



Door Station

User Manual

Legal Information

©2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 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 INSPECTION, 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

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.
- 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.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in 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 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.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.

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.

This equipment complies with FCC/IC RSS-102 radiation exposure limits set forth for an uncontrolled environment.

ce matériel est conforme aux limites de dose d'exposition aux rayonnements, FCC / CNR-102 énoncée dans un autre environnement.

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.

Contents

1 Appearance Description	1
1.1 Appearance of 80 Series Door Station	1
1.2 Appearance of 81 Series Door Station	2
1.3 Appearance of 30 Series Door Station	2
2 Terminal and Wiring Description	4
2.1 Terminal Description	4
2.2 Wiring Description	6
2.2.1 D-Series Door Lock Wiring	6
2.2.2 D-Series Door Contact Wiring (8081 Series)	6
2.2.3 D-Series Exit Button Wiring (8081 Series)	7
2.2.4 External Card Reader Wiring	8
2.2.5 D-Series Elevator Controller Wiring	10
2.2.6 Alarm Input Device Wiring	10
2.2.7 Alarm Output Device Wiring	11
3 Installation	13
3.1 Installation of 80 Series Door Station	13
3.1.1 Gang Box for 80 Series Door Station	13
3.1.2 Flush Mounting with Gang Box	13
3.2 Installation of 81 Series Door Station	16
3.2.1 Gang Box for 81 Series Door Station	16
3.2.2 Flush Mounting with Gang Box	17
3.3 Installation of 30 Series Door Station	18

3.3.1 Gang Box of 30 Series Door Station	19
3.3.2 Flush Mounting with Gang Box	19
4 Activation	22
4.1 Activate Device Locally	22
4.2 Activate Device via Client Software	23
4.3 Activate Device via Web	24
5 Local Operation	25
5.1 Local Configuration	25
5.1.1 Edit Network Parameters	25
5.1.2 Door Station Settings	25
5.1.3 Add Residents	26
5.1.4 About	27
5.2 Video Intercom Operation	27
5.2.1 Call Resident	27
5.2.2 Call Center	28
5.3 Unlock Door	28
5.3.1 Unlock by Password	28
5.3.2 Unlock by Presenting Card	29
5.3.3 Unlock by Fingerprint	29
5.3.4 Unlock by QR Code	29
6 Remote Configuration via Web	31
6.1 Live View	31
6.2 User Management	31
6.3 Device Management	32

6.4 Parameters Settings	32
6.4.1 Local Parameters Settings	32
6.4.2 System Settings	34
6.4.3 Network Settings	36
6.4.4 Video & Audio Settings	41
6.4.5 Display Settings	43
6.4.6 Event Settings	44
6.4.7 Intercom Settings	47
6.4.8 Access Control Settings	49
7 Configuration via Client Software	54
7.1 Edit Network Parameters	54
7.2 Add Device	54
7.2.1 Add Online Device	54
7.2.2 Add Device by IP Address	55
7.2.3 Add Device by IP Segment	55
7.3 Remote Configuration	56
7.4 Device Management	56
7.5 Organization Management	56
7.5.1 Add Organization	56
7.5.2 Modify and Delete Organization	57
7.6 Person Management	57
7.6.1 Add Person	57
7.6.2 Modify and Delete Person	59
7.6.3 Import and Export Person Information	59

7.6.4 Get Person Information from Device	59
7.6.5 Change Person to Other Organization	60
7.6.6 Add Person in Batch	60
7.6.7 Issue Card in Batch	61
7.6.8 Permission Settings	62
7.7 Video Intercom Settings	63
7.7.1 Receive Call from Door Station	63
7.7.2 Live View via Door Station	64
7.7.3 Release Notice	64
7.7.4 Search Video Intercom Information	65
A. Communication Matrix and Device Command	67

1 Appearance Description

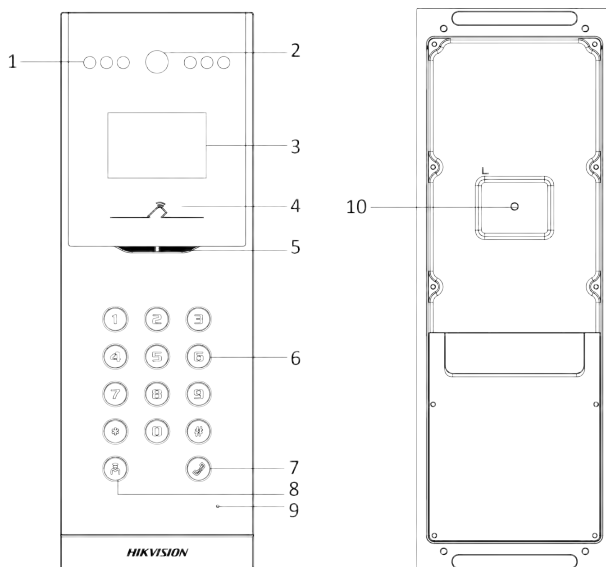


Figure 1-1 Appearance of 80 Series Door Station

Table 1-1 Descriptions

No.	Description	No.	Description
1	Low Illumination Supplement Light	6	Keypad
2	Built-in Camera	7	Call Button
3	LCD Display Screen	8	Microphone
4	Card Reading Area	9	Call Center Button
5	Loudspeaker	10	TAMPER

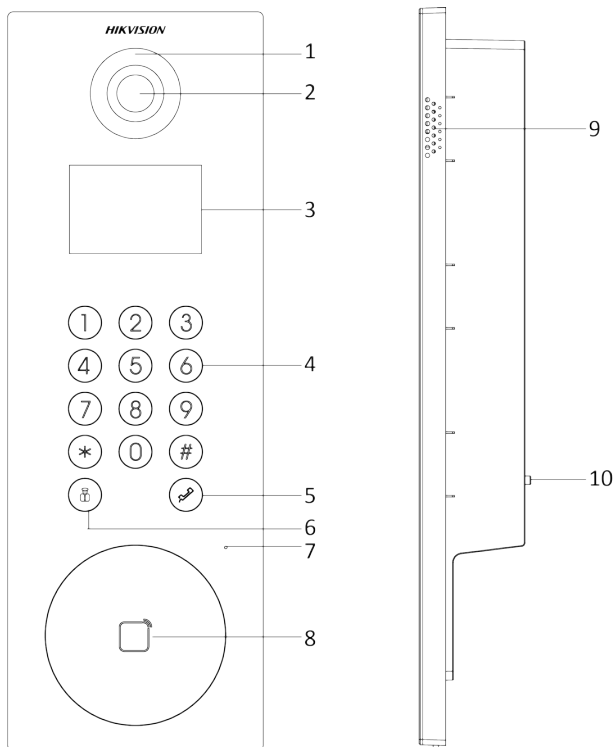


Figure 1-2 Appearance of 81 Series Door Station

Table 1-2 Descriptions

No.	Descripton	No.	Description
1	Low Illumination Supplement Light	6	Call Center Button
2	Built-in Camera	7	Microphone
3	LCD Display Screen	8	Card Reading Area
4	Keypad	9	Loudspeaker
5	Call Button	10	TAMPER

Appearance of 30 Series Door Station

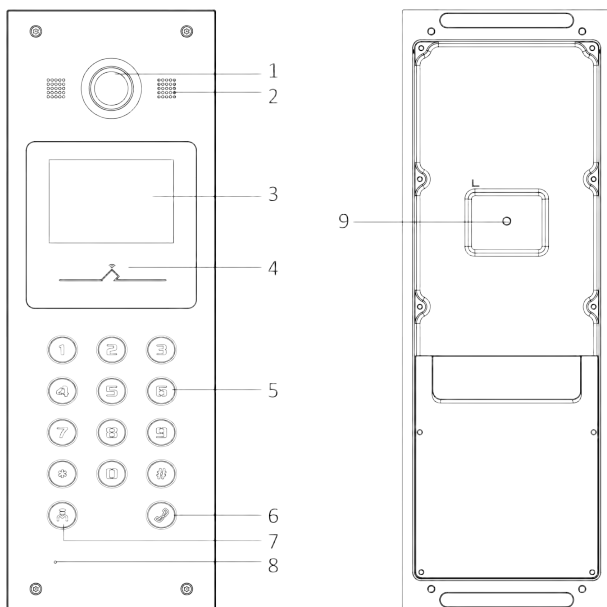


Table 1-3 Descriptions

No.	Description	No.	Description
1	Low Illumination Supplement Light	6	Call Button
2	Loudspeaker	7	Call Center Button
3	LCD Display Screen	8	Microphone
4	Card Reading Area	9	TAMPER
5	Keypad		

2 Terminal and Wiring Description

2.1 Terminal Description

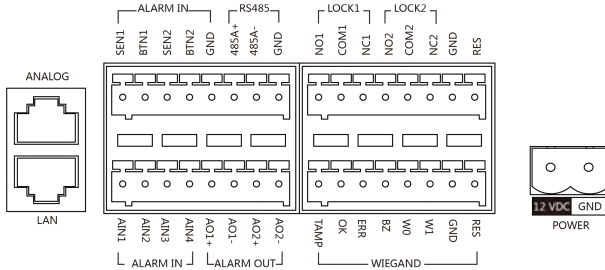


Figure 2-1 Terminal Description

Table 2-1 Descriptions

Name	Interface	Description
LAN	ANALOG	Analog Interface
	LAN	Network Interface
ALARM IN	SEN1	Door Contact Detection Input 1/Door Contact
	BTN1	Door Contact Detection Input 1/Door Contact
	SEN2	Door Contact Detection Input 2/Door Contact
	BTN2	Door Contact Detection Input 2/Door Contact
	GND	Grounding
	AIN1	Alarm Input 1
	AIN2	Alarm Input 2
	AIN3	Alarm Input 3
	AIN4	Alarm Input 4
RS485	485A+	RS-485 Communication Interfaces

Name	Interface	Description
	485A-	
	GND	Grounding
LOCK1	NO1	Door Lock Relay Output (NO)
	COM1	Common Interface
	NC1	Door Lock Relay Output (NC)
LOCK2	NO2	Door Lock Relay Output (NO)
	COM2	Common Interface
	NC2	Door Lock Relay Output (NC)
ALARM OUT`	AO1+	Alarm Relay Output 1
	AO1-	
	AO2+	Alarm Relay Output 2
	AO2-	
WIEGAND	TAMP	Tamper-proof Input of Wiegand Card Reader
	OK	Card Reader Indicator Output (Valid Card Output)
	ERR	Card Reader Indicator Output (Invalid Card Output)
	BZ	Card Reader Buzzer Output
	W0	Data Input Interface Wiegand Card Reader: Data 0
	W1	Data Input Interface Wiegand Card Reader: Data 1
	GND	Grounding
	RES	Reserved
RESERVED	GND	Grounding

Name	Interface	Description
	RES	Reserved
POWER	12 VDC	DC 12 V Power Supply Input

2.2 Wiring Description

2.2.1 D-Series Door Lock Wiring

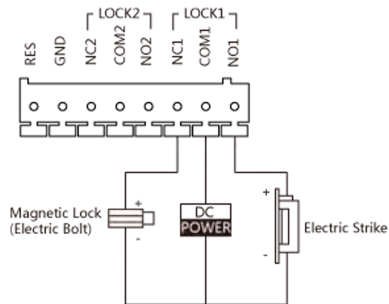


Figure 2-2 Door Lock Wiring

Note

- Terminal NC1/COM1 is set as default for accessing 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 D-Series Door Contact Wiring (8081 Series)

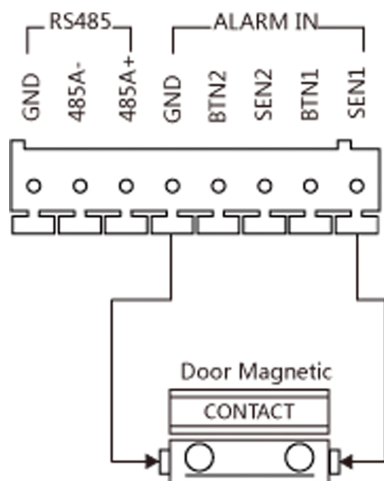


Figure 2-3 Door Contact Wiring

 Note

Terminal SEN1/SEN2 can both connect to door contact.

2.2.3 D-Series Exit Button Wiring (8081 Series)

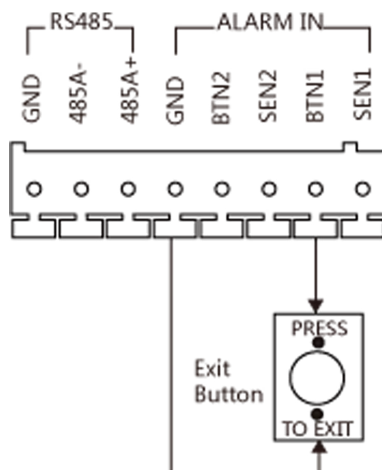


Figure 2-4 Exit Button Wiring

Note

Terminal BTN1/BTN2 can both connect to exit button.

2.2.4 External Card Reader Wiring

Note

- Please set the DIP switch first before connecting the card reader.
- If the DIP switch should be configured when the card reader is power-on, please reboot the card reader after configuring the DIP switch.
- The DIP switch description is shown in the following table:

Table 2-2 DIP Switch Description

No.	Description	How to Configure
1 to 4	Set the RS-485 address	ON: 1 OFF: 0
6	Select Wiegand protocol or RS-485 protocol	ON: Wiegand

No.	Description	How to Configure
		OFF: RS-485
7	Set the Wiegand protocol (It is invalid when setting OFF in 6.)	ON: Wiegand 26 OFF: Wiegand 34

RS-485 Card Reader Wiring

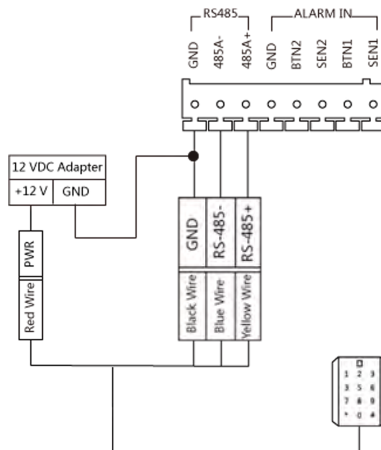


Figure 2-5 RS-485 Card Reader Wiring

Note

When card reader is accessed via RS-485, the door station cannot connect to elevator controller.

Wiegand Card Reader Wiring

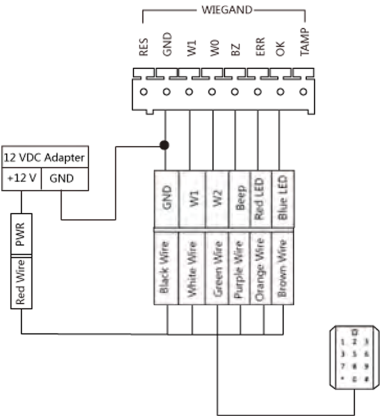


Figure 2-6 Wiegand Card Reader Wiring

2.2.5 D-Series Elevator Controller Wiring

Enter a short description of your concept here (optional).

This is the start of your concept.

2.2.6 Alarm Input Device Wiring

The alarm input wiring diagram is as follows:

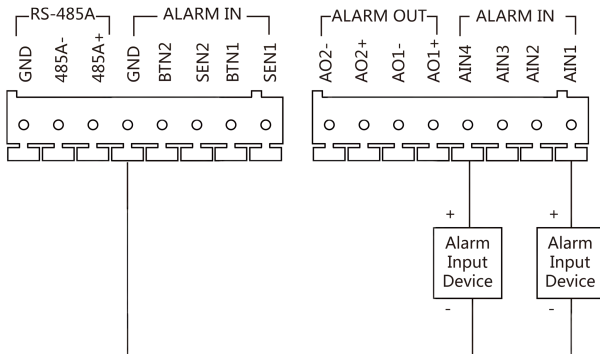


Figure 2-7 Alarm Input Wiring Diagram

2.2.7 Alarm Output Device Wiring

The alarm output wiring diagram is as follows:

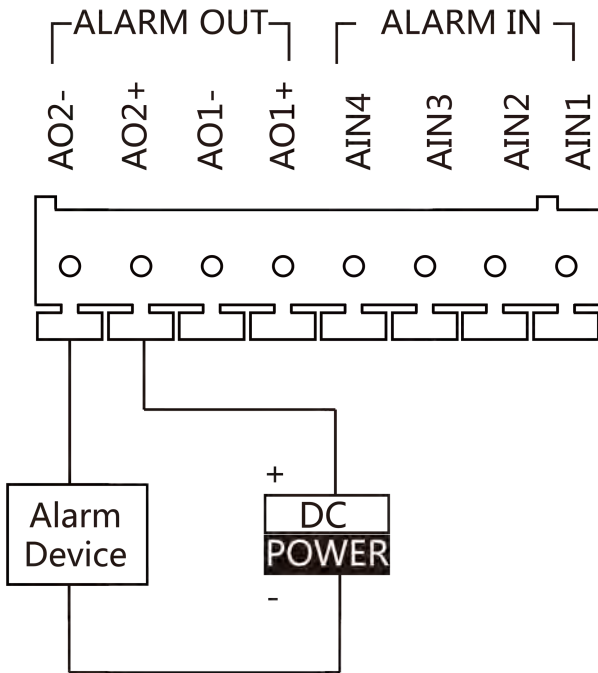


Figure 2-8 Alarm Output Wiring Diagram

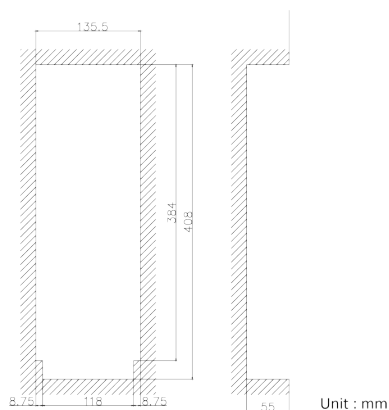


Figure 3-2 Drill an Installation Hole

2. Insert the gang box into the hole and fix it with 4 PA4 screws.

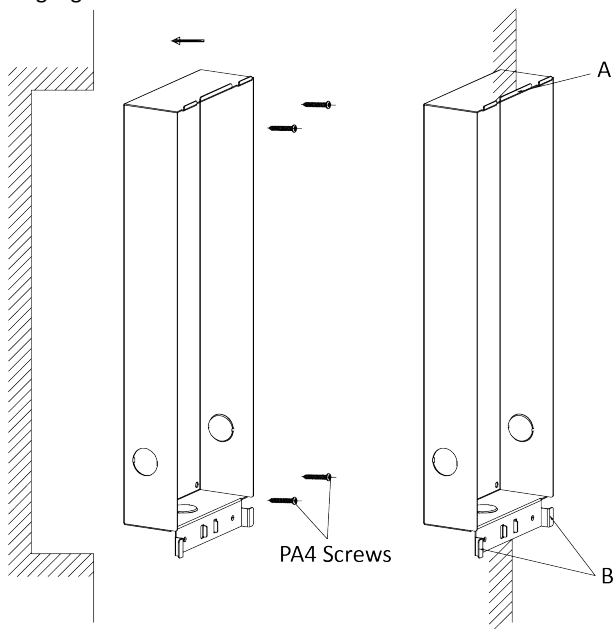


Figure 3-3 Insert the Gang Box

3. Make sure the edges of the gang box align to the wall and the hook A and hook B of the gang box hook onto the wall.
4. Route the cables of the door station through the cable hole.
5. Insert the door station into the gang box and then move the door station downward to hook the lock catches on the rear panel onto the hook C of the gang box.

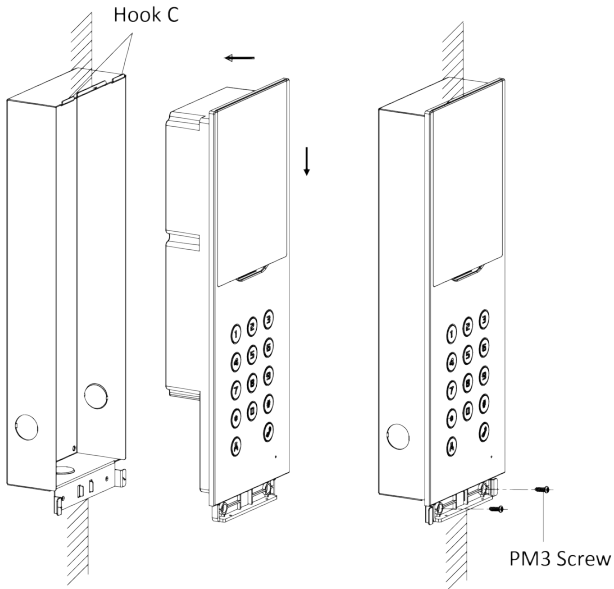


Figure 3-4 Insert the Door Station

6. Fix the door station with 2 PM3 screws.
7. After fixing the door station onto the gang box, secure it by inserting the plate and insert 2 POM2 screws.



Figure 3-5 Fix the Door Station

To install the door station onto the wall, you are required to use a matched gang box.

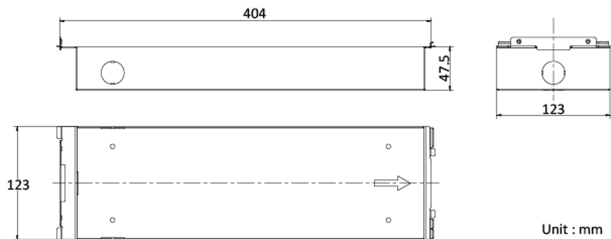


Figure 3-6 Gang Box



Note

- The dimension of gang box is: 404 (W) × 123 (H) × 47.5 (D) mm.
- The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.

3.2.2 Flush Mounting with Gang Box

Steps

1. Drill a hole in the wal for inserting the gang box. The size of the hole should be larger than that of the gang box. The suggested size of the hole is 404.5 (W) × 123.5 (H) × 48 (D) mm.

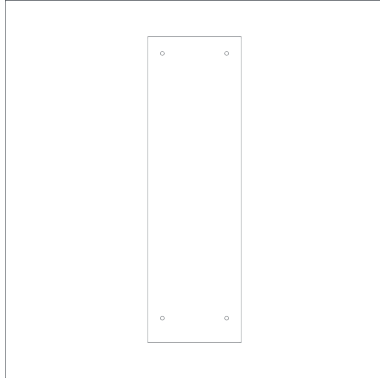


Figure 3-7 Drill an Installation Hole

2. Insert the gang box into the hole and fix it with 4 PA4 screws. Make sure the edges of the gang box align to the wall.

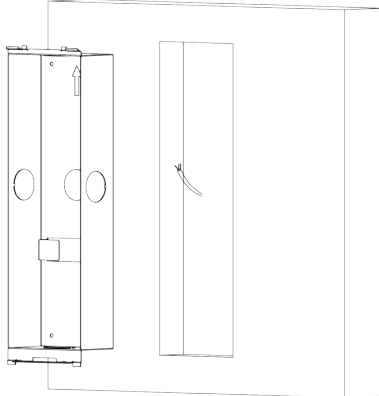


Figure 3-8 Insert the Gang Box

3. Route the cables of the door station through the cable hole.

4. Put the door station into the gang box and hook the lock catches on the rear panel.

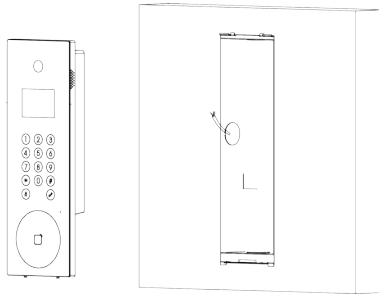


Figure 3-9 Install the Door Station

5. Pull the door station downward and then push it towards the inside to make sure it fits the hole.
6. Tighten the screws of the door station with the wrench.

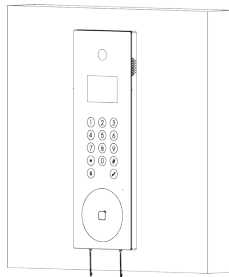


Figure 3-10 Fix the Door Station

To install the door station onto the wall, you are required to use a matched gang box.

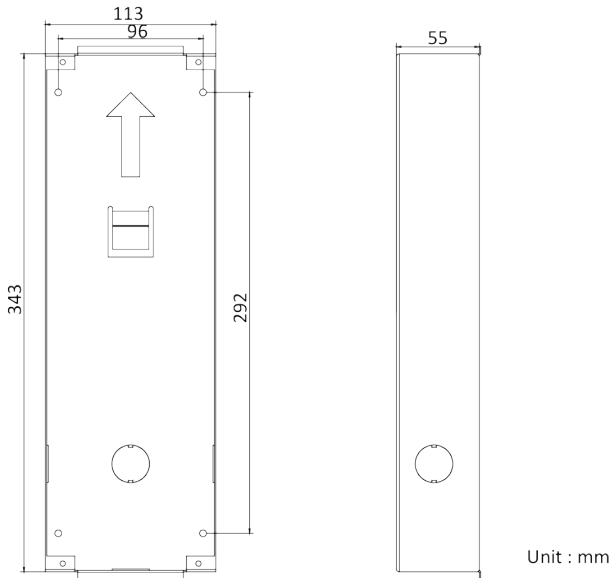


Figure 3-11 Gang Box

Note

- The dimension of gang box is: 343 (W) × 113 (H) × 55 (D) mm.
 - The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.
-

3.3.2 Flush Mounting with Gang Box

Steps

1. Drill a hole in the wall for inserting the gang box. The size of the hole should be larger than that of the gang box. The suggested size of the hole is 343.5 (W) × 113.5 (H) × 55.5 (D) mm.

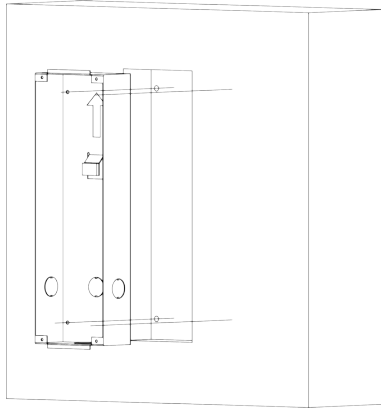


Figure 3-12 Drill an Installation Hole

2. Insert the gang box into the hole and fix it with 4 PA4 screws.
3. Make sure the edges of the gang box align to the wall.
4. Route the cables of the door station through the cable hole.
5. Put the door station into the gang box.
6. Fix the door station to the gang box with 4 screws.

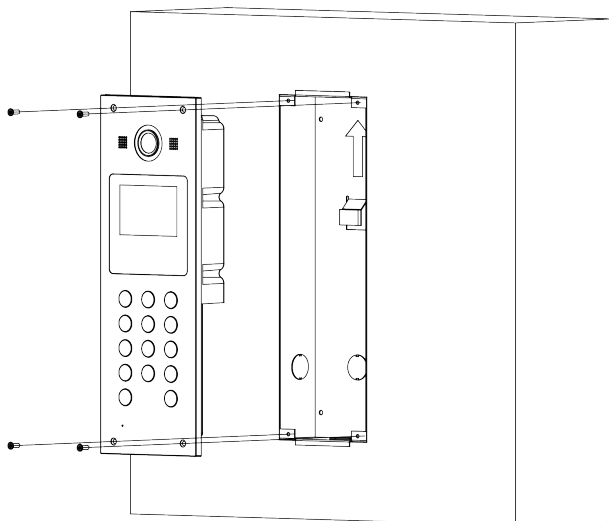


Figure 3-13 Fix the Door Station

4 Activation

4.1 Activate Device Locally

You are required to activate the device first by settings a strong password for it before you can use the device.

Steps

1. Power on the device to enter the activation page automatically.
2. Create a password and confirm it.

Table 4-1 Number Button Description

No.	Description	No.	Description
1	1,.,?! -*#	6	6mnoMNO
2	2abcABC	7	7pqrsPQRS
3	3defDEF	8	8tuvTUV
4	4ghiGHI	9	9wxyzWXYZ
5	5jklJKL	0	0

Hold 0 to enter special characters.

Table 4-2 Number Button Description

No.	Description	No.	Description
1	1,.,#?	6	6_ =+
2	2!@%	7	7[];:
3	3^\$*	8	8" <
4	4()\	9	9>{ }
5	5&/-		

 Note

- The password required 8 to 16 characters.
 - The way to enter the password, take button 2 as an example: Press 2 to enter the number '2' or hold 2 for 1.5 s and press 2 again to enter the character 'a'.
 - When you have entered the password, press # to switch to confirm the password.
 - Press * to delete the wrong character.
-

3. Press # to activate.

4.2 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.
-

4.3 Activate Device via Web

You are required to activate the device first by setting a strong password for it before you can use the device.

Default parameters of the door station are as follows:

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

Steps

1. Power on the device, and connect the device to the network.
2. Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation page.

 Note

The computer and the device should belong to the same subnet.

3. Create and enter a password into the password field.
4. Confirm the password.
5. Click **OK** to activate the device.

5 Local Operation

5.1 Local Configuration

5.1.1 Edit Network Parameters

After activating, you should edit the network parameters.

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to Network settings according to the tips on the page. Press # to enter the settings page.
4. Edit the parameters according to your needs.
5. Press * to save and exit.

5.1.2 Door Station Settings

Edit the parameters of the door station (including but not limited to, community No., building No., floor No., room No. and device mode).

Steps

1. Configure the parameters according to the actual needs.

Note

- Outer door station can only edit the Community No., Project No. and No.
 - The No. of the main door station is 0.
 - The No. of sub door stations should be larger than 0 and ranges from 1 to 99.
 - Each unit should add 1 main door station. Up to 8 sub door stations can be added to the main door station.
-

2. **Optional:** Adjust the brightness of the screen.
3. **Optional:** Enable the **Channel Mode** according to your needs.
4. **Optional:** Select the language.

5. After configuration, press * to save and exit.

5.1.3 Add Residents

User Management

You can add, edit and delete the informations of the users.

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to User Management according to the tips on the page.
4. Press # to enter the settings page.

Add Users

You can add cards, face pictures, fingerprints, permissions and room No. for the users.

Steps

1. Select **+Add**, and press # to enter the adding page.
2. Edit the room No.
3. Add cards.
 - 1) Switch to the card and press #.
 - 2) Enter the card No. manually or present the card on the card reading area to get the card No. automatically.
 - 3) Press # to add.
4. Add face pictures.
 - 1) Switch to the face and press #.
 - 2) Press # to capture. Press # again to save.

 Note

- Press * to capture again.
 - Up to 5000 face pictures can be added to the device. Refers to the actual model.
 - Each user can add one face picture only.
-

5. Add fingerprints.

- 1) Switch to the fingerprint and press #.
 - 2) Select **+Add Fingerprint** and press # to add.
 - 3) Put your finger on the fingerprint recognition area.
 - 4) Press * to save and exit.
-

 Note

Up to 10 fingerprints can be added to the same user.

6. Switch to the permission and press # to set.
7. Press * to save and exit.

5.1.4 About

You can view the device model, system version and QR Code of the device.

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to About according to the tips on the page.
4. Press # to enter the page.

5.2 Video Intercom Operation

5.2.1 Call Resident

The door station can work as main/sub door station, and outer door station, which correspond to different calling resident modes respectively.

Call Resident from Main/Sub Door Station

Press any digit button on the main/sub door station page to enter the calling page.

Enter the room No. and press call button.

Call Resident from Outer Door Station

Press call button on the outer door station page to enter the calling page .

Enter 【Building No. + # + Unit No. + # + Room No.】 and press call button to call resident.

5.2.2 Call Center

Press any digit button on the main/sub door station page to enter the calling page.

Press center button to call., and press * to cancel during calling management center.

5.3 Unlock Door

5.3.1 Unlock by Password

Unlock by Common Password

Press any digit button on the main/sub door station page to enter the calling page.

Enter 【 # + Room No. + Common Password + #】 to unlock the door.

Unlock by Public Password

Note

Make sure you have created the public password via iVMS-4200 Client Software remotely.

Press any digit button on the main/sub door station page to enter the calling page.

Enter **【# + Public Password + #】** to unlock the door.

5.3.2 Unlock by Presenting Card

 Note

Make sure you have issued the card to the device.

Present the card on the card reading area to unlock.

 Note

You cannot unlock the door by presenting the main card.

5.3.3 Unlock by Fingerprint

 Note

- Make sure you have added the fingerprint to the device.
- Fingerprint function may vary with different modules. Please refer to the actual devices.

Put your finger on the finger recognition module to unlock.

5.3.4 Unlock by QR Code

The device supports unlocking by QR code. You can use the camera to scan the QR code which is created via mobile client.

Steps

 Note

- Make sure the door station has been added to the indoor station.
 - Make sure the indoor station is connected to Wi-Fi.
 - Make sure the door station has issued the card and connected to the indoor station.
-

1. Search and install the **Hik-Connect** to your mobile phone.
2. Register and login the client according to the notice on the page.
3. Scan the QR code/bar code on the device or enter the serial No. manually to add the indoor station.
4. Create a QR code.

5. Press **Scan QR Code** on the main page to enter the scanning page.
6. Use the camera to scan the QR code.



Note

- Choose a location that will not reflect light when installing the door station, and tear off surface film of the acrylic door station.
 - Align the QR code with the camera horizontally when scanning the QR code.
 - QR code scanning is not supported at night.
-

6 Remote Configuration via Web

6.1 Live View

In the browser address bar, enter the IP address of the device, and press the Enter key to enter the login page.

Enter the user name and password and click **Login** to enter the Live View page. Or you can click **Live View** to enter the page.



Figure 6-1 Live View

- You can start/stop live view, capture, record, audio on/off, two-way audio, etc.
- The stream type can be set as main stream or sub stream.
- For IE (Internet Explorer) or Google users, the device support two-way audio communication.

6.2 User Management

You can add, delete or search the information of the user.

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

- Click **Add** and enter the username, floor No. and room No. to add.
- Click **Edit** to modify the informations of the user.
- Check the box of the user and click **Delete** to delete the selected user.
- Enter the keyword and click **Search**. The information will display in the list.

6.3 Device Management

You can manage the linked device on the page.

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

Add Device

- Click **Add** to add the indoor station or sub door station. Enter the parameters and click **OK** 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.

Upgrade

- Click **Upload Package** to select the upgrade package.
- Click **Timing Upgrading**, slide **Enable auto-upgrade** to set the start time and end time. The device will upgrade from start time to end time automatically.
- Click **Upgrading Status** to view the version for the device.

6.4 Parameters Settings

Click **Configuration** to set the parameters of the device.

Remote configuration in iVMS-4200 and Batch Configuration Tool is the same as that in Web. Here takes the configuration in web for example.



Note

Run the browser, click  → **Internet Options** → **Security** to disable the Protected Mode.

6.4.1 Local Parameters Settings

You can configure the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and capture by using the web browser. You can also set and view the saving paths of the captured pictures and recorded videos on the PC that running the web browser.

Live View Parameters

Stream Type

Set the stream type as **Main Stream** or **Sub-stream**.

Play Performance

Set the live view performance to **Shortest Delay**, **Balanced** or **Fluent**.

Auto Start Live View

Check **Yes** to enable the function.

Image Format

Select the image format for picture capture.

Click **Save** to enable the settings.

Record File Parameters

Record File Size

Select the packed size of the manually recorded and downloaded video files to **256M**, **512M** or **1G**. After the selection, the maximum record file size is the value you selected.

Save record files to

Set the saving path for the manually recorded video files.

Click **Save** to enable the settings.

Picture and Clip Settings

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Note

You can click **Browse** to change the directory for saving the clips and pictures, and click **Open** to open the set folder of clips and picture saving.

Click **Save** to enable the settings.

6.4.2 System Settings

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

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

Basic Information

Click **System Settings → Basic Information** to enter the settings page. On the page, you can edit **Device Name** and **Device No.** Set the **Language** and **System Type** according to your needs.

Click **Save** to enable the settings.

Time Settings

Click **System Settings → Time Settings** to enter the settings page. Select the **Time Zone** of your location from the drop-down list.

- Enable **NTP**, set the **Server Address**, **NTP Port** and **Interval**.
- Enable **Manual Time Sync.**, set the time manually or check the **Sync. with computer time**.

Click **Save** to enable the settings.

DST

Click **System Settings → DST** to enable DST. Set the parameters according to your needs and click **Save** to enable the settings.

Maintenance

Click **Maintenance → Upgrade & Maintenance** to enter the settings page.



Figure 6-2 Maintenance

- Reboot: Click **Reboot** to reboot the device.
- **Restore**
Click **Restore** to reset all the parameters, except the IP parameters and user information, to the default settings.

Default

Click **Default** to restore all parameters to default settings.

- Export parameters:
 1. Click **Device Parameters** to pop up the dialog box.
 2. Set and confirm the encryption password.
 3. Click **OK** to export parameters.
- Import Config. File:
 1. Click **Browse** to select the configuration file.
 2. Click **Import** and enter the encryption password to import.
- Upgrade: Click **Browse** to select the upgrade file.

Note

The upgrading process will last 1 to 10 minutes, do not power off during the upgrading. The device reboots automatically after upgrading.

User Management

Click **User Management** to enter the settings page.

Administrator can edit the permission for the users.

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.

Online Users

Click **User Management** → **Online Users** to enter the page.



No.	User Name	Level	User Operation Time
1	admin	Administrator	2020-02-27 15:40:23
2	admin	Administrator	2020-02-27 16:02:23

Total 2 items

Figure 6-3 Online Users

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

Arming/Disarming Information

Click **User Management** → **Arming/Disarming Information** to view the information. Click **Refresh** to get the present information.

6.4.3 Network Settings

TCP/IP Settings

TCP/IP settings must be properly configured before you operate the device over network. The device supports IPv4.

Steps

1. Click **Network** → **Basic Settings** → **TCP/IP** to enter the settings page.

☐ DHCP

IPv4 Address: 10.6.112.102

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 192.0.0.1

Mac Address: 00:40:65:3b:19:01

MTU: 1500

DNS Server

Preferred DNS Server: 8.8.8.8

Alternate DNS Server: 114.114.114.114

Save

Figure 6-4 TCP/IP Settings

2. Configure the network parameters.
 - Check **DHCP**, the device will get the parameters automatically.
 - Set the **IPv4 Address**, **IPv4 Subnet Mask** and **IPv4 Default Gateway** manually.
3. Configure the DNS server.
4. Click **Save** to enable the settings.

Port Settings

Steps

1. Click **Network → Basic Settings → Port** to enter the settings page.

HTTP Port: 80

RTSP Port: 554

Server Port: 8000

Save

Figure 6-5 Port Settings

2. Set the ports of the device.

HTTP Port

The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port

The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

Server Port

The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

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

SIP Setting

Steps

1. Click **Network → Basic Settings → SIP** to enter the settings page.
2. Check **Enable VOIP Gateway**.
3. Configure the SIP parameters.
4. Click **Save** to enable the settings.

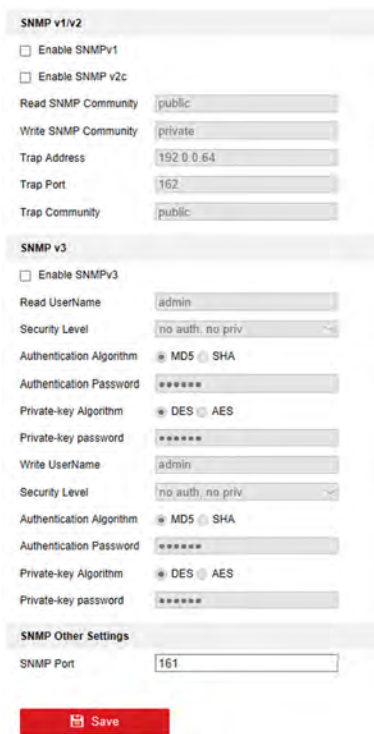
SNMP Settings

Before You Start

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

Steps

1. Click **Network → Advanced Settings → SNMP** to enter the settings page.



The image shows a web-based configuration form for SNMP settings, divided into three sections: SNMP v1/v2, SNMP v3, and SNMP Other Settings. Each section has a header bar. The SNMP v1/v2 section includes checkboxes for enabling v1 and v2c, and text input fields for Read/Write Communities, Trap Address, Trap Port, and Trap Community. The SNMP v3 section includes checkboxes for enabling v3, and text input fields for Read/Write UserNames, Security Levels (dropdown), Authentication Algorithms (radio buttons), Authentication Passwords (masked), Private-key Algorithms (radio buttons), and Private-key passwords (masked). The SNMP Other Settings section includes a text input field for the SNMP Port. A red 'Save' button is located at the bottom of the form.

SNMP v1/v2

☐ Enable SNMPv1

☐ Enable SNMP v2c

Read SNMP Community: public

Write SNMP Community: private

Trap Address: 192.0.0.64

Trap Port: 162

Trap Community: public

SNMP v3

☐ Enable SNMPv3

Read UserName: admin

Security Level: no auth, no priv

Authentication Algorithm: MD5 SHA

Authentication Password: *****

Private-key Algorithm: DES AES

Private-key password: *****

Write UserName: admin

Security Level: no auth, no priv

Authentication Algorithm: MD5 SHA

Authentication Password: *****

Private-key Algorithm: DES AES

Private-key password: *****

SNMP Other Settings

SNMP Port: 161

Save

Figure 6-6 SNMP Settings

2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3 to enable the feature correspondingly.
3. Configure the SNMP settings.
4. Click **Save** to enable the settings.

 Note

To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

FTP Settings

Steps

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

FTP Settings

☐ Enable FTP

Server Type: Server IP Address

Server IP Address: 0.0.0.0

Port: 21

☐ Enable Anonymous

User Name:

Password:

Directory Structure: Save in the child directory

Parent Directory: Building No. & Unit No.

Child Directory: Time

Picture Naming Rules

Delimiter: _

Named Item: Option1

Named Element: Time

Save

Figure 6-7 FTP Settings

2. Check **Enable FTP**.
3. Select **Server Type**.
4. Input the **Server IP Address** and **Port**.
5. Configure the FTP Settings, and the user name and password are required for the server login.
6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
7. Set the picture naming rules.
8. Click **Save** to enable the settings.

6.4.4 Video & Audio Settings

Video Parameters

Steps

1. Click **Video/Audio** → **Video** to enter the settings page.

Stream Type	Main Stream	▼
Video Type	Video&Audio	▼
Resolution	1280*720P	▼
Bitrate Type	Variable	▼
Video Quality	Medium	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	▼ Kbps
Video Encoding	H.264	▼
I Frame Interval	50	

Save

Figure 6-8 Video Parameters

2. Select the **Stream Type**.
3. Configure the video parameters.

Stream Type

Select the stream type to main stream or sub stream.

Video Type

Select the stream type to video stream, or video & audio composite stream.
The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

Resolution

Select the resolution of the video output.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Video Encoding

The device supports H.264.

I Frame Interval

Set I Frame Interval from 1 to 400.

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

Audio Parameters

Steps

1. Click **Video/Audio → Audio** to enter the settings page.

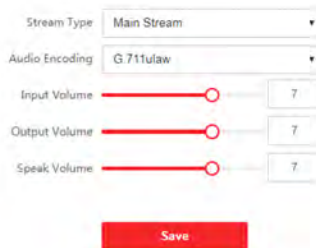


Figure 6-9 Audio Settings

2. Configure the stream type and the audio encoding type.

Stream Type

Select the stream type to main stream or sub stream.

Audio Encoding

The device support G.711ulaw and G.711 alaw.

3. Adjust the **Input Volume**, **Output Volume** and **Speak Volume**.



Note

Available range of volume: 0 to 10.

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

6.4.5 Display Settings

Configure the image adjustment, backlight settings and other parameters in display settings.

Steps

1. Click **Image → Display Settings** to enter the display settings page.



Figure 6-10 Display Settings

2. Select the **Format**.
3. Set the display parameters.

WDR

Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

Brightness

Brightness describes bright of the image, which ranges from 1 to 100.

Contrast

Contrast describes the contrast of the image, which ranges from 1 to 100.

Saturation

Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

Sharpness

Sharpness describes the edge contrast of the image, which ranges from 1 to 100.

BLC Area

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right and Center are selectable.

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

6.4.6 Event Settings

Motion Detection

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

Steps

1. Click **Event** → **Motion** to enter the settings page.

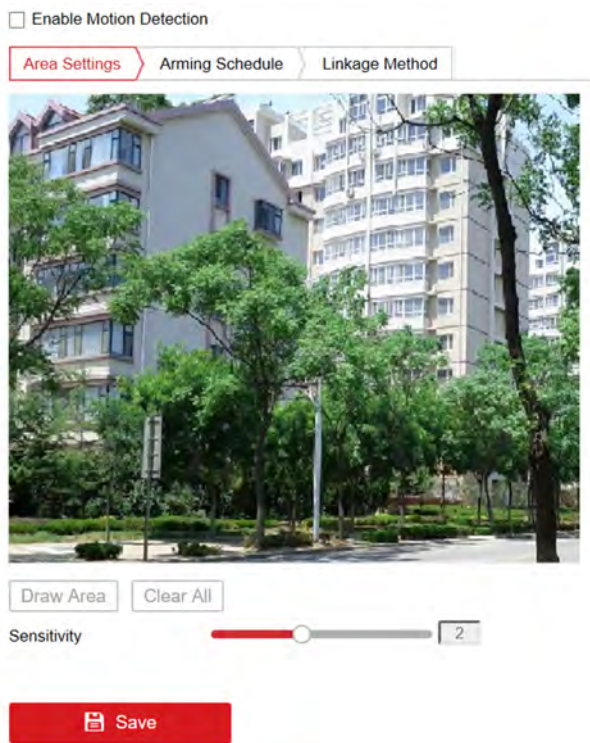


Figure 6-11 Motion Detection

2. Check **Enable Motion Detection** to enable the function.
3. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area. Click **Save** to save the settings.
 - Clear Area** Click **Clear All** to clear all of the areas.
 - Adjust Sensitivity** Move the slider to set the sensitivity of the detection.
4. Click **Arming Schedule** to edit the arming schedule.
5. Click on the time bar and drag the mouse to select the time period. Click **Save** to save the settings.
 - Delete Schedule** Click **Delete** to delete the current arming schedule.
6. Click **Linkage Method** to enable the linkages.

Notify Surveillance Center

Send an exception or alarm signal to the remote management software when an event occurs.

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

Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Click **Event** → **Basic Event** → **Video Tampering** to enter the settings page.
2. Check **Enable Video Tampering**.
3. Draw area.
 - 1) Click **Area Settings**.
 - 2) Click , and drag the mouse in the live view page to draw an area.
 - 3) **Optional:** Click  to clear the drawing area.
4. Drag the block to set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
5. **Optional:** Click **Linkage Method**, and check the normal linkage or notify surveillance center according to your actual needs.

Normal Linkage

Set the normal alarm linkage.

Notify Surveillance Center

The alarm information is uploaded to the surveillance center when an alarm event is detected.

6. **Optional:** Click  or  to perform the record or capture operation.
7. Click **Save** to save the settings.

Event Linkage

Steps

1. Click **Event** → **Basic Event** → **Event Linkage** to enter the settings page.

Major Type Device Event ▼

Minor Type Tampering Alarm ▼

☒ **Normal Linkage**

☒ Notify Surveillance Center

Save

Figure 6-12 Event Linkage

2. Select the **Major Type** as **Device Event** or **Door Event**.
3. Select the type of the **Normal Linkage** for the event.
4. Click **Save** to enable the settings.

6.4.7 Intercom Settings

Device ID Configuration

Steps

1. Click **Device ID Settings** to enter the page.



Figure 6-13 Device ID Settings

2. Select the device type from the drop-down list, and set the corresponding information.
3. Click **Save** to enable the device number configuration.

Note

- For main door station (D series or V series), the serial No. is 0.
 - For sub door station (D series or V series), the serial No. cannot be 0. Serial No. ranges from 1 to 99.
 - For each villa or building, at least one main door station (D series or V series) should be configured, and one sub door stations (D series or V series) can be customized.
 - For one main door station (D series or V series), up to 8 sub door stations can be configured.
-

Linked Network Settings

Steps

1. Click **Intercom → Linked Network Settings** to enter the settings page.

Register Number	000000
Password	
Master Station IP	0.0.0.0
Master Station SIP Client Port	21
Private SIP Server IP	0.0.0.0
Private SIP Server Port	1234
SIP Client Port	123

Save

Figure 6-14 Linked Network Settings

2. Set the master station IP address and master station SIP client Port.
3. Set the private SIP server IP address and private SIP Server Port.
4. Set the SIP Client Port.
5. Enter the password.
6. Click **Save** to enable the settings.

Time Parameters

Click **Intercom** → **Time Parameters** to enter the page.

Configure the time parameters and click **Save**.

Note

Maximum speaking time varies from 90s to 120s, and maximum message time varies from 30s to 60s.

6.4.8 Access Control Settings

Permission Password

Steps

1. Click **Access Control** → **Permission Password** to enter the settings page.



The screenshot shows a web form for setting a permission password. It includes a dropdown menu for 'Password Type' with 'Public Password1' selected, a text input field for 'Password', and another text input field for 'Doorphone'. Below these fields is a red 'Save' button.

Figure 6-15 Permission Password

2. Select the password type.
3. Change the password.
4. Set the number of doorphone.
5. Click **Save** to enable the settings.

Door Parameters

Steps

1. Click **Access Control** → **Door Parameters** to enter the settings page.



The screenshot shows a web form for setting door parameters. It includes a dropdown menu for 'Door' with 'Door1' selected, a text input field for 'Door Name', a radio button group for 'Door Contact' with 'Remain Open' selected, and a text input field for 'Lock Action Time' with '15' entered. Below these fields is a red 'Save' button.

Figure 6-16 Door Parameters

2. Select the door and edit the door name.
3. Set door contact status.
4. Set lock action time.
5. Click **Save** to enable the settings.

Card Security

Click **Access Control** → **Card Security** to enter the settings page.

Slide to enable card encryption parameters. Click **Save** to enable the settings.

Elevator Control

Before You Start

- Make sure your door station is in the mode of main door station. Only the main door station support elevator control function.
- Make sure your door station has been connected to the elevator controller via RS-485 wire if you want to use RS-485 interface.

Steps

1. Click **Access Control** → **Elevator Control** to enter the corresponding configuration page.

☐ Enable elevator control

Elevator No. Elevator No.1

Elevator Controller Type

Interface Type Network Interface

Negative Floor Capacity

Alarm Receiver Type IP

Server IP Address

Port

User Name

Password

Save

Figure 6-17 Elevator Control

2. Check to enable elevator control function.
3. Select an Elevator No., and select an elevator controller type for the elevator.
4. Set the Negative Floor.
5. Select the Interface Type as RS-485 or Network Interface. And enable the elevator control.
 - If you select RS-485, make sure you have connected the door station to the elevator controller with RS-485 wire.
 - If you select Network interface, enter the elevator controller's IP address, port No., user name, and password.
6. Click **Save** to enable the settings.

 Note

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

RS-485 Settings

Set the working mode to linked device.

Steps

1. Click **Access Control** → **RS485 Settings** to enter the settings page.



The screenshot shows a web interface for RS-485 Settings. It features two dropdown menus. The first dropdown is labeled 'No.' and has a value of '1' selected. The second dropdown is labeled 'Working Mode' and has 'Elevator.Control' selected. Below these menus is a prominent red button labeled 'Save'.

Figure 6-18 RS-485 Settings

2. Select the No.
3. Select the working mode.
4. Click **Save** to enable the settings.

7 Configuration via Client Software

7.1 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.
-

7.2 Add Device

You should add device to the software so as to configure the device remotely.

7.2.1 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 10.6.112.48
* Address 10.6.112.48
* Port 8000
* User Name admin
* Password ••••••••

Synchronize Time ☒
Import to Group ☒

① 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

7.2.2 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**.

7.2.3 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**.

7.3 Remote Configuration

Select the device, click  to configure the parameters remotely.

7.4 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.

7.5 Organization Management

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

7.5.1 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.

7.5.2 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.
-

7.6 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 10,000 persons or cards can be added.

7.6.1 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, gender, 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.

7.6.2 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.

7.6.3 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.

7.6.4 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.
 - The gender of the persons will be **Male** by default.
-

7.6.5 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.

7.6.6 Add Person in Batch

Enter a short description of your task here (optional).

Before You Start

Enter the prerequisites here (optional).

Enter the context of your task here (optional).

Steps

1. Enter your first step here.

Enter the result of your step here (optional).

Example

Enter an example that illustrates the current task (optional).

What to do next

Enter the tasks the user should do after finishing this task (optional).

7.6.7 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.

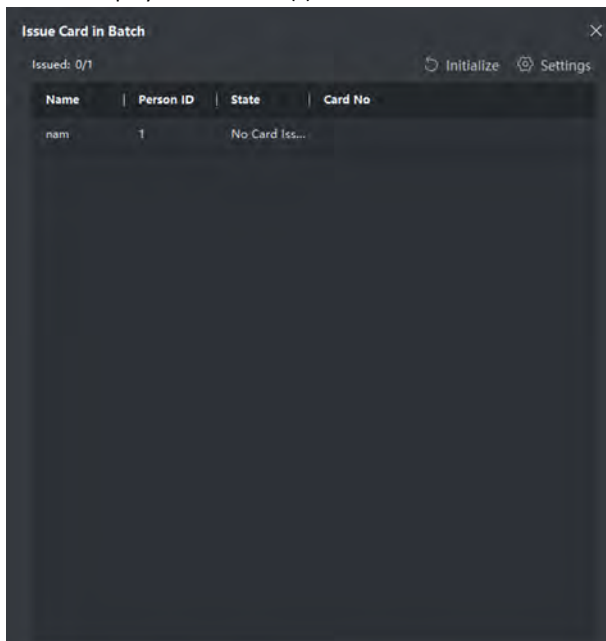


Figure 7-2 Issue Card in Batch

2. Click **Settings**.

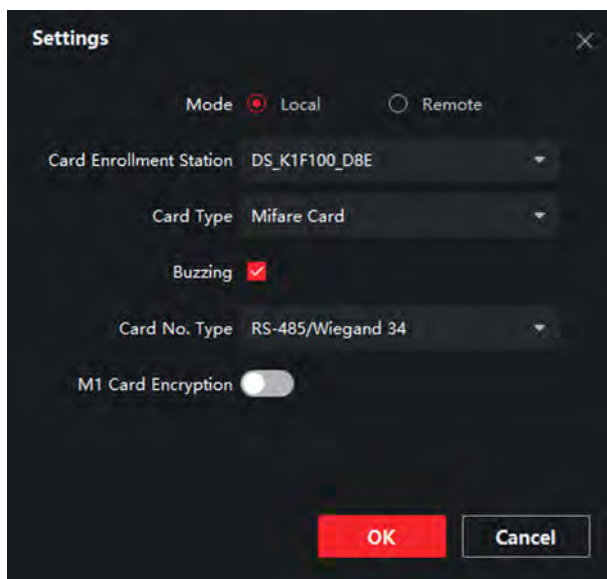


Figure 7-3 Card Settings

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.

7.6.8 Permission Settings

Add Permissions

Steps

1. On the main page, click  **AccessControlInfo** → **Access Group** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Configure the parameters.
 - 1) Enter the **Name** of the permission.

- 2) Select the **Template** of the schedule.
- 3) Check the person to **Selected** according to your needs.
- 4) Check the device to **Selected** according to your needs.
4. Click **Save**.
5. Check the permission and click **Apply All to Device**.
The status of the permission displays as **Applied**.
6. **Optional**: Click **Applying Status** to check the details.

Modify/Delete Permissions

On the page of the permission settings, click  to edit the parameters of the permission.

Select one or more permissions, click **Delete** to remove the permissions.

7.7 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.

7.7.1 Receive Call from Door Station

Steps

1. Select the client software in the device page to start calling the **iVMS-4200 Client Software** 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 window.

- Click  to adjust the volume of the loudspeaker.
- Click  to adjust the volume of the microphone.
- Click **Hang Up** to hang up the dialog.
- 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.
-

7.7.2 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.

7.7.3 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.

7.7.4 Search Video Intercom Information

Search Call Logs

Steps

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

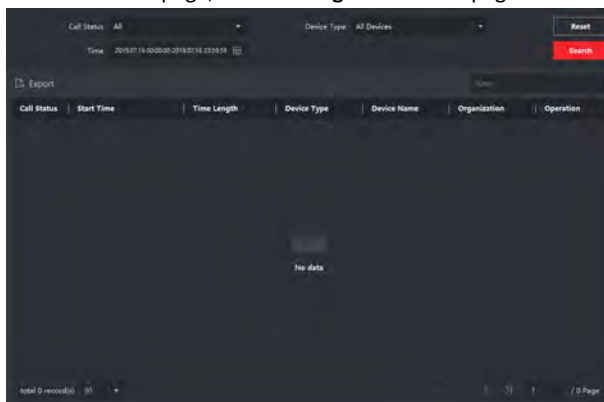


Figure 7-4 Search Call Logs

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.

A. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.



Figure A-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.



Figure A-2 Device Command

