# KB8113 Vandal-Resistant Video Intercom 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 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 LATTER 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 devices with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint devices, 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 and 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 |
|---|---|
| ⚠ Warning | 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. |
| 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 the 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 overheating or a 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 a wall or ceiling, ensure the device is firmly affixed.
- If smoke, odors, or noise rise from the device, turn off the power at once, unplug the power cable, and then contact the service center.
- If the product does not work properly, 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 installing the equipment on vibrating surfaces or places subject to shock (ignoring this 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.
- Keep the device cover for indoor use from rain and moisture.
- Do not expose the equipment to direct sunlight, low ventilation, or heat source such as heater or radiator (ignoring this can cause fire danger).
- Do not aim the device at the sun or extra bright light. Blooming or smearing may occur otherwise (which is not a malfunction however), and affect the sensor endurance.
- Use the provided glove when opening the device cover; avoid direct contact with the device cover, because the acidic sweat of the fingers may erode its surface coating.
- Use a soft, dry cloth when cleaning inside and outside surfaces of the device cover, do not use alkaline detergents.
- Keep all wrapping materials after unpacking, for future use. In case any failure occurs, you need to return the device to the factory in the original wrapping. Shipping without the original wrapping may result in damage to the device and lead to additional costs.
- Improper use or replacement of the battery may result in explosion hazard. 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 in 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 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 of 7.9" (20 cm) 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:

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

**EU Conformity Statement**
CE 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:

- This device may not cause interference, and
- 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:

- l'appareil ne doit pas produire de brouillage, et
- 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 operate only 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 of 7.9" (20 cm) 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

# 1.0 Appearance

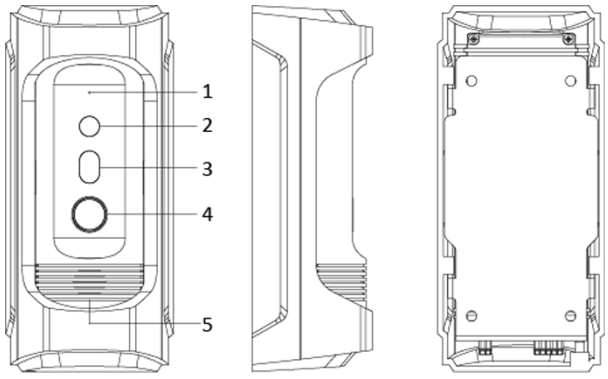


Figure 1-1 Appearance

Table 1-1 Component Description

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

# 2.0 Terminal and Wiring Description

## 2.1 Terminals Description

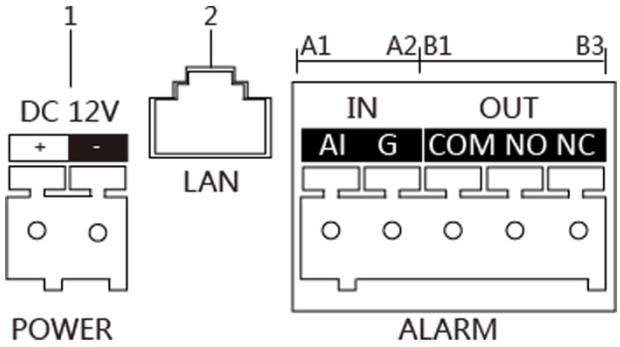


Figure 2-1 Terminals Description

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.

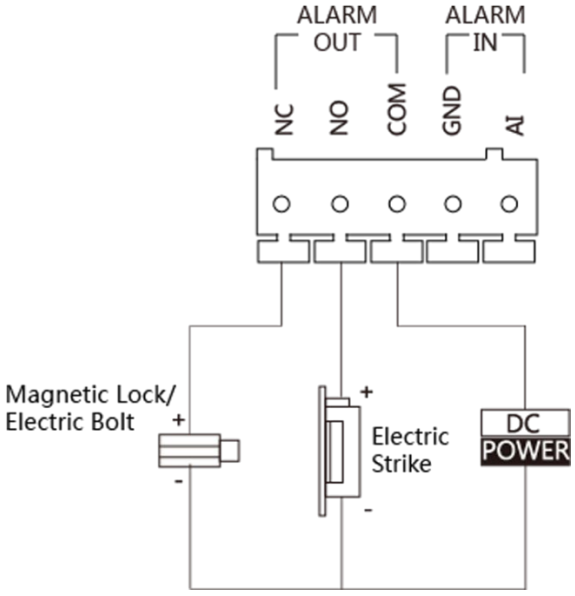


Figure 2-2 Door Lock Wiring

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.

### 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.

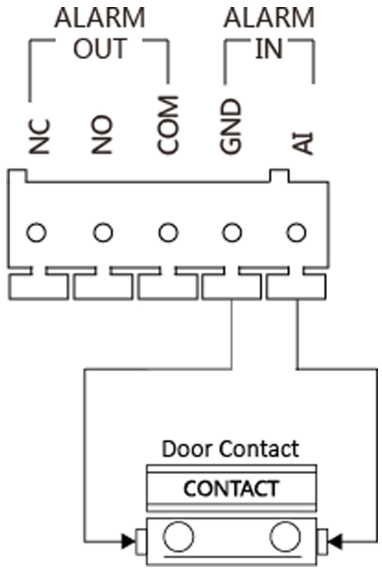


Figure 2-3 Door Contact Wiring

### 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.

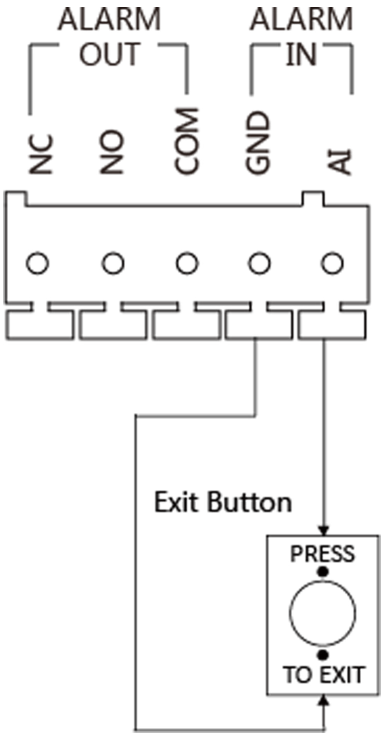


Figure 2-4 Exit Button Wiring

### 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.

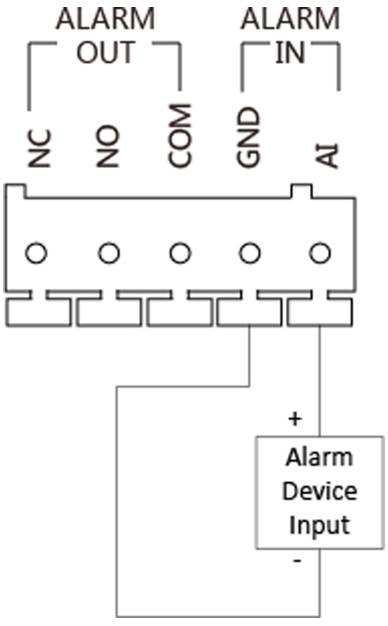


Figure 2-5 Alarm Device Input Wiring

# 3.0 Doorbell Installation

## 3.1 Wall Mounting Plate

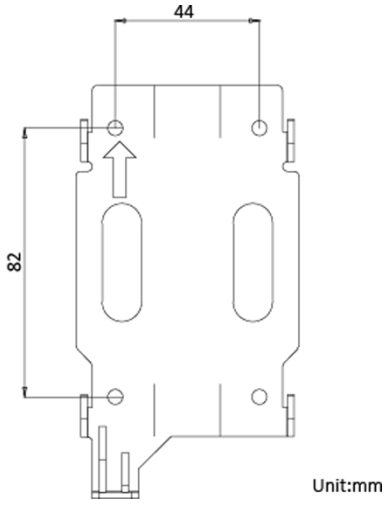


Figure 3-1 Wall Mounting Plate

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

## 3.2 Wall Mounting

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

**NOTE:** Recommended Installation height is 47" to 55".

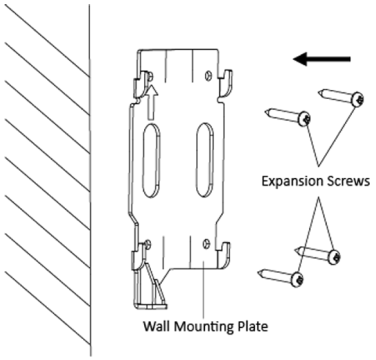


Figure 3-2 Install the Plate

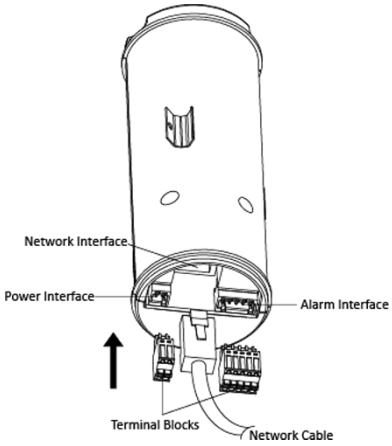


Figure 3-3 Insert Terminals and Network Cable

2. Insert terminal blocks into the interfaces of the doorbell body, and connect the network cable.
3. Fix the doorbell body to the protective shield tightly.

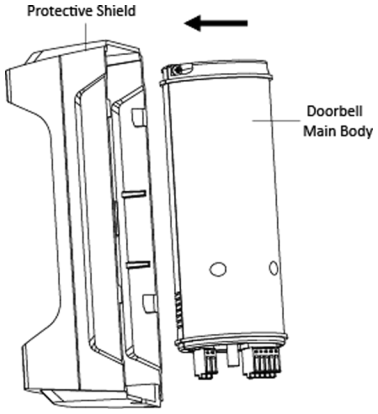


Figure 3-4 Fix the Body to the Shield

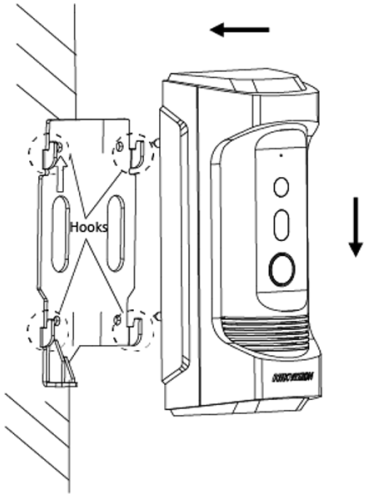


Figure 3-5 Hook the Doorbell to the Plate

4. Hook the doorbell to the wall mounting plate tightly.
5. Use the set screw to secure the doorbell with the mounting plate.

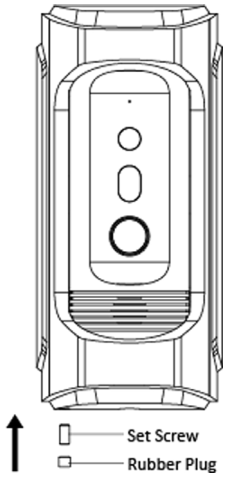


Figure 3-6 Secure the Doorbell

# 4.0 Activate Device via over the Web

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

Default door station parameters are as follows:

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

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.

# 5.0 Remote Configuration via Indoor Station

## 5.1 Set Up Doorbell via Indoor Station

1. Choose Language and tap **Next**.
2. Set network parameters and tap **Next**.
   - Edit Local IP, Subnet Mask, and Gateway parameters.
   - Enable DHCP, the device will get network parameters automatically.
3. Configure the indoor station.
   1) Choose **Indoor Station Type**.
   2) Edit **Floor** and **Room No.**
   3) Tap **Next**.
4. Linked related devices and tap **Next**. If the device and the indoor station are in the same LAN, the device will be displayed in the list. Tap the device or enter the **serial no.** to link.
   1) Tap the doorbell in the list to link.

      **NOTE:** If the doorbell is inactive, the system will pop up the dialog to activate the doorbell.

   2) Tap ⚙ to pop up the **Network Settings** page.
   3) Edit the network parameters of the doorbell manually or enable **DHCP** to get the network parameters automatically.
   4) (Optional): Enable **Synchronize Language** to synchronize the language of doorbell with indoor station.
   5) Tap **OK** to save the settings.
5. Tap **Finish** to save the settings.

## 5.2 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.

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 the doorbell's live view is displayed on other devices or doorbell is calling resident, the doorbell will detect the video brightness. When the brightness is lower than the expected threshold, the supplement light will be enabled.

When the supplement light is enabled, the keys' backlight will be auto-enabled, otherwise, the doorbell will detect the live view brightness and enable the keys' backlight when the live view brightness is lower than expected threshold.

# 6.0 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.

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 log in to the client.

## 6.2 Set Up Doorbell via Client

To operate the doorbell normally, add the doorbell to the client.

1. On the client home page, tap **Add Device**.
   - Scan QR code of the device 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 on the cloud service page in the device.

   Tap Off to enable the flashlight if the scanning environment is too dark.

   If there are device QR codes in photo album of the phone, tap to extract QR code from local album.

   If the system fails to recognize the QR code, tap and enter the serial no. to add the device manually.
2. Connect to the network.
   1) Tap **Next**.
   2) Connect the device to the router with a network cable.

   **NOTE:** Make sure your mobile phone is connected to the same router.

   3) Tap **Connected**.
3. The account is connected to the device.

## 6.3 Remote Operation via Client

You can realize 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.

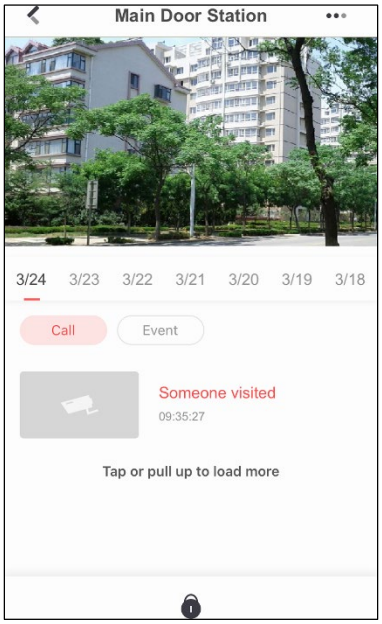


Figure 6-1 Live View

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.

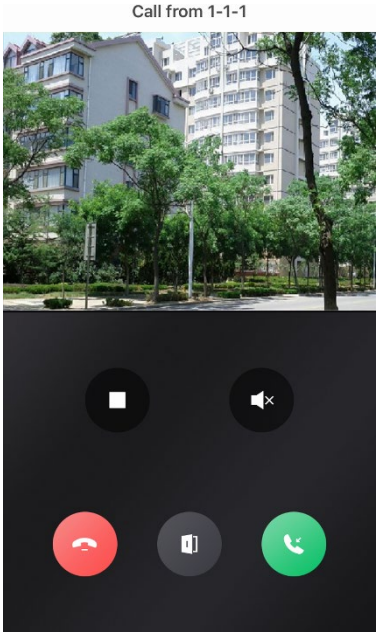


Figure 6-2 Receive Call from Device

Tap to receive the call. Tap to decline the call.

Tap to unlock the door remotely. Tap to adjust the volume.

When communicating 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**

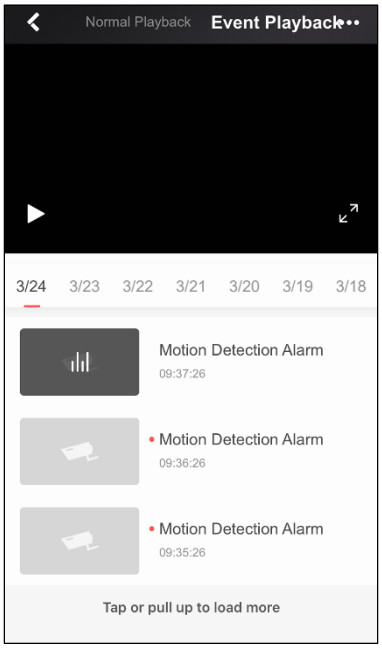


Figure 6-3 Playback

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

**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.

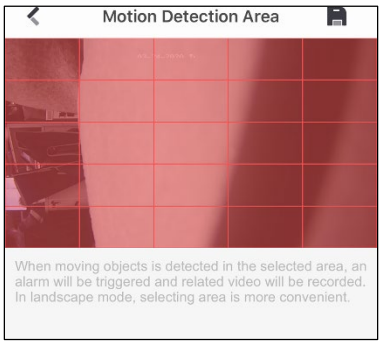


Figure 6-4 Draw Motion Detection Area

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

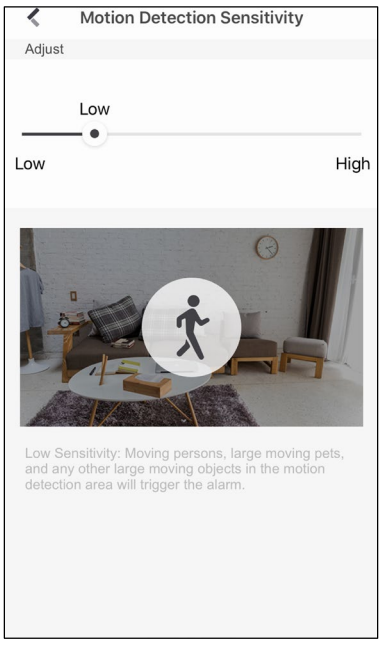


Figure 6-5 Motion Detection Sensitivity

**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 four accounts can be added to share.

# 7.0 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.

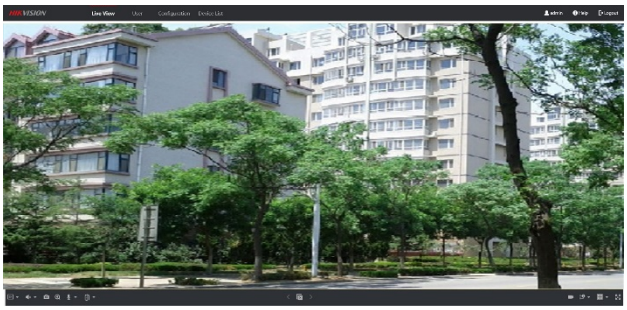

Figure 7-1 Live View

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.

- 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 supports 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.


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.

**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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


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.

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

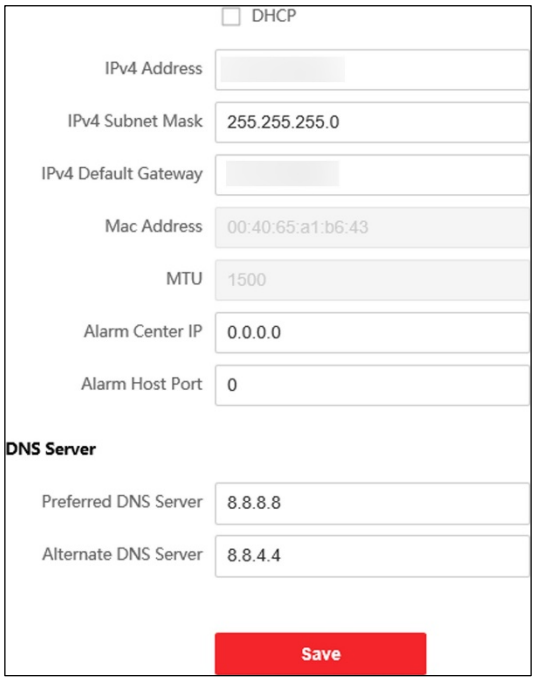


Figure 7-4 TCP/IP Settings

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**

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

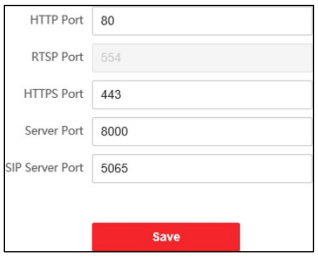


Figure 7-5 Port Settings

2. Set the device ports.
   - **HTTP Port:** The default port number is 80, and it can be changed to any port no. that is not occupied.
   - **HTTPS Port:** The default port number is 443, and it can be changed to any port no. that 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. that is not occupied.

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

### SIP Setting

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

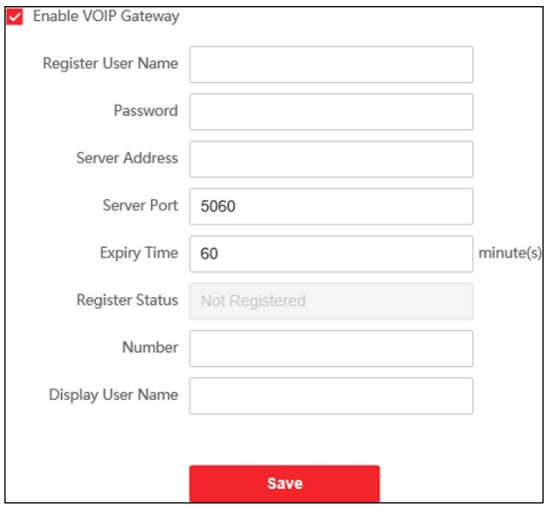


Figure 7-6 SIP Settings

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

### FTP Settings

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

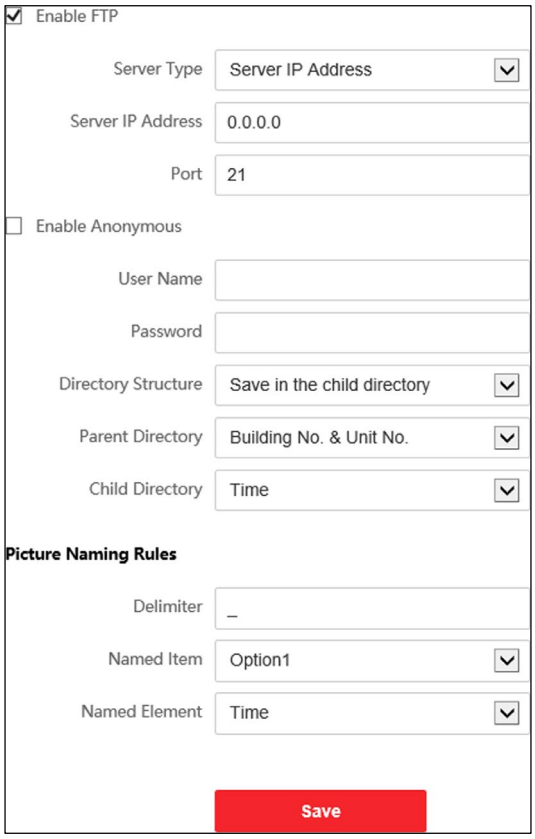


Figure 7-7 FTP Settings

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**

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


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 eight letters or numbers.

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

### 7.4.4 Video & Audio Settings

**Video Parameters**

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

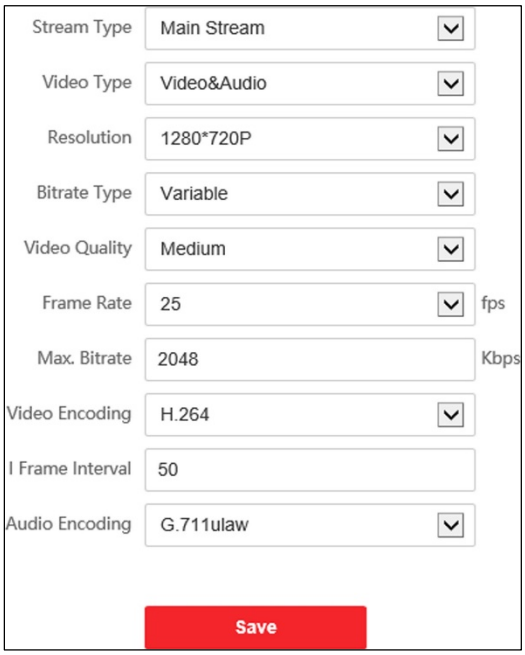


Figure 7-9 Video Parameters

2. Select the **Stream Type**.
3. Configure the video parameters.
    - **Stream Type:** Set the stream type to main stream or sub stream.
    - **Video Type:** Set 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:** Set the bitrate type to constant or variable.
    - **Video Quality:** When bitrate type is set as Variable, six levels of video quality are selectable.
    - **Frame Rate:** Set the frame rate. The frame rate describes the frequency at which the video stream is updated, and it is measured in 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. A higher value corresponds to higher video quality, but 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

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.

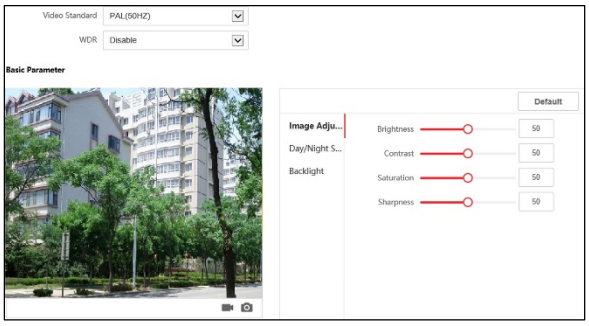


Figure 7-10 Display Settings

1. Click **Image** → **Display Settings** to enter the display settings page.
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 of the image, ranges from 1 to 100.
   - **Contrast:** Contrast of the image, ranges from 1 to 100.
   - **Saturation:** Color intensity of the image, ranges from 1 to 100.
   - **Sharpness:** Sharpness describes the edge contrast of the image, ranges from 1 to 100.
4. Set the **Day/Night Mode**.

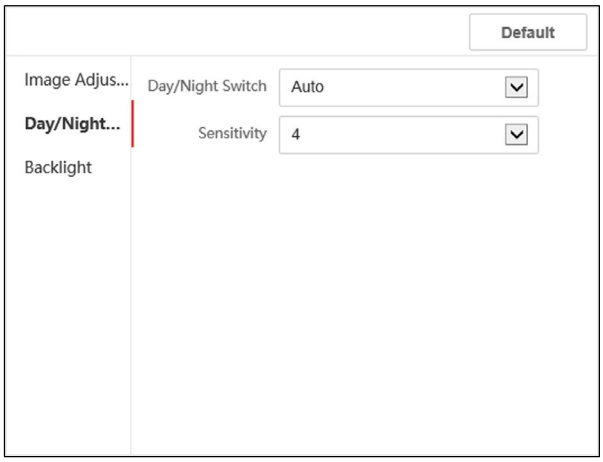


Figure 7-11 Day/Night Mode

- 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.

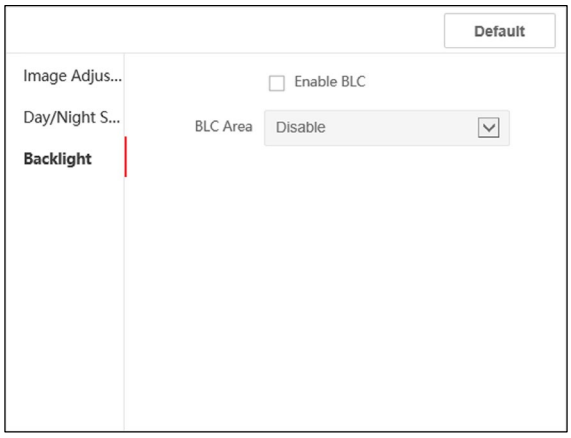


Figure 7-12 Backlight

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.

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.

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

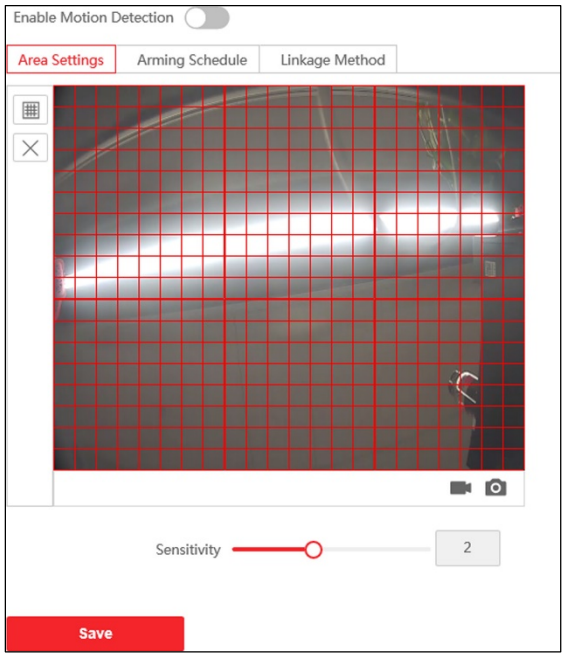


Figure 7-13 Motion Detection

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.
6. Click **Save** to save the settings.
   - **Delete Schedule:** Click **Delete** to delete the current arming schedule.
7. 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.
8. Click **Save** to enable the settings.

## Access Control Events

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

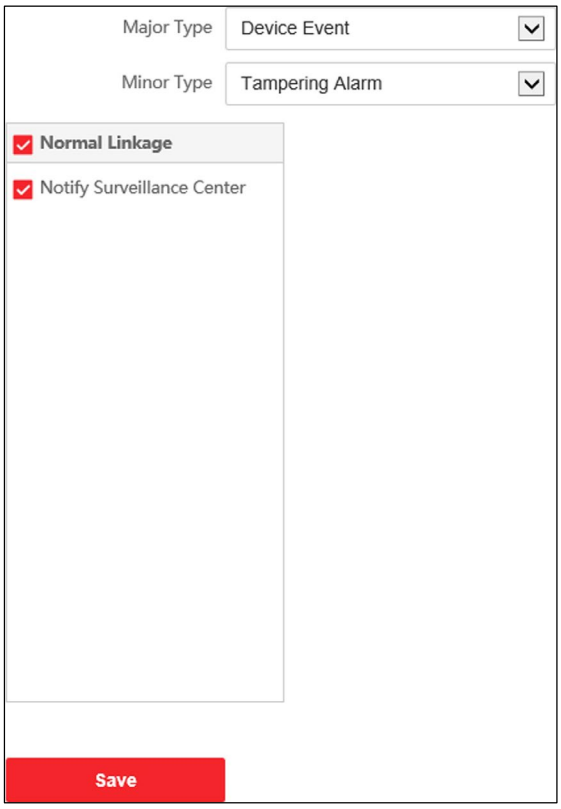


Figure 7-14 Access Control Event

2. Set 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


Figure 7-15 Device ID Settings

1. Click **Device ID Settings** to enter the page.
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 eight sub door stations can be configured.

## Linked Network Settings

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

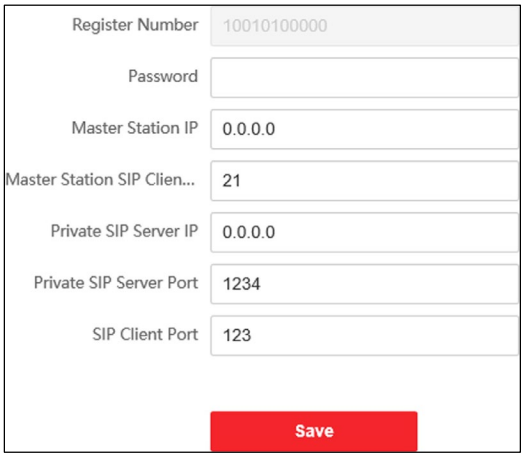


Figure 7-16 Linked Network Settings

2. Set the master station IP address and master station SIP client 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**

1. Click **Intercom** → **Time Parameters** to enter the page.
2. 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

1. Click **Intercom** → **Ringbacktone Settings** to enter the settings page.
2. Click **Add** to select the ring tone from PC.

**NOTE:** Available Audio Format: WAV, AAC
Size: Less than 600 KB
Sample Rate: 8000 Hz, mono

## Press Button to Call

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

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 four I/O input terminals. By default, Terminals 1 and 2 correspond to Door Status. Terminals 3 and 4 correspond to door switch interfaces.

For door station, there are two I/O Output Terminals. Terminals 1 and 2 correspond to door station door interfaces (NO1/COM/NC1; NO2/COM/NC2). Door 1 is enabled by default. You can enable/disable IO Out according to needs.

### 7.4.8 Access Control

#### Settings

#### Door Parameters

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

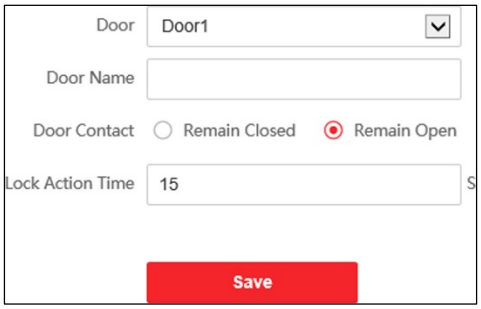


Figure 7-17 Door Parameters

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 cable if you want to use RS-485 interface.

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

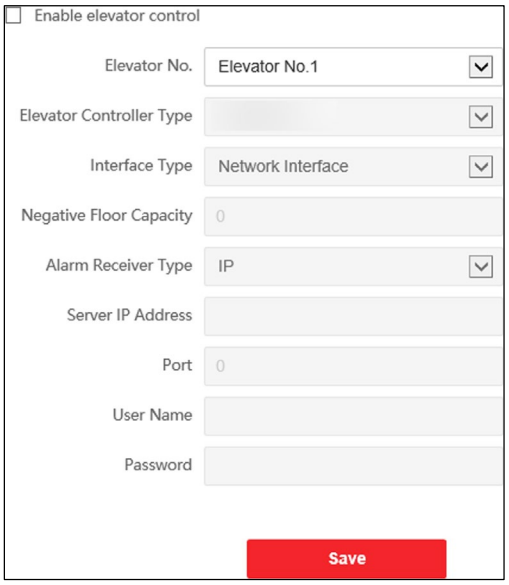


Figure 7-18 Elevator Control

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. Set 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 an RS-485 cable.
   - 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 four elevator controllers can be connected to one door station.

Up to 10 negative floors can be added.

Make sure the elevator controller interface types 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.

# 8.0 Appendix 1

## Installation Notice

While installing the doorbell, make sure that the distance between any two devices is far enough to avoid 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 |

# 9.0 Appendix 2 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