

Video Intercom Master Station

User Manual

UD02932B

User Manual

©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

This user manual is intended for users of DS-KM8301 Video Intercom Master Station. 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.

0104001060822

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 2004/108/EC, the RoHS Directive 2011/65/EU.



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



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: <u>www.recyclethis.info</u>

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) 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.

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



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.)



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.

Contents

1	Overview	2
	1.1 Appearance of DS-KM8301 Model	2
	1.2 Typical Application	4
	1.3 Terminals and Interfaces	4
2	Before You Start	6
3	Local Operation	7
	3.1 Activating Device	7
	3.2 User Interface Description	
	3.3 Status	
	3.4 Configuration Settings	9
	3.4.1 Changing Configuration Password	9
	3.4.2 Setting Local Information	
	3.4.3 Setting Network	10
	3.4.4 SIP (Session Initiation Protocol) Server Management	
	3.4.5 Adding Devices	
	3.4.6 Synchronizing Time 3.4.7 Restoring Default Settings	
	3.5 Video Call Settings	
	3.5.1 Callling Resident	
	3.5.2 Callling Master Station	
	3.5.3 Adding Resident Information	
	3.5.4 Viewing Call Logs	
	3.6 Viewing Alarm Messages	
	3.7 Live View	20
4	Remote Configuration via Batch Configuration Tool	23
	4.1 Activating Device Remotely	23
	4.2 Editing Network Parameters	24
	4.3 Adding Device	25
	4.3.1 Adding Online Device	
	4.3.2 Adding by IP Address	
	4.3.3 Adding by IP Segment	
	4.4 Configuring Devices Remotely	
	4.4.1 System	
	4.4.2 Video Intercom 4.4.3 Network	
	4.5 Batch Upgrading	
	4.5.1 Adding Devices for Upgrading	
	4.5.2 Upgrading Devices	
_		
5	Remote Operation via iVMS-4200	42

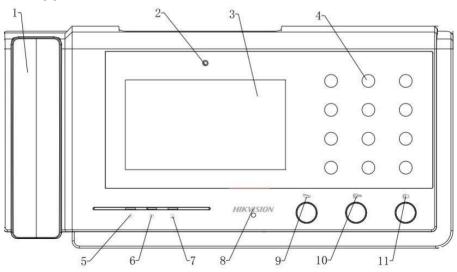
5.1 System Configuration	42
5.2 Device Management	43
5.2.1 Adding Video Intercom Devices	
5.2.2 Modifying Network Information	
5.2.3 Resetting Password	46
5.3 Configuring Devices Remotely via iVMS-4200	48
5.4 Device Arming Control	48
Appendix	50
Wiring Cables	50

1 Overview

The DS-KM8301 master station is an intelligent terminal for video intercom system management. It responses and sends the residents call, receives alarm, and unlocks door remotely. It is normally installed on the management center, it can be operated with a capacitive touch screen, touch buttons and mechanical buttons.

Features:

- Glass panel and aluminum-alloy bracket
- Supports video intercom
- Supports live view of door stations and IP cameras
- Noise suppression and echo cancellation
- Supports hands-free mode
- Alarm processing function
- Supports remote unlocking door function
- Supports on-table mode
- Supports working as a management center and a SIP server simultaneously



1.1 Appearance of DS-KM8301 Model

Figure 1-1 Front Panel

Table 1-1	Descriptions
-----------	--------------

No.	Description
1	Phone
2	Camera
3	Display
4	Dial Keyboard
5	Power Indicator
6	Information Indicator
7	Alarm Indicator
8	Microphone
9	Call/End Call Button
10	Unlock Button
11	Speaker Button

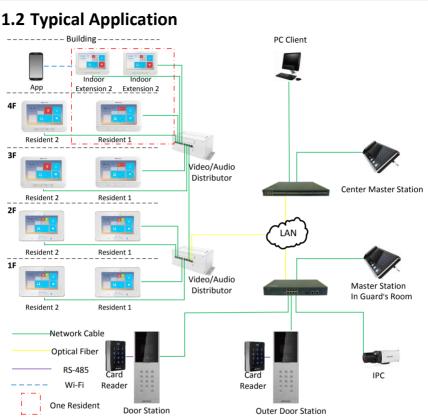


Figure 1-2 Typical Application of Master Station

1.3 Terminals and Interfaces

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

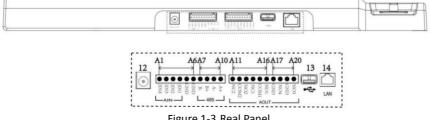


Figure 1-3 Real Panel

Namo	No.	Interface			
Name	-		Description		
Power Supply	12	Power	2-Chip; DC 12V		
USB Interface	13	USB	For U-disk Connection		
Network Interface	14	LAN	Network Interface		
	A1	JIN4	Alarm Input 4 (reserved)		
	A2	JIN3	Alarm Input 3 (reserved)		
ALARM IN	A3	JIN2	Alarm Input 2 (reserved)		
ALARIVI IN	A4	JIN1	Alarm Input 1 (reserved)		
	A5	GND	Grounding		
	A6	GND	Grounding		
	A7	B-			
RS485	A8	B+	RS485 Communication Interfaces		
K3485	A9	A-	K5485 Communication interfaces		
	A10	A+			
	A11	NC2	Alarm Input 2 (NC/reserved)		
	A12	COM2			
	A13	NO2	Alarm Input 2 (NO/reserved)		
	A14	NC1	Alarm Input 1 (NC/reserved)		
	A15	COM1			
ALARM OUT	A16	A16 NO1 Alarm Input 1 (NO/rese	Alarm Input 1 (NO/reserved)		
	A17	GND	Grounding		
	A18	NO4	Optical Coupler Output 4		
	A19	GND	Grounding		
	A20	NO3	Optical Coupler Output 3		

Table 1-2 Descriptions of Terminals and Interfaces

2 Before You Start

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



To remotely activate the device with Batch Configuration Tool or iVMS-4200, refer to Chapter 4, and Chapter 5.

To configure key parameters of the device on the user interface of master station, you are required to enter the admin (configuration) password.

The default admin password is 888999.

You must change the default credential to protect against unauthorized access to the product. Please refer to 3.4.1 and 4.4.2 for changing password.

3 Local Operation

3.1 Activating Device

Connect the power cable to power on the master station.

You must create a password to activate the master station for your first time usage and when it is not activated.

Only after activating the device, you can operate it both locally and remotely.



- The password created for the activation is only used when you add the station to the remote control software such as iVMS-4200.
- To remotely access to the device, use the password here registered to add the device to the remote client.

09:46	2015-10-19 Monday	
Good morning	Create Password	- K
,	Please input new password	
	Please input password again	No Missed Call
	Password length: 8~15 characters	
2	ок	
Contact List	Video Intercom	No New Message

Figure 3-1 Activation Interface

STRONG PASSWORD RECOMMENDED – We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system,

resetting the password monthly or weekly can better protect your product.

3.2 User Interface Description

Please refer to the following figure for the user interface of master station.



Figure 3-2 User Interface

3.3 Status

lcon	Definition	Description
Connected	Normal Status.	The connection between master station and indoor/door stations is normal, and the master station has successfully registered to the SIP server.
(S) Network!	The master station is offline.	Please check the network cable of the master station.
		Invalid SIP server IP address. Set the SIP server IP address.
h 🖵	The master station has not registered to the SIP server.	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.
IP Conflict!	Invalid master station IP address	The master station IP address conflicts with other devices' IP address.

3.4 Configuration Settings

Purpose:

You can set and view the local information, configure the network, manage devices, synchronize the device time, and restore the default settings.

You can get to the configuration interface: Settings -> Configuration.

3.4.1 Changing Configuration Password

The configuration password is required when you configure the master station locally, such as viewing the local information, setting the network, adding devices, setting the time, and restoring default settings.

Steps:

- 1. Press the **Settings** tab on the touch screen and press the **Edit** tab to change the password.
- 2. Enter the old password to change it.
- 3. Enter a new password and confirm it.



• The configuration password is also called admin password on the device.

• The default configuration password (admin password) is 888999.

STRONG PASSWORD RECOMMENDED – We highly recommend you to create a strong



password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, ussword monthly or weekly can better protect your product.

resetting the password monthly or weekly can better protect your product.

3.4.2 Setting Local Information

- 1. Get to the configuration interface: **Settings -> Configuration**, and enter the admin password (configuration password).
- 2. Press the Local Info tab to enter the local information settings interface.
- 3. Set the Community No. and No. for the master station, and set the maximum live view duration.



- The No. ranges from 51 to 99.
- The maximum live view duration varies from 10 seconds to 60 seconds.

	Local Information	Â
@=	Community No. No. 1 51	Local Info Image: Network Image: Network Image: Device Image: Network Image: Network Image: Network <t< th=""></t<>
Ø	Live View Duration *You can set the Max. live view duration 30s +	Mit Restore

Figure 3-3 Local Information Settings

3.4.3 Setting Network



Make sure the network cable is well-connected.

Purpose:

The connection of the network is mandatory for the use of the master station.

Steps:

- Get to the configuration interface: Settings -> Configuration, and enter the admin password (configuration password).
- 2. Press the **Network** tab to enter the network settings interface.

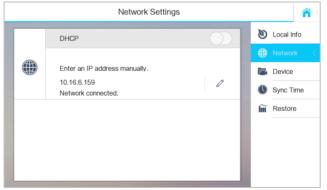


Figure 3-4 Network Settings Interface

3. Press the 2 tab to pop up network settings dialogue box.

	Net	×	
Loc	al IP	10.16.6.159	
Sub	onet Mask	255.255.255.0	
Gat	teway	10.16.6.254	

Figure 3-5 Setting Network

- 4. Enter a local IP address, subnet mask, and gateway.
- 5. Press the **Save** tab.



Enable DHCP function to obtain an IP address automatically.

3.4.4 SIP (Session Initiation Protocol) Server Management

The master station can work as a management center and SIP server simultaneously.

Working as a SIP server

When setting the master station's IP address as the SIP server address on the master station and on the indoor/door station simultaneously, the master station can receive alarm messages from indoor/door stations once there are alarms triggered in the indoor/door stations.

Requiring Connecting to a SIP server

The master station can also be connected to an independent SIP server.

- 1. Get to the configuration interface: **Settings -> Configuration**, and enter the admin password (configuration password).
- 2. Press the **Device** tab, and press the **SIP Server** tab.



Video Intercom Master Station • User Manual

Figure 3-6 SIP Server Adding

- 3. Enter the IP address of the SIP server.
- 4. Press the **Save** button to save the SIP server added.

3.4.5 Adding Devices

Purpose:

The master station never works alone. You can connect the door station, outer door station, IP camera, DVR, DVS, and NVR. Once connected, those devices can work together as a whole video intercom system.



- Hold the device to open the device operation menu for deleting the selected device or clearing all devices (excluding management center and SIP server).
- SIP server and management center can only be edited but not deleted.

- Get to the configuration interface: Settings -> Configuration, and enter the admin password (configuration password).
- 2. Press the **Device** tab.



Video Intercom Master Station · User Manual

Figure 3-7 Device Management

Adding the Door Station or Outer Door Station

Steps:

1. Press the Add Device tab to pop up the Select Device Type dialogue box.

Add device	3	1 SIP Server		2 enter	9	Local Info
_		Select Devic	e Type	×	15	Device
	Q Door Station	Q Outer Door	S IP Camera	Sa DVR/DVS/N	() ()	Sync Tim Restore

Figure 3-8 Device Type Selecting

- 2. Select Door Station or Outer Door Station.
- 3. Enter the corresponding device information required on the pop-up device adding dialogue box.

Please input device name. Please input IP Address. Please input IP Address. Please input the project No Please input the community No Please input the community No	Add Device	×		Add Device	>
Please input the project No			Please	e input device name.	
Please input the community No			Please	input IP Address.	
	Please input the community No		Please	input the project No	
Please input the building No	Please input the building No		Please	input the serial No	



Figure 3-10 Outer Door Station Adding

4. Press the \Box tab on the upper left corner of the dialogue box.



- When the door station being added, the device name, IP address, project number, community number, building number, and serial number need to be entered.
- When the outer door station being added, the device name, IP address, project number, and serial number need to be entered.
- When the door station and outer door station added successfully, you can get the live view of door station and outer door station in the **Live View** interface.

Adding the IP Camera

Steps:

- 1. Press the Add Device tab to pop up the Select Device Type dialogue box.
- 2. Select IP Camera.
- 3. Enter the corresponding device information required on the pop-up device adding dialogue box.



Figure 3-11 IP camera Adding Interface

4. Press the 🔒 tab on the upper left corner of the dialogue box.



- The default Port No. is 554, the default user name is admin.
- The port No. should be consistent with the RTSP (Real Time Streaming Protocol) port No. of the IP camera.
- When the IP camera added successfully, you can get the live view of IP camera on the live view interface.

Adding DVR/DVS/NVR

Steps:

- 1. Press the Add Device tab to pop up the Select Device Type dialogue box.
- 2. Select DVR/DVS/NVR.
- 3. Enter the corresponding device information required on the pop-up device adding dialogue box.



Figure 3-12 NVR/DVS/NVR Adding Interface

4. Press the 🗖 tab on the upper left corner of the dialogue box.



- The default Port No. is 554, the default channel No. is 1, and the default user name is admin.
- The port No. should be consistent with the RTSP (Real Time Streaming Protocol) port No. of DVR/DVS/NVR.

3.4.6 Synchronizing Time

- Get to the configuration interface: Settings -> Configuration, and enter the admin password (configuration password).
- 2. Press the Sync Time tab.
- 3. Switch \bigcirc to \bigcirc to enable NTP.

4. Set the synchronizing interval, enter the IP address of NTP server and port No., and select the time zone.



The unit of synchronizing interval is minute, and the default port No. is 123.

		Time Synchronization		â
[Enable NTP		0	Local Info Network
	Sync Interval IP Address	0.0.0.0		Device Sync Time
	Port No. Time Zone	123 (GMT+08:00) Beijing, Urumqi, Singapore	Ĩ	Restore

Figure 3-13 Time Synchronizing

3.4.7 Restoring Default Settings

- 1. Get to the configuration interface: **Settings -> Configuration**, and enter the admin password (configuration password).
- 2. Press the Restore tab.
- 3. Press the **RESTORE** tab to reboot the system after restoring the default settings.

Restore Default Settings		^
Press the RESTORE button to reboot the system after restoring the default settings.		Local Info Network Device
	0	Sync Time

Figure 3-14 Default Settings Restoring

3.5 Video Call Settings

3.5.1 Callling Resident

Steps:

NOTE

- 1. Press the video Intercomentation that tab on the touch screen to enter the residents calling interface.
- 2. Enter the corresponding residents' Room No..
- 3. Press the 🤽 tab to start a video intercom call.
- 4. Press the Cancel tab to stop the video intercom call.
- The room No. format should be like 1-1-1-102 as Community 1, Building 1, Unit 1, and Room 102. The community No. can be omitted.
- Switch 🕖 to 🚺 on the upper right corner to enable the camera function.

		Call Re	esident		Â
1-	-2-3	+B	Call Resident C		
1	2	3	—		Call Log
4	5	6	0	C	
7	8	9	×		
*Enter 1-2-3-4	05 as Commun	itv 1. Ruildina 2	Unit 3 Room 4	105	

Figure 3-15 Call Resident Interface

3.5.2 Callling Master Station

Master Stations can call each other by entering the master station No..



- 1. Press the Video Intercom tab to enter the resident calling interface.
- 2. Enter the corresponding master stations' No..

- 3. Press the 🨉 tab to start a video intercom call.
- 4. Press the Cancel

tab to stop the video intercom call.

- NOTE
- The master station No. format should be like 1-51 as Community 1, No. 51. The community No. can be omitted.
- to on the upper right corner to enable the camera function. • Switch



Figure 3-16 Calling Master Station Interface

3.5.3 Adding Resident Information

Steps:



- tab on the touch screen to enter the contact list interface. 1. Press the
- 2. Press the Add Contact tab.
- 3. Enter the corresponding residents' information required on the pop-up adding dialogue box.
- 4. Press the 🔒 tab on the upper left corner of the dialogue box.

3.5.4 Viewing Call Logs



- 1. Press the button on the touch screen to enter the Call Log interface.
- 2. Press tab Missed Call or All Calls to view missed call logs or all call logs.

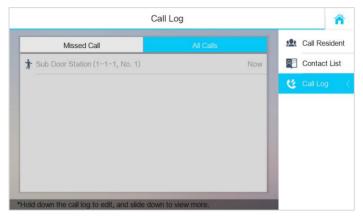


Figure 3-17 Call Log Interface



C

• Hold down a piece of call log to open the call log handling menu.



- Press the **Call** tab to call back.
- Press the **Delete** tab to delete the piece of call log.
- Press the **Clear** tab to delete all pieces of call logs.
- When there is any missed call, the number of missed call will display on the tab

as a prompt, e.g. the icon means there is 1 missed call.

3.6 Viewing Alarm Messages

After connecting indoor/door stations to the master station via the SIP server, the master station can automatically receive alarm messages of indoor/door stations, such as alarm message for not-closed door, tamper alarm, and so on.

Press the **New Message** tab on the user interface to view alarm messages of indoor/door stations.

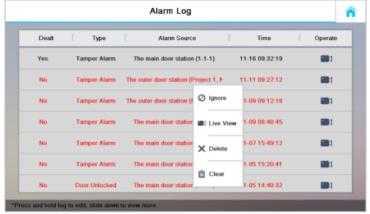


Figure 3-18 Alarm Log Interface



• Hold down a piece of alarm message to open the alarm message handling menu.



- Press the **Ignore** tab to ignore the piece of alarm message.
- Press the **Live View** tab to enter the live view interface.
- Press the **Delete** tab to delete the piece of alarm message.
- Press the **Clear** tab to delete all pieces of alarm messages.



3.7 Live View

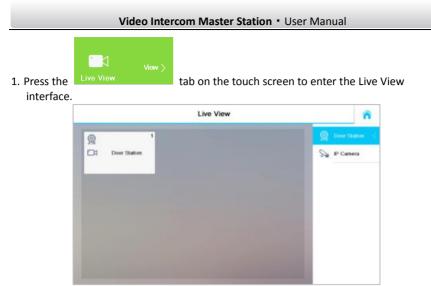


Figure 3-19 Live View Interface

2. Press the **Door Station** tab and press the door station device to view the live view of the corresponding door station.



Figure 3-20 Live View of Door Station

3. Press the **IP Camera** tab and press the IPC device to view the live view of the corresponding IPC.



Figure 3-21 Live View of IPC

4 Remote Configuration via Batch Configuration Tool

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

- Default IP Address: 192.0.0.64.
- Default Port No.: 8000.
- Default User Name: admin.

4.1 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.

Online Dev	vnline Devices: 5 🛛 🏦 🖉 🖊 Edit NET Parameters 🝪 Reset Password 🛛 🦻 Activate									
Index $ riangle$	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-XXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes			
2	XX-XXXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No			
3	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No			
4	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxx	XX-XXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No			
5	XX-XXXX-XX	192.0.0.64	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Inactive	No			

Figure 4-1 Selecting Inactive Device

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

		Activat	e	
Pa	issword:			
		Valid password r You can use a co of numbers, lowe uppercase and s character for you with at least two them contained.	mbination ercase, pecial r password	
Co	onfirm password:			
			ОК	Cancel

Figure 4-2 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.



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

4.2 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 Dev	Online Devices: 5 🔒 🕼 🖊 Edit NET Parameters 🍪 Reset Password 👘 Activate							
Index $ riangle$	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-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes	
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No	
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No	
4	XX-XXXX-XX	192.0.0.64	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No	
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No	

Figure 4-3 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		
	ОК	Cancel

Figure 4-4 Editing Network Parameters



- The default port No. is 8000.
- The default IP address of the master station is 192.0.0.64.
- 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.

4.3 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.

4.3.1 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:

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

Video Intercom Master Station • User Manual

Online De	Dnline Devices: 5 🛛 😰 🐠 🥒 Edit NET Parameters 🍪 Reset Password 🖤 Activate									
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-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes			
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxx	XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No			
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxx	XX-X00X-XX0000000000000000000000000000	Activated	No			
4	XX-XXXX-XX	10.16.2.88	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No			
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-X00X-X0000000000000000000X	Activated	No			

Figure 4-5 Online Devices Interface

2. Click the 🚊 button to pop up the login dialog box.

	Login
Log into the s	selected device(s):
User Name:	admin
Password:	
	OK Cancel

Figure 4-6 Login Dialog Box

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



- 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.

4.3.2 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)	Device(s) in the list will be configured.										
Device List: 1	🛨 × 🕸 🎡	Remote Configura	tior 💼	Flash rom 🛛 🔓 Batch Up	pdate 💮 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	10.16.2.8	8000	V x.x.x build xxxxx	XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Strong password					

Figure 4-7 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: [
Port No.: 8000 User Name: admin	~
User Name: admin	_
uunin	
Password:	
ок	Cancel

Figure 4-8 Adding by IP Address

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



- 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, or IP Segment, the devices should be online devices.

4.3.3 Adding by IP Segment

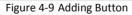
Purpose:

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 I	List: 1	🛨 🗙	@	Remote Configur	atior 💼	Flash rom 🛛 🔓 Batch U	pdate 💮 Linked Network Batch	Configuration	Filter: Device List	~	
	$\operatorname{Index} \bigtriangleup$	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 xxxxx	xx-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Strong password			



- 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 v
Start IP Addres	K
End IP Address	5
Port No.:	8000
User Name:	admin
Password:	••••

Video Intercom Master Station • User Manual

Figure 4-10 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.

4.4 Configuring Devices Remotely

In the device list area, select a device and click we remote configuration interface.

0	Device(s) in the list will be c	onfigured.						
Device	List 1	+ × @	🞡 Remote Configurat	ior 💼 F	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-XXXXXXXXXXXXX	Weak password		<u></u>
							Rem	ote Configuration and Ex	configuration

Figure 4-11 Remote Configuration

4.4.1 System

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

Device Information

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

Basic Information	
Device Type:	XX-XXXX-XX
Device Serial No.:	xx-xxxx-xxxxxxxxxxxxxxxxx
Version Information	
Version:	Vx.x.x build xxxxxx
Hardware Version:	XXXXXXX

Figure 4-12 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.

Embedded Net VIS		
255		
Save		

Figure 4-13 General

Time

Steps:

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

Select Time Zone:	(GMT+08:00) Beijing, Hon	g 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 Wee	k 🗸 Sun 🗸 2 👘 : 00		
End Time:	October 🚽 Last Wee	k 🗸 Sun 🗸 2 👘 : 00		
DST Bias:	60 min 🔍			

Figure 4-14 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.



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.

	Reboot	
	Restore Default Settings	
	Restore All	
	Import Configuration File	
	Export Configuration File	
Remote Upgrade		
Upgrade File	v	Upgrade
Pro	cess:	

Figure 4-15 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.

	translations AMRemConfig.xml AudioIntercom.dll AudioRender.dll BatchConfigTool.exe Batch Configuration User Manual.pdf	e 11 e 10 e 10 e	iconv.dll iVMSGUIToolkit.dll libeay32.dll libxml2.dll LocalXml.zip OpenAL32.dll	000000	QtSvg4.dll QtWebKit4 QtXml4.dll qwt.dll qwtd.dll Sadp.dll SerialSDk
8 8 1 1	BatchUpgrading.exe calib.dll D3DX9_43.dll DevInfo.xml DsSdk.dll	00000	PackageConfig.xml PlayCtrl.dll QosControl.dll QtCore4.dll QtCored4.dll	000	Setup.xml ShowRem sqlite3.dll ssleay32.o StreamTra

Video Intercom Master Station • User Manual

Figure 4-16 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.

rganize 🔻 New f	older					6
Favorites	-	Name	Date modified	Туре	Size	
Autodesk 360		Abilities	8/22/2016 2:18 PM	File folder		
E Desktop		CopyPackage	8/22/2016 3:46 PM	File folder		
Downloads		📕 DownLoad	8/22/2016 3:46 PM	File folder		
📃 Recent Places		HCNetSDKCom	8/22/2016 11:08 AM	File folder		
		imageformats	8/22/2016 11:08 AM	File folder		
Jibraries		📕 plugins	8/22/2016 11:08 AM	File folder		
Documents		🕌 qss	8/22/2016 11:08 AM	File folder		
J Music		translations	8/22/2016 11:08 AM	File folder		
E Pictures						
Subversion						
H Videos	- 4		m			
File name:						
Save as type: Co	onfig F	ile(*.bin)				

Figure 4-17 Export File

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

Remote Upgrade			
Upgrade File	·	[]	Upgrade
Proc	ess:		

Figure 4-18 Remote Upgrade



- 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.

🕒 Add	Modify	📅 Delete	
User Name	Priority		
admin	Administrator		

Figure 4-19 Select User Name

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

User Type:	Administrator	 User Name: 	admin
Password:		Confirm Password:	
IP Address:	0.0.0	MAC Address:	00:00:00:00:00:00
User Primission			
🛃 Local PTZ Co	ntrol		
🛃 Local Manual	Recording		
Local Playba	ck		
Jucal Param	eter Settings		
Local Log Se	arch	U	
Local Advance	ed Operation		
🛃 Local Param	eters View		
🖌 Local Camer	a Management		
Local Video E	Export		
Local Shutdo	wn / Reboot		

Figure 4-20 Modify User Information

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



• The new password and confirm password should be identical.

After editing the password of device, click education 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.

RS485:	1	~
Bitrate:	9600	~
Data Bit:	8	~
Stop Bit:	1	~
Parity:	None	~
Flow Control:	None	~
Vorking Mode:	Disable	~
	Save	
F 1	- 4 31 DC 40F	

Figure 4-21 RS-485



For indoor station and master station, there are 3 choices for the working mode: transparent channel, disable, and custom.

4.4.2 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, IP Camera Information, and Volume Input and Output Configuration.

Device ID Configuration

Steps:

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

Device No. Configuration		
Device Type:	Master Station	~
Community No.:	1	
No.:	51	
	Save	

Figure 4-22 Device No. Configuration

- 2. Set the corresponding information.
- 3. Click the **Save** button to enable the device number configuration.

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 maximum speaking time.
- 3. Click the Apply button.

lime Parameters		
Device Type:	Master Station	
Max. Ring Duration:	30	
Max. Live View Duration:	30	-
Max. Speaking Duration:	90	1975
	Save	

Figure 4-23 Time Parameters



- Maximum ring duration is the maximum duration of master station when it is called without being received. The range of maximum ring duration varies from 30s to 60s.
- Maximum live view time is the maximum time of playing live view of the master station. The range of maximum live view time varies from 10s to 60s.
- Maximum speaking duration is the maximum time of master station when it communicates with other video intercom devices. The range of maximum speaking duration varies from 90s to 120s.

Password

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

You can change the admin password of the master password on this interface.

Permission Password		
Password Type:	Admin Password	~
Old Password:		
New Password:		
Confirm Password:		
	Save	

Figure 4-24 Password Configuration

Volume Input and Output

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

Volume Input			
Volume Input:		-0	- 7
Volume Output			
Volume Output:		-0	- 7
	Save		

Figure 4-25 Volume Configuration

IP Camera Information

Purpose:

You can add, delete and modify devices that can be added to the master station, such as IP cameras, door stations, outer door stations, and DVR/NVR/DVS. By exporting and importing the added device information, you can edit added devices parameters in batch.

Adding IP Camera, DVR/NVR/DVS, Door Station and Outer door Station

Steps:

1. Click the **IP Camera Information** button to enter IP camera information interface.

A	Add	Modify	Delete	Export	mport	_			
Index	Device Name	Getting Stream	Mode URL	Manufacturer Protocol	User	Password	IP Address	Port	Camera
1	IP Camera	Direct		XXX Protocol	ad	****	10.16.2.1	8000	0
2	DVR	Direct		XXX Protocol	ad	*****	10.16.6.1	8000	4
3	Door Station						10.16.6.85		
4	Outer Door						10.16.6.99		

Figure 4-26 IP Camera Information

2. Click the Add button to pop up the device adding dialogue box.

3. Select the device type from the drop-down list menu: IP Camera, door station, outer door station, and DVR/NVR/DVS.

4. Enter corresponding information, and click the **OK** button.



Figure 4-27 Adding Devices

Exporting and Importing Added Device Information

Steps:

Video Intercom Master Station • User Manual

1. Click the **Export** button to export the added device information file.

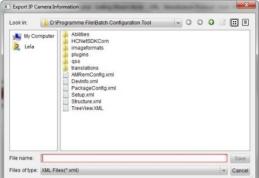


Figure 4-28 Export Information

- 2. Edit parameters of added devices in batch in the exported file.
- 3. Click the **Import** button to pop up importing box, and open the edited added device information file.

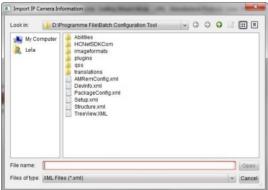


Figure 4-29 Import Information

4.4.3 Network

Local Network Configuration

Steps:

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

ocal Network Configuration	
Local IP Address:	10.16.6.159
IP Address Subnet Mask:	255.255.255.0
Default Gateway:	10.16.6.254
Port:	8000
HTTP Port:	80
	Save

Figure 4-30 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.



- 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.



Figure 4-31 Linked Network Configuration

- 2. Enter the SIP server IP address, security control panel IP address and security control panel port No..
- 3. Click the Save button to enable the settings.

4.5 Batch Upgrading

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

				Batch Up	grading		- 0
🔈 Batch Up	grading						
evice List		nline Devices Manual	📀 Refresh Up	date Status		You can clic select multip	k to select a device or hold the Ctri or Shift ke ple devices for simultaneously upgrading.
PAddress 🗸	Port	Device Serial No.	Version	Upgrade Status	Online Upgrade	Download State	
0.16.2.221	8000	xx-xxxx-xxxxxxxxxxxxxxx	Vx.x.x build xx	Not upgraded	Not Need Upgrade	Not Download	0000000100000010000030000003e80
0.16.2.85	8000	XX-XXXX-XXXXX-XXXXXXX	Vx.x.x build xx	Not upgraded	Not Need Upgrade	Not Download	
orade Mode:	Upgrade	by File - Select Path:					Upgrad
grade aloue.	0001000	og i no - Gelect Haut.					re Default Settings 🗸 Reboot after Upgrad

Video Intercom Master Station • User Manual

Figure 4-32 Batch Upgrading

4.5.1 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.

		Online [
P You can clic		a device or hold the Ctrl or Shift ke	ey to select multiple devices.	Status
0.16.2.102	8000			Status
0.16.2.102	8000	XX-XXXX-XXXXXXXXXXXXXXXXX	Vx.x.x build xxxxxx	
		XX-XXXX-XXXXXXXXXXXXXXXXX	Vx.x.x build xxxxxx	
0.16.2.11	8000	Log	in	
0.16.2.85	8000			
).16.2.225	8000	User Name:		
		Password:		
			OK Cancel	
				in Device Add Device



- 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.

			Online	Devices		×
🚺 You can	click	to selec	t a device or hold the Ctrl or Shift F	ey to select multiple de	vices.	
IP Address	∇	Port	Device Serial No.	Version	Status	
10.16.2.102		8000	XX-XXXX-XXXXXXXXXXXXXX	Vx.x.x build xxxxxx		
10.16.2.221		8000	XX-XXXX-XXXXXXXXXXXX	Vx.x.x build xxxxxx	Added	
10.16.2.11		8000	XX-XXXX-XXXXXXXXXXXXXXXXX	Vx.x.x build xxxxxx		
10.16.2.85		8000	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXX	Vx.x.x build xxxxxx	Logged in	
10.16.2.225		8000	XX-XXXX-XXXXXXXXXXXXXXXX	Vx.x.x build xxxxxx		
					Login Device	Add Device

Figure 4-34 Online Devices

Adding by IP Address/IP Segment

Steps:

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

	Search	×
P. ID		
By IP IP Address;	1	
Port:	8000	
User Name:		
Password:		
		Add>>
By IP Segmen		
Start IP:		
End IP:		
Port	8000	
User Name:		
Password:		
		Add>>
		Add>>
		Cancel

Figure 4-35 Adding by IP Address/IP Segment

4.5.2 Upgrading Devices

There are 2 upgrading modes available: upgrading by file, and online upgrading.

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.

Address V Port 162221 8000 16285 8000	Device Serial No. XX-3000X-300000000X XX-3000X-30000000X	Version Upgrade Status Vx.x.x build xx Not upgraded Vx.x.x build xx Not upgraded	Online Upgrade Not Need Upgrade Not Need Upgrade	Download State Not Download	Code 000000010000000100000300000003e80.
					0000000100000010000030000003e80.
16.2.85 8000	XX-XXXX-XXXXXX.	Vx.x.x build xx Not upgraded	Not Need Upgrade		
			Notheed opgrade	Not Download	
		Select Path			×
	Look in: 🍡 C1Us	ers\daijun5\Desktop\Upgrade File	- 0 0	0	0
	👞 My Computer -	🚹 digicap dav			
	File name: digicap.c	lav		Open V Canor	

Video Intercom Master Station · User Manual

Figure 4-36 Upgrade by File

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

Online Upgrading

Online Upgrading: The batch upgrading tool will search the latest upgrading file for the device automatically. You upgrade the device or devices via the local upgrade files. *Steps:*

- Select a device or multiple devices, and select "Online Upgrading" as the upgrading mode.
- 2. Click the **Download** button. Click the **Upgrade** button after the online upgrading file has been wholly downloaded.

5 Remote Operation via iVMS-4200

5.1 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 station 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.

	System Configuration			×
General	Configure Video Intercom Parameters.			
Keyboard and Joystick	Ringtone: D:/Programme File/IV/MS-4200/Ringtone … Max. Ring Duration:	40		
H Video Intercom	Max. Speaking Duration with Indoor Station:	(S) (S)		
		(S)		
			Default Value	Save

Figure 5-1 System Configuration Interface

5.2 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.

5.2.1 Adding Video Intercom Devices



- 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 **second** 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**.

A	dd New Device Type	×
Select Device Type for the Client:		
Device Type:		
Encoding Device	Storage Server	
Stream Media Server	Decoding Device	
Cascading Server	✓ Transcoder	
 EZVIZ Cloud P2P Device 	Video Wall Controller	
Security Control Panel	Indoor Station/Master Station	
Third-party Encoding Device		
Device Type Instruction		*
	ОК	Cancel

Figure 5-2 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	e (5)		Refresh Every 60s					
+ Add to C	lient	t 🕂 Add All	🗹 Modify Netinfo 🛛 🥱 Reset F	Password	Activate	Filter		
IP		Device Type	Firmware Version	Security	Server Port	Start Time	Added	ŕ
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 5-3 Online Devices



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's port No.. The default value is 8000.

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

Password: Input the device's password. By default, the password is 12345.

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.



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.

	Add	_	×
Adding Mode:			
IP/Domain IP Segmen	t 🔘 IP Server	HIDDNS	 Batch Import
Add Offline Device			
Nickname:	Door Station		
Address:	10.16.1.24		
Port:	8000		
User Name:	admin		
Password:	•••••		
Export to Group			
Set the device name as t connected to the device t	he group name and add a o the group.	all the channels	
		Add	Cancel
		Add	Calicer

Figure 5-4 Adding Device by IP/Domain



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.

5.2.2 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.

	Modify Network Parameter	×
Device Information:		
MAC Address:	44-19-b6-5e-fb-4a	Сору
Software Version:	V5.3.0build 150513	Сору
Device Serial No.:	DS-2CD2312-I20140806CCCH475372976	Сору
Network Information:		
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:		
	ОК	Cancel

Figure 5-5 Modifying Network Information



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

5.2.3 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:



This option is available to door stations.

	Reset Password ×
Export Key	
Key File:	Export
Import Key	
Key Importing Mode	Import File 🗸
Import Key:	
Password:	
Confirm 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.
	OK Cancel

Figure 5-6 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 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:

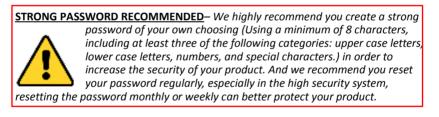
If the window with import file and export file buttons, password and confirm password field pops up, follow the steps below to reset the password:

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

	Reset Password ×
Export File:	Export
Import File:	Import
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 Passw	
	OK Cancel

Figure 5-7 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.



5.3 Configuring Devices Remotely via iVMS-4200

Configuring devices remotely via iVMS-4200 is the same with that via Batch Configuration Tool, please refer *4.4 Configuring Devices Remotely* for detail steps.

5.4 Device Arming Control

Steps:

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



Video Intercom Master Station • User Manual

Figure 5-8 Tool Menu

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

ð	All	Arming Status
1	Indoor Station	8
	Master Station	-

Figure 5-9 Device Arming Control

Intt. Alarr	m Time	Alarm Source	Alarm Details	Alarm Content	Live View	Send E Note		
2 2016	6-07-04 10:38:49	Encoding Device:Door Statio	Trigger Camera: Camera1_Door	Video Intercom Event	0			
1 2016	6-07-04 10:37:26	Encoding Device:Door Statio	Trigger Camera: Camera1_Door	Video Intercom Event	0			

Figure 5-10 Alarm Events



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

Appendix

Wiring Cables

Cables	Specification
Power Cable	RVV 2*1.0
Network Cable	Cat5e



To avoid echo and whistles, set the wire distance longer than 8 meters.

