Video Intercom Door Station

(D Series)

User Manual

UD06326B

User Manual

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

Series	Model
Door Station (D Series)	DS-KD8102-V
	DS-KD8002-VM
	DS-KD3002-VM

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.

FCC Conditions

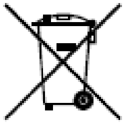
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

EU Conformity Statement

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

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



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

Industry Canada ICES-003 Compliance

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

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

- The working temperature of the device is from -40 °C to 60 °C.
- 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.)
- The power supply must conform to LPS. The recommended adaptor models and manufacturers are shown as below. Use the attached adaptor, and do not change the adaptor randomly.

Model	Manufacturer	Standard
DSA-12PFG-12 FCH 120100	Dee Van Electronics Co., Ltd.	GB
DSA-12PFG-12 FEU 120100	Dee Van Electronics Co., Ltd.	EN
DSA-12PFT-12FUS120100	Dee Van Electronics Co., Ltd.	ANSI

Model	Manufacturer	Standard
DSA-12PFG-12 FUK 120100	Dee Van Electronics Co., Ltd.	BSW
DSA-12PFG-12 FAU 120100	Dee Van Electronics Co., Ltd.	AS

⚠ **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-KD8102-V 2
2.2 Appearance of DS-KD8002-VM 3
2.3 Appearance of DS-KD3002-VM 4

3 Typical Application 6

4 Terminal and Wiring 7

4.1 Terminal Description 7
4.1.1 Terminals and Interfaces of DS-KD8102-V/ DS-KD8002-VM 7
4.1.2 Terminals and Interfaces of DS-KD3002-VM 9
4.2 Wiring Description 11
4.2.1 Door Lock Wiring 11
4.2.2 Door Magnetic Wiring 11
4.2.3 Exit Button Wiring 13
4.2.4 External Card Reader Wiring 14
4.2.5 External Elevator Controller Wiring 16
4.2.6 Alarm Device Input Wiring 17
4.2.7 Alarm Device Output Wiring 18

5 Installation 19

5.1 Installation of DS-KD8102-V 19
5.1.1 Gang Box for DS-KD8102-V 19
5.1.2 Wall Mounting with Gang Box of DS-KD8102-V 20
5.2 Installation of DS-KD8002-VM 22
5.2.1 Gang Box for DS-KD8002-VM 22
5.2.2 Wall Mounting with Gang Box of DS-KD8002-VM 22
5.3 Installation of DS-KD3002-VM 25
5.3.1 Gang Box for DS-KD3002-VM 25
5.3.2 Wall Mounting with Gang Box of DS-KD3002-VM 25

6 Before You Start 28

7 Local Operation 29

7.1 Keys Description 29
7.2 Activating Device 29
7.3 Status 31
7.4 Setting Parameters 31
7.4.1 Local Settings 32
7.4.2 Editing Network Parameters 33

7.4.3 Changing Password.....34
7.4.4 Issuing Card.....36
7.4.5 Setting Volume.....38
7.4.6 About.....39
7.5 Calling Resident.....39
7.6 Unlocking Door.....39

8 Remote Operation via Batch Configuration Tool.....43

8.1 Activating Device Remotely.....43
8.2 Editing Network Parameters.....44
8.3 Adding Device.....45
8.3.1 Adding Online Device.....45
8.3.2 Adding by IP Address.....46
8.3.3 Adding by IP Segment.....47
8.4 Configuring Devices Remotely.....48
8.4.1 System.....48
8.4.2 Video Intercom.....53
8.4.3 Network.....57
8.4.4 Video Display.....60
8.5 Video Intercom Device Set-up Tool.....61
8.5.1 Setting a Community Structure.....62
8.5.2 Setting Main/Sub Door Station.....62
8.6 Batch Upgrading.....65
8.6.1 Adding Devices for Upgrading.....65
8.6.2 Upgrading Devices.....67

9 Remote Operation via iVMS-4200 Client Software.....69

9.1 System Configuration.....69
9.2 Device Management.....70
9.2.1 Adding Video Intercom Devices.....70
9.2.2 Modifying Network Information.....73
9.2.3 Resetting Password.....73
9.3 Configuring Devices Remotely via iVMS-4200.....75
9.4 Picture Storage.....76
9.4.1 Adding Storage Server.....76
9.4.2 Formatting the HDDs.....77
9.4.3 Configuring Storage Server Picture Storage.....78
9.5 Live View.....79
9.6 Video Intercom Configuration.....81
9.6.1 Group Management.....83
9.6.2 Video Intercom.....88
9.6.3 Card Management.....90
9.6.4 Notice Management.....99
9.7 Device Arming Control.....101

Appendix.....103

Installation Notice 103
Wiring Cables... 103

1 Overview

1.1 Introduction

The video intercom system can realize functions such as video intercom, resident-to-resident video call, live view of HD video, access control, one-card system, elevator linkage, 8-ch zone alarm, notice information and visitor messages to provide a complete smart community video intercom solution.

The video intercom door station is mainly applied to situations such as community, villa, and official buildings.

1.2 Main Features

- Video intercom function
- HD video surveillance (Max. resolution 1280×720@30fps, 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
- Elevator linkage
- Door magnetic alarm and tamper-proof alarm function
- Noise suppression and echo cancellation
- IR detection (only supported by DS-KD8102-V model)
- Remote upgrade, batch setting, upgrade via USB flash disk functions

2 Appearance

2.1 Appearance of DS-KD8102-V

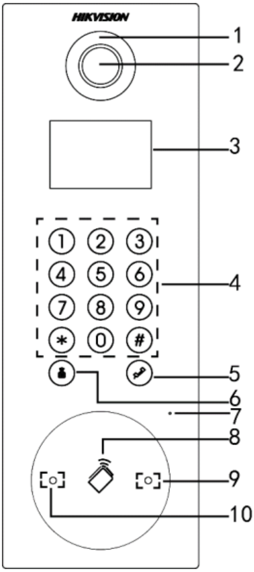


Figure 2-1 Front View

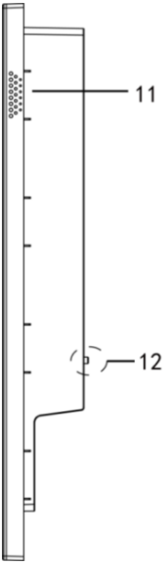


Figure 2-2 Side View

Table 2-1 Descriptions of Keys

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

9	IR Emission
10	IR Receiver
11	Loudspeaker
12	TAMPER

2.2 Appearance of DS-KD8002-VM

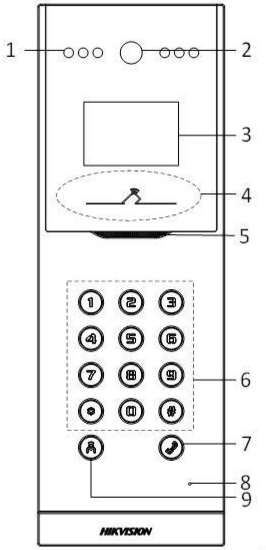


Figure 2-3 Front View

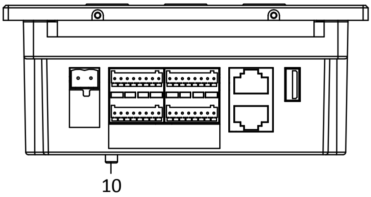


Figure 2-4 Side View

Table 2-2 Descriptions of Keys

No.	Description
1	Low Illumination Supplement Light
2	Built-in Camera
3	LCD Display Screen
4	Card Induction Area
5	Loudspeaker
6	Keypad

7	Call Button
8	Microphone
9	Call Center Key
10	TAMPER

2.3 Appearance of DS-KD3002-VM

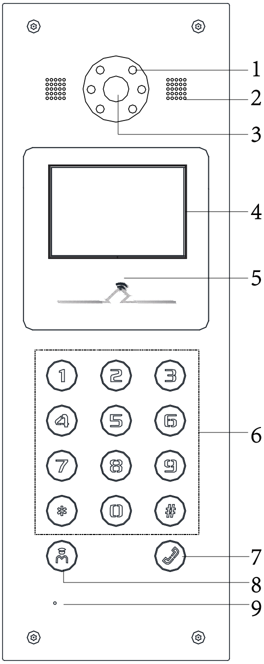


Figure 2-5 Front View

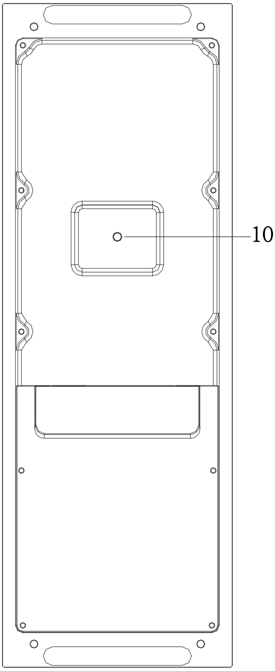


Figure 2-6 Rear View

Table 2-3 Descriptions Keys

No.	Description
1	Low Illumination Supplement Light
2	Built-in Camera
3	Loudspeaker

No.	Description
4	LCD Display Screen
5	Card Induction Area
6	Keypad
7	Call Button
8	Call Center Key
9	Microphone
10	TAMPER

3 Typical Application

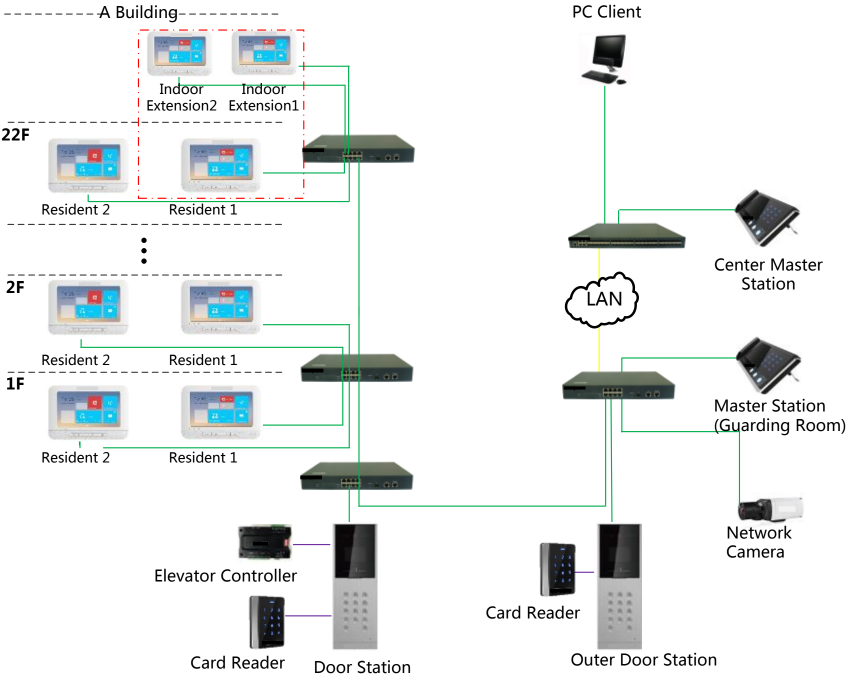


Figure 3-1 Typical Application of Door Station

4 Terminal and Wiring

4.1 Terminal Description

4.1.1 Terminals and Interfaces of DS-KD8102-V/ DS-KD8002-VM

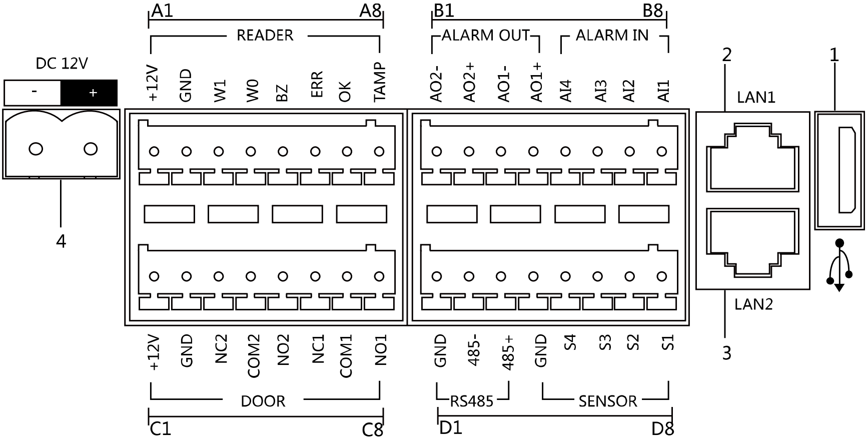


Figure 4-1 Terminals and Interfaces of DS-KD8102-V/DS-KD8002-VM

Table 4-1 Descriptions of Terminals and Interfaces

Name	No.	Interface	Description
USB	1	USB	USB Interface
LAN	2	LAN1	Network Interface
	3	LAN2	Analog Interface
Power Supply	4	DC 12V	DC 12V Power Supply Input
READER	A1	12V	Power Supply Output
	A2	GND	Grounding
	A3	W1	Data Input Interface Wiegand Card Reader: Data1
	A4	W0	Data Input Interface Wiegand Card Reader: Data0
	A5	BZ	Card Reader Buzzer Output

Name	No.	Interface	Description
	A6	ERR	Card Reader Indicator Output (Invalid Card Output)
	A7	OK	Card Reader Indicator Output (Valid Card Output)
	A8	TAMP	Tamper-proof Input of Wiegand Card Reader
ALARM OUT	B1	AO2-	Alarm Relay Output 2
	B2	AO2+	
	B3	AO1-	Alarm Relay Output 1
	B4	AO1+	
ALARM IN	B5	AI4	Alarm Input 4
	B6	AI3	Alarm Input 3
	B7	AI2	Alarm Input 2
	B8	AI1	Alarm Input 1
DOOR	C1	12V	Power Supply Output
	C2	GND	Grounding
	C3	NC2	Door Lock Relay Output (NC)
	C4	COM2	Grounding Signal
	C5	NO2	Door Lock Relay Output (NO)
	C6	NC1	Door Lock Relay Output (NC)
	C7	COM1	Grounding Signal
	C8	NO1	Door Lock Relay Output (NO)
RS485	D1	GND	RS-485 Communication Interfaces
	D2	485-	
	D3	485+	
SENSOR	D4	GND	Grounding Signal
	D5	S4	Door Magnetic Detection Input 4/Exit Button
	D6	S3	Door Magnetic Detection Input 3/Exit Button
	D7	S2	Door Magnetic Detection Input 2/Exit Button
	D8	S1	Door Magnetic Detection Input 1/Exit Button

4.1.2 Terminals and Interfaces of DS-KD3002-VM

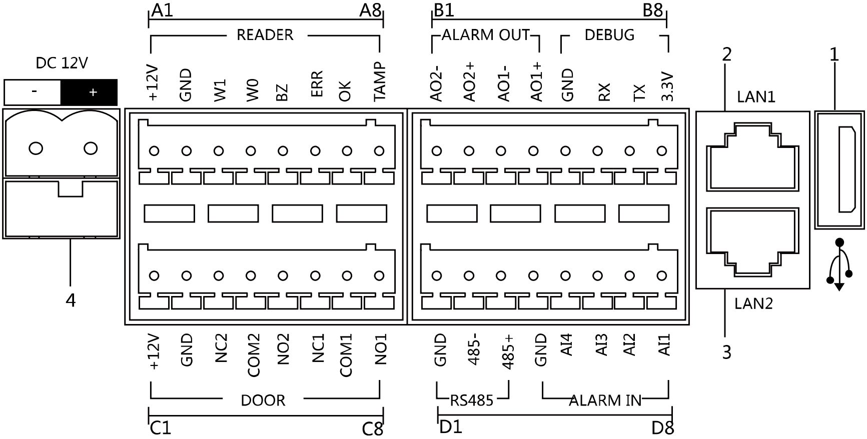


Figure 4-2 Terminals and Interfaces of DS-KD3002-VM

Table 4-2 Descriptions of Terminals and Interfaces

Name	No.	Interface	Description
USB	1	USB	USB Interface
LAN	2	LAN1	Network Interface
	3	LAN2	Analog Interface
Power Supply	4	DC 12V	DC 12V Power Supply Input
READER	A1	12V	Power Supply Output
	A2	GND	Grounding
	A3	W1	Data Input Interface Wiegand Card Reader: Data1
	A4	W0	Data Input Interface Wiegand Card Reader: Data0
	A5	BZ	Card Reader Buzzer Output
	A6	ERR	Card Reader Indicator Output (Invalid Card Output)
	A7	OK	Card Reader Indicator Output (Valid Card Output)
	A8	TAMP	Tamper-proof Input of Wiegand Card Reader
ALARM	B1	AO2-	Alarm Relay Output 2

Name	No.	Interface	Description
OUT	B2	AO2+	
	B3	AO1-	Alarm Relay Output 1
	B4	AO1+	
DEBUG	B5	GND	Grounding
	B6	RX	Serial Port Debugging/Receive data
	B7	TX	Serial Port Debugging/Send data
	B8	3.3V	Serial Port Debugging/Power Supply
DOOR	C1	12V	Power Supply Output
	C2	GND	Grounding
	C3	NC2	Door Lock Relay Output (NC)
	C4	COM2	Grounding Signal
	C5	NO2	Door Lock Relay Output (NO)
	C6	NC1	Door Lock Relay Output (NC)
	C7	COM1	Grounding Signal
	C8	NO1	Door Lock Relay Output (NO)
RS485	D1	GND	RS-485 Communication Interfaces
	D2	485-	
	D3	485+	
ALARM IN	D4	GND	Grounding Signal
	D5	AI4	Alarm Input 4
	D6	AI3	Alarm Input 3
	D7	AI2	Alarm Input 2
	D8	AI1	Alarm Input 1

4.2 Wiring Description

4.2.1 Door Lock Wiring

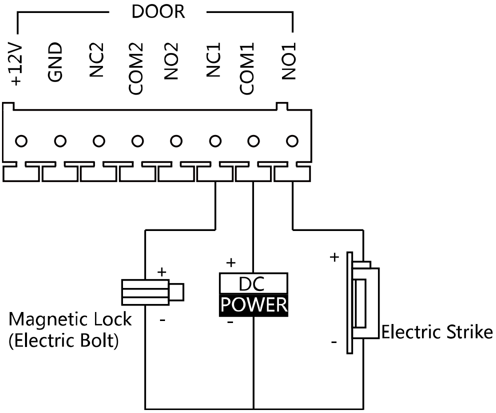


Figure 4-3 Door Lock Wiring

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 Batch Configuration Tool or iVMS-4200.

4.2.2 Door Magnetic Wiring

Door Magnetic Wiring for DS-KD8102-V/DS-KD8002-VM

For DS-KD8102-V/DS-KD8002-VM, there are two optional ways of door magnetic wiring.

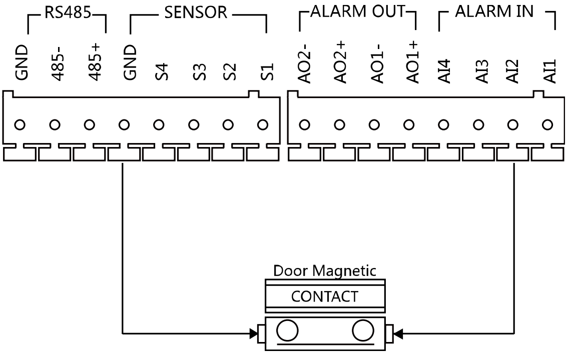


Figure 4-4 Door Magnetic Wiring for DS-KD8102-V/DS-KD8002-VM (1)

NOTE

To connect the door magnetic, it is required to set the output of terminal AI2 to be door magnetic with Batch Configuration Tool or iVMS-4200.

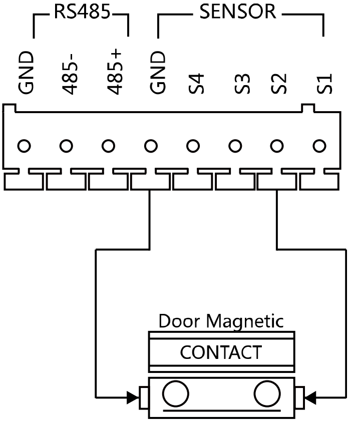


Figure 4-5 Door Magnetic Wiring for DS-KD8102-V/DS-KD8002-VM (2)

NOTE

Terminal S2 is set as default for connecting door magnetic.

Door Magnetic Wiring for DS-KD3002-VM

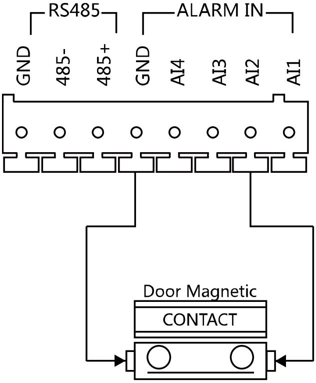


Figure 4-6 Door Magnetic Wiring for DS-KD3002-VM

NOTE

To connect the door magnetic, it is required to set the output of terminal AI2 to be door magnetic with Batch Configuration Tool or iVMS-4200.

4.2.3 Exit Button Wiring

Exit Button Wiring for DS-KD8102-V/DS-KD8002-VM

For DS-KD8102-V/DS-KD8002-VM, there are two optional ways of exit button wiring.

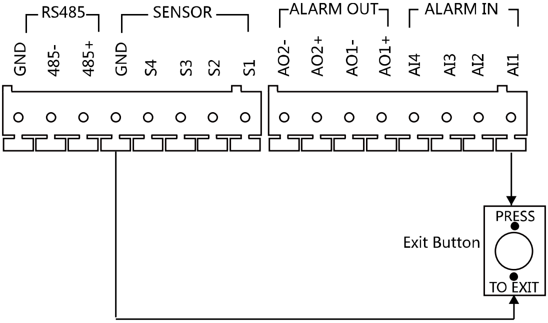


Figure 4-7 Exit Button Wiring for DS-KD8102-V/DS-KD8002-VM (1)

NOTE

To connect the exit button, it is required to set the output of terminal AI1 to be exit button with Batch Configuration Tool or iVMS-4200.

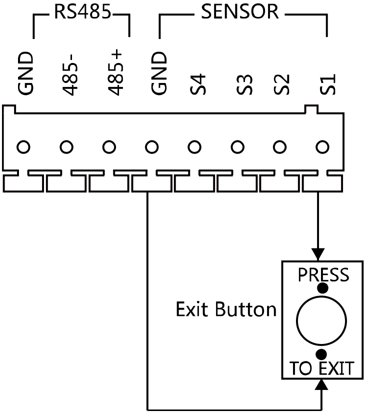


Figure 4-8 Exit Button Wiring for DS-KD8102-V/DS-KD8002-VM (2)

Exit Button Wiring for DS-KD3002-VM

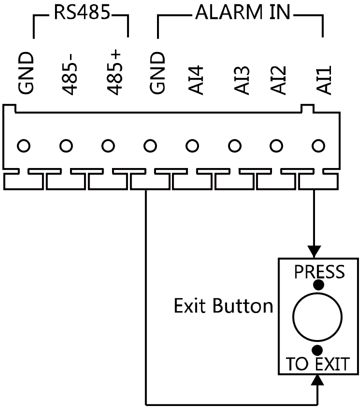


Figure 4-9 Exit Button Wiring for DS-KD3002-VM

NOTE

Terminal S1 is set as default for connecting exit button.

4.2.4 External Card Reader Wiring

NOTE

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

No.	Description	How to Configure
1-4	Set the RS-485 address	ON: 1 OFF: 0
6	Select Wiegand protocol or RS-485 protocol	ON: Wiegand OFF: RS-485
7	Set the Wiegand protocol (It is invalid when setting OFF in 6.)	ON: Wiegand 26 OFF: Wiegand 34

RS-485 Card Reader Wiring

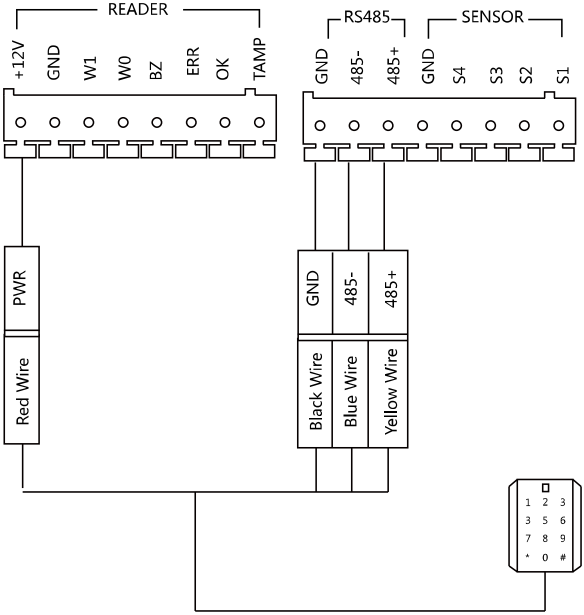


Figure 4-10 RS-485 Card Reader Wiring

Wiegand Card Reader Wiring

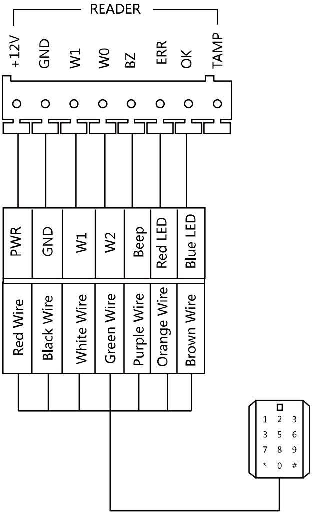


Figure 4-11 External Card Reader Wiring

4.2.5 External Elevator Controller Wiring

You can connect the door station to the elevator controller via RS-485 interface.

There are 4 groups of RS-485 interfaces on the elevator controller: group A, group B, Group C, and Group D. Group C is used to connect to the door station.

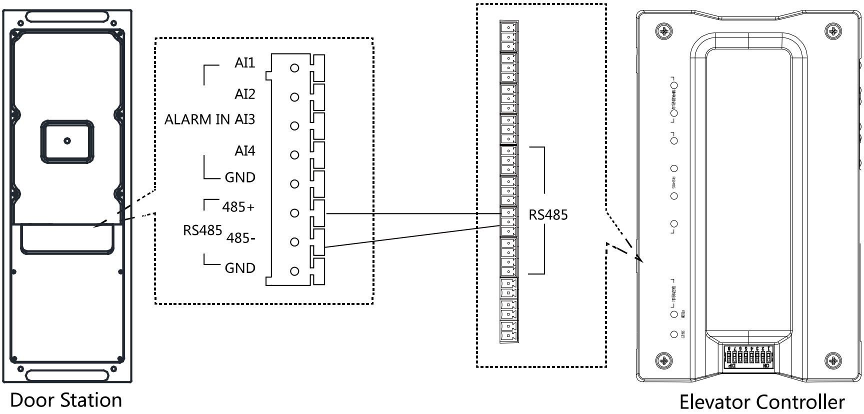


Figure 4-12 External Elevator Controller Wiring

4.2.6 Alarm Device Input Wiring

Alarm Device Input Wiring for DS-KD8102-V

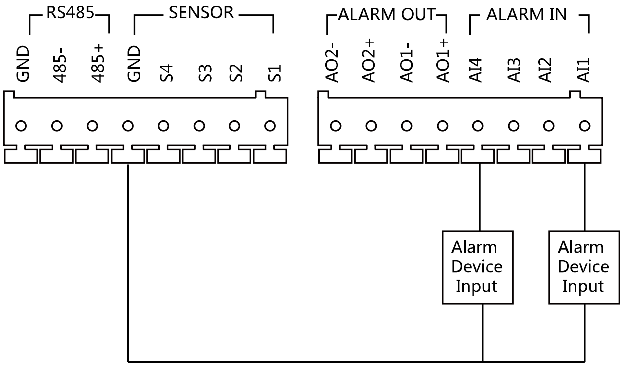


Figure 4-13 Alarm Device Input Wiring for DS-KD8102-V/DS-KD8002-VM

Alarm Device Input Wiring for DS-KD3002-VM

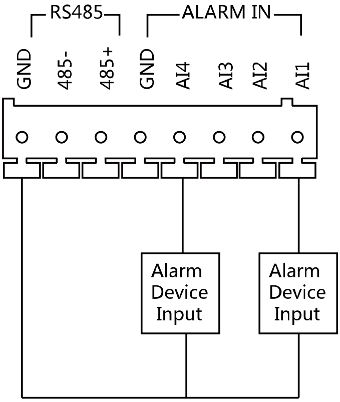


Figure 4-14 Alarm Device Input Wiring for DS-KD3002-VM

4.2.7 Alarm Device Output Wiring

Alarm Device Output Wiring for DS-KD8102-V/DS-KD8002-VM

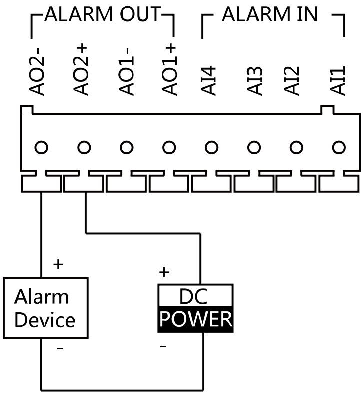


Figure 4-15 Alarm Device Output Wiring for DS-KD8102-V/DS-KD8002-VM

Alarm Device Output Wiring for DS-KD3002-VM

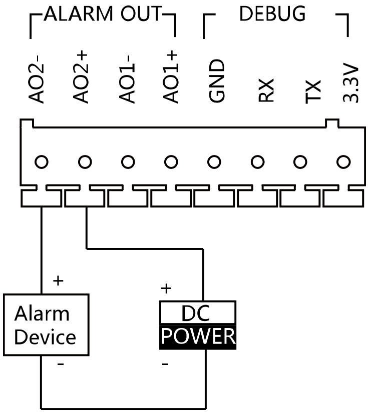


Figure 4-16 Alarm Device Output Wiring for DS-KD3002-VM

5 Installation

Before you start:

- Make sure the device in the package is in good condition and all the assembly parts are included.
- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
- Make sure all the related equipment is power-off during the installation.
- Check the product specification for the installation environment.

5.1 Installation of DS-KD8102-V

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

5.1.1 Gang Box for DS-KD8102-V

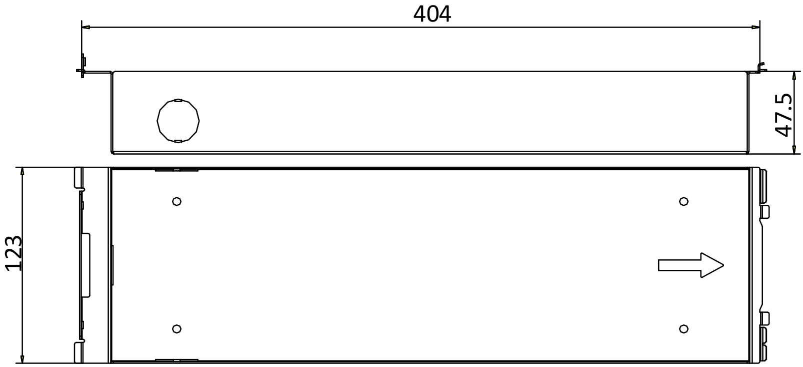


Figure 5-1 Front and Side View

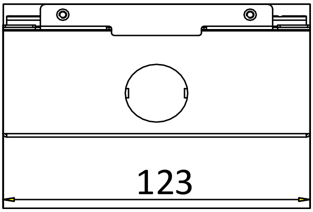


Figure 5-2 Overhead (Plan) View

NOTE

- The dimension of gang box for model DS-KD8102-V door station is: 404 (length)×123 (width)×47.5 (depth) mm.
- The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.

5.1.2 Wall Mounting with Gang Box of DS-KD8102-V

Steps:

1. Chisel a hole in the wall for inserting the gang box. The size of the hole should be larger than that of the gang box. The suggested size of hole is 404.5 (length) × 123.5 (width) ×48 (depth) mm.
2. Insert the gang box into the hole and fix it with 4 PA4 screws. Make sure the edges of the gang box align to the wall.

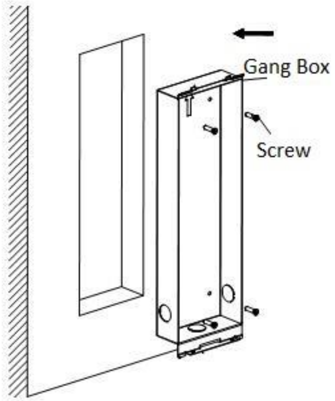


Figure 5-3 Insert the Gang Box into the Wall

3. Route the cables of the door station through the cable hole.
4. Put the door station into the gang box and hook the lock catches on the rear panel onto the hook **A and B** of the gang box.

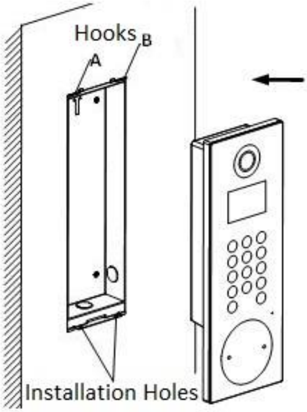


Figure 5-4 Install the Door Station

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

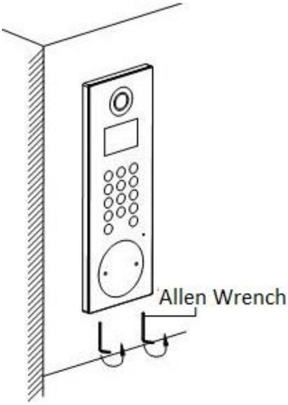


Figure 5-5 Tighten the Screws of Device

5.2 Installation of DS-KD8002-VM

5.2.1 Gang Box for DS-KD8002-VM

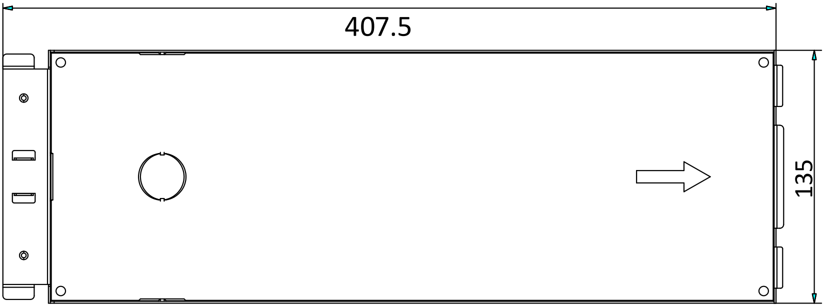


Figure 5-6 Front View

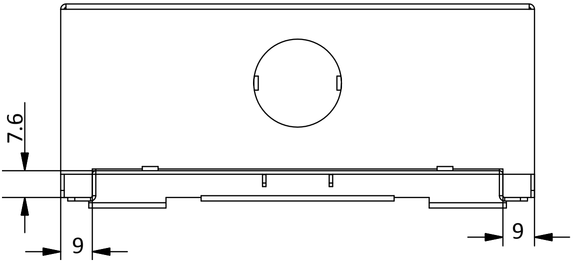


Figure 5-7 Overhead (Plan) View

NOTE

- The dimension of gang box for model DS-KD8002-VM door station is: 407.5 mm × 135 mm × 55 mm.
- The dimensions above are for reference only. The actual size can be slightly larger than the theoretical dimension.

5.2.2 Wall Mounting with Gang Box of DS-KD8002-VM

1. Chisel a hole in the wall for inserting the gang box. The size of the hole should be larger than that of the gang box. The suggested size of hole is 136 (length) × 408.5 (width) × 55.5 (depth) mm.

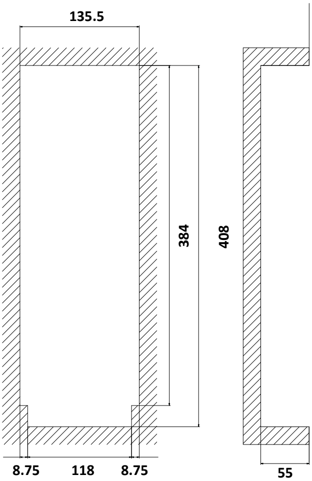


Figure 5-8 Dimensions of the Hole

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

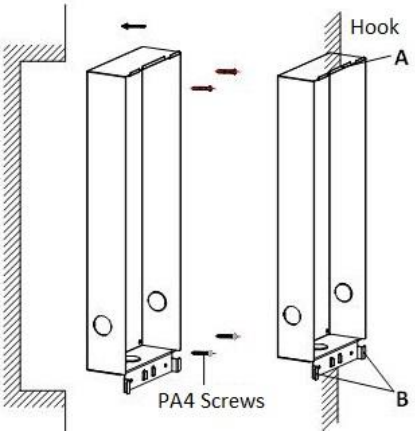


Figure 5-9 Insert the Gang Box into the Wall

3. Make sure the edges of the gang box align to the wall and the hook **A** and hook **B** of the gang box hook onto the wall.
4. Route the cables of the door station through the cable hole.
5. Insert the door station into the gang box and then move the door station downward to hook the lock catches on the rear panel onto the hook **C** of the gang box.
6. Fix the door station with 2 PM3 screws.

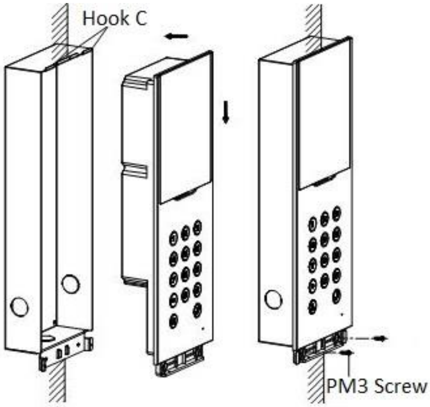


Figure 5-10 Install the Door Station

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

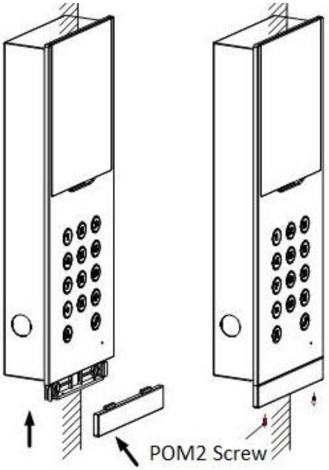


Figure 5-11 Secure the Door Station

5.3 Installation of DS-KD3002-VM

5.3.1 Gang Box for DS-KD3002-VM

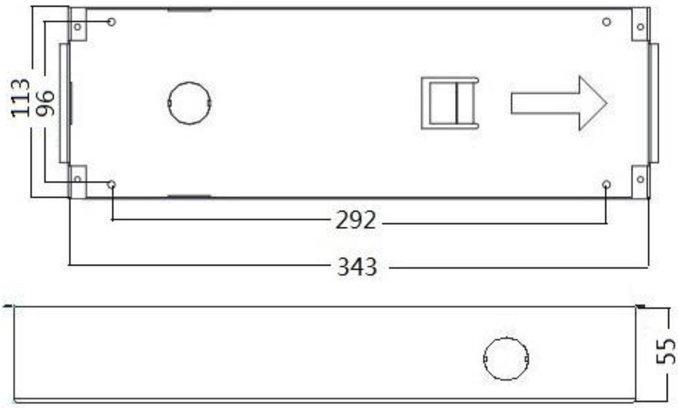


Figure 5-12 Front and Side View

NOTE

- The dimension of gang box for model DS-KD3002-VM door station is: 343(length)× 113(width)×55(depth) mm.
- The dimensions above are for reference only. The actual size can be slightly different from the theoretical dimension.

5.3.2 Wall Mounting with Gang Box of DS-KD3002-VM

Steps:

1. Chisel a hole in the wall for inserting the gang box. The size of the hole should be larger than that of the gang box. The suggested size of hole is 343.5 (length) × 113.5 (width) × 55.5 (depth) mm.
2. Insert the gang box into the hole and fix it with 4 PA4 screws.

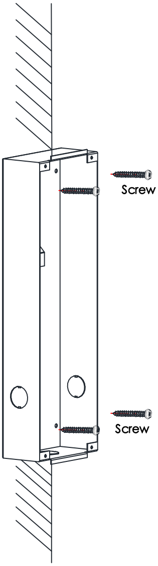


Figure 5-13 Insert the Gang Box into the Wall

3. Make sure the edges of the gang box align to the wall.
4. Route the cables of the door station through the cable hole.
5. Put the door station into the gang box.

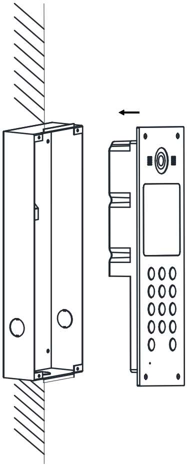


Figure 5-14 Install the Door Station

6. Fix the door station to the gang box with 4 crews.

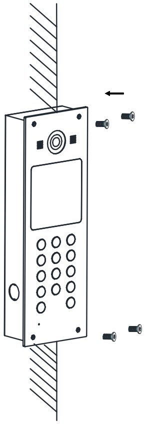


Figure 5-15 Tighten the Screws of Device

6 Before You Start

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

To activate the device with Batch Configuration Tool or iVMS-4200, refer to 8 *Remote Operation via Batch Configuration Tool* or 9 *Remote Operation via iVMS-4200 Client Software*.

To activate the device locally, refer to *7 Local Operation.*

To configure the key parameters of device on the user interface of door station, you are required to input the admin password. Here the admin password refers to the configuration password.

The default admin password (configuration password) is 888999.

You can set the login password of the device by yourself.

You must change the default credential to protect against unauthorized access to the product. Please refer to *7.4.3 Changing Password*.

7 Local Operation

7.1 Keys Description

Key descriptions of door stations are illustrated in Table 7-1.

Table 7-1 Key Descriptions

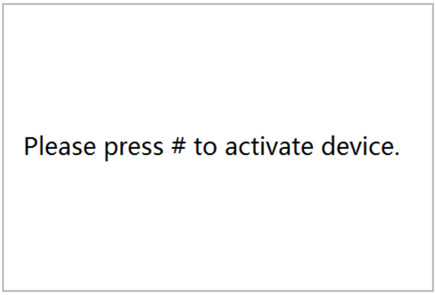
Key	Description
Numeric Key **2**	▲
Numeric Key **4**	▼
Numeric Key **6**	◀
Numeric Key **8**	▶
#	Call Key (When calling residents or center)
	Confirm
*	Return
	Delete

7.2 Activating Device

You cannot use the door station until you activate it.

Steps:

1. Power on the door station to enter the activation interface automatically.



Please press # to activate device.

Figure 7-1 Activate the Device (Option 1)

2. Press the **#** key.

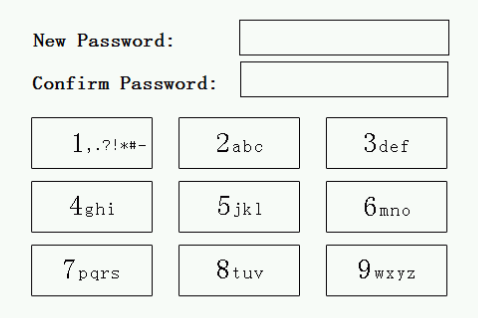


Figure 7-2 Set Password

3. Enter a new password, and confirm the password.

   The character description for each numeric key is shown in Table 7-2.

Table 7-2 Character Description

Key	Description	Key	Description
1	1,.?!*#-	6	6mnoMNO
2	2abcABC	7	7pqrsPQRS
3	3defDEF	8	8tuvTUV
4	4ghiGHI	9	9wxyzWXYZ
5	5jklJKL	0	0

NOTE

When entering the password, taking the numeric key **2** as example, press the numeric key **2** once, the text field shows "**2**", and press it again, the text field shows "**a**", and press it again, the text field shows "**b**", and so on.

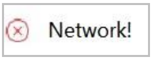
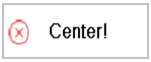
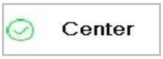
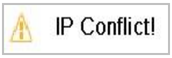
STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your 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.*

4. Press the **#** key to complete the activation.

7.3 Status

The door station can display different status with icons in Table 7-3.

Table 7-3 Icon Description

Icon	Description
 ⓧ Network!	Please check the network cable of the door station.
 ⓧ Center!	Invalid SIP server IP address. Set the SIP server IP address.
	Network of SIP server is not available. Check the SIP server network connection.
	SIP server communication is not available. Check if the SIP server IP address is correct.
	SIP server rejected to login the device. Check if the device No. has been registered.
 ✓ Center	The network connection of the main door station/outer door station is normal, and the main door station/outer door station has been successfully registered to the SIP server.
	The network connection of the sub door station is normal, and the sub door station has been successfully registered to the main door station/SIP server.
 ⚠ IP Conflict!	IP address of the door station conflicts with other devices' IP address

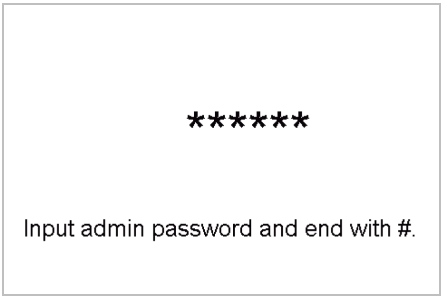
7.4 Setting Parameters

You can set the network configuration, local settings, password and volume of the door station. You can also view the version of the device and issue cards with it.

To set parameters for the door station, you should go to the configuration mode first.

Steps:

1. Hold down the ***** key and the **#** key for 2s to enter the admin password interface.
2. Enter the admin password, and press the **#** key.



******

Input admin password and end with #.

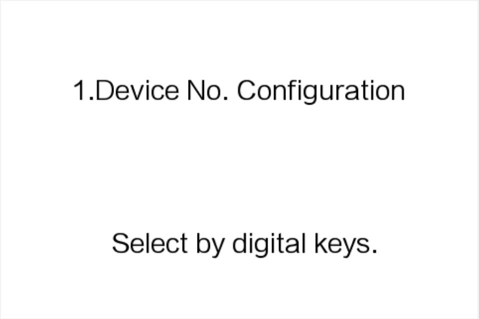
Figure 7-3 Admin Password Interface

- The default admin password is 888999.
- Under the configuration mode, press the number key **2** and **8** to switch the parameter interfaces.

7.4.1 Local Settings

For the local settings, you can set the door station No. such as community No., building No., floor No., and so on.

Press the numeric keys **4** and **6** to switch to the local settings interface.



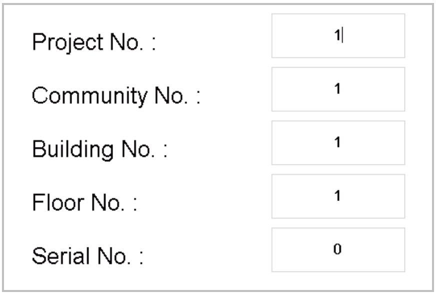
1.Device No. Configuration

Select by digital keys.

Figure 7-4 Local Settings Interface

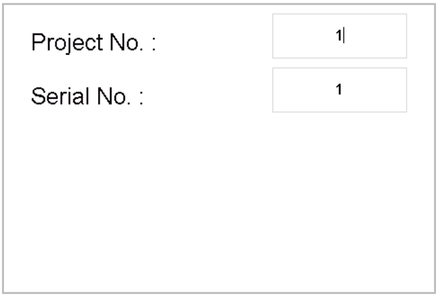
Steps:

1. On the local settings interface, press the numeric key **1** to enter the device No. settings interfaces.



Project No. :	1
Community No. :	1
Building No. :	1
Floor No. :	1
Serial No. :	0

Figure 7-5 Device No. Settings Interface (Door Station)



Project No. :	1
Serial No. :	1

Figure 7-6 Device No. Settings Interface (Outer Door Station)

2. Edit parameters.
    1) Move the cursor to parameters to be configured.
    2) Press the **#** key to enter the editing mode, and input numbers.
    3) Press the **#** key to exit the editing mode.
3. Press the ***** key to exit the device No. settings interface.

NOTE

- In the main/sub door station mode, the serial No. of main door station should be set as 0, and the serial No. of sub door station should be larger than 0.
- For each main door station, at most 8 sub door stations can be installed.
- For the outer door station, the serial No. cannot be set as 0.

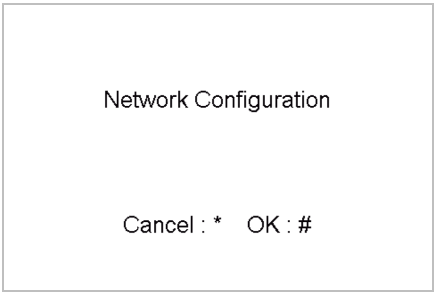
7.4.2 Editing Network Parameters

Purpose:

Network connection is mandatory for the use of door station.

Steps:

1. Enter the network parameters settings interface.
    1) Press the numeric keys **4** and **6** to switch to the network configuration interface

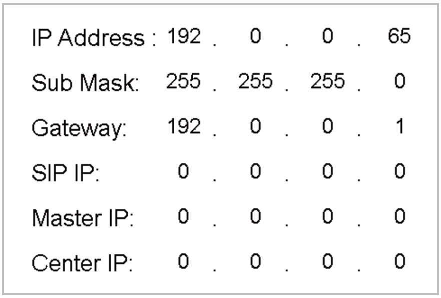


Network Configuration

Cancel : *   OK : #

Figure 7-7 Network Configuration Interface

2) Press the **#** key to enter the network parameters settings interface.



IP Address :	192 .	0 .	0 .	65
Sub Mask:	255 .	255 .	255 .	0
Gateway:	192 .	0 .	0 .	1
SIP IP:	0 .	0 .	0 .	0
Master IP:	0 .	0 .	0 .	0
Center IP:	0 .	0 .	0 .	0

Figure 7-8 Network Parameters Settings Interface

2. Edit network parameters.
    1) Move the cursor to parameters to be configured.
    2) Press the **#** key to enter or exit the editing mode.
3. Press the ***** key to exit the network configuration interface.

7.4.3 Changing Password

Purpose:

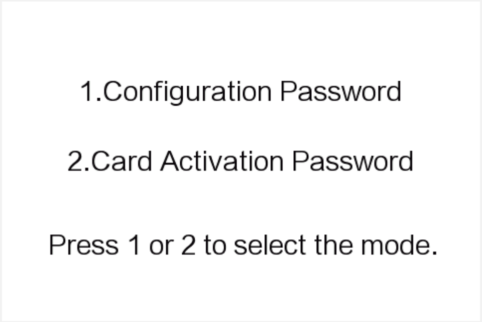
2 kinds of password are available when using the door station: configuration password (admin password) and card activation password.

Configuration Password: It is necessary when you want to configure parameters of the door station, such as IP parameters, door station No., system type, and so on.

Card Activation Password: It is necessary when you want to issue cards via password.

> ⚠ *The default configuration password is 888999. We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.*

Press the numeric keys **4** and **6** to switch to the password settings interface.



1.Configuration Password

2.Card Activation Password

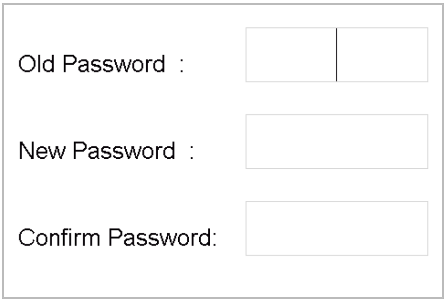
Press 1 or 2 to select the mode.

Figure 7-9 Password Settings Interface

Chaning Configuration Password

Steps:

1. On the password settings interface, press the numeric key **1** to enter the configuration password changing interface.



Old Password :

New Password :

Confirm Password:

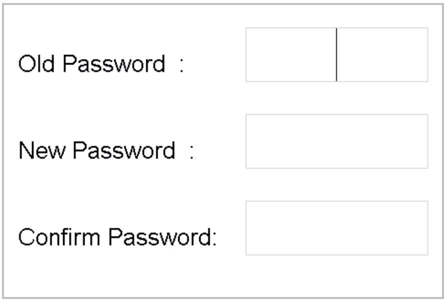
Figure 7-10 Configuration Password Changing Interface

2. Enter the old password, and the new password, and confirm the new one.
    1) Move the cursor to parameters to be configured.
    2) Press the **#** key to enter or exit the editing mode.
3. Press the * key to exit the password settings interface.

Chaning Card Activation Password

Steps:

1. On the password settings interface, press the numeric key **2** to enter the card activation password changing interface.



Old Password :

New Password :

Confirm Password:

Figure 7-11 Card Activation Password Changing Interface

2. Enter the old password, and the new password, and confirm the new one.
    3) Move the cursor to parameters to be configured.
    4) Press the **#** key to enter or exit the editing mode.
3. Press the * key to exit the password settings interface.

7.4.4 Issuing Card

Purpose:

You cannot open door by swiping the card until you have issue the card.

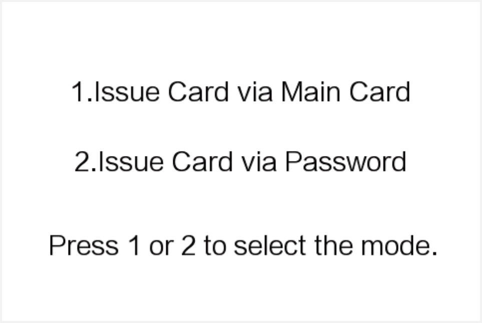
You can issue the card both locally or remotely. For the detail information about issuing card remotely, please refer to *9.6.3 Card Management*.

2 methods of issuing card locally are available: issuing card via the main card, and issuing card via the card activation password.

Issuing Card via Main Card: You can swipe card to issue it after swiping the main card in advance.

Issuing Card via Password: You can swipe card to issue it after inputting the card activation password in advance.

Press the numeric key 4 and 6 to enter the card issuing interface.



1.Issue Card via Main Card

2.Issue Card via Password

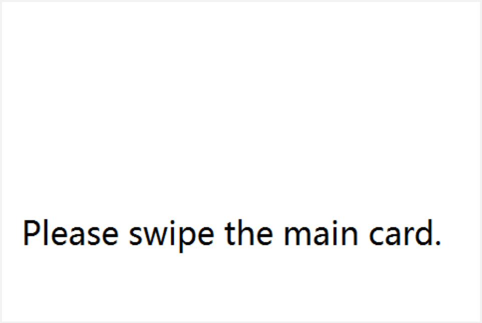
Press 1 or 2 to select the mode.

Figure 7-12 Card Issuing Interface

Issuing Card via Main Card

Steps:

1. On the card issuing interface, press the numeric key **1** to enter the main card swiping interface.



Please swipe the main card.

Figure 7-13 Main Card Swiping Interface

2. Swipe the main card on the card induction area, and hear a voice prompt: Issuing card succeed.
3. Swipe the unauthorized sub cards in turn after hearing a voice prompt: Please swipe the sub card.
4. Press the * key to exit the card issuing interface.

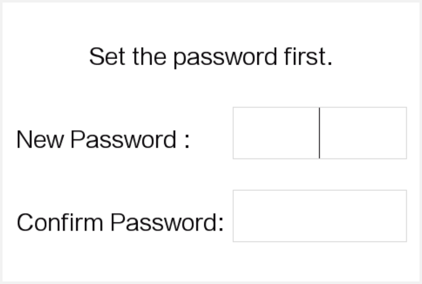
NOTE

- If the main card is invalid, it prompts the message: Incorrect Main Card.
- For the door station (D series), if the amount of sub cards exceeds 2500, no more sub card can be issued and the station prompts the message: No more sub card can be issued.
- For the outer door station, if the amount of sub cards exceeds 50000, no more sub card can be issued and the station prompts the message: No more sub card can be issued.
- After enrolling cards with client software, the card issuing function will be disabled on the user interface.

Issuing Card via Password

Steps:

1. On the card issuing interface, press the numeric key **2** to enter the card activation password settings interface (Figure 7-14) or the card activation password inputting interface (Figure 7-15).

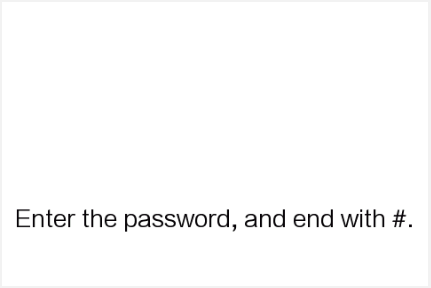


Set the password first.

New Password :

Confirm Password:

Figure 7-14 Card Activation Password Settings Interface



Enter the password, and end with #.

Figure 7-15 Card Activation Password Inputting Interface

2. Set the card activation password or input the card activation password to enter the card swiping interface.
3. Swipe the authorized card in turn.
4. Press the * key to exit the card issuing interface.

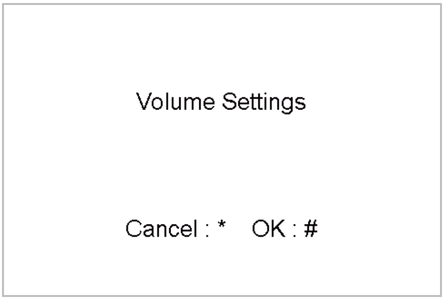
NOTE

- For the door station (D series), if the amount of sub cards exceeds 2500, no more sub card can be issued and the station prompts the message: No more sub card can be issued.
- For the outer door station, if the amount of sub cards exceeds 50000, no more sub card can be issued and the station prompts the message: No more sub card can be issued.
- After enrolling cards with client software, the card issuing function will be disabled on the user interface.

7.4.5 Setting Volume

Steps:

1. Enter the password settings interface.
   1) Press the numeric keys **4** and **6** to switch to the volume settings interface

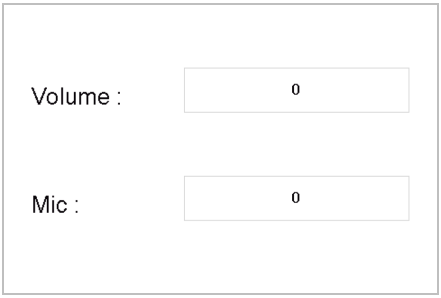


Volume Settings

Cancel : *   OK : #

Figure 7-16 Volume Settings Interface

   2) Press the **#** key to enter the volume parameters settings interface.



Volume : 0

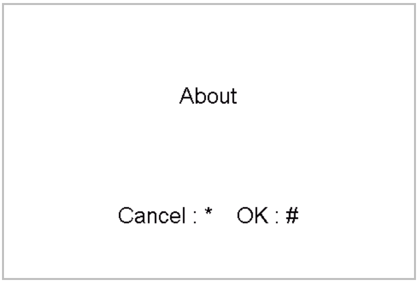
Mic : 0

Figure 7-17 Volume Parameters Settings Interface

2. Set the volume.
   1) Move the cursor to parameters to be configured.
   2) Press the **#** key to enter or exit the editing mode.
3. Press the * key to exit the volume settings interface.

7.4.6 About

On the settings interface, press numeric keys **4** and **6** to switch to the **About** interface, and press the **#** key to view the version of the device.



About

Cancel : * OK : #

Figure 7-18 Device Version Interface

7.5 Calling Resident

You can call residents via the door station no matter the door station is in the network intercom system or the analog intercom system.

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

Working as Main/Sub Door Station

Steps:

1. Enter the Room No..
2. Press the **#** key or the ☎ key to start calling the resident.

Working as Outer Door Station

Steps:

1. Enter the Community No. and the **#** key, the Building No. and the **#** key, the Unit No. and the **#** key, and the Room No. and the **#** key.
2. Press the ☎ key to start calling the resident.

7.6 Unlocking Door

Before you start:

Make sure your door station works as the main/sub door station.

Purpose:

2 ways are available to unlock the door: unlocking door via password, and unlocking door via card.

Unlocking Door by Password

Unlocking the door by inputting the password is only available in the network intercom system.

Steps:

1. Enter the **#** key and the Room No..
2. Enter the password and the **#** key.

NOTE

- The password varies according to different rooms.
- The default unlocking password is 123456.

Unlocking Door by Card

Before you start:

Make sure the card has been issued. You can issue the card via the door station, or via iVMS-4200 client software. Please refer to *9.6.2 Video Intercom*

Receiving Call from Door Station

Purpose:

When the door station has been added to the client software, you can call the client via door station.

Before you start:

- Make sure the door station has been added to the client software.
- Make sure the SIP server IP address of the door station is not configured (or abnormal).

Steps:

Press **Calling Center** key on the door station.

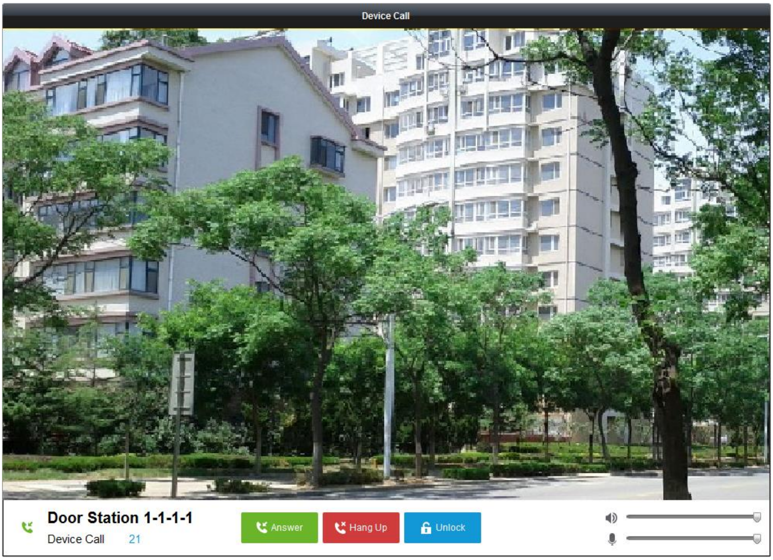


Figure 9-1 Calling from Door Station

NOTE

- When the SIP server IP of the door station is configured, press **Calling Center** key on the door station to call the master station instead of the client software.
- Click **Unlock** to unlock the building or villa door via the client software, no matter whether answering the call from door station or not.
- Click **Answer** to answer the call from door station.
- Click **Hang Up** to end the call from door station.

Call Log

On the Video Intercom tab page, there are four types of call logs you can search: **All**, **Dialed**, **Received**, and **Missed**.

On the dial log area, you can view detail information of the dialog, and click **Call** to start the audiovisual call with the indoor station.

Click Clear Log to clear all logs in the list (optional).

Card Management for detail steps.

Unlocking the door by swiping the card is available both in the network intercom system and the analog intercom system.

Steps:

Swipe the card on the card induction area to unlock the door.

NOTE

The main card does not support unlocking the door.

8 Remote Operation via Batch Configuration Tool

You can configure and operate the video intercom devices via Batch Configuration Tool. Default parameters of door station are as follows:

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

8.1 Activating Device Remotely

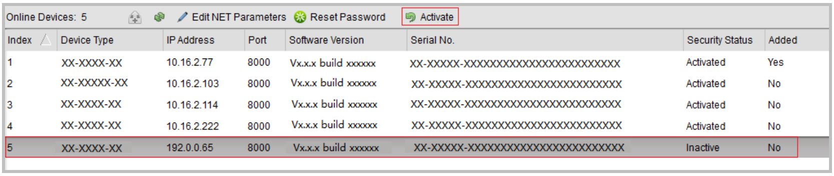
Purpose

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

Activation via Batch Configuration Tool, and Activation via iVMS-4200 are supported. Here take activation via Batch Configuration Tool as example to introduce the device activation. Please refer to the user manual for the activation via iVMS-4200.

Steps:

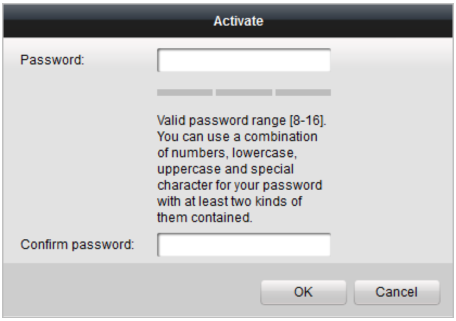
1. Run the Batch Configuration Tool.



Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Added
1	XX-XXXX-XX	10.16.2.77	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	192.0.0.65	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Inactive	No

Figure 8-1 Selecting Inactive Device

2. Select an inactivated device and click the **Activate** button.


Activate

Password:

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm password:

Figure 8-2 Activation

3. Create a password, and confirm the password.

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.*

4. Click the **OK** button to activate the device.

NOTE

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

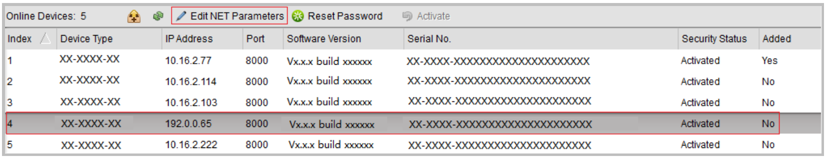
8.2 Editing Network Parameters

Purpose:

To operate and configure the device via LAN (Local Area Network), you need connect the device in the same subnet with your PC. You can edit network parameters via batch configuration tool, and iVMS-4200 software. Here take editing network parameters via batch configuration tool as example.

Steps:

1. Select an online activated device and click the **Edit NET Parameters** button.

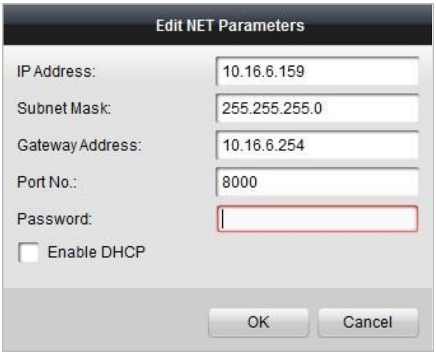


Online Devices: 5

Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Added
1	XX-XXXX-XX	10.16.2.77	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	192.0.0.65	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No

Figure 8-3 Clicking Edit NET Parameters Button

2. Change the device IP address and gateway address to the same subnet with your computer.
3. Enter the password and click the **OK** button to activate the network parameters modification.



Edit NET Parameters

IP Address: 10.16.6.159

Subnet Mask: 255.255.255.0

Gateway Address: 10.16.6.254

Port No.: 8000

Password:

□ Enable DHCP

Figure 8-4 Editing Network Parameters

NOTE

- The default port No. is 8000.
- The default IP address of the door station is 192.0.0.65.
- After editing the network parameters of device, you should add the devices to the device list again.
- Enable DHCP, and the software can obtain network parameters for the device automatically.

8.3 Adding Device

Before you start:

Make sure the device to be added has been activated.

Purpose:

For batch configuration tool software, you should add device to the software so as to configure the device remotely.

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

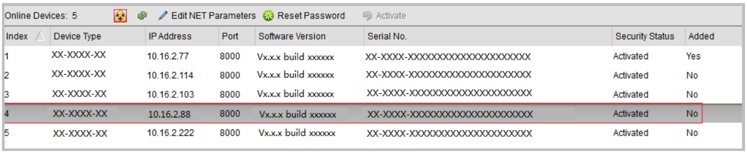
8.3.1 Adding Online Device

Before you start:

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

Steps:

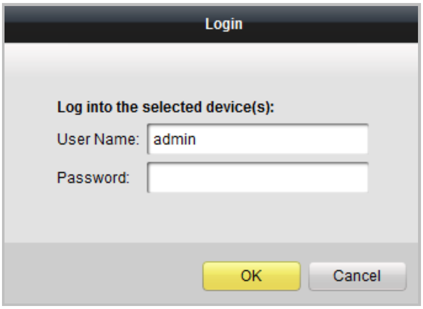
4. Select an active online device or hold the **Ctrl** or **Shift** key to select multiple devices in the online devices list.



Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Added
1	XX-XXXX-XX	10.16.2.77	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	10.16.2.88	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXX	Activated	No

Figure 8-5 Online Devices Interface

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



Log into the selected device(s):

User Name: admin

Password:

Figure 8-6 Login Dialog Box

6. Enter the user name and password.
7. Click the **OK** button to save the settings.

NOTE

- Only devices successfully logged in will be added to the device list for configuration.
- If you add devices in batch, please make sure selected devices have the same user name and password.

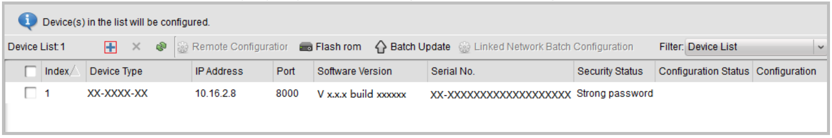
8.3.2 Adding by IP Address

Purpose:

You can add the device by entering IP address.

Steps:

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

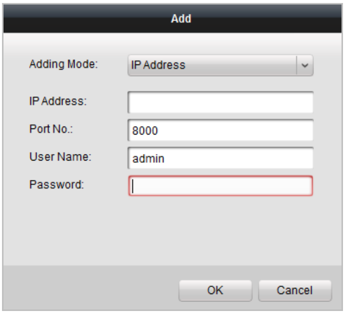


Device(s) in the list will be configured.

□	Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Configuration Status	Configuration
□	1	XX-XXXX-XX	10.16.2.8	8000	V x.x.x build xxxxxx	XX-XXXXXXXXXXXXXXXXXXX	Strong password		

Figure 8-7 Adding Button

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



Adding Mode: IP Address

IP Address:

Port No.: 8000

User Name: admin

Password:

Figure 8-8 Adding by IP Address

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

NOTE

- You cannot add the device(s) to the device list if the user name and password are not identical.
- When you add devices by IP Address, IP Segment or Port No., the devices should be online devices.

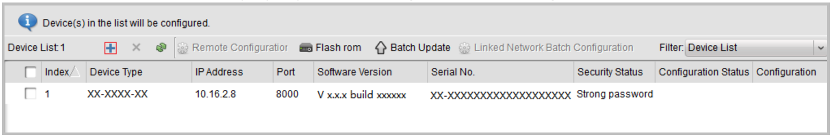
8.3.3 Adding by IP Segment

Purpose:

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

Steps:

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



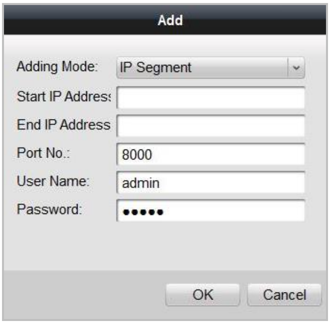
Device(s) in the list will be configured.

Device List:1

	Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Configuration Status	Configuration
□	1	XX-XXXX-XX	10.16.2.8	8000	V x.x.x build xxxxxx	XX-XXXXXXXXXXXXXXXXXXX	Strong password		

Figure 8-9 Adding Button

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



Adding Mode: IP Segment

Start IP Addres:

End IP Address

Port No.: 8000

User Name: admin

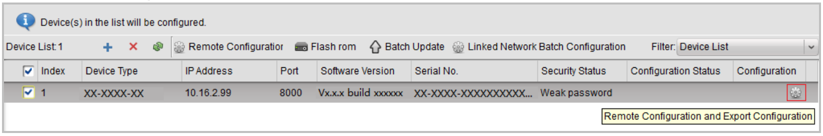
Password: ●●●●●

Figure 8-10 Adding by IP Segment

5. 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 Configuring Devices Remotely

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



Device(s) in the list will be configured.

Device List:1
Remote Configuratio
Flash rom
Batch Update
Linked Network Batch Configuration
Filter: Device List

☑ Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Configuration Status	Configuration
☑ 1	XX-XXXX-XX	10.16.2.99	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXX...	Weak password		⚙

Remote Configuration and Export Configuration

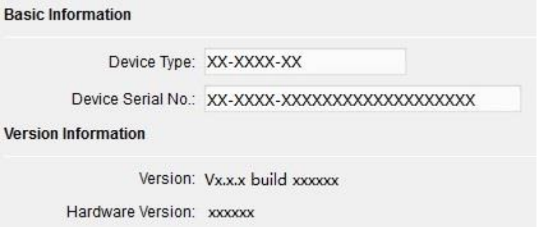
Figure 8-11 Remote Configuration

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, and so on.

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.



Basic Information

Device Type: XX-XXXX-XX

Device Serial No.: XX-XXXX-XXXXXXXXXXXXXXXXXX

Version Information

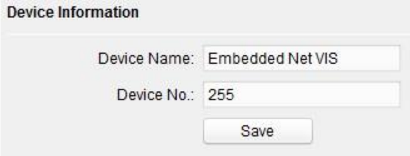
Version: Vx.x.x build xxxxxx

Hardware Version: xxxxxx

Figure 8-12 Device Information

General

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



Device Information

Device Name: Embedded Net VIS

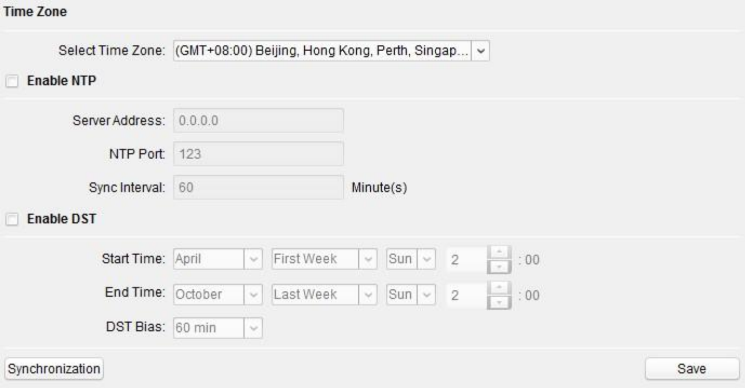
Device No.: 255

Figure 8-13 General

Time

Steps:

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



Time Zone

Select Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singap...

□ Enable NTP

Server Address: 0.0.0.0

NTP Port: 123

Sync Interval: 60 Minute(s)

□ Enable DST

Start Time: April First Week Sun 2 :00

End Time: October Last Week Sun 2 :00

DST Bias: 60 min

Figure 8-14 Time Settings

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.

- **DST**

1) Check the checkbox of Enable DST to enable DST.
2) Enter the start time and end time of DST, and set the DST bias.

3. Click the **Save** button to save and realize the time settings.

NOTE

- 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.

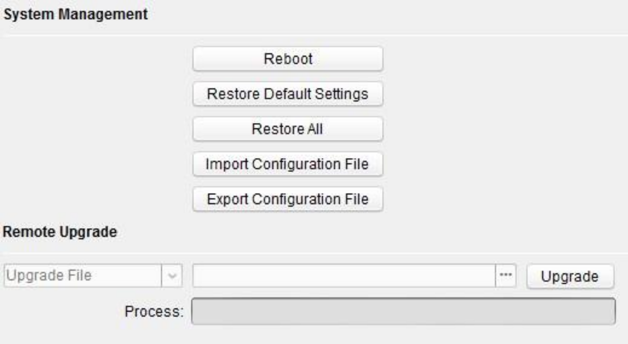
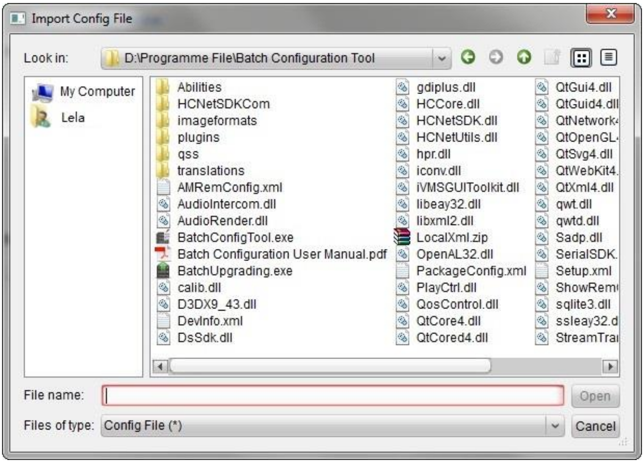


Figure 8-15 System Maintenance

2. Click **Reboot** and the system reboot dialog box pops up. Click **Yes** to reboot the system.
3. Click **Restore Default Settings** to restore the default parameters.
4. Click **Restore All** to restore all parameters of device and reset the device to inactive status.
5. Click **Import Configuration File** and the import file window pops up. Select the path of remote configuration files. Click **Open** to import the remote configuration file. The configuration file is imported and the device will reboot automatically.

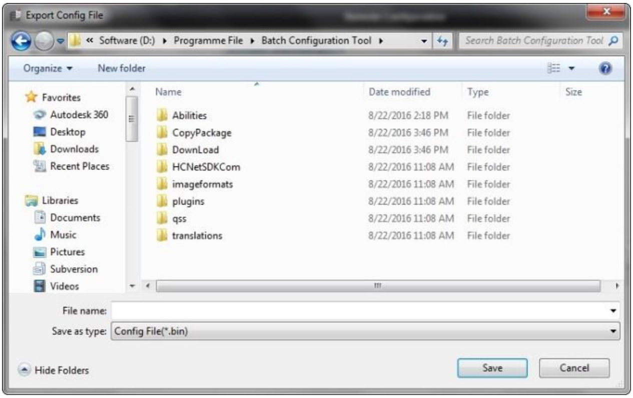


Look in: D:\Programme File\Batch Configuration Tool

Files of type: Config File (*)

Figure 8-16 Import File

6. Click **Export Configuration File** and the export file window pops up. Select the saving path of remote configuration files and click **Save** to export the configuration file.



Name	Date modified	Type	Size
Abilities	8/22/2016 2:18 PM	File folder	
CopyPackage	8/22/2016 3:46 PM	File folder	
DownLoad	8/22/2016 3:46 PM	File folder	
HCNetSDKCom	8/22/2016 11:08 AM	File folder	
imageformats	8/22/2016 11:08 AM	File folder	
plugins	8/22/2016 11:08 AM	File folder	
qss	8/22/2016 11:08 AM	File folder	
translations	8/22/2016 11:08 AM	File folder	

Save as type: Config File(*.bin)

Figure 8-17 Export File

7. Click ... to select the upgrade file and click **Upgrade** to remote upgrade the device. The process of remote upgrade will be displayed in the process bar.

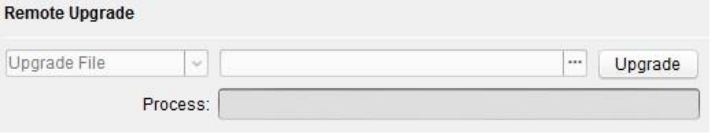


Figure 8-18 Remote Upgrade

NOTE

- Click **Restore Default Settings** button, all default settings, excluding network parameters, will be restored.
- Click **Restore All** button, all default settings, including network parameters, will be restored. The device will be reset to inactivated status.

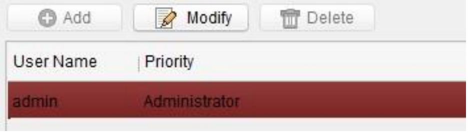
User

Purpose:

You can edit the password for logging in the device.

Steps:

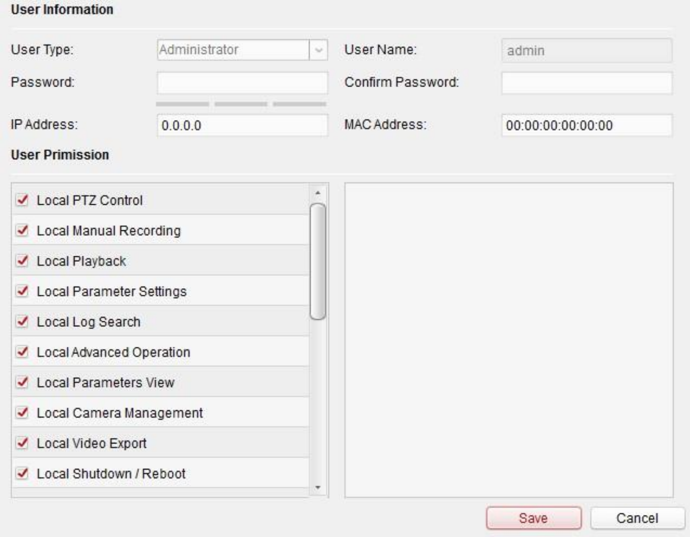
1. Click the **User** button to enter the user information editing interface.



User Name	Priority
admin	Administrator

Figure 8-19 Select User Name

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



User Information

User Type:	Administrator	User Name:	admin
Password:		Confirm Password:	
IP Address:	0.0.0.0	MAC Address:	00:00:00:00:00:00

User Primission

- ☑ Local PTZ Control
- ☑ Local Manual Recording
- ☑ Local Playback
- ☑ Local Parameter Settings
- ☑ Local Log Search
- ☑ Local Advanced Operation
- ☑ Local Parameters View
- ☑ Local Camera Management
- ☑ Local Video Export
- ☑ Local Shutdown / Reboot

Figure 8-20 Modify User Information

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

NOTE

- The new password and confirm password should be identical.

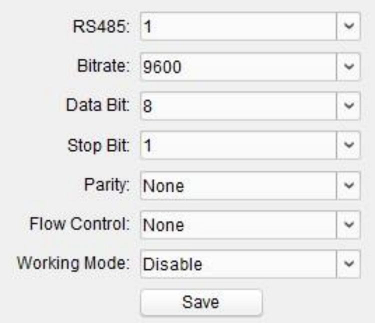
- After editing the password of device, click ♻ button from the device list, the added device will not be there. You should add the device again with new password to operate the remote configuration.

RS485

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

When use RS-485 interface to connect the door station and the card reader, you should set the bitrate as **19200**, and set the working mode as **Card Reader**.

When use RS-485 interface to connect the door station and the elevator controller, you should set the bitrate as **19200**, and set the working mode as **Elevator Control**.



RS485:	1
Bitrate:	9600
Data Bit:	8
Stop Bit:	1
Parity:	None
Flow Control:	None
Working Mode:	Disable

Figure 8-21 RS-485

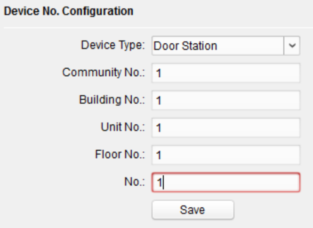
8.4.2 Video Intercom

Click the **Video Intercom** button on the remote configuration interface to enter the video intercom parameters settings: Device Number Configuration, Time Parameters, Password, Zone Configuration, IP Camera Information, and Volume Input and Output Configuration, and so on.

Device ID Configuration

Steps:

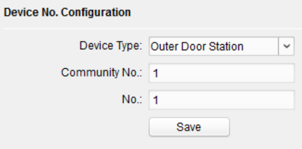
1. Click the **ID Configuration** button to enter device ID configuration interface.



Device No. Configuration

Device Type:	Door Station
Community No.:	1
Building No.:	1
Unit No.:	1
Floor No.:	1
No.:	1

Figure 8-22 Door Station



Device No. Configuration

Device Type:	Outer Door Station
Community No.:	1
No.:	1

Figure 8-23 Outer Door Station

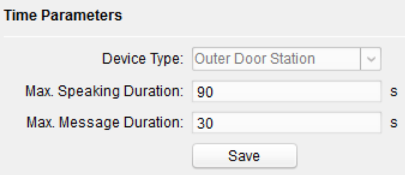
2. Select the device type from the drop-down list, and set the corresponding information.
3. Click the **Save** button to enable the device number configuration.

NOTE

- For main door station (D series or V series), the serial No. is 0.
- For sub door station (D series or V series), the serial No. is higher than 0. Serial No. ranges from 1 to 99.
- For each villa or building, at least one main door station (D series or V series) should be configured, and sub door stations (D series or V series) can be customized.
- For one main door station (D series or V series), at most 8 sub door stations can be customized.
- Select doorphone as device type, and the serial No. is not necessary to configure. Please utilize the doorphone along with the main door station (V Series or D Series).

Time Parameters

1. Click the **Time Parameters** button to enter time parameters settings interface.
2. Configure the maximum ring duration, maximum live view time, and call forwarding time.
3. Click the **Save** button.



Time Parameters

Device Type: Outer Door Station

Max. Speaking Duration: 90 s

Max. Message Duration: 30 s

Figure 8-24 Time Parameters

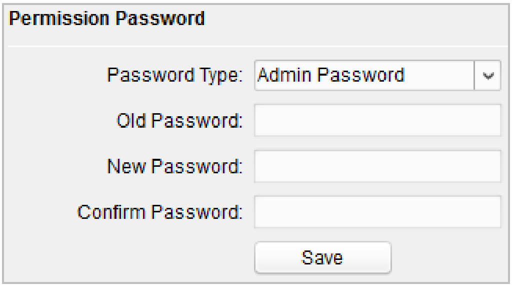
NOTE

- For door station, maximum speaking time and maximum message time should be configured. Maximum speaking time varies from 90s to 120s, and maximum message time varies from 30s to 60s.

Password

Click the **Password** button to enter password changing interface.

For door station, only admin password can be changed.



Permission Password

Password Type: Admin Password

Old Password:

New Password:

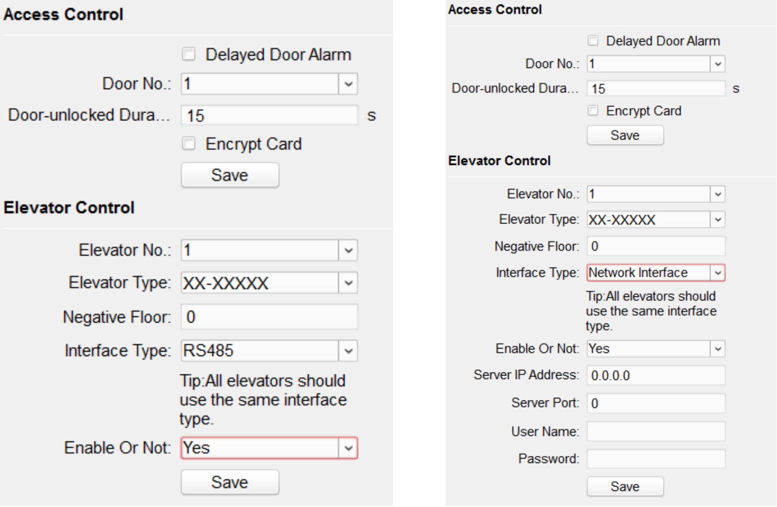
Confirm Password:

Save

Figure 8-25 Password Configuration

Access Control and Elevator

Click ***Access Control and Elevator*** to enter corresponding configuration page.



Access Control

□ Delayed Door Alarm

Door No.: 1

Door-unlocked Dura...: 15 s

□ Encrypt Card

Save

Elevator Control

Elevator No.: 1

Elevator Type: XX-XXXXX

Negative Floor: 0

Interface Type: RS485

Tip:All elevators should use the same interface type.

Enable Or Not: Yes

Save

Access Control

□ Delayed Door Alarm

Door No.: 1

Door-unlocked Dura...: 15 s

□ Encrypt Card

Save

Elevator Control

Elevator No.: 1

Elevator Type: XX-XXXXX

Negative Floor: 0

Interface Type: Network Interface

Tip:All elevators should use the same interface type.

Enable Or Not: Yes

Server IP Address: 0.0.0.0

Server Port: 0

User Name:

Password:

Save

Figure 8-26 Access Control and Elevator Configuration

Access Control

1. Select the door No.
2. Set the door-unlocked duration.
3. (Optional) Enable **Delay Door Alarm**.
4. Click **Save** to enable the settings.

NOTE

- The door-unlocked duration ranges from 1s to 225s.
- If you check **Delayed Door Alarm**, an alarm will be triggered automatically if the door is not locked in the configured duration.

- Enabling **Card Encrypt**, the door station can recognize the encrypted information of the card when you swiping the card on the door station.

Elevator Control

Before you start

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

Connection between the door station and the elevator controller supports 2 types: RS-485 or Network interface.

Step:

1. Select an elevator No., and select an elevator controller type for the elevator.
2. Set the negative floor.
3. Select the interface type: RS-485 or Network Interface.

   If you select RS-485, please make sure you have connected the door station to the elevator controller with RS-485 wire.

   If you select Network Interface, please enter the elevator controller's IP address, port No., user name, and password.
4. Enable the elevator control.

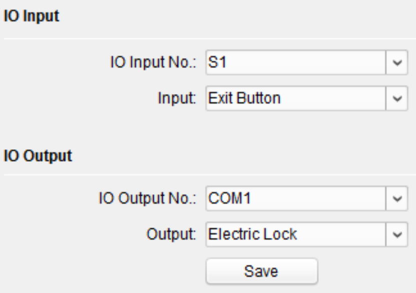
NOTE

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

IO Input and Output

Step:

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



IO Input

IO Input No.: S1

Input: Exit Button

IO Output

IO Output No.: COM1

Output: Electric Lock

Figure 8-27 IO Input/Output Configuration

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

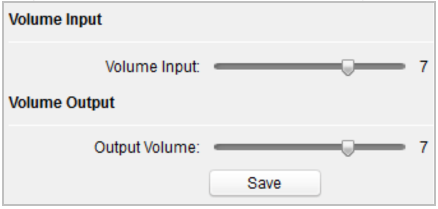
NOTE

- For door station (D series), there are 8 I/O Input Terminals. Terminal 1~4 correspond to **SENSOR** interfaces (S1, S2, S3, S4) of door station. Terminal 5~8 correspond to interfaces of **ALARM IN** (A1, A2, A3, A4). You can select an I/O input No. (S1, S2, S3, S4, AI, A2, A3, A4) from the drop-down list and set the I/O input as door magnetic exit button.
- For door station (V series), there are 4 I/O Input Terminals, corresponding to **SENSOR** interfaces (S1, S2, S3, S4) of door station.
- For door station (D series and V series), there are 4 I/O Output Terminals. Terminal 1~2 correspond to **DOOR** interfaces (NO1/COM1/NC1; NO2/COM2/NC2) of door station. You can enable/disable IO Out by selecting from the dropdown list. Terminal 3~4 correspond to interfaces of **ALARM OUT** (AO1+, AO1-; AO2+, AO2-).

Volume Input and Output

Step:

1. Click **Volume Input/Output** button to enter the volume input and output interface.



Volume Input

Volume Input: 7

Volume Output

Output Volume: 7

Figure 8-28 Volume Configuration

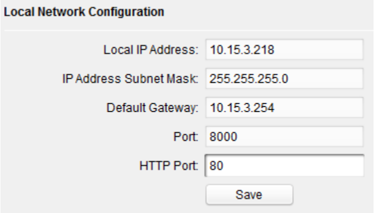
2. Slide the slider to adjust the volume input and volume output.
3. Click the **Save** button to enable the settings.

8.4.3 Network

Local Network Configuration

Steps:

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



Local Network Configuration

Local IP Address: 10.15.3.218

IP Address Subnet Mask: 255.255.255.0

Default Gateway: 10.15.3.254

Port: 8000

HTTP Port: 80

Figure 8-29 Local Network Parameters

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

NOTE

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

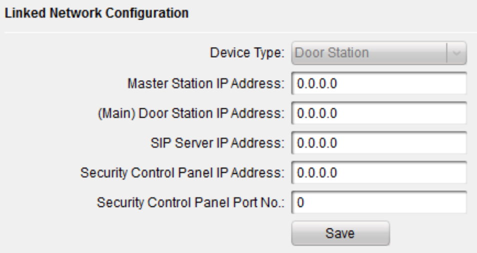
Linked Devices Network Configuration

Purpose:

In the linked devices network configuration interface, you can configure the network parameters of master stations, SIP servers and management centers of the same LAN. The devices can be linked to the door station and realize the linkage between these devices.

Steps:

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



Linked Network Configuration

Device Type: Door Station

Master Station IP Address: 0.0.0.0

(Main) Door Station IP Address: 0.0.0.0

SIP Server IP Address: 0.0.0.0

Security Control Panel IP Address: 0.0.0.0

Security Control Panel Port No.: 0

Figure 8-30 Linked Network Configuration

2. Enter the master station IP address, (main) door station IP address, SIP server IP address, management center IP address, and doorphone IP address.
3. Select the main door station type from the drop-down list.
4. Click the **Save** button to enable the settings.

NOTE

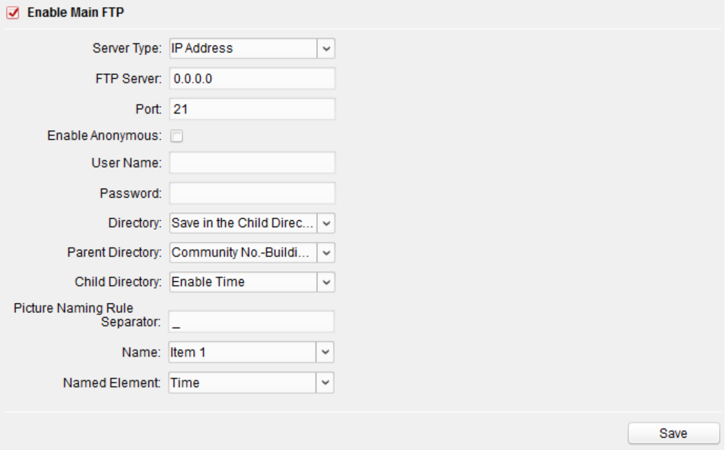
- After adding master station IP Address, the linkage between indoor station and master station can be realized.

- After adding the door station IP Address, the video intercom between indoor stations of same building can be realized.
- After adding SIP Server Address IP, the video intercom of same community: 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.
- For indoor extension, only parameter about the main indoor station should be configured.

FTP

Steps:

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



☑ Enable Main FTP

Server Type: IP Address

FTP Server: 0.0.0.0

Port: 21

Enable Anonymous: □

User Name:

Password:

Directory: Save in the Child Direc...

Parent Directory: Community No.-Buildi...

Child Directory: Enable Time

Picture Naming Rule Separator: _

Name: Item 1

Named Element: Time

Figure 8-31 FTP Configuration

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 **Save** button to enable the FTP parameters settings.

NOTE

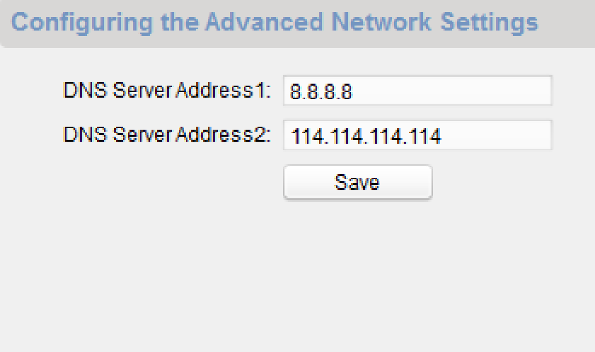
- The default port No. is 21.

- 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.
- This function only applies to the door station, except for the doorphone.

Advanced Settings

Steps:

1. Click the **Advanced Settings** button to enter the advanced network settings interface.



Configuring the Advanced Network Settings

DNS Server Address1: 8.8.8.8

DNS Server Address2: 114.114.114.114

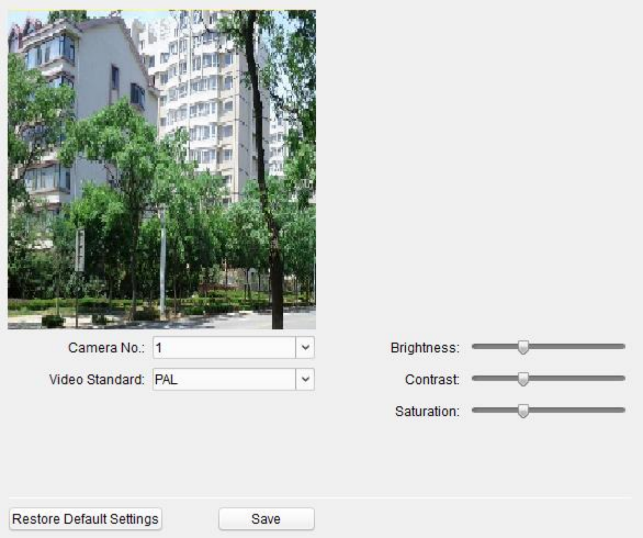
Figure 8-32 Advanced Settings

2. Enter the DNS server addresses.
3. Click the **Save** button to enable the advanced network settings.

8.4.4 Video Display

Steps:

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



Camera No.: 1

Video Standard: PAL

Figure 8-33 Video Display

2. Select the camera No..
3. Select the video standard (PAL and NTSC can be selected).
4. Set the brightness, contrast, and saturation of the video.
5. Click the **Save** button to enable the settings.

NOTE

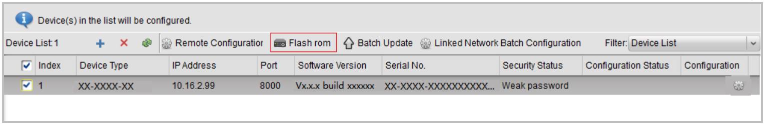
Click the **Restore Default Settings** button to restore all parameters excluding network parameters to the factory settings.

8.5 Video Intercom Device Set-up Tool

Purpose:

You can assign the device to the community, activate and set the device, and configure the network parameters and linked network parameters for the device by using the video intercom device set-up tool.

In the device list area, click Flash rom to enter the video intercom device set-up tool.


Device(s) in the list will be configured.
Remote Configuratior
Flash rom
Batch Update
Linked Network Batch Configuration

Device List: 1

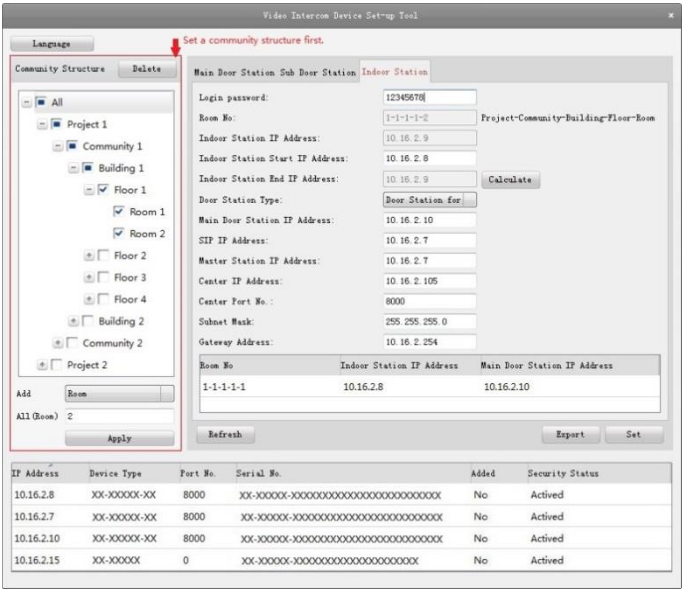
Filter: Device List

☑	Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Configuration Status	Configuration
☑	1	XX-XXXX-XX	10.16.2.99	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXX...	Weak password		⚙

Figure 8-34 Video Device Set-up Tool

8.5.1 Setting a Community Structure

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



Add: Room

All (Room): 2

Login password: 12345678

Room No: 1-1-1-1-2 Project-Community-Building-Floor-Room

Indoor Station IP Address: 10.16.2.9

Indoor Station Start IP Address: 10.16.2.8

Indoor Station End IP Address: 10.16.2.9

Door Station Type: Door Station for

Main Door Station IP Address: 10.16.2.10

SIP IP Address: 10.16.2.7

Master Station IP Address: 10.16.2.7

Center IP Address: 10.16.2.105

Center Port No.: 8000

Subnet Mask: 255.255.255.0

Gateway Address: 10.16.2.254

Room No	Indoor Station IP Address	Main Door Station IP Address
1-1-1-1-1	10.16.2.8	10.16.2.10

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.16.2.8	XX-XXXXX-XX	8000	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.16.2.7	XX-XXXXX-XX	8000	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.16.2.10	XX-XXXXX-XX	8000	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.16.2.15	XX-XXXXX	0	XX-XXXXX-XXXXXXXXXXXXXXXXXXXX	No	Actived

Figure 8-35 Setting a Community Structure

8.5.2 Setting Main/Sub Door Station

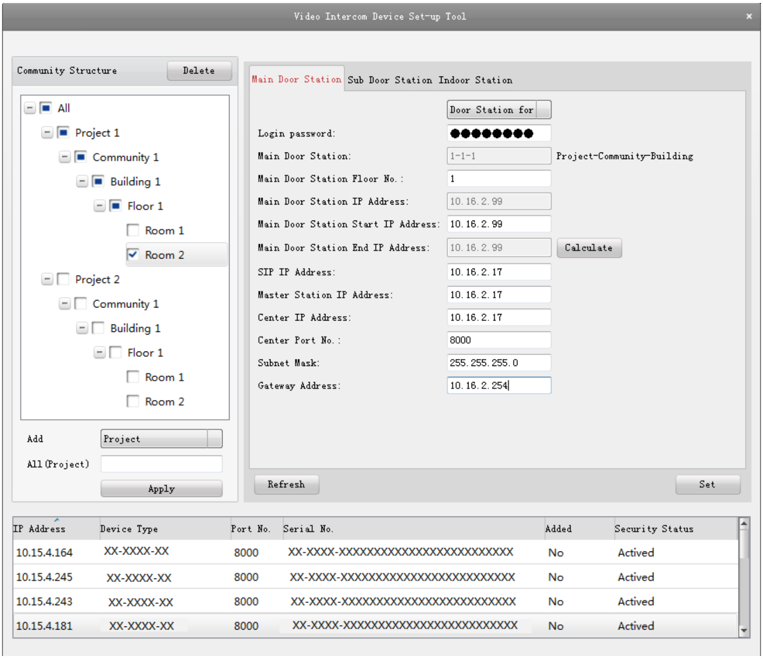
Setting Main Door Station

Purpose:

You can activate the online main door station, and configure the building No. for the online main door station.

Steps:

1. Select the community, and press the **Main Door Station** tab to switch to the main door station configuration interface.



Video Intercom Device Set-up Tool

Community Structure   Delete

- ☑ All
  - ☑ Project 1
    - ☑ Community 1
      - ☑ Building 1
        - ☑ Floor 1
          - □ Room 1
          - ☑ Room 2
  - □ Project 2
    - □ Community 1
      - □ Building 1
        - □ Floor 1
          - □ Room 1
          - □ Room 2

Add: Project

All (Project):

Apply

Main Door Station | Sub Door Station | Indoor Station

Door Station for

Login password: ●●●●●●●●●

Main Door Station: 1-1-1   Project-Community-Building

Main Door Station Floor No.: 1

Main Door Station IP Address: 10.16.2.99

Main Door Station Start IP Address: 10.16.2.99

Main Door Station End IP Address: 10.16.2.99   Calculate

SIP IP Address: 10.16.2.17

Master Station IP Address: 10.16.2.17

Center IP Address: 10.16.2.17

Center Port No.: 8000

Subnet Mask: 255.255.255.0

Gateway Address: 10.16.2.254

Refresh   Set

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.15.4.164	XX-XXXX-XX	8000	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.15.4.245	XX-XXXX-XX	8000	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.15.4.243	XX-XXXX-XX	8000	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXX	No	Actived
10.15.4.181	XX-XXXX-XX	8000	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXX	No	Actived

Figure 8-36 Setting Main Door Station

2. Select the door station type from the drop-down list menu: Door Station for Unit, or Door Station for Villa.
3. Enter the main door station start IP address, set the main door station floor No., and then click the **Calculate** button to generate the main door station end IP address and main door station No. (like 1-1-1) automatically.
4. Set the linked network parameters for the main door station: SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
5. Select an online door station, enter the login password, and click the **Set** button.

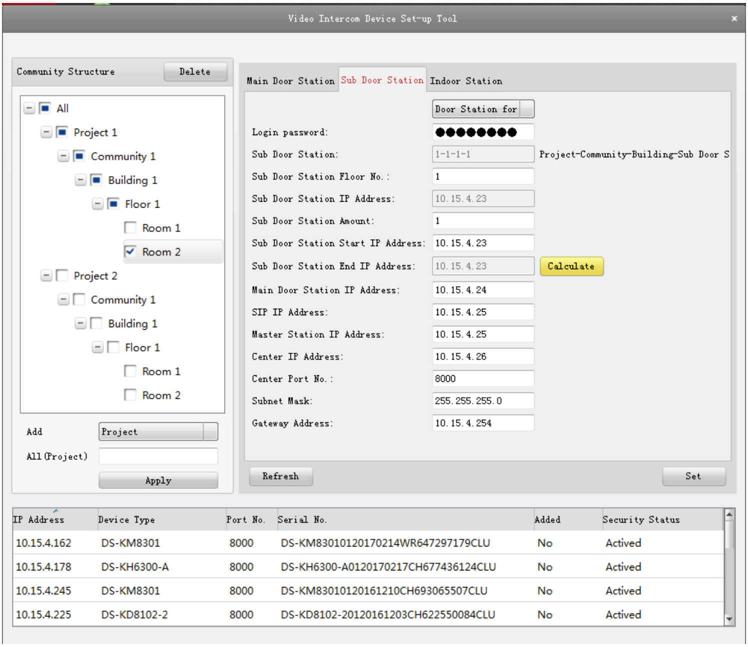
NOTE

- The default main door station floor No. is 1.
- For the login password, if the main door station has been activated, enter the activation password here. If the main door station is not activated, create a login password here, and the main door station will be activated simultaneously.
- When the device is successfully configured, it prompts the note: Configuring main door station parameters succeeded.

Setting Sub Door Station

Steps:

1. Select the community, and press the **Sub Door Station** tab to switch to the sub door station configuration interface.



- ■ All
  - ■ Project 1
    - ■ Community 1
      - ■ Building 1
        - ■ Floor 1
          - □ Room 1
          - ☑ Room 2
  - □ Project 2
    - □ Community 1
      - □ Building 1
        - □ Floor 1
          - □ Room 1
          - □ Room 2

Add: Project
All (Project):

Door Station for
Login password: ●●●●●●●●●
Sub Door Station: 1-1-1-1 Project-Community-Building-Sub Door S
Sub Door Station Floor No.: 1
Sub Door Station IP Address: 10.15.4.23
Sub Door Station Amount: 1
Sub Door Station Start IP Address: 10.15.4.23
Sub Door Station End IP Address: 10.15.4.23
Main Door Station IP Address: 10.15.4.24
SIP IP Address: 10.15.4.25
Master Station IP Address: 10.15.4.25
Center IP Address: 10.15.4.26
Center Port No.: 8000
Subnet Mask: 255.255.255.0
Gateway Address: 10.15.4.254

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.15.4.162	DS-KM8301	8000	DS-KM83010120170214WR647297179CLU	No	Actived
10.15.4.178	DS-KH6300-A	8000	DS-KH6300-A0120170217CH677436124CLU	No	Actived
10.15.4.245	DS-KM8301	8000	DS-KM83010120161210CH693065507CLU	No	Actived
10.15.4.225	DS-KD8102-2	8000	DS-KD8102-20120161203CH622550084CLU	No	Actived

Figure 8-37 Setting Sub Door Station

2. Select the door station type from the drop-down list menu: Door Station for Unit, or Door Station for Villa.
3. Set the sub door station parameters (sub door station amount, floor No., start IP address, end IP address), and then click the **Calculate** button to generate the sub door station end IP address and sub door station No. (like 1-1-1-1) automatically.
4. Set the linked network parameters for the sub door station: main door station IP address, SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
5. Select an online door station, enter the login password, and click the **Set** button.

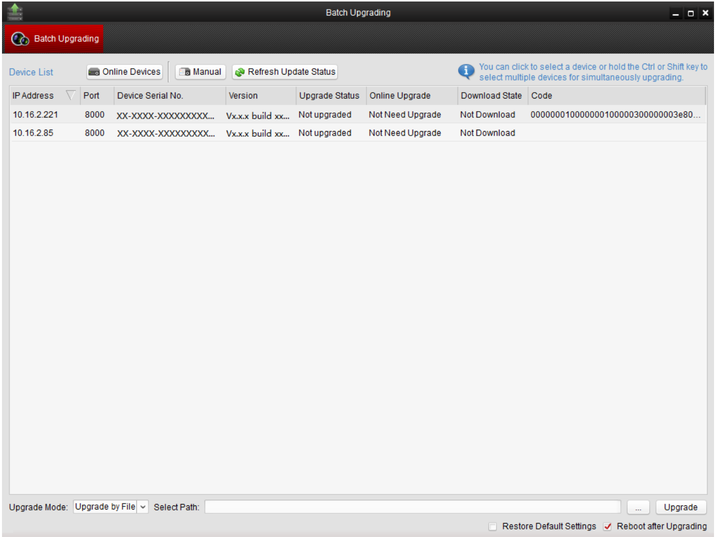
NOTE

- The default sub door station floor No. is 1.
- Up to 8 sub door stations can be added to a main door station.

- For the login password, if the sub door station has been activated, enter the activation password here. If the sub door station is not activated, create a login password here, and the sub door station will be activated simultaneously.
- When the device is successfully configured, it prompts the note: Configuring main door station parameters succeeded

8.6 Batch Upgrading

In the device list area, click Batch Update to enter the batch upgrading interface.



You can click to select a device or hold the Ctrl or Shift key to select multiple devices for simultaneously upgrading.

IP Address	Port	Device Serial No.	Version	Upgrade Status	Online Upgrade	Download State	Code
10.16.2.221	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	000000010000000100003000000003e80...
10.16.2.85	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	

Upgrade Mode: Upgrade by File Select Path: ... Upgrade

□ Restore Default Settings ☑ Reboot after Upgrading

Figure 8-38 Batch Upgrading

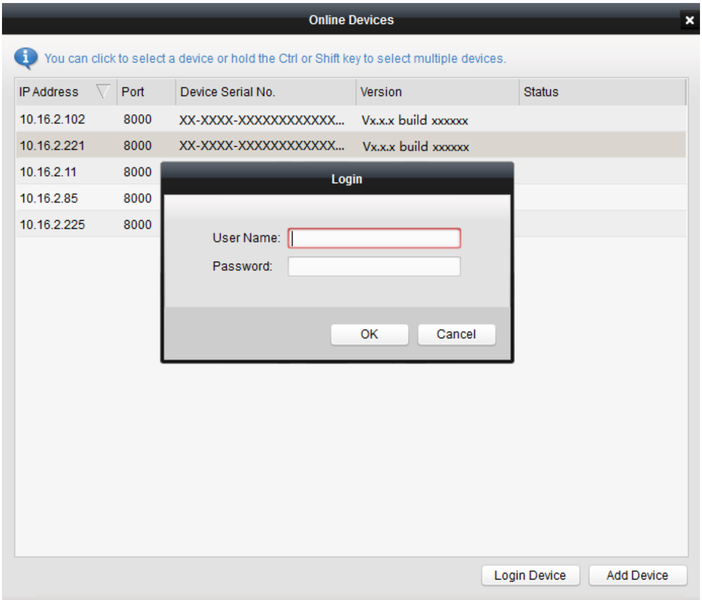
8.6.1 Adding Devices for Upgrading

You should add the device to the batch upgrading tool first before upgrading the device. There are 2 ways to add the device: adding online device, and adding by IP address/IP segment.

Adding Online Device

Steps:

1. In the batch upgrading interface, click the Online Devices to open the online device window.



You can click to select a device or hold the Ctrl or Shift key to select multiple devices.

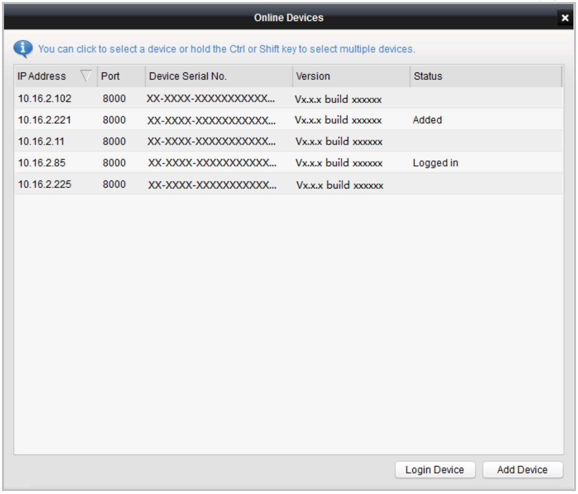
IP Address	Port	Device Serial No.	Version	Status
10.16.2.102	8000	XX-XXXX-XXXXXXXXXXXX...	Vx.x.x build xxxxxx	
10.16.2.221	8000	XX-XXXX-XXXXXXXXXXXX...	Vx.x.x build xxxxxx	
10.16.2.11	8000			
10.16.2.85	8000			
10.16.2.225	8000			

User Name:

Password:

Figure 8-39 Login

2. Select a device, enter the user name and password, and click the **Login Device** button.
3. Click the **Add Device** button, and the device is added to the batch upgrading tool.



You can click to select a device or hold the Ctrl or Shift key to select multiple devices.

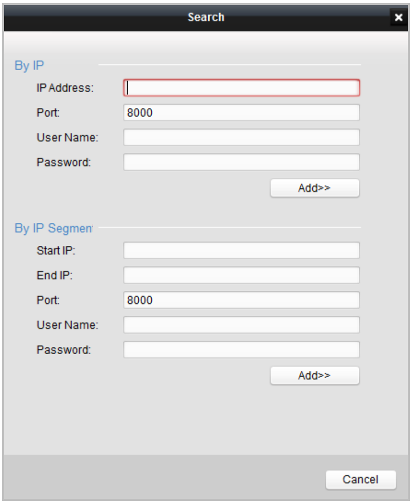
IP Address	Port	Device Serial No.	Version	Status
10.16.2.102	8000	XX-XXXX-XXXXXXXXXXX...	Vx.x.x build xxxxxx	
10.16.2.221	8000	XX-XXXX-XXXXXXXXXXX...	Vx.x.x build xxxxxx	Added
10.16.2.11	8000	XX-XXXX-XXXXXXXXXXX...	Vx.x.x build xxxxxx	
10.16.2.85	8000	XX-XXXX-XXXXXXXXXXX...	Vx.x.x build xxxxxx	Logged in
10.16.2.225	8000	XX-XXXX-XXXXXXXXXXX...	Vx.x.x build xxxxxx	

Figure 8-40 Online Devices

Adding by IP Address/IP Segment

Steps:

1. Click the **Manual** button to open the device adding window.
2. Enter the corresponding information (IP address, user name, password, start IP address, end IP address).
3. Click the **Add** button.



Search

By IP

IP Address:

Port: 8000

User Name:

Password:

Add>>

By IP Segmen

Start IP:

End IP:

Port: 8000

User Name:

Password:

Add>>

Cancel

Figure 8-41 Adding by IP Address/IP Segment

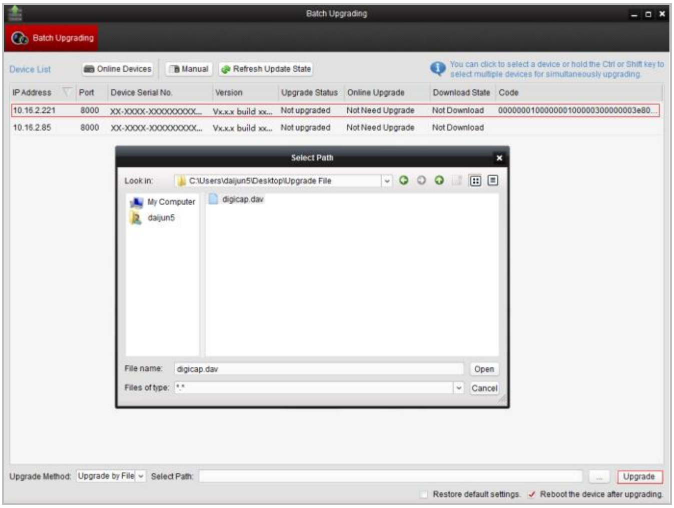
8.6.2 Upgrading Devices

Door station supports upgrading by file.

Upgrading by File: You upgrade the device or devices via the local upgrade files.

Steps:

1. Select a device or multiple devices, and select “Upgrade by File” as the upgrading mode.
2. Click ··· to pop up the window for opening the upgrading file.



You can click to select a device or hold the Ctrl or Shift key to select multiple devices for simultaneously upgrading.

IP Address	Port	Device Serial No.	Version	Upgrade Status	Online Upgrade	Download State	Code
10.16.2.221	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	000000010000000100000300000003e80...
10.16.2.85	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	

Look in: C:\Users\daijun5\Desktop\Upgrade File

File name: digicap.dav

Files of type: *.*

Upgrade Method: Upgrade by File

Select Path:

□ Restore default settings. ✓ Reboot the device after upgrading.

Figure 8-42 Upgrade by File

3. Open the upgrading file, and click the **Upgrade** button.

9 Remote Operation via iVMS-4200 Client Software

The Video Intercom module provides remote control and configuration on video intercom products via the iVMS-4200 client software.

Before remote configure and control the video intercom, you are required to add the device to the software first. Refer to *9.2 Device Management.*

For remote configuration of video intercom device via the iVMS-4200 client software, refer to *9.3 Configuring Devices Remotely via iVMS-4200.*

For the picture storage on storage server, refer to *9.4 Picture Storage.*

For remote control of video intercom devices, please refer to *9.6 Video Intercom Configuration*.

9.1 System Configuration

Purpose:

You can configure the video intercom parameters accordingly.

Steps:

1. Open the System Configuration page.

   Path: **Control Panel -> Maintenance and Management -> System Configuration -> Video Intercom**.
2. Click the **Video Intercom** tab to enter the Video Intercom Settings interface.
3. Input the required information.

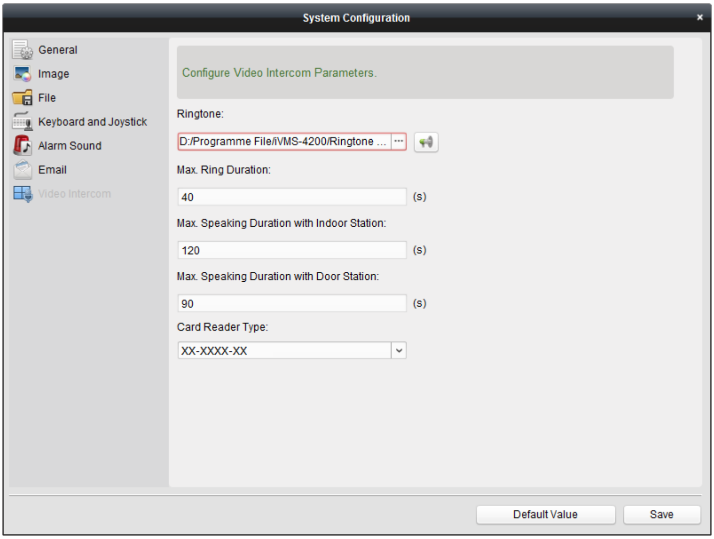
   Ringtone: Click the icon ··· and select the audio file from the local path for the ringtone of indoor station. Optionally, you can click the icon 🔊 for a testing of the audio file.

   Max. Ring Duration: Input the maximum duration of the ringtone, ranging from 15 seconds to 60 seconds.

   Max. Speaking Duration with Indoor Station: Input the maximum duration of speaking with the indoor station, ranging from 120 seconds to 600 seconds.

   Max. Speaking Duration with Door Station: Input the maximum duration of speaking with the door station, ranging from 90 seconds to 120 seconds.

   Card Reader Type: Select the card reader to issue cards.
4. Click **Save** to save the settings.



Configure Video Intercom Parameters.

Ringtone: D:/Programme File/iVMS-4200/Ringtone ...

Max. Ring Duration: 40 (s)

Max. Speaking Duration with Indoor Station: 120 (s)

Max. Speaking Duration with Door Station: 90 (s)

Card Reader Type: XX-XXXX-XX

Figure 9-2 System Configuration Interface

9.2 Device Management

Purpose:

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

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

9.2.1 Adding Video Intercom Devices

NOTE

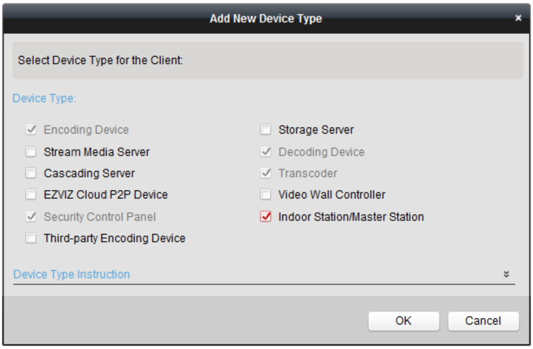
- You can add at most 512 indoor stations and master stations in total to the iVMS-4200, and add at most 16 door stations to the iVMS-4200.
- For video intercom devices, you are required to create the password to activate them before they can be added to the software and work properly. For device activation via creating password, please refer *User Manual of iVMS-4200 (Video Intercom) V2.4.2* in the disk for detail steps.
- You can add online video intercom devices, and add them manually. Here take adding online video intercom devices as example. For adding video intercom devices manually, please refer *User Manual of iVMS-4200 (Video Intercom) V2.4.2* in the disk for detail steps.

Steps:

1. Click the icon on the control panel, or click **Tools->Device Management** to open the Device Management page.
2. Click the **Server** tab.

To add indoor station or master station:

1) Click **Add New Device Type** to enter add new device type interface. Select **Indoor Station/Master Station** and click **OK**.



Add New Device Type

Select Device Type for the Client:

Device Type:

- ☑ Encoding Device
- ☐ Stream Media Server
- ☐ Cascading Server
- ☐ EZVIZ Cloud P2P Device
- ☑ Security Control Panel
- ☐ Third-party Encoding Device
- ☐ Storage Server
- ☑ Decoding Device
- ☑ Transcoder
- ☐ Video Wall Controller
- ☑ Indoor Station/Master Station

Device Type Instruction

OK | Cancel

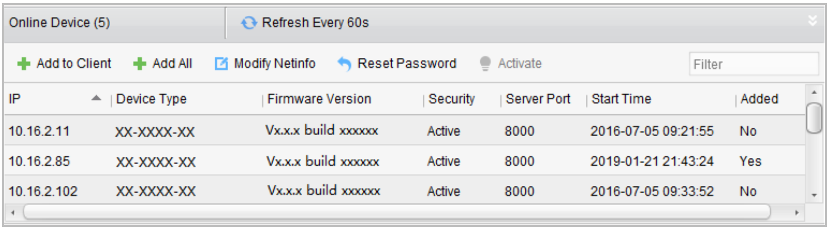
Figure 9-3 Adding New Device Type

2) In the Server tab, Video Intercom Device will display, select **Video Intercom Device** and add indoor station and master station.

To add door station:

In the Server tab, select **Encoding Device/Outdoor Device** and add door station.

3. The active online devices in the same local subnet with the client software will be displayed on the **Online Device** area. You can click the **Refresh Every 60s** button to refresh the information of the online devices.



Online Device (5) | Refresh Every 60s

Add to Client | Add All | Modify Netinfo | Reset Password | Activate | Filter

IP	Device Type	Firmware Version	Security	Server Port	Start Time	Added
10.16.2.11	XX-XXXX-XX	Vx.x.x build xxxxxx	Active	8000	2016-07-05 09:21:55	No
10.16.2.85	XX-XXXX-XX	Vx.x.x build xxxxxx	Active	8000	2019-01-21 21:43:24	Yes
10.16.2.102	XX-XXXX-XX	Vx.x.x build xxxxxx	Active	8000	2016-07-05 09:33:52	No

Figure 9-4 Online Device

- To add online devices to the software, you are required to change the device IP address to the same subnet with your computer first.

4. Select the devices to be added from the list.
5. Click **Add to Client** to open the device adding dialog box.
6. Input the required information.

   Nickname: Edit a name for the device as you want.

   Address: Input the device's IP address. The IP address of the device is obtained automatically in this adding mode.

   Port: Input the device port No.. The default value is 8000.

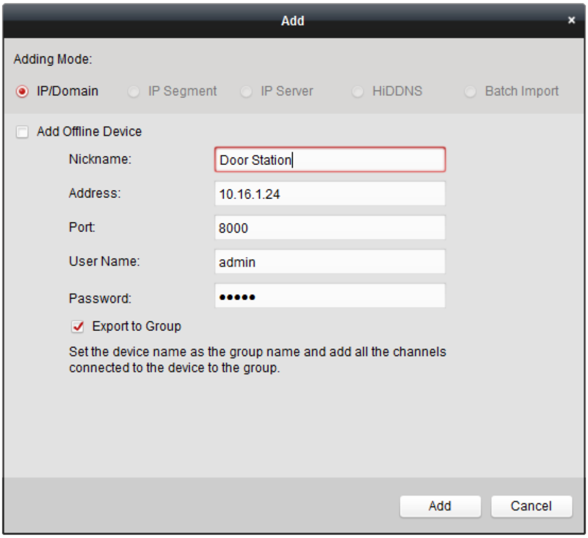
   User Name: Input the device user name. By default, the user name is admin.

   Password: Input the device password. By default, the password is 12345.
7. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

NOTE

- iVMS-4200 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.

8. Click **Add** to add the device.



Nickname: Door Station

Address: 10.16.1.24

Port: 8000

User Name: admin

Password: •••••

☑ Export to Group

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

Figure 9-5 Adding Device by IP/Domain

NOTE

Add Multiple Online Devices

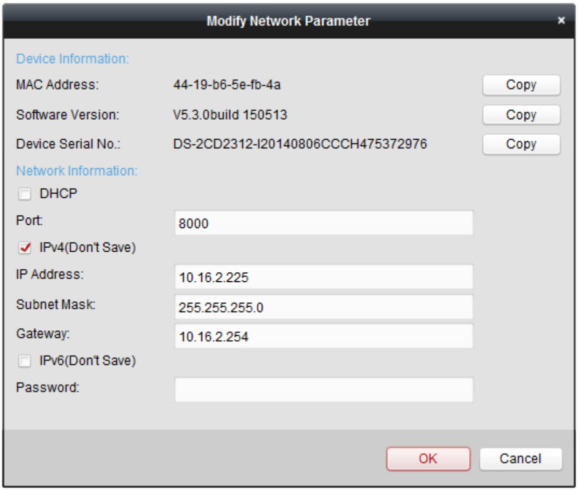
If you want to add multiple online devices to the client software, click and hold Ctrl key to select multiple devices, and click **Add to Client** to open the device adding dialog box. In the pop-up message box, enter the user name and password for the devices to be added.

Add All the Online Devices

If you want to add all the online devices to the client software, click Add All and click **OK** in the pop-up message box. Then enter the user name and password for the devices to be added.

9.2.2 Modifying Network Information

Select the device from the online list, click **Modify Netinfo**, and then you can modify the network information of the selected device.



Device Information:

MAC Address: 44-19-b6-5e-fb-4a

Software Version: V5.3.0build 150513

Device Serial No.: DS-2CD2312-I20140806CCCH475372976

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Don't Save)

IP Address: 10.16.2.225

Subnet Mask: 255.255.255.0

Gateway: 10.16.2.254

□ IPv6(Don't Save)

Password:

Figure 9-6 Modifying Network Parameter

You should enter the admin password of the device in the **Password** field of the pop-up window to modify the parameters.

9.2.3 Resetting Password

According to the different video intercom devices, the software provides two different methods for restoring the default password or resetting the password.

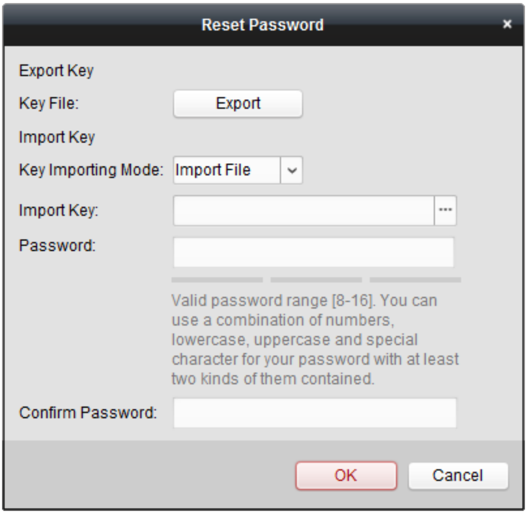
Select the device from the online device list, click **Reset Password**.

Option 1:

If the window with import file button, key importing mode drop-down list, password and confirm password field pops up, follow the steps below to reset the password:

NOTE

This option is available to door stations.



Reset Password

Export Key

Key File:

Import Key

Key Importing Mode: Import File

Import Key:

Password:

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm Password:

Figure 9-7 Resetting Password (Option 1)

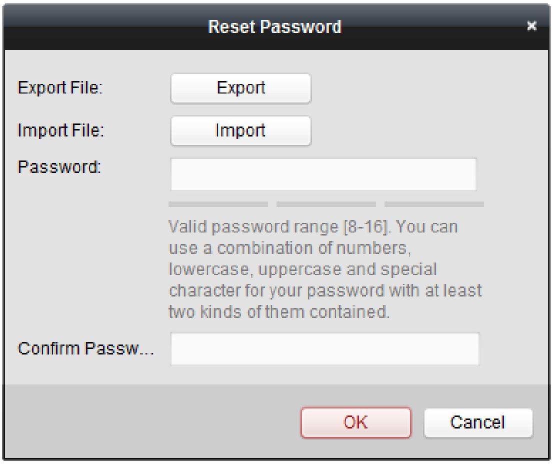
1. Click **Export** to save the device file on your computer.
2. Send the file to our technical engineers.
3. Our technical engineer will send you a file to you. After receiving a file from the technical engineer, select **Import File** from Key Importing Mode drop-down list and click ··· to import the file.
4. Input new password in text fields of **Password** and **Confirm Password**.
5. Click **OK** to reset the password.

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.*

Option 2:

If the window with import file and export file buttons, password and confirm password field pops up, follow the steps below to reset the password:

Note: This option is available to indoor stations and master stations.



Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Figure 9-8 Resetting Password (Option 2)

1. Click **Export** to save the device file on your computer.
2. Send the file to our technical engineers.
3. Click **Import** and select the file received from the technical engineer.
4. Input new password in text fields of **Password** and **Confirm Password**.
5. Click **OK** to reset the password.

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.*

9.3 Configuring Devices Remotely via iVMS-4200

Configuring devices remotely via iVMS-4200 is the same with that via Batch Configuration Tool, please refer *8.4 Configuring Devices Remotely* for detail steps.

9.4 Picture Storage

When the video intercom 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.

When starting the live view of door station via iVMS-4200, you can capture the live view picture. The captured picture can be uploaded and stored in the storage server.

NOTE

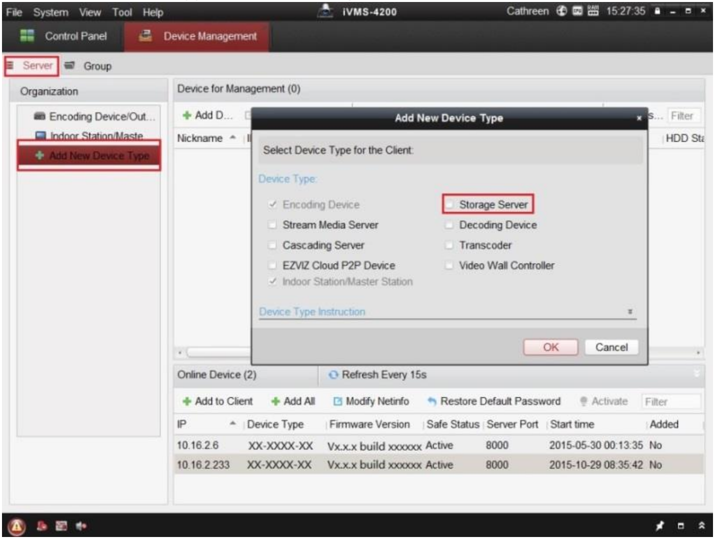
- This function is only available to door stations.
- You are required to add storage server to the iVMS-4200, and format the HDDs first before uploading and storing captured pictures.

9.4.1 Adding 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 of **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**.



IP	Device Type	Firmware Version	Safe Status	Server Port	Start time	Added
10.16.2.6	XX-XXXX-XX	Vx.x.x build xxxxxx	Active	8000	2015-05-30 00:13:35	No
10.16.2.233	XX-XXXX-XX	Vx.x.x build xxxxxx	Active	8000	2015-10-29 08:35:42	No

Figure 9-9 Adding Storage Server Type

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

NOTE

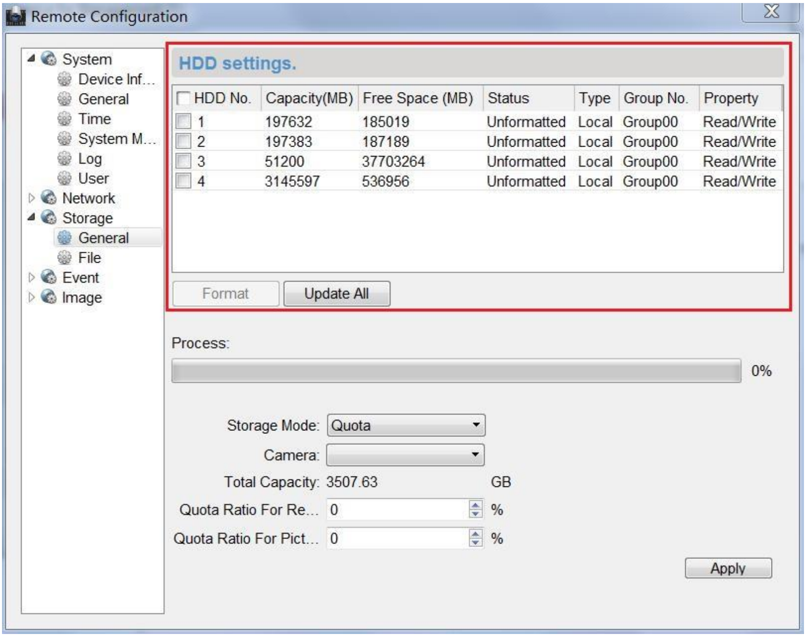
For adding the storage server, please refer to *User Manual of iVMS-4200 (Video Intercom) V2.4.2* in the disk.

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*.



☐ HDD No.	Capacity(MB)	Free Space (MB)	Status	Type	Group No.	Property
☐ 1	197632	185019	Unformatted	Local	Group00	Read/Write
☐ 2	197383	187189	Unformatted	Local	Group00	Read/Write
☐ 3	51200	37703264	Unformatted	Local	Group00	Read/Write
☐ 4	3145597	536956	Unformatted	Local	Group00	Read/Write

Process: 0%

Storage Mode: Quota

Camera:

Total Capacity: 3507.63 GB

Quota Ratio For Re... 0 %

Quota Ratio For Pict... 0 %

Figure 9-10 Formatting HDDs

NOTE

Formatting the HDDs is to pre-allocate the disk space for storage and the original data of the formatted HDDs will be deleted.

9.4.3 Configuring Storage Server Picture Storage

Before you start:

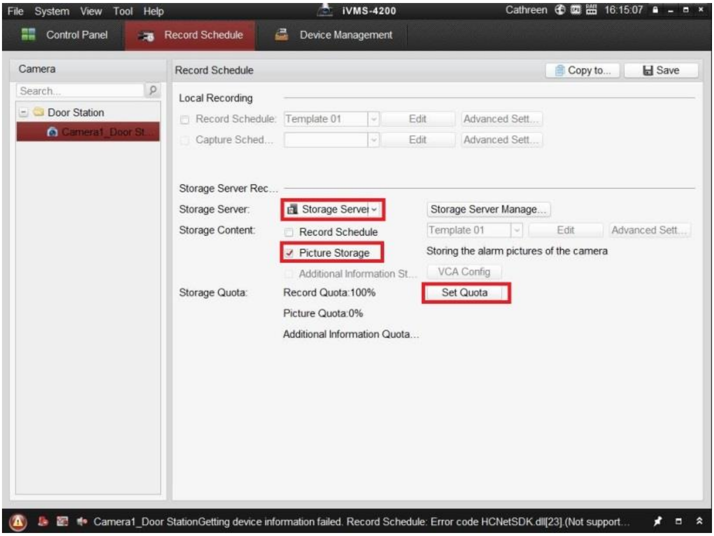
The storage server needs to be added to the client software and the HDDs need to be formatted for the captured pictures storage.

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.

   NOTE

   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.



☐ Record Schedule: Template 01 Edit Advanced Sett...

☐ Capture Sched... Edit Advanced Sett...

Storage Server: Storage Server

Storage Content: ☐ Record Schedule Template 01 Edit Advanced Sett...

☑ Picture Storage Storing the alarm pictures of the camera

☐ Additional Information St...

Storage Quota: Record Quota:100%

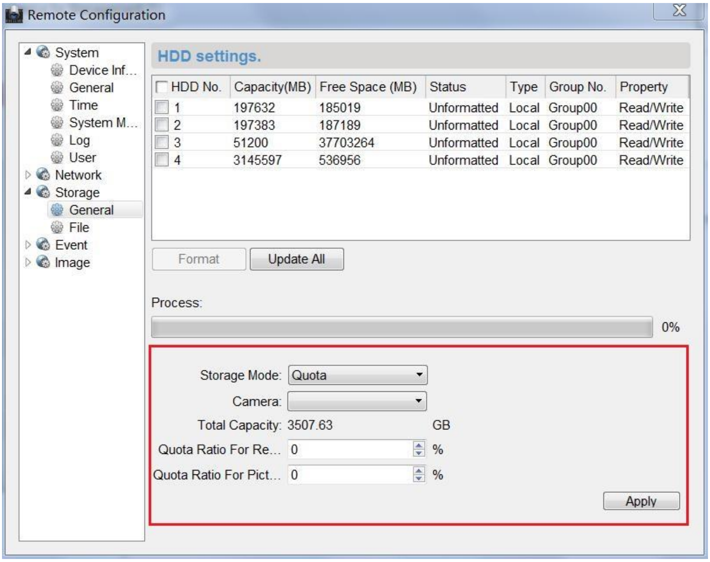
Picture Quota:0%

Additional Information Quota...

Camera1_Door StationGetting device information failed. Record Schedule: Error code HCNetSDK.dll[23].(Not support...

Figure 9-11 Setting Storage Server

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.



HDD No.	Capacity(MB)	Free Space (MB)	Status	Type	Group No.	Property
□ 1	197632	185019	Unformatted	Local	Group00	Read/Write
□ 2	197383	187189	Unformatted	Local	Group00	Read/Write
□ 3	51200	37703264	Unformatted	Local	Group00	Read/Write
□ 4	3145597	536956	Unformatted	Local	Group00	Read/Write

Process: 0%

Storage Mode: Quota

Camera:

Total Capacity: 3507.63 GB

Quota Ratio For Re... 0 %

Quota Ratio For Pict... 0 %

Figure 9-12 Setting Quota

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 Live View

Steps:

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

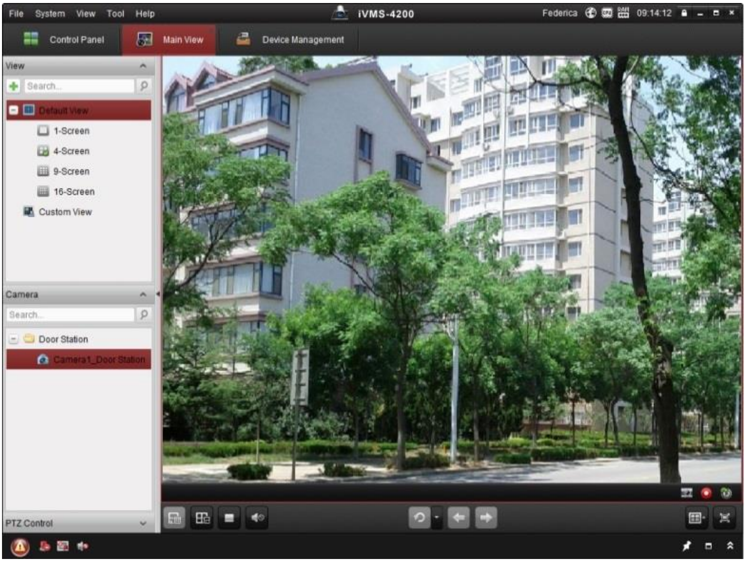


Figure 9-13 Live View of Doo Station (D Series)

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

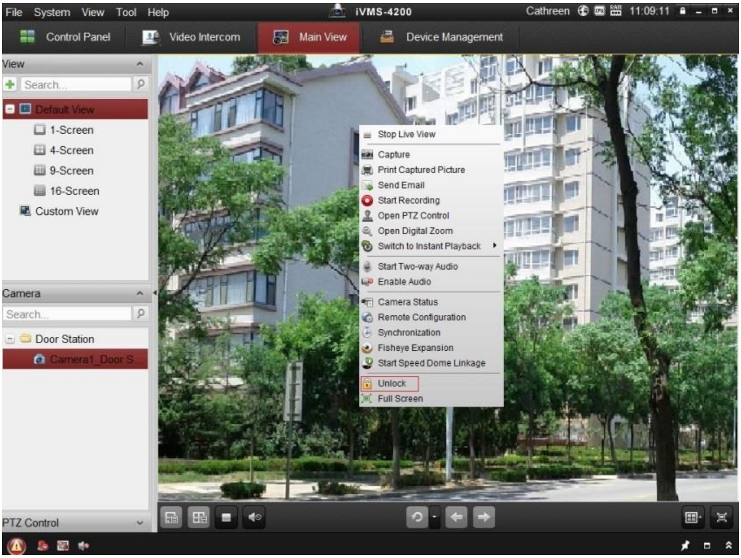


Figure 9-14 Menu of Live View Interface

9.6 Video Intercom Configuration

Click the icon on the control panel of iVMS-4200 or click **View -> Video Intercom** to open the Video Intercom page. On the Video Intercom page, you can control video intercom devices remotely. There are 4 modules on the Video Intercom page:

Video Intercom: Start visual communication with door stations, and manage incoming calls from indoor stations and door stations and master stations. Refer *9.6.2 Video Intercom* for detail steps.

Group Management: Construct virtual communities according to the real community situations, and assign door stations and indoor stations to the community accordingly. Refer *9.6.1 Group Management* for detail steps.

NOTE

You should manage groups first before starting the visual communication with indoor stations or door stations.

Card Management: Add unauthorized cards to the iVMS-4200, and issue card to the door station via the iVMS-4200. Refer *9.6.2 Video Intercom*

Receiving Call from Door Station

Purpose:

When the door station has been added to the client software, you can call the client via door station.

Before you start:

- Make sure the door station has been added to the client software.
- Make sure the SIP server IP address of the door station is not configured (or abnormal).

Steps:

Press **Calling Center** key on the door station.

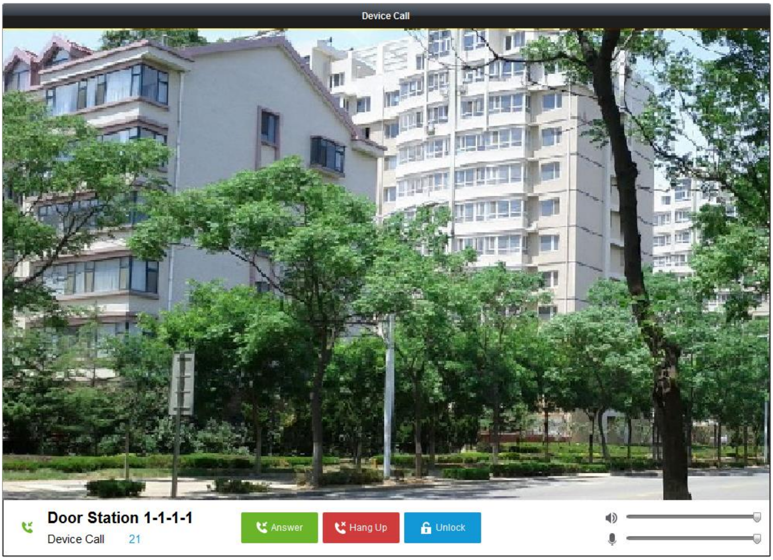


Figure 9-15 Calling from Door Station

NOTE

- When the SIP server IP of the door station is configured, press **Calling Center** key on the door station to call the master station instead of the client software.
- Click **Unlock** to unlock the building or villa door via the client software, no matter whether answering the call from door station or not.
- Click **Answer** to answer the call from door station.
- Click **Hang Up** to end the call from door station.

Call Log

On the Video Intercom tab page, there are four types of call logs you can search: **All**, **Dialed**, **Received**, and **Missed**.

On the dial log area, you can view detail information of the dialog, and click **Call** to start the audiovisual call with the indoor station.

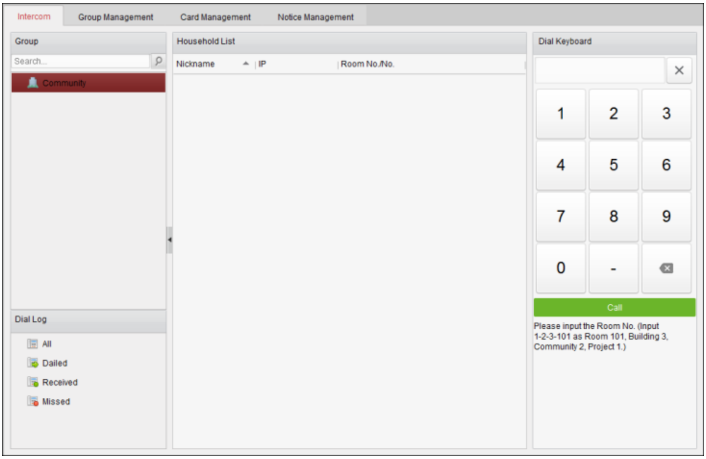
Click Clear Log to clear all logs in the list (optional).

Card Management for detail steps.

NOTE

Once you issue cards via the iVMS-4200, the card issuing function of the corresponding door station will be disabled automatically.

Notice Management: Send information to indoor stations, search information, search call logs, and search unlocking logs. Refer *9.6.4 Notice Management* for detail steps.



Please input the Room No. (Input 1-2-3-101 as Room 101, Building 3, Community 2, Project 1.)

Figure 9-16 Intercom Interface

9.6.1 Group Management

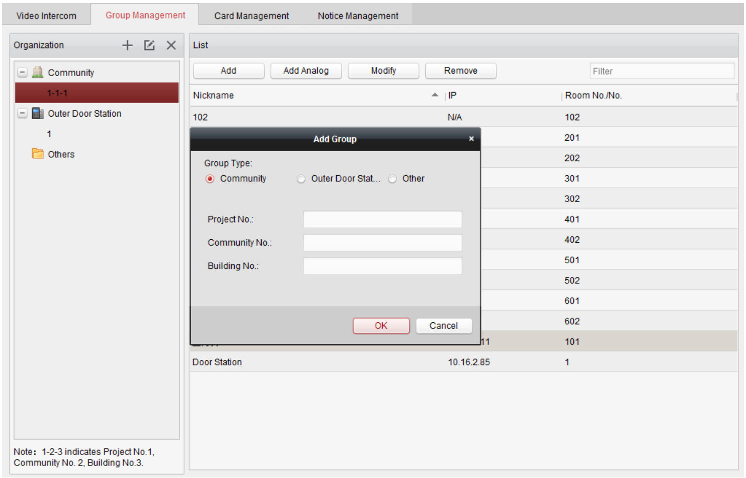
Purpose:

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

Enter **Control Panel -> Video Intercom -> Group Management** to add, edit, and delete groups. Three group types can be selected: community, outer door station and other.

Adding Group

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



Group Type: ● Community ○ Outer Door Stat... ○ Other

Project No.:

Community No.:

Building No.:

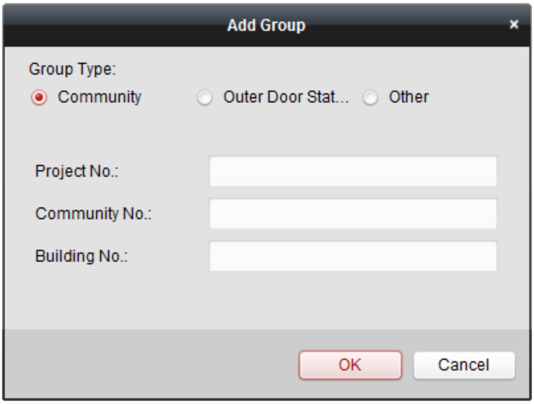
Nickname	IP	Room No./No.
102	N/A	102
		201
		202
		301
		302
		401
		402
		501
		502
		601
		602
	11	101
Door Station	10.16.2.85	1

Note：1-2-3 indicates Project No.1, Community No. 2, Building No.3.

Figure 9-17 Adding Group

2. Click + to pop up group adding window, and input the corresponding information accordingly.

- Select **Community** as group type, and then Input the Community No., building No., and Unit No. to set the community structure, as shown in the figure below.



Group Type: ● Community ○ Outer Door Stat... ○ Other

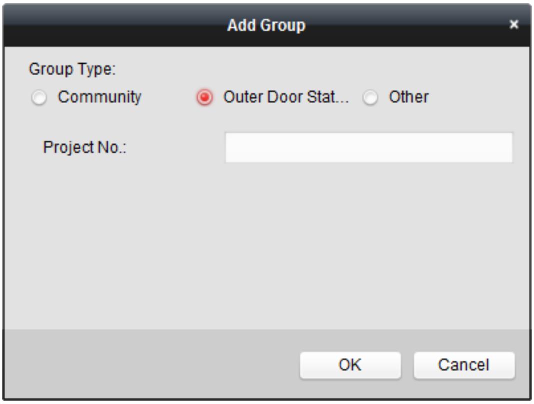
Project No.:

Community No.:

Building No.:

Figure 9-18 Adding Community

- Select **Outer Door Station** as group type, and then input the outer door station No. (Range: 1 to 9) to set the outer door station, as shown in the figure below.



Add Group

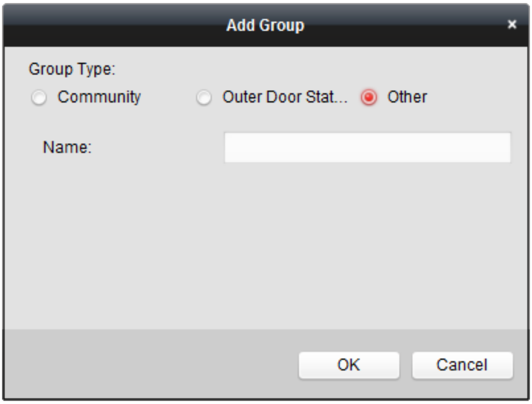
Group Type:

○ Community ● Outer Door Stat... ○ Other

Project No.:

Figure 9-19 Adding Outer Door Station

- Select **Other** as group type, and then input the group name.



Add Group

Group Type:

○ Community ○ Outer Door Stat... ● Other

Name:

Figure 9-20 Adding Other

For example: You can name the group as administrator, entrance guard and cleaning staff, etc.

NOTE

When selecting **Other** as the group type, you can set different groups for staff other than residents, such as administrator, security guard and cleaning staff, etc., and you can assign cards to these staff and configure different permissions to them.

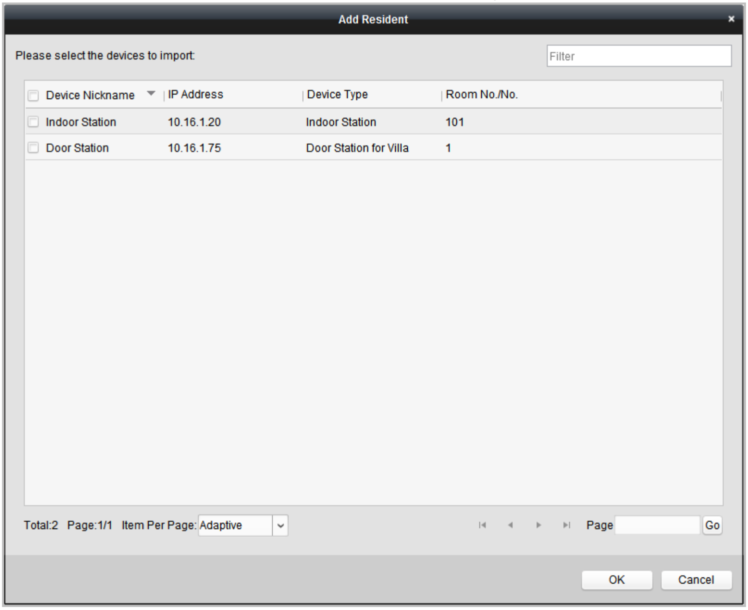
3. Click **OK** to complete group adding.

Assigning IP Devices to Group

After adding groups to Community, Outer Door Station, or Other, you should assign devices to the group.

For example: You should assign indoor stations and door stations to the group 1-1-1 in Community.

1. Click **Add** to enter the Add Resident Interface and the video intercom devices added to the client software will be listed, as shown in the figure below.



Please select the devices to import:

□ Device Nickname	IP Address	Device Type	Room No./No.
□ Indoor Station	10.16.1.20	Indoor Station	101
□ Door Station	10.16.1.75	Door Station for Villa	1

Total:2 Page:1/1 Item Per Page: Adaptive

Figure 9-21 Adding Resident

2. Check the checkbox of device.

   Indoor Station: set a Room No. for the indoor station.

   Door Station: set a No. for the door station.

3. Click **OK** to save the settings.

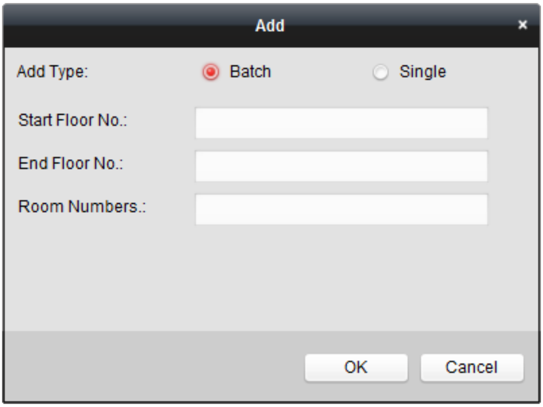
Assigning Analog Devices to Group

NOTE

When assigning analog devices to group, only analog indoor stations are supported.

1. Click **Add Analog** to pop up analog device adding window. You can add analog devices singly or in batch.

- Adding Devices in Batch: Enter the start floor and end floor, and set the room numbers.



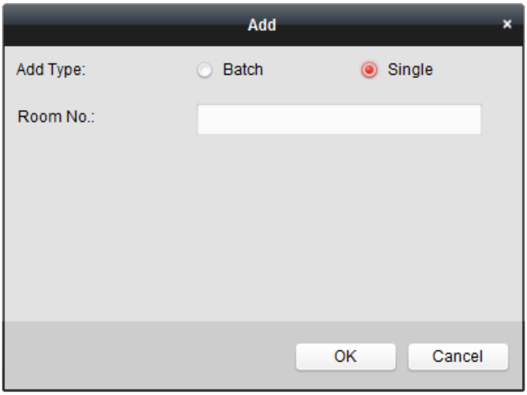
Add Type: ● Batch ○ Single

Figure 9-22 Adding Devices in Batch

NOTE

Room Numbers here refers to the room numbers in each floor.

- Adding Devices Singlly: Enter the room No..



Add Type: ○ Batch ● Single

Figure 9-23 Adding Device Singly

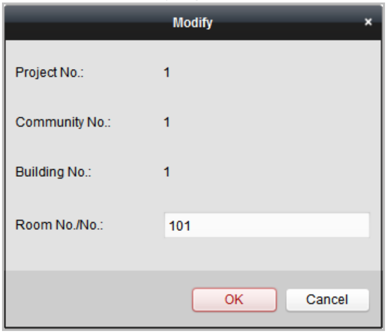
NOTE

The room No. format is like 101.

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

Modifying Device Information

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



Modify

Project No.: 1

Community No.: 1

Building No.: 1

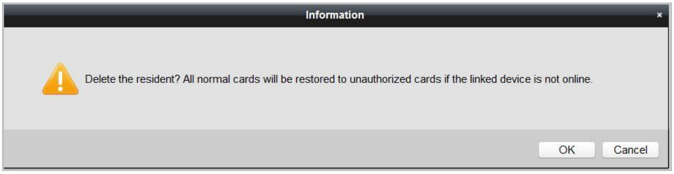
Room No./No.: 101

Figure 9-24 Modifying Device Information

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

Deleting Device

1. Select an added device.
2. Click **Remove** to pop up a dialog box.



Information

Delete the resident? All normal cards will be restored to unauthorized cards if the linked device is not online.

Figure 9-25 Information

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

9.6.2 Video Intercom

Receiving Call from Door Station

Purpose:

When the door station has been added to the client software, you can call the client via door station.

Before you start:

- Make sure the door station has been added to the client software.

- Make sure the SIP server IP address of the door station is not configured (or abnormal).

Steps:

Press **Calling Center** key on the door station.

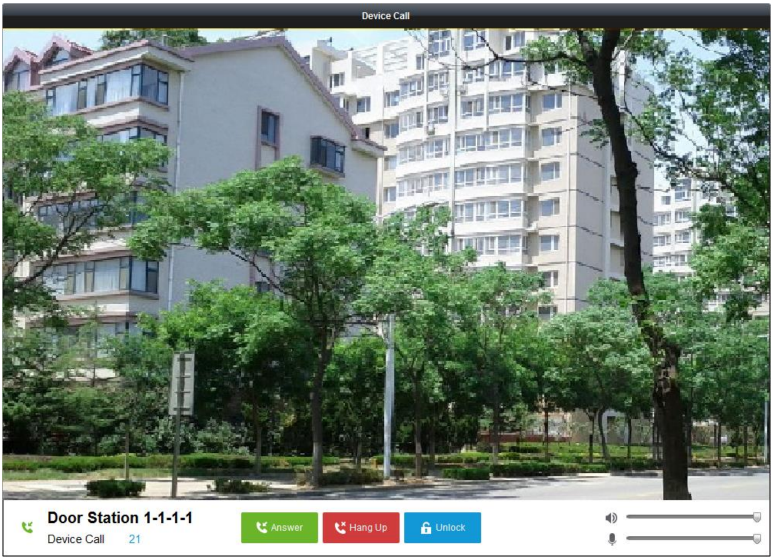


Figure 9-26 Calling from Door Station

NOTE

- When the SIP server IP of the door station is configured, press **Calling Center** key on the door station to call the master station instead of the client software.
- Click **Unlock** to unlock the building or villa door via the client software, no matter whether answering the call from door station or not.
- Click **Answer** to answer the call from door station.
- Click **Hang Up** to end the call from door station.

Call Log

On the Video Intercom tab page, there are four types of call logs you can search: **All**, **Dialed**, **Received**, and **Missed**.

On the dial log area, you can view detail information of the dialog, and click **Call** to start the audiovisual call with the indoor station.

Click Clear Log to clear all logs in the list (optional).

9.6.3 Card Management

Purpose:

You can add unauthorized cards to the community and then you can assign the cards to the corresponding indoor station and door 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 multiple cards, and you can assign these cards to the door station in the same building.

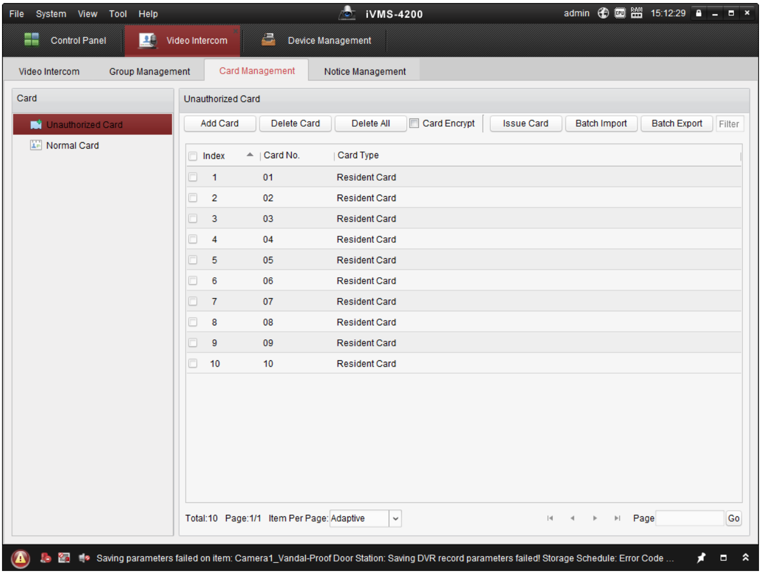
Note: Indoor extension does not support **Card Management**.

Before you start:

Make sure the indoor station and door station have been added to the iVMS-4200 client software.

Steps:

Click **Video Intercom -> Card Management** to enter the card management page.



□ Index	Card No.	Card Type
□ 1	01	Resident Card
□ 2	02	Resident Card
□ 3	03	Resident Card
□ 4	04	Resident Card
□ 5	05	Resident Card
□ 6	06	Resident Card
□ 7	07	Resident Card
□ 8	08	Resident Card
□ 9	09	Resident Card
□ 10	10	Resident Card

Total:10 Page:1/1 Item Per Page: Adaptive

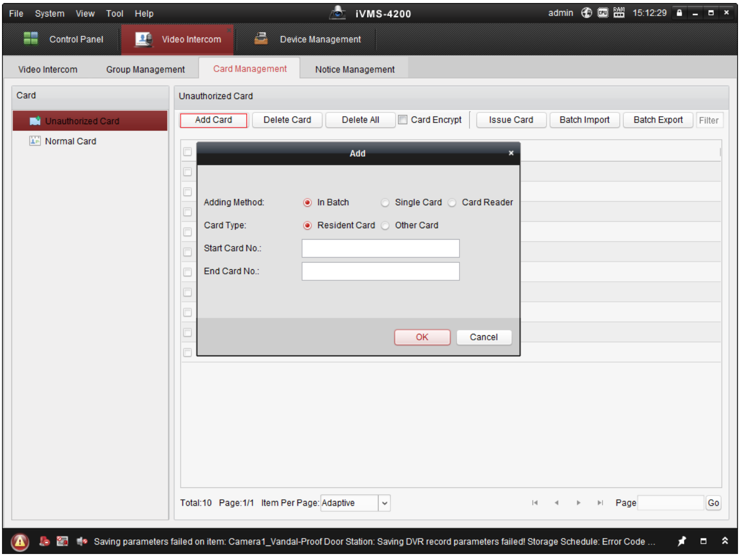
Saving parameters failed on item: Camera1_Vandal-Proof Door Station: Saving DVR record parameters failed! Storage Schedule: Error Code ...

Figure 9-27 Card Management Interface

Adding Card

Steps:

1. Click **Unauthorized Card -> Add Card** to pop up card adding window.



Adding Method: ● In Batch ○ Single Card ○ Card Reader

Card Type: ● Resident Card ○ Other Card

Start Card No.:

End Card No.:

Total:10 Page:1/1 Item Per Page: Adaptive

Saving parameters failed on item: Camera1_Vandal-Proof Door Station: Saving DVR record parameters failed! Storage Schedule: Error Code ...

Figure 9-28 Adding Cards in Batch

2. Select card adding mode and card type.

NOTE

Two types of card are available. Resident Card is used by residents living in the community, and Other Card is used by visitors (guest, serviceman, etc.) in the community.

- If you add card in batch, please set the start card No. and the end card No..
- If you add card singly, please enter the card No..
- If you add card via card reader, please swipe the card in the card reader, and the corresponding card No. will be shown automatically in the Card No. textbox.

3. Click **OK** to accomplish carding adding operation.

NOTE

- Click **Delete All** to delete all cards added in iVMS-4200.
- Select one or multiple cards, and click **Delete Card** to delete selected cards added in iVMS-4200.
- **Card Encrypt** is only available to cards added via card reader. Enabling Card Encrypt can improve the card security to prevent it from being copied. But the same time, the default key of all the available sectors of the card is modified.

Issuing Card

Click **Issue Card** to pop up card issuing window.

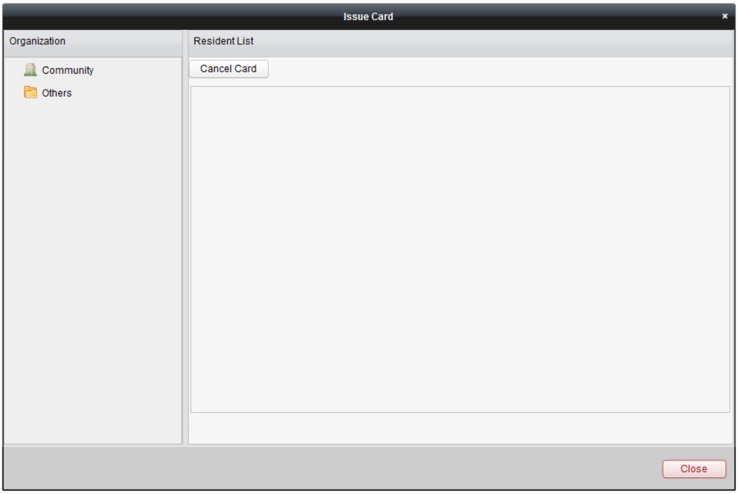
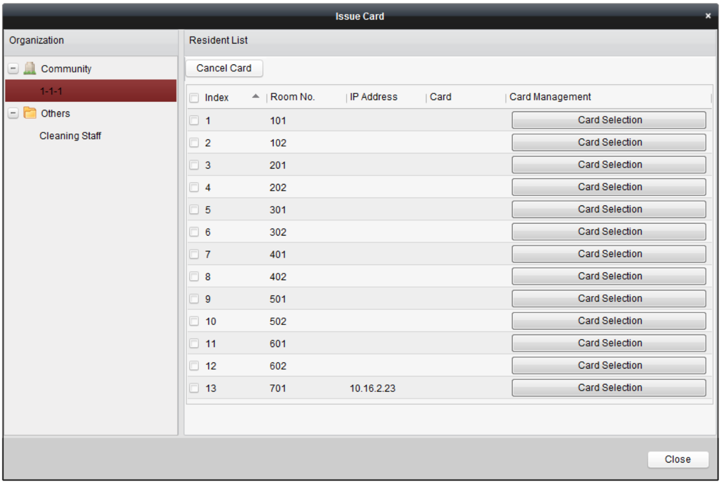


Figure 9-29 Issuing Card

Issuing Resident Cards

Steps:

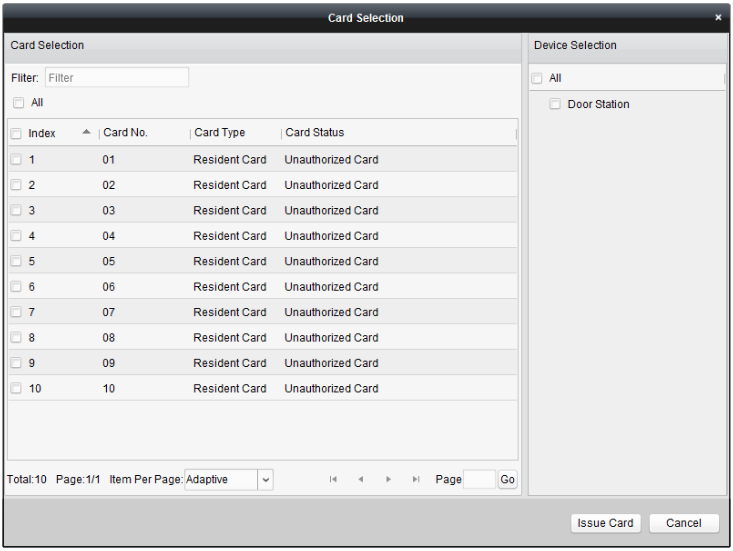
1. Select **Community** from the organization list (like 1-1-1) and the indoor stations of the community will be listed in the resident list.



Index	Room No.	IP Address	Card	Card Management
□ 1	101			Card Selection
□ 2	102			Card Selection
□ 3	201			Card Selection
□ 4	202			Card Selection
□ 5	301			Card Selection
□ 6	302			Card Selection
□ 7	401			Card Selection
□ 8	402			Card Selection
□ 9	501			Card Selection
□ 10	502			Card Selection
□ 11	601			Card Selection
□ 12	602			Card Selection
□ 13	701	10.16.2.23		Card Selection

Figure 9-30 Clicking Card Selection

2. Click **Card Selection** to pop up card selection window where unauthorized resident cards are listed.



□ Index	Card No.	Card Type	Card Status
□ 1	01	Resident Card	Unauthorized Card
□ 2	02	Resident Card	Unauthorized Card
□ 3	03	Resident Card	Unauthorized Card
□ 4	04	Resident Card	Unauthorized Card
□ 5	05	Resident Card	Unauthorized Card
□ 6	06	Resident Card	Unauthorized Card
□ 7	07	Resident Card	Unauthorized Card
□ 8	08	Resident Card	Unauthorized Card
□ 9	09	Resident Card	Unauthorized Card
□ 10	10	Resident Card	Unauthorized Card

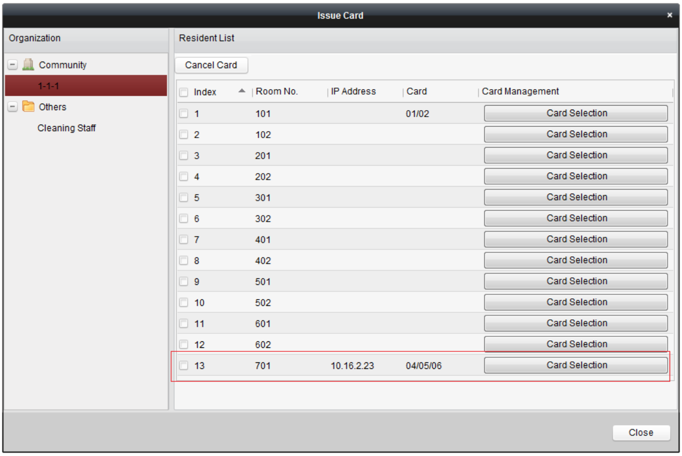
Figure 9-31 Selecting Cards

3. Check the checkboxes of the cards or enter the card No. in the filter textbox you need to assign to the indoor station, and check the checkbox of door stations, doorphones and outer door stations.

NOTE

Only resident cards can be assigned to indoor stations.

4. Click **Issue Card** to complete the card issuing operation.



□	Index	Room No.	IP Address	Card	Card Management
□	1	101		01/02	Card Selection
□	2	102			Card Selection
□	3	201			Card Selection
□	4	202			Card Selection
□	5	301			Card Selection
□	6	302			Card Selection
□	7	401			Card Selection
□	8	402			Card Selection
□	9	501			Card Selection
□	10	502			Card Selection
□	11	601			Card Selection
□	12	602			Card Selection
□	13	701	10.16.2.23	04/05/06	Card Selection

Figure 9-32 Displaying Card Issued

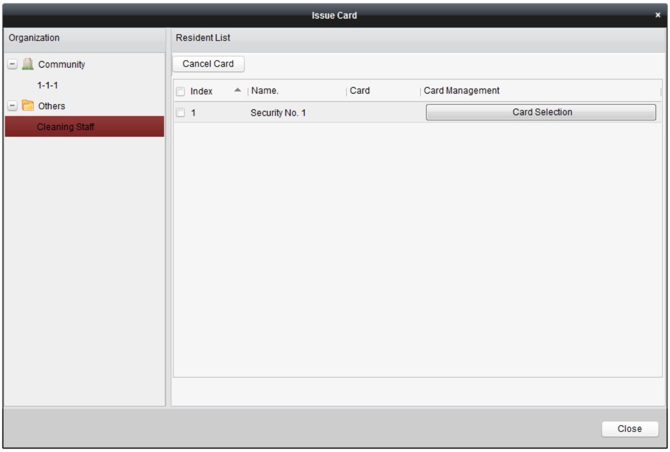
NOTE

After issuing resident cards to the indoor station, the card No. will also be listed in the resident list.

Issuing Other Cards

Steps:

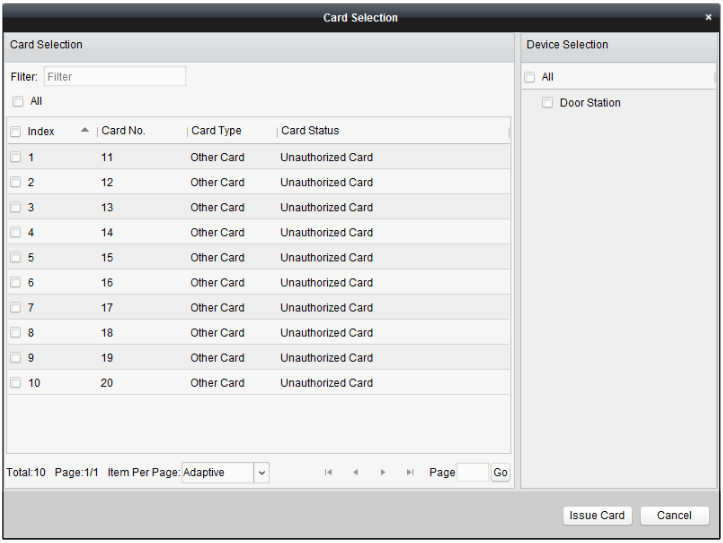
1. Select **Other** from the group list (like Cleaning Staff).



□	Index	Name.	Card	Card Management
□	1	Security No. 1		Card Selection

Figure 9-33 Issuing Other Card

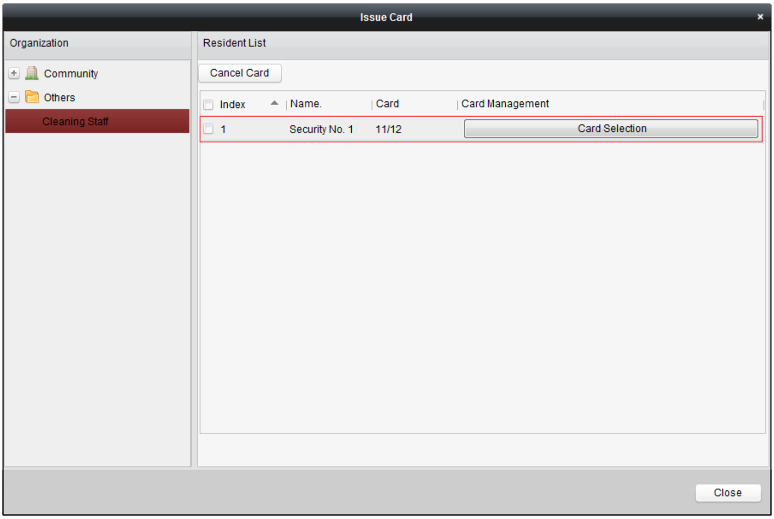
2. Click **Card Selection** to pop up card selection window where unauthorized other cards are listed.



□ Index	Card No.	Card Type	Card Status
□ 1	11	Other Card	Unauthorized Card
□ 2	12	Other Card	Unauthorized Card
□ 3	13	Other Card	Unauthorized Card
□ 4	14	Other Card	Unauthorized Card
□ 5	15	Other Card	Unauthorized Card
□ 6	16	Other Card	Unauthorized Card
□ 7	17	Other Card	Unauthorized Card
□ 8	18	Other Card	Unauthorized Card
□ 9	19	Other Card	Unauthorized Card
□ 10	20	Other Card	Unauthorized Card

Figure 9-34 Selecting Cards

3. Check the checkboxes of the cards or enter the card No. in the filter textbox you need to assign to the person, and check the checkbox of door stations, doorphones and outer door stations.
4. Click **Issue Card** to complete the card issuing operation.



□ Index	Name.	Card	Card Management
□ 1	Security No. 1	11/12	Card Selection

Figure 9-35 Displaying Card Issued

NOTE

After issuing other cards to the person, the card No. will also be listed in the resident list page.

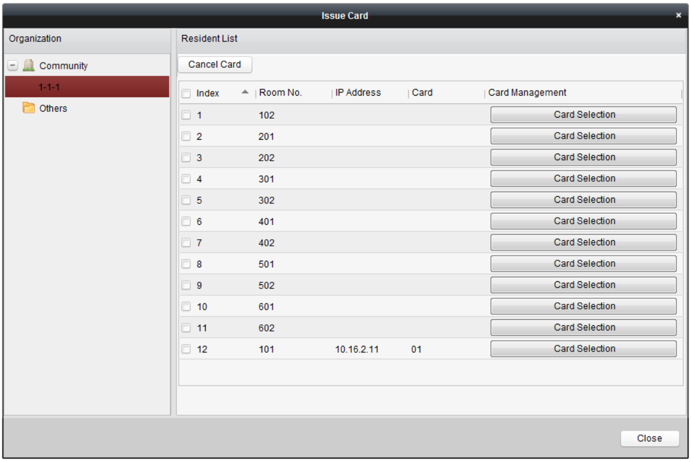
Canceling Cards

When canceling cards, cards that have been issued will be reset to authorized ones. Via iVMS-4200, there are two ways to cancel the cards which have been issued.

Option 1:

Steps:

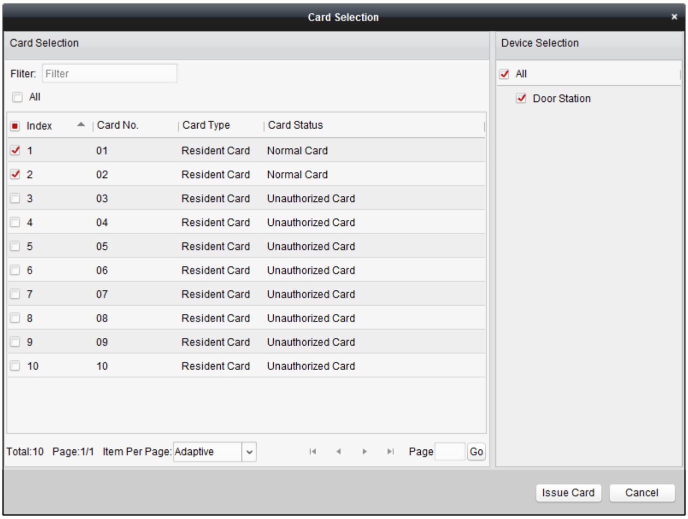
1. Select **Community** from the organization list (like 1-1-1) and the indoor stations of the community will be listed in the resident list.



☐ Index	Room No.	IP Address	Card	Card Management
☐ 1	102			Card Selection
☐ 2	201			Card Selection
☐ 3	202			Card Selection
☐ 4	301			Card Selection
☐ 5	302			Card Selection
☐ 6	401			Card Selection
☐ 7	402			Card Selection
☐ 8	501			Card Selection
☐ 9	502			Card Selection
☐ 10	601			Card Selection
☐ 11	602			Card Selection
☐ 12	101	10.16.2.11	01	Card Selection

Figure 9-36 Card Selection Interface

2. Click **Card Selection** to pop up card selection window where normal cards and unauthorized resident cards are listed.



Fliter: Filter

☐ All

■ Index	Card No.	Card Type	Card Status
☑ 1	01	Resident Card	Normal Card
☑ 2	02	Resident Card	Normal Card
☐ 3	03	Resident Card	Unauthorized Card
☐ 4	04	Resident Card	Unauthorized Card
☐ 5	05	Resident Card	Unauthorized Card
☐ 6	06	Resident Card	Unauthorized Card
☐ 7	07	Resident Card	Unauthorized Card
☐ 8	08	Resident Card	Unauthorized Card
☐ 9	09	Resident Card	Unauthorized Card
☐ 10	10	Resident Card	Unauthorized Card

Total:10 Page:1/1 Item Per Page: Adaptive Page Go

Figure 9-37 Selecting Cards

3. Check the checkboxes of the cards that has been issued (normal cards).
4. Click **Issue Card** to complete the card canceling operation.

Option 2:

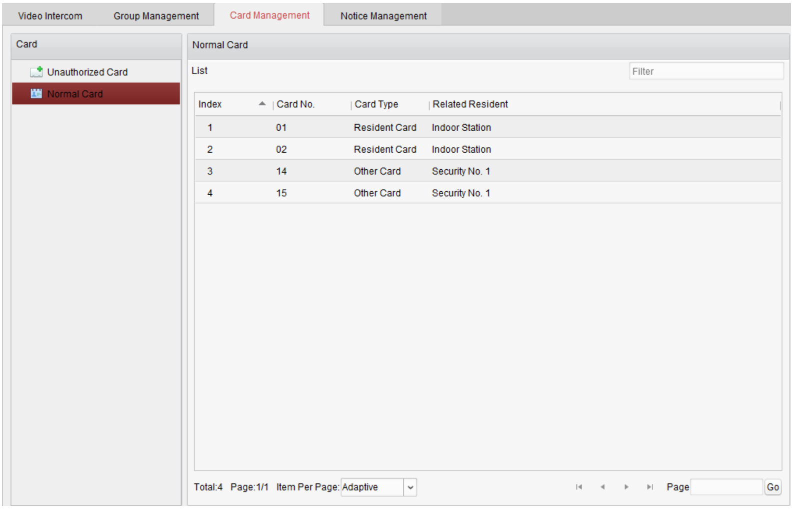
On the card issuing interface, check the checkboxes of Room No. (for resident card) or Name (for other card), click **Cancel Card** to cancel all card issued to the device.

NOTE

- Through Option 1, you can cancel card from single or certain door stations.
- Through Option 2, you will cancel all issued cards at a time.

Normal Card

Click **Normal Card** to display normal card list. After issuing cards, the issued cards will be listed in the normal card list, as shown in the figure below.



Index	Card No.	Card Type	Related Resident
1	01	Resident Card	Indoor Station
2	02	Resident Card	Indoor Station
3	14	Other Card	Security No. 1
4	15	Other Card	Security No. 1

Figure 9-38 Normal Cards Interface

Batch Importing Unauthorized Cards

Steps:

1. Click **Batch Import** to enter the batch import interface, as shown in the figure below.

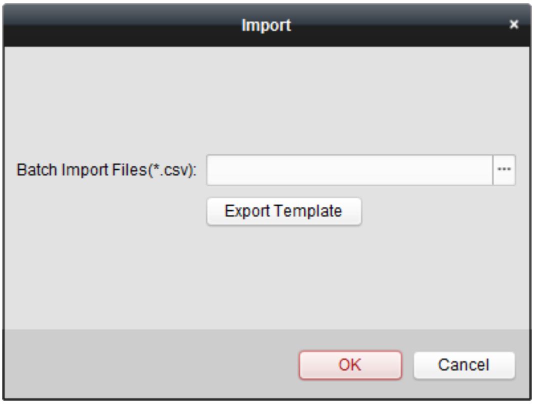


Figure 9-39 Importing File

2. Click **Export Template** to export the template of the batch import file.
3. Fill in the template of the batch import file and save it.
4. Click ··· to select the batch import file and click Open.
5. Click **OK** to start importing the batch import file.

Batch Exporting Unauthorized Cards

Steps:

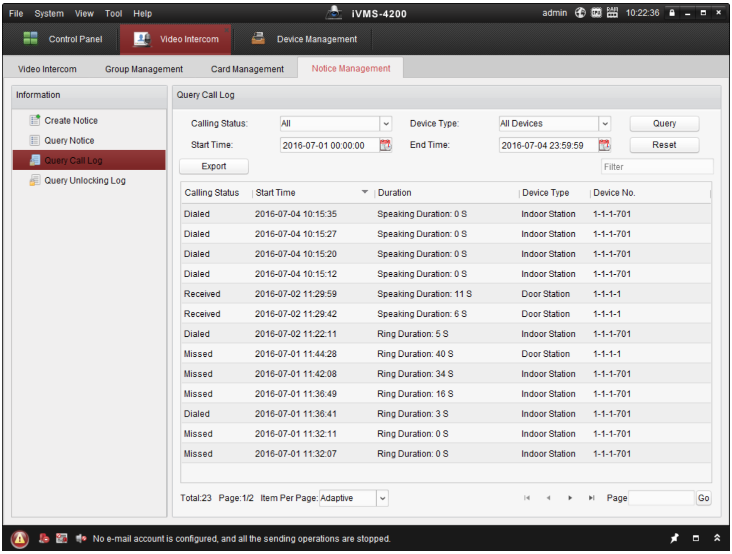
1. After adding unauthorized cards, and click **Batch Export**.
2. Select the saving file path and click **Save**.
3. After batch exporting the unauthorized cards, the excel will be generated in the saving directory.

9.6.4 Notice Management

Querying Call Logs

Steps:

1. Click **Query Call Logs** to enter the call log querying page.
2. Select the calling status, device type, and set the start time and end time, and click **Query** to search the call log.



Calling Status: All

Device Type: All Devices

Start Time: 2016-07-01 00:00:00

End Time: 2016-07-04 23:59:59

Calling Status	Start Time	Duration	Device Type	Device No.
Dialed	2016-07-04 10:15:35	Speaking Duration: 0 S	Indoor Station	1-1-1-701
Dialed	2016-07-04 10:15:27	Speaking Duration: 0 S	Indoor Station	1-1-1-701
Dialed	2016-07-04 10:15:20	Speaking Duration: 0 S	Indoor Station	1-1-1-701
Dialed	2016-07-04 10:15:12	Speaking Duration: 0 S	Indoor Station	1-1-1-701
Received	2016-07-02 11:29:59	Speaking Duration: 11 S	Door Station	1-1-1-1
Received	2016-07-02 11:29:42	Speaking Duration: 6 S	Door Station	1-1-1-1
Dialed	2016-07-02 11:22:11	Ring Duration: 5 S	Indoor Station	1-1-1-701
Missed	2016-07-01 11:44:28	Ring Duration: 40 S	Door Station	1-1-1-1
Missed	2016-07-01 11:42:08	Ring Duration: 34 S	Indoor Station	1-1-1-701
Missed	2016-07-01 11:36:49	Ring Duration: 16 S	Indoor Station	1-1-1-701
Dialed	2016-07-01 11:36:41	Ring Duration: 3 S	Indoor Station	1-1-1-701
Missed	2016-07-01 11:32:11	Ring Duration: 0 S	Indoor Station	1-1-1-701
Missed	2016-07-01 11:32:07	Ring Duration: 0 S	Indoor Station	1-1-1-701

Total:23 Page:1/2 Item Per Page: Adaptive Page

No e-mail account is configured, and all the sending operations are stopped.

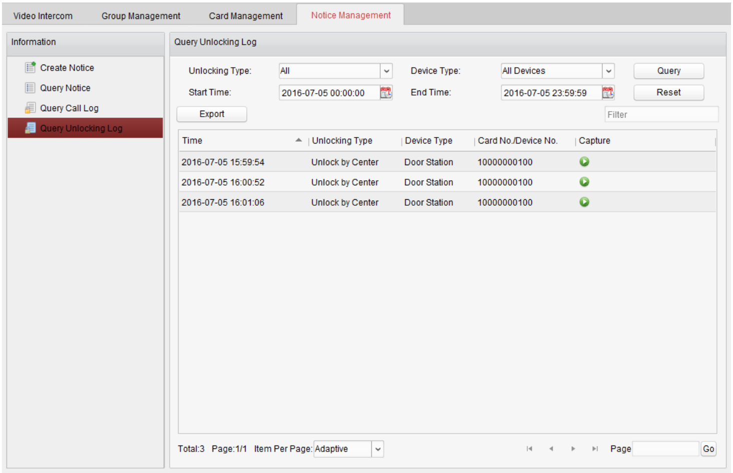
Figure 9-40 Call Log Interface

3. Click **Export** to export the call logs as an excel file.

Querying Unlocking Log

Steps:

1. Click **Query Unlocking Logs** to enter the unlocking log querying page.
2. Select the unlocking type, device type, and set the start time and end time, and click **Query**.



Unlocking Type: All

Device Type: All Devices

Start Time: 2016-07-05 00:00:00

End Time: 2016-07-05 23:59:59

Time	Unlocking Type	Device Type	Card No./Device No.	Capture
2016-07-05 15:59:54	Unlock by Center	Door Station	10000000100	▶
2016-07-05 16:00:52	Unlock by Center	Door Station	10000000100	▶
2016-07-05 16:01:06	Unlock by Center	Door Station	10000000100	▶

Total:3 Page:1/1 Item Per Page: Adaptive Page

Figure 9-41 Unlocking Log Interface

3. Click **Export** to export the unlocking logs as an excel file.

9.7 Device Arming Control

Steps:

1. Select **Tool->Device Arming Control** to pop up device arming control window.

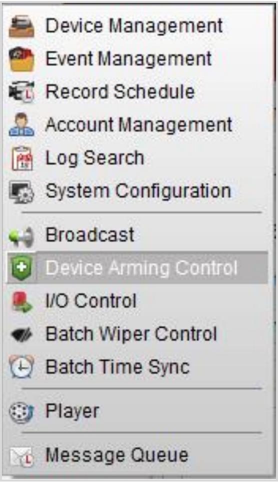
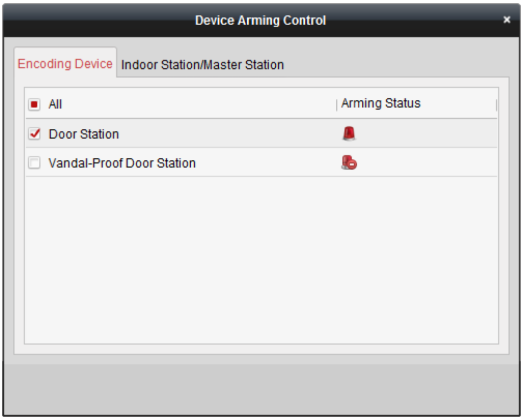


Figure 9-42 Tool Bar

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.

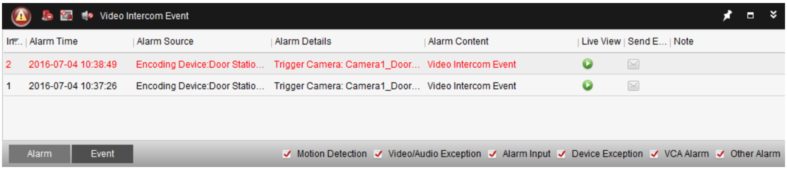


Device Arming Control

Encoding Device | Indoor Station/Master Station

■ All	Arming Status
☑ Door Station	●
□ Vandal-Proof Door Station	●

Figure 9-43 Device Arming Control



Video Intercom Event

In...	Alarm Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send E...	Note
2	2016-07-04 10:38:49	Encoding Device:Door Statio...	Trigger Camera: Camera1_Door...	Video Intercom Event	▶	✉	
1	2016-07-04 10:37:26	Encoding Device:Door Statio...	Trigger Camera: Camera1_Door...	Video Intercom Event	▶	✉	

Alarm | Event

☑ Motion Detection ☑ Video/Audio Exception ☑ Alarm Input ☑ Device Exception ☑ VCA Alarm ☑ Other Alarm

Figure 9-44 Alarm Events

NOTE

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

Appendix

Installation Notice

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

NOTE

Here devices refer to indoor station, outdoor station 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
External Card Reader Wiring	RVVP 4*0.75

First Choice for Security Professionals

www.hikvision.com