Clear All Pictures in Device



Note

All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

Elevator Control via PC Web

Steps

1. Click **Access Control** → **Access Control** → **Elevator Control Parameters** .

Elevator No.

Elevator Control ☒

Main Elevator Controller Model

Interface Type ☒ Network Interface

*Main Elevator Controller Address

Port

*User Name

*Password

Negative Floor Capacity

Installation Location ☒ Out of Elevator Cab ☐ In Elevator Cab

Call Elevator Mode ☐ Call Elevator Only ☒ Call Elevator + Authorize

Figure 6-44 Elevator Control

- 2. Select an elevator No., the parameters settings below will affect the selected elevator.
- 3. Enable **Elevator Control**.
- 4. Set the elevator parameters.

Main Elevator Controller Model

View the elevator model.

Interface Type

Select a communication type from the drop-down list for elevator communication.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select the device installation position. By default, it is **Out of Elevator Cab**.

Call Elevator Mode

Call Elevator Only

After person passes authentication on device, the device will call elevator to its floor.

Call Elevator+Authorize

After person passes authentication on device, the device will call elevator to its floor and authorize the permission of the floor linked to person room. The person can get to the target floor by pressing corresponding floor No.



Note

- Up to 4 elevator controllers can be connected to 1 device.
- Up to 10 negative floors can be added.
- Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.

Set I/O Parameters

You can set I/O Parameters on PC Web.

Steps

1. Click **Access Control** → **Access Control** → **I/O Settings** .

Input Settings

Input1 ☒ Door Contact

Input2 ☒ Disable ☐ Door Contact

Input3 ☒ Exit Button

Input4 ☒ Disable ☐ Exit Button

Output Settings

Output1 ☒ Electric Lock

Output2 ☒ Disable ☐ Electric Lock ☐ Doorbell

Save

Figure 6-45 I/O Settings

2. Select Input 2 as **Disable** or **Door Contact**. Set Input 4 as **Disable** or **Exit Button**.



Note

Because the device only has one lock. The Input 1 is **Door Contact** by default. Input 2 and 4 is set as **Disable** by default.

3. Select Output 2 as **Disable**, **Doorbell** or **Electric Lock**.



Note

The Output 2 is **Disable** by default.

Set Secure Door Control Unit Parameters via PC Web

You can set secure door control unit parameters.

Steps

1. Click **Access Control** → **Access Control** → **Secure Door Control Unit** .
2. You can slide to enable **Auto Binding**.



Note

If the function is enabled, the connected secure door control unit will be automatically bound to the door station and cannot be used for other door stations.

6.8.12 Video Intercom Settings

No. and System Network Settings

Device No. Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **No. and System Network Settings** to enter the page.

The screenshot displays the 'No. and System Network Settings' page for a Video Intercom Villa Door Station. The page is organized into two main sections: 'No. Settings' and 'Video Intercom Network'.

No. Settings

- Device Type: Villa Door Station (selected)
- *Floor No.: 10
- *Door Station No.: 0
- *Community No.: 1
- *Building No.: 1
- *Unit No.: 1

Video Intercom Network

- *Registration Password: [Input field]
- *Main Station IP: [Input field]
- *Private Server IP: [Input field]
- Enable Protocol 1.0: [Toggle switch, currently on]

A red 'Save' button is located at the bottom of the 'Video Intercom Network' section.

2. Select the device type from the drop-down list.
3. If select the device type as **Villa Door Station**, you need to set the corresponding information including **Building No.**, **Floor No.**, **Door Station No.**, **Community No.** and **Unit No.**
4. If select the device type as **Doorphone**. You only need to set **Building No.**, **Community No.** and **Unit No.**.
5. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **No. and System Network Settings** to enter the settings page.

The screenshot displays the 'Video Intercom Network Settings' page. The interface includes a sidebar on the left with 'Call Parameters' and 'Call Log'. The top navigation bar has 'Access Control', 'Video Intercom', 'Person', 'Device', and 'System and Maintenance'. Below this is a sub-navigation bar with 'No. and System Network Settings', 'Call Settings', 'Ringtone Settings', 'Press Button to Call', and 'VoIP'. The 'No. and System Network Settings' section contains fields for Device Type (Villa Door Station), Floor No. (10), Door Station No. (0), Community No. (1), Building No. (1), and Unit No. (1). A 'More' link is also present. The 'Video Intercom Network' section contains fields for Registration Password, Main Station IP, and Private Server IP, along with an 'Enable Protocol 1.0' toggle and a 'Save' button. Blue callout numbers 2, 3, and 4 highlight the 'No. and System Network Settings' tab, the 'Call Parameters' sidebar, and the 'Video Intercom Network' section respectively.

Figure 6-47 Video Intercom Network Settings

2. Set **Registration Password**.
3. Set **Main Station IP** and **Private Server IP**.
4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Duration Settings

Set the Max. call duration.

Go to **Video Intercom** → **Call Parameters** → **Call Settings** .

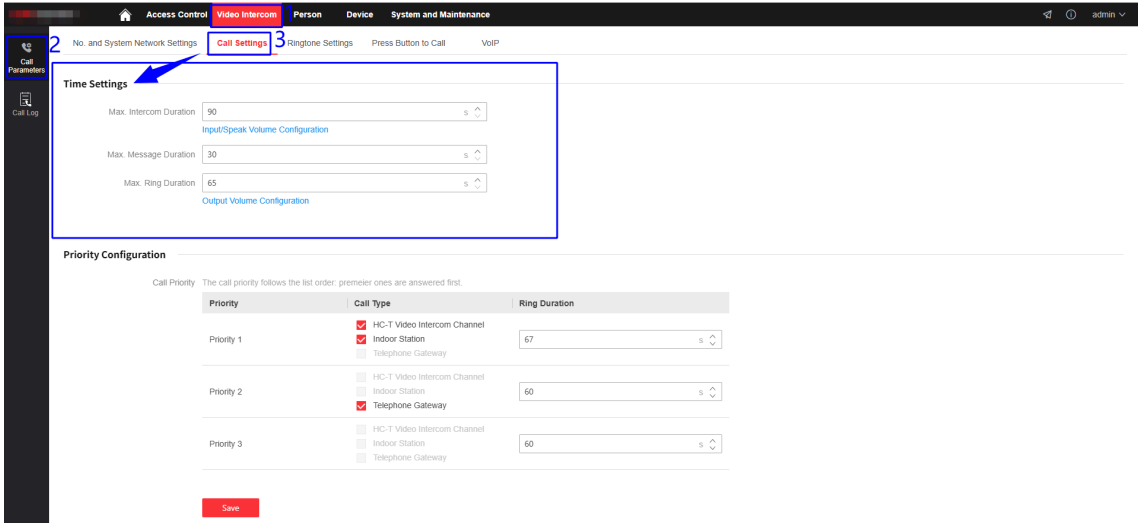


Figure 6-48 Time Settings

Set the **Max. Communication Time**, **Max. Message Duration** and **Max Ring Duration**.

Note

- The Max. communication time range is 90 s to 1800 s.
- The Max. message duration range is 30 s to 60 s.
- The Max. ring duration range is 65 s to 255 s.

Click **Save**.

Call Priority

Steps

1. Click **Video Intercom** → **Call Parameters** → **Call Settings** to enter the settings page.

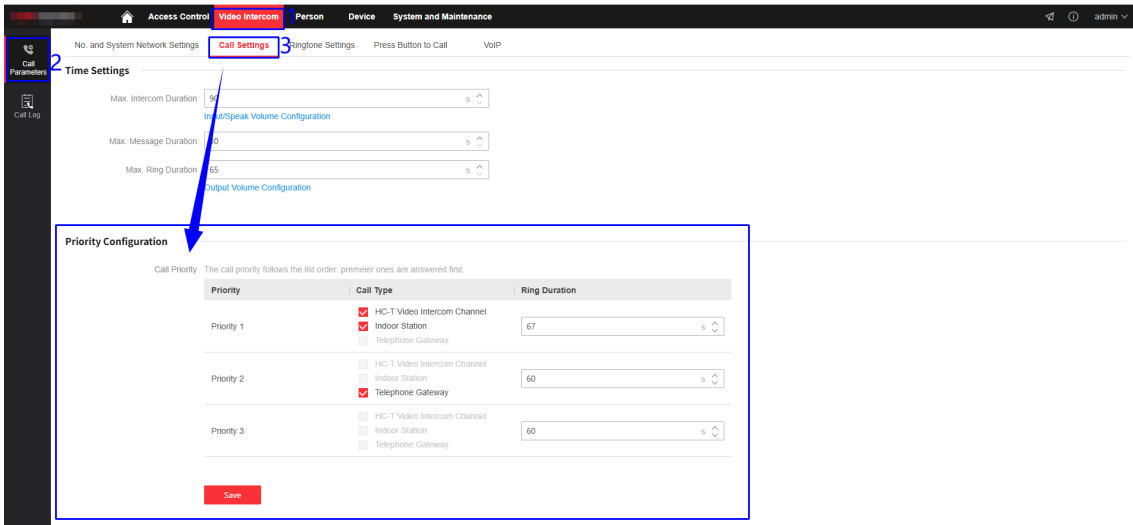


Figure 6-49 Priority Configuration

2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.



Note

The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Ringtone Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **Ringtone Settings** to enter the settings page.
2. Slide to enable **Ringtone**. Click  to import new ringtone.



Note

The supported audio file type for importing is .wav. The file should be less than 800 KB.

Press Button to Call

Steps

1. Click **Video Intercom** → **Call Parameters** → **Press Button to Call** to enter the settings page.

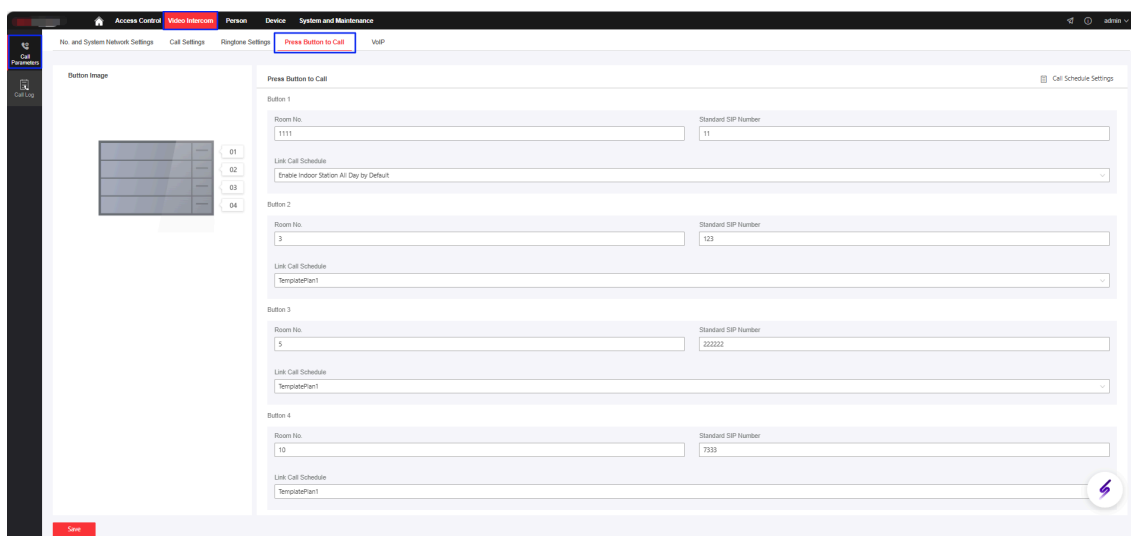


Figure 6-50 Press Button to Call

2. You can configure each button one by one. Fill in **Room No.** and **Standard SIP Number** then select a appropriate **Link Call Schedule** from the drop-down list.
3. **Link Call Schedule:** Select time schedule plan from the drop-down list.



Note

If you want to add new time template, click **Call Schedule Settings** at the upper-right corner of this page, then you can add or edit the template.

4. Click **Save** to enable the settings.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **Video Intercom → Call Parameters → VoIP → Basic Configuration** .

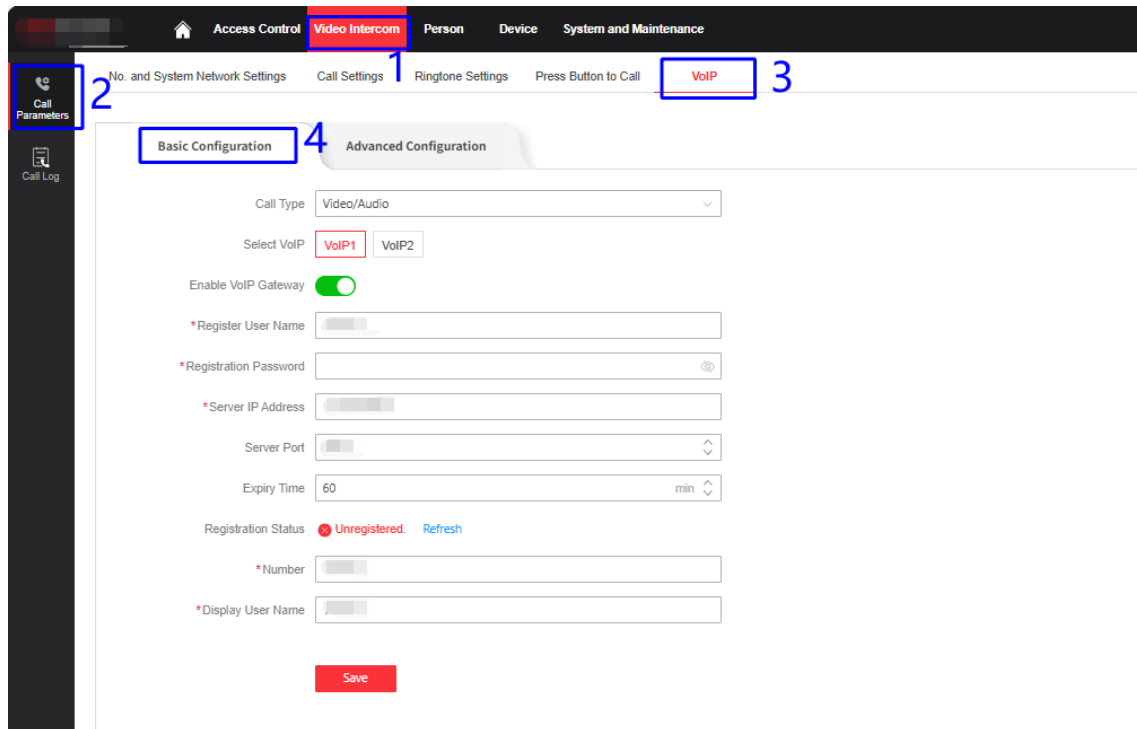


Figure 6-51 Basic Configuration-VoIP

2. Slide to **Enable VoIP Gateway**.
3. Set **Register User Name**, **Registration Password**, **Server IP Address**, **Server Port**, **Expiry Time**, **Register Status**, **Number**, **Display User Name**, and **Center No**.
4. Click **Save**.

SIP No. and P2P No. Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **VoIP** → **Advanced Configuration** to enter the settings page.

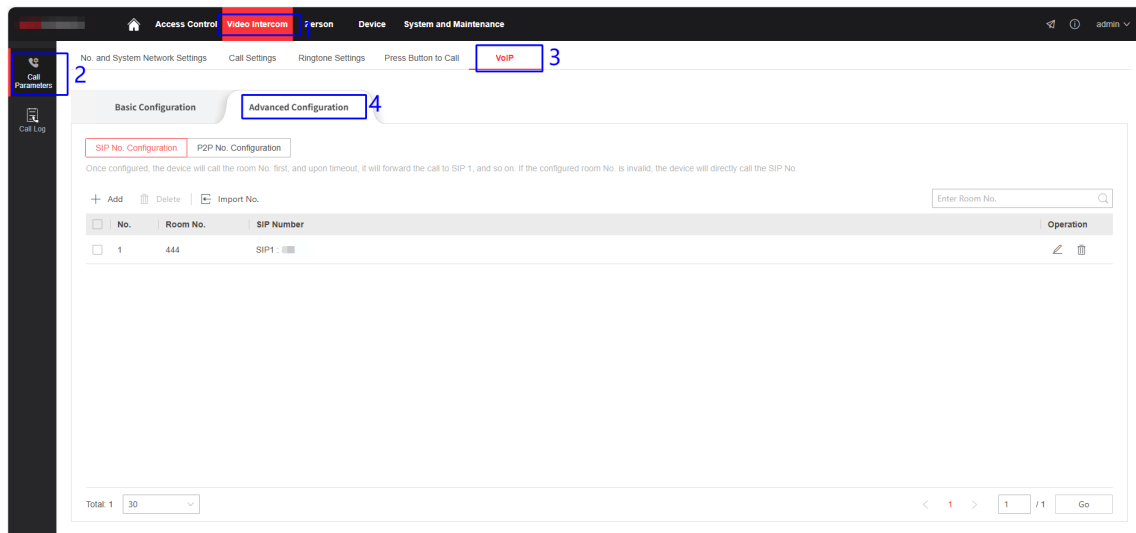


Figure 6-52 Advanced Configuration-VoIP

2. If you want to configure SIP No. Click **+ Add** to add the SIP No. to the device.
 - 1) Select an item, and click **Configure** to edit the parameters.
 - 2) **Optional:** Select SIP numbers in the list, and click **Delete** to delete the selected informations.
 - 3) **Optional:** Click **Clear** to clear the informations in the list.
3. If you want to configure P2P No. Slide to enable P2P first.
 - 1) Fill in the room No., IP Address and port. Click **Save**.
 - 2) **Optional:** Select P2P numbers in the list, and click **Delete** to delete the selected informations.
 - 3) **Optional:** Click **Clear** to clear the informations in the list.

Chapter 7 Configuration via Client Software

7.1 Device Management

Device management includes device activation, adding device, editing device, and deleting device, and so on.

After running the iVMS-4200, video intercom devices should be added to the client software for remote configuration and management.

7.1.1 Add Online Device

Before You Start

Make sure the device to be added is in the same subnet with your computer. Otherwise, please edit network parameters first.

Steps

1. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter corresponding information, and click **Add**.

Add ✕

Adding Mode

☒ IP/Domain

☐ IP Segment

☐ Cloud P2P

☐ EHome

☐ HiDDNS

☐ Batch Import

Add Offline Device

☐

* Name

* Address

* Port

* User Name

admin

* Password

●●●●●●●●

Synchronize Time

☒

Import to Group

☒

ⓘ Set the device name as the group name and add all the channels connected to the device to the group.

Add and New

Add

Cancel

Figure 7-1 Add to the Client

7.1.2 Add Device by IP Address

Steps

1. Click **+Add** to pop up the adding devices dialog box.
2. Select **IP/Domain** as **Adding Mode**.
3. Enter corresponding information.
4. Click **Add**.

7.1.3 Add Device by IP Segment

You can add many devices at once whose IP addresses are among the IP segment.

Steps

1. Click **+Add** to pop up the dialog box.
2. Select **IP Segment** as **Adding Mode**.
3. Enter corresponding information, and click **Add**.

7.2 Live View via Door Station

Steps

1. On the main page of the client software, click **Main View** to enter the Live View page.
2. In the left list of the window, double-click the device IP or click the play icon to live view.
3. **Optional:** On the Live View page, control-click and select **Capture** to get the picture of the live view.

7.3 Organization Management

On the main page of the Client Software, click  **Personal Management** to enter the configuration page.

7.3.1 Add Organization

Steps

1. In the organization list on the left, click **+Add**.
2. Enter the **Organization Name** as desired.
3. Click **OK** to save the adding.
4. **Optional:** You can add multiple levels of organizations according to the actual needs.
 - 1) You can add multiple levels of organizations according to the actual needs.
 - 2) Then the added organization will be the sub-organization of the upper-level organization.



Note

Up to 10 levels of organizations can be created.

7.3.2 Modify and Delete Organization

You can select the added organization and click  to modify its name.

You can select an organization, and click **X** button to delete it.



Note

- The lower-level organizations will be deleted as well if you delete an organization.
 - Make sure there is no person added under the organization, or the organization cannot be deleted.
-

7.4 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc.



Note

- Up to 2,000 persons can be added.
 - Up to 5 cards can be added to each person.
-

7.4.1 Add Person

Person information is necessary for the video intercom system. And when you set linked device for the person, the intercom between intercom devices can be realized.

Steps

1. Select an organization in the organization list and click **Add** on the Person panel to pop up the adding person dialog.
-



Note

The Person No. will be generated automatically and is editable.

2. Set basic person information.
 - 1) Enter basic information: name, tel, birthday details, effective period and email address.
-



Note

The length of person name should be less than 15 characters.

- 2) Click **Add** face to upload the photo.
-

Note

The picture should be in *.jpg format.

Click Upload Select the person picture from the local PC to upload it to the client.

Click Take Phone Take the person's photo with the PC camera.

Click Remote Collection Take the person's photo with the collection device.

3. Issue the card for the person.

- 1) Click **Credential → Card**.
- 2) Click **+** to pop up the Add Card dialog.
- 3) Select **Normal Card** as **Card Type**.
- 4) Enter the **Card No.**
- 5) Click **Read** and the card(s) will be issued to the person.

4. Link the device to the person.

- 1) Set the linked devices.

Linked Device

You can bind the indoor station to the person.

Note

If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

Room No.

You can enter the room No. of the person.

- 2) Click **OK** to save the settings.

5. Click **Add** to save the settings.

7.4.2 Modify and Delete Person

Select the person and click **Edit** to open the editing person dialog.

To delete the person, select a person and click **Delete** to delete it.

Note

If a card is issued to the current person, the linkage will be invalid after the person is deleted.

7.4.3 Change Person to Other Organization

You can move the person to another organization if needed.

Steps

1. Select the person in the list and click **Change Organization**.
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

7.4.4 Import and Export Person Information

The person information can be imported and exported in batch.

Steps

1. Exporting Person: You can export the added persons' information in Excel format to the local PC.
 - 1) After adding the person, you can click **Export Person** to pop up the following dialog.
 - 2) Click ... to select the path of saving the exported Excel file.
 - 3) Check the checkboxes to select the person information to export.
 - 4) Click **OK** to start exporting.
2. Importing Person: You can import the Excel file with persons information in batch from the local PC.
 - 1) Click **Import Person**.
 - 2) You can click **Download Template for Importing Person** to download the template first.
 - 3) Input the person information to the downloaded template.
 - 4) Click ... to select the Excel file with person information.
 - 5) Click **OK** to start importing.

7.4.5 Get Person Information from Device

If the added device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

Steps



Note

This function is only supported by the device the connection method of which is TCP/IP when adding the device.

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get from Device** to pop up the dialog box.
3. The added device will be displayed.
4. Click to select the device and then click **Get** to start getting the person information from the device.



Note

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
 - If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
-

7.4.6 Issue Card in Batch

You can issue multiple cards for the person with no card issued in batch.

Steps

1. Click **Batch Issue Cards** to enter the dialog page. All the added person with no card issued will display in the Person(s) with No Card Issued list.

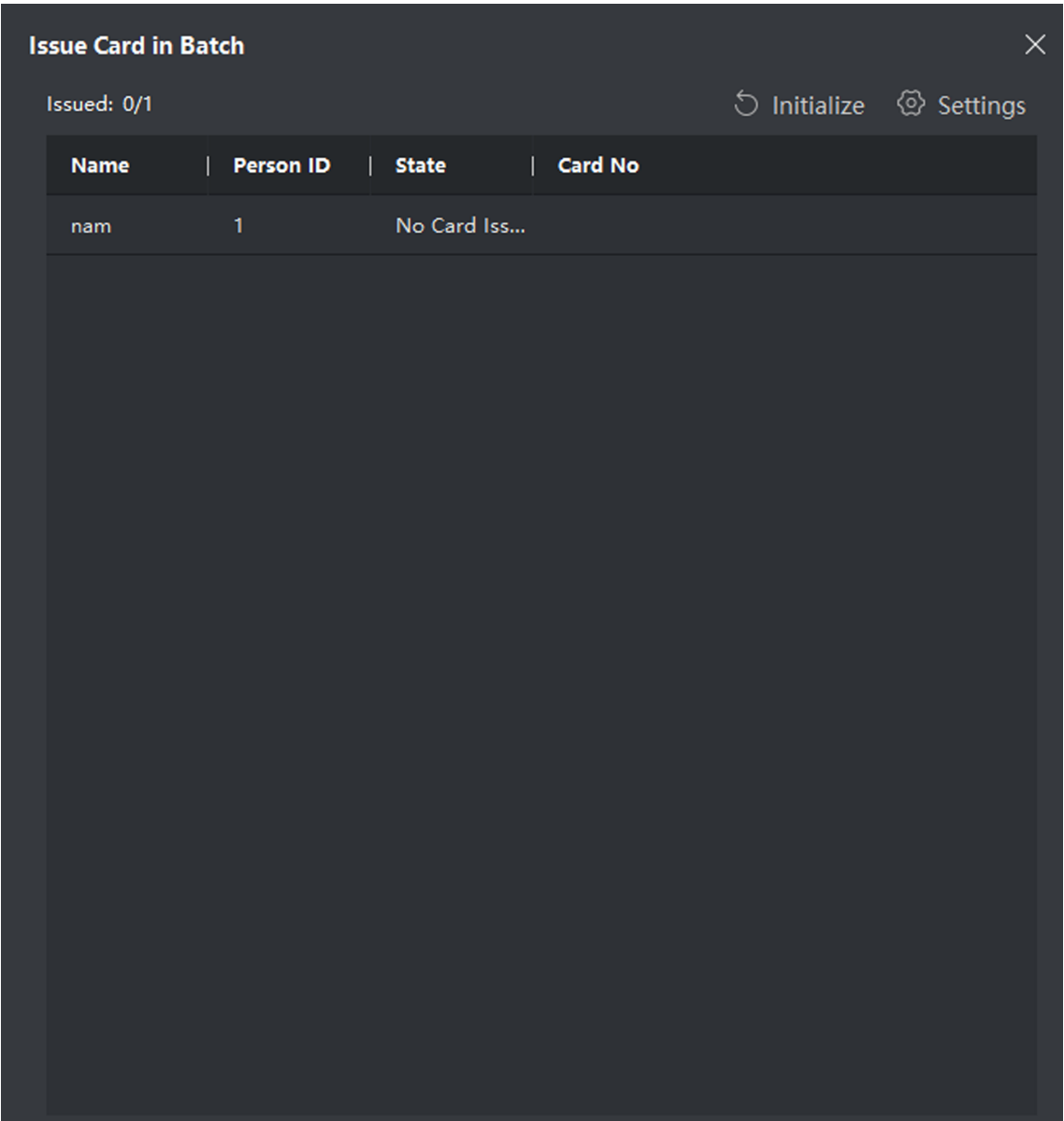


Figure 7-2 Issue Card in Batch

2. Click **Settings**.

Settings [X]

Mode ☒ Local ☐ Remote

Card Enrollment Station [Dropdown]

Card Type [Dropdown]

Buzzing ☒

Card No. Type [Dropdown]

M1 Card Encryption ☐

OK Cancel

Figure 7-3 Card Settings

3. Select **Card Type** and **Card No. Type**.
4. Click **OK** to save the settings.

Result

After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.

7.5 Video Intercom Settings

The Video Intercom Management module provides the function of video intercom, checking call logs and managing notice via the iVMS-4200 Client Software.

Note

For the user with access control module permissions, the user can enter the Access Control module and manage video intercom and search information.

You should add the device to the software and configure the person to link the device in Access Control module before your configuration remotely.

On the main page, click  **AccessControlInfo** → **Video Intercom** → **Video Intercom** on the left bar to enter the Video Intercom page.

7.5.1 Receive Call from Door Station

Steps

1. Select the client software in the page to start calling the client and an incoming call dialog will pop up in the client software.
2. Click **Answer** to answer the call. Or click **Hang Up** to decline the call.
3. After you answer the call, you will enter the In Call page.

Adjust the Volume of Loudspeaker

Click  to adjust the volume of loudspeaker.

Hang Up

Click **Hang Up** to hang up.

Adjust the Volume of Microphone

Click  to adjust the volume of microphone.

Unlock Remotely

For door station, you can click  to open the door remotely.

Note

- One video intercom device can only connect with one client software.
 - The maximum ring duration can be set from 15s to 60s via the Remote Configuration of the video intercom device.
 - The maximum speaking duration between indoor station and iVMS-4200 can be set from 120s to 600s via the Remote Configuration of indoor station.
 - The maximum speaking duration between door station and iVMS-4200 can be set from 90s to 120s via the Remote Configuration of door station.
-

7.5.2 Release Notice

You can create different types of notices and send them to the residents. Four notice types are available, including Advertising, Property, Alarm and Notice Information.

Before You Start

Make sure the person has been added to the client.

Steps

1. On the video intercom settings page, click **Notice** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Select the person according to your needs.
4. Edit the **Subject**, **Type** and **Information**.
5. Click **View** to select the picture.
6. Click **Send**.



Note

- Up to 63 characters are allowed in the Subject field.
 - Up to 6 pictures in the JPGE format can be added to one notice. And the maximum size of one picture is 512KB.
 - Up to 1023 characters are allowed in the Information field.
-

7.5.3 Search Video Intercom Information

Search Call Logs

Steps

1. On the Video Intercom page, click **Call Log** to enter the page.

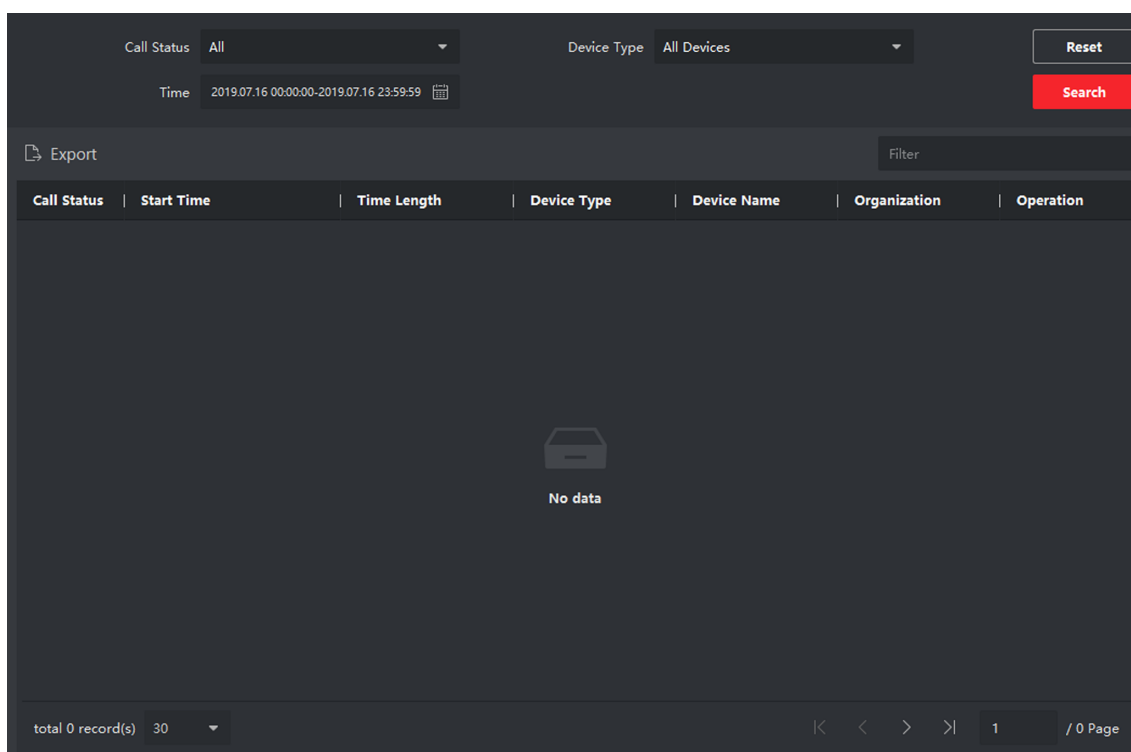


Figure 7-4 Search Call Logs

2. Set the search conditions, including call status, device type, start time and end time.

Call Status

Click ▼ to unfold the drop-down list and select the call status as **Dialed**, **Received** or **Missed**. Or select **All** to search logs with all statuses.

Device Type

Click ▼ to unfold the drop-down list and select the device type as **Indoor Station**, **Door Station**, **Outer Door Station** or **Analog Indoor Station**. Or select **All Devices** to search logs with all device types.

Start Time/End Time

Click the time icon to specify the start time and end time of a time period to search the logs.

Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and all the matched call logs will display on this page.
4. **Optional:** Check the detailed information of searched call logs, such as call status, ring/speaking duration, device name, resident organization, etc.
5. **Optional:** Input keywords in the Search field to filter the desired log.
6. **Optional:** Click **Export** to export the call logs to your PC.

Search Notice

Steps

1. On the Video Intercom page, click **Notice** to enter the page.
2. Set the search conditions, including notice type, start time and end time.

Type

Select **Advertising Information**, **Property Information**, **Alarm Information** or **Notice Information** as **Type** according to your needs.

Start Time/End Time

Click the time icon to specify the start time and end time of a time period to search the logs.

Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and the matched notice will display on this page.
4. **Optional:** Click **Export** to export the notices to your PC.

7.5.4 Upload Armed Information

Steps

1. On the main page, click upper right  → **Tool** → **DeviceGuard** to enter the page.
2. Enable to arm or disarm the device.



Note

- While device has been added to the client software, the device armed by default.
- When the device is armed, the alarm logs upload to the client software automatically.
- Click **Alarm Application** → **Event Search** to search the alarm logs.

-
3. **Optional:** Click **Arm All** or **Disarm All** to arm or disarm all the device.

Chapter 8 Video Intercom Operation

8.1 Call Resident

You can press the call button of the door station to call resident.



- Make sure you have added contacts to the device.
 - Make sure you have configured the room No. for the call button. For more details. please refer to: **Press Button to Call**
-

8.2 Unlock Door

After issuing card, you can swipe card on the card reading area to unlock the door.

You can swipe card on the card reading area to unlock the door.



Make sure you have issued cards for the device.

- Issue card via Client Software:
 - **Add Person**
 - **Issue Card in Batch**
 - Issue card via web client:
-



See Far, Go Further