

HIKVISION



Video Intercom Master Station

Quick Start Guide

UD06105B

Quick Start Guide

©2017 Hangzhou Hikvision Digital Technology Co., Ltd.

This quick start guide 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.

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 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 (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.

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



Warnings

All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.

Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.

Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.

Please make sure that the power has been disconnected before you wire, install or dismantle the device.

When the product is installed on wall or ceiling, the device shall be firmly fixed.

If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions

Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetic 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	1
1.1 Appearance.....	1
1.2 Terminals and Interfaces.....	2
2 Local Operation	4
2.1 Activating Device.....	4
2.2 User Interface Description.....	5
2.3 Status.....	5
2.4 Configuration Settings.....	6
2.4.1 Changing Configuration Password.....	6
2.4.2 Setting Local Information.....	6
2.4.3 Setting Network.....	7
2.4.4 SIP (Session Initiation Protocol) Server Management.....	8
2.4.5 Adding Devices.....	9
2.5 Calling Resident.....	11
2.6 Calling Master Station.....	12
2.7 Viewing Alarm Message.....	13
3 Remote Operation via Batch Configuration Tool	15
3.1 Activating Device Remotely.....	15
3.2 Editing Network Parameters.....	16
3.3 Adding Device.....	17
3.3.1 Adding Online Devices.....	17
3.3.2 Adding by IP Address.....	18
Appendix	20
Wiring Cables.....	20

1 Overview

The DS-KM8301 master station is an intelligent terminal for video intercom system management. It responds 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

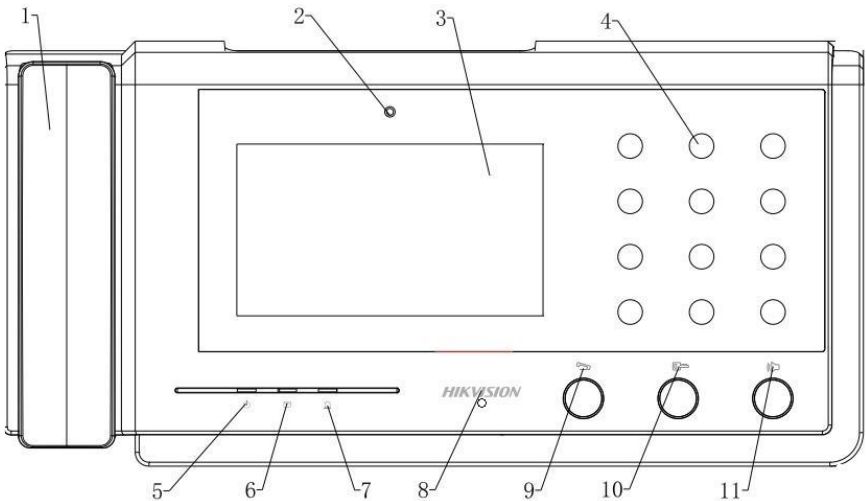


Figure 1-1 Front Panel

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

1.2 Terminals and Interfaces

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

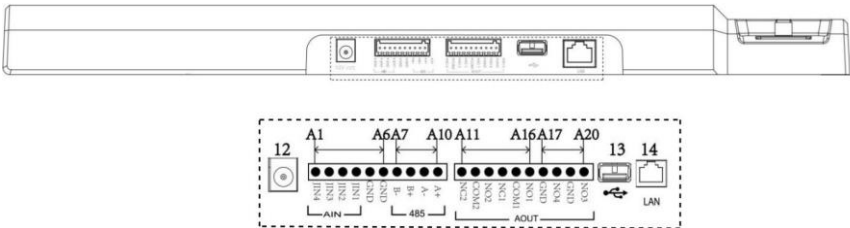


Figure 1-2 Real Panel of DS-KM8301

Table 1-2 Description of Terminals and Interfaces

Name	No.	Interface	Description
Power Supply	12	Power	2-Chip; DC 12V
USB Interface	13	USB	For U-disk Connection
Network Interface	14	LAN	Network Interface
ALARM IN	A1	JIN4	Alarm Input 4 (reserved)
	A2	JIN3	Alarm Input 3 (reserved)

Video Intercom Master Station • Quick Start Guide

Name	No.	Interface	Description
	A3	JIN2	Alarm Input 2 (reserved)
	A4	JIN1	Alarm Input 1 (reserved)
	A5	GND	Grounding
	A6	GND	Grounding
RS485	A7	B-	RS485 Communication Interfaces
	A8	B+	
	A9	A-	
	A10	A+	
ALARM OUT	A11	NC2	Alarm Input 2 (NC/reserved)
	A12	COM2	
	A13	NO2	Alarm Input 2 (NO/reserved)
	A14	NC1	Alarm Input 2 (NC/reserved)
	A15	COM1	
	A16	NO1	Alarm Input 1 (NO/reserved)
	A17	GND	Grounding
	A18	NO4	Optical Coupler Output 4
	A19	GND	Grounding
	A20	NO3	Optical Coupler Output 3

2 Local Operation

2.1 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 the device 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.

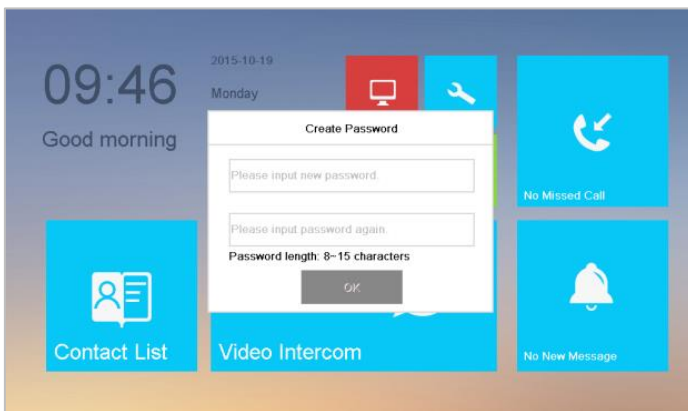


Figure 2-1 Activation Interface

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.



2.2 User Interface Description


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



Figure 2-2 User Interface

2.3 Status

Icon	Definition	Description
	Normal Status.	The connection between master station and indoor/door stations is normal, and the master station has successfully registered to the SIP server.
	The master station is offline.	Please check the network cable of the master station.
	The master station has not registered to the SIP server.	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.

Icon	Definition	Description
	Invalid master station IP address	The master station IP address conflicts with other devices' IP address.

2.4 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**.

2.4.1 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, resetting the password

monthly or weekly can better protect your product.

2.4.2 Setting Local Information

Steps:

1. Go 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.

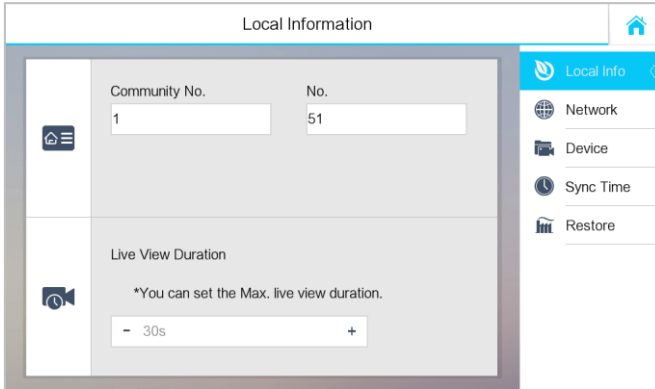


Figure 2-3 Local Information Settings

2.4.3 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:

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

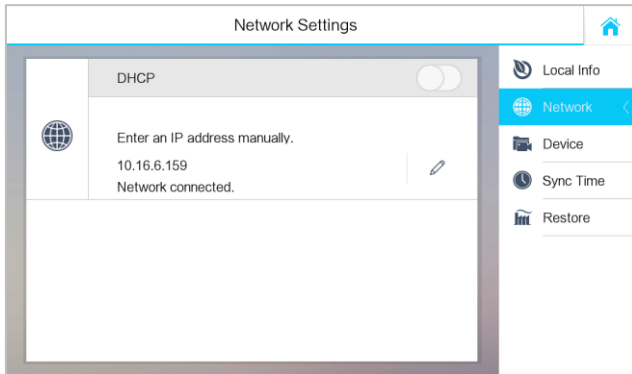



Figure 2-4 Network Settings Interface

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

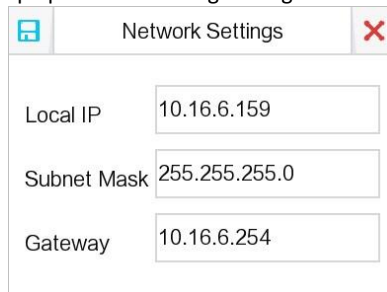


Figure 2-5 Setting Network

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



Enable **DHCP** function to obtain an IP address automatically.

2.4.4 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.

Steps:

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

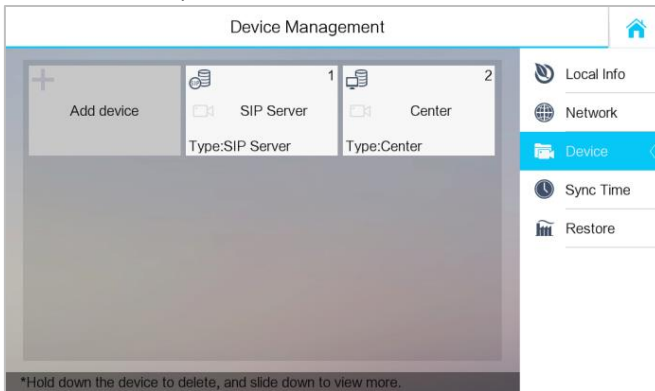


Figure 2-6 SIP Server Adding

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

2.4.5 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.



Adding door station is introduced in the quick start guide. For adding other devices (outer door station, IP camera, DVR, DVS, and DVR), please refer to the user manual in the disk.

Adding the Door Station

Steps:

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

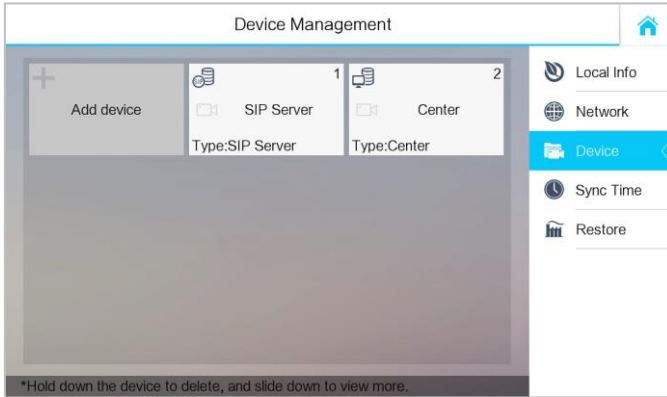


Figure 2-7 Device Management

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

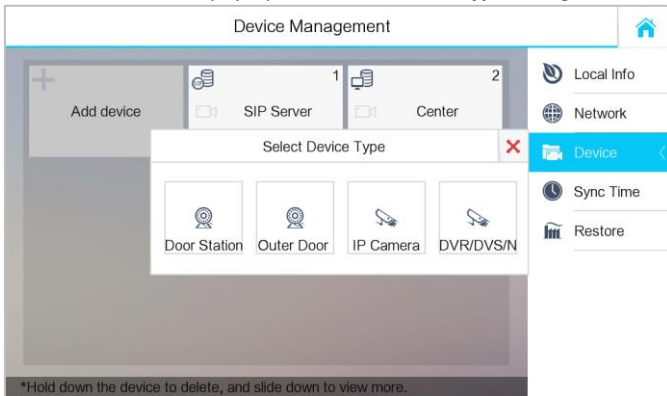



Figure 2-8 Device Type Selecting

4. Select **Door Station**, and enter corresponding device information required on the pop-up device adding dialogue box.

Figure 2-9 Door Station Adding Interface




5. Press the  tab on the upper left corner of the dialogue box.





After adding door station successfully, you can get the live view of door station and outer door station in the **Live View** interface.

2.5 Calling Resident

Steps:

1. Press the  tab on the touch screen to enter the residents calling interface.
2. Enter the corresponding resident's Room No..
3. Press the  tab to start a video intercom call.
4. Press the  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.

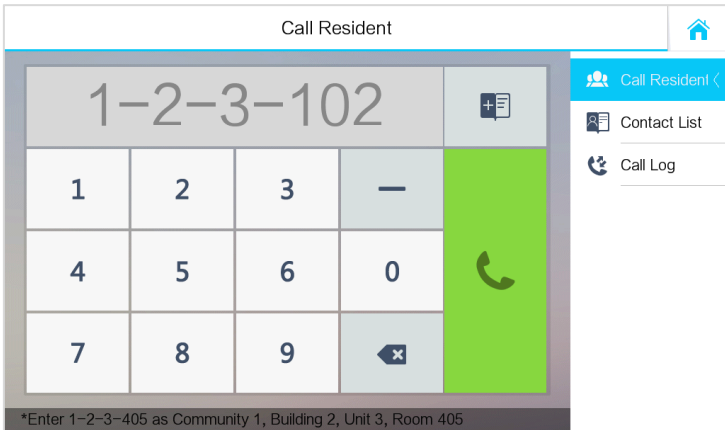





Figure 2-10 Call Resident Interface



2.6 Calling Master Station

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

Steps:

1. Press the  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  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.
- Switch  to  on the upper right corner to enable the camera function.

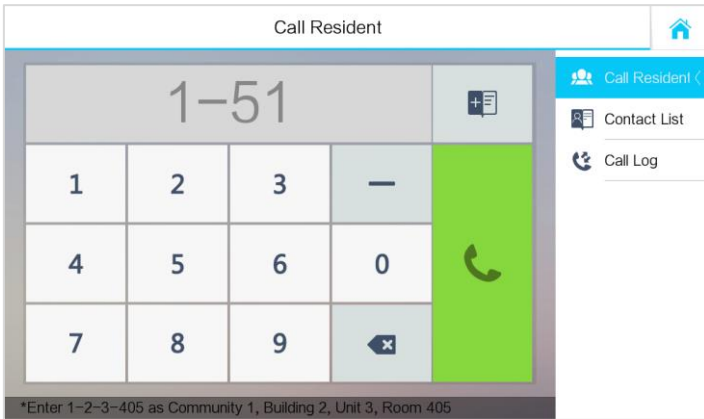


Figure 2-11 Calling Master Station Interface

2.7 Viewing Alarm Message

After connecting indoor station and door station to the master station, you can view the alarm messages of indoor station or door station in the master station. Press the **New Message** tab on the user interface to enter the alarm log interface.

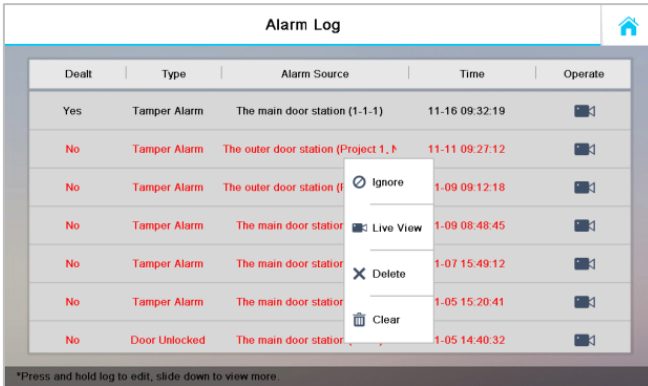
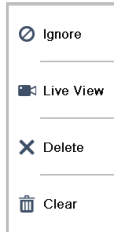




Figure 2-12 Alarm Log Interface



- Hold 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.

- When there is any alarm message, the tab  turns to  as a prompt.

3 Remote Operation via Batch Configuration Tool

3.1 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-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	192.0.0.64	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Inactive	No

Figure 3-1 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:

OK Cancel

Figure 3-2 Creating Activation Password

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.

3.2 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								
🔍 🌐 🔧 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-XXXXXXXXXXXXXXXXXXXXXX	Activated	Yes	
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXX	Activated	No	
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXX	Activated	No	
4	XX-XXXX-XX	192.0.0.64	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXX	Activated	No	
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXX	Activated	No	

Figure 3-3 Click 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.

Figure 3-4 Edit Network Parameters



- The default port No. is 8000.
- After editing the network parameters of device, you should add the devices to the device list again. And the device cannot be added unless it has the same subnet the PC IP address.

3.3 Adding Device

For batch configuration tool and iVMS-4200 software, you should add device to the software so as to configure the device remotely.

3 ways for adding the device are supported: adding active online devices within your subnet, adding device by IP address, and adding device by IP segment. Here take adding online device and adding device by IP address via batch configuration tool as example.


3.3.1 Adding Online Devices

Steps:

1. 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 xxxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	10.16.2.88	8000	Vx.x.x build xxxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxxx	XX-XXXX-XXXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No

Figure 3-5 Online Devices Interface

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

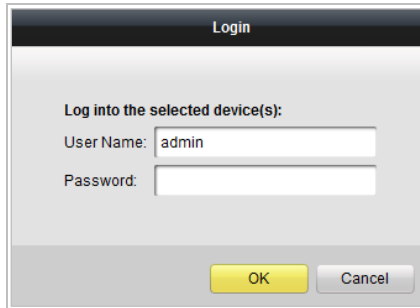


Figure 3-6 Login Dialog Box

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.

3.3.2 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.

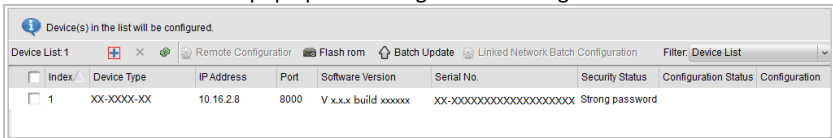
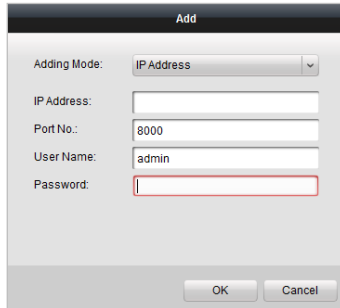


Figure 3-7 Adding Button

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.



The screenshot shows a dialog box titled "Add" with the following fields and values:

- Adding Mode: IP Address (dropdown menu)
- IP Address: (empty text box)
- Port No.: 8000 (text box)
- User Name: admin (text box)
- Password: (empty text box)

Buttons: OK, Cancel

Figure 3-8 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, IP Segment or Port No., the devices should be online devices.

Appendix

Wiring Cables

Cables	Specification
Power Cable	RVV 2*1.0
Network Cable	Cat5e



Warning

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



First Choice for Security Professionals