

The logo consists of a red horizontal bar with a white diagonal stripe on the left side. The word "HIKVISION" is written in white, italicized, uppercase letters on the red background.

***HIKVISION***

# **Module Door Station**

**Configuration Guide**

# Legal Information

## User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

## About this Manual

This Manual is subject to domestic and international copyright protection. Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") reserves all rights to this manual. This manual cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Please use this user manual under the guidance of professionals.

## Trademarks

**HIKVISION** and other Hikvision marks are the property of Hikvision and are registered trademarks or the subject of applications for the same by Hikvision and/or its affiliates. Other trademarks mentioned in this manual are the properties of their respective owners. No right of license is given to use such trademarks without express permission.

## Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THIS MANUAL. HIKVISION DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE OF THE MANUAL, OR THE CORRECTNESS, ACCURACY, OR RELIABILITY OF INFORMATION CONTAINED HEREIN. YOUR USE OF THIS MANUAL AND ANY RELIANCE ON THIS MANUAL SHALL BE WHOLLY AT YOUR OWN RISK AND RESPONSIBILITY.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT




TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

# Symbol Conventions

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

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

## 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

### FCC Conditions

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

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

### EU Conformity Statement



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



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

### Industry Canada ICES-003 Compliance

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

# Contents

1 Device Configuration .....	1
1.1 Activate Device .....	1
1.2 Edit Network Parameters .....	2
1.3 Add Device .....	3
1.4 Reset Password .....	4
1.5 System .....	5
1.6 Configure Video Intercom Parameters .....	9
1.6.1 Device ID Configuration .....	9
1.6.2 Time Parameters .....	10
1.6.3 Permission Password .....	11
1.6.4 Access Control and Elevator .....	11
1.6.5 I/O Input and Output .....	13
1.6.6 Volume Input and Output .....	13
1.6.7 Dial .....	14
1.6.8 Motion Detection .....	15
1.6.9 Intercom Protocol .....	16
1.6.10 Sub Module .....	16
1.7 Configure Video Intercom Network .....	18
1.7.1 Local Network Configuration .....	18
1.7.2 Linked Device Network Configuration .....	19
1.7.3 FTP .....	20
1.7.4 Advanced Settings .....	21

1.8 Person and Card Management .....	22
1.8.1 Organization Management .....	23
1.8.2 Person Management .....	24
1.9 Video Display .....	33
1.9.1 Video Parameters .....	33
1.9.2 Video & Audio .....	34
1.10 BLC Mode .....	35
2 Video Intercom Operation .....	36
2.1 Video Intercom Operation via Device .....	36
2.1.1 Call Resident .....	36
2.1.2 Issue Card .....	36
2.1.3 Unlock Door .....	37
2.2 Video Intercom Operation via Client Software .....	38
2.2.1 Receive Call from Door Station .....	38
2.2.2 Live View via Door Station .....	39
2.2.3 View Call Logs .....	40
2.2.4 Search Video Intercom Information .....	40



# 1 Device Configuration

## 1.1 Activate Device

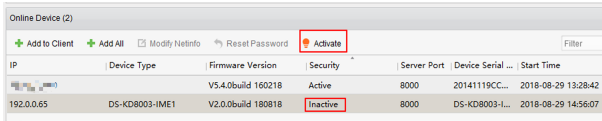
You can only configure and operate the door station after creating a password for the device activation.

Default parameters of door station are as follows:

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

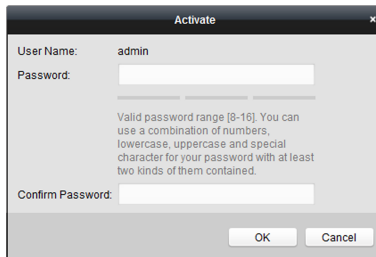
### Steps

1. Run the client software, enter **Device Management**, check the **Online Device** area.
2. Select an inactivated device and click the **Activate**.



**Figure 1-1 Online Device Area**

3. Create a password, and confirm the password.



**Figure 1-2 Activate Device**

### 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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

### Note

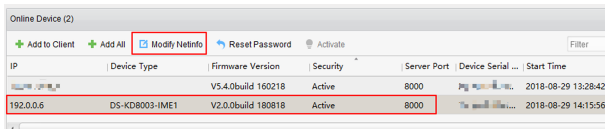
- When the device is not activated, the basic operation and remote operation of device cannot be performed.
- You can hold the **Ctrl** or **Shift** key to select multiple devices in the online devices, and click the **Activate** button to activate devices in batch.

## 1.2 Edit Network Parameters

To operate and configure the device via LAN (Local Area Network), you need connect the device in the same subnet with your PC. You can edit network parameters via **iVMS-4200** client software.

### Steps

1. Select an online activated device and click the **Modify Netinfo**.



**Figure 1-3 Edit Network Parameters**

2. Edit the device IP address and gateway address to the same subnet with your computer.
3. Enter the password and click **OK** to save the network parameters modification.

**Device Information:**

MAC Address:

Software Version:

Device Serial No.:

**Network Information:**

DHCP

Port:

Save IPv4 Settings

IP Address:

Subnet Mask:

Gateway:

Save IPv6 Settings

Password:

**Figure 1-4 Modify Parameters**

### Note

- The default port No. is 8000.
- The default IP address of the door station is 192.0.0.65.
- After editing the network parameters of device, you should add the devices to the device list again.

## 1.3 Add Device

To configure the device remotely, you need to add the device to **iVMS-4200** client software.

### Steps

1. Select the activated device and click **Add to Client**.

IP	Device Type	Firmware Version	Security	Server Port	Device Serial ...
10.6.113.120	DS-KD8003-IME1	V2.0.0build 180818	Active	8000	DS-KD8003-1...

**Figure 1-5 Add Device**

2. Enter corresponding information, and click **Add**.

Adding Mode:

IP/Domain     IP Segment     Hik-Connect D...     EHome     Serial Port

IP Server     HIDDNS     Batch Import

Add Offline Device

Nickname: Main Unit

Address: 10.6.113.120

Port: 8000

User Name: admin

Password: .....

Export to Group

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

Add Cancel

Figure 1-6 Add to the Client

## 1.4 Reset Password

You can restore the default password or resetting the password for the door station.

### Steps

1. Select the device from the online device list, click **Reset Password**. If the window with import file button, key importing mode drop-down list, password and confirm password field pops up.
2. Click **Export** to save the device file on your computer.
3. Send the file to our technical engineers.
4. Our technical engineer will send you a file to you. After receiving a file from the technical engineer, select **Import File** from Key Importing Mode drop-down list and click ... to import the file.
5. Input new password in text fields of **Password** and **Confirm Password**.
6. Click **OK** to reset 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 reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

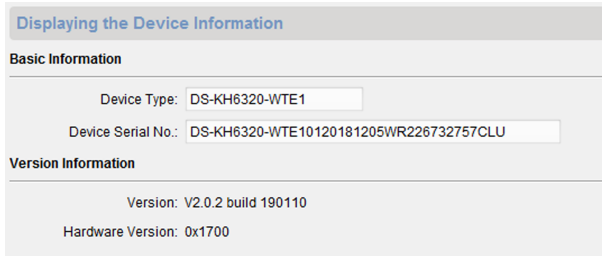
---

## 1.5 System

Click **System** on the remote configuration page to display the device information: Device Information, General, Time, System Maintenance, User, and RS-485.

### Device Information

Click Device Information to enter device basic information page. You can view basic information (the device type, and serial No.), and version information of the device.



The screenshot shows a web interface titled "Displaying the Device Information". It is divided into two sections: "Basic Information" and "Version Information".

Basic Information	
Device Type:	<input type="text" value="DS-KH6320-WTE1"/>
Device Serial No.:	<input type="text" value="DS-KH6320-WTE10120181205WR226732757CLU"/>

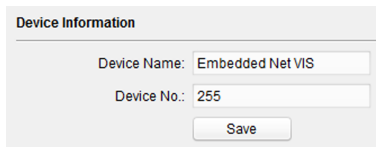
  

Version Information	
Version:	V2.0.2 build 190110
Hardware Version:	0x1700

Figure 1-7 Device Information

### General

Click **General** to enter device general parameters settings page. You can view and edit the device name and device ID.



The screenshot shows a web interface titled "Device Information" with a "General" section. It contains two input fields and a "Save" button.

Device Name:	<input type="text" value="Embedded Net VIS"/>
Device No.:	<input type="text" value="255"/>
<input type="button" value="Save"/>	

Figure 1-8 General

## Time

Click **Time** to enter the device time settings page.

Configuring the Time Settings (e.g., NTP)

Time Zone

Select Time Zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singa...

Enable NTP

Server Address: 0.0.0.0

NTP Port: 123

Sync Interval: 60 Minute(s)

Enable DST

Start Time: April First Week Sun 2 :00

End Time: October Last Week Sun 2 :00

DST Bias: 60 min

Synchronization Save

**Figure 1-9 Synchronize Time**

Select **Time Zone** or **Enable NTP**. Click **Save** to save the time settings.

- Time Zone
  - Select a time zone from the drop-down list menu.
  - Click the **Synchronization**.
- NTP
  - Check the checkbox of Enable NTP to enable NTP.
  - Enter the server address, NTP port, and synchronization interval.
- DST
  - Check the checkbox of Enable DST to enable DST.
  - Enter the start time and end time of DST, and set the DST bias.

---

 **Note**

The default port No. is 123.

---

## System Maintenance

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

The screenshot displays the 'System Maintenance' interface. It is divided into three main sections: 'System Management', 'Remote Upgrade', and 'Language'.  
1. **System Management**: Contains five buttons: 'Reboot', 'Restore Default Settings', 'Restore All', 'Import Configuration File', and 'Export Configuration File'.  
2. **Remote Upgrade**: Includes a 'Select Type' dropdown menu with 'Upgrade File' selected, a 'Select File' input field with a file selection icon (three dots), and an 'Upgrade' button. Below this is a 'Progress' indicator, which is currently a greyed-out progress bar.  
3. **Language**: Features a dropdown menu set to 'English' and a 'Save' button.

**Figure 1-10 System Maintenance**

- Click **Reboot** and the system reboot dialog box pops up. Click **Yes** to reboot the system.
- Click **Restore Default Settings** to restore the default parameters.
- Click **Restore All** to restore all parameters of device and reset the device to inactive status.

---

 **Note**

- Click **Restore Default Settings**, all default settings, excluding network parameters, will be restored.
  - Click **Restore All**, all default settings, including network parameters, will be restored. The device will be reset to inactivated status.
- 
- Click **Import Configuration File** and the import file window pops up. Select the path of remote configuration files. Click **Open** to import the remote configuration file. The configuration file is imported and the device will reboot automatically.

- Click **Export Configuration File** and the export file window pops up. Select the saving path of remote configuration files and click **Save** to export the configuration file.
- Click ... to select the upgrade file and click **Upgrade** to remote upgrade the device. The process of remote upgrade will be displayed in the process bar.
- Select a language, and click **Save** to change the device system language.

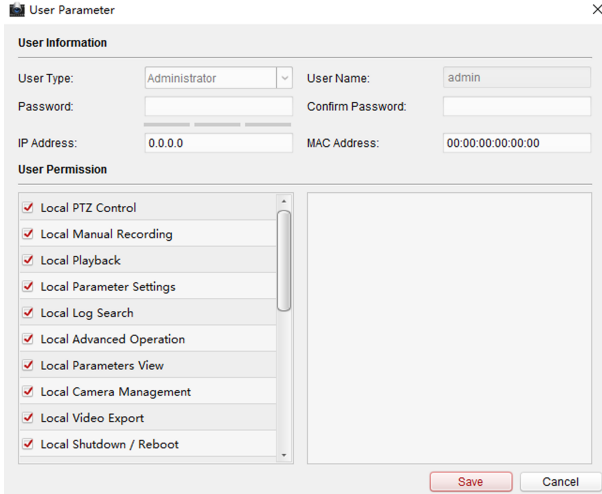
 **Note**

- The device supports 5 languages: English, Russian, French, Portuguese, and Spanish.
- Rebooting the device is required after you change the system language.

## User

Click **User** to enter the user information editing page.

Select the user to edit and click **Modify** to enter the user parameter page.



**Figure 1-11 User Page**

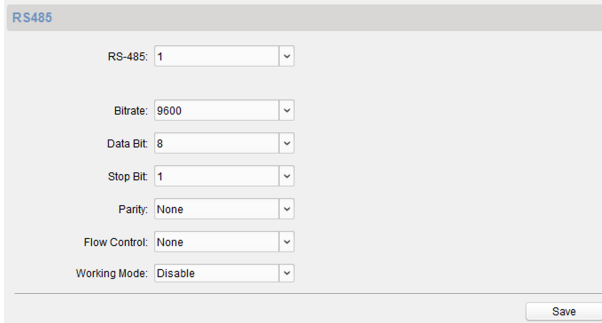


 **Note**

- The new password and confirm password should be identical.
  - After editing the password of device, click refresh button from the device list, the added device will not be there. You should add the device again with new password to operate the remote configuration.
- 

### RS-485

Click **RS485** to enter the RS-485 settings page. You can view and edit the RS-485 parameters of the device.



RS485

RS-485: 1

Btrate: 9600

Data Bit: 8

Stop Bit: 1

Parity: None

Flow Control: None

Working Mode: Disable

Save

**Figure 1-12 RS-485 Settings**

 **Note**

For indoor station and master station, there are 3 choices for the working mode: transparent channel, disable, and custom.

---

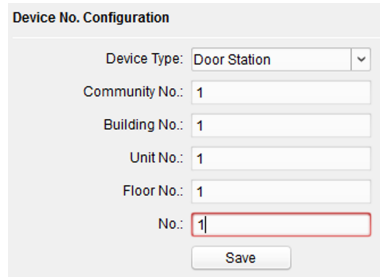
## 1.6 Configure Video Intercom Parameters

Click **Video Intercom** on the remote configuration page to enter the video intercom parameters settings: Device Number Configuration, Time Parameters, Access and Elevator Control, IO Input/Output, Volume, Dial, Sub Module and so on.

### 1.6.1 Device ID Configuration

### Steps

1. Click **ID Configuration** to enter the device ID configuration page.



The screenshot shows a form titled "Device No. Configuration". It contains the following fields: "Device Type" (a dropdown menu set to "Door Station"), "Community No.:" (text input with "1"), "Building No.:" (text input with "1"), "Unit No.:" (text input with "1"), "Floor No.:" (text input with "1"), and "No.:" (text input with "1", highlighted with a red border). A "Save" button is located at the bottom of the form.

**Figure 1-13 Device No. Configuration**

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

---

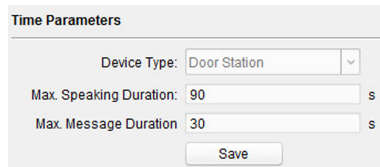
### Note

- For main door station, the serial No. is 0.
  - For sub door station, the serial No. is higher than 0. Serial No. ranges from 1 to 99.
  - For each villa or building, at least one main door station should be configured, and sub door stations can be customized.
  - For one main door station, at most 8 sub door stations can be customized.
- 

## 1.6.2 Time Parameters

### Steps

1. Click **Time Parameters** to enter time parameters settings page.



The screenshot shows a form titled "Time Parameters". It contains the following fields: "Device Type" (a dropdown menu set to "Door Station"), "Max. Speaking Duration:" (text input with "90" and a unit "s"), and "Max. Message Duration" (text input with "30" and a unit "s"). A "Save" button is located at the bottom of the form.

**Figure 1-14 Time Parameters**

2. Configure the maximum ring duration, maximum live view time, and call forwarding time.
3. Click **Save**.

---

 **Note**

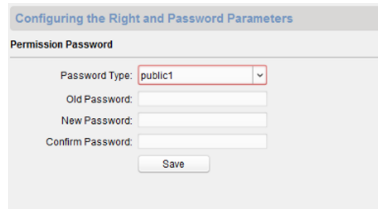
For door station, maximum speaking time and maximum message time should be configured. Maximum speaking time varies from 90 s to 120 s, and maximum message time varies from 30 s to 60 s.

---

### 1.6.3 Permission Password

#### Steps

1. Click **Permission Password** to enter the permission password page.



**Figure 1-15 Permission Password**

2. Edit the password accordingly.
3. Click **Save** to enable the settings.

---

 **Note**

- You can configure 3 public passwords.
  - You can open the door by entering # + public password + # at the door station.
- 

### 1.6.4 Access Control and Elevator

#### Before You Start

- Make sure your door station is in the mode of main door station. Only the main door station support elevator control function.
- Connection between the door station and the elevator controller supports network interface.

### Steps

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

**Access Control**

Upload Alarm for Not-Closed Door

Door No.: 1

Door-unlocked Duration: 15 s

Door Name: \_\_\_\_\_

Encrypt Card

Save

**Elevator Control**

Elevator No.: 1

Elevator Type: DS-K2210

Negative Floor: 0

Interface Type: Network Interface

Tip: All elevators should use the same interface type.

Enable Or Not: No

Server IP Address: 0.0.0.0

Server Port: 0

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Save

**Figure 1-16 Access Control and Elevator**

2. Set the **Access Control** parameters.
  - 1) Select the door No.
  - 2) Set the **Door-unlocked Duration**.
  - 3) **Optional:** Enable **Upload Alarm for Not-Closed Door**.
  - 4) Click **Save** to enable the settings.

---

### Note

- The door-unlocked duration ranges from 1 s to 255 s.
- If you check **Upload Alarm for Not-Closed Door**, an alarm will be triggered automatically if the door is not locked in the configured duration.
- Enabling **Card Encrypt**, the door station can recognize the encrypted information of the card when you swiping the card on the door station.

3. Set the **Elevator Control** parameters.
  - 1) Select an elevator No., and select an elevator controller type for the elevator.
  - 2) Set the negative floor.

- 3) Select **network interface** as **interface type**. Enter the elevator controller's IP address, port No., user name, and password.
- 4) Enable the elevator control.

---

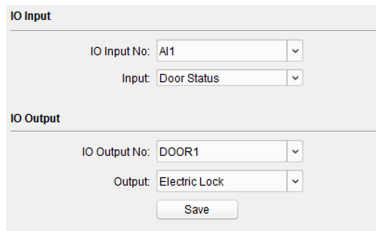
 **Note**

- 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.
- 

### 1.6.5 I/O Input and Output

#### Steps

1. Click **I/O Input and Output** to enter the I/O input and output settings page.



The screenshot shows a configuration interface for I/O settings. It is split into two main sections: 'IO Input' and 'IO Output'.  
In the 'IO Input' section, there are two dropdown menus: 'IO Input No.' is set to 'AJ1' and 'Input' is set to 'Door Status'.  
In the 'IO Output' section, there are two dropdown menus: 'IO Output No.' is set to 'DOOR1' and 'Output' is set to 'Electric Lock'. Below these dropdowns is a 'Save' button.

**Figure 1-17 I/O Input and Output**

2. Select **I/O input No.**, **input mode**, **output No.**, and **output mode**.
3. Click **Save** to enable the settings.

---

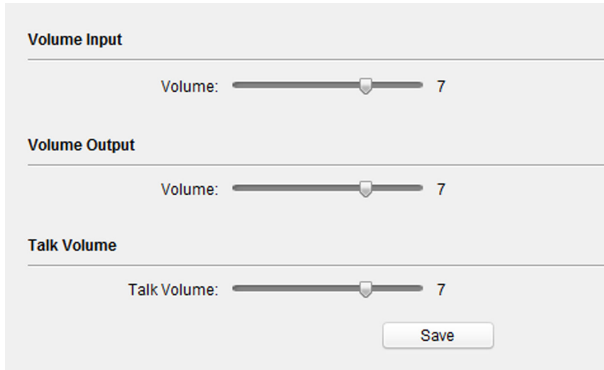
 **Note**

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

### 1.6.6 Volume Input and Output

**Steps**

1. Click **Volume Input/Output** to enter the volume input and output page.



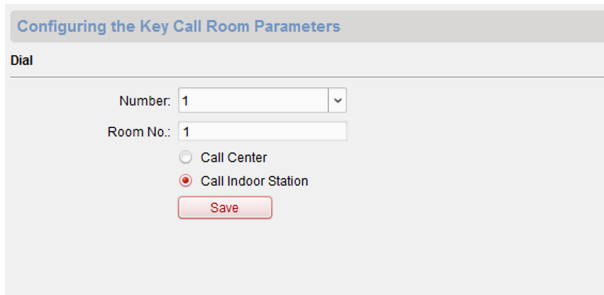
**Figure 1-18 Volume Input and Output**

2. Slide the slider to adjust the **volume input, volume output, and talk volume.**
3. Click **Save** to enable the settings.

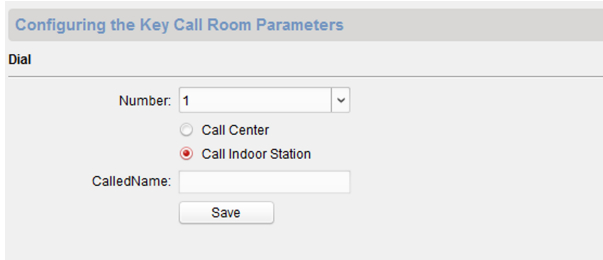
### 1.6.7 Dial

**Steps**

1. Click **Dial** to enter the dial page.



**Figure 1-19 Dial (Private SIP)**



**Figure 1-20 Dial (Standard SIP)**

2. Enter the room No. of the indoor station that the door station connected to.
3. Click **Save** to enable the settings.

---

 **Note**

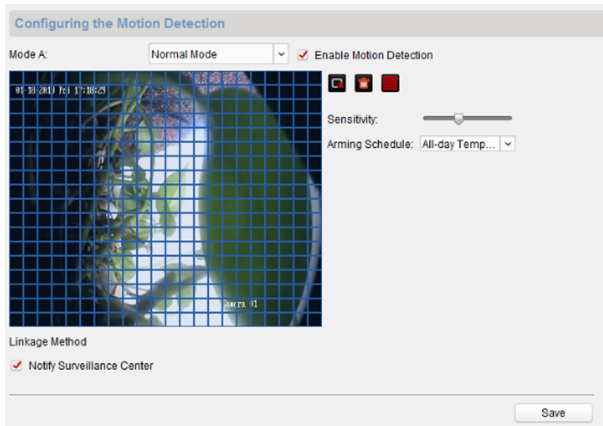
By default, quick press the call button, the door station calls resident. If you check Quick Press for Calling Center, the door station calls the management center when quick press the call button of the main unit.

---

### 1.6.8 Motion Detection

#### Steps

1. Click **Motion Detection** to enter the motion detection page.



**Figure 1-21 Motion Detection**

2. Enable **Enable Motion Detection**.
3. Configure the parameters.
4. Click **Save**.

---

 **Note**

The arming schedule is defaulted as all-day.

---

### 1.6.9 Intercom Protocol

#### Steps

1. Click **Intercom Protocol** to enter the intercom protocol page.
2. Select the protocol according to needs.
3. Click **Save**.

### 1.6.10 Sub Module

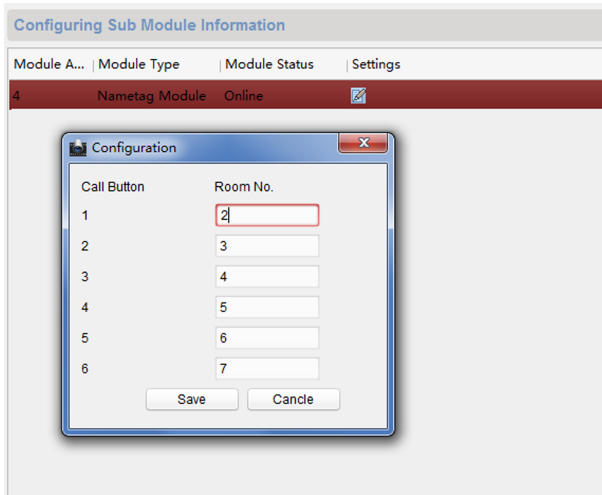
You can configured the room No. of nametag module and adjust the backlight of the display module.

#### Steps

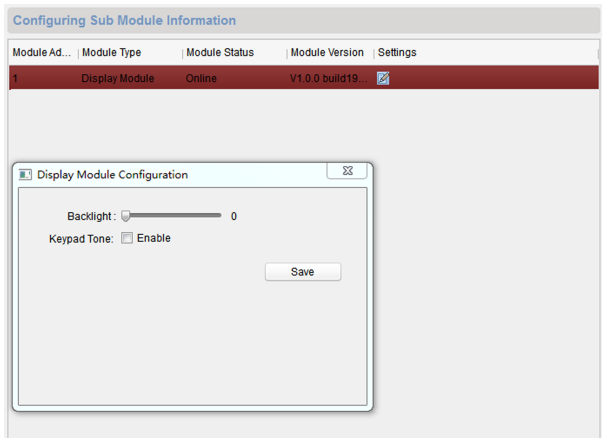
1. Click **Sub Module** to enter the sub module configuration page.



## Module Door Station Configuration Guide



**Figure 1-22 Nametag Module**

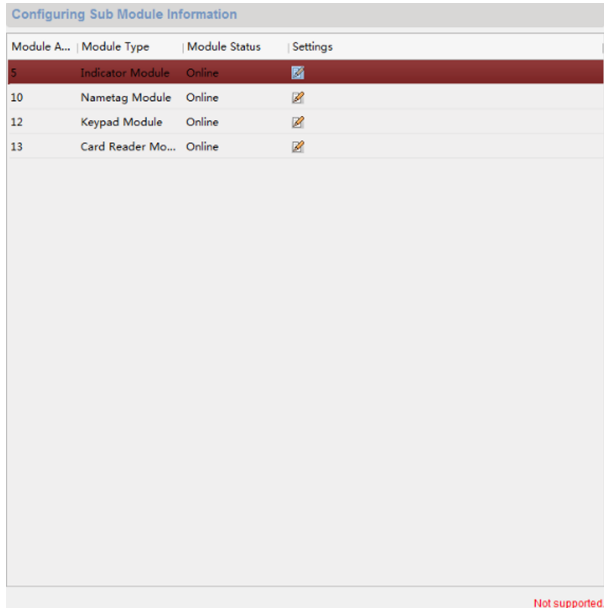


**Figure 1-23 Display Module**

2. **Optional:** Enter the **Room No.** for each call button of the nametag module.
3. Adjust the **Backlight** of the display module.
4. **Optional:** Enable **Keypad Tone**.
5. Click **Save**.

 **Note**

- The module address is used to differentiate the sub modules. See *Configure Sub Module Address* for detailed configuration instructions.
- For the other sub modules (indicator module, keypad module, display module and card reader module), it prompts **Not supported**.



The screenshot shows a table titled "Configuring Sub Module Information" with four columns: "Module A...", "Module Type", "Module Status", and "Settings". The first row is highlighted in red and contains the value "5" in the first column, "Indicator Module" in the second, "Online" in the third, and a pencil icon in the fourth. The second row contains "10", "Nametag Module", "Online", and a pencil icon. The third row contains "12", "Keypad Module", "Online", and a pencil icon. The fourth row contains "13", "Card Reader Mo...", "Online", and a pencil icon. At the bottom right of the table area, the text "Not supported." is visible in red.

Module A...	Module Type	Module Status	Settings
5	Indicator Module	Online	
10	Nametag Module	Online	
12	Keypad Module	Online	
13	Card Reader Mo...	Online	

**Figure 1-24 Configuring Sub Module Information**

- The room No. for the main unit's call button is 1 by default; and the room No. for the nametag modules call buttons are 2 to 7 by default.
- 

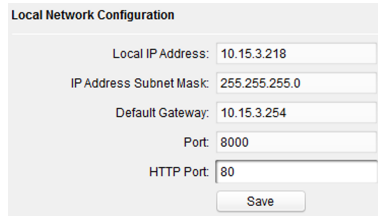
## 1.7 Configure Video Intercom Network

You need to configure video intercom network parameters in the network module. Click **Network** in the remote configuration interface, to configure the local network, linked network and FTP settings.

### 1.7.1 Local Network Configuration

### Steps

1. Click **Local Network Configuration** to enter local network configuration page.



The screenshot shows a web form titled "Local Network Configuration". It contains five input fields: "Local IP Address" with the value "10.15.3.218", "IP Address Subnet Mask" with "255.255.255.0", "Default Gateway" with "10.15.3.254", "Port" with "8000", and "HTTP Port" with "80". A "Save" button is located at the bottom right of the form.

**Figure 1-25 Local Network Configuration**

2. Enter the **Local IP Address, Subnet Mask, Default Gateway, Port** and **HTTP Port**.
3. Click **Save** to enable the settings.

---

### Note

- The default port No. is 8000.
  - After editing the local network parameters of device, you should add the devices to the device list again.
- 

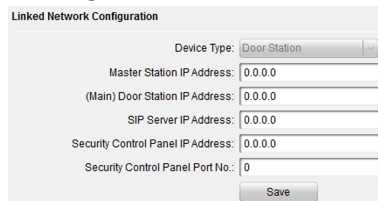
## 1.7.2 Linked Device Network Configuration

### Before You Start

On the linked devices network configuration page, you can configure the network parameters of master stations, SIP servers and management centers of the same LAN. The devices can be linked to the door station and realize the linkage between these devices.

### Steps

1. Click **Linked Network Configuration** to enter linked network configuration page.



The screenshot shows a web form titled "Linked Network Configuration". It features a "Device Type" dropdown menu set to "Door Station". Below it are five input fields: "Master Station IP Address" (0.0.0.0), "(Main) Door Station IP Address" (0.0.0.0), "SIP Server IP Address" (0.0.0.0), "Security Control Panel IP Address" (0.0.0.0), and "Security Control Panel Port No." (0). A "Save" button is at the bottom right.

**Figure 1-26 Linked Device Network**

2. Enter the **Master Station IP Address, (Main) Door Station IP Address, SIP Server IP Address, Security Control Panel IP Address and Port No.**
3. Select the main door station type from the drop-down list.
4. Click **Save** to enable the settings.

---

 **Note**

- After adding master station IP Address, the linkage between indoor station and master station can be realized.
  - After adding the door station IP Address, the video intercom between indoor stations of same building can be realized.
  - After adding SIP Server Address IP, the video intercom of same community: video intercom between indoor stations of different building, calling indoor station from outer door station and video intercom between management center and indoors.
  - After adding management center IP Address, the events can be uploaded to the management center.
  - For indoor extension, only parameter about the main indoor station should be configured.
- 

### 1.7.3 FTP

After configuring the FTP parameters, the captured pictures of door station will be uploaded to the FTP server automatically.

#### Steps

1. Click **FTP** to enter the FTP parameters settings page.

## Module Door Station Configuration Guide

---

**Figure 1-27 FTP Settings**

2. Enable **Enable Main FTP**.
3. Select IP address from the drop-down list of server mode.
4. Enter the FTP server address, and port No.
5. **Optional:** Enable the anonymity.
6. Enter the name and password.
7. Select the directory structure and set the separator, naming item, and naming element.
8. Click **Save** to enable the settings.

---

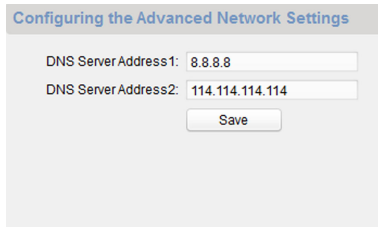
 **Note**

- The default port No. is 21.
  - To enable anonymity or not is according to whether the FTP server enables anonymity.
- 

### 1.7.4 Advanced Settings

#### Steps

1. Click **Advanced Settings** to enter the advanced network settings page.



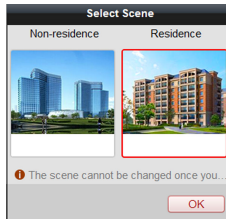
**Figure 1-28 Advanced Settings**

2. Enter the DNS server addresses.
3. Click **Save** to enable the settings.

## 1.8 Person and Card Management

You can add, edit, and delete the organization and person in Person and Card Management module. Organization and person management is necessary for the video intercom function.

For the first time opening the Access Control module, the following dialog will pop up and you are required to select the scene according to the actual needs. You can select the scene as **Non-residence** and **Residence**.



**Figure 1-29 Select Scene**

---

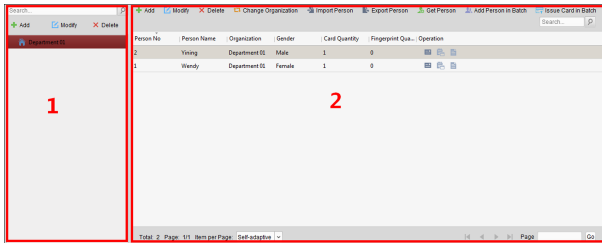
### Note

Once the scene is configured, you cannot change it later.

---

Click  →  to enter the **Person and Card Management** page.

## Module Door Station Configuration Guide



**Figure 1-30 Person and Card Management**

The page is divided into two parts: Organization Management and Person Management.

Organization Management	You can add, edit, or delete the organization as desired.
Person Management	After adding the organization, you can add the person to the organization and issue card to persons for further management.

### 1.8.1 Organization Management

#### Add Organization

##### Steps

1. In the organization list on the left, click **Add** to pop up the adding organization page.
2. Input the **Organization Name** as desired.
3. Click **OK** to save the adding.
4. You can add multiple levels of organizations according to the actual needs.
  - 1) You can add multiple levels of organizations according to the actual needs.
  - 2) Repeat Step 2 and Step 3 to add the sub organization.
  - 3) Then the added organization will be the sub-organization of the upper-level organization.

 **Note**

Up to 10 levels of organizations can be created.

---

## Modify and Delete Organization

You can select the added organization and click **Modify** to modify its name.

You can select an organization, and click **Delete** button to delete it.

---

 **Note**

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

## 1.8.2 Person Management

After adding the organization, you can add person to the organization and manage the added person such as issuing cards in batch, importing and exporting person's information in batch, etc.

---

 **Note**

Up to 10,000 persons or cards can be added.

---

## Add Person

Person information is necessary for the video intercom system. And when you set linked device for the person, the intercom between intercom devices can be realized.

### Steps

1. 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 is not editable.

---

2. Set basic person information.
  - 1) Enter basic information: person name, gender, phone No., birthday details, and email address.



 **Note**

The length of person name should be less than 15 characters.

---

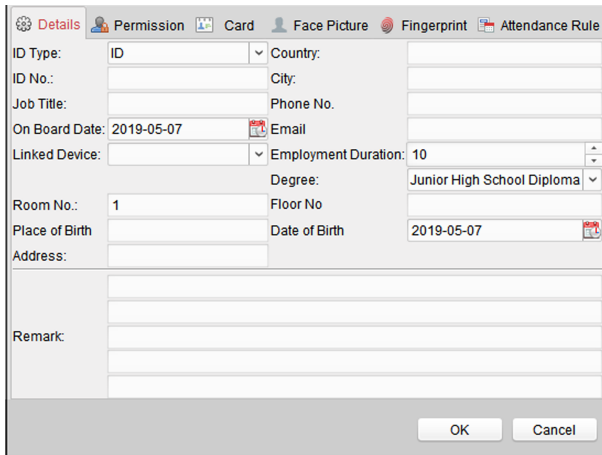
- 2) **Optional:** Click **Upload Picture** to select the person picture from the local PC to upload it to the client.
- 

 **Note**

The picture should be in \*.jpg format.

---

- 3) **Optional:** You can also click **Take Photo** to take the person's photo with the PC camera.
3. Set linked device for the person.
    - 1) Click **Details**.



**Figure 1-31 Details**

---

 **Note**

Room No. can be configured from 1 to 9999.

---

- 2) Set the linked devices.

**Linked Device**

You can bind the indoor station to the person.

 **Note**

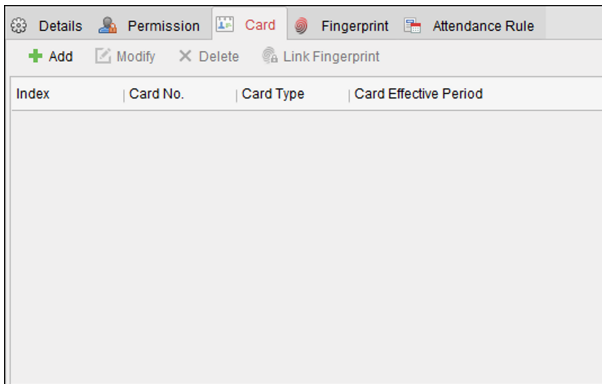
If you select **Analog Indoor Station** in the Linked Device, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

---

**Room No.**

You can enter the room No. of the person.

- 3) Click **OK** to save the settings.
4. Issue the card for the person.
  - 1) Click **Card**.



**Figure 1-32 Issue Card**

- 2) Click **Add** to pop up the Add Card dialog.

Card Smart Card

Card Type: Normal Card

Access Controller ...

Card Reader Mode:  Card Enrollment S...

Manually Input

Index	Card No.	Card Type	Card Class	Card Effic
-------	----------	-----------	------------	------------

**Figure 1-33 Add Card**

- 3) Select **Normal Card**.
- 4) Enter the password of the card itself in the Card Password field. The card password should contain 4 to 8 digits.
- 5) Enter Card Number manually.
- 6) Click **OK** and the card(s) will be issued to the person.

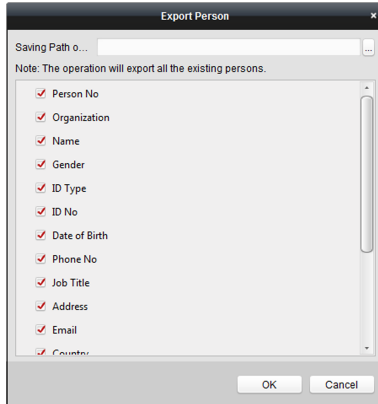
### Import and Export Person Information

The person information can be imported and exported in batch.

#### Steps

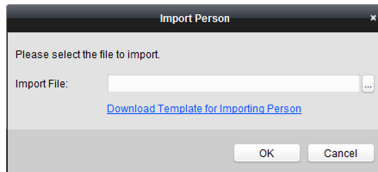
1. Exporting Person: You can export the added persons' information in Excel format to the local PC.

- 1) After adding the person, you can click **Export Person** to pop up the following dialog.
- 2) Click ... to select the path of saving the exported Excel file.
- 3) Check the checkboxes to select the person information to export.



**Figure 1-34 Export Person**

- 4) Click **OK** to start exporting.
2. Importing Person: You can import the Excel file with persons information in batch from the local PC.
- 1) Click **Import Person**.



**Figure 1-35 Import Person**

- 2) You can click **Download Template for Importing Person** to download the template first.
- 3) Input the person information to the downloaded template.
- 4) Click ... to select the Excel file with person information.
- 5) Click **OK** to start importing.

## Get Person Information from Device

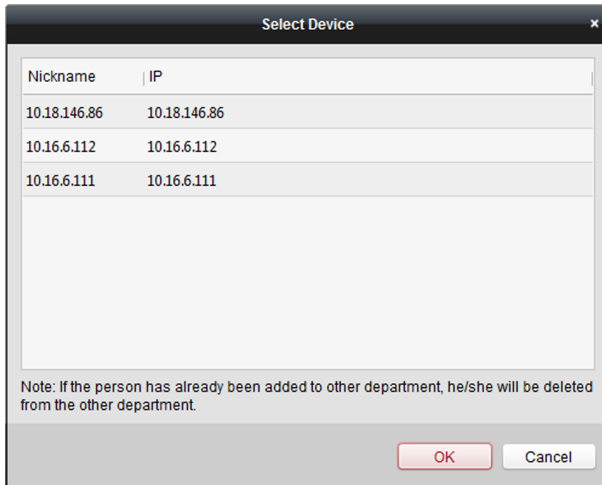
If the added device has been configured with person information (including person details, fingerprint, issued card information), you can get the person information from the device and import to the client for further operation.

### Steps

#### Note

This function is only supported by the device the connection method of which is TCP/IP when adding the device.

1. In the organization list on the left, click to select an organization to import the persons.
2. Click **Get Person** to pop up the following dialog box.





**Figure 1-36 Select Device**


3. The added access control device will be displayed.
4. Click to select the device and then click **OK** to start getting the person information from the device.
5. **Optional:** You can also double click the device name to start getting the person information.

 **Note**

- The person information, including person details, person's fingerprint information (if configured), and the linked card (if configured), will be imported to the selected organization.
  - If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
  - The gender of the persons will be **Male** by default.
- 

## Modify and Delete Person

To modify the person information and attendance rule, click  or  in the Operation column, or select the person and click **Modify** to open the editing person dialog.

You can click  to view the person's card swiping records.

To delete the person, select a person and click **Delete** to delete it.

---

 **Note**

If a card is issued to the current person, the linkage will be invalid after the person is deleted.

---

## Change Person to Other Organization

You can move the person to another organization if needed.

### Steps

1. Select the person in the list and click **Change Organization**.
2. Select the organization to move the person to.
3. Click **OK** to save the settings.

## Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can call contacts via display module.

### Steps

- For one person, you can add up to 4 access groups to one access control point of one device.
  - You can add up to 128 access groups in total.
  - When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).
1. Click **Access Control** → **Access Group** to enter the Access Group interface.
  2. Click **Add** to open the Add window.
  3. In the **Name** text field, create a name for the access group as you want.
  4. Select a template for the access group.

---

### Note

You should configure the template before access group settings. Refer to for details.

---

5. In the left list of the Select Person field, select person(s) and the person(s) will be added to the selected list .
6. In the left list of the Select Door field, select door(s) or door station(s) for the selected persons to access, and the selected door(s) or door station(s) will be added to the selected list.
7. Click **OK**.
8. After adding the access groups, you need to apply them to the access control device to take effect.
  - 1) Select the access group(s) to apply to the access control device.


To select multiple access groups, you can hold the **Ctrl** or **Shift** key and select access groups.
  - 2) Click **Apply All to Devices** to start applying all the selected access group(s) to the access control device or door station.



**Caution**

- Be careful to click **Apply All to Devices**, since this operation will clear all the access groups of the selected devices and then apply the new access group, which may bring risk to the devices.
  - You can click **Apply Changes to Devices** to only apply the changed part of the selected access group(s) to the device(s).
- 
- 3) View the apply status in the Status column or click **Applying Status** to view all the applied access group(s).

The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.

9. **Optional:** Click  to edit the access group if necessary.

## Issue Card in Batch

You can issue multiple cards for the person with no card issued in batch.

### Steps

1. Click **Issue Card in Batch** to enter the dialog page. All the added person with no card issued will display in the Person(s) with No Card Issued list.



## Module Door Station Configuration Guide

Card Type: Normal Card

Card Quantity: 1

Card Reader Mode:

- Access Controller Reader
- Card Enrollment Station
- Manually Input

Buttons: Read, Set Card Enrollment Station, Enter

Person(s) with No Card Issued

Person Name	Gender	Department
-------------	--------	------------

Person(s) with Card Issued

Person Name	Card No.	Gender	Departm
-------------	----------	--------	---------

Buttons: OK, Cancel

**Figure 1-37 Issue Card in Batch**

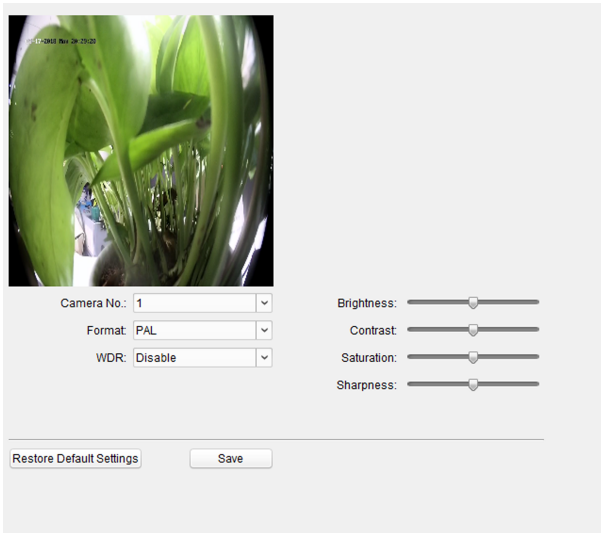
2. Select **Normal Card** as Card Type.
3. Enter the card quantity issued for each person.
4. Select the card reader mode and fill related information.
5. Click **Read/Enter**.
6. After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.
7. Click **OK**.

## 1.9 Video Display

### 1.9.1 Video Parameters

#### Steps

1. Click **Video Parameters** to enter the video parameters settings page.



**Figure 1-38 Video Parameters**

2. Select the **Camera No.**
3. Select the video standard (PAL and NTSC can be selected).
4. **Optional:** Enable **WDR** mode.
5. Set the **Brightness**, **Contrast**, **Saturation** and **Sharpness** of the video.
6. Click **Save**.

---

 **Note**

Click **Restore Default Settings** to restore all video parameters excluding network parameters to the factory settings.

---

### 1.9.2 Video & Audio

#### Steps

1. Click **Video & Audio** to enter the video parameters settings page.

## Module Door Station Configuration Guide

---

Video

Stream Type: Main Stream      Video Type: Video & Audio

Bitrate Type: Variable      Max Bitrate: 2048 Kbps

Video Quality: Medium      Resolution: HD720P(1280\*720)

Frame Type: P      Frame Rate: 25fps

I Frame Interval: 50      Audio Encoding Type: G711\_U

Video Encoding Type: STD\_H264      Video Encoding Co...: Lowest

File Size Per Day: 21.0G

Copy to...      Save

**Figure 1-39 Video & Audio**

2. Set the parameters.
3. Click **Save**.

---

### **Note**

It's suggested to keep the default settings to ensure the video/image quality.

---

## 1.10 BLC Mode

### Steps

1. Click **Back Light Compensation** to enter the settings page.

Back Light Compensation

Camera: Camera1

BLC Mode: Off

Save

**Figure 1-40 BLC Mode**

2. Set the **BLC Mode**.
3. Click **Save**.

# 2 Video Intercom Operation

## 2.1 Video Intercom Operation via Device

### 2.1.1 Call Resident

---

 **Note**

- Make sure you have configured the room No. of the device.
  - Make sure you have add contacts to the device via **iVMS-4200 Client Software**.
- 

You can call corresponding resident in three ways:

- Press the call button on the main unit or on the nametag unit.
  - Enter the Room No. on the keypad module, and press **#** to start calling.
- 

 **Note**

- You can press **\*** via keypad module to hang up.
  - You can press **Back button** via display module to hang up.
- 
- Press **^** or **v** on the display module to enter the contact list.  
Press or hold **^/v** to select a contact.  
Press **OK** and confirm to call.
- 

 **Note**

Hold **^** or **v** to scroll the page up or down faster.

---

### 2.1.2 Issue Card

#### Before You Start

Make sure you have issue the card locally or remotely. See *Person Management for issuing card via Client software* for details.

Issue Card via Main Card: You can swipe card to issue it after swiping the main card in advance.

#### Steps

1. Swipe the main card on the card reading area, and hear two beeps.
2. Swipe the unauthorized sub cards in turn after hearing a beep.

3. Swipe the main card again to end the card issuing process.

---

 **Note**

- DS-KD-M supports Mifare card, DS-KD-E supports EM card.
  - If the amount of sub cards exceeds 10000, no more sub cards can be issued.
  - Up to 5 sub cards can be issued once. The issued frequency is no more than 2000.
- 

### 2.1.3 Unlock Door

#### Unlock Door by Password

You can unlock the door by inputting the password via the keypad module.

Three formats of password are supported. They are:

- **【#】 + Public Password + 【#】**
- **【#】 + Password + 【#】**
- **【#】 + Duress Password + 【#】**

---

 **Note**

- Password contains 6 digits.
  - You're allowed to set 3 public passwords via iVMS-4200 client software.
  - The password varies according to different rooms.
- 

#### Unlock Door by Card

---

 **Note**

Make sure the card has been issued. You can issue the card via the door station, or via **iVMS-4200** client software.

---

Swipe the card on the card induction area to unlock the door.

---

 **Note**

The main card does not support unlocking the door.

---



## 2.2 Video Intercom Operation via Client Software

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

### Note

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

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

Click  →  on the left icon bar to enter the Video Intercom page.

### 2.2.1 Receive Call from Door Station

#### Steps


1. Select the client software in door station page to start calling the client and an incoming call dialog will pop up in the client software.




Figure 2-1 Device Call

2. Click **Answer** to answer the call. Or click **Hang Up** to decline the call.
3. After you answer the call, you will enter the In Call page.


**Adjust the Volume of Loudspeaker**

Click  to adjust the volume of loudspeaker.


### Hang Up

Click  to hang up.

### Adjust the Volume of Microphone

Click  to adjust the volume of the microphone.

### Unlock Remotely

For door station, you can click  to open the door remotely.

---

### Note

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

## 2.2.2 Live View via Door Station

You can get the live view of the main unit in the Main View module and control the door station remotely.

In the Main View module, double-click a door station or drag the device to a display window to start the live view.

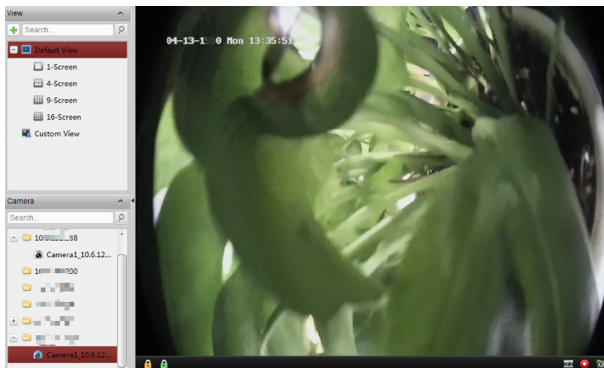


Figure 2-2 Live View

Right click on the live view page, click the unlock icon to remotely unlock the door.

## 2.2.3 View Call Logs

### Before You Start

You can check all the call logs, including dialed call logs, received call logs and missed call logs. You can also directly dial via the log list and clear the logs.

### Steps

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

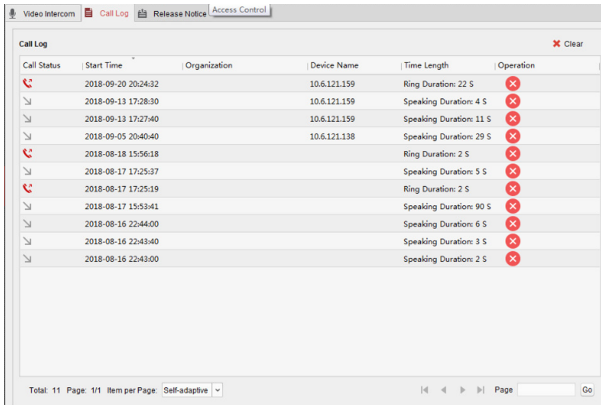



Figure 2-3 View Call Logs

All the call logs will display on this page and you can check the log information, e.g., call status, start time, resident's organization and name, device name and ring or speaking duration.

2. **Optional:** Click the call button to re-dial the resident.
3. **Optional:** Click the cancel button to delete the call log. Or you can click **Clear** to delete all logs.

## 2.2.4 Search Video Intercom Information

You can search the call logs between the iVMS-4200 client software and video intercom devices, device unlocking logs and the sent notice information.

In the Access Control module, click  to open the Search page

### Search Call Logs



### Steps

1. In the Information Search page, click **Call Log** to enter the Call Log page.

The screenshot shows the 'Call Log' page with the following search filters:

- Call Status: All
- Device Type: All Devices
- Start Time: 2017-01-18 00:00:00
- End Time: 2017-01-18 23:59:59

Below the filters is a table with the following data:

Call Status	Start Time	Time Length	Device Type	Device Name	Organization
Received	2017-01-18 20:13:32	Speaking Durati...	Door Station	10.16.6.85	

At the bottom of the page, there is a pagination bar showing 'Total: 1 Page: 1/1 Item per Page: Self-adaptive' and a 'Go' button.

**Figure 2-4 Call Logs**

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

#### Call Status

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

#### Device Type

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

#### Start Time/End Time

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

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

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

## Search Unlocking Logs

### Steps

1. In the Information Search page, click **Unlocking Log** to enter the Unlocking Log page.

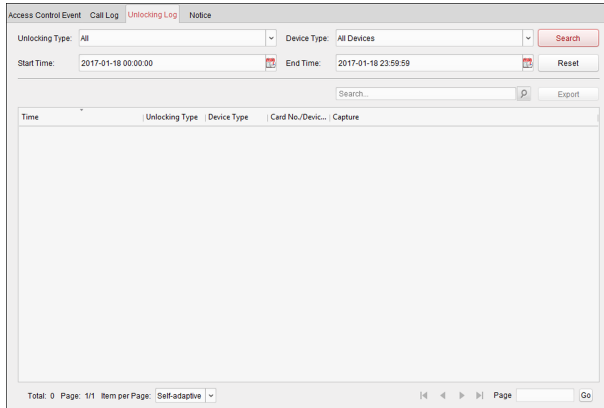


Figure 2-5 Unlocking Logs

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


#### Unlocking Type

Click **∨** to unfold the drop-down list and select the unlocking type as **Unlock by Password**, **Unlock by Duress**, **Unlock by Card**, **Unlock by Resident** or **Unlock by Center**. Or select **All** to search logs with all unlocking types.

#### Device Type


Click **∨** to unfold the drop-down list and select the device type as **Door Station** or **Door Station (V Series)**. Or select **All Devices** to search logs with all device types.

#### Start Time/End Time

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

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

3. Click **Search** and all the matched unlocking logs will display on the page.

- 4. Optional:** Check the detailed information of searched unlocking logs, such as unlocked time, card No., device No., etc.
- 5. Optional:** Input keywords in the Search field to filter the searching result.
- 6. Optional:** Click  on the Capture column to view the captured pictures.

---

 **Note**

Viewing captured picture should be supported by device.

---

- 7. Optional:** Click **Export** to export the unlocking logs to your PC.

