



HIKVISION

Video Intercom Door Station (V Series)

User Manual

UD.6L0206D1104A01

User Manual

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

This user manual is intended for users of the models below:

Series	Model
Door Station (V Series)	DS-KV8102-IM
	DS-KV8202-IM
	DS-KV8402-IM
	DS-KV8102-IP
	DS-KV8102-VP

It includes instructions on how to use the Product. The software embodied in the Product is governed by the user license agreement covering that product.

About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. (“Hikvision”) reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks

HIKVISION and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES

FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, SECURITY BREACHES, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF OR RELIANCE ON THIS MANUAL, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY OR CERTAIN DAMAGES, SO SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

Support

Should you have any questions, please do not hesitate to contact your local dealer.

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.

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

FCC Conditions

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

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the R&TTE Directive 1999/5/EC, the EMC Directive 2004/108/EC, 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.



Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into **Warnings** and **Cautions**:

Warnings: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

	
Warnings Follow these safeguards to prevent serious injury or death.	Cautions Follow these precautions to prevent potential injury or material damage.



Warnings

- 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.)



Cautions

- 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.

Table of Contents

1 Overview	1
1.1 Introduction.....	1
1.2 Main Features.....	1
2 Appearance	2
2.1 Appearance of DS-KV8X02-IM.....	2
2.2 Appearance of DS-KV8102-XP.....	3
3 Typical Application	4
3.1 Typical Application of DS-KV8X02-IM.....	4
3.2 Typical Application of DS-KV8102-XP.....	4
4 Terminals and Interfaces of Wiring	7
5 Installation and Wiring	8
5.1 Installation of DS-KV8X02-IM.....	8
5.1.1 Gang Box for DS-KV8X02-IM.....	8
5.1.2 Wall Mounting with Gang Box of DS-KV8X02-IM.....	9
5.2 Installation of DS-KV8102-XP.....	10
5.2.1 Installation Plate for DS-KV8102-XP.....	10
5.2.2 Wall Mounting with Gang Box of DS-KV8102-XP.....	11
5.3 Wiring Description.....	13
5.3.1 Door Lock Wiring.....	13
5.3.2 Door Magnetic Wiring.....	14
5.3.3 Exit Button Wiring.....	14
5.3.4 Alarm Device Input Wiring.....	15
6 Before You Start	16
7 Video Intercom Device Set-up Tool	17
7.1 Setting a Community Structure.....	17
7.1.1 Setting Project.....	17
7.1.2 Setting Community.....	18
7.1.3 Setting Building.....	19
7.1.4 Setting Floor.....	19
7.1.5 Setting Room.....	20
7.2 Activating and Setting Main Door Station.....	21
7.3 Activating and Setting Sub Door Station.....	22
8 Batch Configuration Tool	25
8.1 Activating Device Remotely.....	25
8.2 Editing Network Parameters.....	26
8.3 Adding Device.....	27
8.3.1 Adding Online Devices.....	27

8.3.2 Adding by IP Address or IP Segment	28
8.4 Remote Configuration	29
8.4.1 System	29
8.4.2 Video Intercom	36
8.4.3 Network	40
8.4.4 Video Display	42
9 Setting the Door Station via iVMS-4200	44
9.1 System Configuration	44
9.2 Device Management	44
9.3 Live View of Device	45
9.4 Picture Storage on Storage Server	46
9.4.1 Adding Storage Server	46
9.4.2 Formatting the HDDs	47
9.4.3 Configuring Storage Server Picture Storage	48
9.5 Group Management	49
9.5.1 Adding Group	50
9.5.2 Assigning Device to Group	51
9.5.3 Modifying Device Information	52
9.5.4 Deleting Device	52
9.6 Card Management	53
9.6.1 Unauthorized Card Management	53
9.6.2 Normal Card Management	59
9.7 Notice Management	60
9.7.1 Querying Unlocking Log	60
9.8 Device Arming Control	60
10 Local Operation	62
10.1 Calling Resident	62
10.1.1 Calling Resident (DS-KV8X02-IM)	62
10.1.2 Calling Resident (DS-KV8102-XP)	63
10.2 Issuing Card	64
10.3 Unlocking Door	64
Appendix	66
Installation Notice	66
Wiring Cables	66
Specification of DS-KV8X02-IM	66
Specification of DS-KV8102-XP	68

1 Overview

1.1 Introduction

The door station (V series) can realize functions such as video intercom, access control, one-card system, zone alarm, and visitor messages to form a complete smart community video intercom solution.

The door station (V series) is mainly applied in the villa, and can work as door station, outer door station, and doorphone.

1.2 Main Features

- Video intercom function
- HD video surveillance (Max. resolution 1280×720@25fps, WDR, 120° wide angle)
- Self-adaptive light supplement
- Access control function
- Activating card via local station function (This function will be invalid if the card has been activated via iVMS-4200)
- Auto-uploading captured pictures to FTP or iVMS-4200 Client while unlocking the door
- Door magnetic alarm and tamper alarm function
- Noise suppression and echo cancellation
- Remote upgrade, batch setting functions

2 Appearance

2.1 Appearance of DS-KV8X02-IM

For device DS-KV8X02-IM, the number of calling buttons varies according to its model. Take the figure of device DS-KV8402-IM as an example.



- For device DS-KV8102-IM, there is only 1 calling button.
- For device DS-KV8202-IM, there are 2 calling buttons.
- For device DS-KV8402-IM, there are 4 calling buttons.

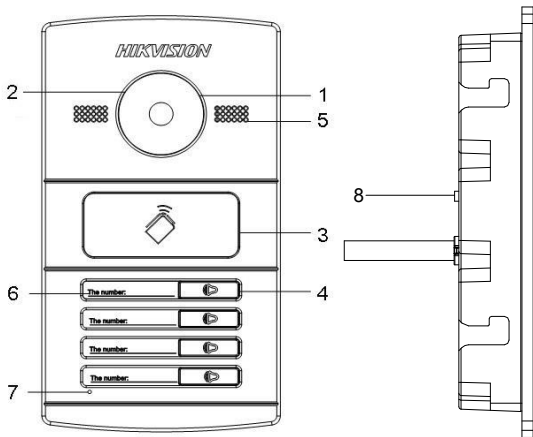


Figure 2-1 Appearance of DS-KV8402-IM

Table 2-1 Description of DS-KV8X02-IM

Models	No.	Description
DS-KV8102-IM DS-KV8202-IM DS-KV8402-IM	1	Low Illumination Supplement Light
	2	Built-in Camera
	3	Card Induction Area
	4	Calling Button
	5	Loudspeaker
	6	Room No. (Customized)

Models	No.	Description
	7	Microphone
	8	Tamper Button



You need not customize the Room No. for device DS-KV8102-IM.

2.2 Appearance of DS-KV8102-XP

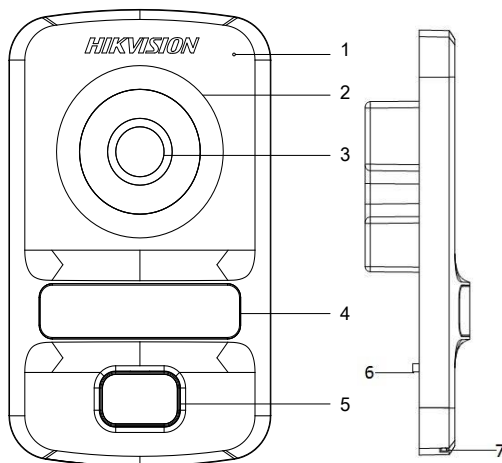


Figure 2-2 Appearance of DS-KV8102-XP

Table 2-2 Description of DS-KV8102-XP

Models	No.	Description
DS-KV8102-IP DS-KV8102-VP	1	Microphone
	2	Low Illumination Supplement Light
	3	Built-in Camera
	4	Card Induction Area
	5	Calling Button
	6	Tamper Button
	7	Loudspeaker

3 Typical Application

3.1 Typical Application of DS-KV8X02-IM

Please refer to the following figure for typical application of DS-KV8102-IM/ DS-KV8202-IM/ DS-KV8402-IM door station.

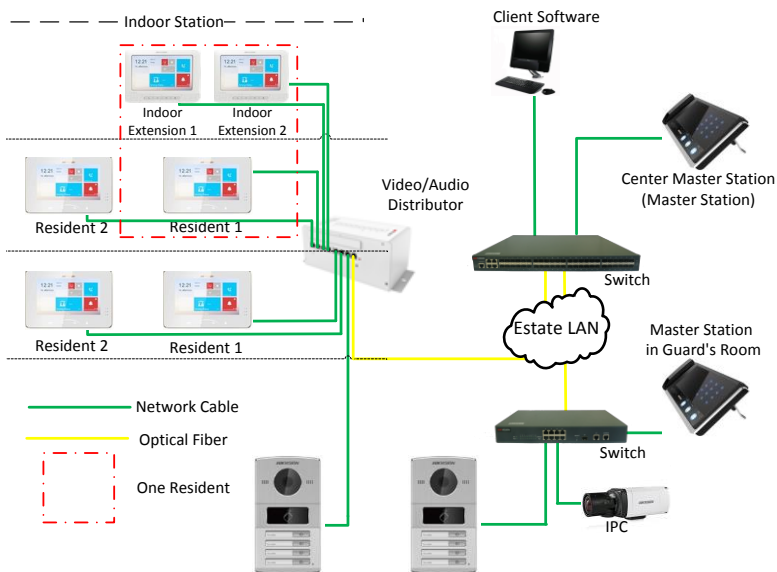


Figure 3-1 Typical Application



DS-KV8102-IM door station can also work as doorphone both in a villa or an apartment. Please refer to the typical application (2) and the typical application (3) in 3.2.

3.2 Typical Application of DS-KV8102-XP

Please refer to the following figures for typical applications of DS-KV8102-IP/ DS-KV8102-VP door station.



DS-KV8102-IP/ DS-KV8102-VP door station can also work as doorphone both in a villa or an apartment. Please refer to the typical application (2) and the typical application (3).

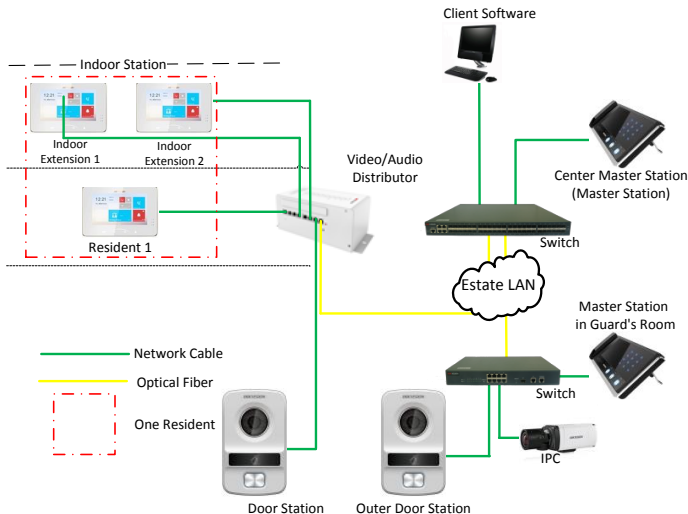


Figure 3-2 Typical Application (1)

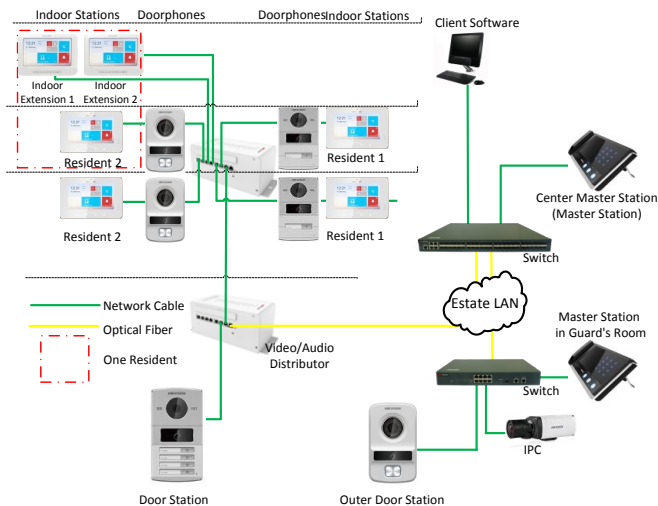


Figure 3-3 Typical Application (2)



In typical applicatin (2), DS-KV8102-IP/ DS-KV8102-VP door station and DS-KV8102-IM door station work as doorphone in a villa.

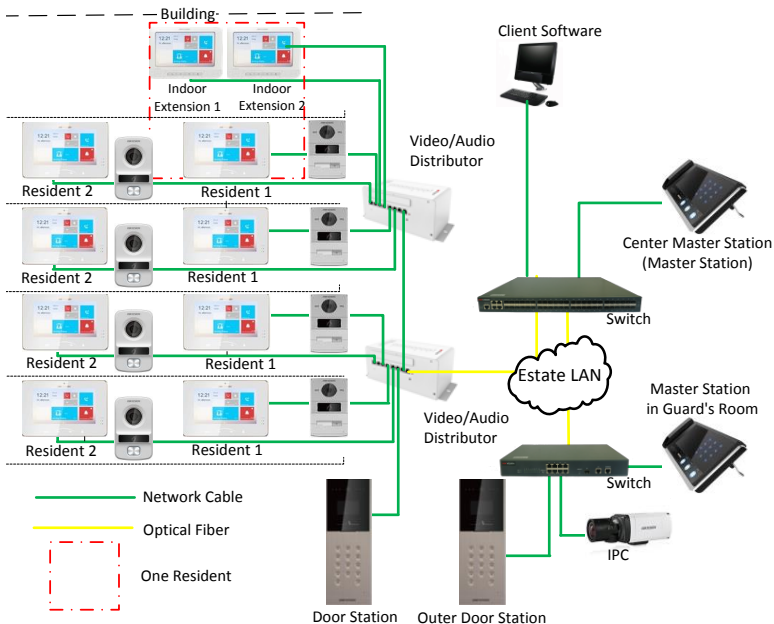


Figure 3-4 Typical Application (3)



In typical applicatin (3), DS-KV8102-IP/ DS-KV8102-VP door station and DS-KV8102-IM door station work as doorphone in an apartment.

4 Terminals and Interfaces of Wiring

Please refer to the following figure for terminals and interfaces of door station.

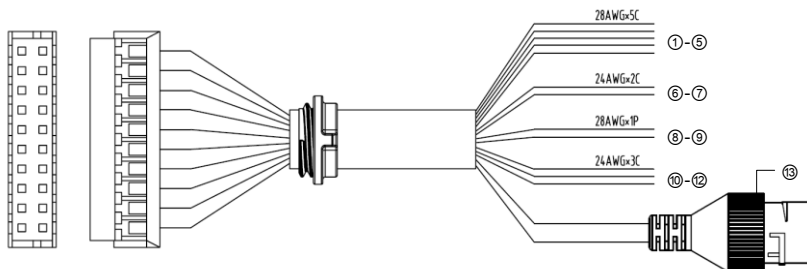


Figure 4-1 Terminals and Interfaces

Table 4-1 Descriptions of Terminals and Interfaces

Terminals and Interfaces			
Name	No.	Color	Description
ALARM IN	1	YELLOW/BLUE	ALARM_1
	2	YELLOW/ORANGE	ALARM_2
	3	YELLOW/GREEN	ALARM_3
	4	YELLOW/BROWN	ALARM_4
	5	YELLOW/BLACK	ALARM_GND
Power Supply	6	RED	DC 12V Power Supply Input
GND	7	BLACK	Grounding
RS485	8	ORANGE	RS485+
	9	YELLOW	RS485-
ALARM OUT	10	PINK	DR_NC
	11	BLUE	DR_NO
	12	BROWN	DR_COM
LAN	13	LAN	Network Interface



- 4 I/O Input terminals (ALARM_1~ALARM_4) can be set as door magnetic input or door switch key input, and terminal ALARM_GND is for grounding connection.
- 1 I/O Output terminal can be enabled for controlling electric lock or disabled.

5 Installation and Wiring

5.1 Installation of DS-KV8X02-IM

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

5.1.1 Gang Box for DS-KV8X02-IM

Please refer to the following figures for the dimensions of gang box for DS-KV8102-IM/ DS-KV8202-IM/ DS-KV8402-IM door station.

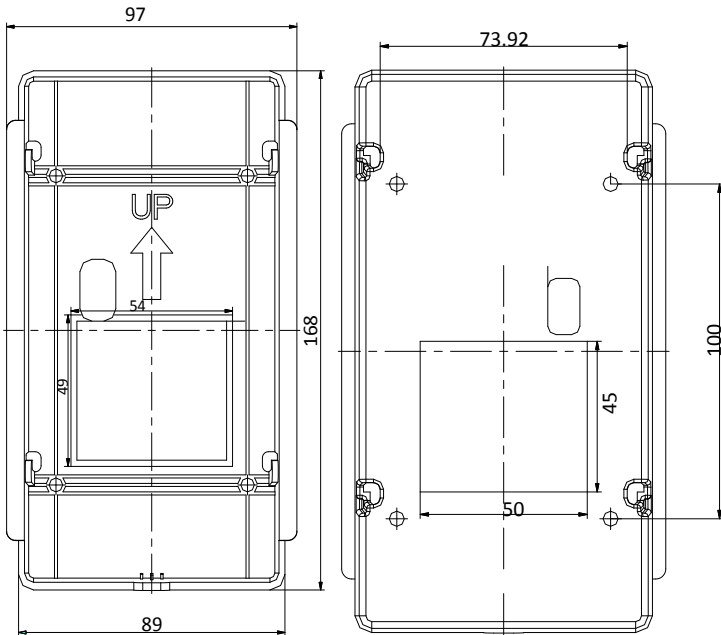


Figure 5-1 Front View & Rear View (DS-KV8X02-IM)



- The dimension of gang box for model DS-KV8102-IM/ DS-KV8202-IM/ DS-KV8402-IM door station is: 89 (width) × 168 (length) × 38 (depth) mm.
- The dimensions above are theoretical. The actual size can be slightly different from the theoretical dimension.

5.1.2 Wall Mounting with Gang Box of DS-KV8X02-IM

Steps:

1. Take the gang box and screws from the packing box.
2. Chisel a hole in the wall for inserting the gang box. The size of the hole should be 90 (width) × 170 (length) × 38 (depth) mm.
3. Insert the gang box into the hole and fix it with 4 PA4 screws, as shown in the figure below.

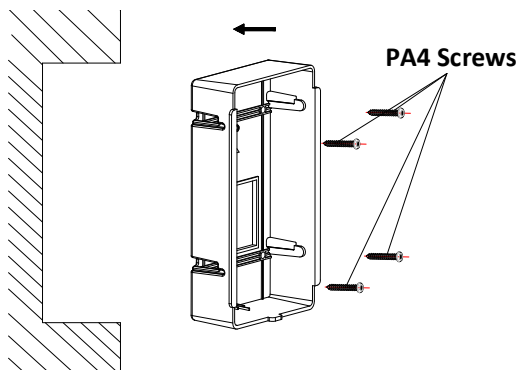


Figure 5-2 Insert the Gang Box (DS-KV8X02-IM)

4. After fixing the gang box, install the door station into the gang box according to the direction of the arrow, as shown in the figure below.

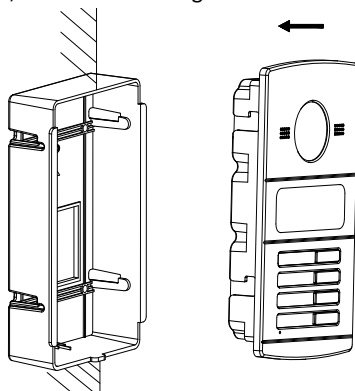


Figure 5-3 Insert the Door Station (DS-KV8X02-IM)

5. After inserting the door station into the gang box, pull the device downwards to hook the door station with the gang box.
6. Secure the door station by inserting the fixing screw according to the direction of the arrow of the figure below.

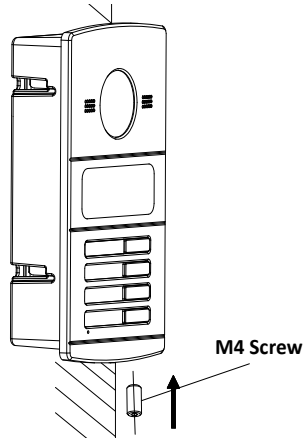


Figure 5-4 Secure the Door Station (DS-KV8X02-IM)

5.2 Installation of DS-KV8102-XP

5.2.1 Installation Plate for DS-KV8102-XP

To install the DS-KV8102-XP model onto the wall, an installation plate and a gang box are required.

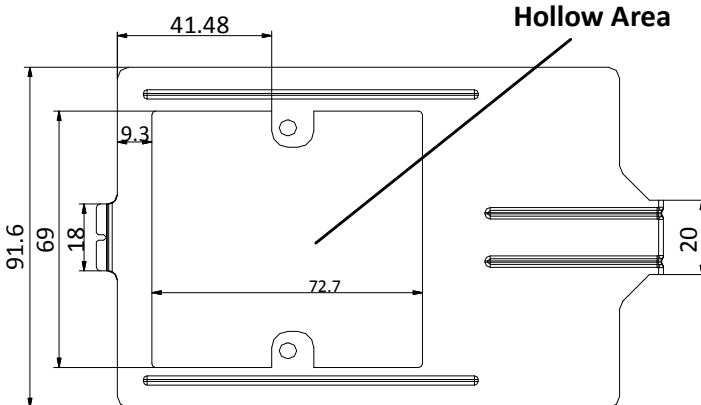


Figure 5-5 Dimensions of Installation Plate (DS-KV8102-XP)



- The dimension of gang box for model DS-KV8102-IP/ DS-KV8102-VP door station is: 75 (width) × 75 (length) × 50 (depth) mm.
- The dimensions above are theoretical. The actual size can be slightly different from the theoretical dimension.

5.2.2 Wall Mounting with Gang Box of DS-KV8102-XP

Steps:

1. Take the gang box, installation plate and screws from the packing box.
2. Chisel a hole in the wall for inserting the gang box. The size of the hole should be 76 (width) × 76 (length) × 50 (depth) mm.
3. Insert the gang box into the hole, as shown in the figure below.

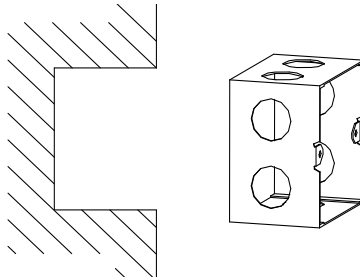


Figure 5-6 Insert the Gang Box (DS-KV8102-XP)

4. Attach the installation plate to the gang box and align the screw holes of the installation plate with the screw holes of the gang box.
5. Insert 2 PA4 screws and a KA4 screw into the screw holes to fix the installation plate onto the gang box. (The KA4 screw is optional.)

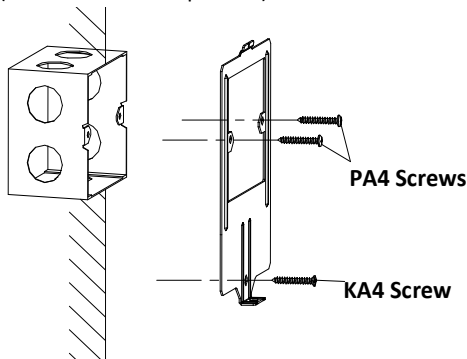


Figure 5-7 Attach the Installation Plate (DS-KV8102-XP)

- After installing the installation plate, install the door station by inserting the rear component into the hollow area of the installation plate.



While inserting the door station into the installation plate, incline the device by 5~10° , as shown in the figure below.

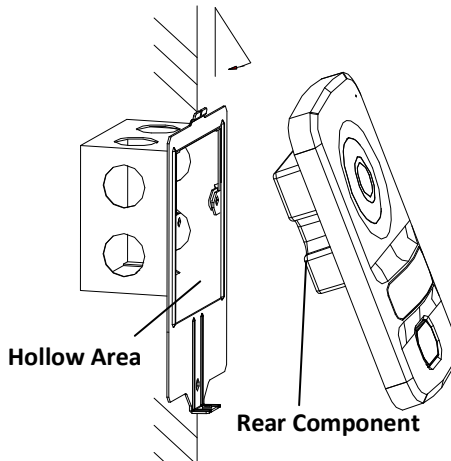


Figure 5-8 Install the Door Station (DS-KV8102-XP)

- Secure the door station by inserting the fixing screw according to the direction of the arrow of the figure below.

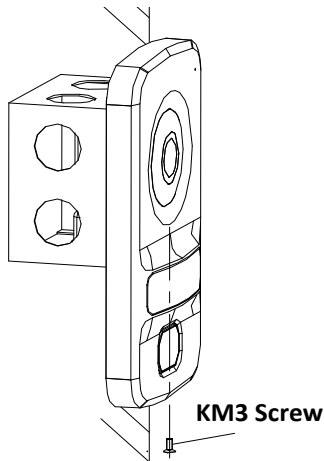


Figure 5-9 Secure the Door Station (DS-KV8102-XP)

5.3 Wiring Description

5.3.1 Door Lock Wiring

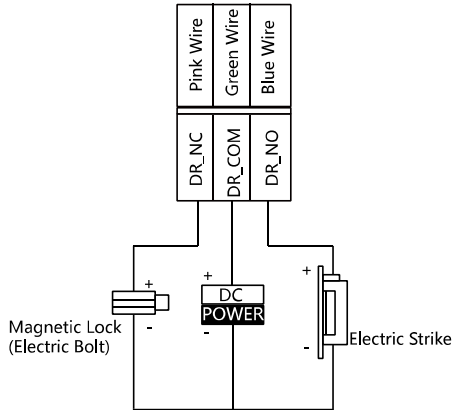


Figure 5-10 Door Lock Wiring



- Terminal DR_NC/DR_COM is set as default for connecting magnetic lock/electric bolt; terminal DR_NO/DR_COM is set as default for connecting electric strike.
- To connect electric lock, it is required to set the output of terminal DR_NC/DR_COM/DR_NO to be electric lock with Batch Configuration Tool or iVMS-4200 client software.

5.3.2 Door Magnetic Wiring

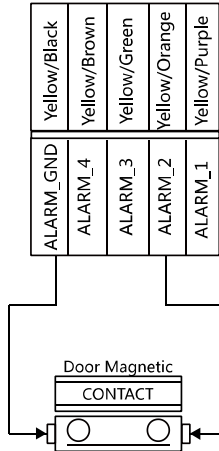


Figure 5-11 Door Magnetic Wiring



To connect door magnetic, it is required to set the input of one alarm in terminal (ALARM_1, ALARM_2, ALARM_3, or ALARM_4) to be door magnetic with Batch Configuration Tool or iVMS-4200 client software.

5.3.3 Exit Button Wiring

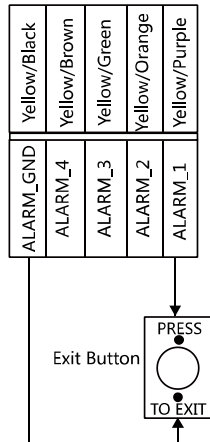


Figure 5-12 Exit Button Wiring



To connect exit button, it is required to set the input of one alarm in terminal (ALARM_1, ALARM_2, ALARM_3, or ALARM_4) to be exit button with Batch Configuration Tool or iVMS-4200 client software.

5.3.4 Alarm Device Input Wiring

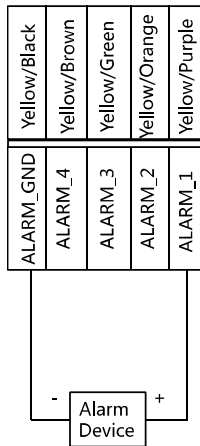


Figure 5-13 Alarm Device Input Wiring



To connect other alarm devices, it is required to set the input of one alarm in terminal (ALARM_1, ALARM_2, ALARM_3, or ALARM_4) to be custom with Batch Configuration Tool or iVMS-4200 client software.

6 Before You Start

For the first time use of the device, you are required to activate the device. You can activate the device and set the device password via internet with Batch Configuration Tool, or with iVMS-4200 client software, or with Video Intercom Set-up Tool.



To activate the device with Video Intercom Device Set-up Tool, refer to Chapter 7.

To activate the device with Batch Configuration Tool or iVMS-4200, refer to Chapter 8 and Chapter 9.

Please refer to 8.1 for creating the device password.

7 Video Intercom Device Set-up Tool

Purpose:

You can assign the device to the community, active and set the device by using the video intercom device set-up tool.

7.1 Setting a Community Structure

Purpose:

You can set a community structure, based on the real community situation, on the video intercom device set-up tool, and then assign devices to the community accordingly.



The concept Project, be self-defined in every individual application, is used to describe a collection of communities. A project can involve multi communities. While if there is only 1 community in a project, the default project No. is 1.

7.1.1 Setting Project

Steps:

1. Run the software to enter the main interface of video intercom device set-up tool.

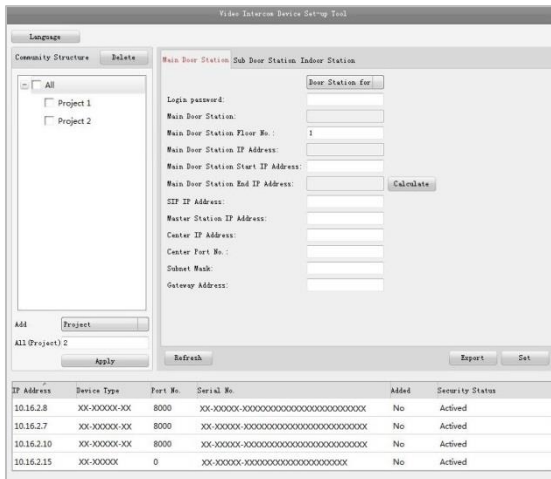


Figure 7-1 Main Interface of Device Set-up Tool

2. Select Project from the drop-down list and enter a number in the textbox to set the amount of project.



Figure 7-2 Project Settings

3. Click the **Apply** button to enable the settings.



The default amount of project is 1 if the amount is not set in the textbox.

7.1.2 Setting Community

Steps:

1. Check the checkbox of a certain project from the community structure.
2. Select Community from the drop-down list and enter a number in the textbox to set the amount of community.

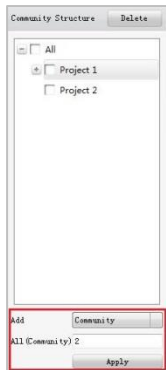


Figure 7-3 Community Settings

3. Click the **Apply** button to enable the settings.



If you check the checkbox of **All**, then all projects in the community structure will be selected, and will be added the same amount of community.

7.1.3 Setting Building

Steps:

1. Check the checkbox of a certain community from the community structure.
2. Select Building from the drop-down list and enter a number in the textbox to set the amount of building.

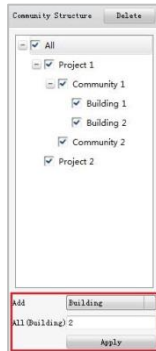


Figure 7-4 Building Settings

3. Click the **Apply** button to enable the settings.



- If you check the checkbox of **All**, then all communities in the community structure will be added the same amount of building.
- If you check the checkbox of a certain project, then all communities in the selected project will be added the same amount of building.

7.1.4 Setting Floor

Steps:

1. Check the checkbox of a certain building from the community structure.
2. Select Floor from the drop-down list and enter a number in the textbox to set the amount of floor.

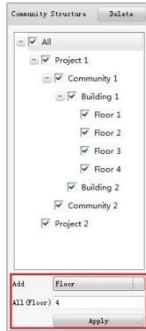


Figure 7-5 Floor Settings

3. Click the **Apply** button to enable the settings.



- If you check the checkbox of **All**, then all buildings in the community structure will be added the same amount of floor.
- If you check the checkbox of a certain project, then all buildings in the selected project will be added the same amount of floor.
- If you check the checkbox of a certain community, then all buildings in the selected community will be added the same amount of floor.

7.1.5 Setting Room

Steps:

1. Check the checkbox of a certain floor from the community structure.
2. Select Room from the drop-down list and enter a number in the textbox to set the amount of room

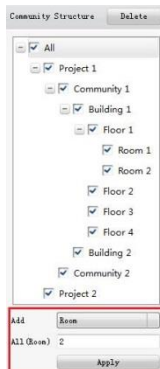


Figure 7-6 Room Settings

3. Click the **Apply** button to enable the settings.



- If you check the checkbox of **All**, then all floors in the community structure will be selected, and will be added the same amount of room.
- If you check the checkbox of a certain project, then all floors in the selected project will be added the same amount of floor.
- If you check the checkbox of a certain community, then all floors in the selected community will be added the same amount of floor.
- If you check the checkbox of a certain building, then all floors in the selected building will be added the same amount of floor.

7.2 Activating and Setting Main Door Station

Purpose:

You can activate the online main door station, and configure the building number of online main door station.

Before You Start:

Press the **Main Door Station** tab to switch to the main door station settings.

Steps:

1. Select the community to configure the building number for the main door station.

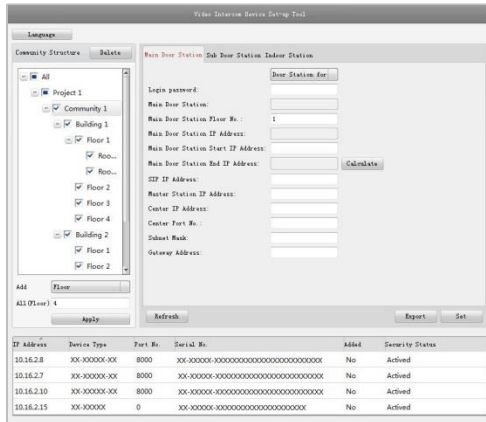


Figure 7-7 Selecting Community

2. Enter the main door station start IP address.
3. Click the **Calculate** button to generate the main door station end IP address automatically.

4. Set the main door station floor No..
5. Enter the SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
6. Click the **Refresh** button to view the online indoor station of the same segment.
7. Select a door station and enter the login password.
8. Click the **Set** button to accomplish the settings of main door station.

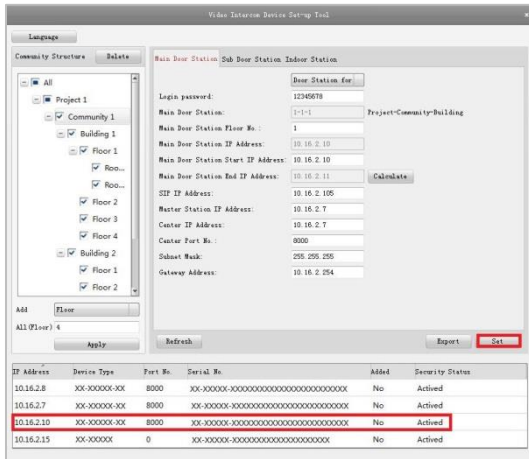


Figure 7-8 Main Door Station Settings Interface



- The default main door station floor No. is 1.
- You can select one project or multiple projects; one community or multiple communities; one building or multiple buildings.
- The Main Door Station IP Address is usually set to be the same as Start IP Address of main door station.
- If the main door station is not activated, create a login password and enter it in the textbox to activate the device.
- If the main door station is not activated, the device is configured and activated simultaneously by clicking the **Set** button.
- When the device is successfully configured, it prompts the note: Configuring main door station parameters succeeded.

7.3 Activating and Setting Sub Door Station

Purpose:

You can activate the online sub door station, and configure the number of online sub door station.

Before You Start:

Press the **Sub Door Station** tab to switch to the sub door station settings.

Steps:

1. Select the community to configure the number for the sub door station.

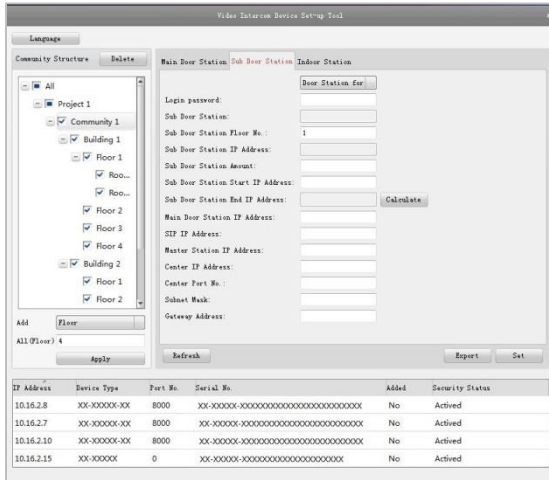


Figure 7-9 Selecting Community

2. Set the sub door station floor No..
3. Set the sub door station amount.
4. Enter the sub door station start IP address.
5. Click the **Calculate** button to generate the sub door station end IP address automatically according to the sub door station amount.
6. Enter the main door station IP address, SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
7. Click the **Refresh** button to view the online indoor station of the same segment.
8. Select a door station and enter the login password.
9. Click the **Set** button to accomplish the settings of sub door station.

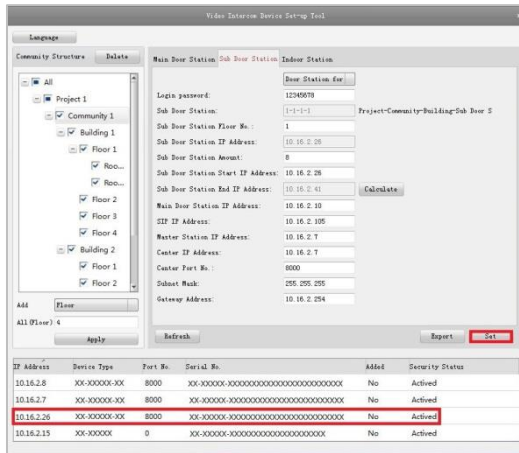


Figure 7-10 Sub Door Station Settings Interface



- The default sub door station floor No. is 1.
- The sub door station amount should be no higher than 8.
- You can select one project or multiple projects; one community or multiple communities; one building or multiple buildings.
- The Sub Door Station IP Address is usually set to be the same as Start IP Address of sub door station.
- If the sub door station is not activated, create a login password and enter it in the textbox to activate the device.
- If the sub door station is not activated, the device is configured and activated simultaneously by clicking the Set button.
- When the device is successfully configured, it prompts the note: Configuring sub door station parameters succeeded.

8 Batch Configuration Tool

8.1 Activating Device Remotely

Purpose:

The device cannot be operated until it is activated. You can remotely activate the device via Batch Configuration Tool or via iVMS-4200 client. Here take the Batch Configuration Tool as example, and for further information, please refer to the user manual in the disk.

Steps:

1. Run the software, and select the inactivated device from the online devices and click the **Activate** button.

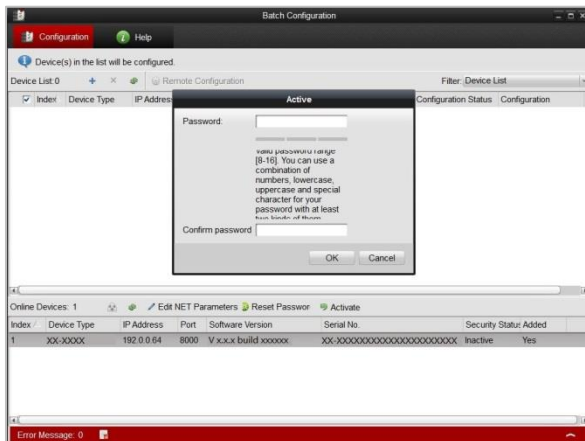


Figure 8-1 Activating Device

2. Create a password, and enter the password into the password field.



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (Using a minimum of 8 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. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Confirm the password.
4. Click the **OK** button to activate the device.



When the device is not activated, the basic operation and remote operation of device cannot be performed.

8.2 Editing Network Parameters

Purpose:

You can edit the network parameters of online devices.

Steps:

1. Select an online device in the online devices list in the lower part of the batch configuration software interface.
2. Click the **Edit NET Parameters** button.



Figure 8-2 Edit NET Parameters

3. Enter a new IP address, subnet mask, gateway address, port No. and the password.
4. Click the **OK** button to accomplish the editing.

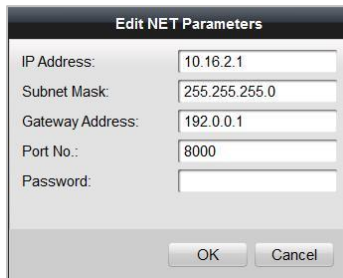


Figure 8-3 Edit Network Parameters



- The default port No. is 8000.
- After editing the network parameters of device, you should add the devices to the device list again.
- When you edit network parameters remotely, the device should be in the same network segment.

8.3 Adding Device

The software provides 3 ways for adding the door station (V series). You can add the active online devices within your subnet, add devices by IP address, and add devices by IP segment.

8.3.1 Adding Online Devices

Steps:

1. Run the software to enter the main interface of video intercom batch configuration tool software.

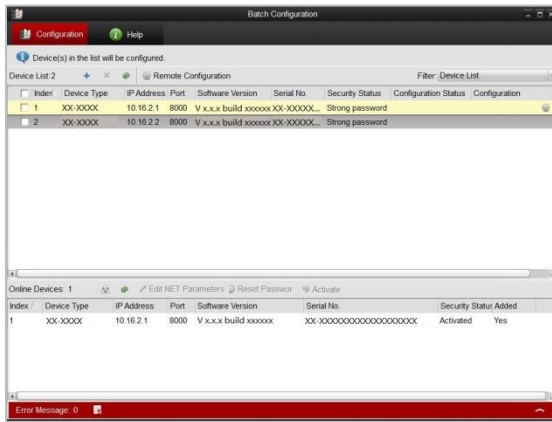



Figure 8-4 Main Interface of Batch Configuration Software

2. Select an online device or hold the **Ctrl** or **Shift** key to select multiple devices in the online devices list in the lower part of the batch configuration software interface.



Figure 8-5 Online Devices Interface

3. Click the  button to pop up the login dialog box.

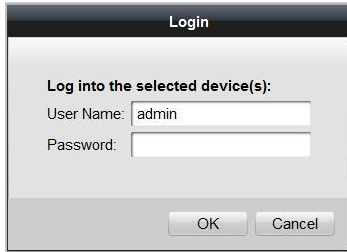



Figure 8-6 Login Dialog Box

4. Enter the user name and password.
5. Click the **OK** button to save the settings.



Only the devices that are successfully logged in will be added to the device list for configuration.

8.3.2 Adding by IP Address or IP Segment.

Click the  button to pop up the adding devices dialog box.

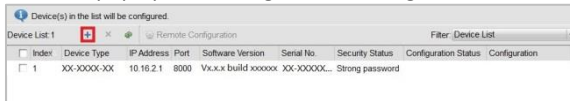


Figure 8-7 Adding Button

● Adding by IP Address

Purpose:

You can add the device by entering IP address.

Steps:

1. Select IP Address in the adding mode drop-down list.
2. Enter the IP address, and set the port No., user name and password of the device.

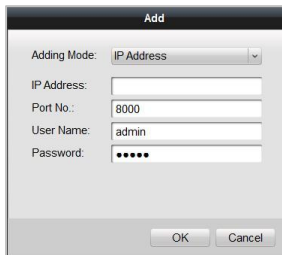


Figure 8-8 Adding by IP Address

3. Click the **OK** button to add the device to the device list.

● Adding by IP Segment

Purpose:

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



Steps:

1. Select IP Segment in the adding mode drop-down list.
2. Set the Start IP Address and End IP Address.
3. Enter port No., user name, and password.

Figure 8-9 Adding by IP Segment

4. Click the **OK** button to search and add the devices whose IP addresses are within the range of the defined IP segment to the device list.

8.4 Remote Configuration

In the device list area, select a device and click  **Remote Configuration** or  to enter the remote configuration interface.

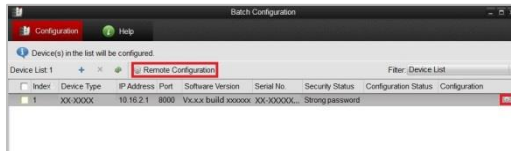


Figure 8-10 Remote Configuration

8.4.1 System

Click the **System** button on the remote configuration interface to display the device information: **Device Information**, **General**, **Time**, **System Maintenance**, **User**, and **RS485**.

Device Information

Click the **Device Information** button to enter device basic information interface. You can view basic information (the device type, and serial No.), and version information of the device.

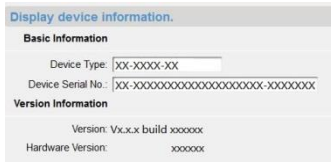


Figure 8-11 Device Information Interface

General

Click the **General** button to enter device general parameters settings interface. You can view and edit the device name and device ID.

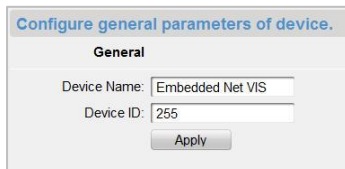


Figure 8-12 Device General Parameters Settings Interface

Time

Steps:

1. Click the **Time** button to enter the device time settings interface.



Figure 8-13 Time Settings Interface

2. Select Time Zone or Enable NTP.

- **Time Zone**

- 1) Select a time zone from the drop-down list menu.
- 2) Click the **Synchronization** button.

- **NTP**

- 1) Check the checkbox of **Enable NTP** to enable NTP.
- 2) Enter the server address, NTP port, and synchronization interval.
3. Click the **Apply** button to save and realize the time settings.



The default Port No. is 123.

System Maintenance

Purpose:

You can operate the system management and remote upgrading on the system maintenance interface.

Steps:

1. Click the **System Maintenance** button to enter the system maintenance interface.

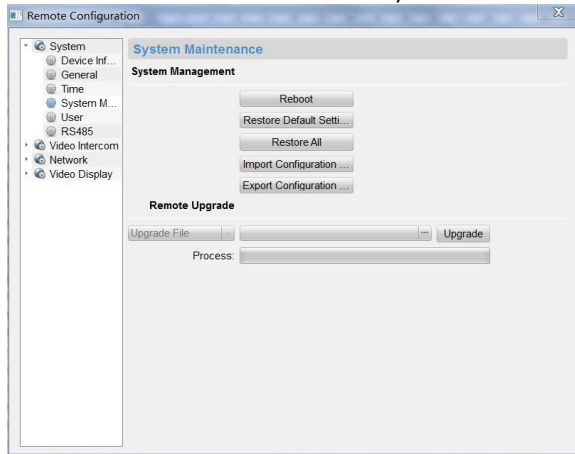


Figure 8-14 System Maintenance Interface

2. Select **System Management** or **Remote Upgrade**.
 - **System Management**
 - **Reboot**
 - 1) Click the **Reboot** button to pop up the reboot dialog box.

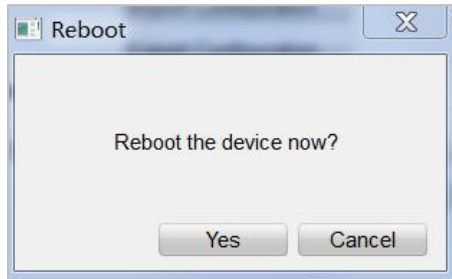


Figure 8-15 Reboot

- 2) Click the **Yes** button to reboot the system.
- **Restore Default Settings**
- 1) Click the **Restore Default Settings** button to pop up the restore default settings dialog box.



Figure 8-16 Restore Default Settings

- 2) Click the **Yes** button to restore the default parameters.
- **Restore All**
- 1) Click the **Restore All** button to pop up the restore all settings dialog box.

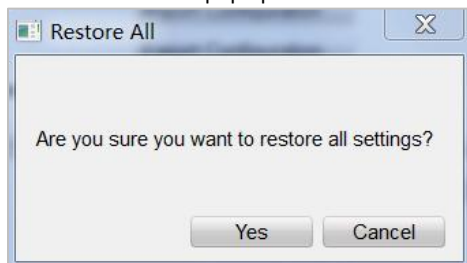


Figure 8-17 Restore All Settings

- 2) Click the **Yes** button to restore all parameters of device and reset the device to inactive status.
- **Import Configuration File**
- 1) Click the **Import Configuration File** button to pop up the import file window.

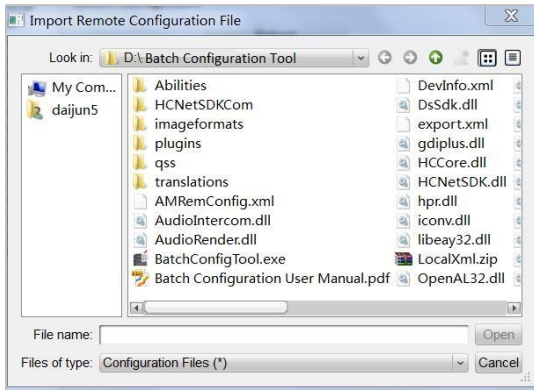


Figure 8-18 Import Configuration File Window

- 2) Select the path of remote configuration files.
- 3) Click the **Open** button to import the remote configuration file and pop up a reboot information dialogue box.

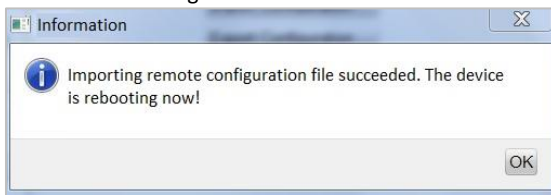


Figure 8-19 Reboot Information

- **Export Configuration File**

- 1) Click the **Export Configuration File** button to pop up the export file window.

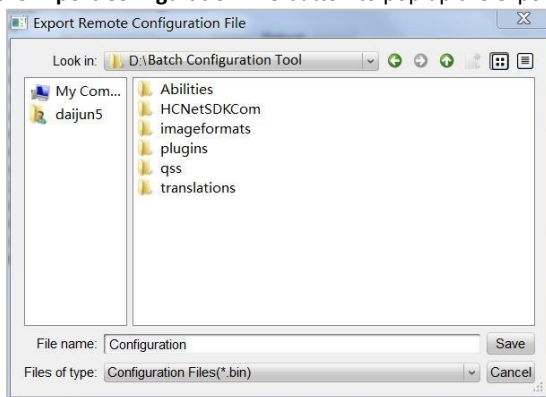


Figure 8-20 Export Configuration File Window

- 2) Select the save path of remote configuration files.

- 3) Click the **Save** button to export the configuration file, and pop up an information box for exporting.

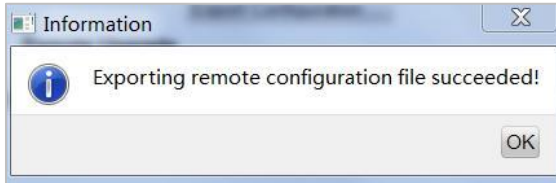


Figure 8-21 Information Box for Exporting

- **Remote Upgrade**
- **Reboot**

- 1) Click the button to pop up the window for opening upgrade file.

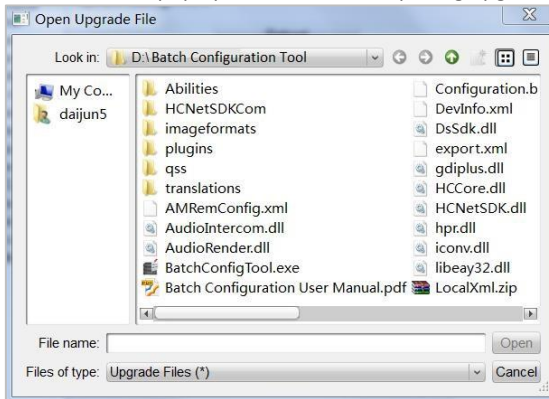


Figure 8-22 Window for Opening Upgrade File

- 2) Select the upgrade file, and click the Open button.
- 3) Click the **Upgrade** button to remotely upgrade the device.

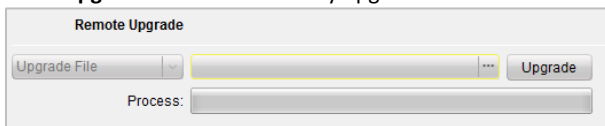


Figure 8-23 Remote Upgrade

User

Purpose:

You can edit the password to log in the device.

Steps:

1. Click the **User** button to enter the user information editing interface

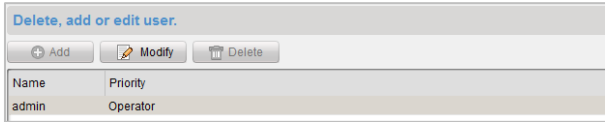


Figure 8-24 User Information Editing Interface

2. Select the user to edit and click the **Modify** button to enter the user parameter interface.

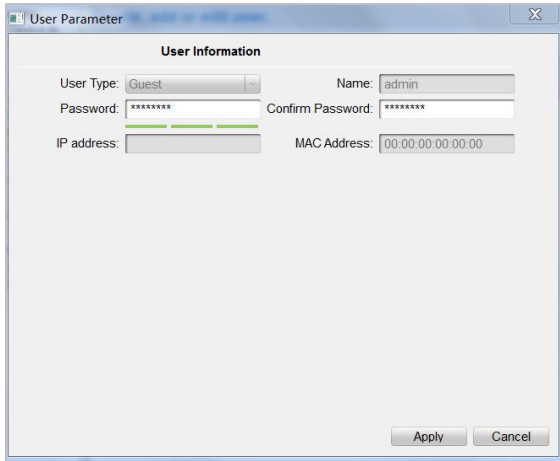



Figure 8-25 User Parameter Interface

3. Enter the new password, and confirm it.
4. Click the **Apply** button to realize the editing of password.



- The new password and confirm password should be identical.
- After editing the password of device, click  button from the device list, the added device will not be there. You should add the device again with new password to operate the remote configuration.

RS485

Click the **RS485** button to enter the RS485 settings interface. You can view and edit the RS485 parameters of the device.

Figure 8-26 RS485 Parameters



RS485 configuration is reserved in this version.

8.4.2 Video Intercom

Device Number Configuration

Steps:

1. Click the **Device Information** button to enter device number configuration interface.

- **Door Station**

1) Select door station from the drop-down list of the device type

Figure 8-27 Device Number Configuration (V Series Door Station)

2) Enter the project No., community No., building No., floor No., and serial No.

3) Select **Yes** or **No** from the drop-down list menu of auto login.

- **Doorphone**

1) Select doorphone from the drop-down list of the device type.



Figure 8-28 Device Number Configuration (Doorphone)

2) Select **Yes** or **No** from the drop-down list menu of auto login.

1. Click the **Apply** button to enable the device number configuration.



- For V series door station, the default serial No. is 0. When the serial No. is 0, the device is main door station, and when the serial No. is larger than 0, the device is sub door station. The serial No. is numeric from 1 to 99.
- For each main door station, at most 8 sub door stations can be installed.
- For doorphone, the serial No. is not necessary to be configured. Please use the doorphone along with the main door station (V series or D series).
- The models DS-KV8102-IP, DS-KV8102-VP and DS-KV8102-IM are supported for using as doorphone and door station (V Series). The models DS-KV8202-IM, DS-KV8402-IM are supported for using only as door station (V Series).

Time Parameters

1. Click the **Time Parameters** button to enter time parameters settings interface.

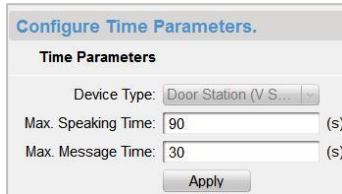


Figure 8-29 Time Parameters Settings Interface

2. Set the maximum speaking time and the maximum message time.

3. Click the **Apply** button to enable the time parameters settings.



Maximum speaking time cannot exceed 120s; and maximum visitor message time cannot exceed 60s.

Access Control and Elevator

1. Click the **Access Control and Elevator** button to enter password changing interface.

Configure parameters of access control and elevator control.

Access Control

Door No.: 1

Door-Unlocked Duration: 15 (s)

Apply

Elevator Control

Elevator No.: 0

Interface:

RS485 Protocol:

LAN Protocol:

Elevator Linkage: No

Server IP Address:

Server Port No.:

Apply

Figure 8-30 Access Control and Elevator Settings Interface

2. Set corresponding parameters on the access control and elevator settings interface.

- **Access Control**

- 1) Select the door No..
- 2) Set the door-unlocked duration.
- 3) Click the **Apply** button to enable the settings.

- **Elevator Control**

- 1) Select the elevator No., interface, RS485 protocol.
- 2) Select Yes/No of the elevator linkage.
- 3) Enter the server IP address and server port No..
- 4) Click the Apply button to enable the settings.



The doorphone does not support the elevator control function.

I/O Input and Output

Steps:

1. Click the **I/O Input and Output** button to enter the I/O input and output interface.

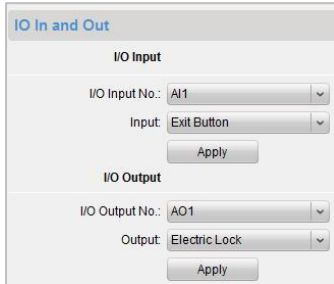


Figure 8-31 I/O Input and Output Interface

2. Select I/O input No., input mode, I/O output No., and output mode.
3. Click the **Apply** button to enable the settings.



- There are 4 I/O Input Terminals, Terminal 1~4 correspond to **ALARM_1~ALARM_4** interfaces of door station. You can enable/disable IO In or set IO In as door magnetic or door switch by selecting from the dropdown list.
- There is only 1 I/O Output Terminals, which corresponds to **DR_NC/DR_COM/DR_NO** interface of door station. You can enable/disable IO Out or set IO Out as electric lock by selecting from the dropdown list.

Volume Input and Output

Click the **Volume Input and Output** button to enter the volume input and output interface. Slide the slider to adjust the volume input and volume output.

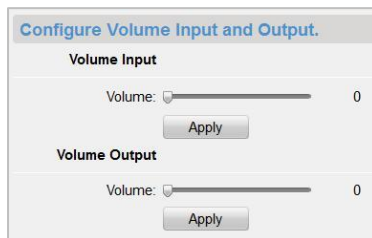


Figure 8-32 Volume Input and Output Interface

Calling Buttons

1. Click the **Calling Buttons** button to enter the calling buttons settings interface.

Configure Key Call Household parameters.

Calling Buttons

Button Number: 1

Floor No.: 0

Room No.: 0

Apply

Figure 8-33 Calling Buttons Interface

2. Select the button number.
3. Enter the floor No. and the room No..
4. Click the **Apply** button to enable the settings.



For DS-KV8102-IM, DS-KV8102-IP, and DS-KV8102-VP, there is no need setting the Room No..

8.4.3 Network

Local Network Configuration

Steps:

1. Click the **Local Network Configuration** button to enter the local network configuration interface.

Configure local network parameters.

Local Network Configuration

Local IP Address: 10.16.2.2

Subnet Mask: 255.255.255.0

Gateway Address: 192.0.0.1

Port No.: 8000

Apply

Figure 8-34 Local Network Configuration Interface

2. Enter the local IP address, subnet mask, gateway address, and port No..
3. Click the **Apply** button to enable the settings.



- The default port No. is 8000.
- After editing the local network parameters of device, you should add the devices to the device list again.

Linked Devices Network Configuration

Purpose:

On the linked devices network configuration interface, you can configure the network parameters of master stations, SIP servers and management centers of the same LAN.

Steps:

1. Click the **Linked Device Network Configuration** button to enter the devices network configuration interface.

Figure 8-35 Linked Devices Network Configuration Interface

2. Select the device type from the drop-down list.
3. Enter the IP address of the master station, SIP server address, management center IP address, and management center port No..
4. Click the **Apply** button to link the master station, SIP server and management center to the device.



- After adding master station IP address, the linkage between door station and master station can be realized.
- After adding SIP server address, the video intercom of the same community can be realized, such as the video intercom between indoor stations of different building, calling indoor station from outer door station and video intercom between management center and indoors.
- After adding management center IP address, the events can be uploaded to the management center.

FTP

Steps:

1. Click the **FTP** button to enter the FTP parameters interface.

Figure 8-36 FTP Parameters Interface

2. Check the checkbox of **Enable Main FTP**.
3. Select IP address from the drop-down list of server mode.
4. Enter the FTP server address, and port No..
5. Check the checkbox to enable the anonymity (optional).
6. Enter the name and password.
7. Select the directory structure and set the separator, naming item, and naming element.
8. Click the **Apply** button to enable the FTP parameters settings.



- The default port No. is 21.
- To enable anonymity or not is according to whether the FTP server enables anonymity.
- After configuring the FTP parameters, the captured pictures of door station will be uploaded to the FTP server automatically.
- **The doorphone does not support the FTP function.**

8.4.4 Video Display

Steps:

1. Click the **Video Display** button to enter the video parameters interface.

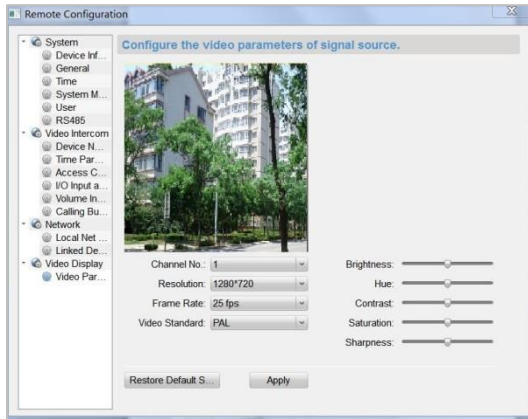


Figure 8-37 Video Parameters Interface

2. Select the channel No.
3. Select the resolution, frame rate, and video format.
4. Select to enable/disable WDR.
5. Set the WDR level.
6. Set the brightness, hue, contrast, saturation, and sharpness of the video.
7. Click the **Apply** button to enable the settings.



Click the **Restore Default Settings** button to restore all parameters excluding network parameters to the factory settings.

9 Setting the Door Station via iVMS-4200

9.1 System Configuration

After running the iVMS-4200, enter **Control Panel -> Maintenance and Management -> System Configuration -> Video Intercom** to configure the video intercom parameters accordingly.

You can configure the ringtone, Max. ring duration, Max. speaking time with indoor station and Max. speaking time with door station.

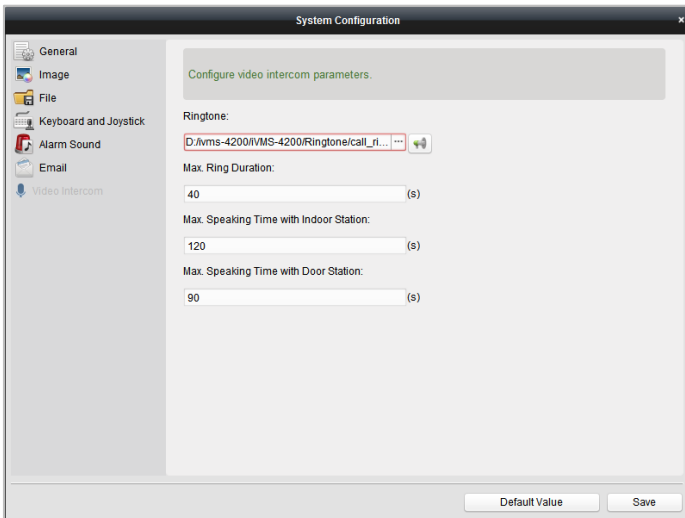


Figure 9-1 System Configuration Interface

9.2 Device Management

Device management includes device activation, adding device, editing device, deleting device and remote configuration. Please refer to Chapter 8 Batch Configuration Tool for detailed information.



- To add door station (V Series) to iVMS-4200 client software, you should add it as encoding device.
- You can add at most 16 door stations to iVMS-4200 client software.

9.3 Live View of Device

Steps:

1. Enter the main view interface of iVMS-4200 client software to display the live view of door station (V Series).



Figure 9-2 Live View of Door Station (V Series)

2. Right click on the live view interface to display the menu and select **Unlock Door** to remote unlock the door.

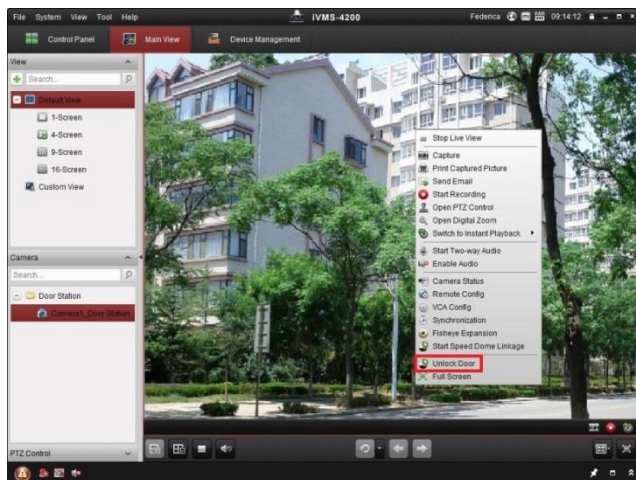


Figure 9-3 Menu of Live View Interface

9.4 Picture Storage on Storage Server


9.4.1 Adding Storage Server

Purpose:

When the device is under armed status, it will capture the picture automatically after unlocking the door. The captured picture can be uploaded and stored in the storage server.

Before you start:

The storage server application software needs to be installed and it is packed in the iVMS-4200 software package. When installing the iVMS-4200, check the checkbox **Storage Server** to enable the installation of storage server.

1. Click the icon  on the desktop to run the storage server.
2. Open the Device Management page and click the **Server** tab.
3. Click **Add New Device Type**, select **Storage Server** and click **OK**.

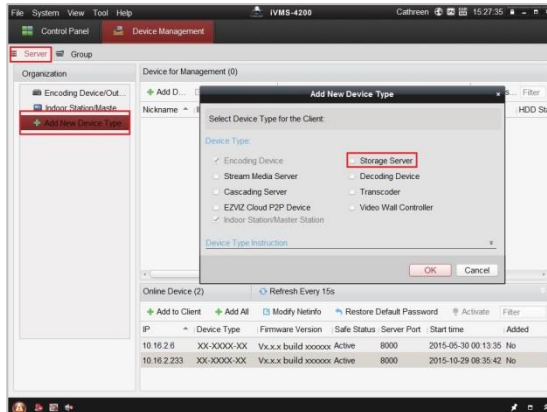


Figure 9-4 Adding Storage Server

4. Click **Storage Server** on the list to enter the Storage Server Adding interface.

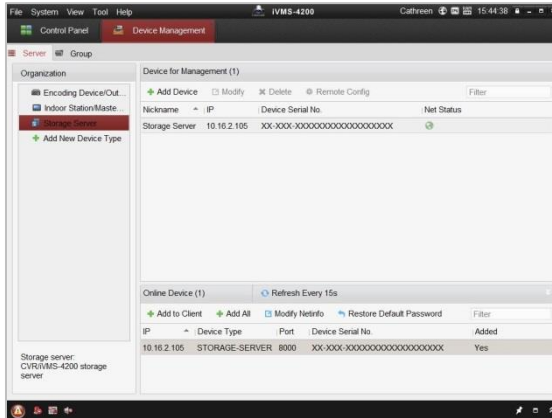


Figure 9-5 Storage Server Interface

You can add the storage server by referring to [Section 8.3 Adding Device](#).



This function does not apply to the doorphone.

9.4.2 Formatting the HDDs

The HDDs of the storage server need to be formatted for the captured picture storage.

Steps:

1. Select the added storage server from the list and click **Remote Config**.
2. Click **Storage->General** to enter the HDD Formatting interface.
3. Select the HDD from the list and click **Format**. You can check the formatting process from the process bar and the status of the formatted HDD changes from *Unformatted* to *Normal Status*.

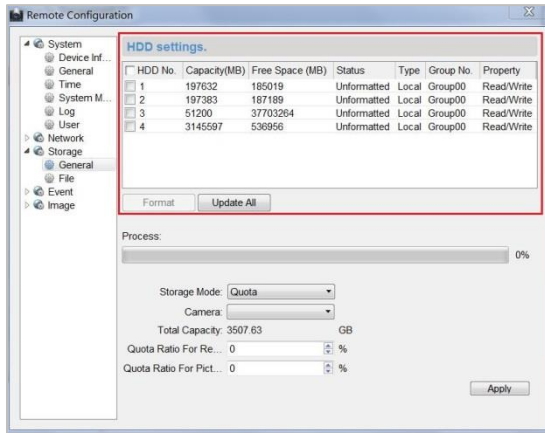


Figure 9-6 Remote Configuration Interface of Storage Server



Formatting the HDDs is to pre-allocate the disk space for storage and the original data of the formatted HDDs will not be deleted.

9.4.3 Configuring Storage Server Picture Storage

Before you start:

The storage server needs to be added to the client software and the HDDs need to be formatted for the captured pictures storage.

Steps:

1. Open the Record Schedule page.
2. Select the camera from the Camera Group list.
3. Select the storage server from the **Storage Server** drop-down list.



You can click **Storage Server Management** to add, edit or delete the storage server.

4. Check the checkbox of **Picture Storage** to store the alarm pictures of the camera when event occurs.

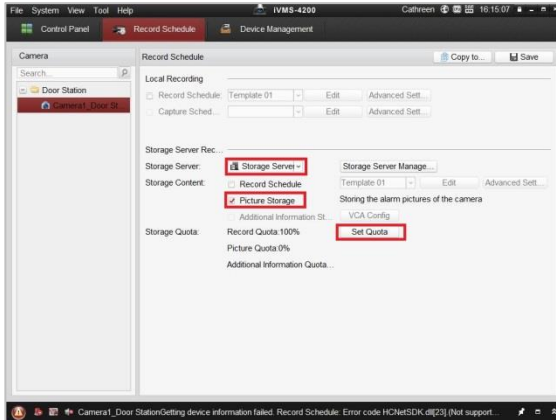


Figure 9-7 Record Schedule Settings

5. Click **Set Quota** to enter the HDD management interface of the storage server. You can set the corresponding quota ratio for captured picture information.

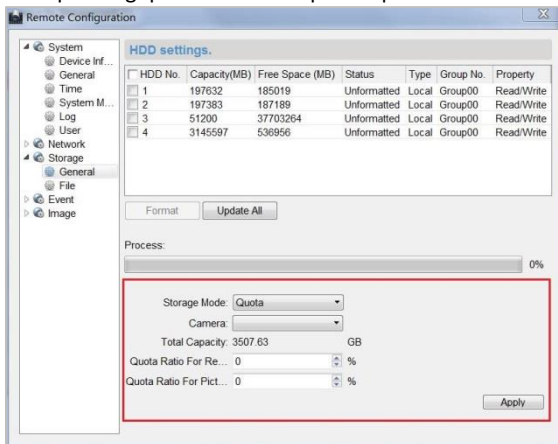


Figure 9-8 Storage Settings

Example: If you set the picture quota as 60%, then the 60% of the storage space can be used for storing the captured pictures.

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

9.5 Group Management

Purpose:

You can add groups to community, outer door station, or other, and assign devices to each group.

9.5.1 Adding Group

1. Click the **Group Management** tab to enter the group management interface.

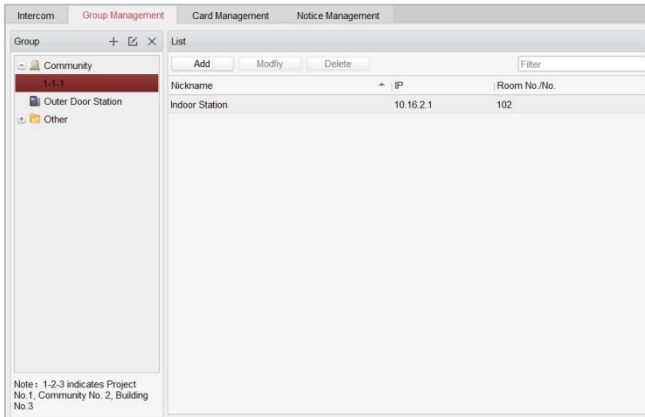



Figure 9-9 Group Management Interface

2. Click the  button on the right group list to pop-up group adding dialog box.
3. Select a kind of group type.

- **Selecting Building as Group Type**

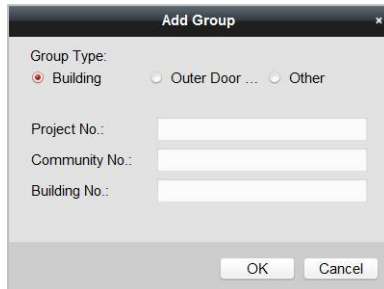


Figure 9-10 Group Adding Interface (Building)

- 1) Check the checkbox of building.
 - 2) Enter the project No., community No., and building No..
- **Selecting Outer Door Station as Group Type**

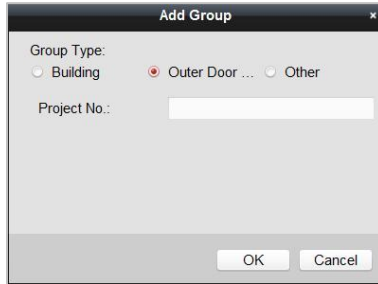


Figure 9-11 Group Adding Interface (Outer Door Station)

- 1) Check the checkbox of outer door station.
- 2) Enter the project No..

● **Selecting Other as Group Type**

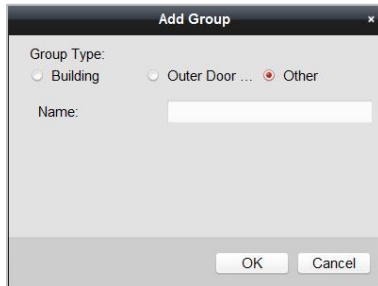


Figure 9-12 Group Adding Interface (Other)

- 1) Check the checkbox of other.
- 2) Enter the name.

4. Click the **OK** button to complete the group adding settings.



- Groups that have been successfully added will be automatically listed in the group list according to different group types.
- You can add group to **Other Group** and set different groups to assign cards to staff other than residents, such as administrator, security guard and cleaning staff, etc.,. So you can assign corresponding cards and configure their different permissions.

9.5.2 Assigning Device to Group

1. Click the **Add** button on the right to enter resident adding interface for adding devices to the list.

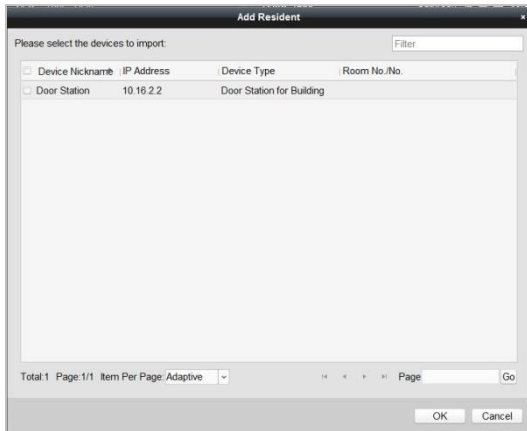


Figure 9-13 Resident Adding Interface

2. Check the checkbox of device and enter the Room No. of indoor stations to assign the device to the community.
3. Click the **OK** button to save the settings.

9.5.3 Modifying Device Information

1. Select an added device.
2. Click the **Modify** button to enter the device modifying interface.

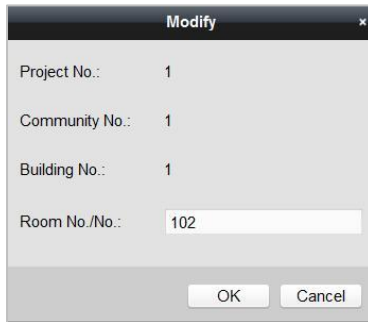


Figure 9-14 Device Modifying Interface

3. Click the **OK** button to complete the device modifying operation.

9.5.4 Deleting Device

1. Select an added device.
2. Click the **Delete** button to pop up a dialog box.

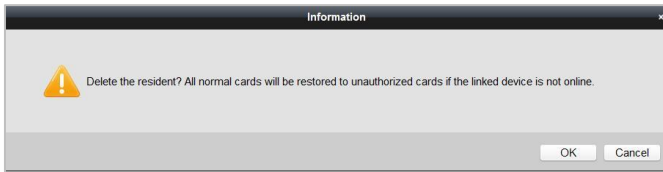


Figure 9-15 Group Deleting Interface

3. Click the **OK** button to complete the group deleting operation.

9.6 Card Management

Purpose:

You can add unauthorized cards to the community and then you can assign the cards to the corresponding indoor station and outdoor stations. For example, if there are 3 residents living in Room 401, you can assign 3 cards to No. 401 indoor Station. For each indoor station, you can assign many cards, and you can assign these cards to the door station from same building.

Steps:

1. Click the **Video Intercom** button on the control panel to enter the video intercom interface.
2. Press the **Card Management** tab to enter the card management interface.

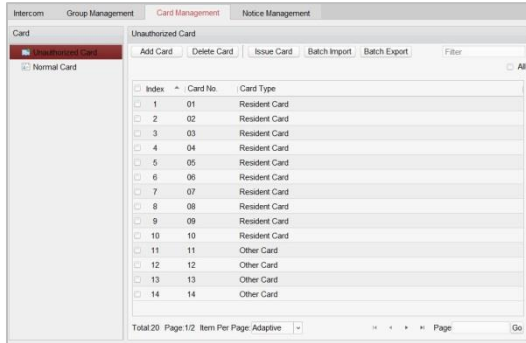


Figure 9-16 Card Management Interface

9.6.1 Unauthorized Card Management

Adding Card

1. Click the **Add Card** button to pop up card adding dialog box.
2. Select card adding mode: In Batch, By Single, Card Reader.

3. Select card type: Resident Card, Other Card.
4. Enter Start Card No. and End Card No. (adding in batch), or enter card No. (adding by single or card reader).

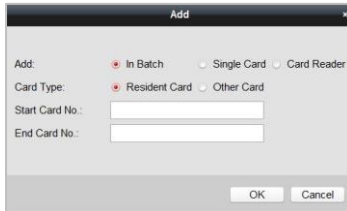


Figure 9-17 Adding in Batch

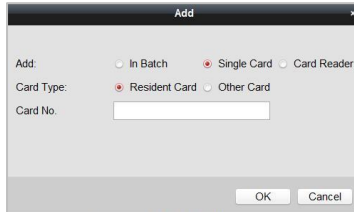


Figure 9-18 Adding by Single or Card Reader

5. Click the **OK** button to save the settings.



Two card types are recommended. Resident card is used by residents living in the community, and other card is used by visitors (guest, serviceman, etc.) in the community.

Issuing Card

1. Click the **Issue Card** button to pop up card issuing dialog box.



Figure 9-19 Card Issuing Interface

2. Issue Resident Card or Other Card.

● **Issuing Resident Card**

- 1) Select **Community** on the left and the indoor stations of the community will be listed in the resident list.

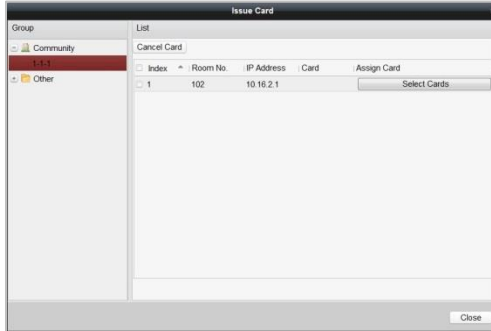


Figure 9-20 Resident Card Issuing Interface

- 2) Click the Select Cards button to pop up card selection interface for selecting unauthorized cards to be issued to the indoor station.

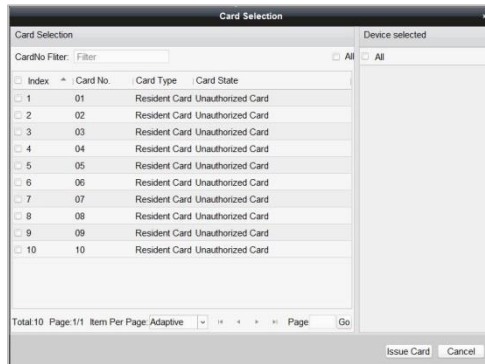


Figure 9-21 Resident Card Selection Interface

- 3) Check the checkboxes of the cards that need issuing to the indoor station, and check the checkbox of door stations, doorphones and outer door stations (only resident cards can be assigned to indoor stations).
- 4) Click the **Issue Card** button to complete the resident card issuing settings.



Multiply resident card can be issued to an indoor station.

● **Issuing Other Card**

- 1) Select **Other** on the left group list and the name for other card issuing will be listed in the right list.

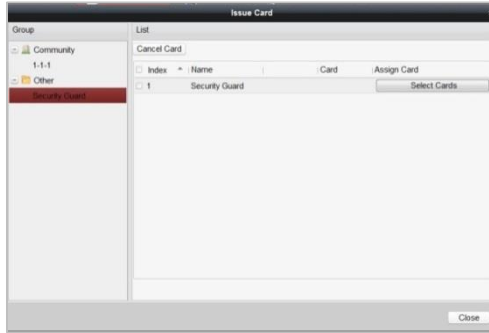



Figure 9-22 Other Card Issuing Interface

- 2) Click the  button to pop up card selection interface for selecting unauthorized cards to be issued to the indoor station.

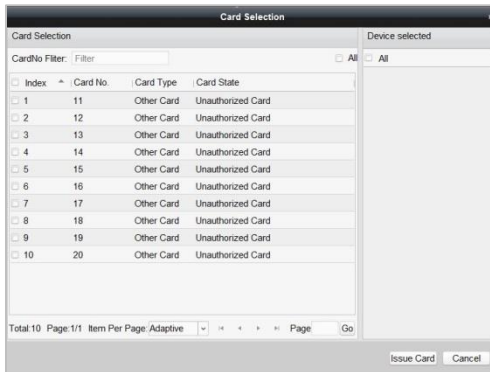


Figure 9-23 Other Card Selection Interface

- 3) Check the checkboxes of the cards that need issuing to the indoor station, and check the checkbox of door stations, doorphones and outer door stations (only resident cards can be assigned to indoor stations).
- 4) Click the **Issue Card** button to complete the other card issuing settings.



Multiply other cards can be issued to a same group.

Deleting Card

- **Deleting Unauthorized Card**

- 1) On the card management interface (Figure 8-11), check the checkbox(ex) of unauthorized card(s).
- 2) Click the **Delete Card** button to pop up unauthorized card deleting box.

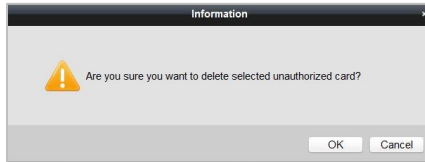



Figure 9-24 Card Deleting Information Box

- 3) Click the **OK** button to delete the card(s).

- **Deleting Issued Card**

- 1) On the resident/other card issuing interface (Figure 8-15, Figure 8-17), select a community group or an Other group.
- 2) Click the  button to enter the card selection interface for deleting issued card.
- 3) Cancel the checkbox(ex) of issued card(s) and check the checkbox door stations, doorphones or outer door stations.
- 4) Click the **Issue Card** button to complete the issued card deleting settings.



- You can cancel issued card(s) from single or certain door stations by cancelling the checkbox(es) from the device list.
- To cancel all issued cards, check the checkbox(es) of Room No. / name, and click the **Cancel Card** button to cancel all cards issued to the device. The card state will be reset to unauthorized card.

Importing Unauthorized Cards in Batch

1. Click the **Batch Import** button to pop up card batch importing dialog box.

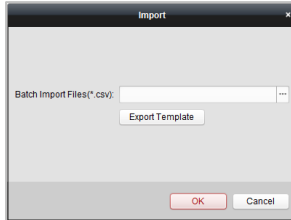


Figure 9-25 Bath Import Interface

2. Click the **Export Template** button to export the template of the batch import file.

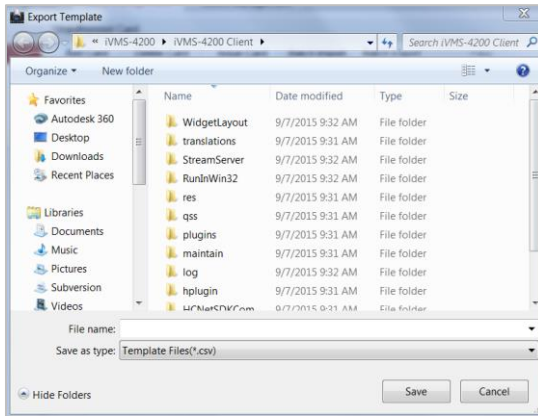


Figure 9-26 Template File Exporting Interface

3. Fill in the template of the batch import file and click the **Save** button to save it.
4. Click the button to select the batch import file.

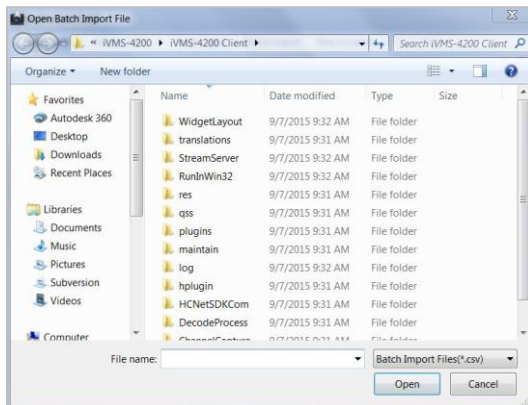


Figure 9-27 Batch Import File Opening Interface

5. Click the **Open** button.
6. Click the **OK** button to start importing the batch import file.

Exporting Unauthorized Cards in Batch

1. Click the **Batch Export** button after adding unauthorized cards.

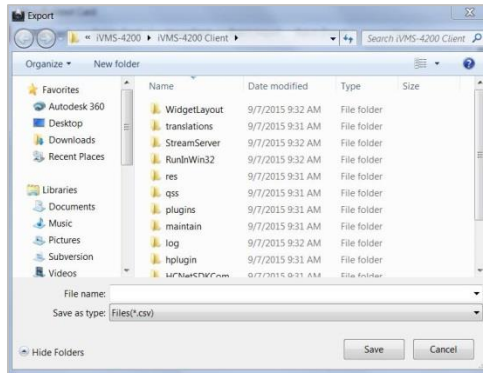


Figure 9-28 Batch Export Interface

2. Select the saving file path and click the **Save** button.
3. Generate an excel file in the saving directory after exporting unauthorized cards in batch.

9.6.2 Normal Card Management

On card management interface, click the **normal card** button to enter the normal card interface for listing normal cards including resident card and other card. After issuing cards, the issued cards will be listed in the normal card list, as shown in the figure below.

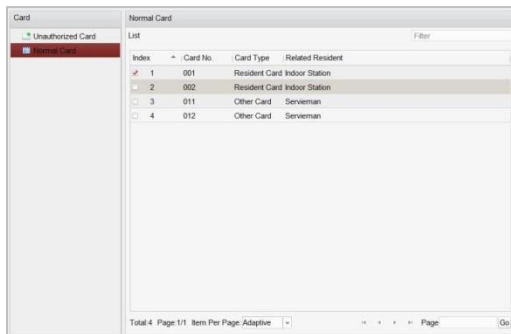


Figure 9-29 Normal Card Interface



- To issue cards with card issuer, please connect the card reader DS-K1F100-D8 (purchased separately) to PC via USB interface. Open iVMS-4200 and enter the directory of **Video Intercom->Card Management->Unauthorized Card->Add Card**. Swipe the unauthorized card in turn and the card No. will be read and added to the device automatically.
- After issuing each card via iVMS-4200, the device plays the voice prompt: Issuing card finished

9.7 Notice Management

9.7.1 Querying Unlocking Log

Steps:

1. Click the **Query Unlocking Logs** button to enter query unlocking logs interface.
2. Select the unlocking type, device type, and set the start time and end time.

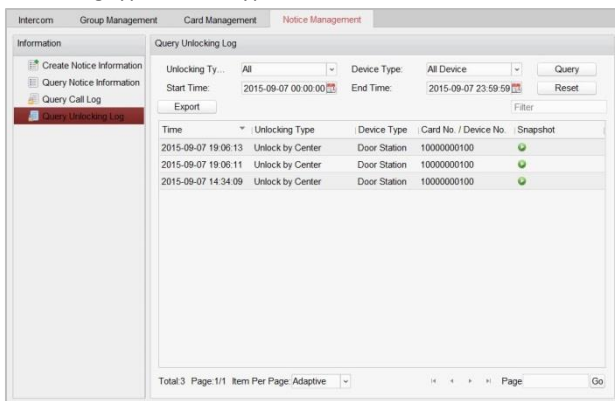


Figure 9-30 Query Unlocking Logs

3. Click the **Query** button to search the unlocking log.
4. Click the **Export** button to export the unlocking logs.

9.8 Device Arming Control

Steps:

1. Select **Tool->Device Arming Control** to enter the device arming control interface.



Figure 9-31 Tool Menu

2. Set the arming status of the device as armed, and the alarm information will be auto uploaded to the client software when alarm occurs

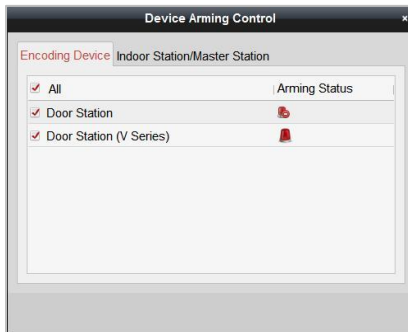


Figure 9-32 Device Arming Control

The screenshot shows the 'Alarm Event' window in the software. It has a table with columns: Index, Alarm Time, Alarm Source, Alarm Details, Alarm Content, Live V..., Send Email, and Note. There are four rows of alarm events listed.

Index	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live V...	Send Email	Note
1	2015-09-07 14:34:09	Encoding Device:Door Station ...	Camera: Camera1_Do...	Video Intercom Event			
2	2015-09-07 14:34:31	Encoding Device:Door Station ...	Close Door Failed Alarm	Close Door Failed Alarm			
3	2015-09-07 15:02:21	Encoding Device:Door Station ...	Tamper Alarm	Tamper Alarm			
4	2015-09-07 15:02:43	Encoding Device:Door Station ...	Close Door Failed Alarm	Close Door Failed Alarm			

Figure 9-33 Alarm Events



After adding the device to the client software, it will be armed automatically.

10 Local Operation

10.1 Calling Resident

10.1.1 Calling Resident (DS-KV8X02-IM)

You can call the resident by pressing the calling button. For device DS-KV8X02-IM, the number of calling buttons varies according to its model. Take the figure of device DS-KV8402-IM as an example.



- For device DS-KV8102-IM, there is only 1 calling button.
- For device DS-KV8202-IM, there are 2 calling buttons.
- For device DS-KV8402-IM, there are 4 calling buttons.

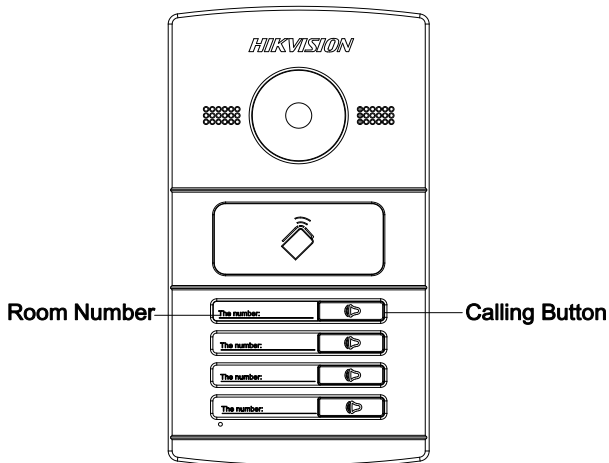


Figure 10-1 Calling Button of DS-KV8402-IM

Steps:

1. Press the corresponding calling button of the resident.
2. The resident can receive/decline the video call, unlock the door, call the elevator, etc.



- When the video intercom between you and the resident is realized, you can speak to the resident, and the live view of door station will be displayed on the connected indoor station.

- When live view of door station is displayed on other devices or door station is calling resident, the door station will detect the brightness of video. When the brightness is lower than the expected threshold, the supplement light will be enabled.
- When the supplement light is enabled, the backlight of key will be auto-enabled, otherwise, the door station will detect the brightness of live view and enable the backlight of key when the brightness of live view is lower than expected threshold.

10.1.2 Calling Resident (DS-KV8102-XP)

You can call the resident by pressing the calling button. For device DS-KV8102-IP/VP, there is only 1 calling button.

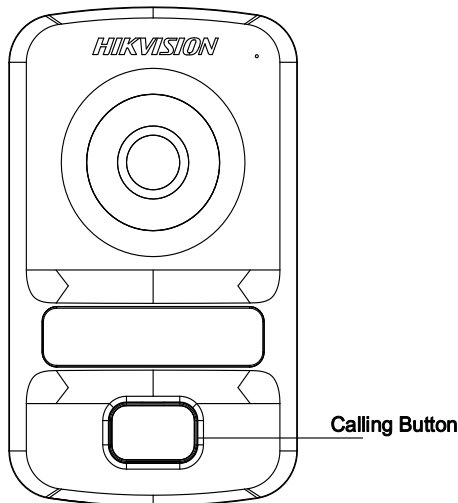


Figure 10-2 Calling Button of DS-KV8102-XP

Steps:

1. Press the corresponding calling button of the resident.
2. The resident can receive/decline the video call, unlock the door, call the elevator, etc.



- When the video intercom between you and the resident is realized, you can speak to the resident, and the live view of door station will be displayed on the connected indoor station.
- When live view of door station is displayed on other devices or door station is calling resident, the door station will detect the brightness of video. When the brightness is lower than the expected threshold, the supplement light will be enabled.

- When the supplement light is enabled, the backlight of key will be auto-enabled, otherwise, the door station will detect the brightness of live view and enable the backlight of key when the brightness of live view is lower than expected threshold.

10.2 Issuing Card

Purpose:

You can assign the card to the door station or doorphone by issuing cards. You can issue cards by swiping the main card with the door station, or issue the card with iVMS-4200 client software. For more information about issuing card by iVMS-4200, please refer to Chapter 9.

Steps:

1. Swipe the main card on the card induction area to enter the card issuing mode.
2. Hear a voice prompt of the device: Issuing card started.
3. Swipe the unauthorized sub card in turn on the card induction area.
4. Hear a voice prompt of the device (Issuing card finished.) after issuing each card successfully.



- Only Mifare card supported, and Mifare card with non-standard shape is recommended.
- No more than 256 cards can be issued to and managed by V series door station. A voice prompt (Card amount exceeds limit.) can be heard when the issued card amount exceeds the upper limit.
- Swipe the main card again or perform no operation for more than 10s, the device will exit the card issuing mode automatically.
- After issuing cards with client software, the local card issuing function will be disabled.
- For each main door station, at most 8 sub door stations can be added.

10.3 Unlocking Door

Purpose:

After issuing the cards, you can unlock the door by swiping the assigned card.

Step:

1. Swipe the card on the card induction area.
2. Hear a voice prompt of the device: Door is open.



You cannot unlock the door by swiping the main card.

Appendix

Installation Notice

While installing the door station, please make sure that the distance between any two devices is far as possible to avoid the howling and echo. The distance between two devices is recommended to be longer than 10 meters.



Devices here refer to indoor station, door station, doorphone and master station.

Wiring Cables

Cable	Specification
Power Cord of Door Station	RVV 2*1.0
Network Cable of Door Station	UTP-five Categories
Door Lock Wiring (With Door Magnetic)	RVV 4*1.0
Door Lock Wiring (Without Door Magnetic)	RVV 2*1.0
Exit Button Wiring	RVV 2*0.5

Specification of DS-KV8X02-IM

Model Parameters	DS-KV8102-IM	DS-KV8202-IM	DS-KV8402-IM
System Parameters			
Processor	High-Performance Embedded SOC Processor		
Operation System	Embedded Linux Operation System		
Video Parameters			
Camera	CMOS Low Illumination 1.3 MP HD Colorful Camera		
Video Compression Standards	H.264		
Resolution	1280 × 720		

Model Parameters	DS-KV8102-IM	DS-KV8202-IM	DS-KV8402-IM
Video Frame	25 fps		
Audio Parameters			
Audio Input	Built-in Omnidirectional Microphone		
Audio Output	Built-in Loudspeaker		
Audio Compression Standard	G.711U		
Audio Compression Rate	64 Kbps		
Audio Quality	Noise Suppression and Echo Cancellation		
Access Control Parameters			
Internal Card Reader	Built-in IC Card Reader		
Exit Button	Exit Button for Opening Door		
NO/NC	Support NO/NC Status Settings		
Door Magnetic Detection	Detect Door Magnetic Status		
Light Supplement			
Light Supplement Mode	IR Supplement		
Network Parameters			
Ethernet	10/100 Mbps Self-Adaptive Ethernet		
Network Protocol	TCP/IP, SNMP, SIP, RTSP		
Alarm Parameters			
Alarm Input	Door Magnetic Alarm, Tamper Alarm		
Device Interfaces			
Internet Access	1 RJ45 10/100 Mbps Self-Adaptive Ethernet Interface		
RS-485	1 RS-485 Half-Duplex Port		
I/O Input	4		
I/O Output	1		

Model Parameters	DS-KV8102-IM	DS-KV8202-IM	DS-KV8402-IM
Other Parameters			
Indoor Station Access Amount	1	2	4
Material	Aluminum Alloy		
Power Supply	DC 24V, Power Over Network Cable (DS-KAD606, DS-KAD612) 是否必须和KAD606联用?		
	DC 12V		
Consumption	≤12 W		
Working Temperature	- 40° C to + 70° C (-40° F to 158° F)		
Working Humidity	10% to 90%		
IP Protection Level	IP65		
Dimension	182 mm × 100 mm × 33 mm (7.17" × 3.94" × 1.30")		
Certification	FCC, IC, CE, C-TICK, ROHS, REACH, WEEE		

Specification of DS-KV8102-XP

Model Parameters	DS-KV8102-IP	DS-KV8102-VP
System Parameters		
Processor	High-Performance Embedded SOC Processor	
Operation System	Embedded Linux Operation System	
Video Parameters		
Camera	CMOS Low Illumination 1.3 MP HD Colorful Camera	
Video Compression Standards	H.264	
Resolution	1280 × 720	
Video Frame	25 fps	
Audio Parameters		

Model		
Parameters	DS-KV8102-IP	DS-KV8102-VP
Audio Input	Built-in Omnidirectional Microphone	
Audio Output	Built-in Loudspeaker	
Audio Compression Standard	G.711 U	
Audio Compression Rate	64 Kbps	
Audio Quality	Noise Suppression and Echo Cancellation	
Access Control Parameters		
Internal Card Reader	Built-in IC Card Reader	
Exit Button	Exit Button for Opening Door	
NO/NC	Support NO/NC Status Setting	
Door Magnetic Detection	Detect Door Magnetic Status	
Light Supplement		
Light Supplement Mode	IR Supplement	Visible Light Supplement
Network Parameters		
Ethernet	10/100 Mbps Self-Adaptive Ethernet	
Network Protocol	TCP/IP, SNMP, SIP, RTSP	
Alarm Parameters		
Alarm Input	Door Magnetic Alarm, Tamper Alarm	
Device Interfaces		
Internet Access	1 RJ45 10/100 Mbps Self-Adaptive Ethernet Interface	
RS-485	1 RS-485 Half-Duplex Port	
I/O Input	4	
I/O Output	1	
Other Parameters		
Material	Plastic	

Model Parameters	DS-KV8102-IP	DS-KV8102-VP
Power Supply	DC 24V, Power Over Network Cable (DS-KAD606, DS-KAD612)	
	DC 12V	
Consumption	≤12 W	
Working Temperature	-40° C to +70° C (-40° F to 158° F)	
Working Humidity	10% to 90%	
IP Protection Level	IP65	
Dimension	164 mm × 97 mm × 40.6 mm (6.46" × 3.82" × 1.60")	
Certification	FCC, IC, CE, C-TICK, ROHS, REACH, WEEE	



First Choice for Security Professionals