



DS-KD9203 Series Video Intercom Face Recognition Door Station

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **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.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

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.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.
- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.

- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- **CAUTION:** Risk of explosion if the battery is replaced by an incorrect type. If a power adapter is provided in the device package, use the provided adapter only.
- If no power adapter is provided, ensure the power adapter or other power supply complies with Limited Power Source. Refer to the product label for the power supply output parameters.

Regulatory Information

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



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

Chapter 1 About this Manual	1
Chapter 2 Appearance	2
Chapter 3 Terminal and Wiring Description	6
3.1 Terminal Description	6
3.2 Wiring Description	7
3.2.1 Door Lock Wiring	7
3.2.2 Exit Button Wiring	8
3.2.3 Door Contact Wiring	8
Chapter 4 Installation	10
4.1 Gang Box	11
4.2 Flush Mounting with Gang Box	12
Chapter 5 Activation	14
5.1 Activate Device Locally	14
5.2 Activate Device via Client Software	15
5.3 Activate via Web Browser	16
Chapter 6 Local Operation	17
6.1 Local Configuration	17
6.1.1 Edit Network Parameters	17
6.1.2 Local Settings	17
6.1.3 Add Residents	18
6.1.4 About	19
6.2 Video Intercom Operation	19
6.2.1 Call Resident	19
6.2.2 Call Center	20
6.3 Unlock Door	20
6.3.1 Unlock by Password	20

6.3.2 Unlock by Presenting Card	20
6.3.3 Unlock by Fingerprint	21
6.3.4 Unlock by Face	21
Chapter 7 Quick Operation via Web Browser	22
7.1 Select Language	22
7.2 Time Settings	22
7.3 Privacy Settings	22
7.4 Administrator Settings	23
7.5 No. and System Network	23
Chapter 8 Operation via Web Browser	26
8.1 Login	26
8.2 Forget Password	26
8.3 Overview	27
8.4 Person Management	28
8.5 Search Event	29
8.6 Device Management	29
8.7 Configuration	31
8.7.1 View Device Information	31
8.7.2 Set Time	31
8.7.3 Set DST	32
8.7.4 Change Administrator's Password	32
8.7.5 Online Users	33
8.7.6 View Device Arming/Disarming Information	33
8.7.7 Network Settings	33
8.7.8 Set Video and Audio Parameters	37
8.7.9 Set Image Parameters	39
8.7.10 Event Settings	39
8.7.11 Access Control Settings	41

8.7.12 Video Intercom Settings	46
8.7.13 Set Card Security	48
8.7.14 Set Privacy Parameters	49
8.7.15 Set Biometric Parameters	50
8.7.16 Customize Audio Content	52
8.8 Maintenance and Security	53
8.8.1 Upgrade and Maintenance	53
8.8.2 Device Debugging	54
8.8.3 Log Query	55
8.8.4 Set Protocol Testing	55
8.8.5 Set Network Diagnosis	55
8.8.6 Security Audit Log	55
8.8.7 Certificate Management	55
Chapter 9 Other Platforms to Configure	58
Appendix A. Appendix	59

Chapter 1 About this Manual

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

Product	Model
Door Station	DS-KD9203 Series

Scan the QR code to get the User Manual for detailed information.



Chapter 2 Appearance

Door Station without Fingerprint Module

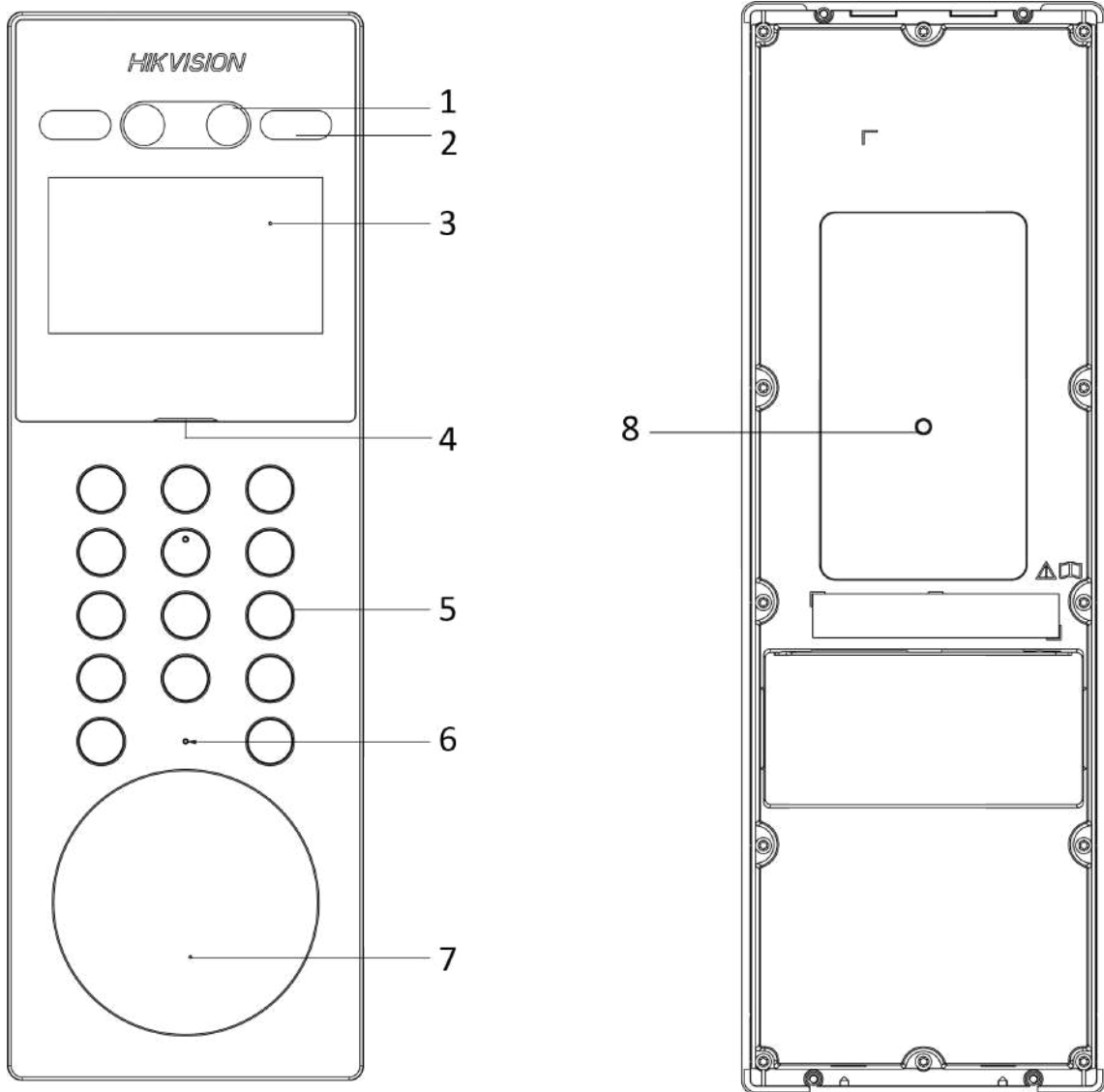


Figure 2-1 Appearance of Door Station without Fingerprint Module

Table 2-1 Description

No.	Description
1	Camera
2	IR Supplement Light
3	Screen
4	Loudspeaker
5	Buttons
6	Microphone
7	Card Reading Area
8	TAMPER

Door Station with Fingerprint Module

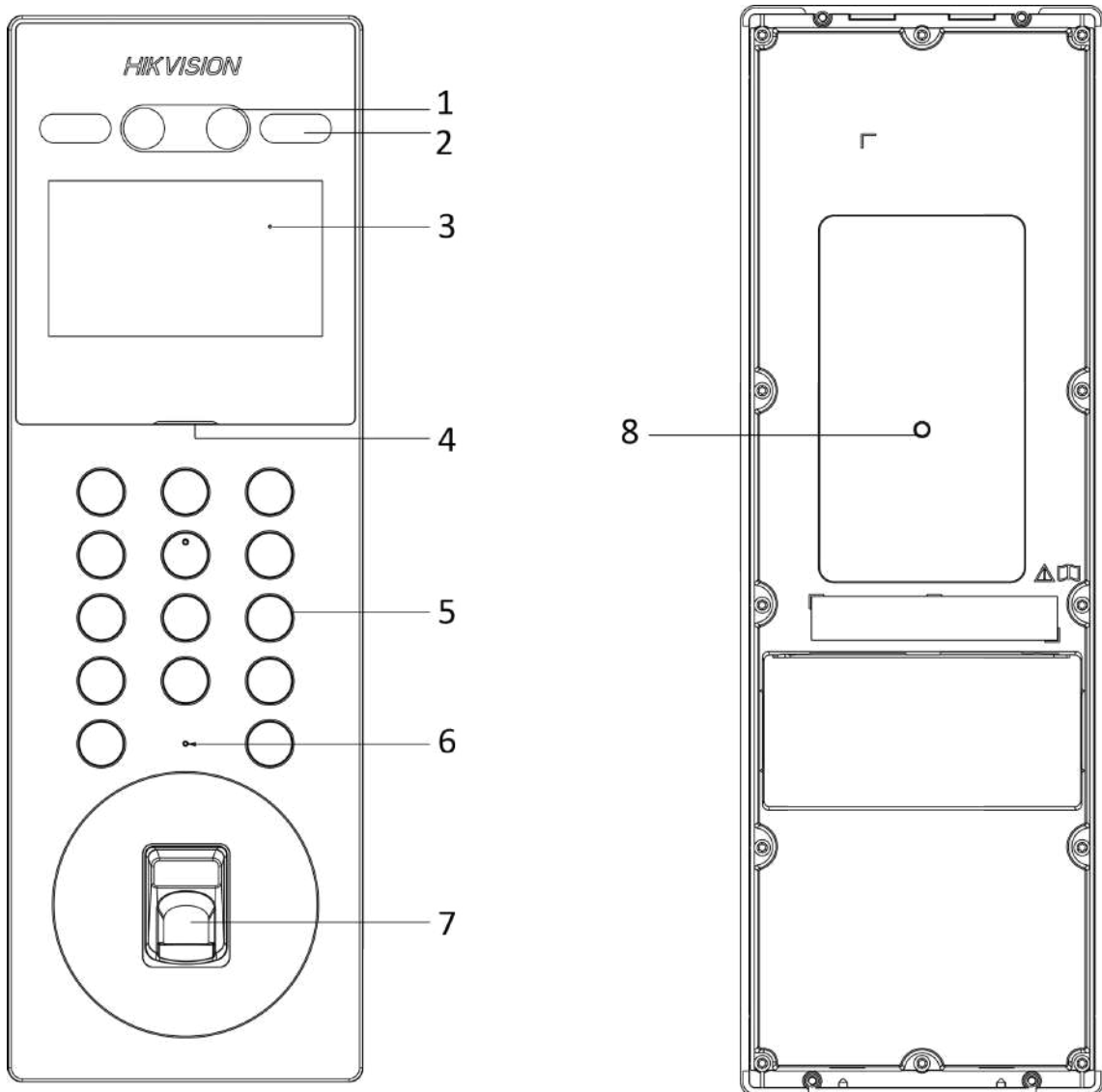


Figure 2-2 Appearance of Door Station with Fingerprint Module

Table 2-2 Description

No.	Description
1	Camera
2	IR Supplement Light
3	Screen
4	Loudspeaker

No.	Description
5	Buttons
6	Microphone
7	Card Reading Area/ Fingerprint Recognition Module
8	TAMPER

Chapter 3 Terminal and Wiring Description

3.1 Terminal Description

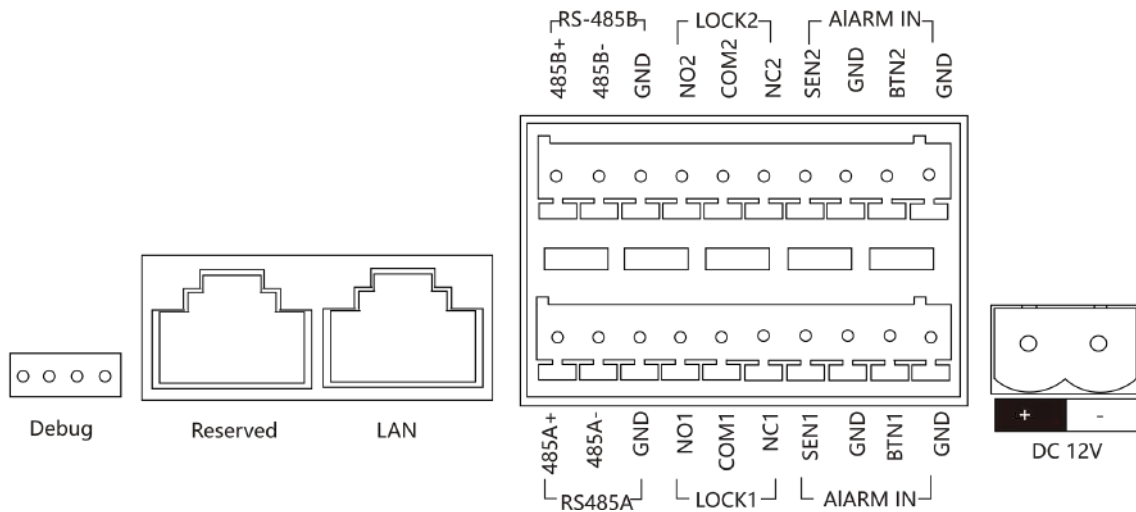


Figure 3-1 Terminal Description

Table 3-1 Description

Name	Terminal	Description
Network Interface	LAN	Network Signal Input
ALARM IN	SEN1	Door Contact Input 1
	SEN2	Door Contact Input 2
	BTN1	Exit Button Input 1
	BTN2	Exit Button Input 2
	GND	Grounding
RS-485	485A+	External RS-485 Card Reader
	485A-	
	485B+	External Elevator Controller
	485B-	
DOOR	NC1	Door Lock Relay Output 1(Normally Close)
	COM1	Common Interface 1

Name	Terminal	Description
	NO1	Door Lock Relay Output 1(Normally Open)
	GND	Grounding
	NC2	Door Lock Relay Output 2(Normally Close)
	COM2	Common Interface 2
	NO2	Door Lock Relay Output 2(Normally Open)
	GND	Grounding
Power Supply	DC 12 V	12 VDC Power Input

Note

- Alarm input interface cannot be edited. Refers to the actual model.
- You can only wire the SEN1/SEN2 terminal with the door contact. And wire the BTN1/BTN2 terminal with the exit button.

3.2 Wiring Description

3.2.1 Door Lock Wiring

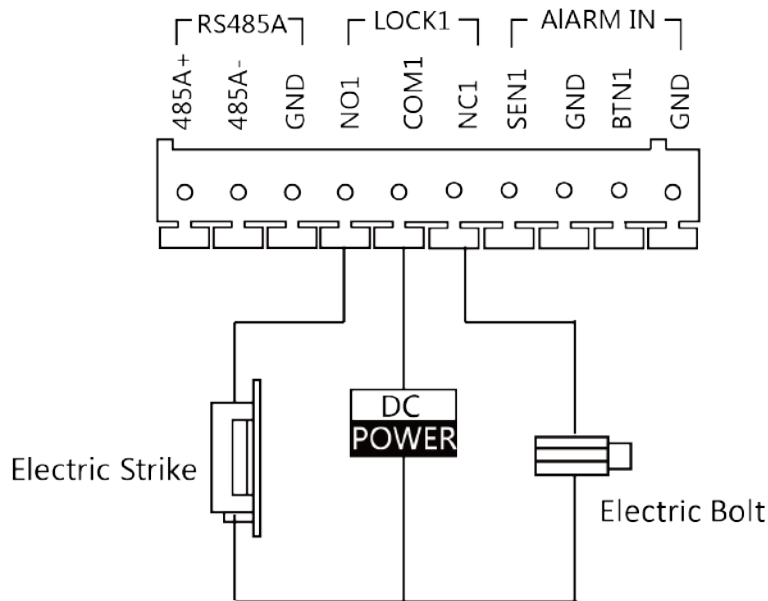


Figure 3-2 Door Lock Wiring

 **Note**

- Terminal NC1/COM1 is set as default for accessing electric bolt. Terminal NO1/COM1 is set as default for accessing electric strike.
 - To connect electric lock in terminal NO2/COM2/NC2, it is required to set the output of terminal NO2/COM2/NC2 to be electric lock with **iVMS-4200** Client Software.
-

3.2.2 Exit Button Wiring

Wire the BTN1/BTN2 terminal with the door contact.

Here takes BTN1 for example.

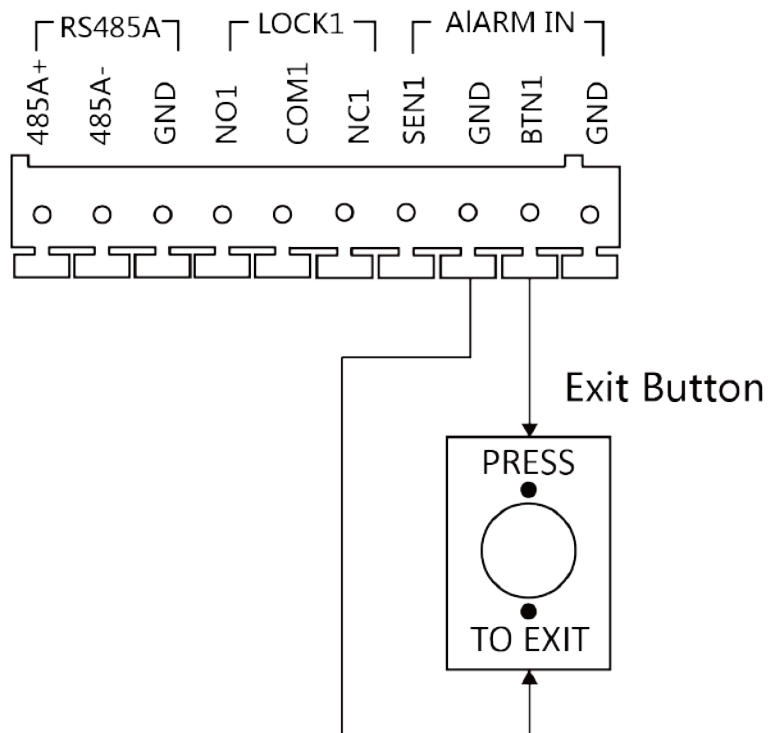


Figure 3-3 Exit Button Wiring

3.2.3 Door Contact Wiring

Wire the SEN1/SEN2 terminal with door contact.

Here takes SEN1 for example.

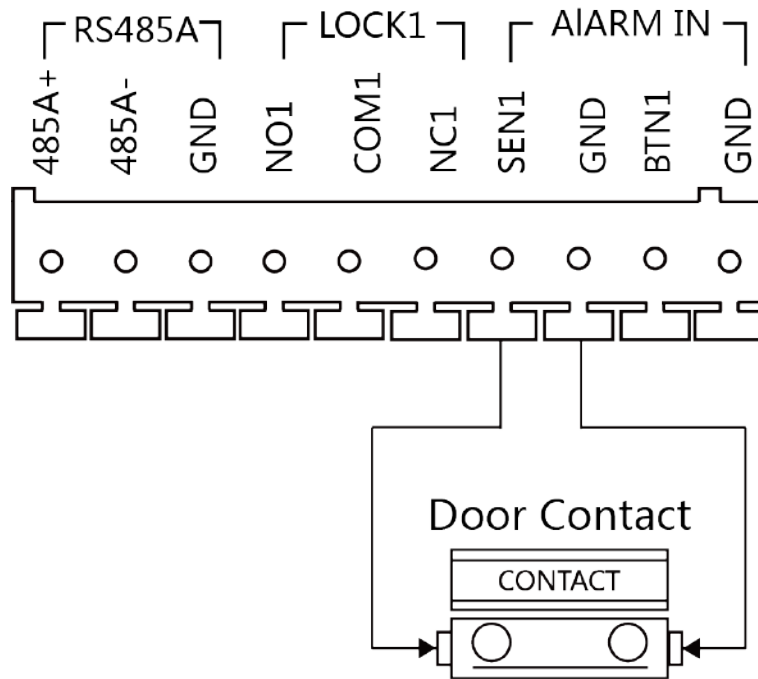


Figure 3-4 Door Contact Wiring

Chapter 4 Installation

 **Note**

- Make sure the device in the package is in good condition and all the assembly parts are included.
 - The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
 - Make sure all the related equipment is power-off during the installation.
 - Check the product specification for the installation environment.
-

4.1 Gang Box

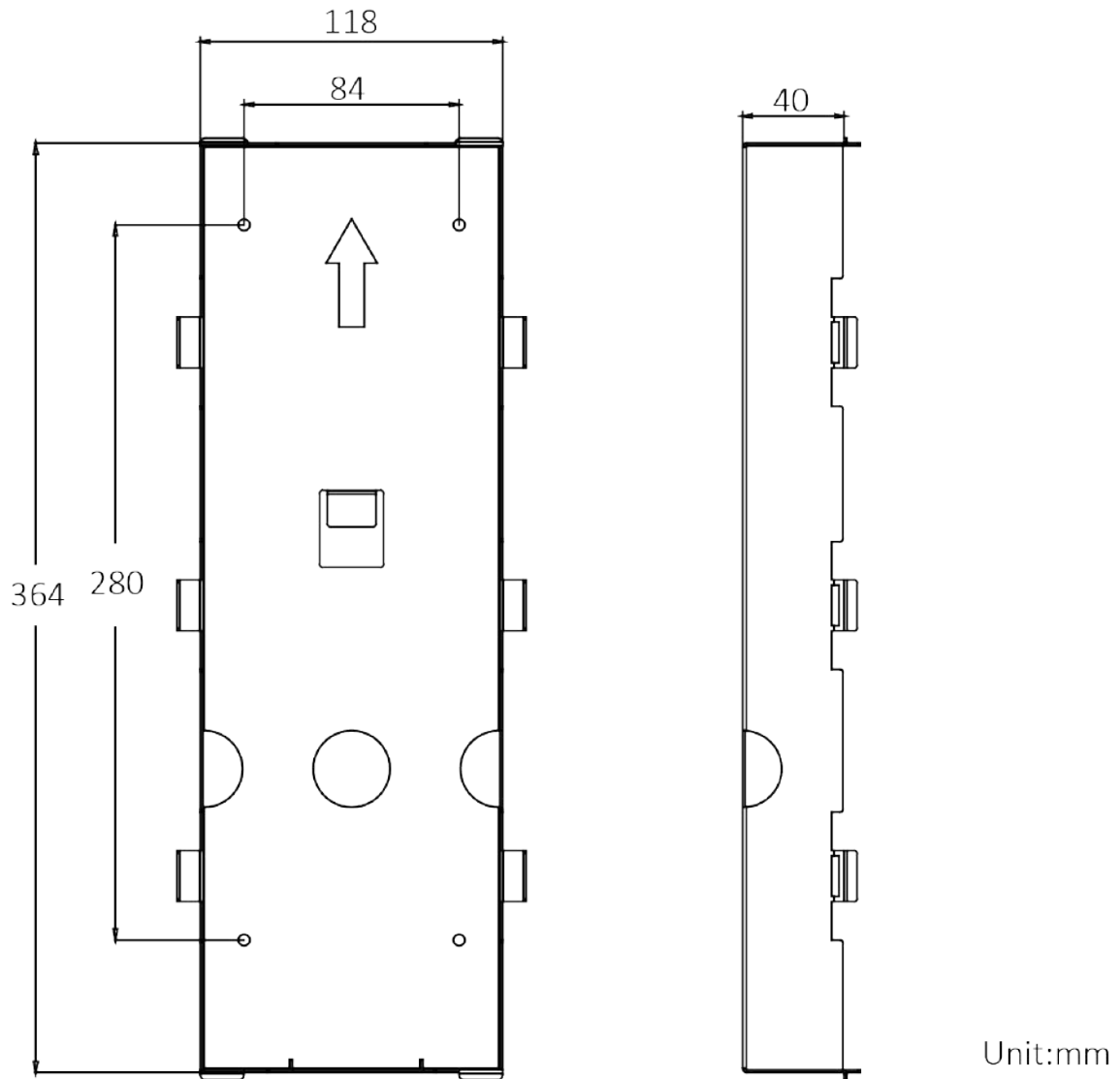


Figure 4-1 Dimension of the Gang Box

 **Note**

- The dimension of the gang box is 364 mm (W) × 118 mm (H) × 40 mm (D).
 - The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).
-

4.2 Flush Mounting with Gang Box

Steps

1. Cave an installation hole in the wall. Pull the cable out from the wall.
-



Note

- The suggested dimension of the installation hole is 364.3 mm (W) × 118.6 mm (H) × 40.2 mm (D).
 - The suggested length of the cables left outside is 250 mm.
-
2. Install the gang box into the wall.
 - 1) Remove the plastic sheet of the gang box with the tool.
 - 2) Insert the gang box into the installation hole. Mark the gang box screw holes' position with a marker, and take out the gang box.
 - 3) Drill 4 holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
 - 4) Fix the gang box with 4 expansion bolts.
 3. Fix the gap between the gang box and wall with concrete. Remove the mounting ears with tool after concrete is dry. Connect the cables according to the *Wiring Description*.
 4. Insert the door station into the gang box. Slide the door station down and fix it with 2 set screws. Apply Silicone sealant among the joints between the device and the wall (except the lower side) to keep the raindrop from entering.

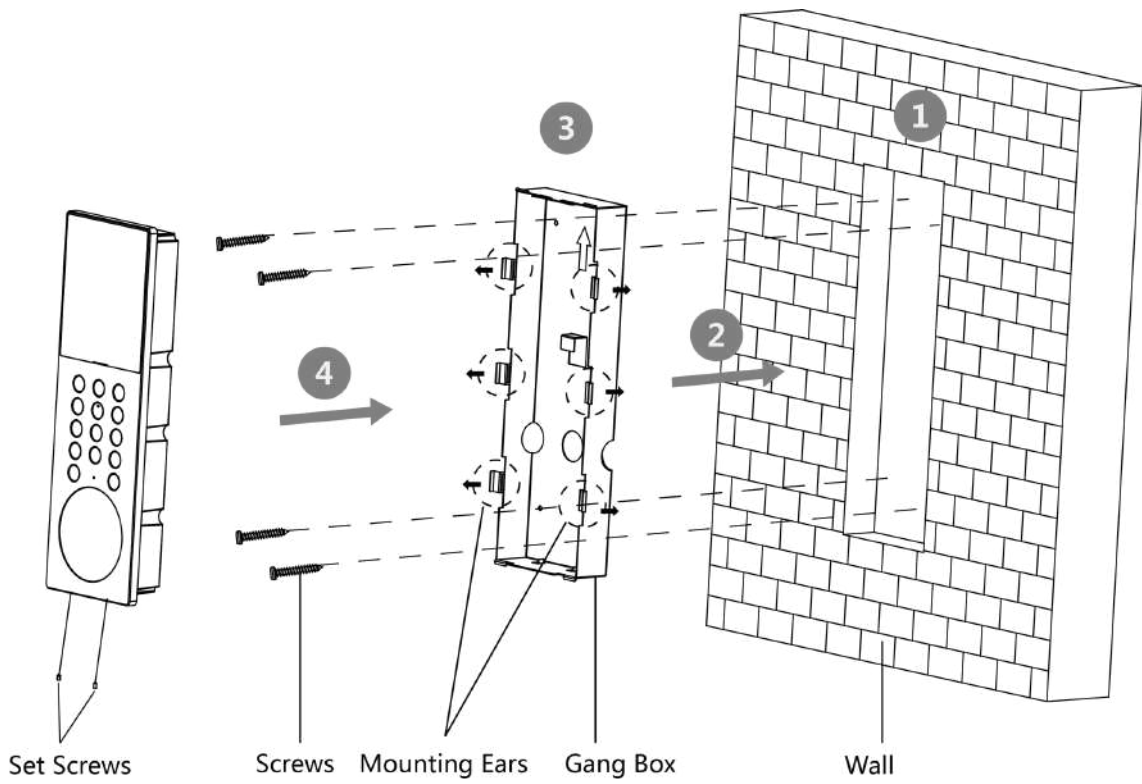


Figure 4-2 Flush Mounting with Gang Box

Chapter 5 Activation

5.1 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.

Table 5-1 Number Button Description

No.	Description	No.	Description
1	1	6	6mnoMNO
2	2abcABC	7	7pqrsPQRS
3	3defDEF	8	8tuvTUV
4	4ghiGHI	9	9wxyzWXYZ
5	5jkIJKL	0	0

Hold 0 to enter special characters.

Table 5-2 Number Button Description

No.	Description	No.	Description
1	1,.#?	6	6_ =+
2	2!@%	7	7[] ; :
3	3^\$*	8	8" <
4	4() \	9	9 > { }
5	5& / -		

Note

- The password required 8 to 16 characters.
- The way to enter the password, take button 2 as an example: Press 2 to enter the number '2' or hold 2 for 1.5 s and press 2 again to enter the character 'a'.
- When you have entered the password, press # to switch to confirm the password.
- Press * to delete the wrong charater.

3. Press # to select language.

4. After selection, press # to finish activation.

5.2 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.



Caution

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. 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. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

-
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.
-

5.3 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.65) in the address bar of the web browser, and press **Enter**.



Note

Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.



Caution

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. 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. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
- (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)

-
3. Click **Activate**.

4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

Chapter 6 Local Operation

6.1 Local Configuration

When entering configuration page, the button is used as follows.

Table 6-1 Button Description

Button	Description	Button	Description
2	Previous	8	Next
*	Exit/Back	#	OK

6.1.1 Edit Network Parameters

After activating, you should edit the network parameters.

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to Network settings according to the tips on the page. Press # to enter the settings page.
4. Edit the parameters according to your needs.
5. Press * to save and exit.

6.1.2 Local Settings

Configure the local parameters (including but not limited to, edit numbers and edit recognition parameters).

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to Local Settings according to the tips on the page.
4. Press # to enter the settings page.

Door Station Settings

Edit the parameters of the door station (including but not limited to, community No., building No., floor No., room No. and device mode).

Steps

1. Configure the parameters according to the actual needs.
-



Note

- Outer door station can only edit the Community No., Project No. and No.
 - The No. of the main door station is 0.
 - The No. of sub door stations should be larger than 0 and ranges from 1 to 8.
 - Each unit should add 1 main door station. Up to 8 sub door stations can be added to the main door station.
-

2. **Optional:** Enable the **Normally Open Mode** according to your needs.

The door remains open.

3. **Optional:** Select the language.
4. After configuration, press * to save and exit.

Recognition with Mask

Steps

1. Enable **Face with Mask Detection**.
2. Select the **Passing Level of Face Mask Recognition**.
3. Edit the **Fce with Mask & Face 1:N Matching Threshold** and **Fce with Mask & Face 1:N Matching Threshold (ECO Mode)**.

6.1.3 Add Residents

User Management

You can add, edit and delete the informations of the users.

Steps

1. Hold * and # at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press # to enter the password to login.
3. Switch to User Management according to the tips on the page.
4. Press # to enter the settings page.

Add Users

You can add cards, permissions and room No. for the users.

Steps

1. Select **+Add**, and press **#** to enter the adding page.
2. Edit the room No.
3. Add cards.
 - 1) Switch to the card and press **#** or present cards on the card reading area to add.
 - 2) Enter the card No. manually or present the card on the card reading area to get the card No. automatically.
 - 3) Press **#** to add.
4. Switch to the permission and press **#** to set.
5. Press ***** to save and exit.

6.1.4 About

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

Steps

1. Hold ***** and **#** at the same time to enter the authentication page.
2. Authenticate via administrator.
 - Authenticate face/card/fingerprint to login.
 - Press **#** to enter the password to login.
3. Switch to About according to the tips on the page.
4. Press **#** to enter the page.

6.2 Video Intercom Operation

6.2.1 Call Resident

The door station can work as main/sub door station, and outer door station, which correspond to different calling resident modes respectively.

Call Resident from Main/Sub Door Station

Press any digit button on the main/sub door station page to enter the calling page.
Enter the room No. and press call button.

Call Resident from Outer Door Station

Press call button on the outer door station page to enter the calling page .

Enter 【Community No. + Building No. + # + Unit No. + # + Room No.】 and press call button to call resident.

Note

When Unit No. is one, it can be omitted. When Unit No. is omitted, Community No. must be omitted at the same time.

6.2.2 Call Center

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

Press center button to call., and press * to cancel during calling management center.

6.3 Unlock Door

6.3.1 Unlock by Password

Unlock by Password

Tap **Call/Open** to enter the calling page.

Enter 【# + Room No. + Password + #】 , and tap unlock button.

Unlock by Public Password

Note

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

Tap **Call/Open** to enter the calling page.

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

6.3.2 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.

6.3.3 Unlock by Fingerprint

 **Note**

- Make sure you have added the fingerprint to the device.
 - Fingerprint function may vary with different modules. Please refer to the actual devices.
-

Put your finger on the finger recognition module to unlock.

6.3.4 Unlock by Face

 **Note**


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

Face forward at the camera to unlock.

Chapter 7 Quick Operation via Web Browser

7.1 Select Language

You can select a language for the device system.

Click  in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.



Note

After you change the system language, the device will reboot automatically.

7.2 Time Settings

Click  in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval


You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

7.3 Privacy Settings

Set the picture uploading and storage parameters.

Click  on the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **Privacy Settings** page.

Picture Uploading and Storage

Save Picture When Auth.

Save picture when authenticating automatically.

Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.


Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Click **Next** to save the settings and go to the next parameters. Or click **Skip** to skip privacy settings.

7.4 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **Administrator Settings** page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.
 - 1) Click **Add Face** to upload a face picture from local storage.

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

- 2) Click **Add Card** to enter the Card No. and select the property of the card.

Note

Up to 5 cards can be supported.

- 3) Click **Add Fingerprint** to add fingerprints.


Note

Up to 10 fingerprints are allowed.

Click **Complete** to complete the settings.

7.5 No. and System Network

Steps

1. Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

- If set the device type as **Door Station**, you can set the **Community No.**, **Building No.**, **Unit No.**, **Floor No.** and **Door Station No.**
 - If set the device type as **Outer Door Station**, you can set **Outer Door Station No.** and **Community No.**
-

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 99.

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Note

The device type is selected as **Door Station** by default. If you select another type, you can reboot device and go to **Configuration → Intercom** for intercom settings.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

Chapter 8 Operation via Web Browser

8.1 Login

You can login via the web browser or the remote configuration of the client software.




Make sure the device is activated.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.

Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click  to enter the Configuration page.

8.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.



The function is supported when the PC/mobile phone is in the same network segment with the device.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

8.3 Overview

You can view the live video of the device, real-time event, linked devices, person information, network status, basic information, and device capacity.

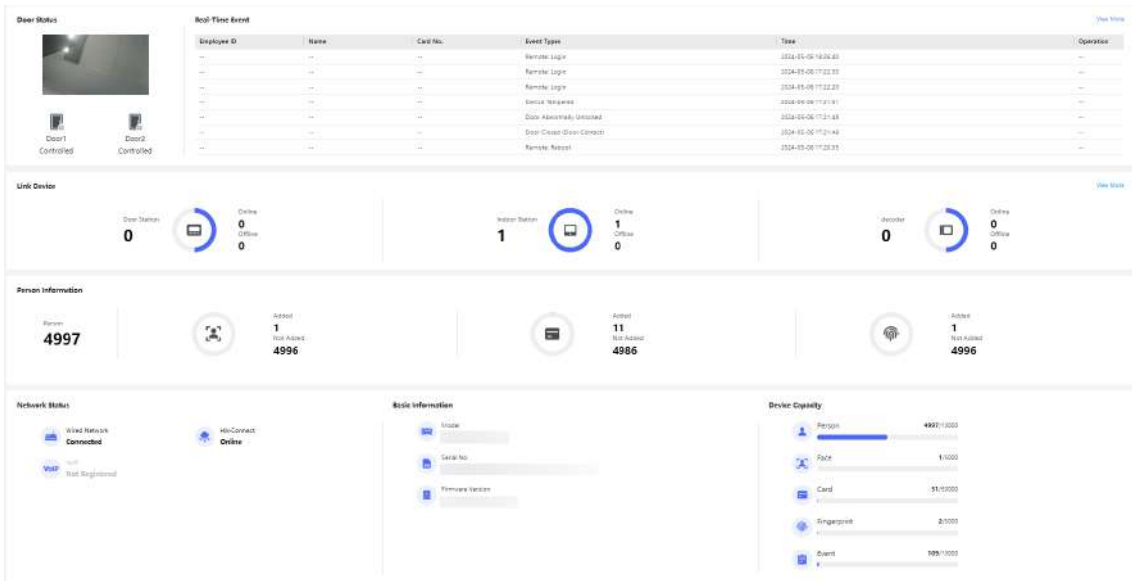


Figure 8-1 Overview Page

Function Descriptions:

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.



You can capture image when starting live view.



Select the streaming type when starting live view. You can select from the main stream and the sub stream.



Full screen view.



The door status is open/closed/remaining open/remaining closed.

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the time, the unit. Click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person face, fingerprint and card.

Network Status

You can view the connected and registered status of wired network, VoIP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the Person, Face, Card, Fingerprint and Event capacity.

8.4 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.

Add Basic Information

Click **Person Management** → **Add** to enter the Add Person page.

Add the person's basic information, including the employee ID, the person's name, floor No., room No., etc.

Click **Save** to save the settings.

Set Permission Time

Click **Person Management** → **Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management** → **Add** to enter the Add Person page.

Set the authentication type.

Click **Save** to save the settings.

Add Face Picture

Click **Person Management** → **Add** to enter the Add Person page.
Click **+** on the right to upload a face picture from the local PC.



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

Click **Save** to save the settings.

Add Card

Click **Person Management** → **Add** to enter the Add Person page.
Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.



Up to 5 cards can be added.

Click **Save** to save the settings.

Add Fingerprint

Click **Person Management** → **Add** to enter the Add Person page.
Click **Add Fingerprint**, and press your finger on the fingerprint module of the device to add your fingerprint.
Click **Save** to save the settings.

8.5 Search Event

Click **Event Search** to enter the Search page.

Select event types, major type and sub type. Enter the search conditions, including the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

8.6 Device Management

You can manage the linked device on the page.

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



Figure 8-2 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.

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.

Synchronization Settings

Click **Synchronization Settings** and enable **Synchronize**. If enabled, the current device's settings will be synchronized to other devices.

Upgrade

Timing Upgrade

You can choose to **Enable Upgrading Device Automatically** or set upgrade time so that the device will upgrade within the time. Click **Save**.

Upload Upgrade Package

You can import upgrading package from local and select device type. Click **OK** to upgrade.

Upgrade Now

Check the device you would like to upgrade and click **OK** to upgrade.



Upgrade Status

You can view the upgrade status of linked devices.

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.

8.7 Configuration

8.7.1 View Device Information

View the device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485, alarm input, alarm output, and device capacity, etc.

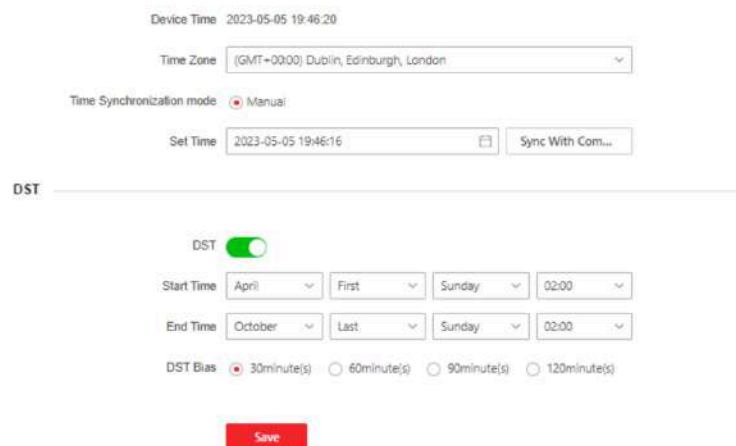
Click **Configuration** → **System** → **System Settings** → **Basic Information** to enter the configuration page.

You can view device name, language, model, serial No., version, available cameras, IO input, IO output, Lock, Local RS-485, alarm input, alarm output, and device capacity, etc.

8.7.2 Set Time

Set the device's time, time zone, synchronization mode, server address, NTP port, and interval.

Click **Configuration** → **System** → **System Settings** → **Time Settings** .



Device Time 2023-05-05 19:46:20

Time Zone (GMT+00:00) Dublin, Edinburgh, London

Time Synchronization mode Manual

Set Time 2023-05-05 19:46:16 Sync With Com...

DST

DST

Start Time April First Sunday 02:00

End Time October Last Sunday 02:00

DST Bias 30minute(s) 60minute(s) 90minute(s) 120minute(s)

Save

Figure 8-3 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.


8.7.3 Set DST

Steps

1. Click **Configuration** → **System** → **System Settings** → **Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

8.7.4 Change Administrator's Password

Steps

1. Click **Configuration** → **System** → **User Management** .
2. Click  .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Caution

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- Do not contain following characters in the password: the user name, 123, admin (case-insensitive), 4 or more continuously increasing or decreasing digits, or 4 or more consecutively repeated characters.

- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. 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. Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
 - (If the device supports AP mode, after the admin password is changed, the password of AP hotspot will be changed simultaneously.)
-

8.7.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration** → **System** → **User Management** → **Online Users** to view the list of online users.

8.7.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

Click **Configuration** → **System** → **User Management** → **Arming/Disarming Information** .

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

8.7.7 Network Settings

Set Basic Network Parameters

Click **Configuration** → **Network** → **Network Settings** → **TCP/IP** .

The screenshot shows a configuration interface for TCP/IP settings. At the top, there is a 'DHCP' toggle switch which is turned on (green). Below it are several input fields: 'IPv4 Address', 'IPv4 Subnet Mask', 'IPv4 Default Gateway', 'Mac Address', and 'MTU'. Further down, there are two fields for alarm-related settings: '*Alarm Center IP' and '*Alarm Host Port'. Below these are three fields for 'DNS Server': 'Preferred DNS Server' and 'Alternate DNS Server'. At the bottom of the form is a red 'Save' button.

Figure 8-4 TCP/IP Settings

Set the parameters and click **Save** to save the settings.

DHCP

If disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server and the Alternate DNS server.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, preferred DNS server and the Alternate DNS server automatically.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Port Parameters

Set the HTTP, HTTPS, RTSP and Server port parameters.

Click **Configuration** → **Network** → **Network Service** → **HTTP(S)** .

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter **http://192.0.0.65:81** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Click **Configuration** → **Network** → **Network Service** → **RTSP** .

RTSP

It refers to the port of real-time streaming protocol.

Click **Configuration** → **Network** → **Device Access** → **SDK Server** .

SDK Server

It refers to the port through which the client adds the device.

Platform Access

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

Steps

1. Click **Configuration** → **Network** → **Device Access** → **Hik-Connect** to enter the settings page.



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

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and verification code.



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

5. Enable **Video Encryption**, and create the password and confirm it.



After adding the device to APP, you need to enter the video encryption password to live view the device.

6. **Optional:** Click **View** to view the device QR code. Scan the QR code to account.



Scan the QR code before it loses efficacy.

7. **Optional:** Click **More** to set the network connection priority.
 - 1) Enable **WLAN** or **Wired Network** according to your actual needs.
 - 1) Hold and drag ☰ to adjust the access priority.
8. Click **Save** to enable the settings.

FTP Settings

You can configure FTP (File Transfer Protocol) parameters.

Steps

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

Enable FTP

Server Type

* Server IP Address

* Port

Anonymous

* User Name

* Password

* Password Confirm

Directory Structure

Parent Directory

Child Directory

* Delimiter

Named Item

Named Element

Figure 8-5 FTP Settings

2. Enable FTP.
3. Select **Server Type**.
4. Enter **Server IP Address** and **Port**.
5. Configure the FTP Settings, and the user name and password are required for the server login.

 **Note**

If you enable **Anonymous**, you will not need to set user name and password.

-
6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
 7. Set naming rules.
 8. Click **Save** to enable the settings.

Set Network Penetration Service

When the device is deployed on the LAN, penetration service can be enabled to achieve remote device management.

Steps

1. Click **Configuration** → **Network** → **Network Service** → **Network Penetration Service** .
2. Click to **Enable Penetration Service**.
3. Enter **Server IP Address** and **Server Port**.
4. Enter login **User Name** and **Password**.
5. Set **Heartbeat Timeout**. The range is 1 to 6000.
6. Click **Save**.
7. You can view **Online Status**. Click **Refresh** to view the latest status.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)** .

View WebSocket and WebSockets port.

8.7.8 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **Configuration** → **Video/Audio** → **Video** .

Stream Type Main Stream Sub-stream

Video Type Video Stream Video&Audio

Resolution 1280*720

Bit Rate Type Variable Constant

Video Quality Medium

Frame Rate 25 fps

* Max. Bitrate 2048 Kbps

Video Encoding H.264

* I Frame Interval 50

Figure 8-6 Video Settings Page

Set the stream type, the video type, the resolution, the Bit Rate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

Click **Save** to save the settings.

 **Note**

The functions vary according to different models. Refers to the actual device for details.

Set Audio Parameters

Click **Configuration** → **Video/Audio** → **Audio** .

Stream Type Main Stream Sub-stream

Audio Encoding G.711u|law

Input Volume 7

Output Volume 7

Audio Sampling Rate 8 KHz

Figure 8-7 Audio Settings Page

Set the stream type, audio encoding, input volume, output volume, speak volume and audio sampling rate.

Click **Save** to save the settings.

8.7.9 Set Image Parameters

You can adjust the image parameters, video parameters, supplement parameters, backlight, beauty, image fusion and capture interval.

Steps

1. Click **Configuration** → **Image** .
2. Configure the parameters to adjust the image.

Video Adjustment (Video Standard)

Set the video frame rate when performing live view remotely. After changing the standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Backlight

Enable or disable the WDR function.

When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

3. Click **Restore Default Settings** to restore the parameters to the default settings.

8.7.10 Event Settings

Set Motion Detection

After enable the function of motion detection, people or stuff enter the configured area will trigger alarm.

Steps

1. Click **Configuration** → **Event** → **Event Detection** → **Motion** .

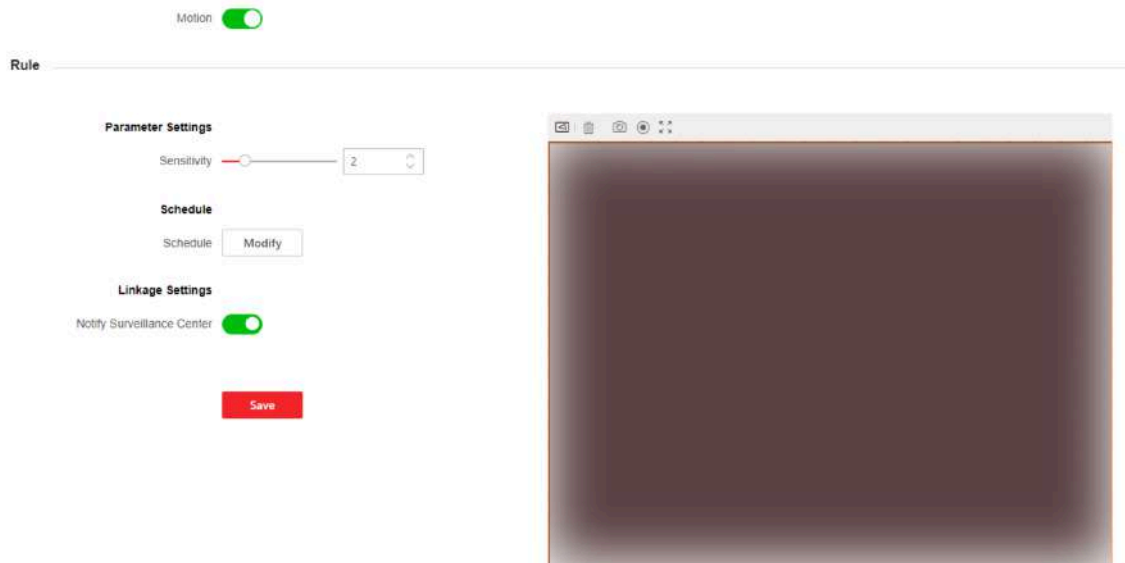


Figure 8-8 Motion Detection

2. Enable **Motion**.
3. Drag the process bar to adjust the **Sensitivity** parameter.
4. Enable **Notify Surveillance Center** according to your actual needs. After enabled, the alarm information is uploaded to the surveillance center when an alarm event is detected.
5. Click **Save**.

 **Note**

The arming schedule is defaulted as all-day.

Linkage Settings

Steps

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



Figure 8-9 Linkage Settings

2. Select event.
 - **Device Event**
 - Tampering Alarm
 - **Door Event**
 - Door Open Timed Out (Door Contact)
3. Enable **Notify Surveillance Center** according to your actual needs. After enabled, the alarm information is uploaded to the surveillance center when an alarm event is detected.
4. Click **Save** to enable the settings.

8.7.11 Access Control Settings

Set Authentication Parameters

Click **Configuration** → **Access Control** → **Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication. In the configured interval, Person A can only recognized once. If another person (Person B) has recognized during the interval, Person A can recognized again.

Set Door Parameters

Click **Configuration** → **Access Control** → **Door Parameters** .

Door No. 1 2

*Door Name

Open Duration s

Relay Reverse Open Disable

Figure 8-10 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Relay Reverse

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Elevator Control

Steps

1. Click **Configuration** → **Access Control** → **Elevator Control Parameters** .

Elevator No.

Elevator Control

Main Elevator Controller Model

Interface Type RS-485 Network Interface

Negative Floor Capacity

Figure 8-11 Elevator Control

2. Select **Elevator No.**
3. Click to enable **Elevator Control**.
4. Set the elevator parameters.

Elevator No.

Select an elevator No.

Main Elevator Controller Model

Select an elevator controller.

Interface Type

If you select **RS-485**, make sure you have connected the device to the elevator controller with RS-485 wire.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.



Note

- Up to 4 elevator controllers can be connected to 1 device.
 - Up to 10 negative floors can be added.
 - Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.
-

Set RS-485 Parameters

You can set the RS-485 parameters.

Click **Configuration** → **Access Control** → **RS-485** .

Click **Save** to save the settings after the configuration.

No.

Set the RS-485 No.

Working Mode

Select a working mode from the drop-down list according the actual situation. You can select from **Elevator Control** or **Disable**.



Note

After the working mode is changed and saved, the device will reboot automatically.

Set Public Password

Set public password.

Click **Configuration** → **Access Control** → **Password Settings** to enter the page.

Click **Add** to add public password.

The screenshot shows a configuration form for adding a public password. It includes a dropdown menu for 'Password Type' with 'Public Password1' selected. There are two password input fields labeled 'Password *' and 'Password Confirm *', both containing the text 'Enter.' and a copy icon. Below these is a 'Remarks' text area. At the bottom, there is a section for 'Enable Electric Lock *' with two radio buttons: 'Electric Lock1' (which is selected) and 'Electric Lock2'. At the very bottom are two buttons: a red 'Save' button and a white 'Cancel' button.

Figure 8-12 Add Public Password

Select password type.

Enter and confirm the password.

Enter remarks.

Select electric lock.

Click **Save** to save the settings.

Set I/O Parameters

You can set I/O Parameters.

Steps

1. Click **Configuration** → **Access Control** → **I/O Settings** .
2. Set input parameters.

Input 1

Select input 1 as **Door Status**.

Input 2

Select input 2 as **DisableorDoor Status**.

Input 3

Select input 3 as **Unlock**.

Input 4

Select input 4 as **Unlock** or **Disable**.

3. Set output parameters.

Output 1

Output 1 is **Electric Lock** by default.

Output 2

Select output 2 as **Electric Lock** or **Disable**.

8.7.12 Video Intercom Settings

Device No. Settings

Steps

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

Device Type: Door Station

Floor No.: 1

*Door Station No.: 0

More

*Community No.: 1

*Building No.: 1

*Unit No.: 1

Save

Figure 8-13 Device No. Settings

2. Select the device type from the drop-down list, and set the corresponding information including **Building No.**, **Floor No.**, **Door Station No.**, **Community No.** and **Unit No.**

Note

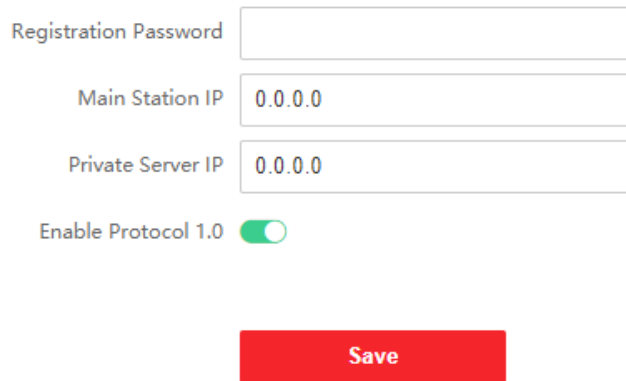
- When you select **Outer Door Station** as **Device Type**, only **Community No.** and **Outer Door No.** can be set.

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

Linked Network Settings

Steps

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



The screenshot shows a settings page with four input fields and a toggle switch. The first field is 'Registration Password' which is empty. The second is 'Main Station IP' with the value '0.0.0.0'. The third is 'Private Server IP' also with '0.0.0.0'. Below these is a toggle switch for 'Enable Protocol 1.0' which is turned on. At the bottom center is a red 'Save' button.

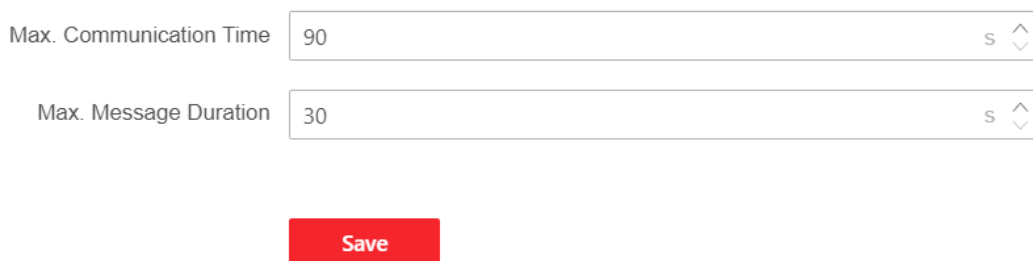
Figure 8-14 Session Settings

2. Set **Registration Password**.
3. Set **Main Station IP** and **Video Intercom Server IP**.
4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Duration Settings

Set the Max. call duration.

Go to **Configuration** → **Intercom** → **Call Settings** .



The screenshot shows two input fields for time durations. The first is 'Max. Communication Time' with a value of '90' and a unit 's' and up/down arrows. The second is 'Max. Message Duration' with a value of '30' and a unit 's' and up/down arrows. Below these is a red 'Save' button.

Figure 8-15 Call Settings

Set the **Max. Communication Time** and **Max. Message Duration**. Click **Save**.

Note

- The Max. communication time range is 90 s to 1800 s.
 - The Max. message duration range is 30 s to 60 s.
-

Ringbacktone Settings

Steps

1. Click **Configuration** → **Intercom** → **Ringbacktone Settings** to enter the settings page.
 2. Click  to import new ringtone.
-


Note

The supported audio file type for importing is .wav. The file should be less than 800 KB.

Number Settings

Link the room No. and SIP numbers.

Click **Configuration** → **Intercom** → **Number Settings** to enter the page.



No.	Room No.	SIP Number	Operation
-----	----------	------------	-----------

Figure 8-16 Number Settings

Click **+Add**, and set the **Room No.** and SIP numbers in the pop-up dialog box.
Click **Save** to save the settings.

8.7.13 Set Card Security

Click **Configuration** → **Card Settings** → **Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

Enable the function and you can present the NFC card to authenticate. In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.



Note

Disable NFC card cannot completely avoid presenting NFC card.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption

Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable CPU Card

Enable CPU card and authenticating by presenting CPU card is available.

8.7.14 Set Privacy Parameters

Set the event storage type, picture upload and storage parameters, and the picture clearing parameters.

Go to **Configuration → Security → Privacy Settings**

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

Picture Uploading and Storage

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Clear All Pictures in Device



All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

Clear Captured Pictures

All captured pictures in the device will be deleted.

8.7.15 Set Biometric Parameters

Set Basic Parameters

Click **Configuration** → **Smart** → **Smart** .



The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Face Anti-spoofing

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.



Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Anti-spoofing Detection Level

After enabling the face anti-spoofing function, you can set the matching security level when performing anti-spoofing detection.

Recognition Distance

Select the distance between the authenticating user and the device camera.

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.

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Fingerprint Security Level

According to the actual situation, select the level.

ECO Mode

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), and ECO mode (1:1).

ECO Mode Threshold

The larger the value, the device enter the ECO Mode easier.

ECO Mode (1:N) Threshold

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

Force to Enable Night Mode

You can click to enable forced night mode when the ECO mode is enabled.

Face with Mask Detection

After enabling the face without mask detection, the system will recognize the captured face with mask picture or not. You can set face with mask 1:N matching threshold, it's ECO mode, and the strategy.

None

The function is disabled. The device will not detect whether a person is wearing a face mask or not.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask 1:N Match Threshold

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face with Mask & Face 1:N Match Threshold (ECO)

Set the matching threshold when authenticating with face mask via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Set Recognition Area

Click **Configuration** → **Smart** → **Area Configuration** .

Drag the yellow frame in the live video to adjust the recognition area. Only the face within the area can be recognized by the system.

Or drag the block of each parameter to set the area.

Click **Save**.

Click  or  , or  to capture pictures, record videos, and view full screen live video.

8.7.16 Customize Audio Content

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration** → **Preference** → **Prompt Schedule** .

2. Enable the function.

3. Set the appellation.

4. Set the time period when authentication succeeded.

1) Click **Add Time Duration**.


2) Set the time duration and the language.

Note

If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

3) Enter the audio content.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click  to delete the configured time duration.

5. Set the time duration when authentication failed.

1) Click **Add Time Duration**.


2) Set the time duration and the language.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Enter the audio content.

4) **Optional:** Repeat substep 1 to 3.

5) **Optional:** Click  to delete the configured time duration.

6. Click **Save**.

8.8 Maintenance and Security

8.8.1 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.


Reboot Device

Click **Maintenance and Security** → **Maintenance** → **Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security** → **Maintenance** → **Upgrade** .

Select an upgrade type from the drop-down list. Click  and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.



Note

Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security** → **Maintenance** → **Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Import and Export Parameters

Click **Maintenance and Security** → **Maintenance** → **Backup and Reset** .

Export

Click **Export** to export the device parameters.



Note

You can import the exported device parameters to another device.

Import

Click  and select the file to import. Click **Import** to start import configuration file.

Advanced Settings

Click **Advanced Settings**, and enter the admin password.

Face Parameter

Custom Anti-spoofing Detection

Anti-spoofing Detection Level

After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.

Anti-Spoofing Detection Threshold

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The smaller the value, the larger the false accept rate and the smaller the false rejection rate.

Lock Face for Anti-spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-spoofing Protection** when anti-spoofing detection failed.

Unlock

You can click **Unlock** according to your needs.

Version Information

You can view the device information.

8.8.2 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security** → **Maintenance** → **Device Debugging** .
2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Print Log

You can select a component from drop-down list and click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start Capture** to capture.

8.8.3 Log Query

You can search and view the device logs.

Go to **Maintenance and Security** → **Maintenance** → **Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

8.8.4 Set Protocol Testing

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **Maintenance and Security** → **Maintenance** → **Protocol Testing** .

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

8.8.5 Set Network Diagnosis

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **Maintenance and Security** → **Maintenance** → **Network Diagnosis** .

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will displayed in **PING Result**.

8.8.6 Security Audit Log

Steps

1. Click **Maintenance and Security** → **Maintenance** → **Security Audit Log** to enter the page.
2. Enable **Log Upload Server**.
3. Enter log server address and port.
4. **Optional:** You can enable **Encrypt Transmission** and **Verify Certificate**.

8.8.7 Certificate Management

It helps to manage the server/client certificates and CA certificate.



The function is only supported by certain device models.

Create and Import HTTPS Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **HTTPS Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
 - Click **View** and the created certificate will be displayed.
 - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
 - 1) In the **Import Key** area, select a certificate from the local, and click **Import**.
 - 2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Create and Import SYSLOG Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **SYSLOG Certificate** area, click **Create Certificate Request**.
3. Input certificate information and click **Save**.
 - Click **View** and the created certificate will be displayed.
 - The certificate will be saved automatically.
4. Download the certificate and save it to an asking file in the local computer.
5. Send the asking file to a certification authority for signature.
6. Import the signed certificate.
 - 1) In the **Import Key** area, select a certificate from the local, and click **Import**.
 - 2) In the **Import Communication Certificate** area, select a certificate from the local, and click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **CA Certificate ID** area.



Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

Chapter 9 Other Platforms to Configure

You can also configure the device via iVMS-4200 Client Software or HikCentral Access Control. For details, see the platforms' user manual.

iVMS-4200 Client Software

Click/tap the link to view the client software's user manual.

<http://enpinfodata.hikvision.com/analysisQR/showQR/ca930247>

HikCentral Access Control (HCAC)

Click/tap the link to view the HCAC's user manual.

<http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42>

Appendix A. Appendix

Tips When Collecting/Comparing Face Picture

- Keep your expression naturally when collecting or comparing face pictures.
- Do not wear hat, sunglasses, or other accessories that can affect the facial recognition function.
- Do not make your hair cover your eyes, ears, etc. and heavy makeup is not allowed.
- In order to get a good quality and accurate face picture, position your face looking at the camera when collecting or comparing face pictures.
- Make sure your face is in the middle of the collecting window.
- The recommended distance when collecting/comparing face pictures is between 400 mm and 500 mm.

Tips When Importing Face Picture

- The requirements of the face pictures are the same as the requirements for collecting.
- Picture format: JPG.
- The photo scale is 5:7. The pixel size is a minimum of 480 and the height is a minimum of 640.
- Picture size cannot exceed 200 KB.
- A pure background color is required. White is the best.



See Far, Go Further