



DS-KV8213-WME1 • DS-KV8413-WME1 • DS-KV8113-WME1

**Video Intercom Villa Door Station  
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 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 LATTER PREVAILS.

## Symbol Conventions

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

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

## Safety Instruction

### **Warning**

- The working temperature of the device is 14° to 131° F (-10° to 55° C).
- All the electronic operation should be in strict compliance with the electrical safety regulations, fire prevention regulations, and other related regulations in your local region.
- Use the power adapter provided by the 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 overheating or fire hazard.
- Make sure that the power has been disconnected before you wire, install, or dismantle the device.
- When the product is installed on a wall or ceiling, the device shall be firmly fixed.
- If smoke, odors, or noise rise from the device, turn off the power at once, unplug the power cable, and then contact the service center.
- If the product does not work properly, 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 electro-magnetic radiation. Avoid equipment installation on vibrating surfaces 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 electro-magnetic radiation.
- Keep the indoor device cover from rain and moisture.
- Exposing the equipment to direct sunlight, low ventilation, or a heat source such as a 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.
- Use the provided glove when opening the device cover, and avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Use a soft and dry cloth when cleaning inside and outside surfaces of the device cover, do not use alkaline detergents.
- Keep all wrappers after unpacking them for future use. In case any failure occurs, return the device to the factory with the original packaging. Transportation without the original packaging may result in damage to 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.
- Input voltage should meet both the SELV and the Limited Power Source according to 60950-1 standard.
- The power supply must conform to LPS. The recommended adaptor models and manufacturers are shown as below. Use the attached adapter, and do not change the adaptor randomly.

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

## Regulatory Information

### FCC Information

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:

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

## EU Conformity Statement



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



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

## Industry Canada ICES-003 Compliance

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

## Contents

<b>1. Appearance .....</b>	<b>10</b>
1.1. Single-Button Villa Door Station.....	10
1.2. Two-Button Villa Door Station .....	11
1.3. Four-Button Villa Door Station .....	12
<b>2. Terminal and Wiring Description .....</b>	<b>13</b>
2.1. Terminal Description .....	13
2.2. Wiring Description .....	13
2.2.1. Door Lock Wiring .....	13
2.2.2. Door Contact Wiring .....	14
2.2.3. Exit Button Wiring .....	14
2.2.4. Alarm Input Device Wiring .....	14
<b>3. Installation.....</b>	<b>15</b>
3.1. Accessory Introduction.....	15
3.2. Surface Mounting with Protective Shield.....	15
3.3. Surface Mounting without Protective Shield.....	16
<b>4. Activation.....</b>	<b>18</b>
4.1. Activate Device via Web .....	18
4.2. Activate Device via Client Software .....	18
4.3. Edit Network Parameters .....	19
<b>5. Remote Configuration via Web .....</b>	<b>20</b>
5.1. Live View .....	20
5.2. User Management .....	20
5.3. Device Management.....	21
5.4. Parameters Settings .....	21
5.4.1. Local Parameters Settings .....	22
5.4.2. Record File Parameters .....	22
5.4.3. Save record files to .....	22
5.4.4. Picture and Clip Settings .....	22
5.5. System Settings.....	23
5.5.1. Network SettingsTCP/IP Settings .....	25
5.5.2. Port Settings.....	25
5.5.3. SIP Setting .....	26
5.5.4. FTP Settings .....	27
5.5.5. Platform Access .....	27

5.5.6. Video & Audio SettingsVideo Parameters.....	28
5.5.7. Audio Parameters.....	29
5.6. Image Settings .....	29
5.6.1. Display Settings.....	29
5.6.2. OSD Settings.....	31
5.6.3. Target Cropping.....	31
5.7. Event Settings.....	32
5.7.1. Motion Detection.....	32
5.7.2. Event Linkage.....	33
5.7.3. Schedule Settings.....	33
5.8. Intercom Settings.....	35
5.8.1. Device ID Configuration .....	35
5.8.2. Linked Network Settings .....	35
5.8.3. Time Parameters .....	36
5.9. Ring-Back Tone Settings.....	36
5.9.1. Press Button to Call.....	36
5.9.2. Number Settings .....	36
5.9.3. Access Control SettingsDoor Parameters .....	37
5.10. Elevator Control.....	37
<b>6. Configuration via Client Software .....</b>	<b>39</b>
6.1. Device Management.....	39
6.1.1. Add Online Device.....	39
6.1.2. Add Device by IP Address.....	40
6.1.3. Add Device by IP Segment .....	40
6.2. Live View via Door Station .....	40
6.3. Organization Management.....	40
6.3.1. Add Organization .....	40
6.3.2. Modify and Delete Organization.....	41
6.4. Person Management .....	41
6.4.1. Add Person.....	41
6.4.2. Modify and Delete Person .....	42
6.4.3. Change Person to Other Organization .....	42
6.4.4. Import and Export Person Information .....	42
6.4.5. Get Person Information from Device.....	43
6.4.6. Issue Card in Batch .....	44

6.4.7. Permission Settings.....	45
6.5. Video Intercom Settings.....	45
6.5.1. Receive Call from Door Station .....	46
6.5.2. Release Notice .....	46
6.5.3. Search Video Intercom Information.....	47
6.5.4. Upload Armed Information .....	48
<b>Appendix: Communication Matrix and Device Command.....</b>	<b>49</b>

## **Table of Figures**

Figure 1, Single-Button Villa Door Station Appearance .....	10
Figure 2, Two-Button Villa Door Station Appearance .....	11
Figure 3, Four-Button Villa Door Station Appearance .....	12
Figure 4, Terminal Description .....	13
Figure 5, Door Lock Wiring.....	13
Figure 6, Door Contact Wiring.....	14
Figure 7, Exit Button Wiring.....	14
Figure 8, Accessory Introduction.....	15
Figure 9, Mounting Template.....	16
Figure 10, Surface Mounting with Protective Shield .....	16
Figure 11, Mounting Template .....	17
Figure 12, Surface Mounting without Protective Shield.....	17
Figure 13, Live View .....	20
Figure 14, User Management .....	20
Figure 15, Device Management.....	21
Figure 16, Local Parameters .....	22
Figure 17, Online Users .....	24
Figure 18, TCP/IP Settings.....	25
Figure 19, Port Settings.....	26
Figure 20, SIP Settings.....	26
Figure 21, FTP Settings.....	27
Figure 22, Video Parameters .....	28
Figure 23, Audio Settings .....	29
Figure 24, Display Settings.....	30
Figure 25, Day/Night Mode .....	30
Figure 26, Backlight.....	31



Figure 27, Motion Detection ..... 32

Figure 28, Event Linkage ..... 33

Figure 29, Weekly Schedule ..... 34

Figure 30, Holiday Schedule ..... 34

Figure 31, Device ID Settings..... 35

Figure 32, Press Button to Call..... 36

Figure 33, Number Settings..... 37

Figure 34, Door Parameters..... 37

Figure 35, Elevator Control ..... 38

Figure 36, Add to the Client..... 39

Figure 37, Issue Card in Batch..... 44

Figure 38, Card Settings ..... 44

Figure 39, Search Call Logs ..... 47

Figure 40, QR Code of Communication Matrix..... 49

Figure 41, Device Command ..... 49

# 1. Appearance

## 1.1. Single-Button Villa Door Station

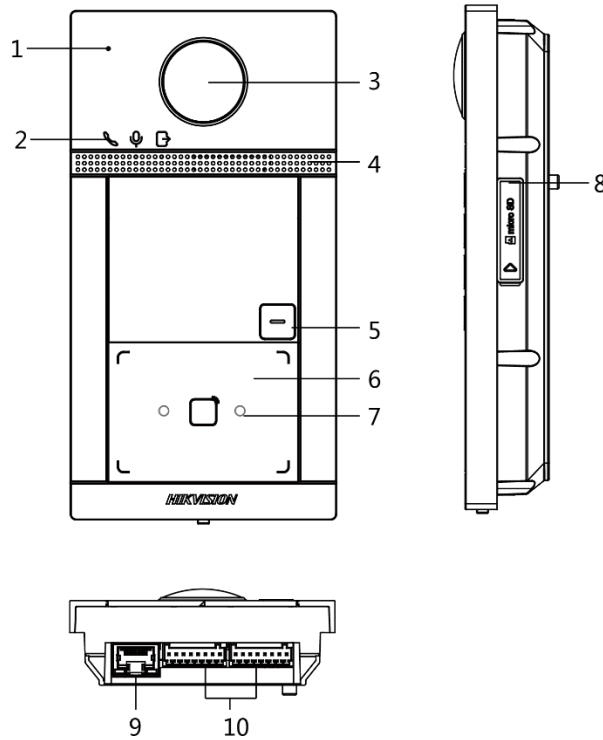


Figure 1, Single-Button Villa Door Station Appearance

Table 1-1 Description

No.	Description
1	Microphone
2	Indicator Unlock (Green)/Call (Orange)/Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	MicroSD Card Slot (Reserved) and Debugging Port
9	LAN
10	Terminals

## 1.2. Two-Button Villa Door Station

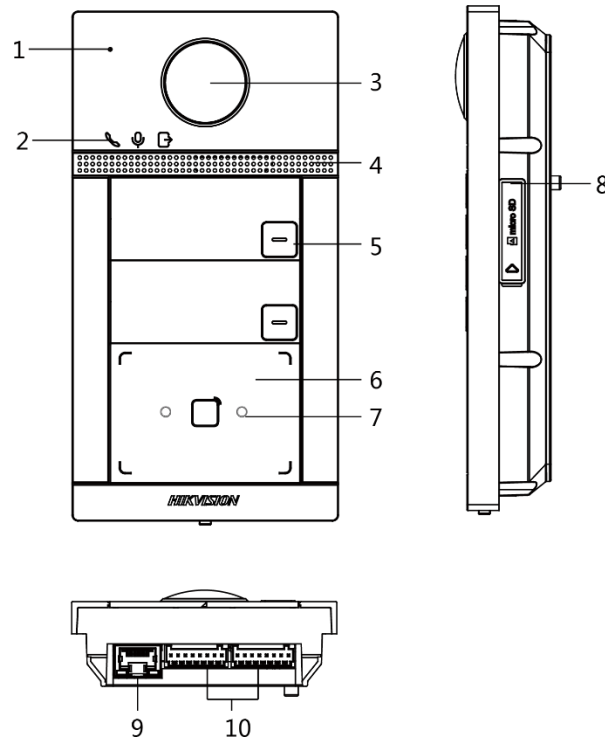


Figure 2, Two-Button Villa Door Station Appearance

Table 1-2 Description

No.	Description
1	Microphone
2	Indicator: Unlock (Green)/Call (Orange)/Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	MicroSD Card Slot (Reserved) and Debugging Port
9	LAN
10	Terminals

## 1.3. Four-Button Villa Door Station

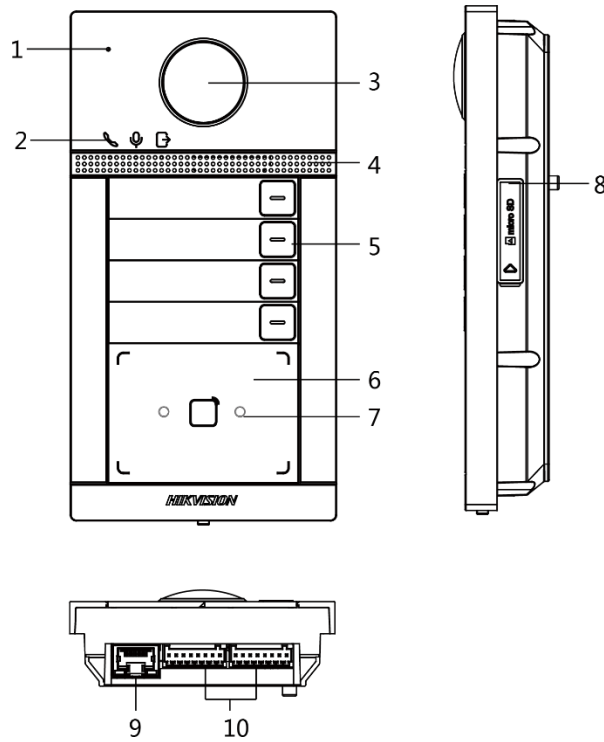


Figure 3, Four-Button Villa Door Station Appearance

Table 1-3 Description

No.	Description
1	Microphone
2	Indicator: Unlock (Green)/Call (Orange)/Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	MicroSD Card Slot (Reserved) and Debugging Port
9	LAN
10	Terminals

## 2. Terminal and Wiring Description

### 2.1. Terminal Description

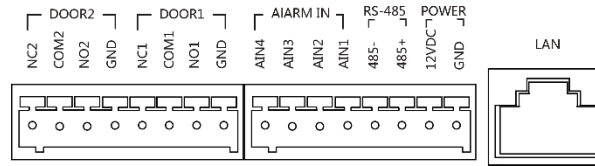


Figure 4, Terminal Description

Table 2-1 Description of Terminal and Interfaces

Name	Interface	Description
DOOR	NC2	Door Lock Relay Output 2 (NC)
	COM2	Common Interface
	NO2	Door Lock Relay Output 2 (NO)
	GND	Grounding
	NC1	Door Lock Relay Output 1 (NO)
	COM1	Common Interface
	NO1	Door Lock Relay Output 1 (NO)
	GND	Grounding
ALARM IN	AI1	Alarm Input 1 (for Door Contact access)
	AI2	Alarm Input 2 (for Door Contact access) <b>NOTE:</b> Before accessing the Door Contact, select <b>Input</b> as <b>Door Status</b> in the <b>I/O Settings</b> page
	AI3	Alarm Input 3 (for Exit Button access)
	AI4	Alarm Input 4 (for Exit Button access) <b>NOTE:</b> Before accessing the Exit Button, select <b>Input</b> as <b>Exit Button</b> in the <b>I/O Settings</b> page
RS-485	485+	RS-485 Communication Interface
	485-	
Power Input	12 VDC	12 VDC Input
	GND	
Network	LAN	Network Interface

## 2.2. Wiring Description

### 2.2.1. Door Lock Wiring

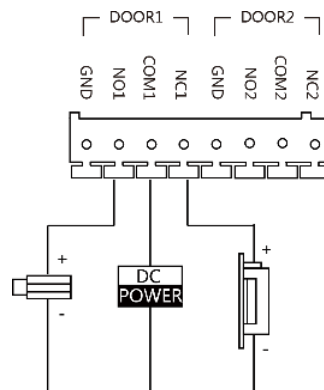


Figure 5, Door Lock Wiring

**NOTE:** Terminal NC1/COM1 is set as default for accessing magnetic lock/electric bolt.  
Terminal NO1/COM1 is set as default for accessing electric strike.

To connect electric lock in terminal NO2/COM2/NC2, it is required to set the output of terminal NO2/COM2/NC2 to be electric lock with the iVMS-4200 client software.

### 2.2.2. Door Contact Wiring

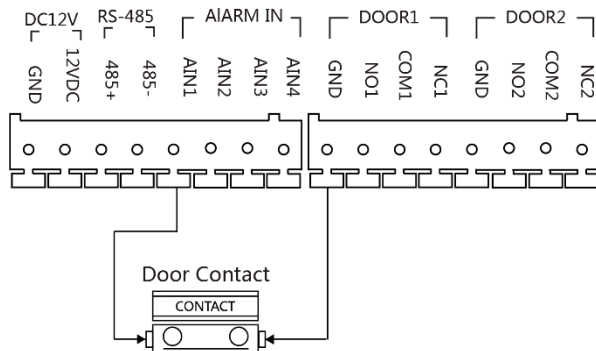


Figure 6, Door Contact Wiring

### 2.2.3. Exit Button Wiring

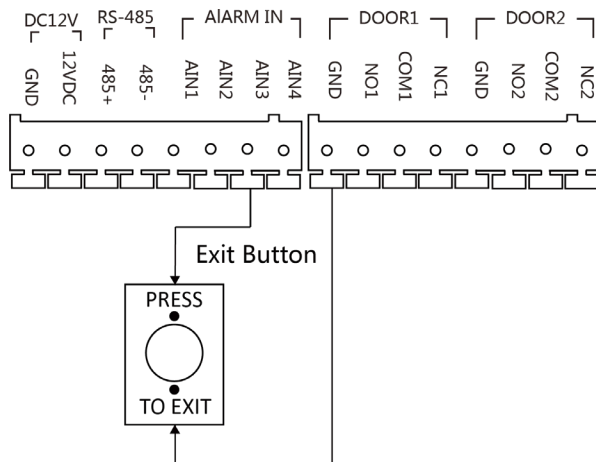


Figure 7, Exit Button Wiring

### 2.2.4. Alarm Input Device Wiring

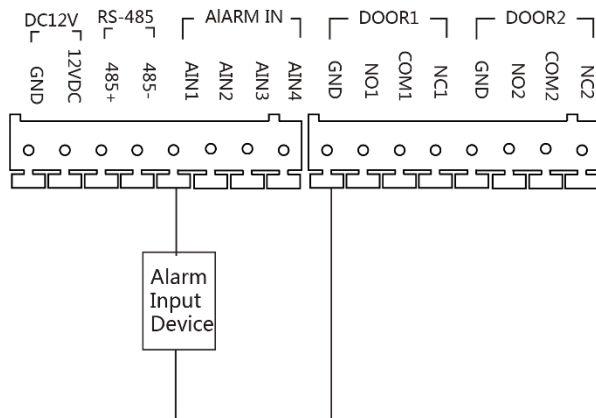


Figure 8, Alarm Input Device Wiring

## 3. Installation

**NOTE:** Make sure the device in the package is in good condition and all the assembly parts are included.

Make sure your power supply matches your door station.

Make sure all the related equipment is powered off during the installation.

Check the product specification for the installation environment.

### 3.1. Accessory Introduction

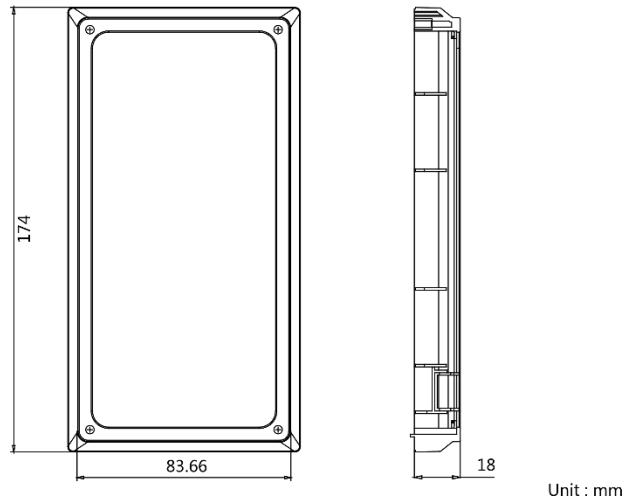


Figure 9, Accessory Introduction

**NOTE:** The door station gang box dimensions are: 174 mm (length) × 83.66 mm (width) × 18 mm (depth).

### 3.2. Surface Mounting with Protective Shield

#### Before You Start

- Tools that you need to prepare for installation: Drill ( $\varnothing 2.846$ ) and gradienter.
- Purchase the protective shield before installation.

#### Steps

1. Stick the mounting template on the wall. Drill screw holes according to the mounting template.
2. Remove the template from the wall.

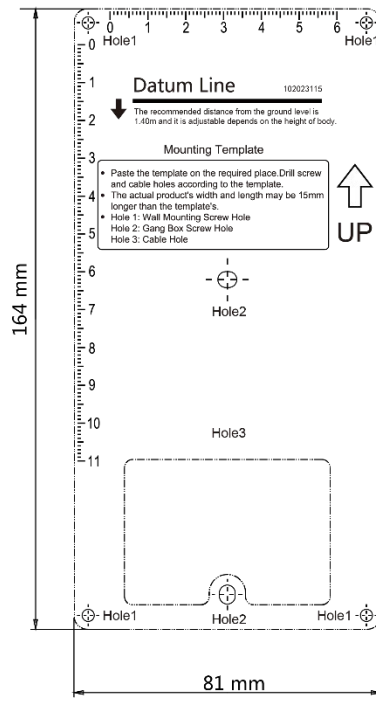


Figure 10, Mounting Template

3. Align the protective shield with the mounting template.
4. Secure the mounting plate on the wall with four supplied screws according to the screw holes.
5. Secure the device on the mounting plate with the four supplied set screws.
6. Affix the cover onto the device with the screw.

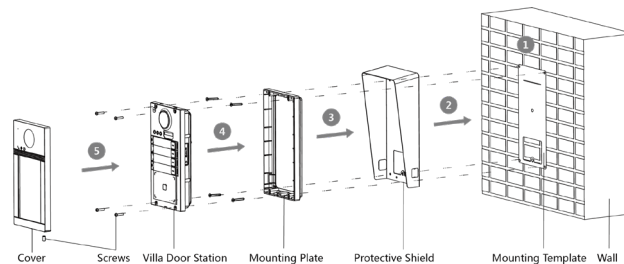


Figure 11, Surface Mounting with Protective Shield

### 3.3. Surface Mounting without Protective Shield

#### Before You Start

Tools that you need to prepare for installation: Drill ( $\varnothing 2.846$ ) and gradienter.

#### Steps

1. Stick the mounting template on the wall. Drill screw holes according to the mounting template.
2. Remove the template from the wall.



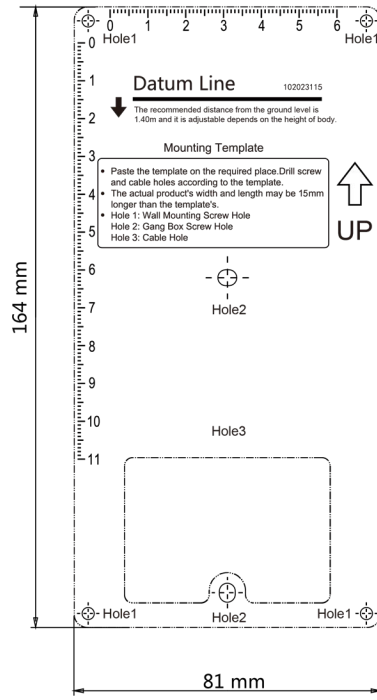


Figure 12, Mounting Template

3. Secure the mounting plate on the wall with four supplied screws according to the screw holes.
4. Secure the device on the mounting plate with the four supplied set screws.
5. Fix the cover onto the device with the screw.

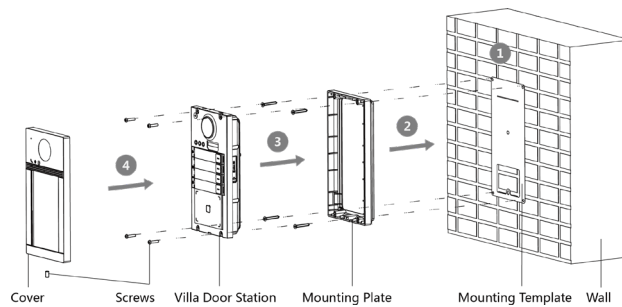


Figure 13, Surface Mounting without Protective Shield

## 4. Activation

### 4.1. 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 a Web browser, and click **Enter** to enter the activation page.

**NOTE:** The computer and the device must 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.

### 4.2. Activate Device via Client Software

You can configure and operate the door station only 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, then 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.



**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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

**NOTE:** If the device is not activated, the basic operation and remote operation of device cannot be performed.

Hold the **Ctrl** or **Shift** key to select multiple online devices, and click the **Activate** button to activate devices in batch.

### 4.3. Edit Network Parameters

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

#### Steps

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

**NOTE:** The default port no. is 8000.

The default door station IP address is 192.0.0.65.

After editing the device network parameters, add the devices to the device list again.

## 5. Remote Configuration via Web

### 5.1. Live View

Enter the device IP address in the browser address bar, and press **Enter** to enter the login page.

Enter the user name and password and click **Login**, or click **Live View**, to enter the Live View page.



Figure 14, 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 supports two-way audio communication.

**NOTE:** The Live View function may vary by model. Please refer to the actual product.

### 5.2. User Management

You can add, delete, or search the user information. Click **User** to enter the settings page.

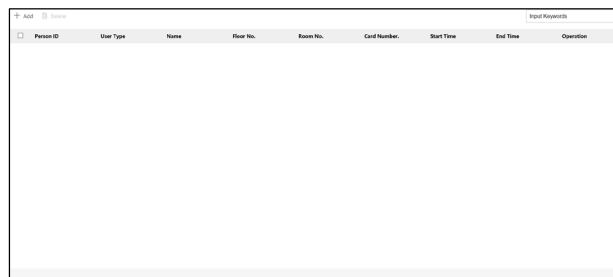


Figure 15, User Management

- Click **Add** and enter the **Name**, **Floor No.** and **Room No.** to add.
- Click **Edit** to modify the user information.
- Check the user box, and click **Delete** to delete the selected user.
- Enter the keyword and click the search icon. The information will display in the list.

**NOTE:** The **User Management** function may vary by model. Please refer to the actual product.



## 5.3. Device Management

You can manage the linked device on the page.

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



Figure 16, Device Management

- **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 device information in the template to import devices in batch.
- **Export**: Click **Export** to export the information to the PC.
- **Delete**: Select the device, and click **Delete** to remove the selected device from the list.
- **Synchronize**: Click Synchronize, enable Synchronize, and click **OK** to synchronize the device list.
- **Upgrade**
  - **Upgrade Automatically**
    1. Click **Timing Upgrade** to pop up the settings dialog.
    2. Enable upgrading device automatically. Edit the start time and end time and click **OK** to save the settings. Upgrading will start at the set time automatically.
  - **Upgrade Manually**
    1. 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 **Upgrade** version and time.
- **Optional: Set Device Information**
  1. Click  to edit device information.
  2. Click  to delete device information from the list.
  3. Select **Status** and **Device Type** to search devices.

## 5.4. Parameter Settings

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

Remote configuration in iVMS-4200 and the Batch Configuration Tool is the same as that on the Web. Here we take the configuration on the Web as an example.

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

### 5.4.1. Local Parameters Settings

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

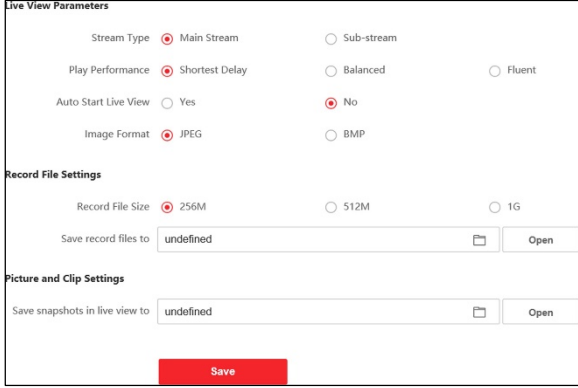


Figure 17, Local Parameters

- **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.

### 5.4.2. 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 selected.

### 5.4.3. Save record files to

- **Set the saving path for the manually recorded video files.**

Click **Save** to enable the settings.

### 5.4.4. 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.

## 5.5. System Settings

Follow the instructions below to configure the system settings, include **System Settings**, **Maintenance**, **Security**, **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.
- **About:** Click **System Settings** → **About** and click **Open Source Software Licenses** to view the details.
- **Maintenance:** Click **Maintenance** → **Upgrade & Maintenance** to enter the settings page.



Figure 18, 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 the 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.

- **Security Service**

1. Click **Security** → **Security Service** to enter the settings page.

2. Enable **SSH** according to your actual needs.

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

- **User Management**

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

2. Administrator can edit the permission for the users.



**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- **Online Users**

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

No.	User Name	Level	Each IP address' segment should be less than 256. 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	10.7.112.28	2020-02-27 15:43:23
2	admin	Administrator	10.6.113.103	2020-02-27 18:22:23

Total 2 Items

Figure 19, Online Users

2. Click Refresh to get the present information.



- **Arming/Disarming Information**

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

### 5.5.1. Network Settings TCP/IP Settings

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

#### Steps

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

The screenshot shows a web-based configuration interface for TCP/IP settings. At the top, there is a checkbox labeled 'DHCP'. Below it are several input fields: 'IPv4 Address' (empty), 'IPv4 Subnet Mask' (255.255.255.0), 'IPv4 Default Gateway' (empty), 'Mac Address' (00:40:65:a1:b6:43), 'MTU' (1500), 'Alarm Center IP' (0.0.0.0), and 'Alarm Host Port' (0). A section titled 'DNS Server' contains 'Preferred DNS Server' (8.8.8.8) and 'Alternate DNS Server' (8.8.4.4). A red 'Save' button is located at the bottom center of the form.

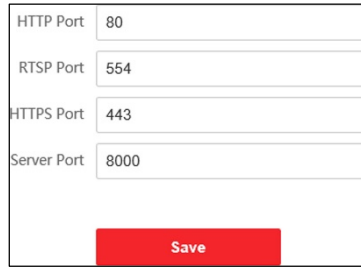
Figure 20, TCP/IP Settings

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.

### 5.5.2. Port Settings

#### Steps

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



HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000

Save

Figure 21, Port Settings

2. Set the device ports.

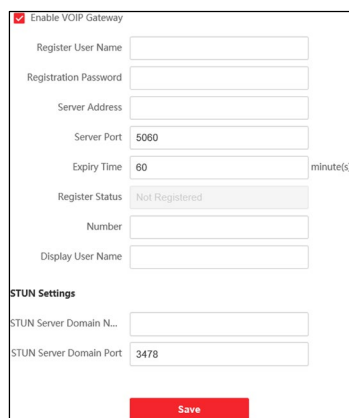
- **HTTP Port:** The default port number is 80, and it can be changed to any port no. that is not occupied.
- **HTTPS Port:** The default port number is 443, and it can be changed to any port no. that is not occupied.
- **RTSP Port:** The default port number is 554.
- **Server Port:** The default server port number is 8000, and it can be changed to any port no. ranging from 2000 to 65535.

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

### 5.5.3. SIP Setting

#### Steps

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



Enable VOIP Gateway

Register User Name

Registration Password

Server Address

Server Port

Expiry Time  minutes

Register Status

Number

Display User Name

**STUN Settings**

STUN Server Domain N.

STUN Server Domain Port

Save

Figure 22, SIP Settings

2. Check **Enable VOIP Gateway**.

3. Configure the **SIP** parameters.

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

## 5.5.4. FTP Settings

### Steps

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

Figure 23, 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.

## 5.5.5. Platform Access

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

### Steps

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

2. Check the **Enable** checkbox 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 a live image of the device, receive alarm notifications, etc.

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

**NOTE:** Use 2 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 eight letters or numbers.

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

## 5.5.6. 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 24, 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:** Set 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**, six levels of video quality are selectable.
- **Frame Rate:** Set the frame rate. The frame rate describes the frequency at which the video stream is updated and is measured in 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. A higher value corresponds to higher video quality, but more bandwidth is required.
- **Video Encoding:** The device supports H.264.
- **I Frame Interval:** Set the I Frame Interval from 1 to 400.

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

## 5.5.7. Audio Parameters

### Steps

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

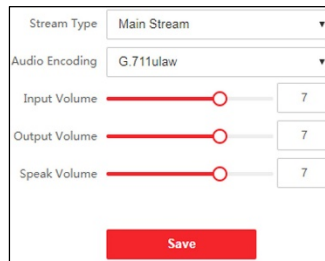


Figure 25, Audio Settings

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

- **Stream Type:** Set the stream type to **Main Stream** or **Sub Stream**.
- **Audio Encoding:** The device support G.711ulaw and G.711alaw.

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

**NOTE:** Available volume range: 0 to 10.

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

## 5.6. Image Settings

### 5.6.1. 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.

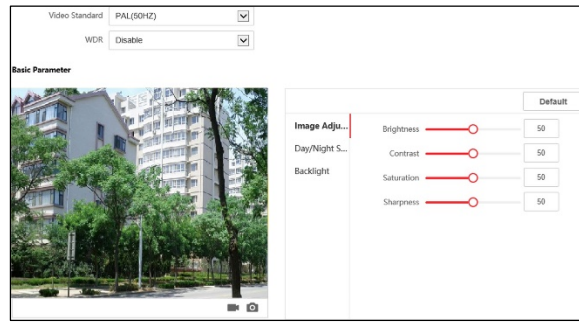


Figure 26, Display Settings

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**: The image brightness, which ranges from 1 to 100.
  - **Contrast**: The image contrast, which ranges from 1 to 100.
  - **Saturation**: The intensity of the image color, which ranges from 1 to 100.
  - **Sharpness**: The edge contrast of the image, which ranges from 1 to 100.
4. Set the **Day/Night Mode**.

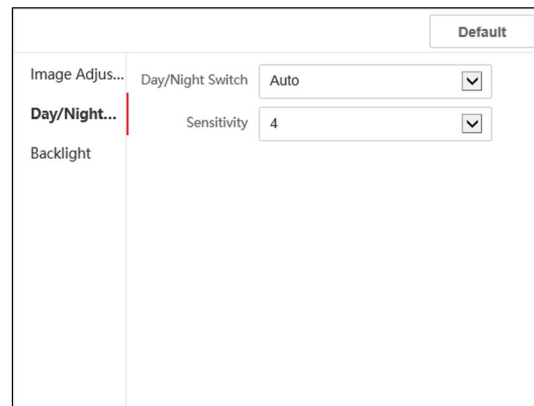


Figure 27, Day/Night Mode

- 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. Set the backlight parameters.

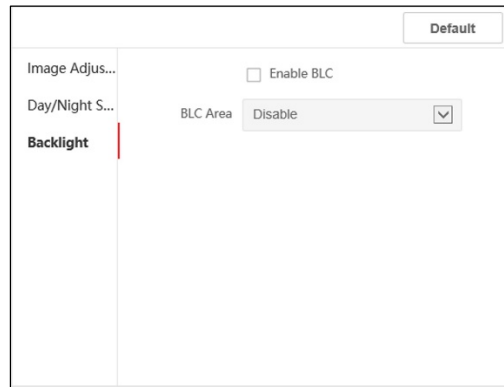


Figure 28, Backlight

- 1) Check the checkbox to enable **BLC**.
- 2) Select **BLC Area**.
6. Click **Save** to enable the settings.

### 5.6.2. OSD Settings



You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

#### Steps

1. Click **Image** → **OSD Settings** to enter the settings page.
2. Check the corresponding checkbox to select the display of camera name, date, or week if required.
3. Edit the **Camera Name**.
4. Select from the drop-down list to set the **Time Format** and **Date Format**.
5. Adjust the **OSD** position.
6. Click **Save** to enable the settings.

### 5.6.3. Target Cropping

#### Steps

1. Click **Image** → **Crop** to enter the page.
2. Check **Enable Target Cropping** to enable the function.
3. Click  to crop photo.
4. Click  to crop video.
5. Select **Cropping Resolution**.
6. Click **Save**.

**NOTE:** You can select the **Cropping Resolution** as 704\*576, 1280\*720, or 1920\*1080.

You can zoom in to or zoom out of the image by selecting **Cropping Resolution** after clicking **Save**.

## 5.7. Event Settings

### 5.7.1. Motion Detection

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

#### Steps

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

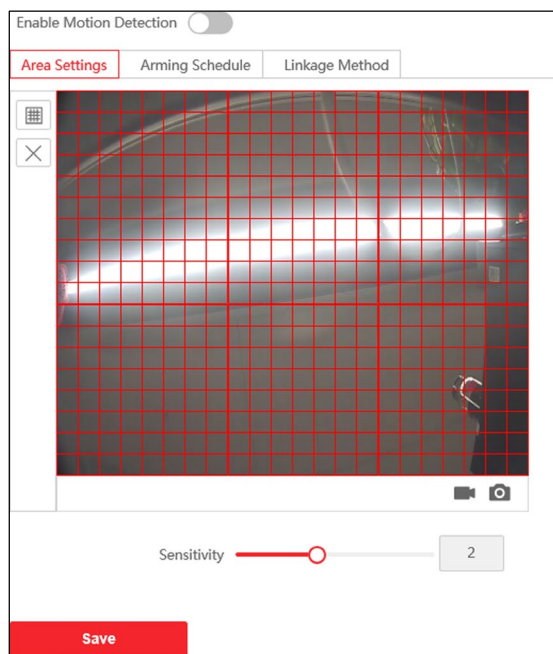


Figure 29, Motion Detection

2. Slide **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 **Save** to save the settings.
  - **Clear Area:** Click **X** to clear all areas.
  - **Adjust Sensitivity:** Move the slider to set the detection sensitivity.
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.



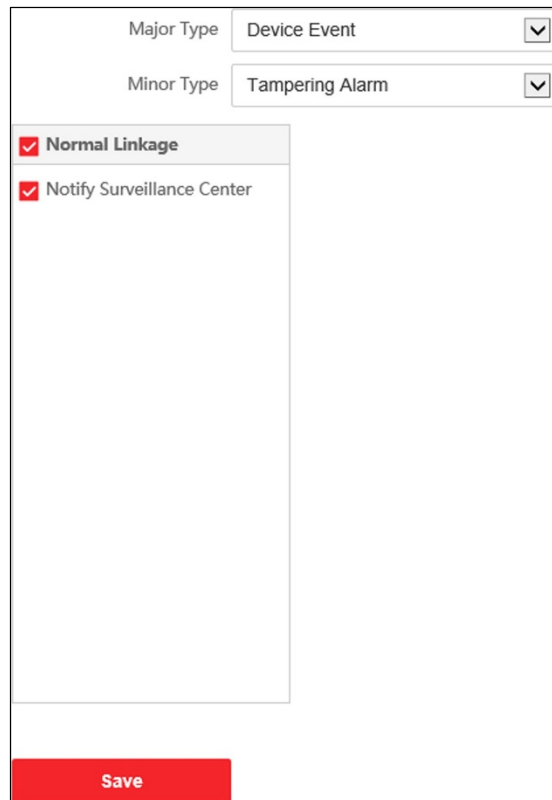
- **Notify Surveillance Center:** Send an exception or alarm signal to the remote management software when an event occurs.

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

## 5.7.2. Event Linkage

### Steps

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



The screenshot shows the 'Event Linkage' configuration interface. At the top, there are two dropdown menus: 'Major Type' is set to 'Device Event' and 'Minor Type' is set to 'Tampering Alarm'. Below these, there is a section titled 'Normal Linkage' with a red checkmark icon. Under this section, the option 'Notify Surveillance Center' is also checked with a red checkmark. At the bottom of the form, there is a prominent red 'Save' button.

Figure 30, Event Linkage

2. Set 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.

## 5.7.3. Schedule Settings

You can create a call schedule, or the device will call the indoor station all day by default.

### Steps

1. Click **Schedule** → **Video Intercom** → **Call Schedule**.
2. Click the next row below **Enable Indoor Station All Day by Default**.
3. Enter **Schedule Name**.

4. Select **Call Type**.
5. Set **Weekly Schedule**.
  - 1) Click **Weekly Schedule**.

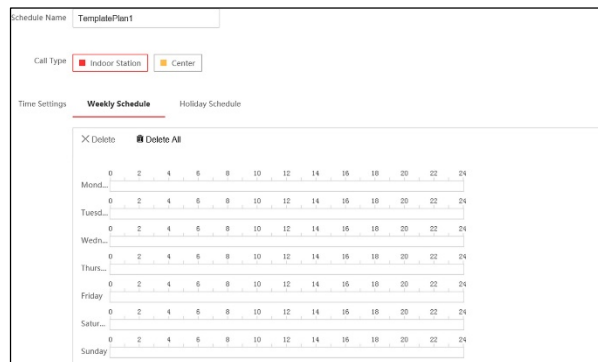


Figure 31, Weekly Schedule

- 2) Drag mouse to set the schedule according to the actual needs.
  - 3) Optional: Click the copy icon to copy the schedule to other days according to the actual needs.
  - 4) Click **Save**.
6. Set **Holiday Schedule**.
    - 1) Click **Holiday Schedule**.

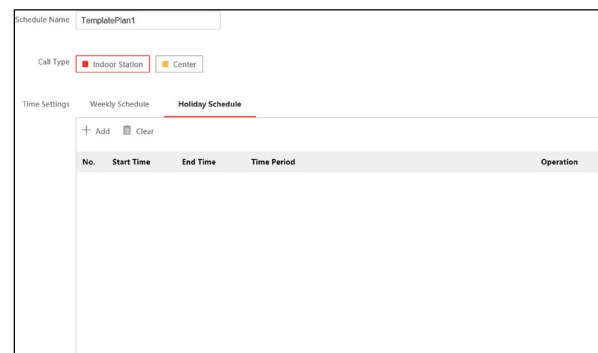


Figure 32, Holiday Schedule

- 2) Click **Add**.
- 3) Set **Start Time** and **End Time**.
- 4) Select **Call Type**.
- 5) Drag mouse to set the schedule according to the actual needs.
- 6) Click **OK**.
- 7) You can edit or delete the schedule according to the actual needs.
- 8) Click **Save**.

**NOTE:** The holiday schedule has higher priority than the weekly schedule when you set the two schedules at the same time.

## 5.8. Intercom Settings

### 5.8.1. Device ID Configuration

#### Steps

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

Device Type	Villa Door Station
Building No.	1
Floor No.	1
Door Station No.	0
<b>Advanced Settings</b>	
Community No.	1
Unit No.	1
<b>Save</b>	

Figure 33, Device ID Settings

2. Select the device type from the drop-down list, and set the corresponding information including Building No., Floor No., Door Station No., Community No., and Unit No.
3. Click **Save** to enable the device number configuration.

**NOTE:** For main door station (D series or V series), the no. is 0.

For sub door station (D series or V series), the no. cannot be 0. The no. of sub door station 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 station (D series or V series) can be customized.

For one main door station (D series or V series), up to eight sub door stations can be configured.

### 5.8.2. Linked Network Settings

#### Steps

1. Go to **Intercom** → **Session Settings** to enter the settings page.
2. Set **Register Number** and **Registration Password**.
3. Get the **Main Station** IP address and the **Video Intercom Server** IP address.
4. Enable **Protocol 1.0**.

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

### 5.8.3. Time Parameters

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

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

**NOTE:** Max. call duration between the module indoor station and client ranges from 90s to 120 s. The call will end automatically when the actual call duration is longer than the configured one.

Max. message duration ranges from 30 s to 60 s. The message will end automatically when the actual message duration is longer than the configured one.

Max. ring duration refers to the maximum duration of the module indoor station when it is called without being accepted. Max. ring duration ranges from 65 s to 255 s.

## 5.9. Ring-Back Tone Settings

Click **Intercom** → **Ringbacktone Settings** to enter the settings page. Click **Add** to select the ring tone from the PC.

**NOTE:** Available Audio Format: WAV, AAC; size: less than 600 KB; sample rate: 8000 Hz, Mono.

### 5.9.1. Press Button to Call

#### Steps

1. Go to **Intercom** → **Press Button to Call** to enter the settings page.

No.	Button Settings	Link Time Schedule
01	1	Enable Indoor Station All Day by [v]

**Save**

Figure 34, Press Button to Call

2. Edit **Room No.** in the button settings and select **Link Time Schedule**.

**NOTE:** The number of buttons may vary by model. Please refer to the actual product.

For schedule settings, refer to *Schedule Settings* for details.

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

### 5.9.2. Number Settings

Link the **Room No.** and **SIP** numbers. Click **Number Settings** to enter the page.

+ Add		Delete	
No.	Room No.	SIP Number	Operation

Figure 35, Number Settings

Click **Add**, set the **Room No.** and **SIP** numbers in the pop-up dialog box.

### 5.9.3. Access Control Settings Door Parameters

#### Steps

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

Door No. Door1

Name Door1

Open Duration 2

Door Contact  Remain Closed  Remain Open

Save

Figure 36, Door Parameters

2. Select the door and edit the door name.
3. Edit **Open Duration**.
4. Set door contact status.
5. Click **Save** to enable the settings.

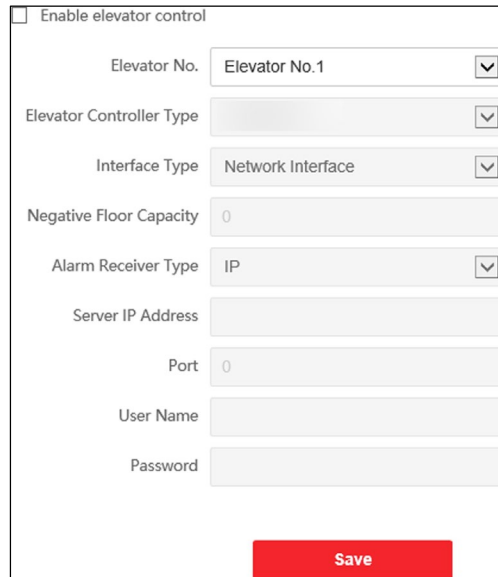
## 5.10. Elevator Control

#### Before You Start

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

#### Steps

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



The screenshot shows a configuration form titled "Enable elevator control" with a checkbox. Below the checkbox are several fields: "Elevator No." (dropdown menu showing "Elevator No.1"), "Elevator Controller Type" (dropdown menu), "Interface Type" (dropdown menu showing "Network Interface"), "Negative Floor Capacity" (text input field with "0"), "Alarm Receiver Type" (dropdown menu showing "IP"), "Server IP Address" (text input field), "Port" (text input field with "0"), "User Name" (text input field), and "Password" (text input field). A red "Save" button is located at the bottom right of the form.

Figure 37, 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. Set the **Interface Type** as **RS-485** or **Network Interface**, and enable the elevator control.
  - **RS-485:** Make sure you connected the door station to the elevator controller with an RS-485 cable.
  - **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 four elevator controllers can be connected to one door station.

Up to 10 negative floors can be added.

Make sure the elevator controller interface types connected to the same door station are consistent.

## 6. Configuration via Client Software

### 6.1. Device Management

Device management includes device activation, add device, edit device, delete device, etc.

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

#### 6.1.1. Add Online Device

##### Before You Start

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

##### Steps

1. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter the 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 38, Add to the Client

## 6.1.2. Add Device by IP Address

### Steps

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

## 6.1.3. Add Device by IP Segment

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

### Steps

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

## 6.2. 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 go to live view.
3. Optional: On the **Live View** page, control-click and select **Capture** to get a picture of the live view.

## 6.3. Organization Management

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

### 6.3.1. Add Organization

#### Steps

1. On the organization list on the left, click **+Add**.
2. Enter the **Organization Name** as desired.
3. Click **OK** to save the adding.
4. Optional: Add multiple levels of organizations, as desired.
  - Add multiple levels of organizations according to the actual needs.



- The added organization will be the sub-organization of the upper-level organization.

**NOTE:** Up to 10 levels of organizations can be created.

### 6.3.2. Modify and Delete Organization

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

## 6.4. Person Management

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

**NOTE:** Up to 2,000 persons can be added.

Up to five cards can be added to each person.

### 6.4.1. Add Person

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

#### Steps

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

**NOTE:** The Person No. will be generated automatically and is editable.

2. Set basic person information.

- 1) Enter basic information: name, gender, tel, birthday details, effective period, and e-mail address.

**NOTE:** The person's name must be fewer than 15 characters.

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

**NOTE:** The photo should be in \*.jpg format.

- **Upload:** Select the person's photo from the local PC to upload it to the client.
- **Take Photo:** Take the person's photo with the PC camera.
- **Remote Collection**

3. Issue the card for the person.

- 1) Click **Credential** → **Card**.
4. Take the person's photo with the collection device.
  - 1) Click **+** to pop up the **Add Card** dialog.
  - 2) Select **Normal Card** as **Card Type**.
  - 3) Enter the **Card No.**
  - 4) Click **Read** and the card will be issued to the person.
5. Link the device to the person.
  - 1) Set the linked devices.
    - **Linked Device:** Binds the indoor station to the person.

**NOTE:** If you select **Analog Indoor Station** as the Linked Device, the **Door Station** field will display. Select the door station to communicate with the analog indoor station.

  - **Room No.:** The room no. of the person.
  - 2) Click **OK** to save the settings.
6. Click **Add** to save the settings.

### 6.4.2. Modify and Delete Person

Select the person and click **Edit** to open the editing person dialog. To delete the person, select a person and click **Delete** to delete it.

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

### 6.4.3. Change Person to Other Organization

You can move the person to another organization if needed.

#### Steps

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

### 6.4.4. Import and Export Person Information

The person information can be imported and exported in batch.

## Steps

- **Exporting Person:** You can export the added persons' information in Microsoft Excel format to a 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 Microsoft Excel file.
  3. Check the checkboxes to select the person information to export.
  4. Click **OK** to start exporting.
- **Importing Person:** You can import the Microsoft 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.

### 6.4.5. Get Person Information from Device

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

## Steps

**NOTE:** This function is supported only by devices that used the TCP/IP connection method when added.

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:** Person's information (person details, person's fingerprint information (if configured), and linked card (if configured), will be imported to the selected organization.

If the person's name stored in the device is empty, the person's name will be filled with the issued card no. after importing to the client.

The person's gender will be **Male** by default.

## 6.4.6. Issue Card in Batch

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

### Steps

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

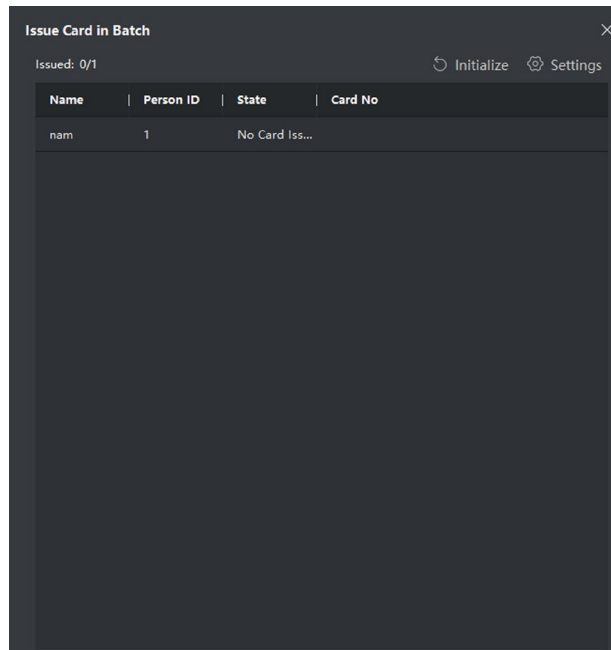


Figure 39, Issue Card in Batch

2. Click **Settings**.

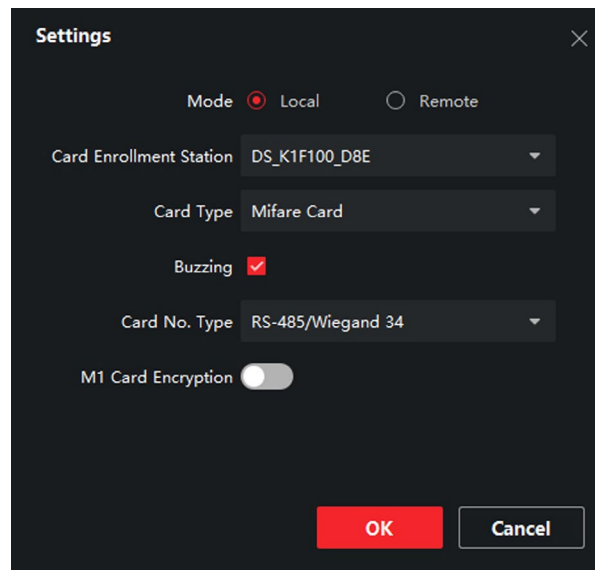


Figure 40, Card Settings


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 on the **Person(s) with Card Issued** list.

## 6.4.7. Permission Settings

### Add Permissions

#### Steps

1. On the main page, click  **AccessControllInfo** → **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 permission settings page, click  to edit the parameters of the permission.

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

## 6.5. Video Intercom Settings

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

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

Add the device to the software and configure the person to link the device in the Access Control module before configuring remotely.


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

## 6.5.1. Receive Call from Door Station

### Steps

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

### Adjust the Loudspeaker Volume

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

### Adjust the Microphone Volume

- Click  to adjust the microphone volume.

### Open Door Remotely

- For door station, click  to open the door remotely.

**NOTE:** One video intercom device can connect with only one client software.

The maximum ring duration can be set from 15s to 60s via the video intercom device's Remote Configuration.

The maximum speaking duration between an indoor station and the iVMS-4200 can be set from 120s to 600s via the indoor station's Remote Configuration.

The maximum speaking duration between a door station and the iVMS-4200 can be set from 90s to 120s via the door station's Remote Configuration.

## 6.5.2. Release Notice

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

### Before You Start

Make sure the person has been added to the client.

### Steps

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

5. Click **View** to select the picture.

6. Click **Send**.

**NOTE:** Up to 63 characters are allowed in the **Subject** field.

Up to six pictures in jpg format can be added to one notice. The maximum size of one picture is 512 KB.

Up to 1023 characters are allowed in the **Information** field.

### 6.5.3. Search Video Intercom Information

#### Search Call Logs

#### Steps

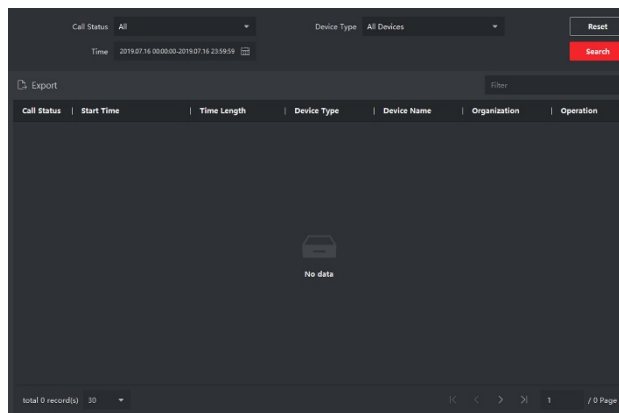


Figure 41, Search Call Logs

1. On the **Video Intercom** page, click **Call Log** to enter the page.
2. Set the search conditions, including call status, device type, start time, and end time.
  - **Call Status:** Click **v** 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 **v** 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.
  1. Click **Search**, and all the matched call logs will display on this page.
  2. **Optional:** Check the detailed information of searched call logs such as call status, ring/speaking duration, device name, resident organization, etc.
  3. **Optional:** Input keywords in the Search field to filter the desired log.

4. 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 matching notices will display on this page.
4. Optional: Click **Export** to export the notices to your PC.

## 6.5.4. Upload Armed Information

### Steps

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

**NOTE:** When a device is added to the client software, the device is armed by default.  
When a device is armed, the alarm logs upload to the client software automatically.  
Click **Alarm Application** → **Event Search** to search the alarm logs.

3. Optional: Click **Arm All** or **Disarm All** to arm or disarm all devices.



# Appendix: 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 42, Communication Matrix QR Code

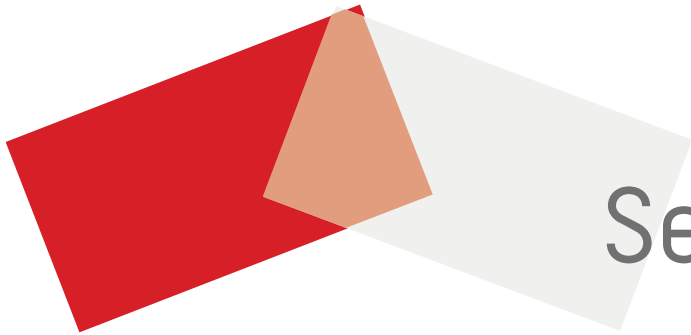
## Device Command

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 43, Device Command



See Far, Go Further