HIKVISION

Video Intercom Vandal-Resistant Doorbell

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN

CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

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

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

Safety Instruction

⚠ **Warning**

- 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.)

⚠ **Caution**

- 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.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

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

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

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

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

Industry Canada ICES-003 Compliance

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

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

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Contents

1 Appearance

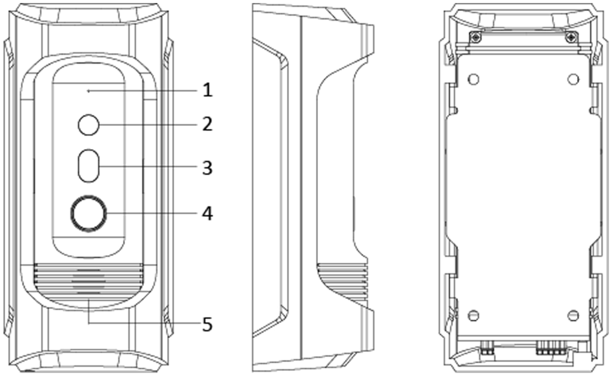


Figure 1-1 Appearance

Table 1-1 Component Description

No.	Description
1	Microphone
2	Built-in Camera
3	Low Illumination Supplement Light
4	Call Button
5	Loudspeaker

2 Terminal and Wiring Description

2.1 Terminal Description

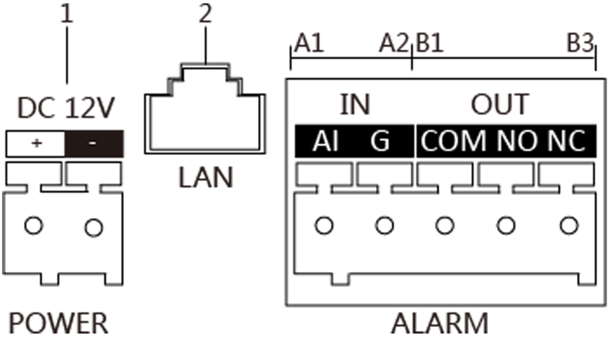


Figure 2-1 Terminals Description

Table 2-1 Description

Name	**No.**	**Interface**	**Description**
Power Supply	1	12 VDC	12 VDC Power Supply Input
LAN	2	LAN	Network Interface (PoE Supported)
ALARM IN	A1	AI	Alarm Input
	A2	GND	Grounding
ALARM OUT	B1	COM	Common Interface
	B2	NO	Door Lock Relay Output (Connect Electric Strike)
	B3	NC	Door Lock Relay Output (Connect Electric Bolt or Contact Lock)

2.2 Wiring Description

2.2.1 Door Lock Wiring

Terminal NC/COM is set as default for connecting magnetic lock/electric bolt; terminal NO/ COM is set as default for connecting electric strike.

To connect electric lock, it is required to set the output of terminal NC/COM/NO to be electric lock via Batch Configuration Tool or **iVMS-4200** client software or the web browser.

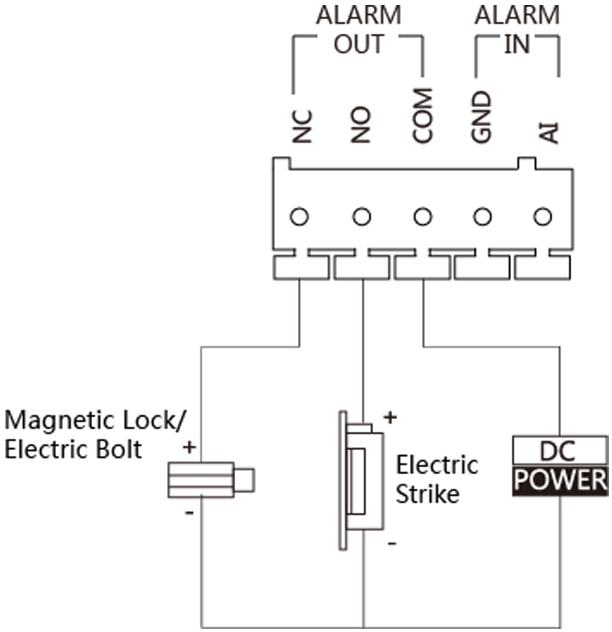


Figure 2-2 Door Lock Wiring

2.2.2 Door Contact Wiring

To connect door contact, it is required to set the output of terminal AI to be door status via Batch Configuration Tool or **iVMS-4200** client software or the web browser.

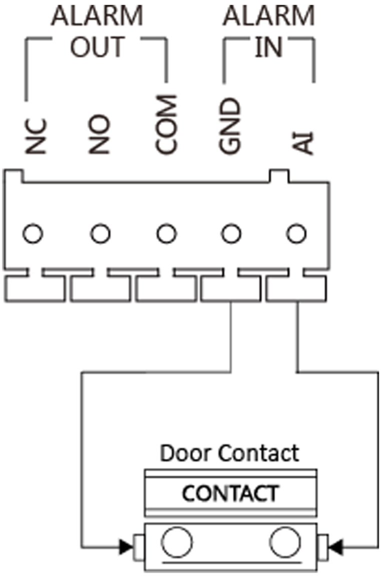


Figure 2-3 Door Contact Wiring

2.2.3 Exit Button Wiring

To connect exit button, it is required to set the output of terminal AI to be door status via Batch Configuration Tool or **iVMS-4200** client software or the web browser.

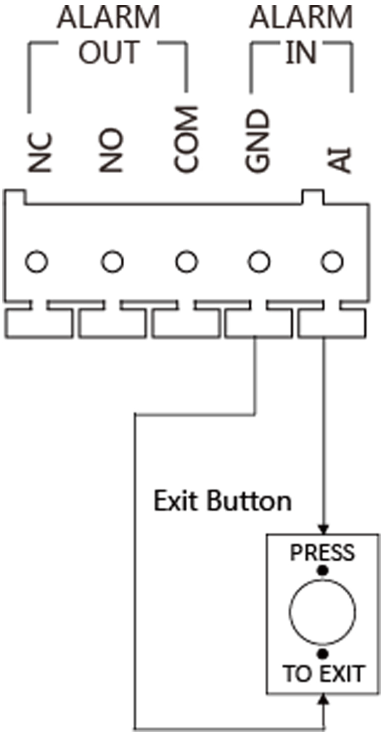


Figure 2-4 Exit Button Wiring

2.2.4 Alarm Device Input Wiring

When you set the output of terminal AI to be custom via Batch Configuration Tool or **iVMS-4200** client software or the web browser, you can connect any alarm input device to the door station via the terminal AI.

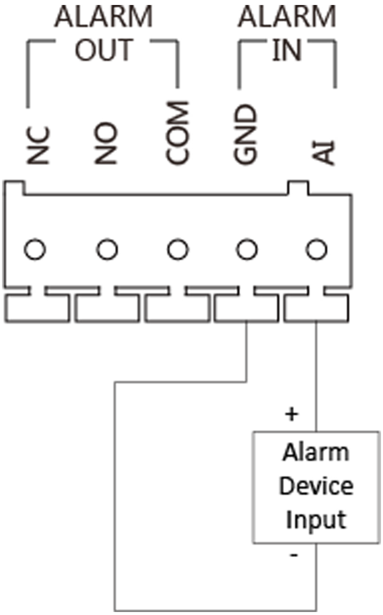


Figure 2-5 Alarm Device Input Wiring

3 Doorbell Installation

3.1 Wall Mounting Plate

To install the doorbell onto the wall, you are required to use a matched mounting plate.

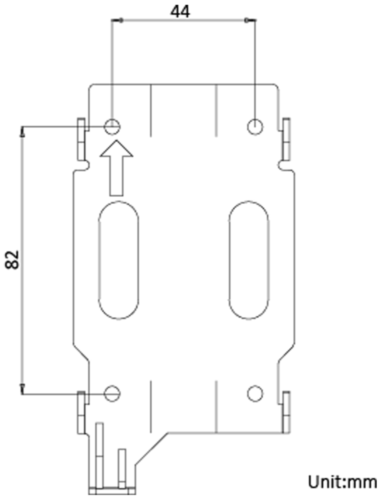


Figure 3-1 Wall Mounting Plate

3.2 Wall Mounting

Steps

1. Fix the wall mounting plate to the wall with 4 expansion screws.

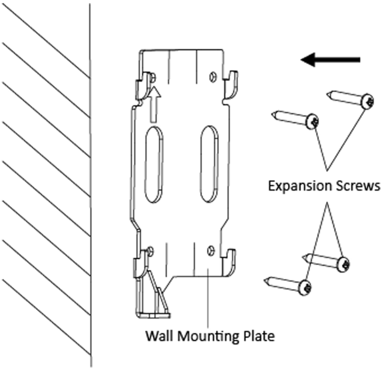


Figure 3-2 Install the Plate

2. Insert terminal blocks into the interfaces of the doorbell body, and connect the network cable.

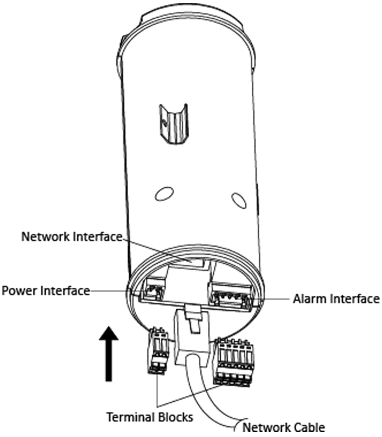


Figure 3-3 Insert Terminals and Network Cable

3. Fix the doorbell body to the protective shield tightly.

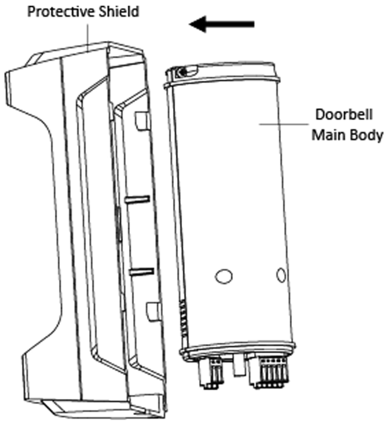


Figure 3-4 Fix the Body to the Shield

4. Hook the doorbell to the wall mounting plate tightly.

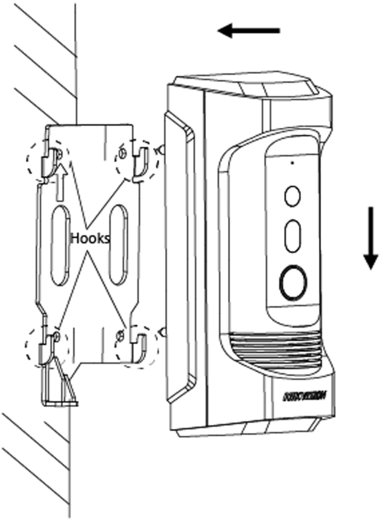


Figure 3-5 Hook the Doorbell to the Plate

5. Use the set screw to secure the doorbell with the mounting plate.

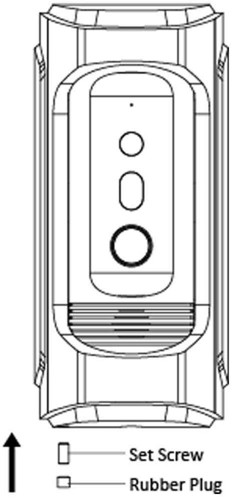


Figure 3-6 Secure the Doorbell

4 Getting Started

4.1 Activation

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

Activation via Batch Configuration Tool, activation via Web and activation via **iVMS-4200** client software are supported.

4.1.1 Activate Device via Web

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

Default parameters of the door station are as follows:

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

Steps

1. Power on the device, and connect the device to the network.
2. Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation page.

   Note

   The computer and the device should belong to the same subnet.

3. Create and enter a password into the password field.
4. Confirm the password.
5. Click **OK** to activate the device.

4.1.2 Activate Device via iVMS-4200 Client Software

Default parameters of doorbell are as follows:

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

Steps

1. Run the client software, click **Maintenance and Management → Device Management → Device** to enter the page.
2. Click **Online Device**.
3. Select an inactivated device and click **Activate**.
4. Create a password, and confirm the password.

   Note

   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 lower case numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can b protect your product.

5. Click **OK** 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 to activate devices in batch.

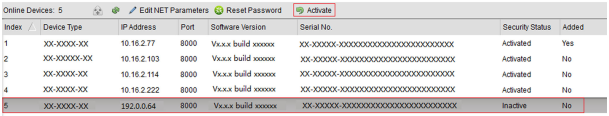
4.1.3 Activate Device via Batch Configuration Tool

Create a password to activate the device before you use the device.

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

Steps

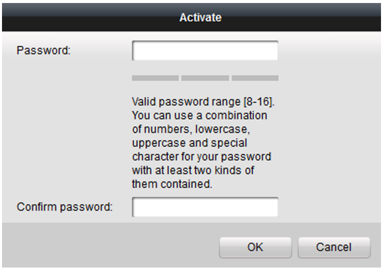
1. Run the Batch Configuration Tool.



Index	Device Type	IP Address	Port	Software Version	Serial No.	Security Status	Added
1	XX-XXXX-XX	10.16.2.77	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	Yes
2	XX-XXXXX-XX	10.16.2.103	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
3	XX-XXXX-XX	10.16.2.114	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
4	XX-XXXX-XX	10.16.2.222	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Activated	No
5	XX-XXXX-XX	192.0.0.64	8000	Vx.x.x build xxxxxx	XX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX	Inactive	No

Figure 4-1 Batch Configuration Tool

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



Password:

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

Confirm password:

Figure 4-2 Activate

3. Create a password, and confirm the passwork.

Note

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

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

Note

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

4.2 Edit Network Parameters

Steps

1. In the online device list, select the activated device and click **Edit Device Network Parameters**.

   Note

   The mobile client will automatically search for online devices in the LAN.

2. Edit **IP Address**, **Subnet Mask**, **Gateway** and other information in the pop-up dialogue box.
3. Enter the password and click **OK**.

   Note

   - When setting IP address, please keep the IP address of doorbell and the IP address of computer in the same network segment.
   - After editing the network parameters, the device needs to be re-added to the client.

5 Local Operation

You can call the resident (the indoor station) or the center (the master station) via the doorbell by pressing or holding the call button. Default settings of the call button: when you press the call button, it calls the resident, and when you hold the call button, it calls the center.

Before You Start

- Make sure the doorbell has been activated.
- Make sure the network cable is well-connected.

Steps

1. Press the call button to call the resident.
2. The resident can accept/decline the calling from the doorbell, and unlock the door via the indoor station.

Note

- Besides the indoor station, you can also unlock the door by the master station, the client software, and the web.
- When the video intercom between you and the resident is realized, you can speak to the resident, and the live view of doorbell will be displayed on the connected indoor station.
- When live view of doorbell is displayed on other devices or doorbell is calling resident, the doorbell will detect the brightness of video. When the brightness is lower than the expected threshold, the supplement light will be enabled.
- When the supplement light is enabled, the backlight of key will be auto-enabled, otherwise, the doorbell will detect the brightness of live view and enable the backlight of key when the brightness of live view is lower than expected threshold.

6 Remote Configuration via Mobile Client

6.1 Set Up Mobile Client

Before You Start

Make sure your mobile device has been connected to Wi-Fi.

Hik-Connect client is necessary for doorbell configuration and operation.

Steps

1. Install **Hik-Connect** client and register a user account for iOS and Android.
   1) Search **Hik-Connect** in App Store or Google Play™ to download and install the client.
   2) Launch the App and follow the on-screen instructions to register a user account.
2. Start the **Hik-Connect** client, and login the client.

6.2 Set Up Doorbell via Client

To operate the doorbell normally, you should add the doorbell to the client, set its Wi-Fi connection via client first, and activate it.

Steps

1. In the home page of the client, tap **Add Device**.
   - Scan QR code of the doorbell to add.

     Note

     The QR code is printed on the label, which is on the rear panel of doorbell. If you have already installed the device, you can scan the QR code in the user manual.
   - Tap 🖼 to select QR code picture to add.
   - Tap ✎ to enter **Serial No.** of the doorbell. Tap 💾 to add.
2. Select device type as **Doorbell** and choose the model.
3. Tap **Connect to a network**.

   Note

   Make sure the doorbell and the mobile device are in the same LAN.

- Wired Connection:

  a. Tap **Wired Connection** to enter the configuration page.

  b. Connect the device to a router with a network cable.

  Note

  Make sure your mobile device is connected to the same router.

  c. Tap **Connected and Next** to complete network connection settings.

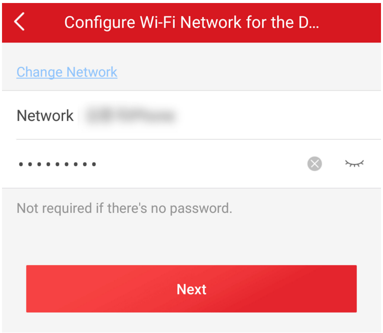
- Wireless Connection:

  a. Tap **Wireless Connection** to enter the configuration page.

  b. Enter the password of Wi-Fi and tap **Next**.

  Note

  Make sure your mobile device has been connected to the same Wi-Fi.



Configure Wi-Fi Network for the D...

Change Network

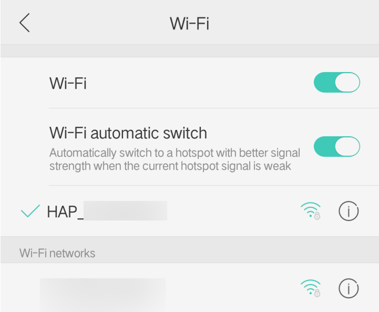
Network [redacted]

••••••••••

Not required if there's no password.

Figure 6-1 Connect to Wi-Fi

c. Connect the mobile device to the Hot Spot of the doorbell and tap **Next**.



Wi-Fi

Wi-Fi

Wi-Fi automatic switch
Automatically switch to a hotspot with better signal strength when the current hotspot signal is weak

✓ HAP_[redacted]

Wi-Fi networks

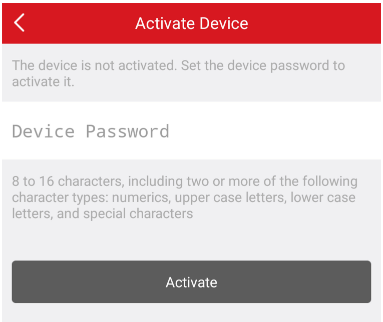
[redacted]

Figure 6-2 Connect to the Hot Spot

Note

- The password of the hot spot is **AP + Verification Code**.
- By default, the device enabled Wi-Fi AP mode. Or hold the reset button for 5 seconds to enter the Wi-Fi AP mode.

4. **Optional:** Enter the device password and tap **Activate**.



Activate Device

The device is not activated. Set the device password to activate it.

Device Password

8 to 16 characters, including two or more of the following character types: numerics, upper case letters, lower case letters, and special characters

Figure 6-3 Activate the Doorbell

Note

- 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

- If the doorbell has been activated, skip the step.

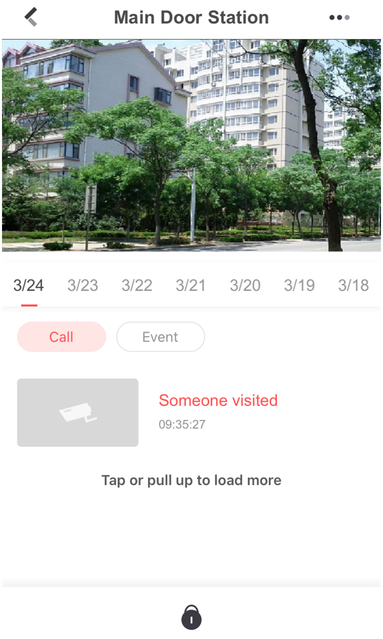
5. The account is connected to the device.

6.3 Remote Operation via Client

You can realize some certain functions of the doorbell via **Hik-Connect** (including, but not limited to, live view, and remote playback).

Live View

Tap the doorbell in the list to open the floating windows. And then tap the floating window to enter the Live View page.



Someone visited
09:35:27

Tap or pull up to load more

Figure 6-4 Live View

Tap the video on the screen, you can tap 📷 to capture the screen.

Tap to record.

Two-Way Audio

Call from client software: On the Live View page, tap to create a call between the client and the device.

Receive call from the device: You can receive or decline the call from device.

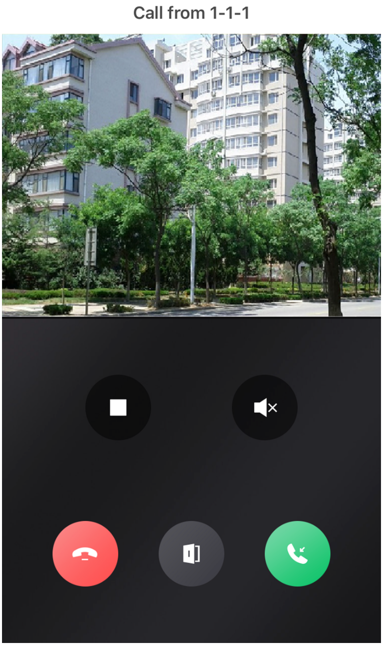


Figure 6-5 Receive Call from Device

Tap to receive the call.

Tap to decline the call.

Tap to unlock the door remotely.

Tap to adjust the volume.

When you communication with the device, you can tap to mute.

Unlock Remotely

On the main page or on the live view page, tap 🔒 to unlock the door.

Playback

On the Live View page, tap **...** → **Playback** to playback the videos stored in the TF card.

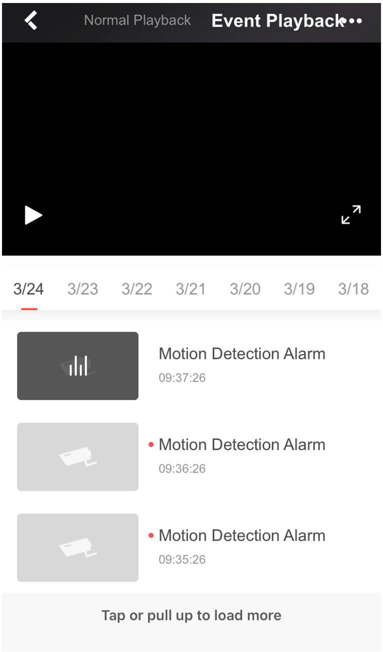


Figure 6-6 Playback

Synchronize Time

On the Live View page, tap **...** → **Settings** , you can set the time of doorbell.

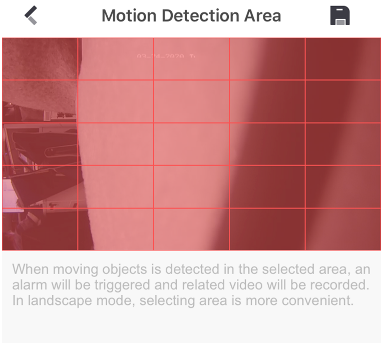
Tap **Time Zone** to select the right time zone.

Tap **Date Format** to change the format.

Alarm Notification

On the Live View page, tap **... → Settings → Notification** , slide the slider to enable alarm notification.

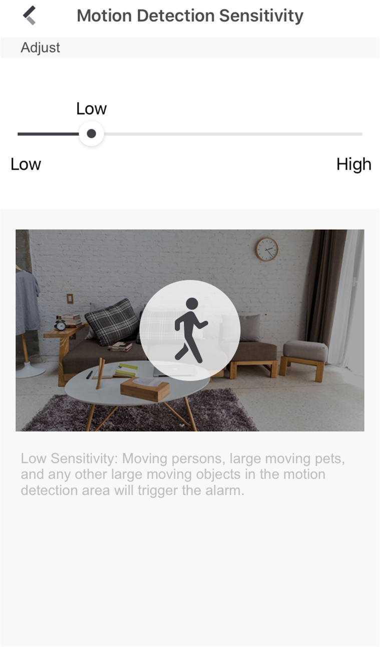
Tap **Draw Motion Detection Area** and select area. Tap 💾 to save.



When moving objects is detected in the selected area, an alarm will be triggered and related video will be recorded. In landscape mode, selecting area is more convenient.

Figure 6-7 Draw Motion Detection Area

Tap **Motion Detection Sensitivity** to adjust the sensitivity.



Low Sensitivity: Moving persons, large moving pets, and any other large moving objects in the motion detection area will trigger the alarm.

Figure 6-8 Motion Detection Sensitivity

Volume

On the Live View page, tap **...** → **Settings** , you can adjust the **Loudspeaker Volume** and **Microphone Volume**.

Note

Loudspeaker volume and microphone volume can be set from 0 to 10.

Notification

On the home page of the client, tap **Notification** to get or edit alarm messages.

Note

- The messages will be pushed automatically by enabling Receive Events and Push Notifications.
- The client can receive the triggered alarm automatically when the doorbell is powered on by Receive Events but NOT Push Notifications.

Share Account

On the main page, tap < to share the information to other accounts. Or on the live view page, tap **...** → **Share** to share.

Note

Up to 4 accounts can be added to share.

7 Remote Configuration via Web

7.1 Live View

In the browser address bar, enter the IP address of the device, and press the Enter key to enter the login page.

Enter the user name and password and click **Login** to enter the Live View page. Or you can click **Live View** to enter the page.

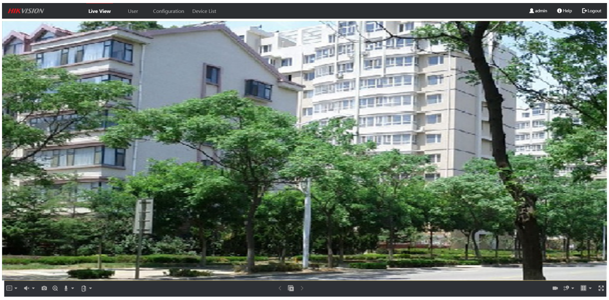


Figure 7-1 Live View

- You can start/stop live view, capture, record, audio on/off, two-way audio, etc.
- The stream type can be set as main stream or sub stream.
- For IE (Internet Explorer) users, the device support two-way audio communication.

7.2 Query

Click **Search** to enter the page.

Input the **Employee ID**, **Name** and **Card No.**. Select **Start Time**, **End Time** and click **Search**, the information will display on the page.

7.3 User Management

You can add, delete or search the information of the user.

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

- Click **Add** and enter the username, floor No. and room No. to add.
- Check the box of the user and click **Delete** to delete the selected user.
- Enter the keyword and click **Search**. The information will display in the list.

7.4 Parameters Settings

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

Remote configuration in iVMS-4200 and Batch Configuration Tool is the same as that in Web. Here takes the configuration in web for example.

Note

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

7.4.1 Local Parameters Settings

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

Live View Parameters

Stream Type

Set the stream type as **Main Stream** or **Sub-stream**.

Play Performance

Set the live view performance to **Shortest Delay**, **Balanced** or **Fluent**.

Auto Start Live View

Check **Yes** to enable the function.

Image Format

Select the image format for picture capture.

Click **Save** to enable the settings.

Record File Parameters

Record File Size

Select the packed size of the manually recorded and downloaded video files to **256M**, **512M** or **1G**. After the selection, the maximum record file size is the value you selected.

Save record files to

Set the saving path for the manually recorded video files.

Click **Save** to enable the settings.

Picture and Clip Settings

Save snapshots in live view to

Set the saving path of the manually captured pictures in live view mode.

Note

You can click **Browse** to change the directory for saving the clips and pictures, and click **Open** to open the set folder of clips and picture saving.

Click **Save** to enable the settings.

7.4.2 System Settings

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

Click **System** to enter the settings page.

Basic Information

Click **System Settings → Basic Information** to enter the settings page. On the page, you can edit **Device Name** and **Device No.** Set the **Language** and **System Type** according to your needs.

Click **Save** to enable the settings.

Time Settings

Click **System Settings → Time Settings** to enter the settings page. Select the **Time Zone** of your location from the drop-down list.

- Enable **NTP**, set the **Server Address**, **NTP Port** and **Interval**.
- Enable **Manual Time Sync.**, set the time manually or check the **Sync. with computer time**.

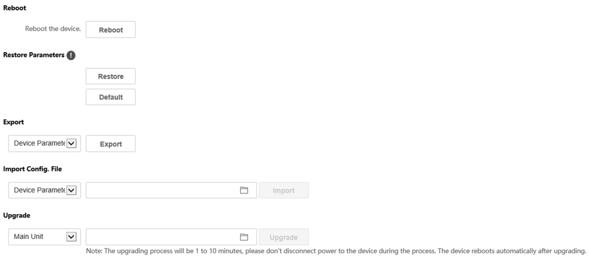
Click **Save** to enable the settings.

DST

Click **System Settings → DST** to enable DST. Set the parameters according to your needs and click **Save** to enable the settings.

Maintenance

Click **Maintenance → Upgrade & Maintenance** to enter the settings page.



Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.

Figure 7-2 Maintenance

- Reboot: Click **Reboot** to reboot the device.
- **Restore**

  Click **Restore** to reset all the parameters, except the IP parameters and user information, to the default settings.

  Default

  Click **Default** to restore all parameters to default settings.

- Export parameters:
  1. Click **Device Parameters** to pop up the dialog box.
  2. Set and confirm the encryption password.
  3. Click **OK** to export parameters.
- Import Config. File:
  1. Click **Browse** to select the configuration file.

2. Click **Import** and enter the encryption password to import.

- Upgrade: Click **Browse** to select the upgrade file.

Note

The upgrading process will last 1 to 10 minutes, do not power off during the upgrading. The device reboots automatically after upgrading.

User Management

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

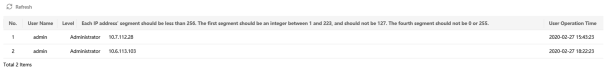
Administrator can edit the permission for the users.

Note

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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Online Users

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



No.	User Name	Level	Each IP address' segment should be less than 256. The first segment should be an integer between 1 and 223, and should not be 127. The fourth segment should not be 0 or 255.	User Operation Time
1	admin	Administrator	10.7.112.28	2020-02-27 15:43:23
2	admin	Administrator	10.6.113.103	2020-02-27 18:22:23

Total 2 Items

Figure 7-3 Online Users

Click **Refresh** to get the present information.

Arming/Disarming Information

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

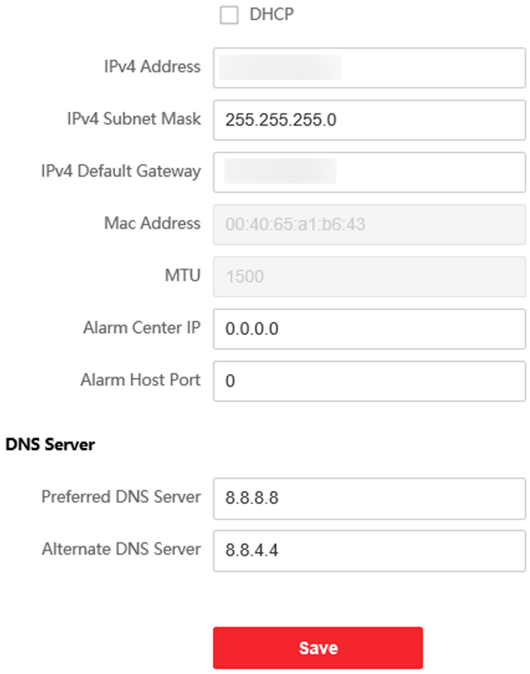
7.4.3 Network Settings

TCP/IP Settings

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

Steps

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



□ DHCP

IPv4 Address [redacted]

IPv4 Subnet Mask 255.255.255.0

IPv4 Default Gateway [redacted]

Mac Address 00:40:65:a1:b6:43

MTU 1500

Alarm Center IP 0.0.0.0

Alarm Host Port 0

DNS Server

Preferred DNS Server 8.8.8.8

Alternate DNS Server 8.8.4.4

Figure 7-4 TCP/IP Settings

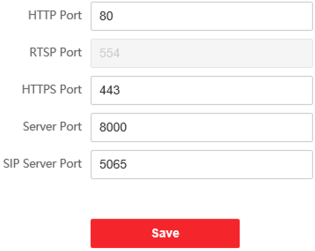
2. Configure the network parameters.
   - Check **DHCP**, the device will get the parameters automatically.
   - Set the **IPv4 Address**, **IPv4 Subnet Mask** and **IPv4 Default Gateway** manually.
3. Configure the DNS server.

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

Port Settings

Steps

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



HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000
SIP Server Port	5065

Figure 7-5 Port Settings

2. Set the ports of the device.

   HTTP Port

   The default port number is 80, and it can be changed to any port No. which is not occupied.

   HTTPS Port

   The default port number is 443, and it can be changed to any port No. which is not occupied.

   RTSP Port

   The default port number is 554.

   Server Port

   The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

   SIP Server Port

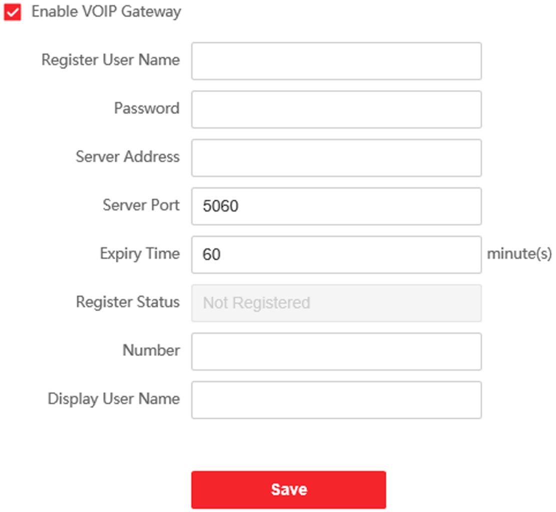
   The default port number is 5065, and it can be changed to any port No. which is not occupied.

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

SIP Setting

Steps

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



☑ Enable VOIP Gateway

Register User Name	
Password	
Server Address	
Server Port	5060
Expiry Time	60 minute(s)
Register Status	Not Registered
Number	
Display User Name	

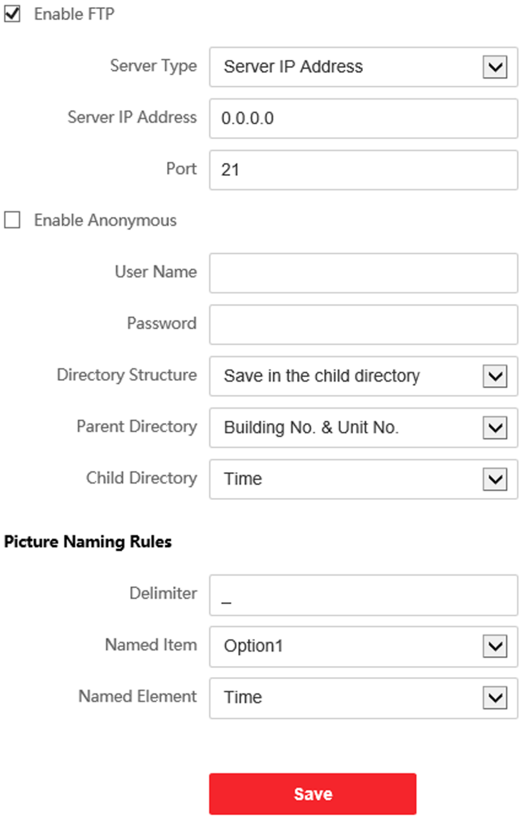
Figure 7-6 SIP Settings

2. Check **Enable VOIP Gateway**.
3. Configure the SIP parameters.
4. Click **Save** to enable the settings.

FTP Settings

Steps

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



☑ Enable FTP

Server Type	Server IP Address
Server IP Address	0.0.0.0
Port	21

□ Enable Anonymous

User Name	
Password	
Directory Structure	Save in the child directory
Parent Directory	Building No. & Unit No.
Child Directory	Time

Picture Naming Rules

Delimiter	_
Named Item	Option1
Named Element	Time

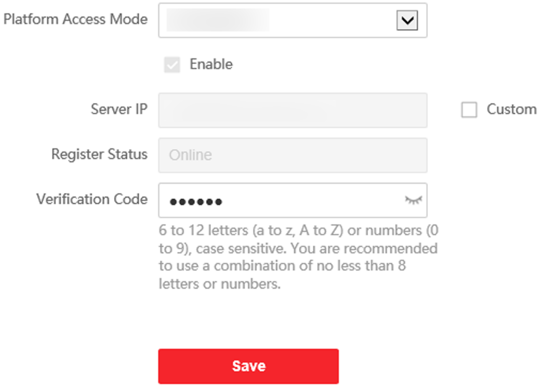
Figure 7-7 FTP Settings

2. Check **Enable FTP**.
3. Select **Server Type**.
4. Input the **Server IP Address** and **Port**.
5. Configure the FTP Settings, and the user name and password are required for the server login.
6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
7. Set the picture naming rules.
8. Click **Save** to enable the settings.

Ezviz Settings

Steps

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



Platform Access Mode

☑ Enable

Server IP □ Custom

Register Status: Online

Verification Code: ●●●●●●

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

Figure 7-8 Ezviz Settings

2. Check the checkbox of **Enable** to enable the function.
3. Select the **Platform Access Mode**.

   Note

   Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

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

   Note

   6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

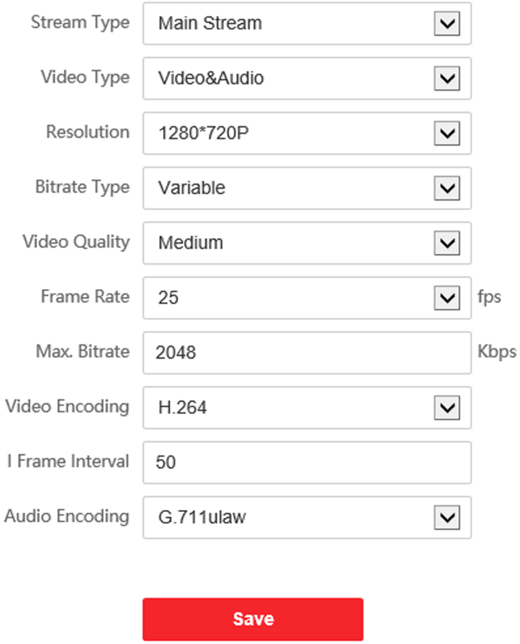
5. Click **Save** to enable the settings.

7.4.4 Video & Audio Settings

Video Parameters

Steps

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



Stream Type	Main Stream	
Video Type	Video&Audio	
Resolution	1280*720P	
Bitrate Type	Variable	
Video Quality	Medium	
Frame Rate	25	fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	
I Frame Interval	50	
Audio Encoding	G.711ulaw	

Figure 7-9 Video Parameters

2. Select the **Stream Type**.
3. Configure the video parameters.

   Stream Type

   Select the stream type to main stream or sub stream.

   Video Type

   Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

   Resolution

   Select the resolution of the video output.

   Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Video Encoding

The device supports H.264.

I Frame Interval

Set I Frame Interval from 1 to 400.

Audio Encoding

The device support G.711ulaw.

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

Audio Parameters

Steps

1. Click **Video/Audio → Audio** to enter the settings page.
2. Adjust the **Input Volume**, **Output Volume** and **Speak Volume**.

Note

Available range of volume: 0 to 10.

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

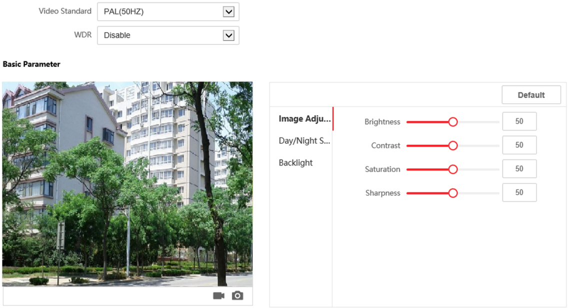
7.4.5 Image Settings

Display Settings

Configure the image adjustment, backlight settings and other parameters in display settings.

Steps

1. Click **Image → Display Settings** to enter the display settings page.



Video Standard PAL(50HZ)

WDR Disable

Basic Parameter

Brightness 50

Contrast 50

Saturation 50

Sharpness 50

Figure 7-10 Display Settings

2. Select the **Format**.

3. Set the display parameters.

   WDR

   Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

   Brightness

   Brightness describes bright of the image, which ranges from 1 to 100.

   Contrast

   Contrast describes the contrast of the image, which ranges from 1 to 100.

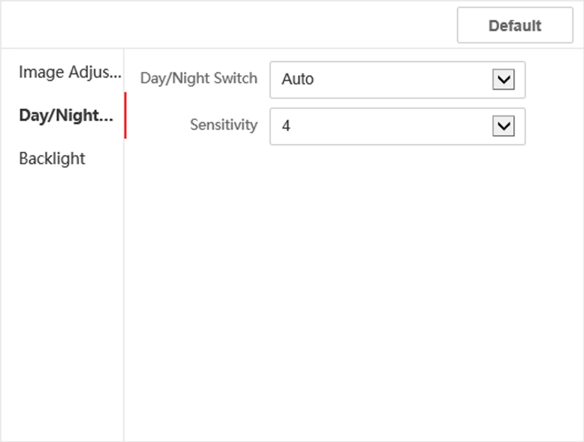
   Saturation

   Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

   Sharpness

   Sharpness describes the edge contrast of the image, which ranges from 1 to 100.

4. Set the **Day/Night Mode**.



Day/Night Switch: Auto
Sensitivity: 4

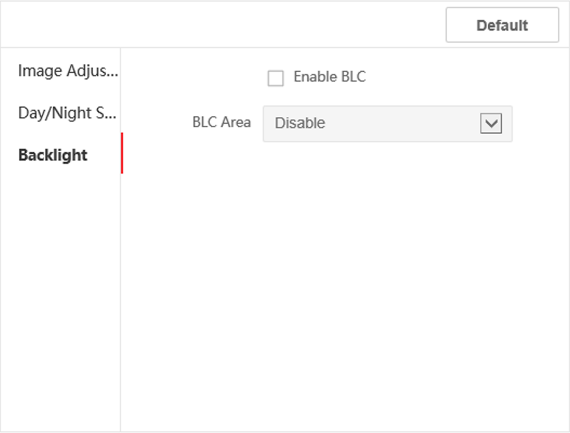
Figure 7-11 Day/Night Mode

- Set **Day Mode** or **Night Mode** manually.
- Set the mode as **Auto** and edit the sensitivity according to your needs.
- Set the mode as **Scheduled-Switch**. Set the start time and end time.

Note

Daytime is from configured start time to configured time. The rest of the time is set as night by default.

5. Set the backlight parameters.



□ Enable BLC

BLC Area: Disable

Figure 7-12 Backlight

1) Check the checkbox to enable BLC.
2) Select **BLC Area**.

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

OSD Settings

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

Steps

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

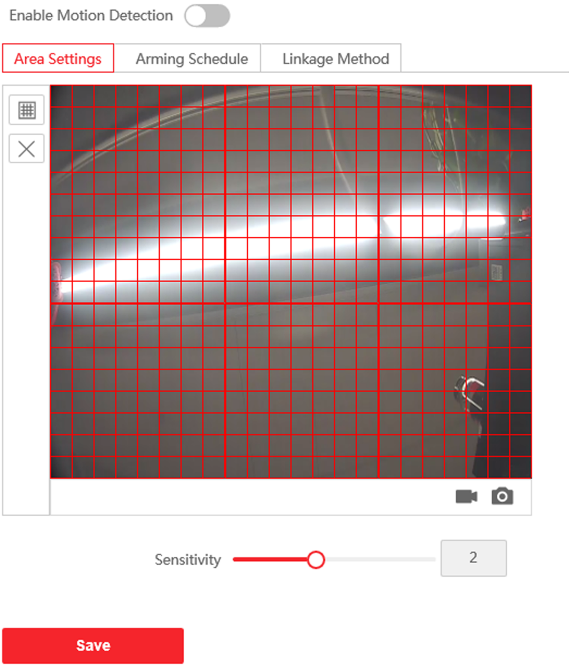
7.4.6 Event Settings

Motion Detection

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

Steps

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



Enable Motion Detection

Figure 7-13 Motion Detection

2. Check **Enable Motion Detection** to enable the function.
3. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area. Click **Save** to save the settings.

Clear Area	Click **Clear All** to clear all of the areas.
Adjust Sensitivity	Move the slider to set the sensitivity of the detection.

4. Click **Arming Schedule** to edit the arming schedule.

5. Click on the time bar and drag the mouse to select the time period. Click **Save** to save the settings.

Delete Schedule	Click **Delete** to delete the current arming schedule.

6. Click **Linkage Method** to enable the linkages.
   Notify Surveillance Center

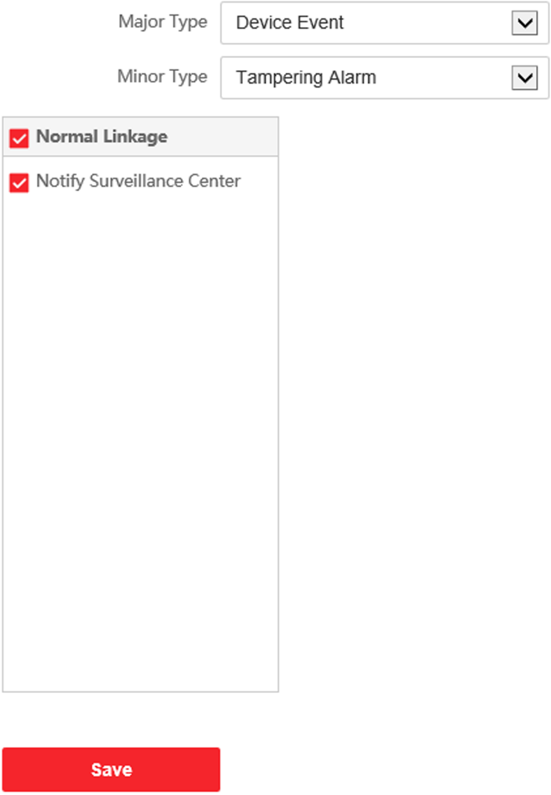
   Send an exception or alarm signal to the remote management software when an event occurs.

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

Access Control Events

Steps

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



Major Type: Device Event

Minor Type: Tampering Alarm

☑ Normal Linkage

☑ Notify Surveillance Center

Figure 7-14 Access Control Event

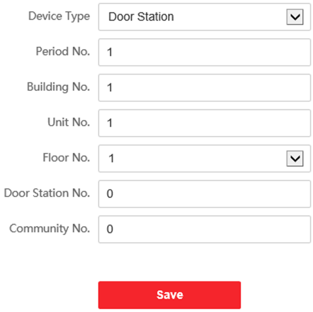
2. Select the **Major Type** as **Device Event** or **Door Event**.
3. Select the type of the **Normal Linkage** for the event.
4. Click **Save** to enable the settings.

7.4.7 Intercom Settings

Device ID Configuration

Steps

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



Device Type	Door Station
Period No.	1
Building No.	1
Unit No.	1
Floor No.	1
Door Station No.	0
Community No.	0

Figure 7-15 Device ID Settings

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

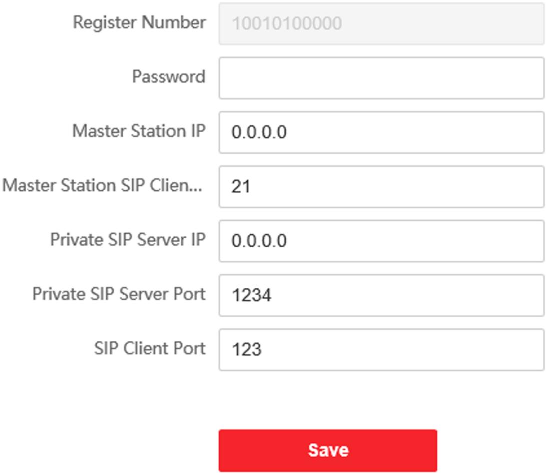
Note

- For main door station (D series or V series), the serial No. is 0.
- For sub door station (D series or V series), the serial No. cannot be 0. Serial No. ranges from 1 to 99.
- For each villa or building, at least one main door station (D series or V series) should be configured, and one sub door stations (D series or V series) can be customized.
- For one main door station (D series or V series), up to 8 sub door stations can be configured.

Linked Network Settings

Steps

1. Click **Intercom → Linked Network Settings** to enter the settings page.



Register Number	10010100000
Password	
Master Station IP	0.0.0.0
Master Station SIP Clien...	21
Private SIP Server IP	0.0.0.0
Private SIP Server Port	1234
SIP Client Port	123

Figure 7-16 Linked Network Settings

2. Set the master station IP address and master station SIP cllient Port.
3. Set the private SIP server IP address and private SIP Server Port.
4. Set the SIP Client Port.
5. Enter the password.
6. Click **Save** to enable the settings.

Time Parameters

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

Configure the time parameters and click **Save**.

Note

Maximum speaking time varies from 90s to 120s, and maximum message time varies from 30s to 60s.

Intercom Protocol

Slide to enable protocol 1.0.

Ring-Back Tone Settings

Click **Intercom → Ringbacktone Settings** to enter the settings page.

Click **Add** to select the ring tone from PC.

Note

Available Audio Format: WAV、AAC, Size: Less than 600 KB, Sample Rate: 8000Hz, Mono.

Press Button to Call

Steps

1. Click **Intercom → Press Button to Call** to enter the settings page.
2. Set the parameters.
   - Edit call No. for every button.
   - Check **Call Management Center** to set the button calling center.

   Note

   If you check **Call Management Center** and set the call No. as well, call management center has higher privilege than call No.

I/O Settings

Steps

1. Click **Intercom → I/O Settings** to enter the I/O input and output settings page.
2. Select **I/O input No.**, **input** mode, **output No.**, and **output** mode.
3. Click **Save** to enable the settings.

   Note

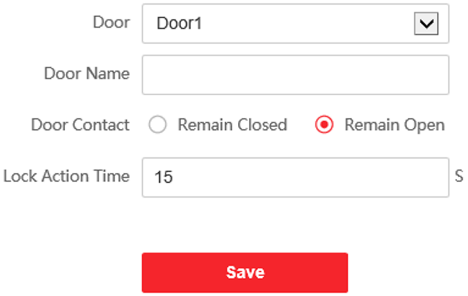
   - For door station, there are 4 I/O input terminals. By default, Terminal 1 and 2 correspond to Door Status. Terminal 3 and 4 correspond to interfaces of Door Switch.
   - For door station, there are 2 I/O Output Terminals. Terminal 1 and 2 correspond to Door interfaces (NO1/COM/NC1; NO2/COM/NC2) of door station. Door 1 is enabled by default. You can enable/disable IO Out according to needs.

7.4.8 Access Control Settings

Door Parameters

Steps

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



Door: Door1

Door Name:

Door Contact: ○ Remain Closed ● Remain Open

Lock Action Time: 15 S

Figure 7-17 Door Parameters

2. Select the door and edit the door name.
3. Set door contact status.
4. Set lock action time.
5. Click **Save** to enable the settings.

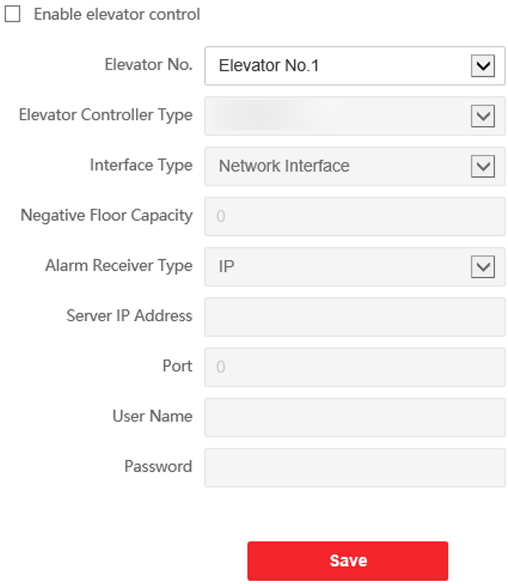
Elevator Control

Before You Start

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

Steps

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



□ Enable elevator control

Elevator No.	Elevator No.1
Elevator Controller Type	
Interface Type	Network Interface
Negative Floor Capacity	0
Alarm Receiver Type	IP
Server IP Address	
Port	0
User Name	
Password	

Figure 7-18 Elevator Control

2. Check to enable elevator control function.
3. Select an Elevator No., and select an elevator controller type for the elevator.
4. Set the Negative Floor.
5. Select the Interface Type as RS-485 or Network Interface. And enable the elevator control.
    - If you select RS-485, make sure you have connected the door station to the elevator controller with RS-485 wire.
    - If you select Network interface, enter the elevator controller's IP address, port No., user name, and password.
6. Click **Save** to enable the settings.

Note

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

7.5 Number Settings

Link the room No. and SIP numbers.

Click **Number Settings** to enter the page.

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

7.6 Device Management

You can manage the linked device on the page.

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

Add Device

- Click **Add** to add the indoor station or sub door station. Enter the parameters and click **OK** to add.
- Click **Import**. Enter the information of the device in the template to import devices in batch.

Export

Click **Export** to export the information to the PC.

Upgrade

- Click **Upload Package** to select the upgrade package.
- Click **Timing Upgrading**, slide **Enable auto-upgrade** to set the start time and end time. The device will upgrade from start time to end time automatically.
- Click **Upgrading Status** to view the version fo the device.

8 Configuration via Client Software

8.1 Device Management

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

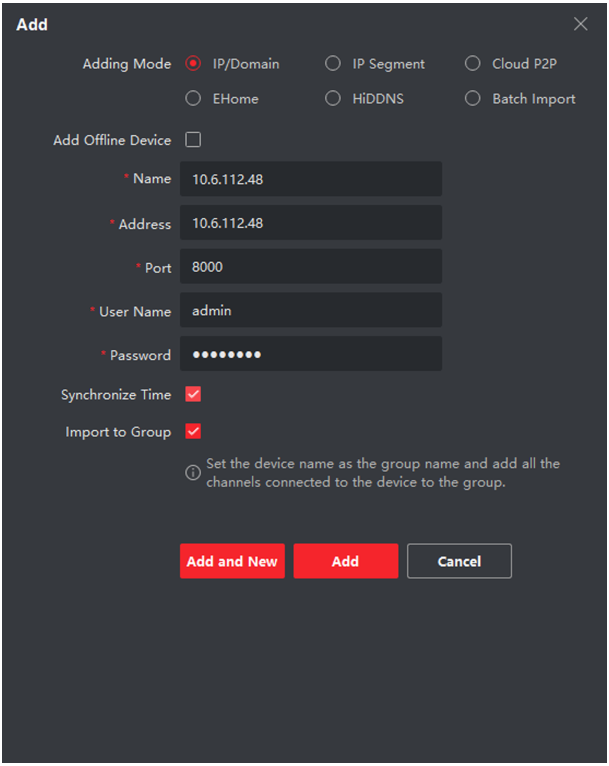
After running the iVMS-4200, video intercom devices should be added to the client software for remote configuration and management.

8.1.1 Add 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. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter corresponding information, and click **Add**.



Add

Adding Mode ● IP/Domain ○ IP Segment ○ Cloud P2P ○ EHome ○ HiDDNS ○ Batch Import

Add Offline Device □

* Name 10.6.112.48

* Address 10.6.112.48

* Port 8000

* User Name admin

* Password ••••••••

Synchronize Time ☑

Import to Group ☑

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

Figure 8-1 Add to the Client

8.1.2 Add Device by IP Address

Steps

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

8.1.3 Add Device by IP Segment

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

Steps

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

8.2 Live View via Door Station

Steps

1. On the main page of the client software, click **Main View** to enter the Live View page.
2. In the left list of the window, double-click the device IP or click the play icon to live view.
3. **Optional:** On the Live View page, control-click and select **Capture** to get the picture of the live view.

8.3 Video Intercom Settings

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

Note

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

You should add the device to the software and configure the person to link the device in Access Control module before your configuration remotely.

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

8.3.1 Receive Call from Door Station

Steps

1. Select the client software in the page to start calling the client and an incoming call dialog will pop up in the client software.
2. Click **Answer** to answer the call. Or click **Hang Up** to decline the call.

3. After you answer the call, you will enter the In Call page.

Adjust the Volume of Loudspeaker	Click 🔊 to adjust the volume of loudspeaker.
Hang Up	Click **Hang Up** to hang up.
Adjust the Volume of Microphone	Click 🎙 to adjust the volume of microphone.
Unlock Remotely	For door station, you can click 🔓 to open the door remotely.

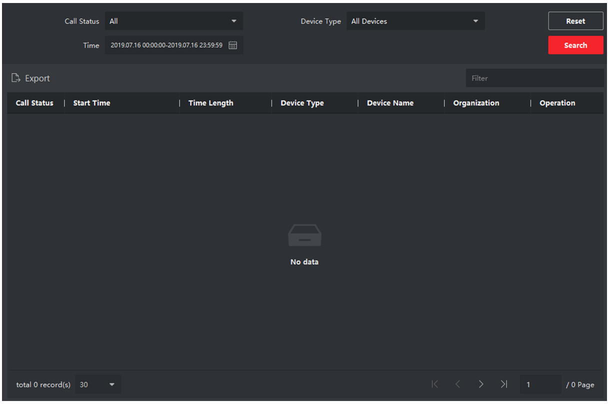
Note

- One video intercom device can only connect with one client software.
- The maximum ring duration can be set from 15s to 60s via the Remote Configuration of the video intercom device.
- The maximum speaking duration between indoor station and iVMS-4200 can be set from 120s to 600s via the Remote Configuration of indoor station.
- The maximum speaking duration between door station and iVMS-4200 can be set from 90s to 120s via the Remote Configuration of door station.

8.3.2 Search Call Logs

Steps

1. On the Video Intercom page, click **Call Log** to enter the page.



Call Status: All

Device Type: All Devices

Time: 2019.07.16 00:00:00-2019.07.16 23:59:59

Call Status	Start Time	Time Length	Device Type	Device Name	Organization	Operation

No data

total 0 record(s) 30

1 / 0 Page

Figure 8-2 Search Call Logs

2. Set the search conditions, including call status, device type, start time and end time.

   Call Status

   Click ˅ to unfold the drop-down list and select the call status as **Dialed**, **Received** or **Missed**. Or select **All** to search logs with all statuses.

   Device Type

   Click ˅ to unfold the drop-down list and select the device type as **Indoor Station**, **Door Station**, **Outer Door Station** or **Analog Indoor Station**. Or select **All Devices** to search logs with all device types.

   Start Time/End Time

   Click the time icon to specify the start time and end time of a time period to search the logs.

   Reset the Settings Click **Reset** to reset all the configured search conditions.

3. Click **Search** and all the matched call logs will display on this page.
4. **Optional:** Check the detailed information of searched call logs, such as call status, ring/speaking duration, device name, resident organization, etc.
5. **Optional:** Input keywords in the Search field to filter the desired log.
6. **Optional:** Click **Export** to export the call logs to your PC.

8.3.3 Upload Armed Information

Steps

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

   Note

   - While device has been added to the client software, the device armed by default.
   - When the device is armed, the alarm logs upload to the client software automatically.
   - Click **Alarm Application** → **Event Search** to search the alarm logs.

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

9 Remote Configuration via Batch Configuration Tool

Enter a short description of your concept here (optional).

This is the start of your concept.

9.1 Link Device in Batch

9.1.1 Create the Organization Structure

Steps

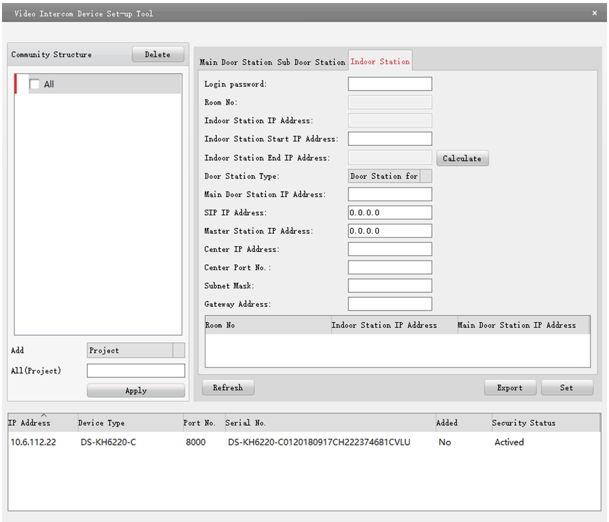
1. Click **Flash rom** to enter the settings page.
2. Set a community structure based on the real community situation, and then assign devices to the community accordingly.

9.1.2 Link Indoor Stations

You can activate the online indoor station, and configure the room No. for the online indoor station.

Steps

1. Click the **Indoor Station** tab to enter the indoor station configuration page.



Login password:

Room No:

Indoor Station IP Address:

Indoor Station Start IP Address:

Indoor Station End IP Address:

Door Station Type: Door Station for

Main Door Station IP Address:

SIP IP Address: 0.0.0.0

Master Station IP Address: 0.0.0.0

Center IP Address:

Center Port No.:

Subnet Mask:

Gateway Address:

Room No	Indoor Station IP Address	Main Door Station IP Address

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.6.112.22	DS-KH6220-C	8000	DS-KH6220-C0120180917CH222374681CVLU	No	Actived

Figure 9-1 Link Indoor Station

2. Select a community, and enter the indoor station start IP address, and then click **Calculate** to generate the indoor station end IP address and indoor station room No. (like 1-1-1-1-2) automatically.
3. Set the main door station parameters: door station type (door station for unit, or door station for villa), main door station IP address.
4. Set the linked network parameters for the indoor station: SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
5. Select an online door station, enter the login password, and click **Set**.

Note

- The indoor station configured successfully will be listed in the configured device area. At the same time, the next indoor station can be easily configured by selecting another indoor station in the online device area and clicking **Set**.
- For the login password, if the indoor station has been activated, enter the activation password here. If the indoor station is not activated, create a login password here, and the indoor station will be activated simultaneously.
- When the device is successfully configured, it prompts the note: Configuring indoor station parameters succeeded.

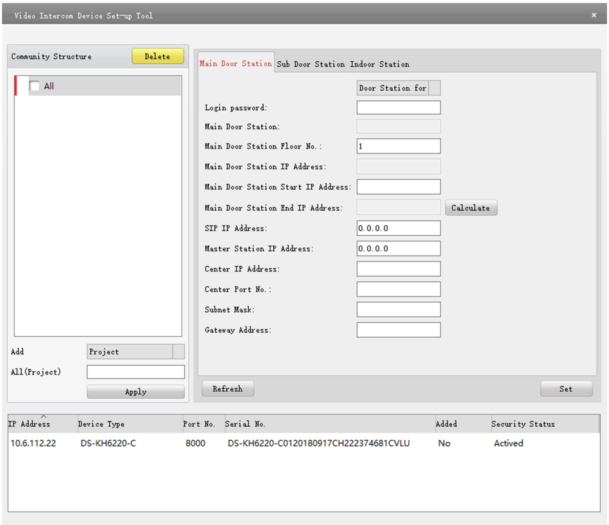
9.1.3 Link Door Stations

Link Main Door Station

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

Steps

1. Select the community, and click the **Main Door Station** tab to enter the main door station configuration page.



Login password:

Main Door Station:

Main Door Station Floor No.: 1

Main Door Station IP Address:

Main Door Station Start IP Address:

Main Door Station End IP Address:

SIP IP Address: 0.0.0.0

Master Station IP Address: 0.0.0.0

Center IP Address:

Center Port No.:

Subnet Mask:

Gateway Address:

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.6.112.22	DS-KH6220-C	8000	DS-KH6220-C0120180917CH222374681CVLU	No	Actived

Figure 9-2 Link Main Door Station

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

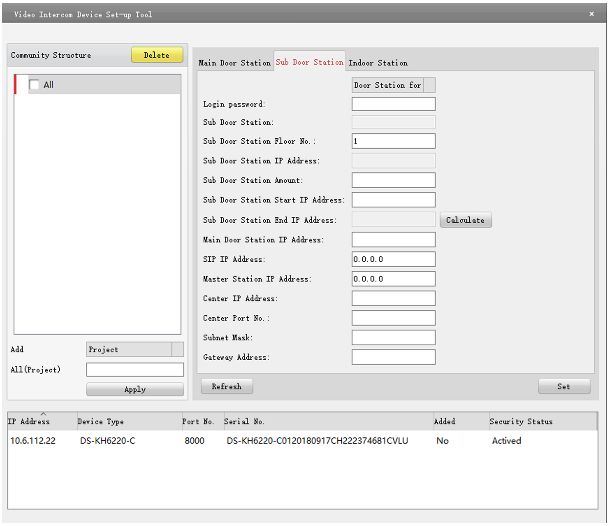
Note

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

Link Sub Door Stations

Steps

1. Select the community, and click the **Sub Door Station** tab to enter the sub door station configuration page.



Add: Project

All(Project):

Door Station for

Login password:

Sub Door Station:

Sub Door Station Floor No.: 1

Sub Door Station IP Address:

Sub Door Station Amount:

Sub Door Station Start IP Address:

Sub Door Station End IP Address:

Main Door Station IP Address:

SIP IP Address: 0.0.0.0

Master Station IP Address: 0.0.0.0

Center IP Address:

Center Port No.:

Subnet Mask:

Gateway Address:

IP Address	Device Type	Port No.	Serial No.	Added	Security Status
10.6.112.22	DS-KH6220-C	8000	DS-KH6220-C0120180917CH222374681CVLU	No	Actived

Figure 9-3 Link Sub Door Station

2. Select the door station type from the drop-down list menu: Door Station for Unit, or Door Station for Villa.
3. Set the sub door station parameters (sub door station amount, floor No., start IP address, end IP address), and then click **Calculate** to generate the sub door station end IP address and sub door station No. (like 1-1-1-1) automatically.

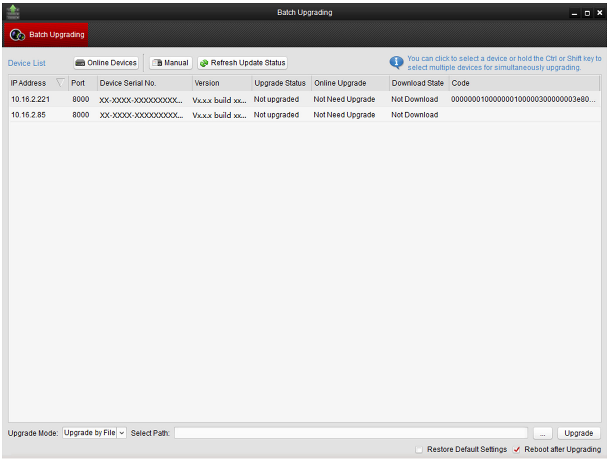
4. Set the linked network parameters for the sub door station: main door station IP address, SIP IP address, master station IP address, center IP address, center port No., subnet mask, and gateway address.
5. Select an online door station, enter the login password, and click **Set**.

Note

- The default sub door station floor No. is 1.
- Up to 8 sub door stations can be added to a main door station.
- For the login password, if the sub door station has been activated, enter the activation password here. If the sub door station is not activated, create a login password here, and the sub door station will be activated simultaneously.
- When the device is successfully configured, it prompts the note: Configuring sub door station parameters succeeded.

9.2 Batch Upgrading

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



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

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

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

□ Restore Default Settings ☑ Reboot after Upgrading

Figure 9-4 Batch Upgrading

9.2.1 Add Devices for Upgrading

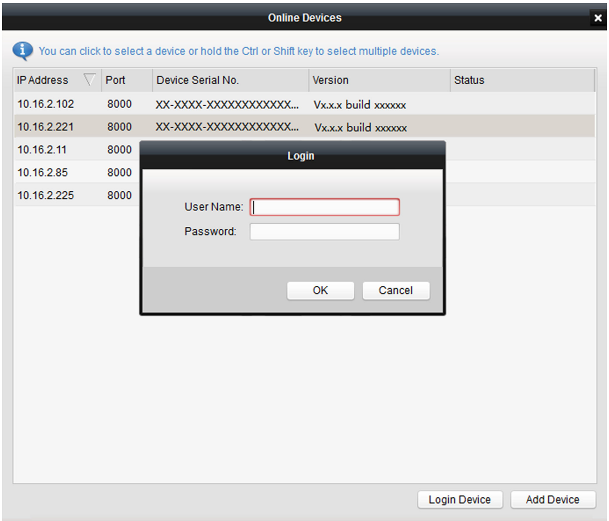
You should add the device to the batch upgrading tool first before upgrading the device. There are 2 ways to add the device: adding online device, and adding by IP address/IP segment.

Add Online Device for Upgrading

Enter a short description of your task here (optional).

Steps

1. In the batch upgrading page, click **Online Devices**.



Online Devices

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

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

Login

User Name:

Password:

Figure 9-5 Upgrading

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

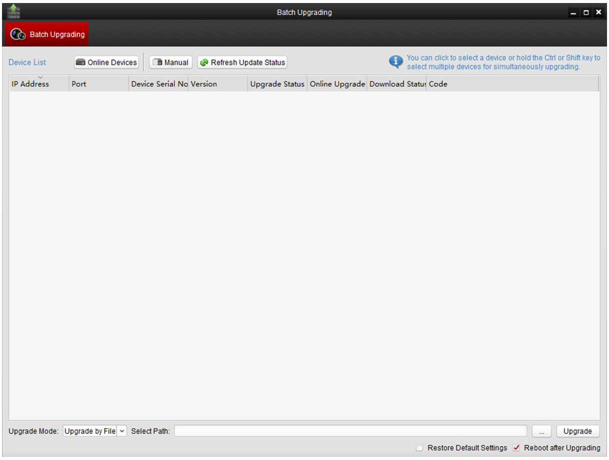
Adding by IP Address/IP Segment for Upgrading

Steps

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

9.2.2 Upgrade Devices

On the main page of the client, click **Batch Update** to enter the batch upgrading page.



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

Upgrade Mode: Upgrade by File

☐ Restore Default Settings ☑ Reboot after Upgrading

Figure 9-6 Upgrade in Batch

Online Upgrading

Steps

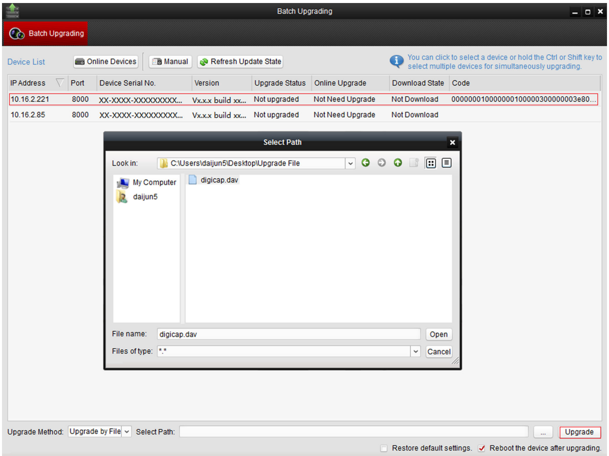
1. Select the **Online Upgrade** as **Upgrade Mode**.
2. Click **Download** to get the upgrade package.
3. When the **Download Status** displays Downloaded, click **Upgrade** to upgrade the device.

Upgrade by File

You can upgrade devices in batch via the local upgrade files.

Steps

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



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

IP Address	Port	Device Serial No.	Version	Upgrade Status	Online Upgrade	Download State	Code
10.16.2.221	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	0000000100000001000003000000003e80...
10.16.2.85	8000	XX-XXXX-XXXXXXXXX...	Vx.x.x build xx...	Not upgraded	Not Need Upgrade	Not Download	

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

File name: digicap.dav

Files of type: *.*

Upgrade Method: Upgrade by File

Select Path:

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

Figure 9-7 Upgrade by File

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

A. Appendix

Installation Notice

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

Note

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

Wiring Cables

Cable	Specification
Power Cord of Doorbell	RVV 2*1.0
Network Cable of Doorbell	UTP-five Categories
Door Lock Wiring (with Door Contact)	RVV 4*1.0
Door Lock Wiring (without Door Contact)	RVV 2*1.0
Exit Button Wiring	RVV 2*0.5

B. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.

Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

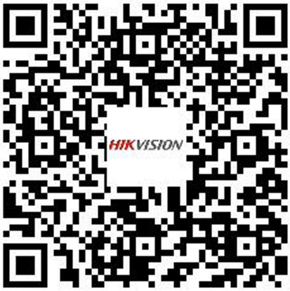


Figure B-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.

Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure B-2 Device Command

See Far, Go Further