

The HIKVISION logo is displayed on a red horizontal bar with a white diagonal stripe on the left side. The word "HIKVISION" is written in a white, italicized, sans-serif font.

HIKVISION

Video Intercom Face Recognition Door Station with 4.3-inch Screen

User Manual

Legal Information

©2021 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 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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.




Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

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.

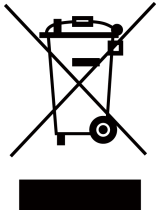
This equipment complies with FCC/IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

ce matériel est conforme aux limites de dose d'exposition aux rayonnements, FCC / CNR-102 énoncée dans un autre environnement. cette équipement devrait être installé et exploité avec distance minimale de 20 entre le radiateur et votre corps.

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.

Contents

| | |
|---|----|
| 1 Appearance | 1 |
| 2 Terminal and Wiring Description | 4 |
| 2.1 Terminal Description | 4 |
| 2.2 Wiring Description | 5 |
| 2.2.1 Door Lock Wiring | 5 |
| 2.2.2 Exit Button Wiring | 6 |
| 2.2.3 Door Contact Wiring | 7 |
| 3 Installation | 8 |
| 3.1 Gang Box | 8 |
| 3.2 Flush Mounting with Gang Box | 9 |
| 4 Activation | 11 |
| 4.1 Activate Device Locally | 11 |
| 4.2 Activate Device via Client Software | 12 |
| 4.3 Activate Device via Web | 13 |
| 5 Local Operation | 14 |
| 5.1 Local Configuration | 14 |
| 5.1.1 Edit Network Parameters | 14 |
| 5.1.2 Local Settings | 14 |
| 5.1.3 Add Residents | 15 |
| 5.1.4 About | 16 |
| 5.2 Video Intercom Operation | 17 |
| 5.2.1 Call Resident | 17 |

| | |
|---|----|
| 5.2.2 Call Center | 17 |
| 5.3 Unlock Door | 17 |
| 5.3.1 Unlock by Password | 17 |
| 5.3.2 Unlock by Presenting Card | 18 |
| 5.3.3 Unlock by Fingerprint | 18 |
| 5.3.4 Unlock by Face | 18 |
| 6 Remote Configuration via Web | 19 |
| 6.1 Live View | 19 |
| 6.2 User Management | 19 |
| 6.3 Device Management | 20 |
| 6.4 Parameters Settings | 21 |
| 6.4.1 System Settings | 21 |
| 6.4.2 Network Settings | 24 |
| 6.4.3 Video & Audio Settings | 29 |
| 6.4.4 Display Settings | 32 |
| 6.4.5 Event Settings | 33 |
| 6.4.6 Intercom Settings | 36 |
| 6.4.7 Access Control Settings | 37 |
| 6.4.8 Smart Settings | 40 |
| 7 Configuration via Client Software | 43 |
| 7.1 Edit Network Parameters | 43 |
| 7.2 Add Device | 43 |
| 7.2.1 Add Online Device | 43 |
| 7.2.2 Add Device by IP Address | 44 |

| | |
|--|----|
| 7.2.3 Add Device by IP Segment | 44 |
| 7.3 Remote Configuration | 45 |
| 7.4 Device Management | 45 |
| 7.5 Organization Management | 45 |
| 7.5.1 Add Organization | 45 |
| 7.5.2 Modify and Delete Organization | 46 |
| 7.6 Person Management | 46 |
| 7.6.1 Add Person | 46 |
| 7.6.2 Modify and Delete Person | 48 |
| 7.6.3 Import and Export Person Information | 48 |
| 7.6.4 Get Person Information from Device | 48 |
| 7.6.5 Change Person to Other Organization | 49 |
| 7.6.6 Issue Card in Batch | 49 |
| 7.6.7 Permission Settings | 51 |
| 7.7 Video Intercom Settings | 52 |
| 7.7.1 Receive Call from Door Station | 52 |
| 7.7.2 Live View via Door Station | 53 |
| 7.7.3 Release Notice | 53 |
| 7.7.4 Search Video Intercom Information | 54 |
| A. Appendix | 56 |
| B. Communication Matrix and Device Command | 57 |

1 Appearance

Door Station without Fingerprint Module

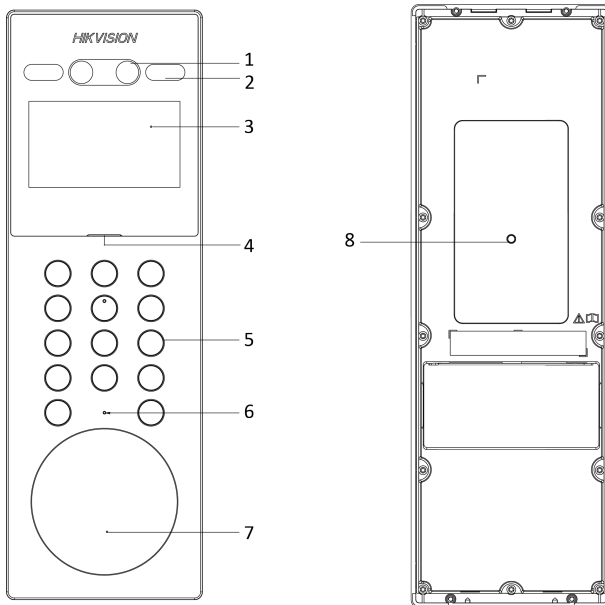


Figure 1-1 Appearance of Door Station without Fingerprint Module

Table 1-1 Description

| No. | Description |
|-----|---------------------|
| 1 | Camera |
| 2 | IR Supplement Light |
| 3 | Screen |
| 4 | Loudspeaker |
| 5 | Buttons |

| No. | Description |
|-----|-------------------|
| 6 | Microphone |
| 7 | Card Reading Area |
| 8 | TAMPER |

Door Station with Fingerprint Module

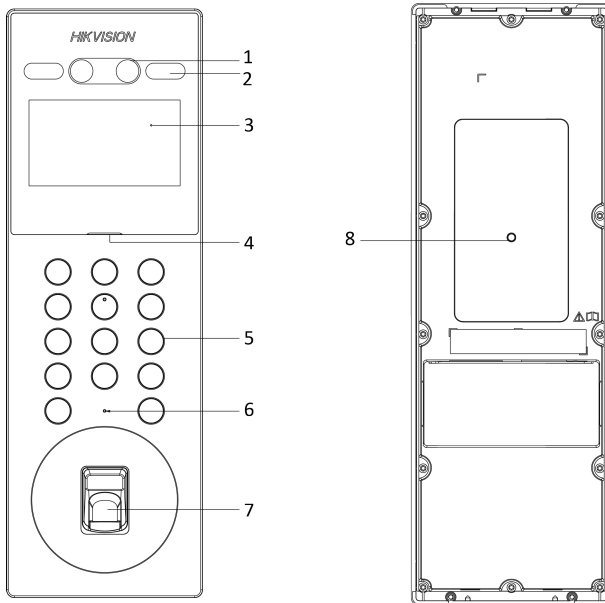


Figure 1-2 Appearance of Door Station with Fingerprint Module

Table 1-2 Description

| No. | Description |
|-----|---------------------|
| 1 | Camera |
| 2 | IR Supplement Light |
| 3 | Screen |

| No. | Description |
|------------|---|
| 4 | Loudspeaker |
| 5 | Buttons |
| 6 | Microphone |
| 7 | Card Reading Area/ Fingerprint Recognition Module |
| 8 | TAMPER |

2 Terminal and Wiring Description

2.1 Terminal Description

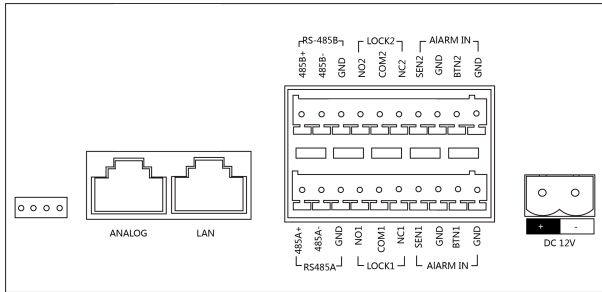


Figure 2-1 Terminal Description

Table 2-1 Description

| Name | Terminal | Description |
|-------------------|----------|--|
| Network Interface | LAN | Network Signal Input |
| ALARM IN | SEN1 | Door Contact Input 1 |
| | SEN2 | Door Contact Input 2 |
| | BTN1 | Exit Button Input 1 |
| | BTN2 | Exit Button Input 2 |
| | GND | Grounding |
| RS-485 | 485A+ | External RS-485 Card Reader |
| | 485A- | |
| | 485B+ | External Elevator Controller |
| | 485B- | |
| DOOR | NC1 | Door Lock Relay Output 1(Normally Close) |

| Name | Terminal | Description |
|--------------|----------|--|
| | COM1 | Common Interface 1 |
| | NO1 | Door Lock Relay Output 1(Normally Open) |
| | GND | Grounding |
| | NC2 | Door Lock Relay Output 2(Normally Close) |
| | COM2 | Common Interface 2 |
| | NO2 | Door Lock Relay Output 2(Normally Open) |
| | GND | Grounding |
| Power Supply | DC 12 V | 12 VDC Power Input |

 **Note**

- Alarm input interface cannot be edited. Refers to the actual model.
- You can only wire the SEN1/SEN2 terminal with the door contact. And wire the BTN1/BTN2 terminal with the exit button.

2.2 Wiring Description

2.2.1 Door Lock Wiring

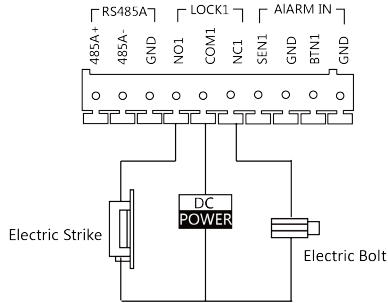


Figure 2-2 Door Lock Wiring

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 Exit Button Wiring

Wire the BTN1/BTN2 terminal with the door contact.

Here takes BTN1 for example.

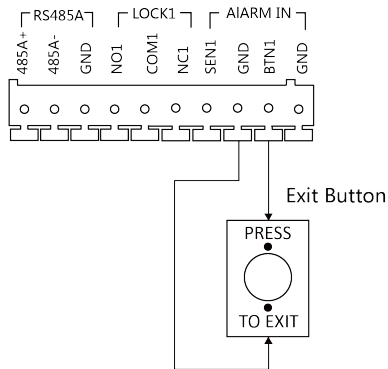


Figure 2-3 Exit Button Wiring

2.2.3 Door Contact Wiring

Wire the SEN1/SEN2 terminal with door contact.

Here takes SEN1 for example.

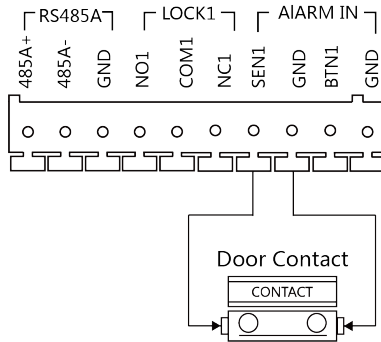


Figure 2-4 Door Contact Wiring

3 Installation

Note

- Make sure the device in the package is in good condition and all the assembly parts are included.
- The power supply the door station supports is 12 VDC. Please 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 Gang Box

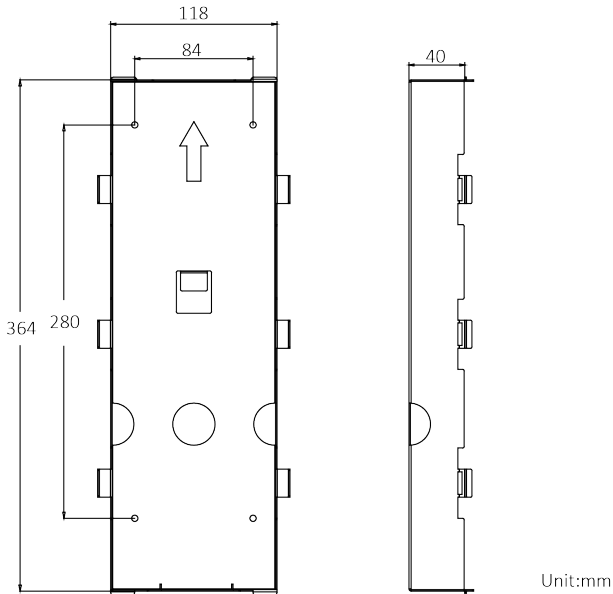


Figure 3-1 Dimension of the Gang Box

 **Note**

- The dimension of the gang box is 364 mm (W) × 118 mm (H) × 40 mm (D).
 - The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).
-

3.2 Flush Mounting with Gang Box

Steps

1. Cave an installation hole in the wall. Pull the cable out from the wall.
-

 **Note**

- The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).
 - The suggested length of the cables left outside is 250 mm.
-

2. Install the gang box into the wall.
 - 1) Remove the plastic sheet of the gang box with the tool.
 - 2) Insert the gang box into the installation hole. Mark the gang box screw holes' position with a marker, and take out the gang box.
 - 3) Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
 - 4) Fix the gang box with 4 expansion bolts.
3. Fix the gap between the gang box and wall with concrete. Remove the mounting ears with tool after concrete is dry. Connect the cables according to the *Wiring Description*.
4. Insert the door station into the gang box. Slide the door station down and fix it with 2 set screws. Apply Silicone sealant among the joints between the device and the wall (except the lower side) to keep the raindrop from entering.

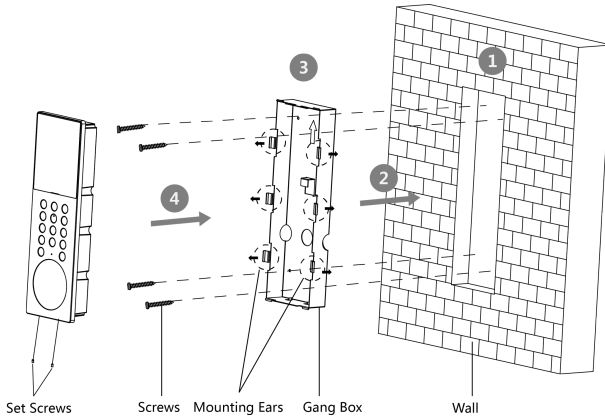


Figure 3-2 Flush Mounting with Gang Box

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 charater.
-

3. Press # to select language.
4. After selection, press # to finish activation.

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

When entering configuration page, the button is used as follows.

Table 5-1 Button Description

| Button | Description | Button | Description |
|--------|-------------|--------|-------------|
| 2 | Previous | 8 | Next |
| * | Exit/Back | # | OK |

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 Local Settings

Configure the local parameters (including but not limited to, edit numbers and edit recognition 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 Local Settings according to the tips on the page.
4. Press # to enter the settings page.

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 8.
 - Each unit should add 1 main door station. Up to 8 sub door stations can be added to the main door station.
-

2. **Optional:** Enable the **Normally Open Mode** according to your needs.
The door remains open.
3. **Optional:** Select the language.
4. After configuration, press * to save and exit.

Recognition with Mask

Steps

1. Enable **Face with Mask Detection**.
2. Select the **Passing Level of Face Mask Recognition**.
3. Edit the **Fce with Mask & Face 1:N Matching Threshold** and **Fce with Mask & Face 1:N Matching Threshold (ECO Mode)**.

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, 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 # or present cards on the card reading area to add.
 - 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. Switch to the permission and press # to set.
5. 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 **【Community No. + Building No. + # + Unit No. + # + Room No.】** and press call button to call resident.

Note

When Unit No. is one, it can be omitted. When Unit No. is omitted, Community No. must be omitted at the same time.

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 Password

Tap **Call/Open** to enter the calling page.

Enter 【 # + Room No. + Password + # 】 , and tap unlock button.

Unlock by Public Password

Note

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

Tap **Call/Open** to enter the calling page.

Enter 【 # + Public Password + # 】 , and tap unlock button.

5.3.2 Unlock by Presenting Card

Note

Make sure you have issued the card to the device. Refers to *User Management* for details.

Present the card on the card reading area to unlock.

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 Face

Note

Make sure you have added your face picture to the device. Refers to the *User Management* for details.

Face forward at the camera to unlock.

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.

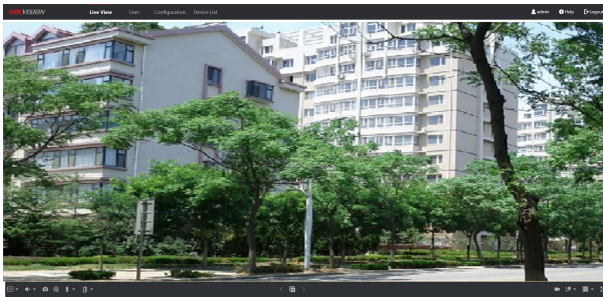


Figure 6-1 Live View

- 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.

Note

Live View function may vary with different models. Please refer to the actual product.

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 Management** 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.



Note

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

Export

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

Upgrade

Upgrade Automatically

Click **Timing Upgrade** to pop-up the settings dialog.

Enable upgrading device automatically. Edit the start time and end time and click **OK** to save the settings.

The upgrading will start at the set time automatically.

Upgrade Manually

Click **Upload Upgrading Package** to import the upgrading package.

Click **Upgrade Now** to start upgrading.

View Version

Put the mouse on the Upgrading button to view the upgrading version and time.

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 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 check **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. Select **Device Parameters**, and click **Export** 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 icon to select the configuration file.
 2. Click **Import** and enter the encryption password to import.
- **Upgrade**: Click browse icon 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.

Authentication

Click **Security** → **Authentication** to enter the settings page. On the page, you can select **RTSP Authentication** according to your actual needs.

Click **Save** to enable the settings.

Security Service

Click **Security** → **Security Service** to enter the settings page. On the page, you can enable SSH according to your actual needs.

Click **Save** to enable the settings.

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 | Each IP address segment should be less than 255. The first segment should be an integer between 1 and 223, and should not be 127. The fourth segment should not be 0 or 255. | User Operation Time |
|---------------|-----------|---------------|--|---------------------|
| 1 | admin | Administrator | 192.168.28 | 2020-02-27 16:48:23 |
| 2 | admin | Administrator | 192.168.103 | 2020-02-27 16:50:23 |
| 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.

6.4.2 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

IPv4 Subnet Mask

IPv4 Default Gateway

Mac Address

MTU

Alarm Center IP

Alarm Host Port

DNS Server

Preferred DNS Server

Alternate DNS Server

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 corresponding DNS server parameters.
4. Click **Save** to enable the settings.

Port Settings

Steps

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

| | |
|-------------|-----------------------------------|
| HTTP Port | <input type="text" value="80"/> |
| RTSP Port | <input type="text" value="554"/> |
| HTTPS Port | <input type="text" value="443"/> |
| Server Port | <input type="text" value="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.

HTTPS Port

The default port number is 443, and it can be changed to any port No. which is not occupied.

RTSP Port

The default port number is 554.

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.

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** → **SNMP** to enter the settings page.
2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c to enable the feature correspondingly.
 - 1) Edit **Read SNMP Community** and **Write SNMP Community**.

- 2) Enter the **Trap Address**, **Trap Port** and **Trap Community**.

 **Note**

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

3. Check the check box of Enable SNMPv3 to set the SNMPv3 parameters.
4. Click **Save** to enable the settings.

FTP Settings

Steps

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

Enable FTP

Server Type

Server IP Address

Port

Enable Anonymous

User Name

Password

Directory Structure

Parent Directory

Child Directory

Picture Naming Rules

Delimiter

Named Item

Named Element

Save

Figure 6-6 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.

Platform Access

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

Steps

1. Click **Network** → **Advanced Settings** → **Platform Access** to enter the settings page.
2. Check the checkbox of **Enable** to enable the function.
3. Select the **Platform Access Mode**.

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.

4. Create a **Stream Encryption/Encryption** for the device.

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

6.4.3 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 6-7 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.

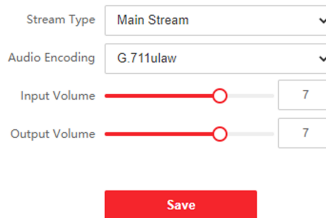


Figure 6-8 Audio Settings

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** and **Output Volume**.

 **Note**

Available range of volume: 0 to 10.

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

6.4.4 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.

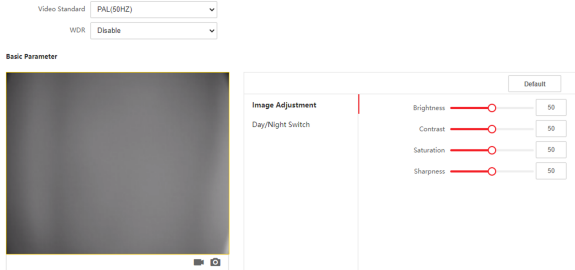


Figure 6-9 Display Settings

- 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.

4. Set the **Day/Night Mode**.

| | | |
|------------------|------------------|---------|
| | | Default |
| Image Adjustment | Day/Night Switch | Auto |
| Day/Night Switch | Sensitivity | 4 |

Figure 6-10 Day/Night Mode

- Set **Day Mode** or **Night Mode** manually.
- Set the mode as **Auto** and edit the sensitivity according to your needs.
- Set the mode as **Scheduled-Switch**. Set the start time and end time.

Note

Daytime is from configured start time to configured time. The rest of the time is set as night by default.

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

6.4.5 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.

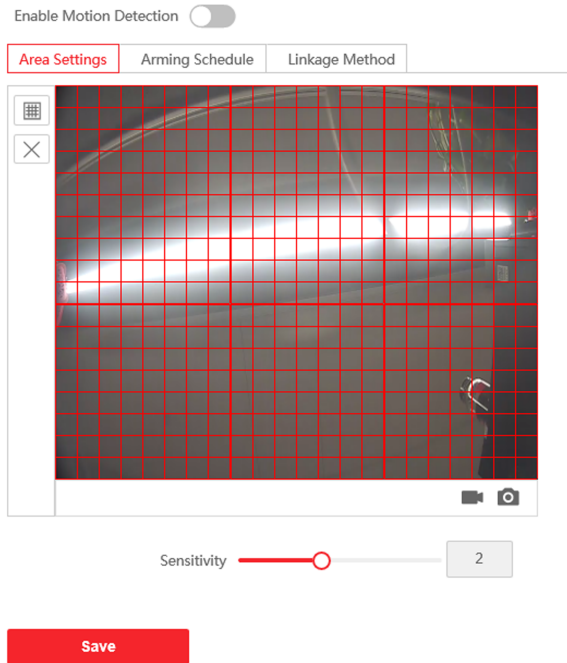


Figure 6-11 Motion Detection

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.

Event Linkage

Steps

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

Major Type

Minor Type

Normal Linkage

Notify Surveillance Center

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.

6.4.6 Intercom Settings

Device ID Configuration

Steps

1. Click **Device No.** to enter the page.

| | |
|------------------|---------------------------------------|
| Device Type | Door Station <input type="checkbox"/> |
| Period No. | 1 |
| Building No. | 1 |
| Unit No. | 1 |
| Floor No. | 1 <input type="checkbox"/> |
| Door Station No. | 0 |
| Community No. | 0 |

Save

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. Go to **Intercom** → **Session Settings** to enter the settings page.
2. Set **Register Number** and **Registration Password**.
3. Set **Main Station IP** and **VideoIntercom Server IP**.
4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Parameters

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

Configure **Max. Call Duration**, **Max. Message Duration**, **Max. Ring Duration**, and click **Save**.

Ring-Back Tone Settings

Click **Intercom** → **Ringbacktone Settings** to enter the settings page.

Click **Add** to select the ring tone from PC.

Note

Available Audio Format: WAV、AAC, Size: Less than 600 KB, Sample Rate: 8000Hz, Mono.

6.4.7 Access Control Settings

Permission Password

Steps

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

Password Type

Password

Doorphone

Figure 6-14 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.

Door

Door Name

Relay reverse Disable ON

Open Duration s

Figure 6-15 Door Parameters

2. Select the door and edit the door name.
3. Set Relay Reverse.
4. Set **Open Duration**.

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

Card Security

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

Slide to enable card encryption parameters and CPU card reading content. 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 Controller Type

Interface Type

Negative Floor Capacity

Save

Figure 6-16 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**

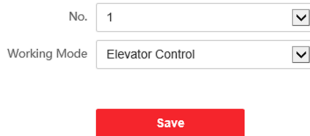
- Up to 4 elevator controllers can be connected to one door station.
 - Up to 10 negative floors can be added.
 - Make sure the interface types of elevator controllers, which are connected to the same door station are consistent.
-

RS-485 Settings

Set the working mode to linked device.

Steps

1. Click **Access Control** → **RS-485** to enter the settings page.



The screenshot shows a settings form with two dropdown menus and a red 'Save' button. The first dropdown menu is labeled 'No.' and has the value '1' selected. The second dropdown menu is labeled 'Working Mode' and has 'Elevator Control' selected. The 'Save' button is a solid red rectangle with the word 'Save' in white text.

Figure 6-17 RS-485 Settings

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

6.4.8 Smart Settings

Biometrics Settings

Adjust the face recognition parameters and fingerprint parameters according to your needs.

Steps

1. Click **Smart** to enter the settings page.
2. Enable face anti-spoofing to edit face capture advanced parameters.

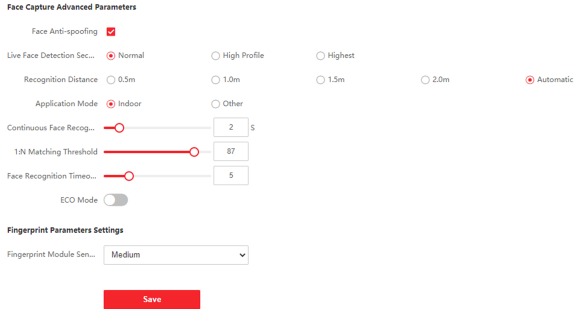


Figure 6-18 Smart Settings
Table 6-1 Face Capture Advanced Parameters

| Parameter | Description |
|--------------------------------------|--|
| Application Mode | Select either others or indoor according to actual environment. |
| Live Face Detection Security Level | After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication. |
| Recognition Distance | Set the valid distance between the user and the camera when authenticating. |
| Continuous Face Recognition Interval | The time interval between two continuous face recognitions when authenticating. Note You can input the number from 1 to 10. |
| 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. |

| Parameter | Description |
|-------------------------|---|
| Face 1:1 Security Level | Set the matching threshold when authenticating via 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. |
| ECO Settings | <p>After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).</p> <p>ECO Threshold</p> <p>When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode.</p> <p>ECO Mode (1:1)</p> <p>Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.</p> <p>ECO Mode (1:N)</p> <p>Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.</p> <p>Force to Enable Night Mode</p> <p>When the environment is not bright enough, you can slide to force to enable the night mode.</p> |

3. Select **Fingerprint Module Sensitivity**.
4. Click **Save** to enable the settings.

Area Configuration

Click **VCA Configuration** → **Area Configuration** to enter the settings page.
 Drag the frame to adjust the size of the recognition area.

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 [X]

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

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

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 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.

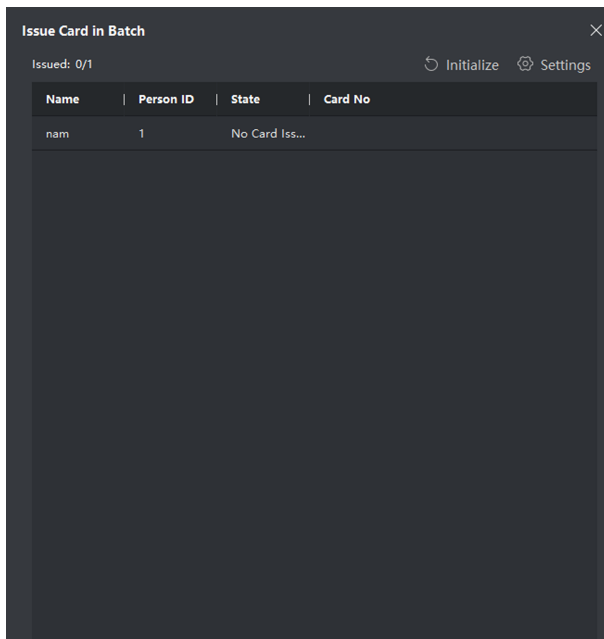


Figure 7-2 Issue Card in Batch

2. Click **Settings**.

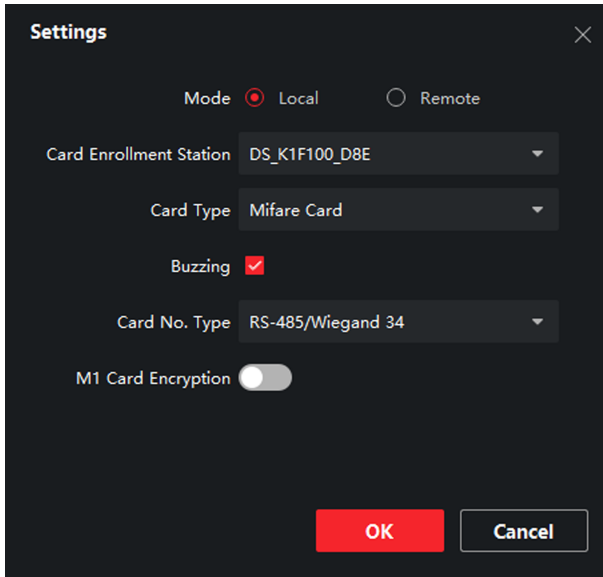


Figure 7-3 Card Settings

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.

7.6.7 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.

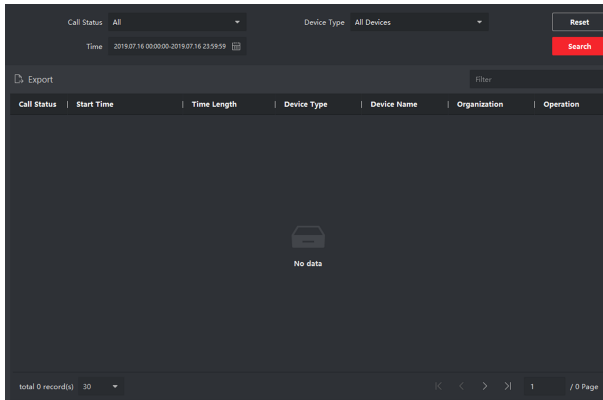


Figure 7-4 Search Call Logs

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. Appendix

Tips When Collecting/Comparing Face Picture

- Keep your expression naturally when collecting or comparing face pictures.
- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.
- In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.
- Make sure your face is in the middle of the collecting window.
- The recommended distance when collecting/comparing face pictures is between 400 mm and 500 mm.

Tips When Importing Face Picture

- The requirements of the face pictures are the same as the requirements for collecting.
- Picture format: JPG.
- The photo scale is 5:7. The pixel size is a minimum of 480 and the height is a minimum of 640.
- Picture size cannot exceed 200 KB.
- A pure background color is required. White is the best.

B. 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 B-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 B-2 Device Command

