Face Recognition Door Station with 8-inch Screen

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 THE 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 INFECTION, 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.
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.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- 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 or the detailed operating temperature), cold, dusty or damp locations.
- The device shall be kept from rain and moisture.
- The device shall be kept from explosives.
- Keep surfaces of the device clean and dry.
- Avoid contact with exposed circuits. Do not touch the exposed contacts and components when the product is powered on.

⚠ Caution

- Keep the device away from children and out of reach.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- 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.
- Used batteries may result in pollution to the environment. Dispose of used batteries according to the instructions provided by the battery manufacturer.

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

1.1 Door Station

Note

Refers to the specific model for the appearance of the device.

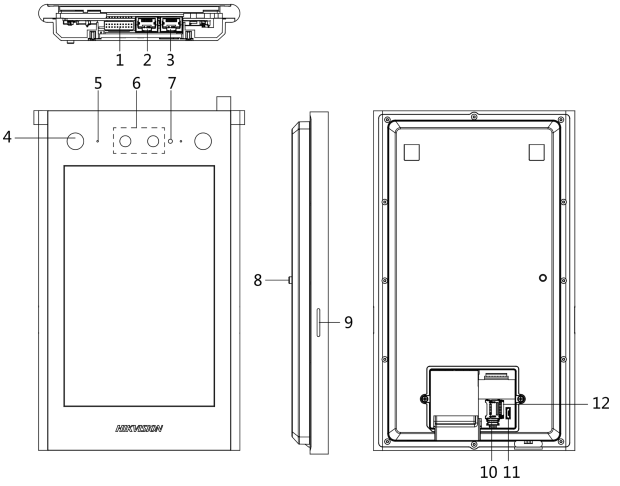

Figure 1-1 Door Station

Table 1-1 Appearance Description

No.	Description	No.	Description
1	Wiring Terminal	7	Ambient Light Sensor
2	Network Interface	8	TAMPER
3	Analog & RS-485 Interface	9	Loudspeaker
4	IR Supplement Light	10	Debugging Port

No.	Description	No.	Description
			Note The debugging port is used for debugging only.
5	Microphone	11	MicroUSB Interface **Note** Micro USB interface is used for debugging only.
6	Camera	12	TF Card Slot

1.2 Door Station with Keypad Module

Note

Refers to the specific model for the appearance of the device.

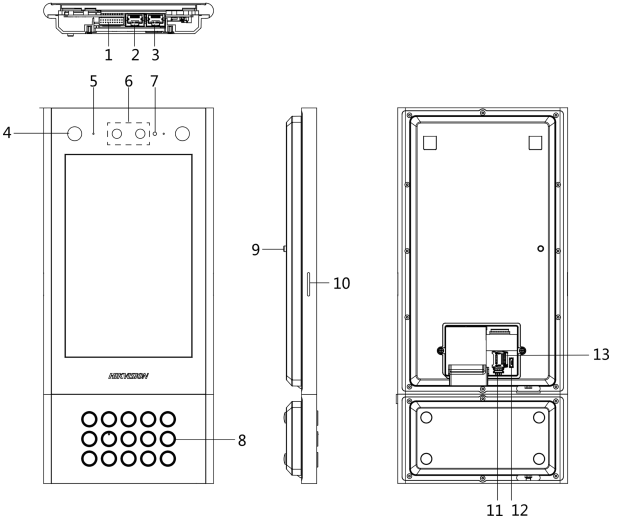

Figure 1-2 Door Station with Keypad Module

Table 1-2 Appearance Description

No.	Description	No.	Description
1	Wiring Terminal	8	Button
2	Network Interface	9	TAMPER
3	Analog & RS-485 Interface	10	Loudspeaker
4	IR Supplement Light	11	Debugging Port **Note** The debugging port is used for debugging only.
5	Microphone	12	MicroUSB Interface **Note** MicroUSB interface is used for debugging only.
6	Camera	13	TF Card Slot
7	Ambient Light Sensor		

2 Terminal and Wiring Description

Door station can be wired to alarm input interface, alarm input interface, door lock, door contact and so on.

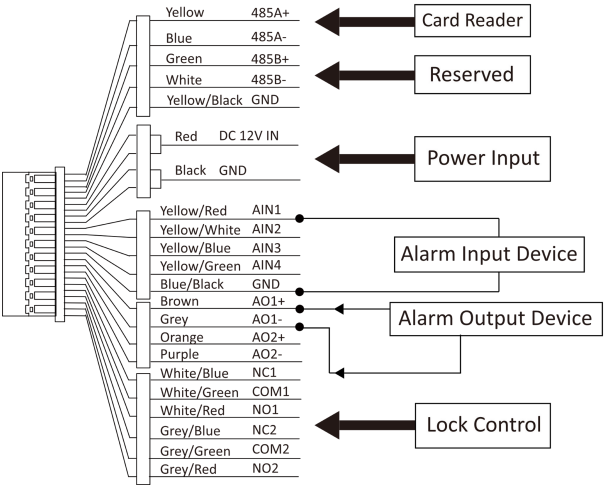

Figure 2-1 Terminal and Wiring Description

3 Installation

3.1 Install Door Station

Note

- Gang box is required for the installation of door station.
- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
- Complete wiring during installation. Refers to*Terminal and Wiring Description* for wiring details.
- Make sure all the related equipment is power-off during the installation.
- Installation Location: the lens of the device shall be 1.5 meters away from the ground.

3.1.1 Door Station Installation Accessories

Mounting Plate

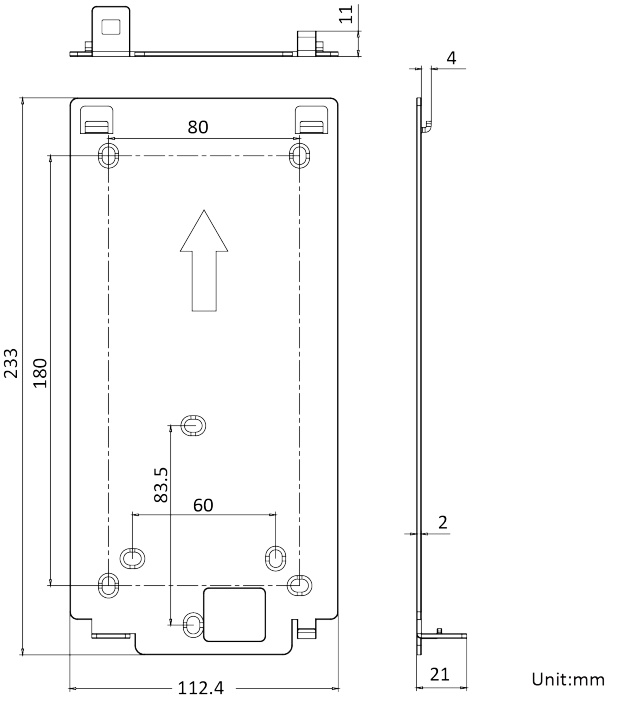

Figure 3-1 Mounting Plate

Note

The dimension of the mounting plate is 233 mm (W) × 112.4 mm (H) × 21 mm (D).

Gang Box

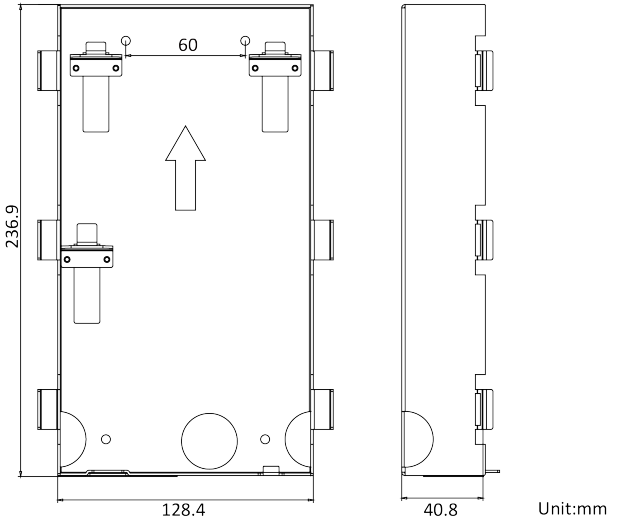

Figure 3-2 Gang Box

Note

- The dimension of the gang box is 236.9 mm (W) × 128.4 mm (H) × 40.8 mm (D).
- The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 237.5 mm (W) × 128.9 mm (H) × 41.3 mm (D).

3.1.2 Surface Mounting

Steps

1. Paste the mounting template on the wall according to the installation location requirements. Drill holes according to the location of the screw holes of the mounting template, and insert the expansion bolts into the screw holes.
2. Fix the mounting plate to the wall with 4 supplied screws.
3. Fix the device to the mounting plate, and fix the device with the set screws.

Note

- Do not touch the SD card slot and other devices during the process of plugging in and unplugging the power interface.
- Apply Silicone sealant among the joints between the device and the wall (except the lower side) to keep the raindrop from entering.

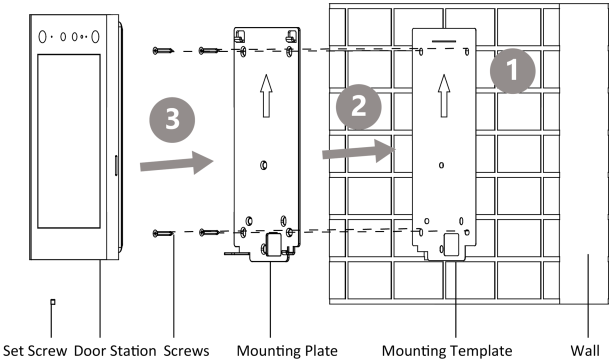

Figure 3-3 Surface Mounting

3.1.3 Flush Mounting

Steps

1. Cave an installation hole in the wall. The suggested dimension of the installation hole is 237.5 mm (W) × 128.9 mm (H) × 41.3 mm (D). Pull the cables out from the wall. Insert the gang box into the installation hole, and mark the gang box screw holes' position with a marker.
2. Take out the gang box. Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes. Fix the gang box with 4 expansion bolts.
3. Insert the door station into the gang box, and fix it with set screws.

Note

Do not touch the SD card slot and other devices during the process of plugging in and unplugging the power interface.

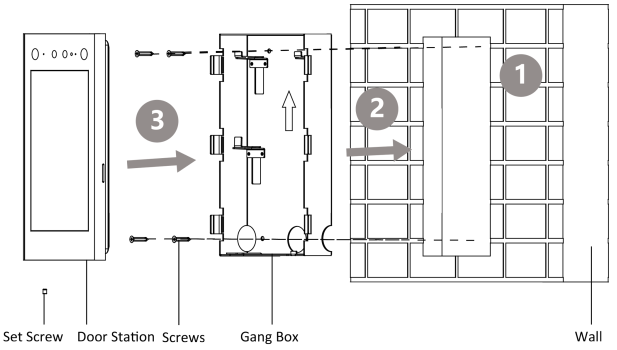

Figure 3-4 Flush Mounting

3.2 Install Door Station with Keypad Module

Note

- Gang box is required for the installation of door station.
- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
- Complete wiring during installation. Refers to *Terminal and Wiring Description* for wiring details.
- Make sure all the related equipment is power-off during the installation.
- Installation Location: the lens of the device shall be 1.5 meters away from the ground.

3.2.1 Door Station with Keypad Module Installation Accessories

Mounting Plate

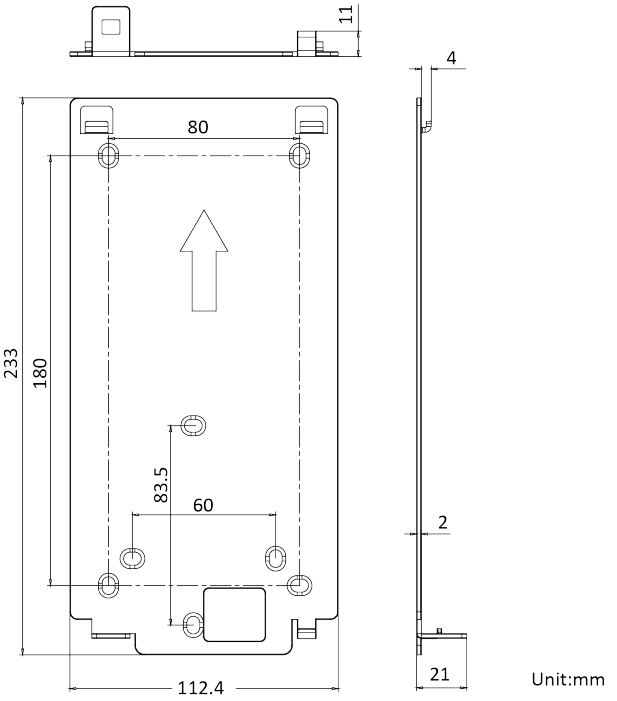

Figure 3-5 Mounting Plate

Note

The dimension of the mounting plate is 233 mm (W) × 112.4 mm (H) × 21 mm (D).

Gang Box

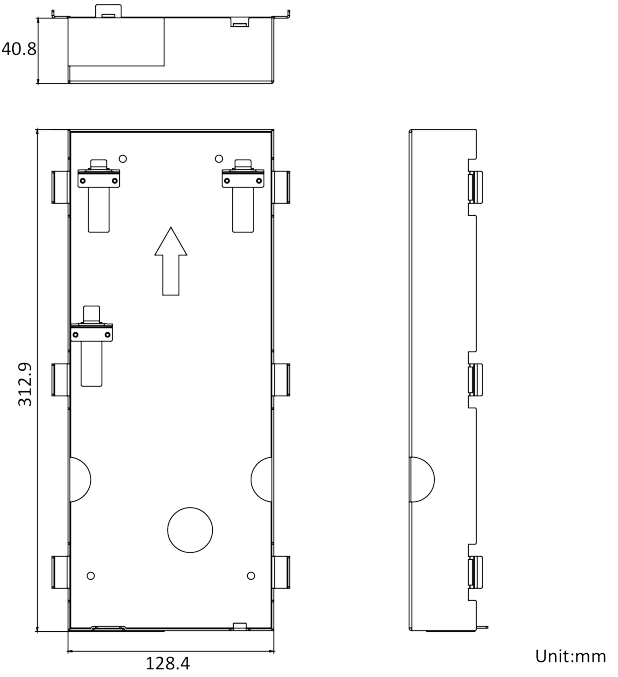

Figure 3-6 Gang Box

Note

- The dimension of the gang box is 312.9 mm (W) × 128.4 mm (H) × 40.8 mm (D).
- The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 313.5 mm (W) × 128.9 mm (H) × 41.3 mm (D).

3.2.2 Surface Mounting

Steps

1. Loosen splice set screws, and separate the host from the keypad module. Paste the mounting template on the wall according to the installation location requirements. Drill holes according to the location of the screw holes of the drill template, and install the expansion bolts into the screw holes.
2. Fix the mounting plate to the wall with 4 supplied screws.
3. Fix the device to the mounting plate, and fix the device with the set screws.
4. Put the Silicone sealant sleeve at the USB part of the keypad module in place. Align the keypad module with the USB interface and install it into the device, and fix it with splice set screws.

Note

- Do not touch the SD card slot and other devices during the process of plugging in and unplugging the power interface.
- Apply Silicone sealant among the joints between the device and the wall (except the lower side) to keep the raindrop from entering.

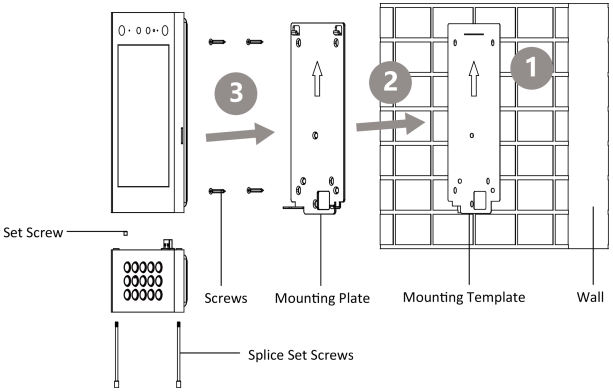

Figure 3-7 Surface Mounting

3.2.3 Flush Mounting

Steps

1. Cave an installation hole in the wall. The suggested dimension of the installation hole is 313.5 mm (W) × 128.9 mm (H) × 41.3 mm (D). Pull the cables out from the wall, insert the gang box into the installation hole, and mark the gang box screw holes' position with a marker.

2. Take out the gang box. Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes. Fix the gang box with 4 expansion bolts.
3. Insert the door station into the gang box, and fix it with set screws.

Note

Do not touch the SD card slot and other devices during the process of plugging in and unplugging the power interface.

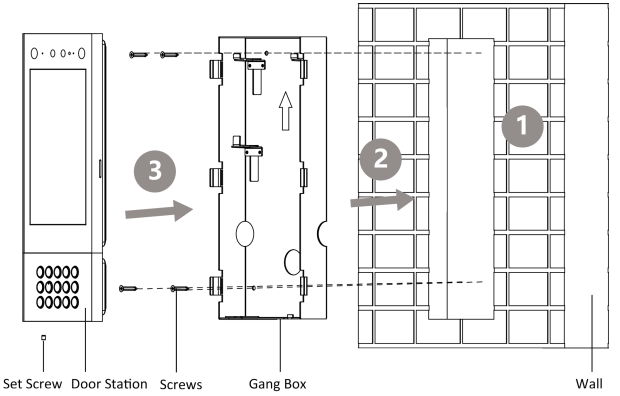

Figure 3-8 Flush Mounting

4 Activation

You can activate the device via iVMS-4200 or Batch Configuration Tool.

Default parameters of door station are as follows:

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

4.1 Activate Device Locally

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

Steps

1. Power on the device to enter the activation page automatically.
2. Create a password and confirm it. Tap **Next** to finish activation.

4.2 Activate Device via Web

Steps

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

   Note

   Default IP Address: 192.0.0.65.

2. Enter the door station IP address into the address bar of the web browser to enter the activation page.

   Caution

   In order to improve the network security, the set password must be from 8 to 16 digits, and be a combination of at least two or more types of numbers, lowercase letters, uppercase letters, and special characters.

3. If there are multiple door stations in your network, please edit the IP address of the door station to prevent IP address conflicts from causing abnormal access to the door station. After logging in the door station, you can click **Configuration →**

Network → TCP/IP to edit the door station IP address, subnet mask, gateway and other parameters.

4.3 Activate Device via Client Software

Steps

1. On the device management page, select **Encoding Device/Door Station**, and select the device to be activated in the online device area.
2. Click **Activate** to enter the activation page.
3. Create a password, and confirm the password. Click **OK** to activate the device.

Note

We highly recommend you to create a strong password of your own choosing (using a password from 8 to 16 characters, including at least two kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product.

4.4 Activate Device via Batch Configuration Tool

Steps

1. Run the batch configuration tool, select the online device that needs to be activated in the online device area, and click **Activate**.
2. Set the activation password in the Activate Device dialog box and click **OK** to complete the activation.

Caution

In order to improve the network security, the set password must be from 8 to 16 digits, and be a combination of at least two or more types of numbers, lowercase letters, uppercase letters, and special characters.

Note

- If the device is in an inactive status, you cannot remotely configure the device.
- By holding Ctrl or Shift, select multiple inactive online devices and click **Activate** to activate the selected devices in batches.

5 Door Station Local Operation

5.1 Door Station Local Configuration

Hold the menu page, enter the password and tap **OK** to enter the configuration page.

5.1.1 Edit Network Parameters

After activating, you should edit the network parameters. Set the IP address of the door station and the IP address of the door station associated device, to realize the network communication between the devices.

Steps

1. Long tap on the menu page, enter the password and tap **OK** to enter the settings page.
2. Tap **Network Settings** to enter the network parameter settings page.
3. Edit the relevant parameters according to the prompts: IP address, subnet mask and address gateway.
4. Exit the settings page.

5.1.2 Door Station Settings

Edit the parameters of the door station (including but not limited to, phase No., building No., floor No.).

Steps

1. Hold the menu page, enter the password and tap **OK** to enter the settings page.
2. Click **Local Settings** to enter the settings page.
3. Set the parameters of the door station (including but not limited to, phase No., building No., unit No., floor No., serial No. and community No.).
4. Enable **Auto Screen Brightness**, or set **Screen Brightness** manually.
5. **Optional:** Enable **Channel Mode** according to your needs.

Note

After the channel mode is enabled, the residents can directly pass through without verification.

6. After the door station settings are completed, exit the settings page to complete the configuration.

Note

- Main Door Station: the serial No. is 0. Sub Door Station: the serial number is greater than 0 (Serial number of sub door station ranges from 1 to 8).
- One unit is equipped with at least one main door station. One main door station can be equipped with up to 8 sub door stations.

5.1.3 User Management

Enter User Management Page

Steps

1. Hold the menu page, enter the password and tap **OK** to enter the settings page.
2. Click **User Management** to enter the user management page.

Add User

On the user management page, you can add new users, configure the user's room information, card information, face information, and fingerprint information.

Steps

1. Long tap on the menu page, enter the password and tap **OK** to enter the settings page.
2. Tap **User Management** to enter the user management page.
3. Tap **+** to enter the add user page.
4. Set **Room No.**
5. Add **Card**.
   1) Select **Card**, and tap **+** to enter the add card page.
   2) Enter the card No. manually or present the card in the card presenting area to obtain the card No.

3) Tap **OK** to enable the settings.

6. Add **Face**.
   1) Select **Face**, and point the face at the camera.
   2) Tap  to add the face.
   3) Tap  to enable the settings.
7. Add **Fingerprint**.
   1) Select **Fingerprint**, and tap **+**.
   2) Put your finger on the fingerprint reader and add the fingerprint.
8. Set **User Permission** as **User** or **Administrator**.
9. Exit the settings page.

5.1.4 Search Version

You can view the device system version and QR Code of the device.

Steps

1. Hold the menu page, and enter the password (activation password) to enter the settings page.
2. Tap **About**.

Result

You can view QR Code of the device Cloud Intercom, **System Model**, **System Version** and open source notice.

5.2 Video Intercom Operation

Door station supports calling users or management center.

5.2.1 Call Resident

Call Resident from Main/Sub Door Station

Tap any digit button on the main/sub door station page to enter the calling page.

Enter the **Room No.**, and tap  to call residents.

Note

- Both the main and sub door station support the elevator control function, that is, after calling the residents successfully, tap the unlock button on the indoor station, the elevator will automatically arrive at the floor where the door station is located, and the permission of the floor where the household is located will be opened (The elevator calling will take effect only after the elevator control is configured and the corresponding configuration of the door machine is completed).
- Door Station Elevator Control Settings: In batch configuration tool, tap **Door Station Remote Configuration → Video Intercom → Access Control and Elevator Control** , set **Elevator No.**, **Elevator Controller Type**, **The Number of Underground Floor**, and set **Interface Type** as **RS-485** or **Network Interface**. Enable elevator control.
  In batch configuration tool, tap **Door Station Remote Configuration → System → RS-485** to enter RS-485 settings page and set elevator control type.

Call Resident from Outer Door Station

On the main page of the outer door station, tap Call to enter the calling page.

Enter **Phase No.** + **#** + **Building No.** + **#** + **Unit No.** + **#** + **Room No.**, and tap Call again to call residents.

Enter **Phase No.** + **#** + **Building No.** + # + Unit No. + **#** + **Room No.**, and tap Call again to call residents.

Enter **Phase No.** + **#** + **Building No.** + # + Unit No. + **#** + **Room No.**, and tap Call again to call residents.

Enter **Phase No.** + **#** + **Room No.**, and tap Call again to call residents.

5.2.2 Call Center

Tap on the main/sub door station page to enter the calling page.

Tap to call management center administrator. Tap cancel button to cancel during calling management center.

5.3 Unlock Door

You can unlock door station in following methods: Unlock by password, unlock by presenting card, unlock by face, and unlock by fingerprint.

5.3.1 Unlock by Password

Unlock by Password

On the menu page, Tap to enter the calling page.

Enter【 # + Password + unlock button】 to unlock door.

Unlock by Public Password

Note

Make sure you have created the public password via iVMS-4200 Client Software remotely.

On the menu page, tap to enter the calling page.

Enter【 # + Password + #】 to unlock door.

5.3.2 Unlock by Face

Note

Make sure that you have added your face picture to the device. Refers to the *User Management* for details.

Face forward at the camera to unlock.

5.3.3 Unlock by Presenting Card

Note

Make sure you have issued the card to the device. Refers to User Management for details.

Present the card on the card reading area to unlock.

5.3.4 Unlock by QR Code

Door station supports unlock by QR code. You can generate a QR code through the mobile phone client, and use the door station camera to scan the mobile phone QR code to open the door.

Steps

Note

- Make sure that the door station IP has been added to the indoor station, and the indoor station and the door station can communicate normally.
- Make sure that the door station is connected to the network.
- Make sure to issue the card first and link it to the door station.

1. Installing Mobile Client Software
   - Login to the App Store, enter ***Hikvision Cloud Management*** in the search box, download and install the iOS version of the mobile client software.
   - Log in to Hikvision's official website, and click **Help → Download → Tools and And Software** , download and install the Android version of the mobile client software.

   Note

   Operating environment of Hikvision Cloud Management

   - iOS System: iOS 6.0 and above.
   - Android System: Android 4.0 and above.

   Here takes Android system as an example.
2. Register user accounts according to the prompts, and login to the client software.
3. Follow the prompts to add the indoor station by scanning the QR code/barcode or manually entering the serial number.
4. Enter unlock by QR code page and generate the QR code.
5. On the main page of door station, tap down button to enter the unlock by QR code page.
6. Aim the QR code generated by the phone at the camera and scan the code to open the door.

   Note

   - It is recommended that when installing the door station, try to select a location that does not cause reflections, otherwise it may affect the QR code

scanning. If it is acrylic door station, make sure that the membrane on the surface of the door machine has been torn off.

- It is recommended to align the mobile phone's QR code with the door station camera horizontally when scanning the QR code.
- QR code recognition is not supported at night.

6 Remote Configuration via Web

6.1 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.

Figure 6-1 Live View Interface

- 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) or Google users, the device supports two-way audio communication. Live View function may vary with different models. Please refer to the actual product.

6.2 Person Management

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

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

Click **Add** and enter the user name, floor No. and room No. to add user.

Click **Edit** to modify the information of the user.

Check the box of the user and click **Delete** to delete the selected user.

Enter the keyword and click **Search**, and the information will be displayed in the list.

Click **View Face** in the operation bar to view the face photos added by the user.

6.3 Number Settings

Configure the corresponding SIP number for the device room number for communication.

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

Click **+Add** to enter room No. and the corresponding SIP number.

Check the number information to be deleted, and click **Delete** to delete number information.

6.4 Device Management

You can manage the linked device on the page.

Add Linked Device

Click **Add** to add the indoor station or sub door station. Enter the parameters and click **OK** to add the device.

Click **Import**. Enter the information of the device in the template to import devices in batch.

⚠ Caution

When importing device information in batches, the original data will be cleared automatically.

Export Device Information

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

Upgrade Linked Device

Click **Upload Upgrading Package**, and click **Browse** to import the upgrading package.

Click **Timing Upgrade** to pop-up the settings dialog. Slide **Enable Upgrading Device Automatically**, and set the start time and end time. The upgrading will start at the set time automatically.

View Upgrading Version

Put the mouse on the **Upgrading Version** to view the upgrading version and time.

6.5 Parameters Settings

Note

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

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

6.5.1 Local Settings

Video Parameters:

- Stream Type: Select the stream type to**Main Stream**or**Sub Stream**.
- Play Performance: select**Shortest Delay**,**Balance**or**Good Fluency**according to your needs.
- Auto Preview: If you select**Yes**, when you enable preview, the page will automatically play the preview image; if you select**No**, when you enable the preview, you need to manually click the play button to preview image.
- Capture File Format: Set the save format of captured images.

Video File

- Packaged Size of Video File: Select the packaged size of the video file according to your needs.
- Video File Saving Path: Video file is stored locally, you can select**Browse**to change the saving path. Click**Open Folder**to open the folder under the archive path.

Capture and Clipping

Preview Captures Saving Path: Capture file is stored locally, you can select**Browse**to change the saving path. Click**Open Folder**to open the folder under the archive path.

Note

Only IE and Google browsers support saving path settings. Other browsers default to the C drive download path. Please refer to the actual device page for more details.

6.5.2 System Configuration

In system configuration, you can view device information, set system time, configure maintenance settings, and configure user information, etc.

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

Basic Information

Click **System Settings → Basic Information** to enter the settings page.

Device system information includes device name, device No., device language, device system type, device model, serial No., version information, channel number, number of alarm input and output, etc. On the page, you can edit **Device Name** and **Device No.**, and set **Language** and **System Type** according to your needs.

Time Settings

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

NTP

Enable **NTP**, and set **Server Address**, **NTP Port**, and **Interval**.

Manual Time Sync

Enable Manual Time Sync., and set the time manually. Check **Sync. with computer time**.

Click **Save** to enable the settings.

Open Source Disclaimer

Click **System Settings → About Device** to enter the settings page.

Click **View Licenses** to view the device license.

System Maintenance

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

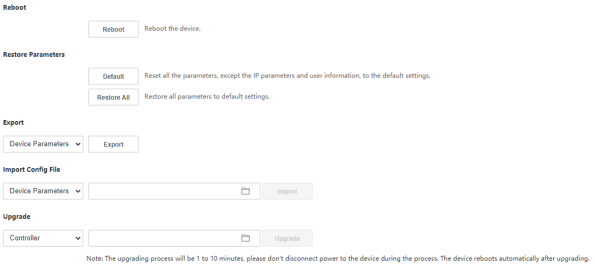

Figure 6-2 System Maintenance

- Reboot：Click **Reboot** to reboot the device.
- Restore: Click **Restore** to restore parameters to default settings.
  Restore

  Reset all the parameters, except IP address, subnet mask and default gateway, to the default settings.

  Default

  Restore all parameters to default settings.

- Export Parameters: Export device parameter files, which can be used to configure the same parameters for another device.
  1. Click **Device Parameters** to show the file encryption configuration.
  2. Set and confirm the encryption password.
  3. Click **OK** to export parameters.
- Import Parameters: Import device parameter files, which can be used to configure the same parameters for another device.
  1. Click **Browse**, select the storage path of the device parameter file, and click **Open**.

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

- Upgrade: When the device program needs to be updated, you can upgrade the device.
  When the device needs to be upgraded, you can copy the upgrade program to the local computer, click **Browse** to select the saving path, and click **Upgrade** to start the upgrading.

Note

Do not power off during the upgrading. The device will reboot automatically after upgrading.

Security Service

SSH is generally used for remote debugging. For device security, it is recommended not to enable SSH when the service is not needed.

Click **Security → Security Service** to enter the settings page.

Slide to enable **Save** to enable the settings.

User Management

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

Administrator can click **Edit** to edit the permission for the users.

Caution

- Admin is the default user. Admin name cannot be edited, and only its password can be edited.
- In order to ensure the security of account information, it is recommended to set a password with the length of 8 to 16 digits, and at least consist of a combination of two or more types of numbers, lowercase letters, uppercase letters and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~Space). The password cannot contain the user name.
- The following types of passwords are risky passwords: the password length is less than 8 digits, the password contains only type 1 characters, and the password is the same as the user name, or the password is the

reverse of the user name. In order to protect your privacy and improve product security, we recommend you change the risky password to a strong password.

- Password strength rules are as follows:
  If the password contains three or more types (numbers, lowercase letters, uppercase letters, special characters), it is a strong password.
  If the password is a combination of numbers and special characters, lowercase letters and special characters, uppercase letters and special characters, lowercase letters and uppercase letters, it is a medium password.
  If the password is a combination of numbers and lowercase letters, or a combination of numbers and uppercase letters, it is a weak password.

Online User

Click **User Management → Online Users** to enter the settings page. The user can view all user information logged in to the device, including the No., logged-in user name, user type, IP address, and user operating time. Click **Refresh** to get the present information.

⚠ Caution

- If the IP address and user name are the same, only one user login information will be displayed.
- The online user interface can display the login information up to 30 users.

Arming/Disarming Information

Click **User Management → Arming/Disarming Information** to enter the settings page. The user can view the arming information of the device, including the No., arming type and IP address. Click **Refresh** to refresh the current arming information.

6.5.3 Network Settings

TCP/IP Settings

Steps

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

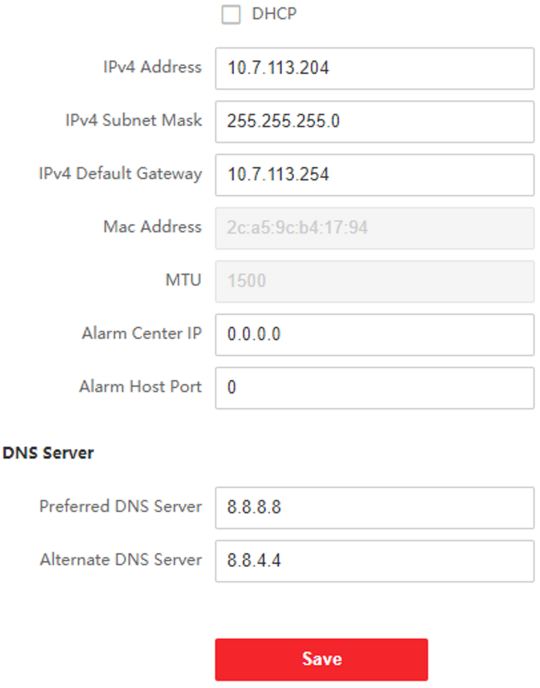

Figure 6-3 TCP/IP Settings

2. Configure the network parameters.
   - Set the **IPv4 Address**, **IPv4 Subnet Mask**, **IPv4 Default Gateway**, **Preferred DNS Server** and **Alternate Server**.
   - Check **DHCP**, the device will get the parameters automatically.
3. Configure **Alarm Center IP** and **Alarm Host Port**.
4. Click **Save** to enable the settings.

Port Settings

Port setting parameters consist of **HTTP Port**, **RTSP Port**, **HTTPS Port** and **Server Port**. When accessing the device through the network, you can set the corresponding port according to your needs.

Steps

1. Click **Settings → Network → Basic Settings → Port** to enter the settings page.
2. The port No. needs to be changed when there are port conflicts.

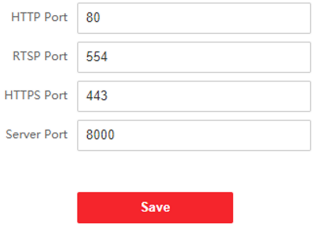

Figure 6-4 Port Configuration

HTTP Port

When you log in with a browser, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81, you need to enter ***http://192.0.0.65 : 81*** when you log in with a browser.

RTSP Port

Real-time transmission protocol port, please make sure that your modified port is available.

HTTPS Port

When you log in with a browser, you need to add the modified port number after the address. For example, when the HTTP port number is changed to 81, you need to enter ***http://192.0.0.65 : 81*** when you log in with a browser.

Server Port

When you login to the device via Client Software, you need to enter the port number in the login page to login to the device normally if you have changed the server port.

Note

Do not change the default port parameters randomly.

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

SIP Settings

SIP server enables communication between terminals in different network segments. If you do not register with the SIP server, you can only make calls between terminals on the same network segment. After successfully registering with the SIP server, the terminals can dial the SIP ID to complete the call.

Steps

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

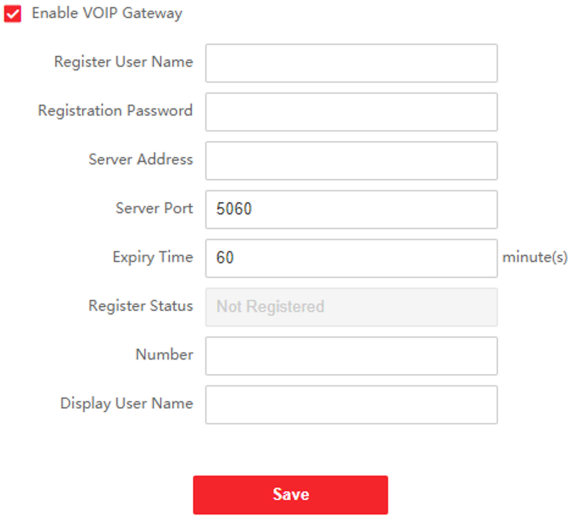

Figure 6-5 SIP Settings

2. Check **Enable VOIP Gateway**.
3. Enter **User Name** and **Password**.
4. Set SIP **Server Address** and **Server Port**.
5. Enter dialing **Number** and **Display the User Name**.
6. Click **Save** to enable the settings.

FTP Settings

You can upload the device capture file to the set FTP server by configuring FTP parameters.

Steps

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

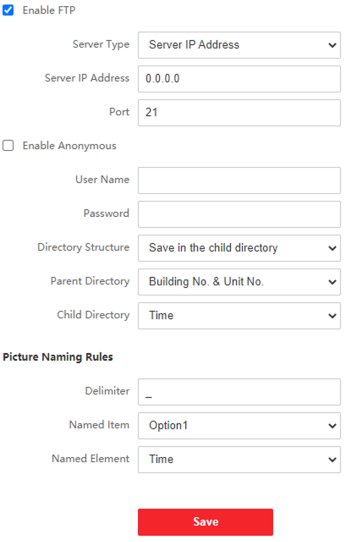

Figure 6-6 FTP Settings

2. Check **Enable FTP**, and select **Server Type**, enter **Server IP Address**, **Port**, **User Name** and **Password**.
3. **Optional:** Check **Enable Anonymous**, you do not need to configure the user name and password.
4. You can save the configuration file in **Root Directory**, **Parent Directory** or **Child Directory**.
   - You can set device name, device IP, time, building No. and unit No. in parent directory.
   - You can set building No., unit No. and door station number in parent directory.
5. You can set the name for FTP captures, set the delimiter, naming item, and naming element according to your needs.
6. Click **Save** to enable the settings.

Note

You can select IP address as the server address.

Platform Access Settings

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **Configuration → Network → Advanced Settings → Platform Access** to enter the settings page.

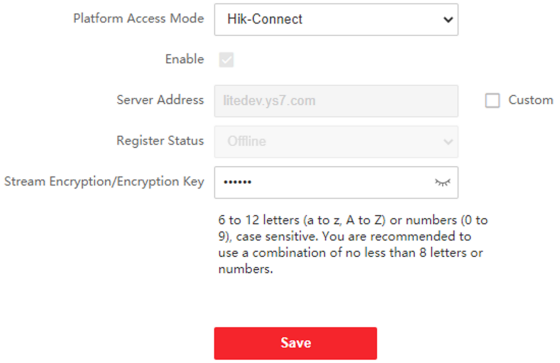

Figure 6-7 Platform Access

2. Select platform access mode.
3. Check **Enable**, configure the server IP address and set **Access Server IP Address** and **Verification Code**.
4. Click **Save** to enable the settings.

Note

- The verification code is used when adding devices to the mobile client. It can be modified. Please keep it properly.
- The verification code should contain 6 to 12 characters (it is recommended to be the combination of numeric and letter, and more than 8 characters).

HTTP Listening

Click **Configuration → Network → Advanced → HTTP Listening** to enter the settings page.

Enter the parameters according to the page and click **Save** to enable the function.

6.5.4 Video & Audio Settings

Video Parameters

Steps

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

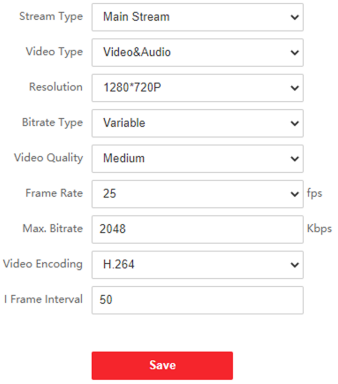

Figure 6-8 Video Parameters

2. Configure the video parameters.

Stream Type

Set the video parameters of main stream and sub-stream.

Video Type

Select the stream type as video stream, or video & audio composite stream. The video & audio composite stream includes audio signal and video signal.

Resolution

You can select the main stream resolution as **1280*720P** or **1920*1080P**, and select the sub-stream resolution as **640*480P** or **1280*720P**. You can select the corresponding resolution according to your actual needs.

Bitrate Type & Max. Bitrate

Select the bitrate type as constant or variable. Constant bitrate means to transmit at the set constant bitrate. Max. Bitrate ranges from 32 to 16384.

Image Quality

You can set the quality level of the image.

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). You can set it according to your actual needs.

Video Encoding

The device supports H.264. Please refer to the specific model for the video encoding type.

I Frame Interval

The number of frames between two key frames before and after. You can set I Frame Interval from 1 to 400.

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

Audio Parameters

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

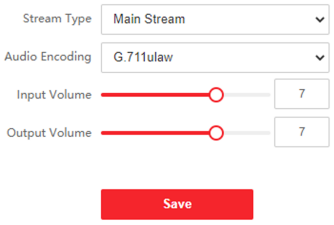

Figure 6-9 Audio Parameters

You can set the stream type and audio encoding of the device audio. You can also set the device input volume, output volume and intercom volume. Drag the slider or enter the value in the input box to adjust. The adjustable range is from 1 to 100. Click **Save** to enable the settings.

Stream Type

Select the stream type of the main stream or sub-stream.

Audio Encoding

The device supports the audio encoding of G.711ulaw.

6.5.5 Image Settings

The display setting parameters can be adjusted according to the actual installation environment of the device.

Steps

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

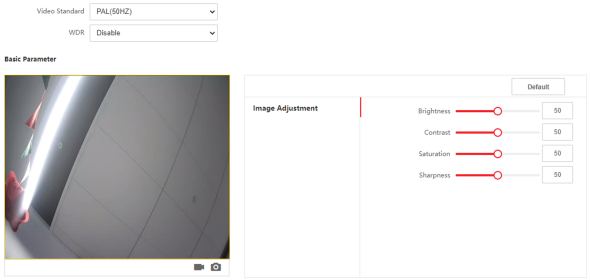

Figure 6-10 Display Settings

2. Select the **Format**.
3. **Optional:** Enable **WDR**.
4. Set the display parameters.
   - Adjust the **brightness**, **contrast**, **saturation**, and **sharpness** of the preview screen by dragging the progress bar.
   - Adjust the screen by entering the corresponding value in the input box.

Note

- If the current settings do not meet expectations, you can click **Restore Defaults** to restore the parameters to the initial status.
- The adjustable range of brightness, contrast, saturation and sharpness are all from 0 to 100.

5. Set the Day/Night Mode.
   1) Set **Day/Night Mode** as **Day** or **Night**.

2) Set the Auto mode, and set the **sensitivity**. When the device perceives the low brightness of the environment, it will automatically turn on the night mode.

3) Set the Scheduled-Switch mode, and set the start time and end time.

Note

The daytime is from the beginning of the day to the end of the day, and the rest of the time is the night time by default.

6. Configure the Supplement Light Parameters.

1) Set **Supplement Light Type**.

2) Set **Supplement Light Mode**.

3) Adjust **Supplement Light Brightness** by dragging the progress bar.

4) Set the **Daytime Start Time** and **Daytime End Time**.

7. Exit the settings page.

6.5.6 Event Settings

When an event occurs, an alarm linkage will be triggered.

Motion Detection Settings

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.

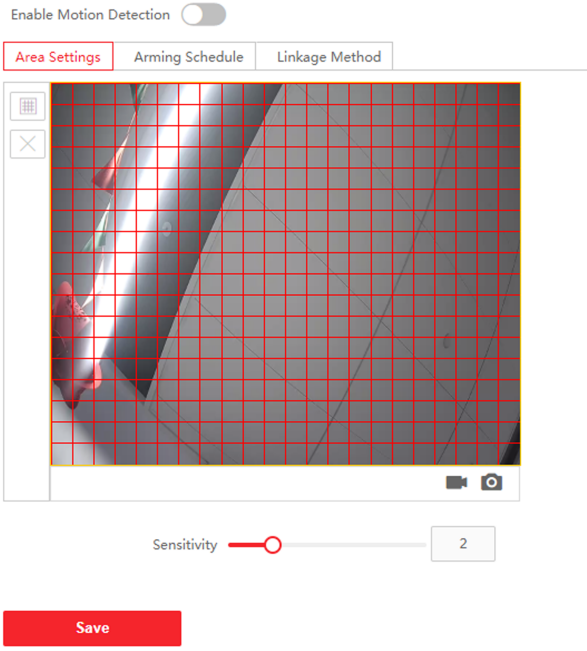

Figure 6-11 Motion Detection

2. Slide **Enable Motion Detection** to enable the function.

Note

If the motion detection function is disabled, you cannot draw the detection area and adjust the sensitivity.

3. Click **Draw Area**. Click and drag the mouse on the window to draw a motion detection area. Click **Stop Drawing** to finish the drawing.

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

Note

When the sensitivity is 0, motion detection will not work.

4. Set the arming time. The device defaults to arming all day. Click the time period of arming, you can display and adjust the arming time of motion detection.

   Note

   - If other time periods need to be set to the same arming time, click the green copy button on the right side of the timeline.
   - You can configure the start time and end time of 8 time periods in detail in one day.

5. Set linkage method as Notify Surveillance Center, and motion detection can link the alarm.
6. Click **Save** to enable the settings.

Event Linkage

When an event occurs, you can specify the event linkage.

Steps

1. Click **Settings → Event → Basic Event → Event Linkage** to enter the settings page.

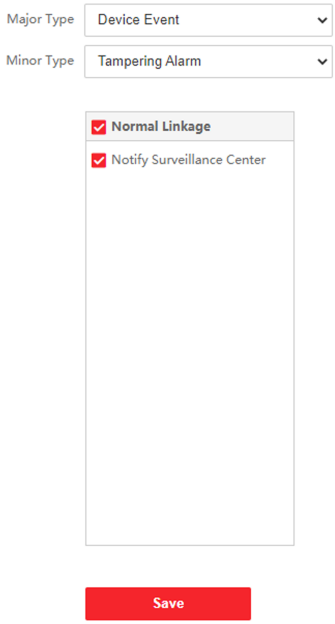

Figure 6-12 Event Linkage

2. Configure the major types of events, the major types of access control events are divided into **Device Event** and **Door Event**.
3. Configure minor types of events.
   - When the major type of access control event is selected as **Device Event**, the minor type is **Host Tamper Alarm**.
   - When the major type of access control event is selected as **Door Event**, the minor type is **Door Open Timeout**.
4. Linkage Mode Settings: events can trigger alarm linkage, and linkage modes consist of **Normal Linkage** and **Upload Center**.
   Normal Linkage

   Set alarm notifications.

   Upload Center

   When an alarm occurs, the alarm information will be uploaded to the surveillance center.
5. Click **Save** to enable the settings.

6.5.7 Two-way Audio Configuration

Device No. Settings

Identify the organization the device belongs to and the device No.

Steps

1. Click **Settings → Intercom → Device No.** to enter the settings page.

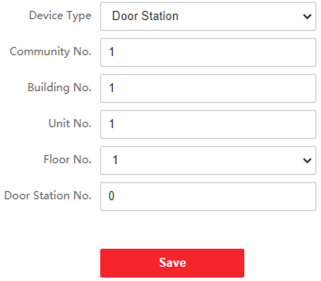

Figure 6-13 Device No. Settings

2. Select **Device Type** as door station or outer door station.
3. Set **Phase No.**, **Building No.**, **Unit No.**, **Floor No.**, **No.** and **Community No.** of the device.
4. Click **Save** to enable the settings.

Session Settings

Enable the communication between door station, main station, and video intercom server.

Steps

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

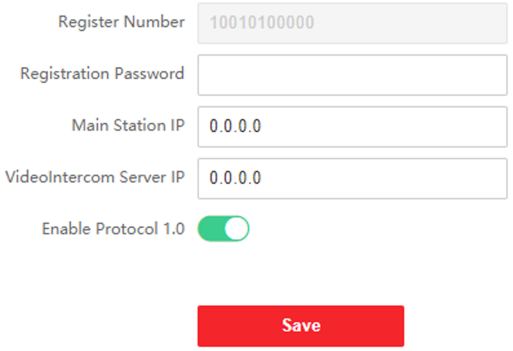

Figure 6-14 Session Settings

2. Set activation password, main station IP, intercom serve and enable 1.0 protocol.
   Register Number

   Register Number of the device, created by default.

   Registration Password

   Activation password of the main station.

   Main Station IP

   IP address of the main station.

   Video Intercom Server IP

   Server IP of the video intercom server.

   Enable Protocol 1.0

   After enabling, door station will register to the main station via previous protocol. After enabling, door station will register to the main station via new protocol.

3. Click **Save**.

Time Parameters

Click **Configuration → Intercom → Time Parameter** to enter the settings page.

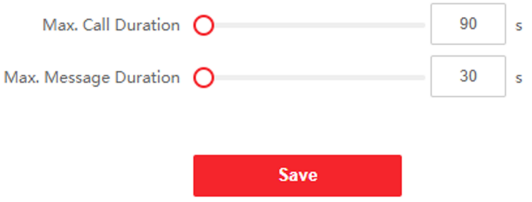

Figure 6-15 Time Parameter

You can drag the slider to configure **Max. Call Duration** and **Max. Message Duration**, and click **Save** to enable the settings.

Note

- The Max. call duration ranges from 90 s to 120 s.
- The Max. message duration ranges from 30 s to 60 s.

6.5.8 Access Control Settings

Permission Password

In order to improve password security, it is recommended to modify the permission password regularly.

Steps

1. Click **Configuration → Access Control → Permission Password** to enter the settings page.

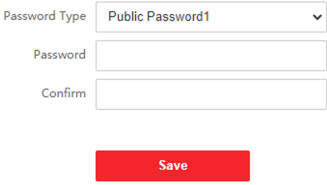

Figure 6-16 Permission Password

2. Select **Password Type**.
3. Edit the password.

Caution

In order to prevent security risks, you must modify the initial password in time after the initial login to prevent others from logging in to your device without authorization or causing other undesirable consequences.

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

Set Door Parameters

Steps

1. Click**Settings → Access Control → Door Parameters**to enter the settings page.
2. Select the**Door**, and edit the**Door Name**.
3. Set**Relay Reverse**and**Open Duration**.
4. Click**Save**to enable the settings.

Card Security Settings

You can encrypt the card to ensure its security.

Steps

1. Slide**The Card Encryption Parameter**to encrypt the card.
2. Configure encrypted sectors.
3. Click**Save**.

Elevator Control

Steps

1. Click **Settings → Access Control → Elevator Control** to enter the settings page.

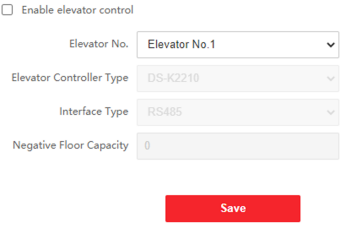

Figure 6-17 Elevator Control

2. Check **Enable Elevator Control**.
3. Select an **Elevator No.**, **Elevator Controller Type** and **Interface Type**.

Note

- Only main door station supports elevator control.
- If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password.
- You can connect the door station to the elevator controller with RS-485 wire.
- Opening Time: Ranges from 1 second to 255 seconds.

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

RS-485 Settings

Set the working mode of an external ladder controller or card reader.

Steps

1. Click **Settings → Access Control → RS-485** to enter the settings page.

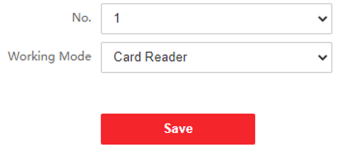

Figure 6-18 RS-485 Settings

2. Select the No.
3. Select the working mode.

Note

No. 1 can be set to work mode as ladder control, card reader or disabled.

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

6.5.9 Smart Settings

Biometrics Settings

Steps

1. Click **Configuration → Smart → Biometrics Settings** to enter the settings page.

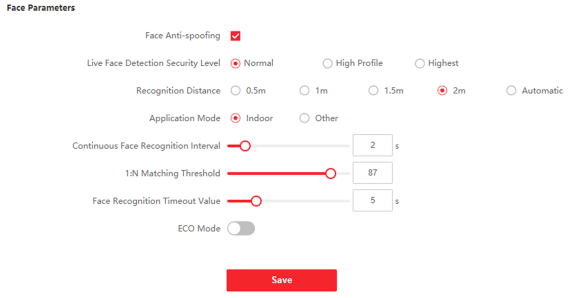

Figure 6-19 Biometrics Settings

2. Slide to enable **Face Anti-spoofing**, and set **Live Face Detection Security Level**.
3. Select **Application Mode** as **Indoor** or **Other**.
4. Set **Continuous Face Recognition Interval** and **1:N Matching Threshold**.
5. **Optional:** Slide to enable **Night Mode**.
6. Click **Save** to enable the settings.

Area Configuration

Draw the location, and adjust the size of the face recognition area.

Steps

1. Click **Configuration → Smart Settings → Area Configuration** .

Figure 6-20 Area Configuration

2. Drag the frame to adjust the size of the recognition area.
3. Click **Save**.
4. **Optional:** Click or in Live View to record or capture.

6.5.10 Theme Settings

Set the advertisement on the main page of the device.

Steps

1. Click **Configuration → Theme** to enter the settings page.
2. Check to enable screen saving function.
3. Set the advertisement theme.
   1) Click **+ Add Theme**.

2) Create a theme name, and select the advertisement body as **picture** or **Video**.

3) Click **Save**.

4. Click **+** to select a picture from the local as the material to be played in standby, and click **upload**.

5. Set the play schedule.

1) Select a theme and drag the time interval to be played on the timeline.

2) **Optional:** Click the drawn area to edit the time manually.

3) Click **Delete** to delete the selected area. Click **Delete All** to delete all selected areas.

6. Adjust **Slide Show Interval**.

Drag the block or enter the number to set the slide show interval. The picture will be changed according to the interval.

7. **Optional:** Slide to enable show custom content and edit custom content.

The custom content displays on the main page of the device.

8. Click **Save**.

7 Remote Configuration via Client Software

You can set Video Intercom system and manage video intercom products including indoor station, door station and main station via iVMS-4200 client software.

7.1 Edit Device Network Parameters

Before You Start
Before configuring the device remotely, make sure that the device is activated.

Steps

1. On the person management page, click **Online Device**.
2. Click to pop up the network parameter settings page.
3. Edit the device IP address, subnet mask, default gateway, etc.
4. Enter the device activation password.
5. Click **Save** to enable the settings.

Note

Please keep the device IP address and the local computer IP address in the same network segment.

7.2 Add Device

You can add devices via the following methods: add device online, add device via IP address, add device via IP segment, add device in batch, and add device via EHome.

7.2.1 Add Online Device

Steps

1. Click **Online Device**.
2. In the online device area, select an activated online device, or press the **Shift** or **Ctrl** to select multiple activated online devices.
3. Click **Add**.

4. Enter the device **Name**, **User Name**, **Password**, and click **Add**.

   Note

   - Only when the doorphone is added to the client software, you can remotely configure the indoor station.
   - Only online devices with the same user name and activation password can support batch activation.

   After the device is added, the device information will be listed in the device list area.

7.2.2 Add Device via IP Address

Steps

1. In the device list area, click **Add** to pop up the device adding dialog box.
2. Select the adding mode as **IP/Domain Name**.
3. Enter the corresponding information of the device: **Name**, **Address**, **User Name**, and **Password**.
4. Click **Add**.

7.2.3 Add Device via IP segment

Steps

1. In the device list area, click **Add** to pop up the device adding dialog box.
2. Select adding method as **IP segment**, and enter the corresponding information: **Starting IP Address**. **Ending IP Address**, **Port No.**, **User Name**, and **Password**.
3. Click **Add**.

   After adding, the device information will be displayed in the device list area.

7.2.4 Add Devices in Batch

Steps

1. In the device list area, click **Add** to pop up the device adding dialog box.
2. Select the adding mode as **Import in Batch**.
3. Click **Export Template**, and enter the device parameters to be imported according to the template.

4. Select the file and click **Add** to import.

Note

The file format for batch import is .csv format.

7.2.5 Add Device Via EHome

Steps

1. In the device list area, click **Add** to pop up the device adding dialog box.
2. Select the adding mode as **EHome**.
3. Enter the corresponding information of the device: **Name**, **Device Account** , and **ISUP login key**.
4. Click **Add**.

7.3 Local Configuration via Client Software

Click **Maintenance and Management → System Settings → Access Control and Video Intercom** , and you can set the incoming ringtone, ring timeout time, the maximum speaking duration with the indoor station, and the maximum speaking duration with the access control device.

Note

- Click the speaker icon to hear the test ringtone.
- The imported ringtone must be in wav format.
- Ringing Timeout Time: The maximum time that the client software can ring the bell when no one answers the call from the the door station or indoor station. Ringing timeout time ranges from 15 s to 60 s.
- The maximum speaking duration with indoor station ranges from 120 s to 600 s. After the speaking duration exceeds the maximum speaking duration, the call will end automatically.
- The maximum speaking duration with door station ranges from 90 s to 120 s. After the speaking duration exceeds the maximum speaking duration, the call will end automatically.

7.4 Device Management

You can add device, modify device, delete device, perform remote configuration, etc. in device management page. The specific method is similar to web configuration . For details, please refer to the iVMS-4200 client user manual.

Note

- When adding a third-party door station encoding device, the client only supports the management of device information, and does not support direct preview. Third-party encoding device must be used in conjunction with the TV wall.
- The client can add up to 256 door stations (including unit door station and doorphone).

7.5 Live View

7.6 Intercom Organization Structure Configuration

7.6.1 Add Organization

Steps

1. On the main page of the client, click **User Management** to enter the settings page.
2. Click **Add**, enter the organization name to add the organization.

7.6.2 Modify and Delete Organization

- You can select the added organization and click to modify its name.
- You can select an organization, and click **X** to delete it.

Note

- Make sure there is no person added under the organization, or the organization cannot be deleted.
- The lower-level organizations will be deleted as well if you delete an organization.

7.7 Person Management

You can add, edit, import, and export person information.

7.7.1 Add Person

Steps

1. On the main page of the client, click **Person Management** to enter the person information configuration page.
2. Select an organization in the organization list and click **Add** on the person panel to pop up the adding person dialog.

   Note

   The Person No. will be generated automatically, and it is editable.

3. Set the person basic information.
   1) Enter basic information: name, gender, tel, effective period and E-mail address.

      Note

      Up to 15 characters are allowed for person name.

   2) Click **Add face** to upload the photo.

      Note

      The picture should be in *.jpg format.

Upload	Click **Upload**, select the person picture from the local PC to upload it to the client.
Take Photo	Click **Take Photo**, and slide to enable device verification. After the face collector is initialized successfully, you can take a photo to obtain a face picture.
Remote Collection	Click **Remote Collection**, select the collection device, click the photo to get the photo, and click **OK** to complete the collection.

4. Issue the card for the person.
   1) Click **Credential → Card**.
   2) Click **+** to pop up the Add Card dialog, select **Normal Card** as **Card Type**, and enter the Card No.
   3) Click **Read** and the card(s) will be issued to the person.
5. Add fingerprint permissions for the person.

1) Click **Credential → Fingerprint**.
2) Select **Collection Mode** and **Collection Recorder**.
3) Click **Start to Scan** to add the fingerprint.
4) Click **Add** to save the fingerprint.

Note

Only some models of the devices support fingerprint function, please refer to the specific product.

6. Click **Access Control** and check the access control permissions that need to be configured.
7. Linked Device
   1) Click **Resident Information**, and select the device to be bound.
   2) Set the floor No. and room No.
8. Click **Save** to enable the settings.

7.7.2 Modify and Delete Person

Steps

1. Select the person and click **Edit** to open the editing person dialog.
2. Modify the person information in the pop-up window and click **OK** to save the settings.
3. Select the person in the organization, and click **Delete** to delete the person.
4. Select the person in the organization, click **Change Organization**, search or select the organization to be moved to, and click **OK** to complete the organization change.

7.7.3 Import and Export Person Information

Import Person Information

Steps

1. On the person management page, click **Import**.
2. In the pop-up dialog box, click **...**, and select the CVS file to import.
3. Click **OK**, and the system will display the imported results.

4. Click **Close** to complete the import.

Note

- Click **Download Template for Importing Person** to download the template.
- The import template contains the following information: person name, gender, department code, certificate type, certificate number, phone number and address.
- The number of persons can not exceed 5000 in a single import.
- If the imported person No. already exists in the client database, the system will automatically replace the original person information.

Export Person Information

Steps

1. On the person management page, click **Export**.
2. Select **Person Information** or **Face Picture**.

Note

Check the checkboxes to select the person information to export.

3. Click **Export**, select the saving path of the exported file and click **Save**.

   All person information will be exported to specified location.

7.7.4 Get Person Information

Steps

1. In the person management page, click **Get Person Information**.
2. Select device(s) to get person information.
3. Click **Get**, the person information will be imported to the client software.

Note

The device added using COM or ISUP connection mode does not support get person information function.

7.7.5 Issue Card in Batch

Steps

1. On the person management page, click **Batch Issue Cards**.
2. Click **Settings** to set issue card paramrters.
   - If you set issue card **Mode** as **Local**, you need to set **Card Issuer**, **Card Type** and **Card No.**, and enable **Buzzer** and **M1 Card Encryption** and click OK to issue card.
   - If you set **Issue Card Mode** as **Remote**, select card issuing device, and click **OK** to issue card.

7.7.6 Permission Settings

Add Permissions

Steps

1. On the main page of the client, click **Access Control → Access Group** to enter the settings page.
2. Click **Add** to pop up the adding dialog box.
3. Configure the parameters.
   1) Enter **Name** of the permission.
   2) Select the **Schedule Template**.
   3) Check the person to **Selected** according to your needs.
   4) Check the device to **Selected** according to your needs.
4. Click **Save**.
5. Check the permission and click **Apply All to Device**.

   The status of the permission displays as Applied.
6. **Optional:** Click **Applying Status** to check the details.

Modify/Delete Permissions

On the page of the permission settings, click to edit the parameters of the permission.

Select one or more permissions, click **Delete** to remove the permissions.

7.8 Video Intercom Settings

7.8.1 Video Intercom

You can call residents on the video intercom page, and the residents can also call the client software through the indoor station. The door station can also call the client software.

Steps

1. On the main page, click **Access Control → Video Intercom → Video Intercom** to enter the video intercom page.
2. Select an organization from the list, and the residents list on the right displays the residents information under the organization.
3. Select a resident from the list, and click to call the corresponding resident.
4. If the indoor station calls the client software, you can click **Answer** or **Hang Up**.

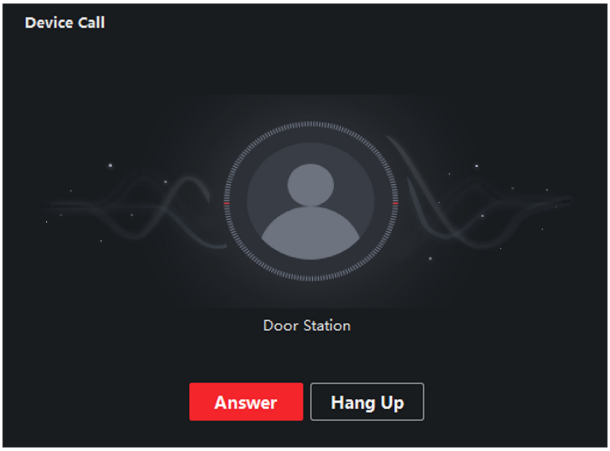

Figure 7-1 Answer the Call

5. After the call is connected, the device will enter the dialog page.

Adjust the Volume	Click to adjust the volume of the microphone. Click to adjust the volume of the microphone.
Hang up the Dialog	Click **Hang Up** to hang up the dialog.
Unlock Remotely	If the indoor station is connected to the door station, click to open the door associated with the door station.

Note

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

7.8.2 Search Video Intercom Information

Search Call Logs

Steps

1. On the Video Intercom page, click **Access Control → Video Intercom → Call Log** to enter the page.
2. Set the search conditions.
   Call Status

   You can select the call status as dialed, received or missed.

   Device Type

   Select the device type as indoor station, door station, outer door station or analog indoor station.

   Time

   Set the start time and end time of a time period to search the logs.
3. Click **Search**.
4. **Optional:** You can reset the settings or export the notice after the search.

Reset the Settings	Click **Reset** to reset search conditions.
Export Search Results	Click **Export** to export the search results to your PC.

Search Notice

Steps

1. On the Video Intercom page, click **Access Control → Video Intercom → Notice** to enter the page.
2. Set the search conditions.

Information Type

You can set the information type as all, advertising Information, property information, alarm information or notice information according to your needs.

Time

Set the start time and end time of a time period to search the logs.

3. Click **Save**.
4. **Optional:** You can reset the settings or export the notice after the search.

Reset the Settings	Click **Reset** to reset all the configured search conditions.
Export Search Results	Click **Export** to export the notices to your PC.

7.8.3 Upload Arming Information

Steps

1. On the upper-right corner of menu page of the client software, click → **Tool** → **Device Arming Control** to enter the settings page.
2. Slide the slider to set the arming state of the device.

Caution

- When the device is added to the client software, the client software will automatically establish an arming connection, and the device is automatically in the arming state.
- Only support 1-channel arming connection. If the device is added to client software A and the automatic arming is successful, the arming connection cannot be established if you add device to client software B at this time. The alarm information will only be uploaded to client software A.

Note

- After the arming setting, when an alarm occurs, the alarm information can be automatically uploaded to the client software.
- After the arming setting, you can view alarm records in the alarm events page.
- When adding device to the client software, the device will automatically enter arming state by default.

3. **Optional:** Click **Arm All** or **Disarm All** to arm or disarm devices.

8 Batch Configuration Tool

You can only configure and operate the door station after creating a password for the device activation.

Default parameters of door station are as follows:

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

8.1 Create the Organization Structure

In the batch configuration tool settings page, click **Flash Rom** to enter the settings page. Through the rebooting tool, you can complete the network configuration, associated network configuration and room No. configuration of all indoor stations in a community in batches, and quickly realize the communication between the indoor stations in the community and the door station, main station, and central platform.

8.1.1 Create Community Structure

Steps

1. Click **Flash Tool** to enter the page.
2. On the flashing tool page, according to the actual situation of the community, edit/display area in the community structure, and create the community structure (including district, building, unit, building, floor and room).

   Note

   - Click **Delete** to delete all community structure.
   - Click + or - to expand or collapse the community structure list. You can also select a structure and click **Expand All** or **Collapse All** to expand or collapse community structure list.

8.1.2 Door Station Flash

Link Main Door Station

Steps

1. Select the community structure. Here takes building 1 (with 1 unit, 1 floor, 2 rooms) as an example.

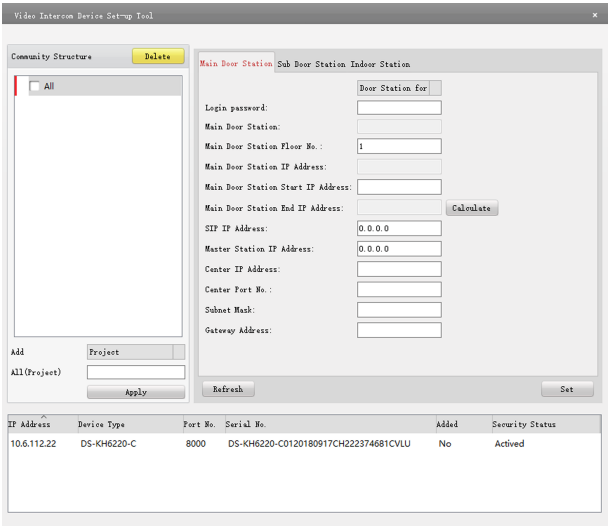

Figure 8-1 Link Main Door Station

2. Set the starting IP address of main door station (The default starting IP is paired with the unit 1 sub door station).
3. Click **Calculate** to get the end IP address of door station and main door station No.(such as 1-1-1-1). The ending IP address depends on the number of units in selected structure.
4. Set the corresponding network information. Set the SIP server IP address, main station IP address, central platform IP address and port No. Set the subnet mask and gateway address.
5. In the online device area, select a door station, enter the login password, and click **Root**.

Caution

- During the rooting process, if the door station has been activated locally on the device or the configuration tool, the login password entered here is the activation password.
- During the rooting process, if the door station is not activated, then entering the login password here is to set a password by yourself. At the same time as the rooting, the door station will be activated.

Link Sub Door Station

Steps

1. Select the community structure. Here takes building 1 (with 1 unit, 1 floor, 2 rooms) as an example.

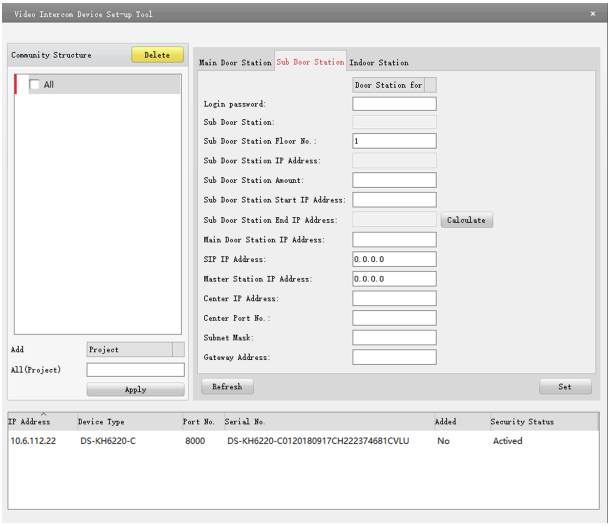

Figure 8-2 Link Sub Door Station

2. Set the starting floor, starting IP address and the number of sub door station.
3. Click **Calculate** to get the end IP address of sub door station and sub door station No.(such as 1-1-1-1). The ending IP address depends on the number of sub door station.

4. Set the corresponding network information. Set the main door station IP address, SIP server IP address, main station IP address, central platform IP address and port No. Set the subnet mask and gateway address.
5. In the online device area, select a door station, enter the login password, and click **Root**. At this time, the corresponding No. (such as 1-1-1-1) and IP address of the sub door station are generated.

Caution

- During the rooting process, if the sub door station has been activated locally on the device or the configuration tool, the login password entered here is the activation password.
- During the rooting process, if the sub door station is not activated, then entering the login password here is to set a password by yourself. At the same time as the rooting, the sub door station will be activated.

8.2 Upgrade in Batch

In the batch tool settings page, click**Upgrade in Batch**to enter the page. Through upgrading in batch, you can upgrade multiple intercom devices in batch.

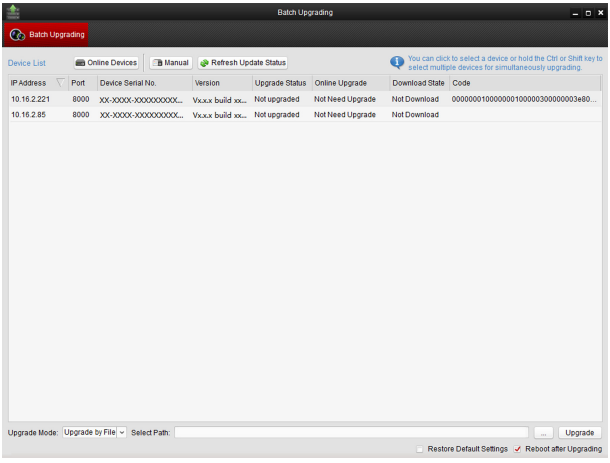

Figure 8-3 Batch Upgrading

8.2.1 Add Devices to be Upgraded

You can add online devices to be upgraded in the same network segment, or add devices to be upgraded by IP address or IP segment.

Add Online Device for Upgrading

Steps

1. On the batch upgrade page, click **Online Devices** to open the online device window.
2. Select a device, click **Login Device**, enter the user name and password, and click **OK**.

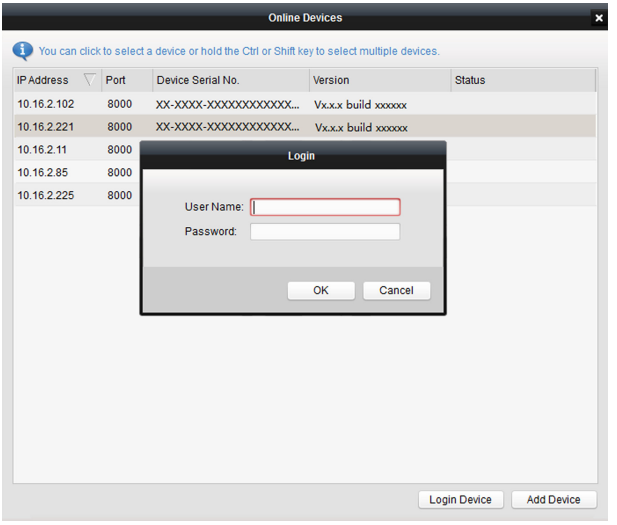

Figure 8-4 Add Online Device

3. After the device is logged in, the status column will be marked as logged in. Select one or more logged-in devices and click **Add Devices to the List** . After adding, the status column will indicate that the device has been added.

Add via IP or IP Segment

Steps

1. On the batch upgrade page, click **Add via IP** to open the IP/IP segment search window.

2. Search and add devices.
   Search via IP

   Enter the device IP address and search for the device to be added.

   Search via IP Segment

   Enter the device IP segment and search for the device to be added.

3. Click **Add Device**.

8.2.2 Upgrade Device

You can upgrade the device via the file, or upgrade the device online.

Online Upgrade

The client can search for the new upgrade file information of the device automatically on the server. When a new upgrade file is found, the online upgrade column will display "Required", otherwise it will display "Not required".

Steps

1. Select the device to be upgraded, select the upgrade method as online upgrade, and click **Download Upgrade File**. The client will automatically download the latest upgrade file.
2. When the download status shows 100%, the download of the upgrade file is completed, click **Start Upgrade**, and the device starts to upgrade.

Upgrade Device by File

The device can be upgraded via the local upgrade file.

Steps

1. Select the device that needs to be upgraded, select the upgrade mode as file upgrade, and click **...** to enter the settings page.

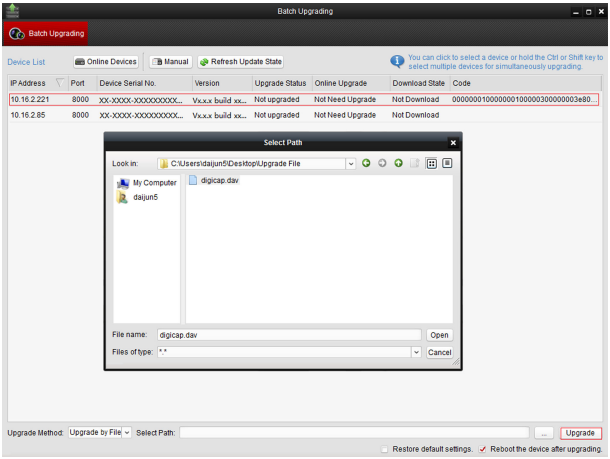

Figure 8-5 Upgrade by File

2. Select the upgrade file, click **Open** and **Start to Upgrade**, and the device starts to upgrade.

Note

Device will reboot automatically after upgrading.

A. 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 A-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 A-2 Device Command


See Far, Go Further