Video Intercom Face Recognition Door Station

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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 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 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 About this Manual 1
2 Appearance 2
2.1 Door Station 2
2.2 Keypad Module 3
2.3 Fingerprint Sub Module 4
3 Terminal and Wiring Description 5
4 Installation 7
4.1 Install Door Station 7
4.1.1 Door Station Installation Accessories 7
4.1.2 Surface Mounting 9
4.1.3 Flush Mounting 10
4.2 Install Door Station with Sub Module 11
4.2.1 Door Station with Sub Module Installation Accessories 11
4.2.2 Surface Mounting 14
4.2.3 Flush Mounting 15
5 Sub Module Description 17
6 Activation 18
6.1 Activate Device Locally 18
6.2 Activate Device via Web 18
6.3 Activate Device via Client Software 19
6.4 Activate Device via Web 20

7 Local Configuration 21
7.1 Quick Configuration 21
7.2 Authentication via Admin 26
7.3 Network Parameters Settings 27
7.3.1 Edit Wired Network Parameters 27
7.3.2 Cloud Service Settings 28
7.4 Device No. Settings 29
7.5 User Management 30
7.6 Call Settings 31
7.7 Forget Admin Password 32
7.8 System Settings 33
7.8.1 Change Language 33
7.8.2 Adjust Brightness 34
7.8.3 Keypad Sound Settings 35
7.8.4 Channel Mode Settings 35
7.8.5 Theme Settings 36
7.8.6 Restore Door Station 36
7.9 Device Information 37
8 Local Operation 39
8.1 Call from the Device 39
8.1.1 Call Resident 39
8.1.2 Call Center 41
8.2 Unlock Door 41
8.2.1 Unlock by Password 41

8.2.2 Unlock by Face 42
8.2.3 Unlock by Presenting Card 42
8.2.4 Unlock by QR Code 42
9 Remote Configuration via Web 44
9.1 Live View 44
9.2 User Management 44
9.3 Device Management 45
9.4 Parameters Settings 47
9.4.1 Local Settings 48
9.4.2 System Parameters 49
9.4.3 Network Settings 55
9.4.4 Video & Audio Settings 60
9.4.5 Display Settings 63
9.4.6 Card Security 64
9.4.7 Intercom Settings 65
9.4.8 Access Control Settings 68
9.4.9 Smart Settings 71
9.4.10 Theme Settings 74
10 Remote Configuration via Client Software 77
10.1 Edit Device Network Parameters 77
10.2 Add Device 77
10.2.1 Add Online Device 77
10.2.2 Add Device via IP Address 78
10.2.3 Add Device via IP segment 78

10.2.4 Add Devices in Batch 78
10.2.5 Add Device Via EHome 79
10.3 Local Configuration via Client Software 79
10.4 Device Management 79
10.5 Live View 80
10.6 Intercom Organization Structure Configuration 80
10.6.1 Add Organization 80
10.6.2 Modify and Delete Organization 80
10.7 Person Management 80
10.7.1 Add Person 81
10.7.2 Modify and Delete Person 82
10.7.3 Import and Export Person Information 82
10.7.4 Get Person Information 83
10.7.5 Issue Card in Batch 83
10.7.6 Permission Settings 84
10.8 Video Intercom Settings 84
10.8.1 Video Intercom 84
10.8.2 Search Video Intercom Information 86
10.8.3 Upload Arming Information 87
A. Communication Matrix and Device Command 88

1 About this Manual

Get the manual and related software from or the official website (http://www.hikvision.com).

Product	Model
Door Station	DS-KD9403-E6

2 Appearance

2.1 Door Station

Note

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

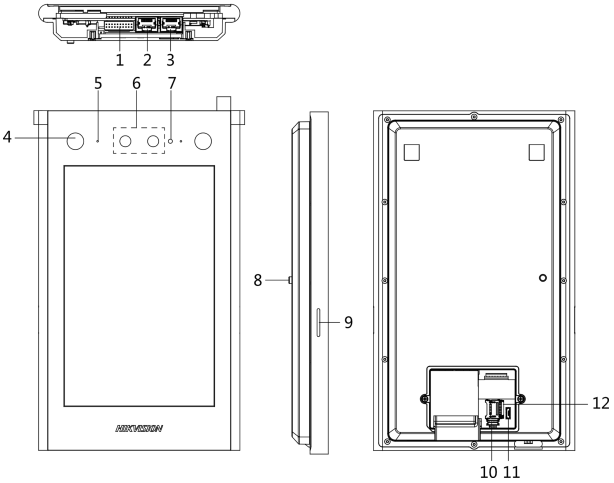


Figure 2-1 Door Station

Table 2-1 Appearance Description

No.	Description	No.	Description
1	Wiring Terminal	7	Ambient Light Sensor
2	Network Interface	8	TAMPER
3	Reserved	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

2.2 Keypad Module

Note

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

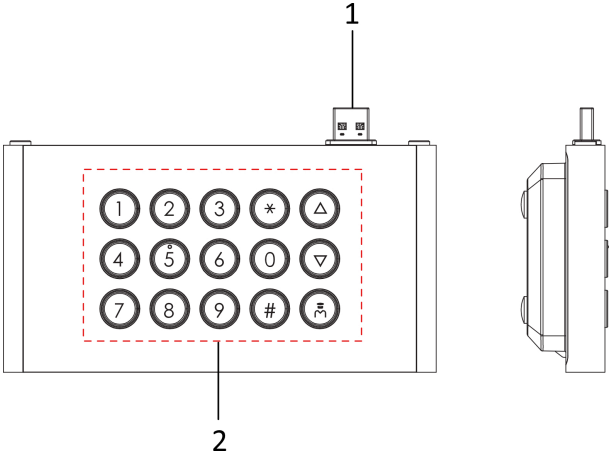


Figure 2-2 Appearance of Keypad Module

Table 2-2 Appearance Description

No.	Description
1	Type-A Interface
2	Keypad

2.3 Fingerprint Sub Module

Note

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

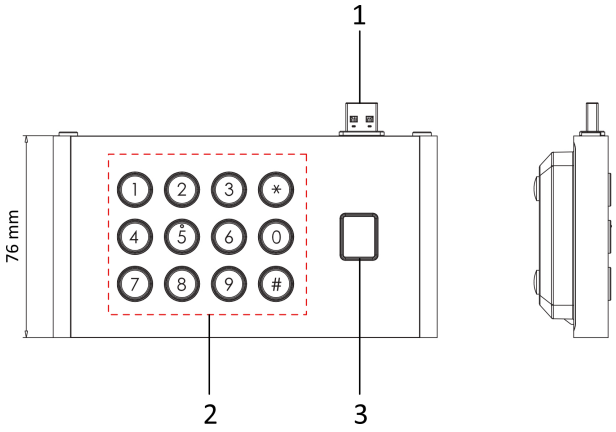


Figure 2-3 Appearance of Fingerprint Module

Table 2-3 Appearance Description

No.	Description
1	Type-A Interface
2	Keypad
3	Fingerprint Reader

3 Terminal and Wiring Description

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

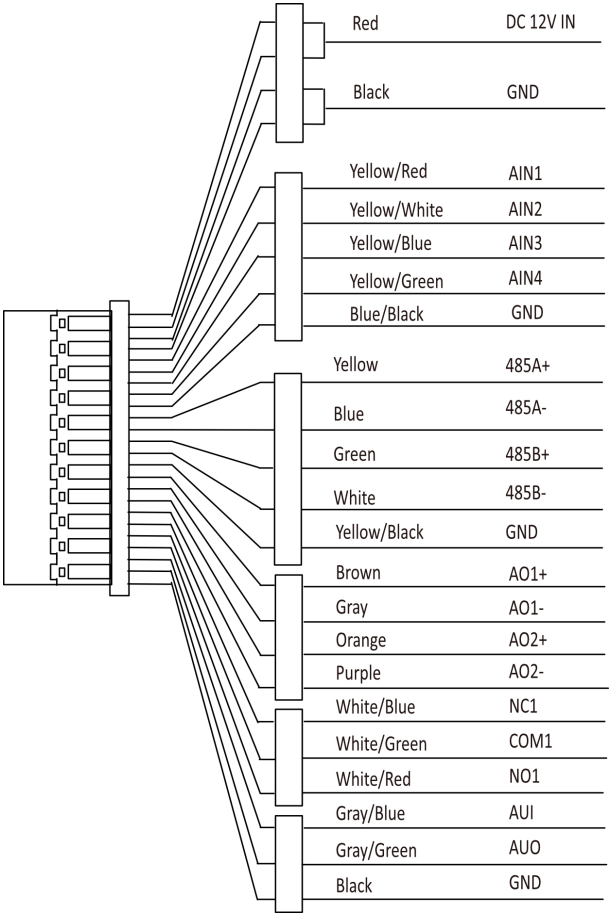


Figure 3-1 Terminal and Wiring Description

Wiring description:

- AIN1: door contact connection
- AIN2: reserved
- AIN3: exit button connection
- AIN4: fire alarm connection
- NO, COM and NC: door lock connection
- RS-485A: connect to card reader or elevator controller (configured via web).
- RS-485B: connect to secure door control unit.

Note

The function of unmentioned interfaces are reserved.

4 Installation

4.1 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.

4.1.1 Door Station Installation Accessories

Mounting Plate

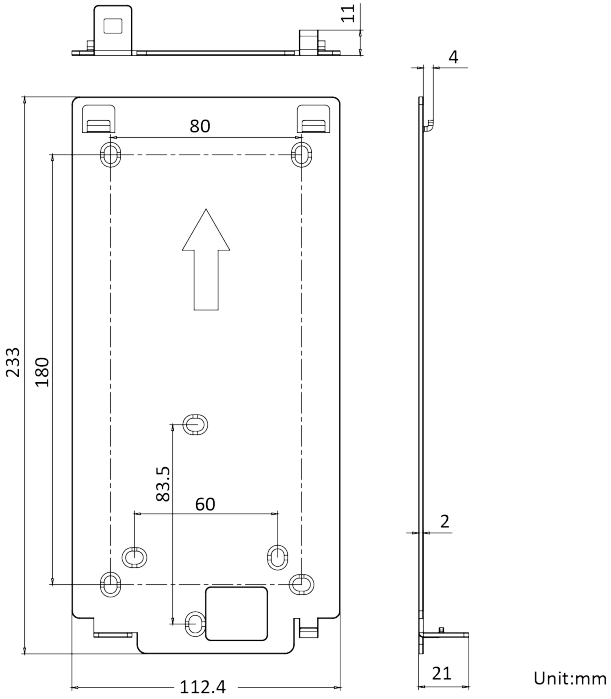


Figure 4-1 Mounting Plate

Note

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

Gang Box

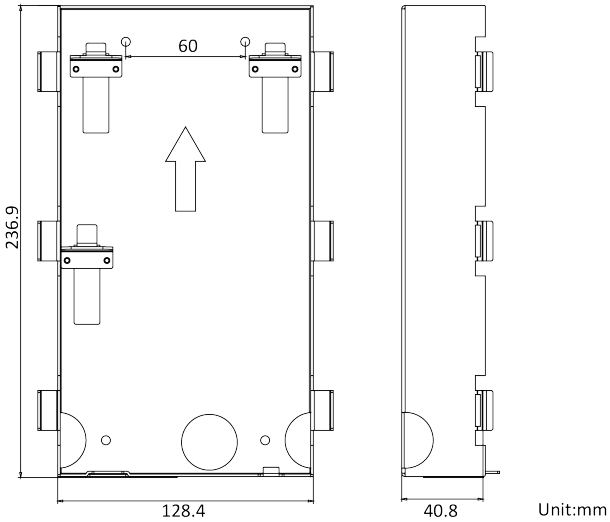


Figure 4-2 Gang Box

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).

4.1.2 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.

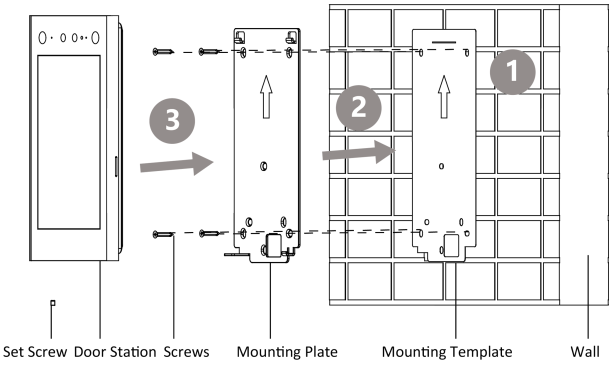


Figure 4-3 Surface Mounting

4.1.3 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 TF 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.

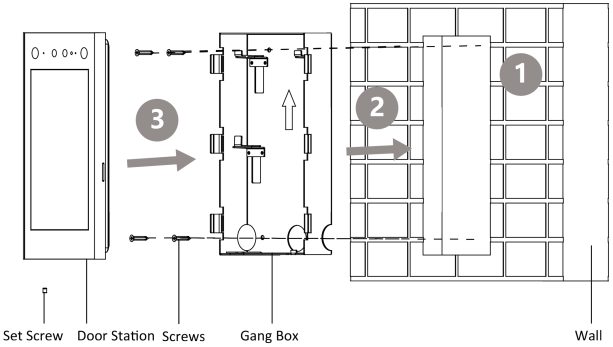


Figure 4-4 Flush Mounting

4.2 Install Door Station with Sub 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.
- The installation steps of door station with different sub modules are the same, and here takes door station with keypad module for example.

4.2.1 Door Station with Sub Module Installation Accessories

Mounting Plate

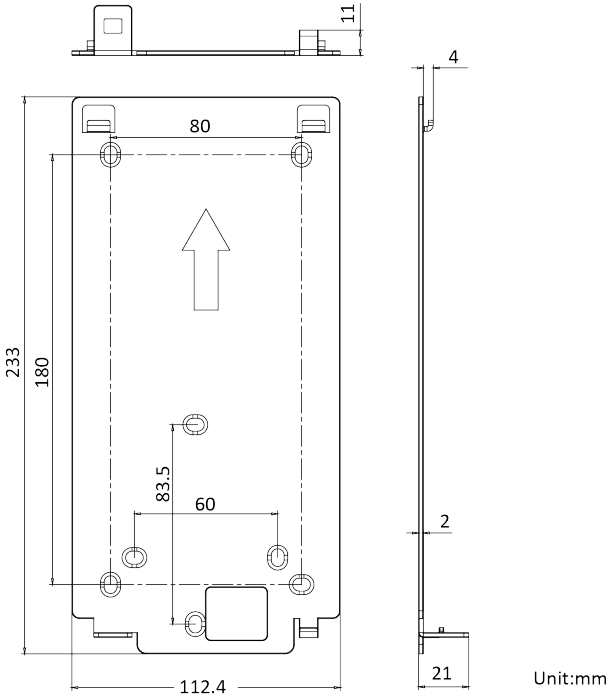


Figure 4-5 Mounting Plate

Note

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

Gang Box

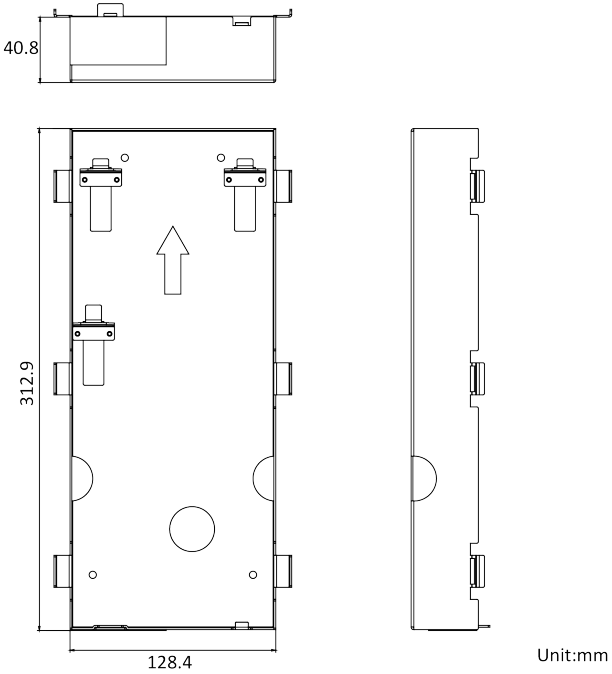


Figure 4-6 Gang Box

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).

- 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).
- The gang box for flush mounting of the door station with sub module is not contained in the package. Contact us or purchase need.

4.2.2 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 TF 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.

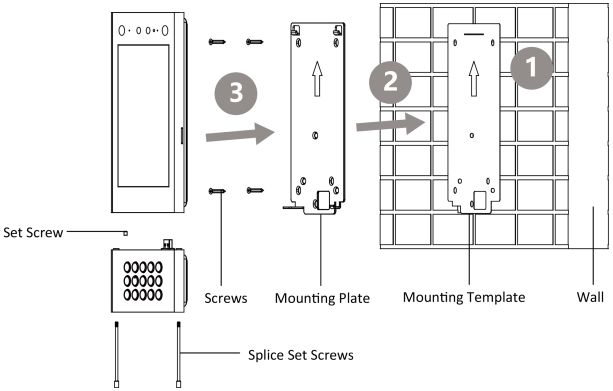


Figure 4-7 Surface Mounting

4.2.3 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. Remove the mounting ears of the gang box.
3. Fix the sub module to the door station with 2 set screws. Wire the device and cover the rear panel with 2 screws. Insert the door station into the gang box, and fix it with set screws.

Note

- Do not touch the TF 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.

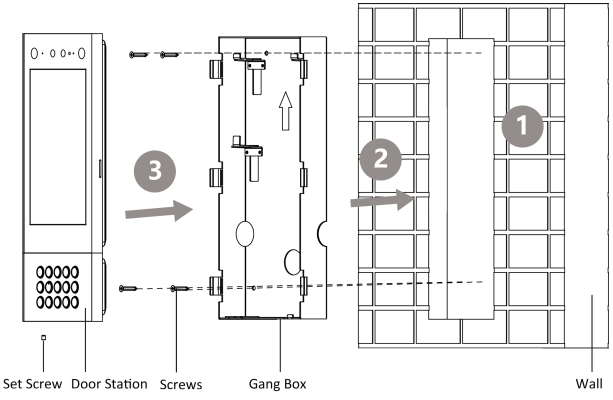


Figure 4-8 Flush Mounting

5 Sub Module Description

Both keypad module and fingerprint module are supported by the door station.

Select a sub module according to your actual needs.

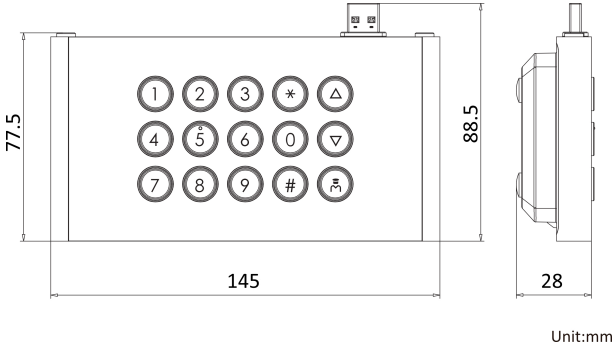


Figure 5-1 Keypad Module

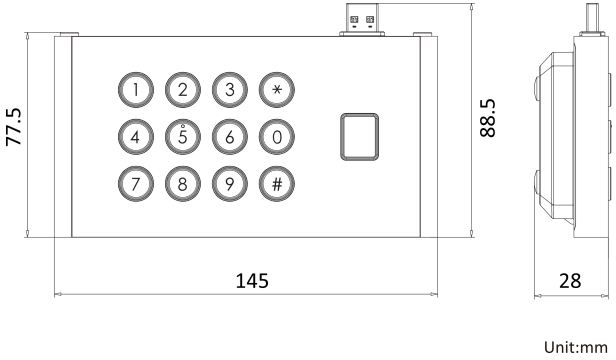


Figure 5-2 Fingerprint Module

After installation, power on the device. Door station will recognize the sub module automatically.

Device will restart automatically in 10 s when the sub module is removed from the door station. Turn off the device before plugging the sub module to the door station.

6 Activation

6.1 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.

   Note

   You can tap to enable or disable password reveal.

3. Tap **Next** to finish activation.

   Note

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

What to do next

After activating the device, the quick configuration page will pop-up automatically. Refers to ***Quick Configuration*** for details.

6.2 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.

6.3 Activate Device via Client Software

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.

Steps

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

Note

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

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

Note

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

6.4 Activate Device via Web

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

Default parameters of the door station are as follows:

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

Steps

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

   Note

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

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

7 Local Configuration

7.1 Quick Configuration

After activating the device, the quick configuration page will pop up automatically.

Steps

1. Select the system language and tap **NEXT**.

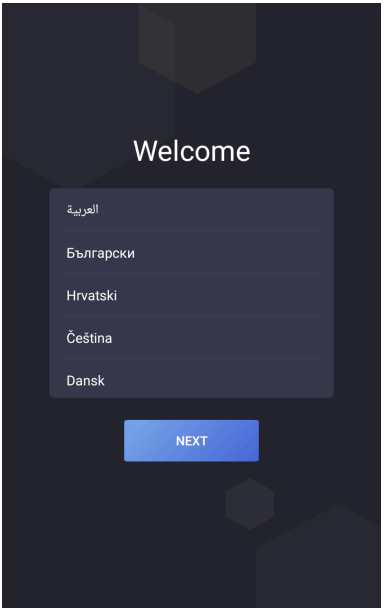


Figure 7-1 Select Language

2. Set network parameters and tap **NEXT**.

- Set the **IP address**, **Subnet Mask** and **Gateway** manually.
- Enable **DHCP**, the device will get network parameters automatically.

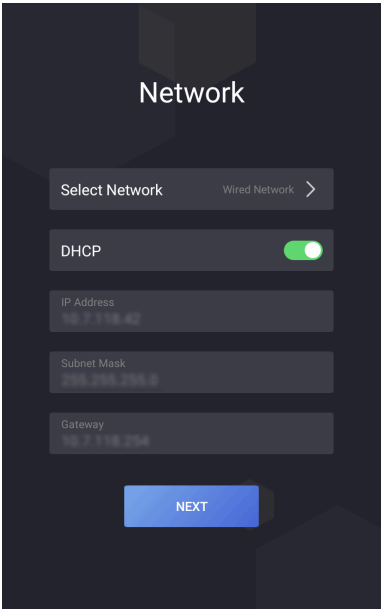


Figure 7-2 Network Parameters Settings

3. Set password reset method and tap **NEXT**.

- Enter the Reserved Email address, then you can reset the admin password by email.

Note

On the security questions settings page, you can tap **Change to Reserved Email** to modify the password reset method.

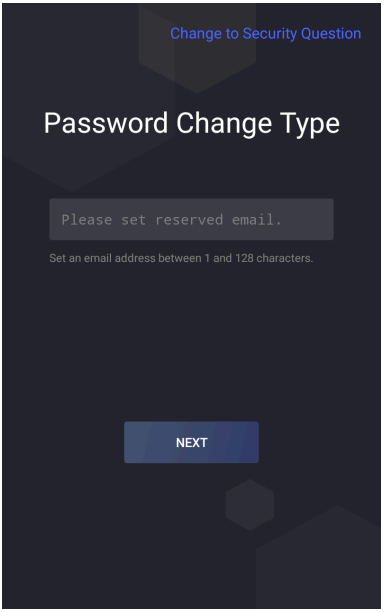


Figure 7-3 Password Reset by Setting Reserved Email Address

- Tap **Change to Security Question**. Select 3 security questions from deficiency list and enter the answers of the questions, then you can reset the password by answering security questions.

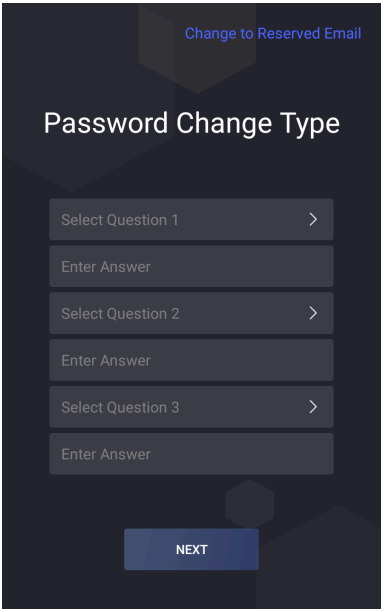


Figure 7-4 Password Reset by Setting Security Questions

4. Enable the cloud service functions and create a verification code. Tap **NEXT**.

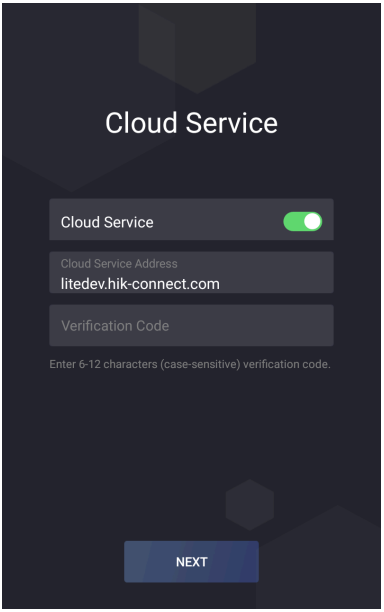


Figure 7-5 Cloud Service

5. Select theme of the system.

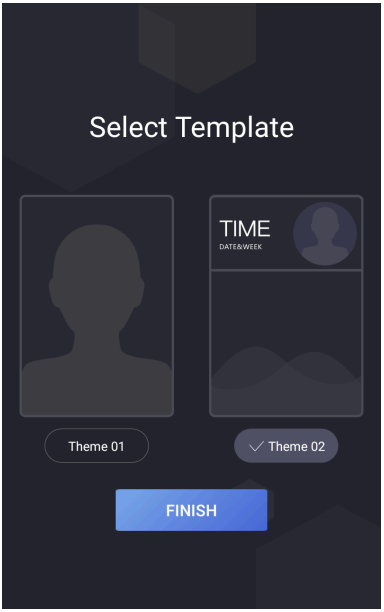


Figure 7-6 Theme Settings

6. Tap **FINISH**.

7.2 Authentication via Admin

You can configure the parameters of the device on the menu page. You should authenticate to enter the menu.

If you want to authenticate via face/card/fingerprints, you should add administrator first. Refers to ***User Management*** for details.

Steps

1. Hold the screen to enter the authentication page.

2. You can enter the admin password or authentication via Face/Card/Fingerprints to enter the menu.

Note

Admin password is set as activation password.

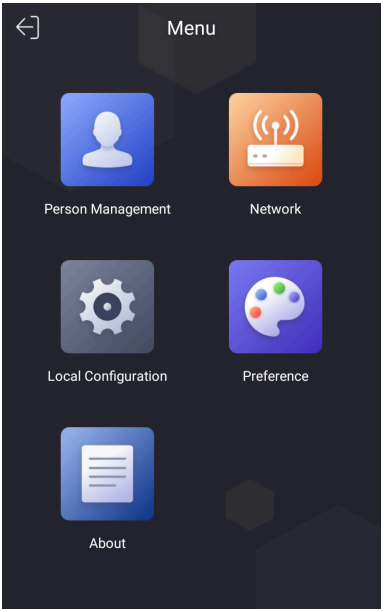


Figure 7-7 Menu Page

7.3 Network Parameters Settings

The device support wired network, wireless network and cloud service settings.

Note

Only parts of the devices support the wireless network, please refers to the actual device for detailed information.

7.3.1 Edit Wired Network Parameters

The device should be connected to the network.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Network → Wired Network** to enter the settings page.

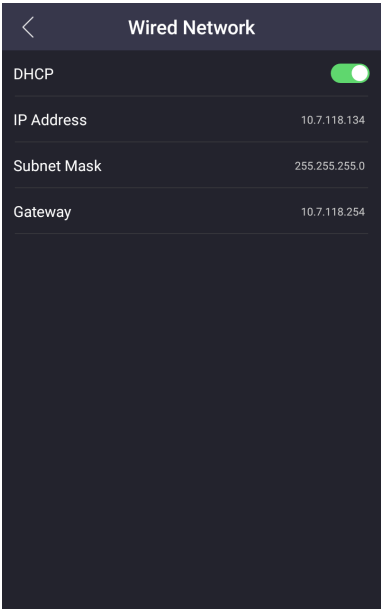


Figure 7-8 Wired Network Settings

2. Edit the wired network parameters.
- Edit the wired network parameters manually.
- Enable **DHCP**, and the system will get the parameters automatically.

7.3.2 Cloud Service Settings

Enable the function, you can configure and operate the device via mobile client remotely.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Network → Cloud Service** to enter the settings page.

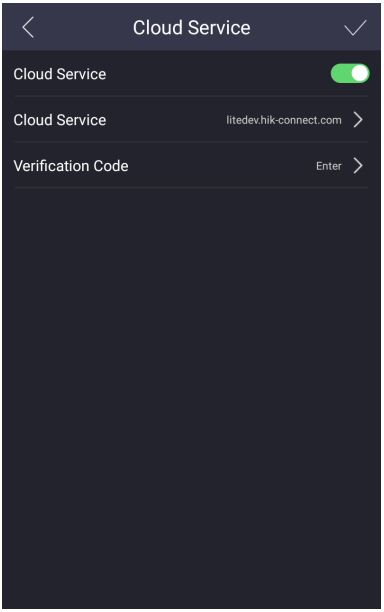


Figure 7-9 Cloud Service Settings

2. Slide to enable the function.

3. Edit the **Cloud Service Address** and create a **Verification Code**.

4. Tap **√** to save the settings.

7.4 Device No. Settings

Configure the No. of the device to make the communitcation easily.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

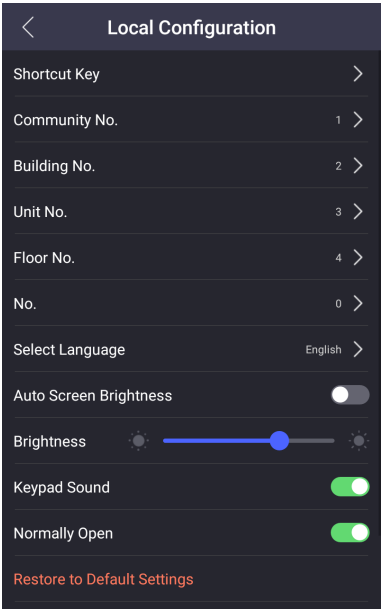


Figure 7-10 Local Configuration

2. Edit **Community No.**, **Building No.**, **Unit No.**, **Floor No.** and **No.** according to the actual needs.

7.5 User Management

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

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Person Management** to enter the settings page.
2. Tap **+** to enter the add user page.
3. Set **Room No.**
4. Add **Card**.

1) Tap **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.

5. Add **Face**.

1) Tap **Face Picture**, and point the face at the camera.
2) Tap to add the face.
3) Tap to enable the settings.

6. Add **Fingerprint**.

1) Select **Fingerprint**, and tap **+**.
2) Put your finger on the fingerprint reader and add the fingerprint.

7. Set **User Permission** as **User** or **Administrator**.

8. Exit the settings page.

7.6 Call Settings

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

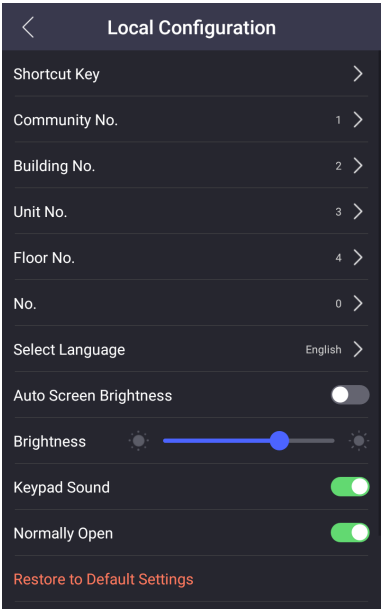


Figure 7-11 Local Configuration

2. Tap **Shortcut Key** to select call mode.

   Calling Menu

   Select call mode as **Calling Menu**. On the main page, tap call button to enter the calling page.

   Call Specified Room

   Select call mode as **Call Specified Room** and set the **Specified Room No.**. On the main page, tap call button to call the room you set.

   Call Center

   Select call mode as **Call Center**. On the main page, tap call button to call the management.

3. Exit the page to enable the settings.

7.7 Forget Admin Password

Admin password is used for authenticating to enter the local configuration menu. If you forget the password, you can change it by entering security questions' answers.

Steps

1. Hold the main page to enter the authentication page.

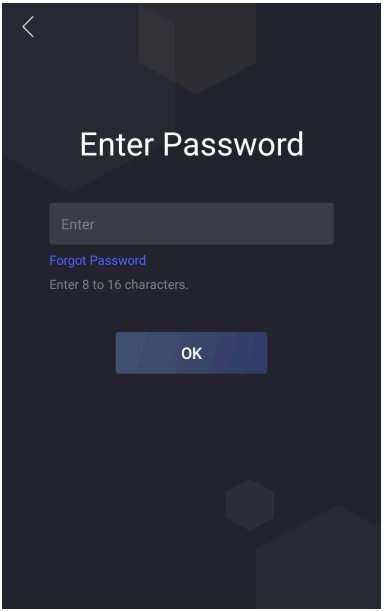


Figure 7-12 Authentication Page

2. Tap **Forgot Password**.

3. Change the admin password via entering answers of security questions or email address.

4. Create and confirm a new password.

7.8 System Settings

7.8.1 Change Language

Change language according to your actual needs.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

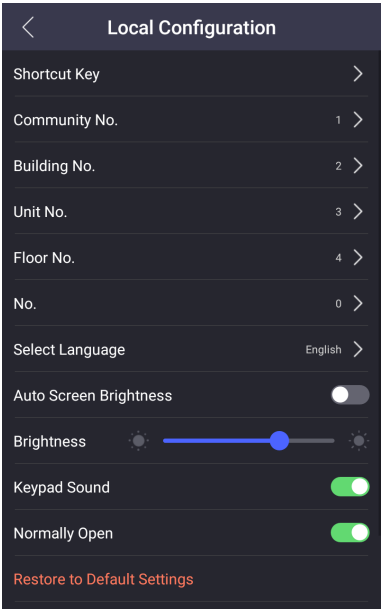


Figure 7-13 Local Configuration

2. Tap **Select Language** to switch the system language.

7.8.2 Adjust Brightness

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

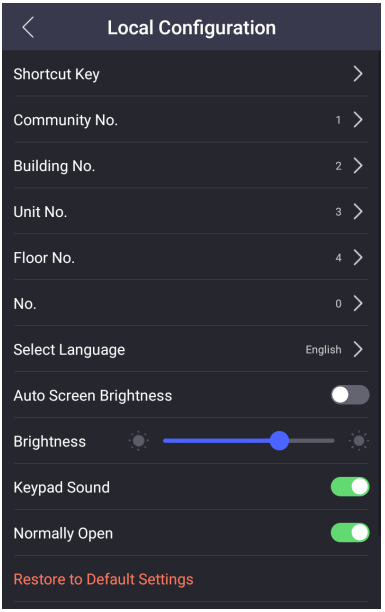


Figure 7-14 Local Configuration

2. Adjust the brightness of the device.

- Enable the **Auto Screen Brightness**, the device will adjust the brightness according to the environment automatically.
- Edit the number to adjust the brightness manually.

7.8.3 Keypad Sound Settings

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

On the menu, tap **Local Configuration** to enter the settings page.

Slide to enable or disable the **Keypad Sound**.

7.8.4 Channel Mode Settings

Enable the function, the door stays open.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

2. Slide to enable the function.

7.8.5 Theme Settings

Select theme of the system to make the device user friendly.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Preference** to enter the settings page.

2. Select theme of the system.

Note

If you select theme 2, you can edit advertisement or welcome words.

7.8.6 Restore Door Station

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **Local Configuration** to enter the settings page.

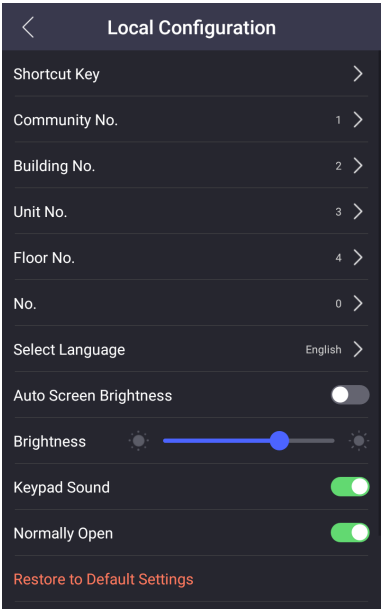


Figure 7-15 Local Configuration

2. Restore the device.

Restore to Default Settings

Tap **Restore to Default Settings** to reset all parameters, except IP address, subnet mask and default gateway, to the default settings.

Restore to Factory Settings

Tap **Restore to Factory Settings** to restore all parameters to default settings.

7.9 Device Information

View the device model, system version, App version and open source software licenses.

Before You Start

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

Steps

1. On the menu, tap **About** to enter the page.

Figure 7-16 About

2. You can view the device model, system version, App version and open source software licenses.

3. Optional: Scan the QR code to add the device to mobile client.

8 Local Operation

8.1 Call from the Device

Door station supports calling users or management center.

8.1.1 Call Resident

Call Resident from Main/Sub Door Station

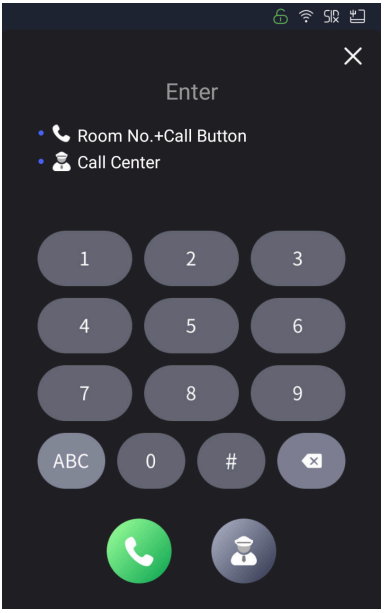


Figure 8-1 Call Resident

On the main page, tap 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).
- You can enter the related No. and tap to call residents if the function is enabled for the indoor stations. Refer to ***Device Management*** for details about related No. settings.

On the main page, tap contact button to enter the contact list.

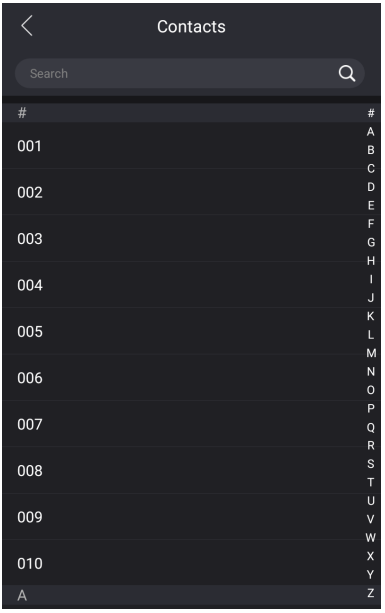


Figure 8-2 Contacts

Select a contact from the list to call. You can enter the name in the search bar or tap the letter on the right side of the screen to find a target contact.

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

8.1.2 Call Center

Refers to ***Call Settings*** to set the calling shortcut key.

Call Center by Calling Menu

If you set call mode as **Calling Menu**.

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.

Call Center by Shortcut Key

If you set call mode as **Call Center**, you can tap the call button on the main page to call.

8.2 Unlock Door

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

8.2.1 Unlock by Password

Tap call button on the main page to enter the calling page.

Enter 【# + Password】, and tap unlock button.

8.2.2 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.

8.2.3 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.

8.2.4 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.

9 Remote Configuration via Web

9.1 Live View

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

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

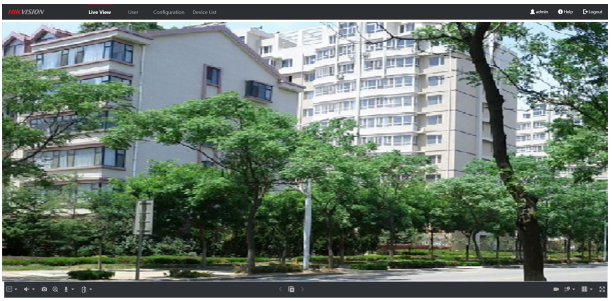


Figure 9-1 Live View

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

Note

Live View function may vary with different models. Please refer to the actual product.

9.2 User Management

You can manage user information on the page.

Steps

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

2. Click **Add** and complete related information to add users.

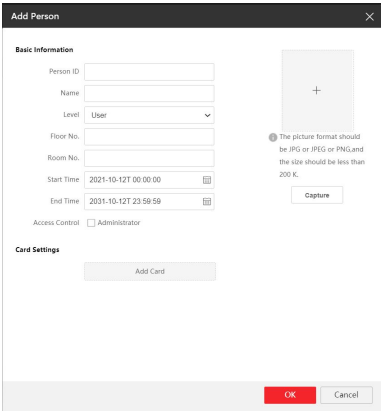


Figure 9-2 Add User

1) Enter **Person ID**, **Name**, **Floor No.**and**Room No.**. Select **Level**.
2) Configure **Start Time** and **End Time**.
3) Check **Administrator** and the person added will be able to log in by face recognition.
4) Click **Add Card**, enter **Card No.** and select **Property**. Or you can click **Read** and place the card on the card-reding zone.
5) Click **Capture** and make sure the face image of the person can be captured properly. Or you can click **+** to upload local images.

Note

The picture format should be JPG, JPEG or PNG, and the size should be less than 200 k.

6) Click **OK** to complete person adding.

3. Delete or edit users.
- Select users and click **Delete** to delete users.
- Click to edit user information.

4. Input keywords in the bar and click to search users, and the qualified users will be displayed on the result list.

9.3 Device Management

You can manage the linked device on the page.

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

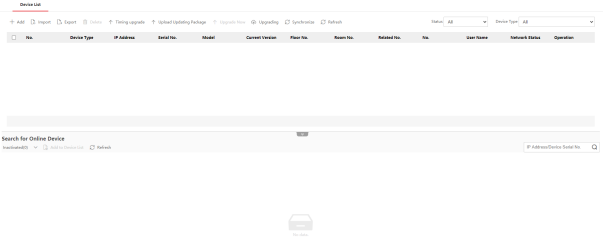


Figure 9-3 Device Management

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.

Note

You can set related No. with uppercase letters (must be contained) and digits for indoor stations. You can call residents or unlock door via related No.

Export

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

Delete

Select the device and click **Delete** to remove the selected device from the list.

Upgrade

Click **Timing Upgrade**, click to **Enable Upgrading Device Automatically** and configure **Start Time** and **End Time**. The devices will upgrade automatically at the set time.

Click **Upload Updating Package**, select **Upgrade File** and click **Browse** to upload upgrading package.

Select devices to be upgraded, and click **Upgrade Now** to upgrade devices manually.

Upgrading Status

Click **Upgrading** to view the upgrading status of the devices.

Synchronize

Click **Synchronize** and enable **Synchronize** for device synchronization.

Refresh

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

Optional: Set Device Information.

- Click to edit device information.
- Click to delete device information from the list.
- Select **Status** and **Device Type** to search devices.

Search for Online Devices

Click **Refresh** and the online devices will be list.

Check to select the device and click **Add to Device List**, you can link the device in the list to the door station.

9.4 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.

9.4.1 Local Settings

Live View 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 Start Live View: 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.
- Image Format: Set the save format of captured images.

Record File Settings

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

Picture and Clip Settings

Save snapshots in live view to: Capture file is stored locally, you can select**Browse**to change the saving path. Click**Open**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.

9.4.2 System Parameters

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

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

System Settings

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

Basic Information

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

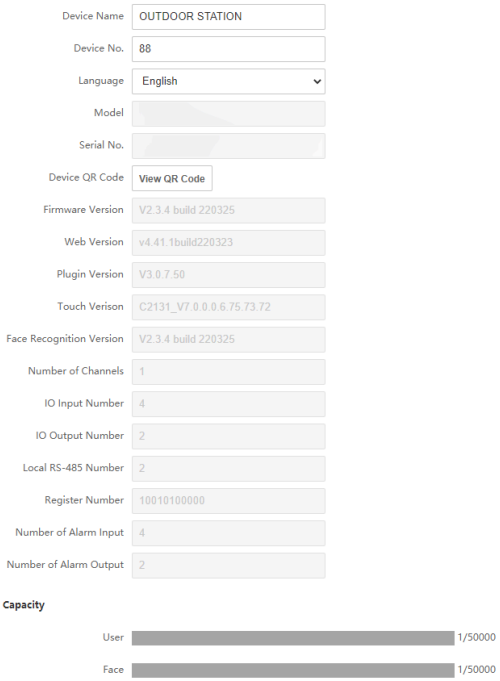


Figure 9-4 Basic Information

Click **View QR Code**, and you can use the mobile client to scan to add the device.

You can view the quantities of added users, face pictures and cards in **Capacity**.

Click **Save** to enable the settings.

Time Settings

Click **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.

About

Click **About** to enter the page. Click **View Licenses** to view open source software Licenses.

Maintenance

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

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

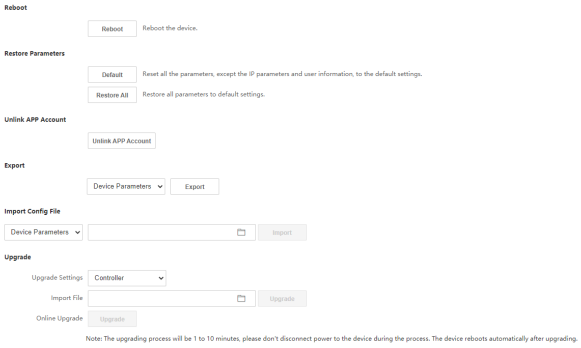


Figure 9-5 Maintenance

Reboot

Click **Reboot** to reboot the device.

Restore Parameters

Default

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

Restore All

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

Unlink APP Account

Click **Unlink APP Account** to unlink the account from the mobile client.

Export Parameters

1. Select **Device Parameters**, and click **Export** 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 icon to select the configuration file.
2. Click **Import** and enter the encryption password to import.

Upgrade

1. Click browse icon to select the upgrade file.
2. Click **Upgrade**.

Note

- The upgrading process will last 1 to 10 minutes, do not power off during the upgrading. The device reboots automatically after upgrading.
- You can select controller, display module and sub modules to upgrade.

Security Settings

Set the security service and certificate of the device.

Security Service

The device support SSH, ADB and HTTP protocols.

Steps

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

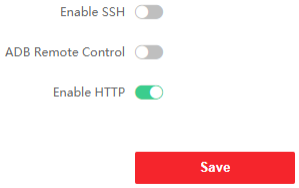


Figure 9-6 Security Service

2. On the page, you can enable SSH, ADB remote control and HTTP according to your actual needs.
3. Click **Save** to enable the settings.

Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Create Certificate

Steps

1. Select **Certificate Type** from the drop-list.
2. Click **Create**.
3. Follow the prompt to enter **Certificate ID**, **Country/Region**, **Hostname/IP**, **Validity** and other parameters.

   Note

   The certificate ID should be digits or letters and be no more than 64 characters.

4. Click **OK**
5. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate.

Import Passwords

Steps

1. Select **Certificate Type** from the drop-list.
2. Click **Browser** and select the certificate files from the PC.
3. Click **Install**.

Import Communication Certificates

Steps

1. Select **Certificate Type** from drop-list.
2. Click **Browser** to select the certificate and click **Install**.

Note

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

Import CA Certificate

Steps

1. Edit **Custom ID**.
2. Click **Browser** and select certificate files.
3. Click **Install**.

Note

Up to 16 certificates are allowed.

User Management

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

This is the start of your concept.

9.4.3 Network Settings

TCP/IP Settings

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

Steps

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

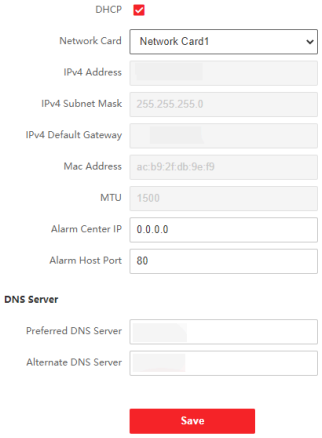


Figure 9-7 TCP/IP Settings

2. Select **Network Card**.

3. 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.

4. Configure the DNS server.

5. Edit **Alarm Center IP** and **Alarm Host Port**.

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

Port Settings

Steps

1. Click **Network → Basic Settings → Port** to enter the settings page.
2. Set the ports of the device.

   HTTP Port

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

   HTTPS Port

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

   RTSP Port

   The default port number is 554.

   Server Port

   The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.
3. Click **Save** to enable the settings.

SIP Setting

Steps

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

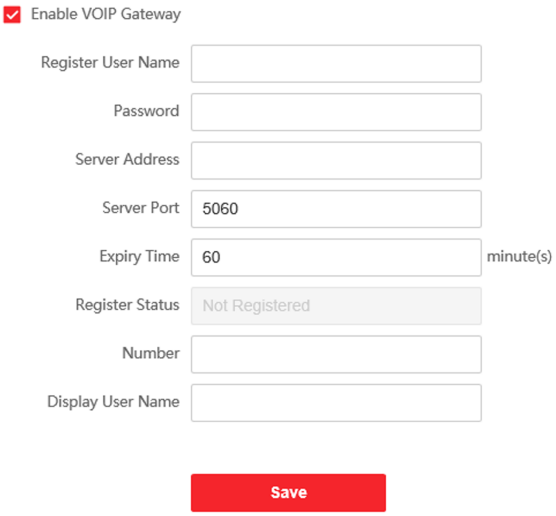


Figure 9-8 SIP Settings

2. Check **Enable VOIP Gateway**.

3. Configure the SIP parameters.

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

FTP Settings

Steps

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

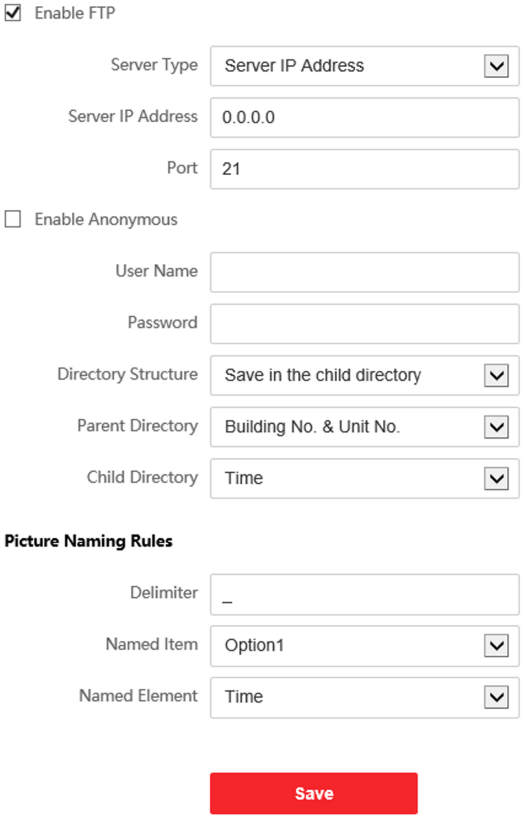


Figure 9-9 FTP Settings

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.

Platform Access

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.

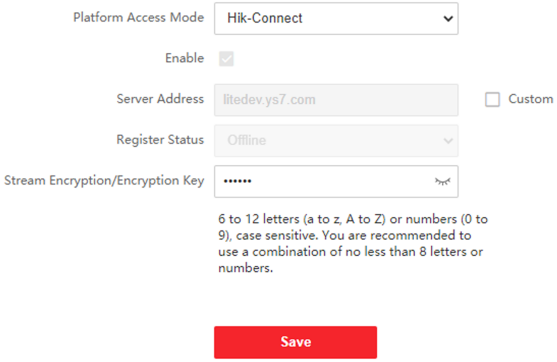


Figure 9-10 Platform Access

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.

Figure 9-11 HTTP Listening Settings

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

Capture Network Packet

Click **Network → Capture Network Packet** to enter the settings page.

Slide to adjust the **Capture Packet Duration** and **Capture Packet Size**.

Click **Capture** to get the network packet.

9.4.4 Video & Audio Settings

Video Parameters

Steps

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

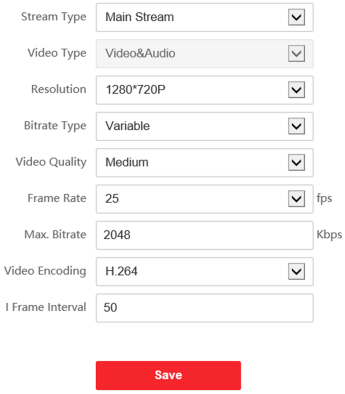


Figure 9-12 Video Parameters

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

Stream Type

Select the stream type to main stream or sub stream.

Video Type

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

Resolution

Select the resolution of the video output.

Bitrate Type

Select the bitrate type to constant or variable.

Video Quality

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

Frame Rate

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

Max. Bitrate

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

Video Encoding

The device supports H.264.

I Frame Interval

Set I Frame Interval from 1 to 400.

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

Audio Parameters

Steps

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

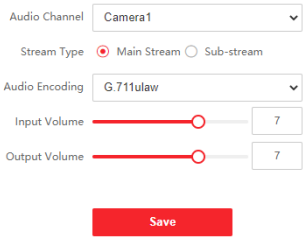


Figure 9-13 Audio Settings

2. Configure the stream type and the audio encoding type.

Audio Channel

Select the audio channel to adjust the audio parameters.

Stream Type

Select the stream type to main stream or sub stream.

Audio Encoding

The device support G.711ulaw and G.711 alaw.

3. Adjust the **Input Volume** and **Output Volume**.

Note

Available range of volume: 0 to 10.

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

9.4.5 Display Settings

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

Steps

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

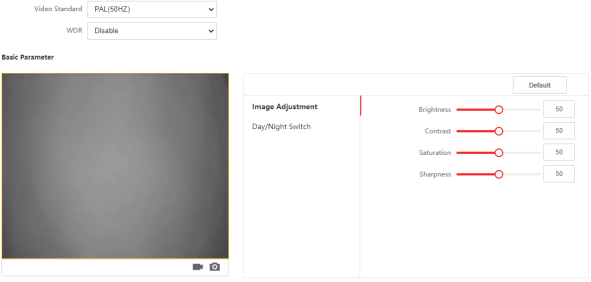


Figure 9-14 Display Settings

2. Select the **Format**.
3. Set the display parameters.

   WDR

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

   Brightness

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

   Contrast

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

   Saturation

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

   Sharpness

   Sharpness describes the edge contrast of the image, which ranges from 1 to 100.
4. Click **Day/Night Switch** to set the parameters.

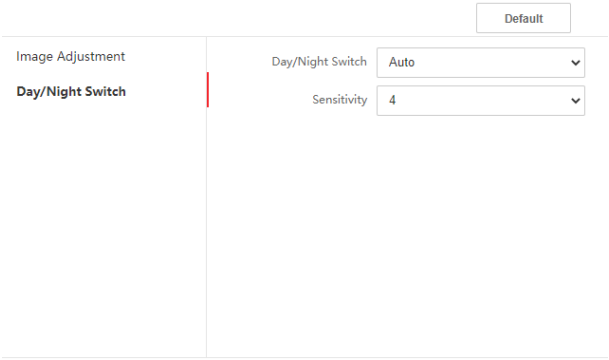


Figure 9-15 Day/Night Switch

Auto

Select **Day/Night Switch** as **Auto**, and set the **Sensitivity**. The device will switch between Day Mode and Night Mode automatically according to the environment.

Daytime

Select **Day/Night Switch** as **Daytime**. The device will keep the mode as daytime.

Night

Select **Day/Night Switch** as **Night**. The device will keep the mode as night.

Scheduled-Switch

Select **Day/Night Switch** as **Scheduled-Switch** and set the duration. The device will keep the mode as daytime during the duration you set. And switch to the night mode except the duration.

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

9.4.6 Card Security

Click **General → Card Security** to enter the settings page.

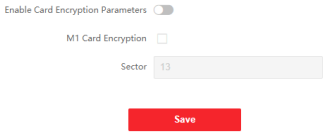


Figure 9-16 Card Security

Slide to enable card encryption parameters.

Click **Save** to enable the settings.

9.4.7 Intercom Settings

Device No. Configuration

Set the No. of the device, and linked devices can build a communication.

Steps

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

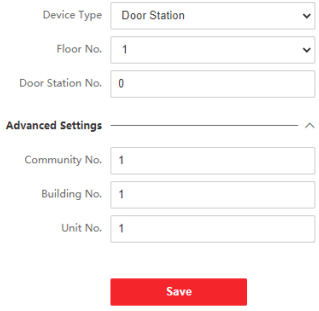


Figure 9-17 Device No. Settings

2. Select the device type from the drop-down list, and set the corresponding information.

3. Click **Save** to enable the device number configuration.

Note

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

Linked Network Settings

Steps

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

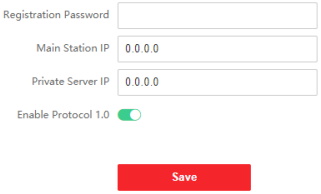


Figure 9-18 Session Settings

2. Set **Registration Password**.

3. Set **Main Station IP** and **VideoIntercom Server IP**.

4. Enable Protocol 1.0.

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

Permission Password

Steps

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

Figure 9-19 Password Settings

2. Click **+Add** to create a password.

1) Create a password.

2) Check to select unlock permission.

3) **Optional:** Enter the remarks of the password.

3. Click **OK** to save the password.

Call Settings

Click **Intercom → Call Settings** to enter the page.

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

Note

- For door station, maximum call duraion and maximum message duration should be configured.
- Maximum speaking time varies from 90s to 120s, and maximum message time varies from 30s to 60s.

Ringbacktone Settings

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

Click **+Add** to select the ringtone file from the local PC.

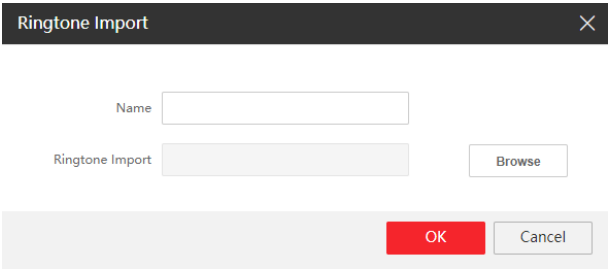


Figure 9-20 Ringtone Settings

Note

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

Number Settings

Steps

1. Click **Intercom → Number Settings** , and you can view the No., room No., and SIP number.
2. Add the number.
   1) Click **Add**.
   2) Enter **Room No.**, and **SIP**.
   3) **Optional:** Click **Add** to add SIP according to the actual needs.
   4) Click **OK**.
3. **Optional:** Click ⚙ to edit the number.

9.4.8 Access Control Settings

Door Parameters

Set the parameters of the door which is linked to the device.

Steps

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

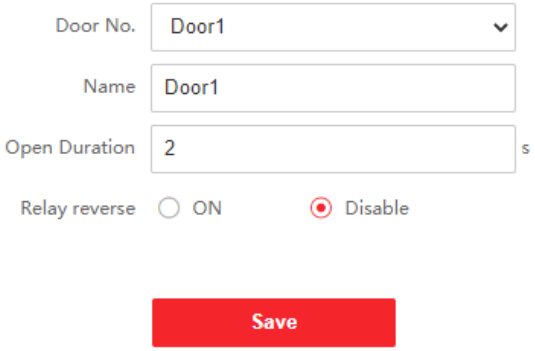


Figure 9-21 Door Parameters

2. Select **Door No.**, and edit the **Name**.
3. Set **Open Duration**. When the time to open over the open duration you set, the door will be locked again.
4. Select **Relay Reverse** as **ON** or **Disable**.
5. Click **Save** to enable the settings.

Elevator Control

Before You Start

Make sure that the door station is in the mode of main door station. Only the main door station supports elevator control function.

Steps

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

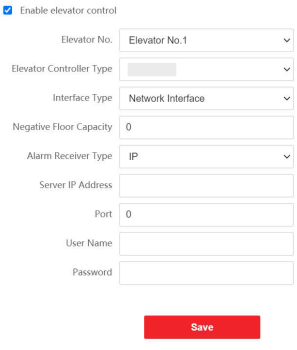
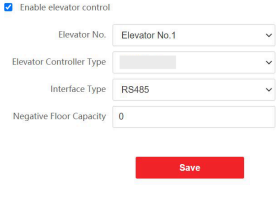


Figure 9-22 Elevator Control

2. Check to enable elevator control function.
3. Select an Elevator No., and select an elevator controller type for the elevator.
4. Select **Interface Type**.

Note

If you select **Interface Type** as **RS-485**, you only need to enter **Negative Floor Capacity**.



5. Enter **Negative Floor Capacity**, and select **Alarm Receiver Type**.
6. Enter the elevator controller's **Server IP Address**, **Port No.**, **User Name**, and **Password**.
7. Click **Save** to enable the settings.

Note

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

RS-485 Settings

Set the working mode to linked device.

Steps

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

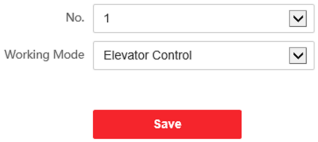


Figure 9-23 RS-485 Settings

2. Select the No.

3. Select the working mode.

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

9.4.9 Smart Settings

Biometrics Settings

Adjust the face recognition parameters and fingerprint parameters according to your needs.

Steps

1. Click **Smart** to enter the settings page.

2. Enable face anti-spoofing to edit face capture advanced parameters.

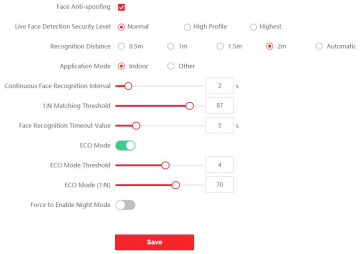


Figure 9-24 Smart Settings

Table 9-1 Face Capture Advanced Parameters

Parameter	Description
Face Anti-spoofing	Enable face anti-spoofing to detect real people face for recognition.
Live Face Detection Security Level	After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.
Recognition Distance	Set the valid distance between the user and the camera when authenticating.
Application Mode	Select either others or indoor according to actual environment.
Continuous Face Recognition Interval	The time interval between two continuous face recognitions when authenticating. **Note** You can input the number from 1 to 10.
1:N Matching Threshold	Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. **Note** You can input the number from 1 to 99.

Parameter	Description
Face Recognition Timeout Value	When the face recognition time exceed the value you set, the recognition will be determined as a timeout operation. **Note** You can input the number from 1 to 20.
ECO Settings	After enabling the ECO mode, the device will use the IR camera to authenticate faces in the low light or dark environment. And you can set the ECO mode threshold, ECO mode (1:N). **ECO Threshold** When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode. **Note** You can input the number from 1 to 7. **ECO Mode (1:N)** Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. **Note** You can input the number from 1 to 100. **Force to Enable Night Mode** When the environment is not bright enough, you can slide to force to enable the night mode.

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

Area Configuration

Click **VCA Configuration → Area Configuration** to enter the settings page.

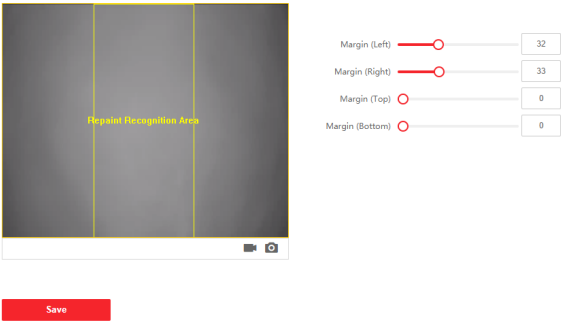


Figure 9-25 Area Configuration

Drag the frame or enter the digits behind the parameters to adjust the size of the recognition area.

9.4.10 Theme Settings

Set the advertisement on the main page of the device.

Steps

1. Click **Configuration → Theme** to enter the settings page.

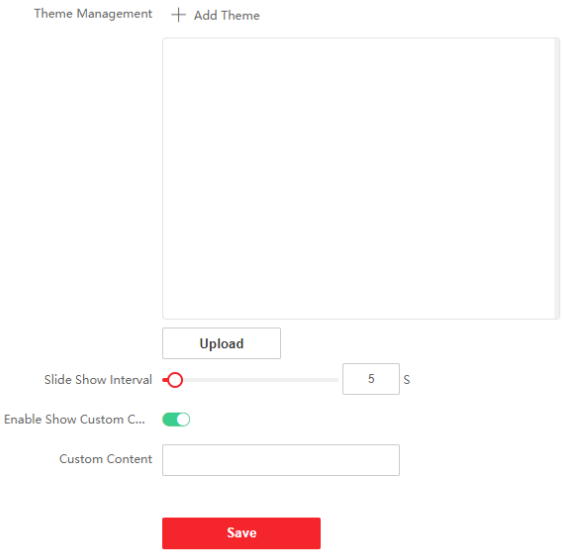


Figure 9-26 Theme Settings

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**.

10 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.

10.1 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.

10.2 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.

10.2.1 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.

10.2.2 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**.

10.2.3 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.

10.2.4 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.

10.2.5 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**.

10.3 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.

10.4 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).

10.5 Live View

10.6 Intercom Organization Structure Configuration

10.6.1 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.

10.6.2 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.

10.7 Person Management

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

10.7.1 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.

10.7.2 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.

10.7.3 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.

10.7.4 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.

10.7.5 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.

10.7.6 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.

10.8 Video Intercom Settings

10.8.1 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**.

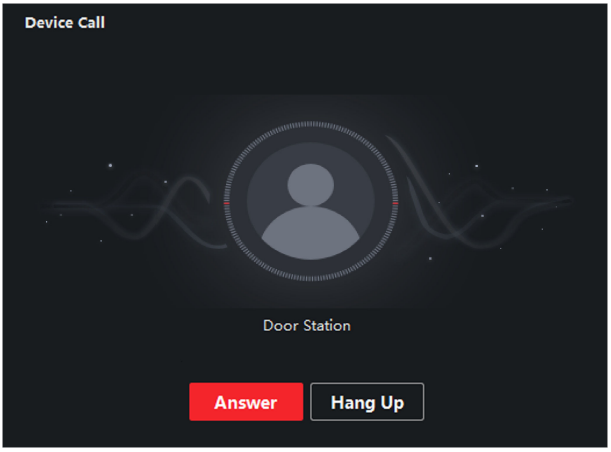


Figure 10-1 Answer the Call

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.

10.8.2 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.

10.8.3 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.

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

UD27981B