






Video Intercom Villa Door Station

User Manual

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.

Video Intercom Villa Door Station User Manual

- 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.
- Input voltage should meet both the SELV and the Limited Power Source according to 60950-1 standard.
- The power supply must conform to LPS. The recommended adaptor models and manufacturers are shown as below. Use the attached adapter, and do not change the adaptor randomly.

Model	Manufacturer	Standard
ADS-24S-12 1224GPCN	SHENZHEN HONOR ELECTRONIC CO.,LTD	CEE
G0549-240-050	SHENZHEN GOSPELL DIGITAL TECHNOLOGY CO.,LTD	CEE
TS-A018-120015Ec	SHENZHEN TRANSIN TECHNOLOGIES CO., LTD	CEE

Battery:

Do not ingest battery. Chemical burn hazard! This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death. Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

CAUTION: Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the 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 the 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. + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.

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



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.

About this Manual

Product	Wireless Description
Villa Door Station	2.4 G Wi-Fi + 13.56 MHz

Contents

Chapter 1 Appearance	1
Chapter 2 Terminal and Wiring Description	8
2.1 Terminal Description	8
2.2 Wiring Description	9
2.2.1 Door Lock Wiring	9
2.2.2 Door Contact Wiring	10
2.2.3 Exit Button Wiring	11
2.2.4 Alarm Input Device Wiring	12
Chapter 3 Installation	13
3.1 Accessory Introduction	13
3.2 Surface Mounting with Protective Shield	14
3.3 Surface Mounting without Protective Shield	16
3.4 Flush Mounting with Protective Shield	18
3.5 Flush Mounting without Protective Shield	20
Chapter 4 Activation	23
4.1 Activate via SADP	23
4.2 Activate via Web Browser	24
4.3 Activate Device via Client Software	24
4.4 Edit Network Parameters	25
Chapter 5 Quick Operation via Web Browser	26
5.1 Select Language	26
5.2 Time Settings	26
5.3 Privacy Settings	26
5.4 Administrator Settings	27
5.5 No. and System Network	27
Chapter 6 Operation via PC Web	29

6.1 Login Web Browser	29
6.2 Forget Password	29
6.3 Overview	29
6.4 Person Management	30
6.5 Search Event	32
6.6 Device Management	32
6.7 Configuration	33
6.7.1 View Device Information via PC Web	33
6.7.2 Set Time	34
6.7.3 Set DST	35
6.7.4 Change Administrator's Password	35
6.7.5 Online Users	35
6.7.6 Set Secure Door Control Unit Parameters via PC Web	36
6.7.7 Set I/O Parameters	36
6.7.8 View Device Arming/Disarming Information	36
6.7.9 Network Settings	37
6.7.10 Set Video and Audio Parameters	42
6.7.11 Adjust Display Settings	44
6.7.12 Event Settings	46
6.7.13 Access Control Settings	47
6.7.14 Video Intercom Settings	51
6.8 Maintenance and Security	55
6.8.1 Set Protocol Testing	55
6.8.2 Set Network Diagnosis	55
6.8.3 Upgrade and Maintenance	56
6.8.4 Device Debugging	57
6.8.5 View Log via PC Web	58
6.8.6 Certificate Management	58

Chapter 7 Configuration via Client Software	60
7.1 Device Management	60
7.1.1 Add Online Device	60
7.1.2 Add Device by IP Address	60
7.1.3 Add Device by IP Segment	60
7.2 Live View via Door Station	61
7.3 Organization Management	61
7.3.1 Add Organization	61
7.3.2 Modify and Delete Organization	61
7.4 Person Management	62
7.4.1 Add Person	62
7.4.2 Modify and Delete Person	63
7.4.3 Change Person to Other Organization	63
7.4.4 Import and Export Person Information	63
7.4.5 Get Person Information from Device	64
7.4.6 Issue Card in Batch	64
7.5 Video Intercom Settings	66
7.5.1 Receive Call from Door Station	67
7.5.2 Release Notice	67
7.5.3 Search Video Intercom Information	68
7.5.4 Upload Armed Information	70
Chapter 8 Video Intercom Operation	71
8.1 Call Resident	71
8.2 Unlock Door	71

Chapter 1 Appearance

Single-Button Villa Door Station

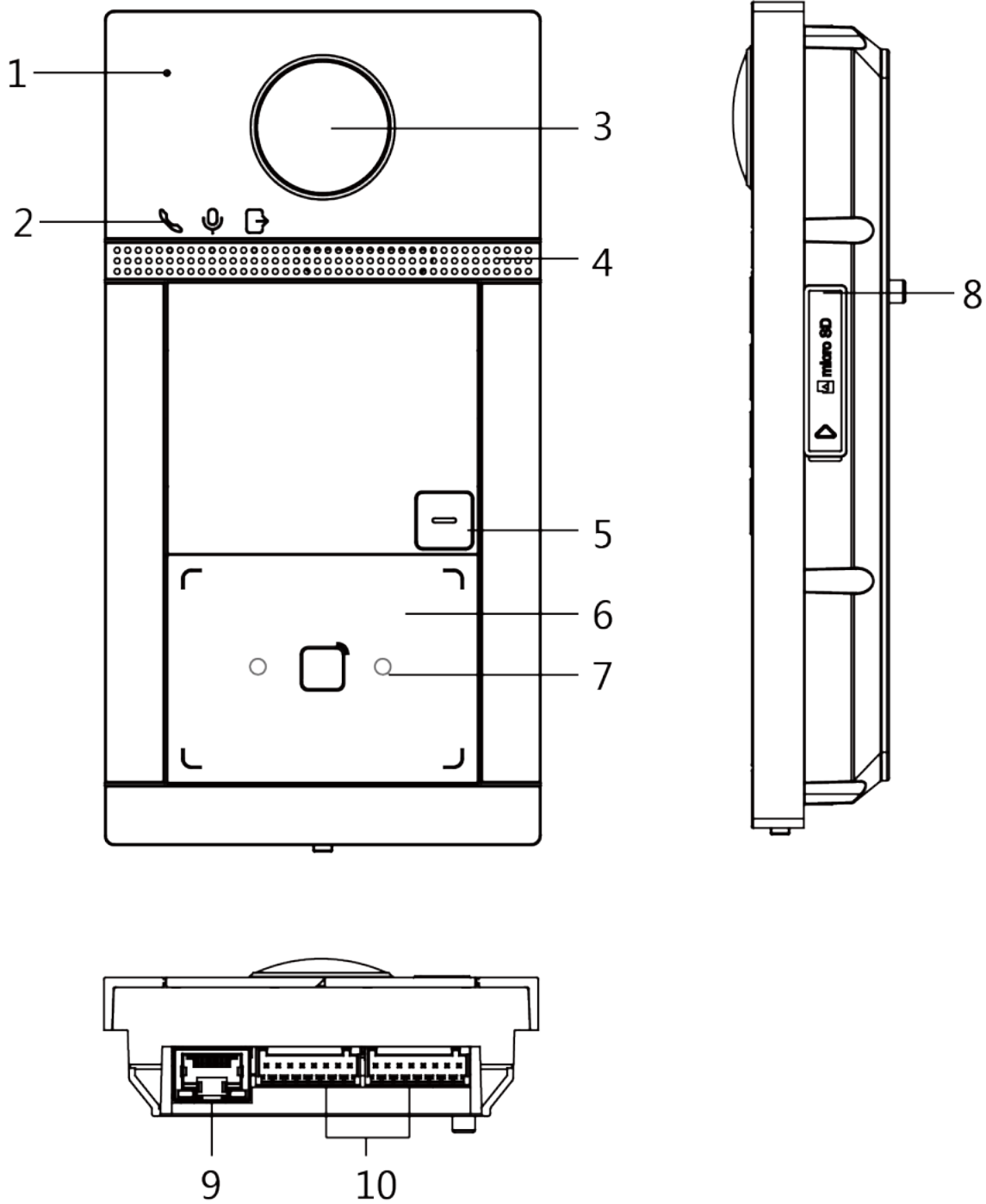


Figure 1-1 Single-Button Villa Door Station Appearance

Table 1-1 Description

No.	Description
1	Microphone
2	Indicator Unlock (Green)/ Call (Orange)/ Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	TF Card Slot (Reserved) & Debugging Port
9	LAN
10	Terminals

Two-Button Villa Door Station

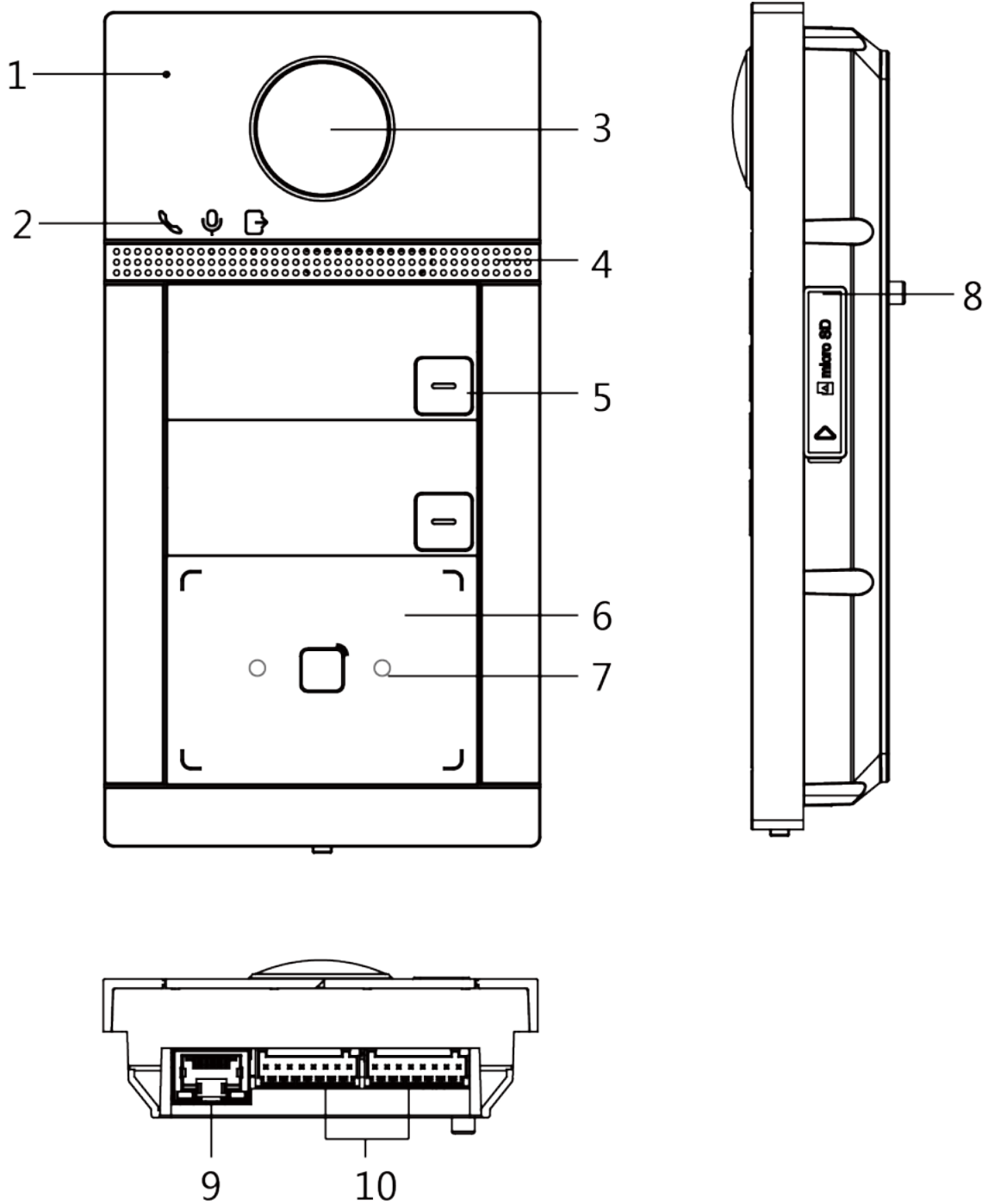


Figure 1-2 Two-Button Villa Door Station Appearance

Table 1-2 Description

No.	Description
1	Microphone
2	Indicator Unlock (Green)/ Call (Orange)/ Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	TF Card Slot (Reserved) & Debugging Port
9	LAN
10	Terminals

Four-Button Villa Door Station

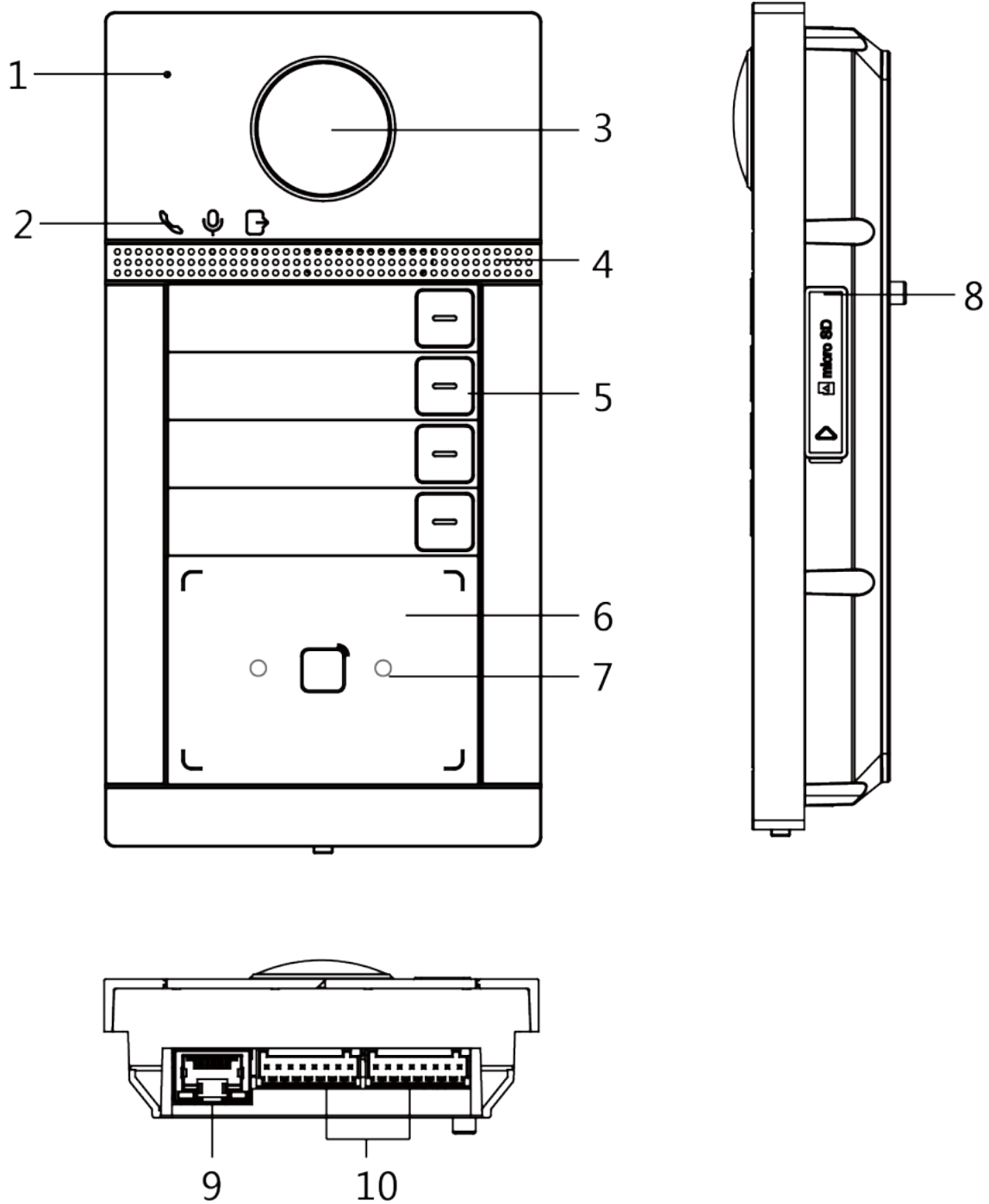


Figure 1-3 Four-Button Villa Door Station Appearance

Table 1-3 Description

No.	Description
1	Microphone
2	Indicator Unlock (Green)/ Call (Orange)/ Communicate (White)
3	Camera
4	Loudspeaker
5	Button
6	Card Reading Area
7	IR Light
8	TF Card Slot (Reserved) & Debugging Port
9	LAN
10	Terminals

Chapter 2 Terminal and Wiring Description

2.1 Terminal Description

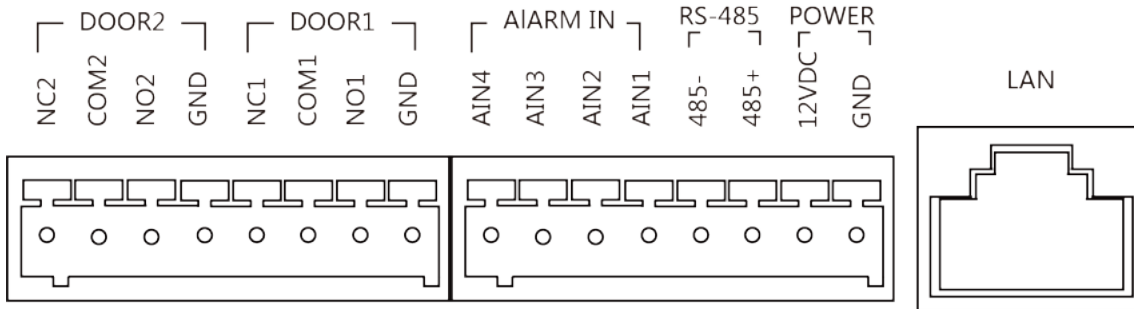




Figure 2-1 Terminal Description

Table 2-1 Description of Terminal and Interfaces

Name	Interface	Description
DOOR	NC2	Door Lock Relay Output 2 (NC)
	COM2	Common Interface
	NO2	Door Lock Relay Output 2 (NO)
	GND	Grounding
	NC1	Door Lock Relay Output 1 (NO)
	COM1	Common Interface
	NO1	Door Lock Relay Output 1 (NO)
	GND	Grounding
ALARM IN	AI1	Alarm Input 1 (For the access of Door Contact)
	AI2	Alarm Input 2 (For the access of Door Contact)
		 Note Before accessing to the Door Contact, select Input as Door Status in I/O Settings page first.
	AI3	Alarm Input 3 (For the access of Exit Button)
	AI4	Alarm Input 4 (For the access of Exit Button)

Name	Interface	Description
		 Note Before accessing to the Exit Button, select Input as Exit Button in I/O Settings page first.
RS-485	485+	RS-485 Communication Interface
	485-	
Power Input	12 VDC	12 VDC Input
	GND	
Network	LAN	Network Interface

2.2 Wiring Description

2.2.1 Door Lock Wiring

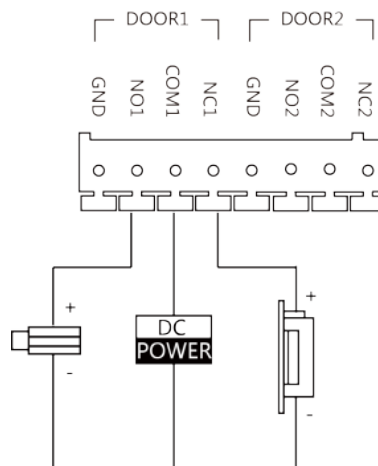


Figure 2-2 Door Lock Wiring

Note

- Terminal NC1/COM1 is set as default for accessing magnetic lock/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 Guarding Vision client software.

2.2.2 Door Contact Wiring

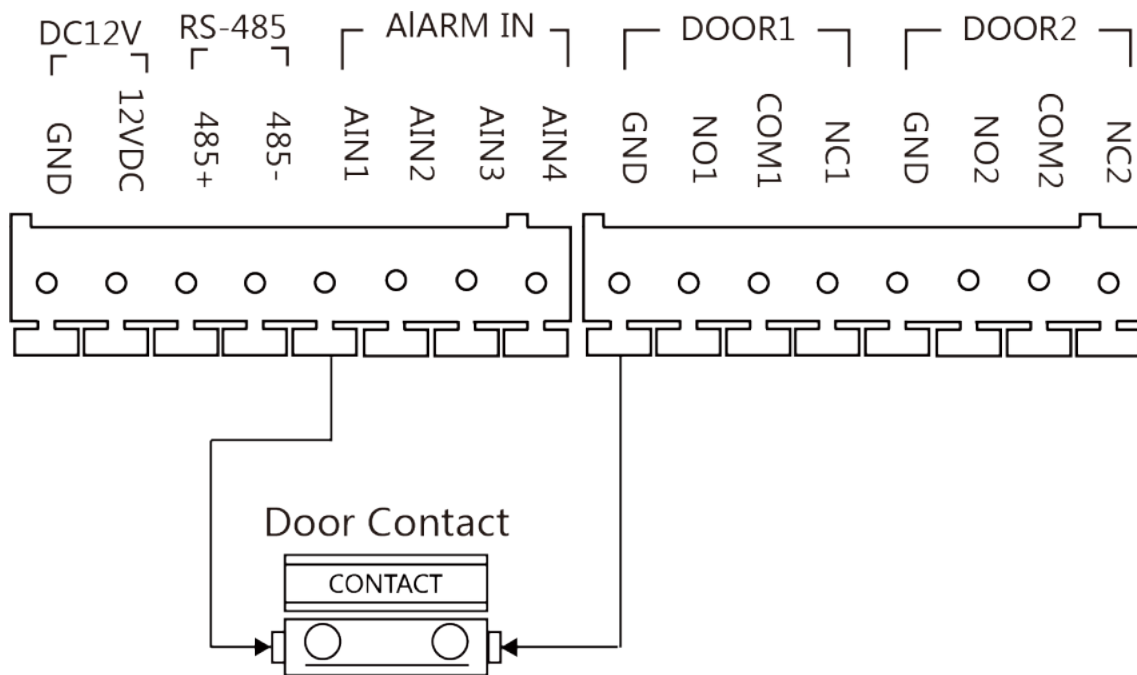


Figure 2-3 Door Contact Wiring

Note

If the door contact is not used, the corresponding input interface needs to be grounded. Otherwise the door light will stay open.

2.2.3 Exit Button Wiring

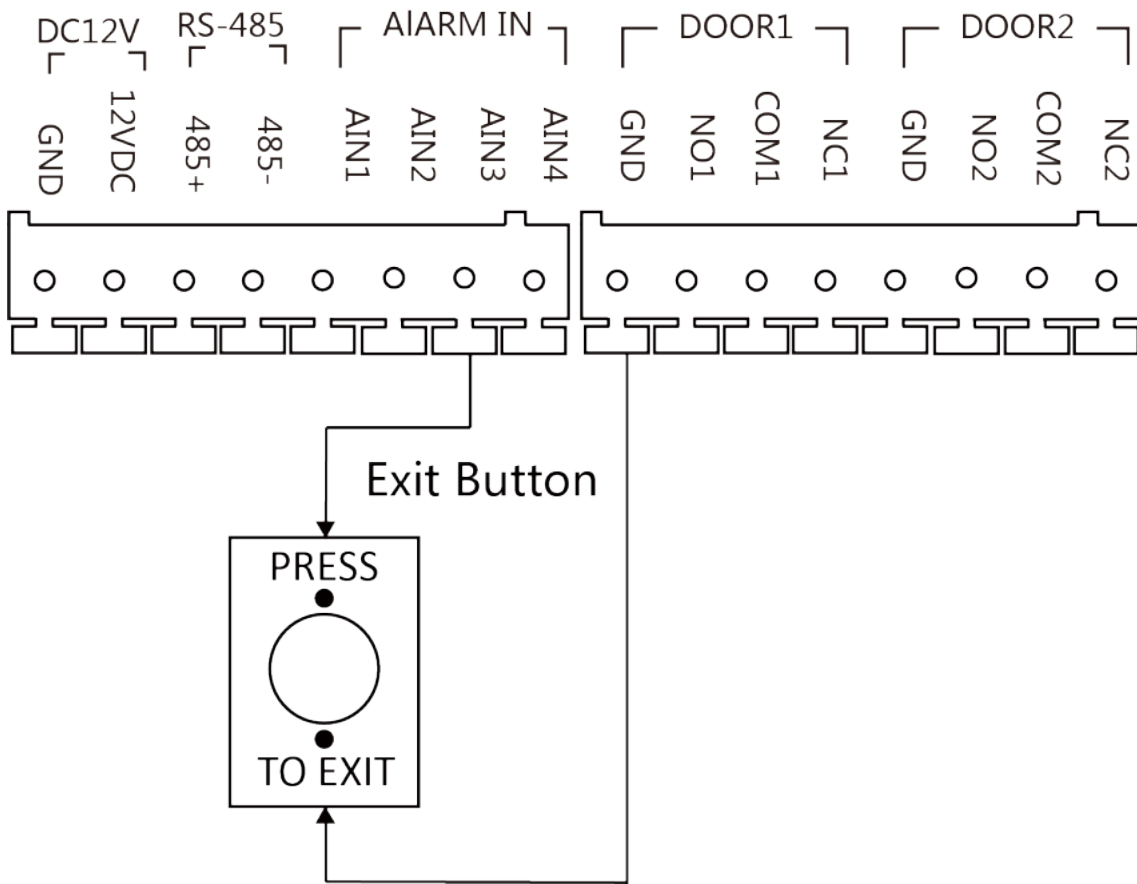


Figure 2-4 Exit Button Wiring

2.2.4 Alarm Input Device Wiring

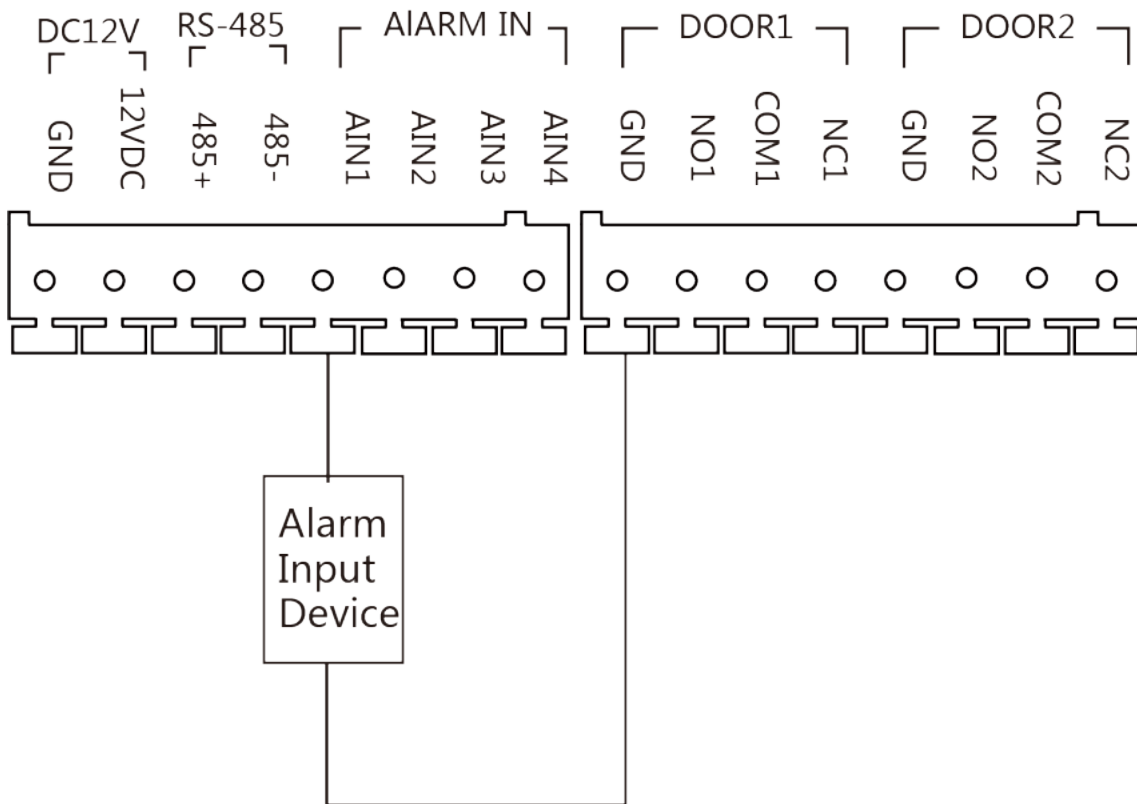


Figure 2-5 Alarm Input Device Wiring

Chapter 3 Installation

Note

- Make sure the device in the package is in good condition and all the assembly parts are included.
 - 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.
-

3.1 Accessory Introduction

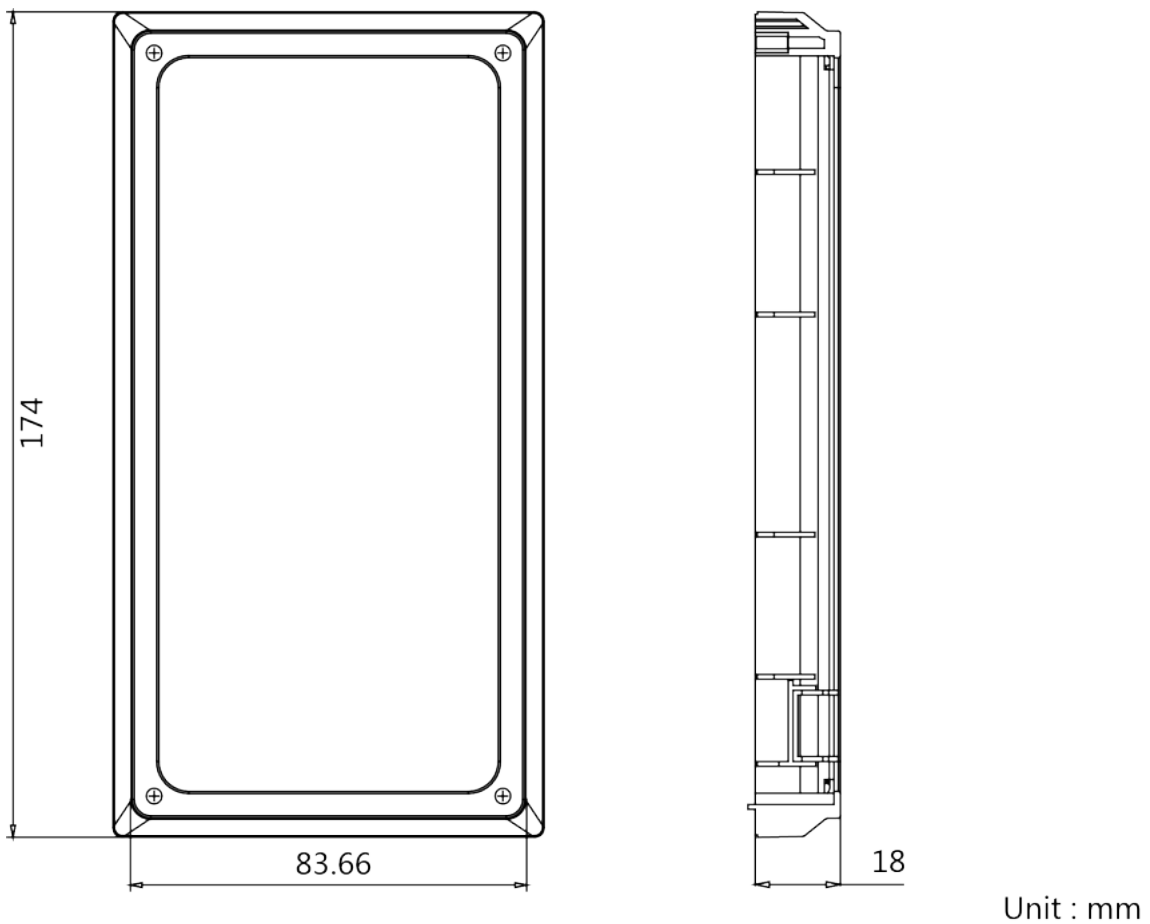


Figure 3-1 Accessory Introduction

Note

The dimension of gang box for door station is: 174 (length) × 83.66 (width) × 18 (depth) mm.

3.2 Surface Mounting with Protective Shield

Before You Start

- Tools that you need to prepare for installation: Drill ($\varnothing 2.846$) and gradienter.
- Purchase the protective shield before installation.

Steps

1. Stick the mounting template on the wall. Drill screw holes according to the mounting template.
Remove the template from the wall.

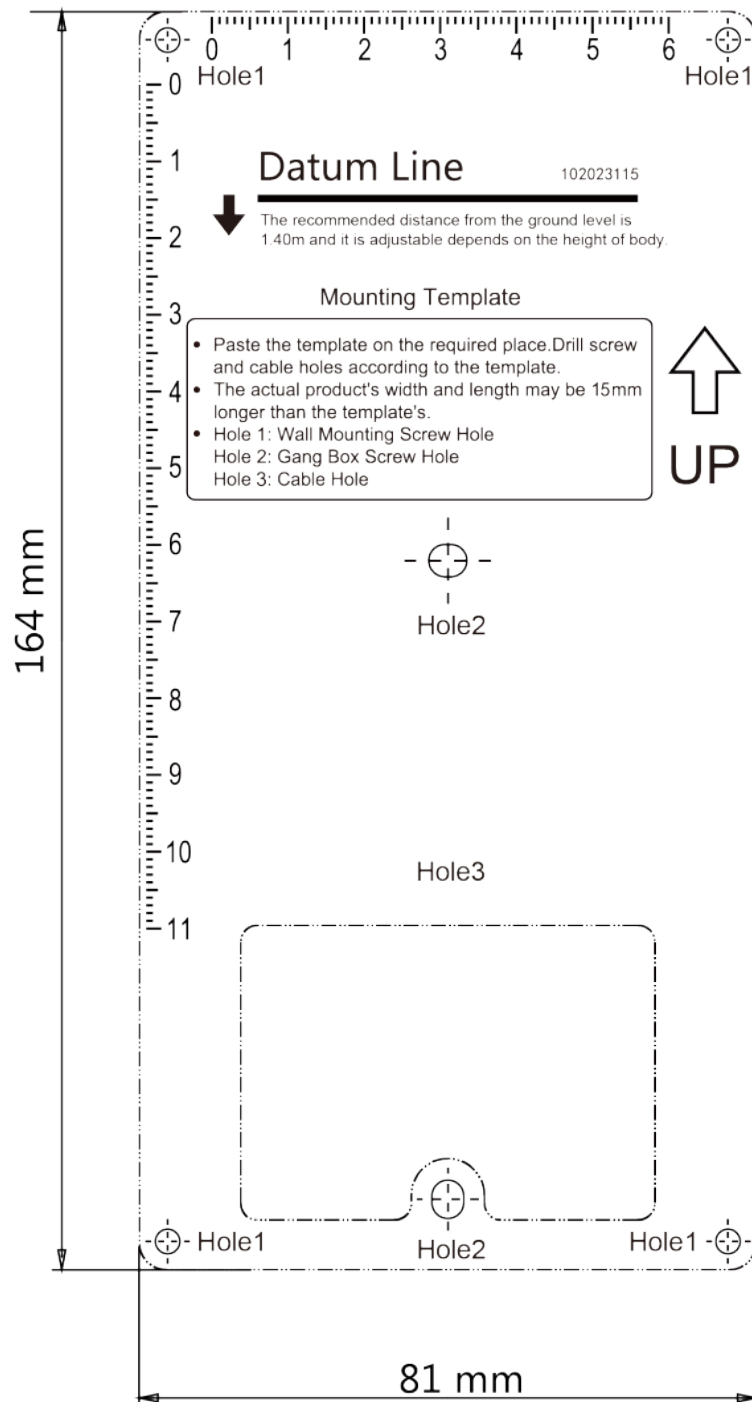


Figure 3-2 Mounting Template

2. Align the protective shield with mounting template.
3. Secure the mounting plate on the wall with 4 supplied screws according to the screw holes.
4. Secure the device on the mounting plate with 4 supplied set screws.
5. Fix the cover onto the device with the screw.

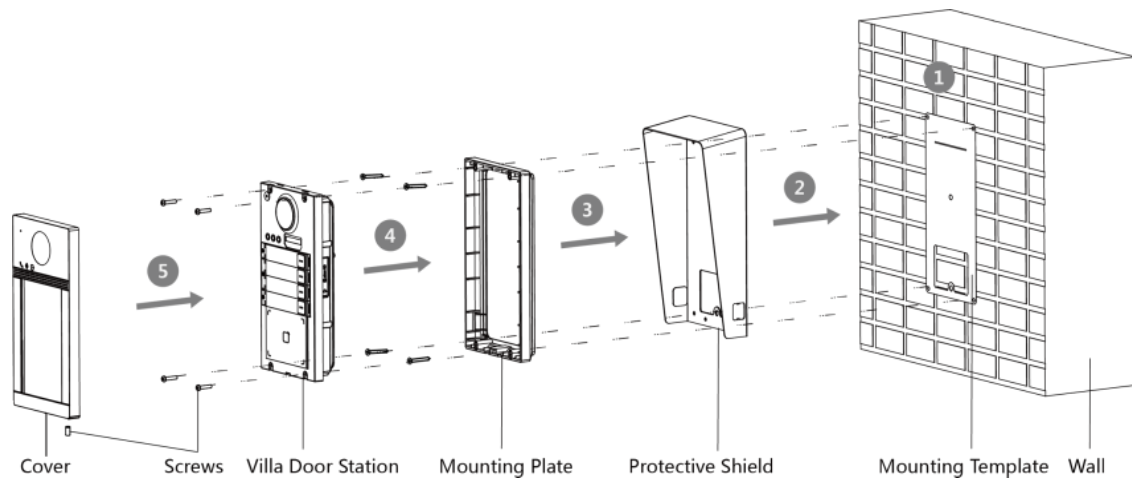


Figure 3-3 Surface Mounting with Protective Shield

3.3 Surface Mounting without Protective Shield

Before You Start

Tools that you need to prepare for installation: Drill ($\varnothing 2.846$) and gradienter.

Steps

1. Stick the mounting template on the wall. Drill screw holes according to the mounting template. Remove the template from the wall.

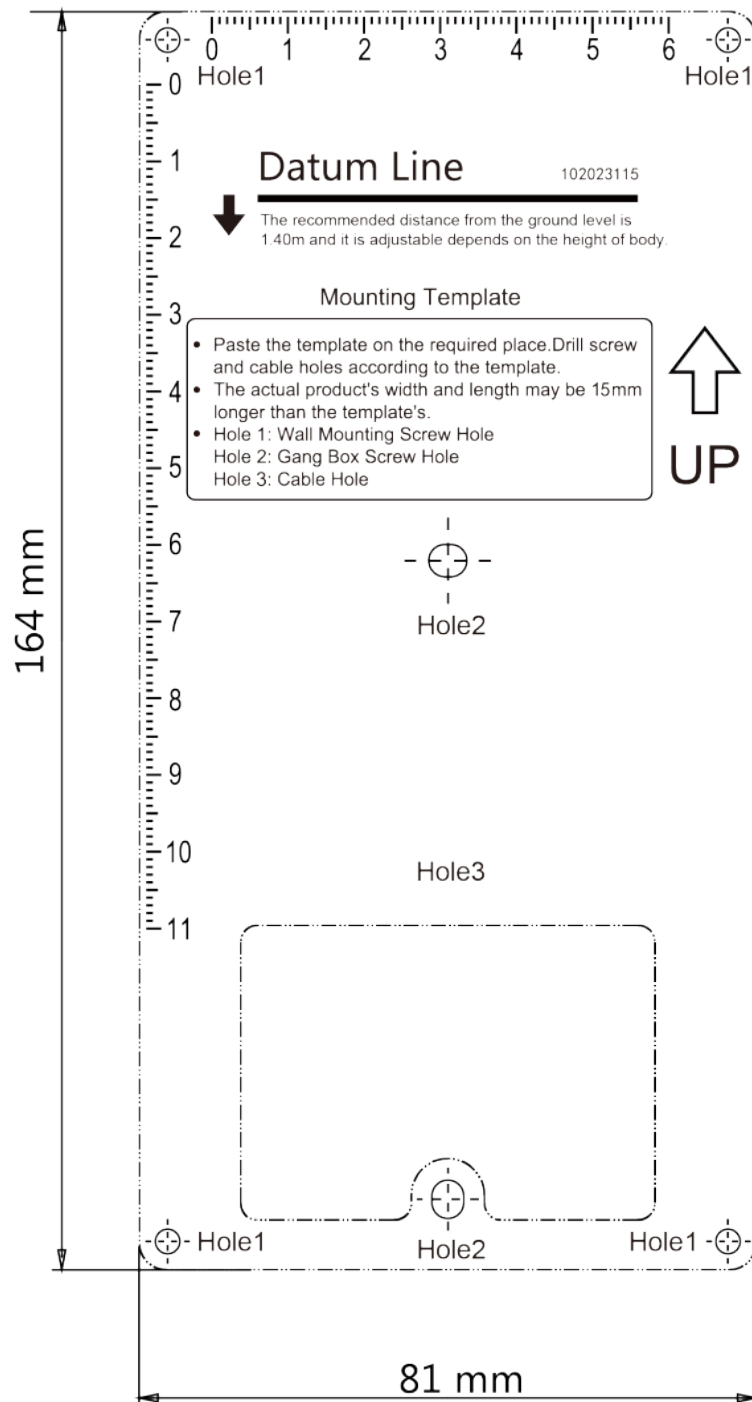


Figure 3-4 Mounting Template

2. Secure the mounting plate on the wall with 4 supplied screws according to the screw holes.
3. Secure the device on the mounting plate with 4 supplied set screws.
4. Fix the cover onto the device with the screw.

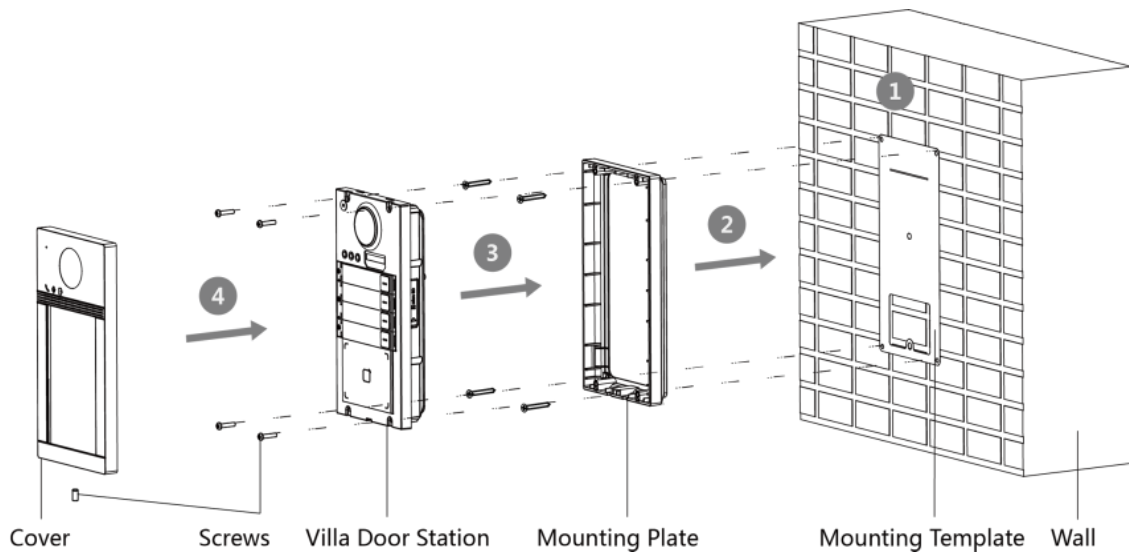


Figure 3-5 Surface Mounting without Protective Shield

3.4 Flush Mounting with Protective Shield

Before You Start

- Tools that you need to prepare for installation: Drill ($\varnothing 2.846$) and gradienter.
- Purchase the protective shield before installation.

Steps

1. Stick the mounting template on the wall. Drill the hole according to the mounting template. Remove the template from the wall.

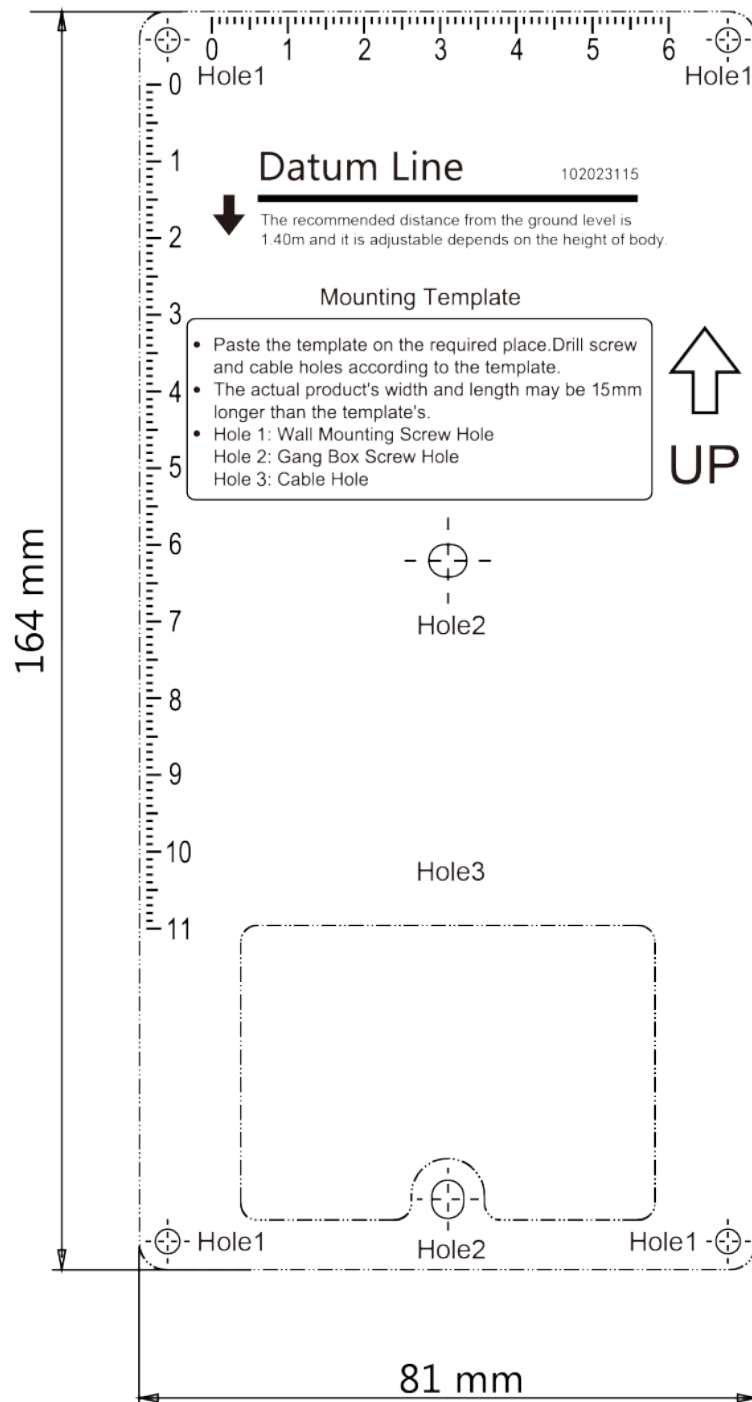


Figure 3-6 Mounting Template

Note

The suggested size of hole is 175 mm × 84 mm × 19 mm.

2. Install the gang box into the hole with 4 screws.

3. Align the protective shield with the gang box.
4. Insert the device to the gang box. Secure the device with 4 supplied screws.
5. Fix the cover onto the device with the screw.

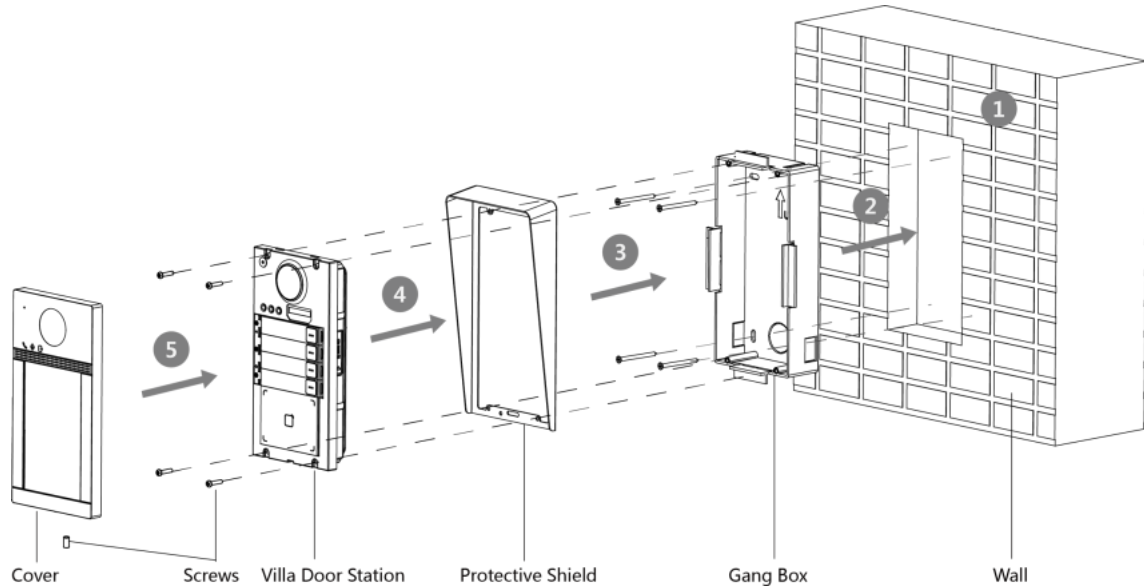


Figure 3-7 Flush Mounting with Protective Shield

3.5 Flush Mounting without Protective Shield

Before You Start

Tools that you need to prepare for installation: Drill ($\varnothing 2.846$) and gradienter.

Steps

1. Stick the mounting template on the wall. Drill the hole according to the mounting template. Remove the template from the wall.

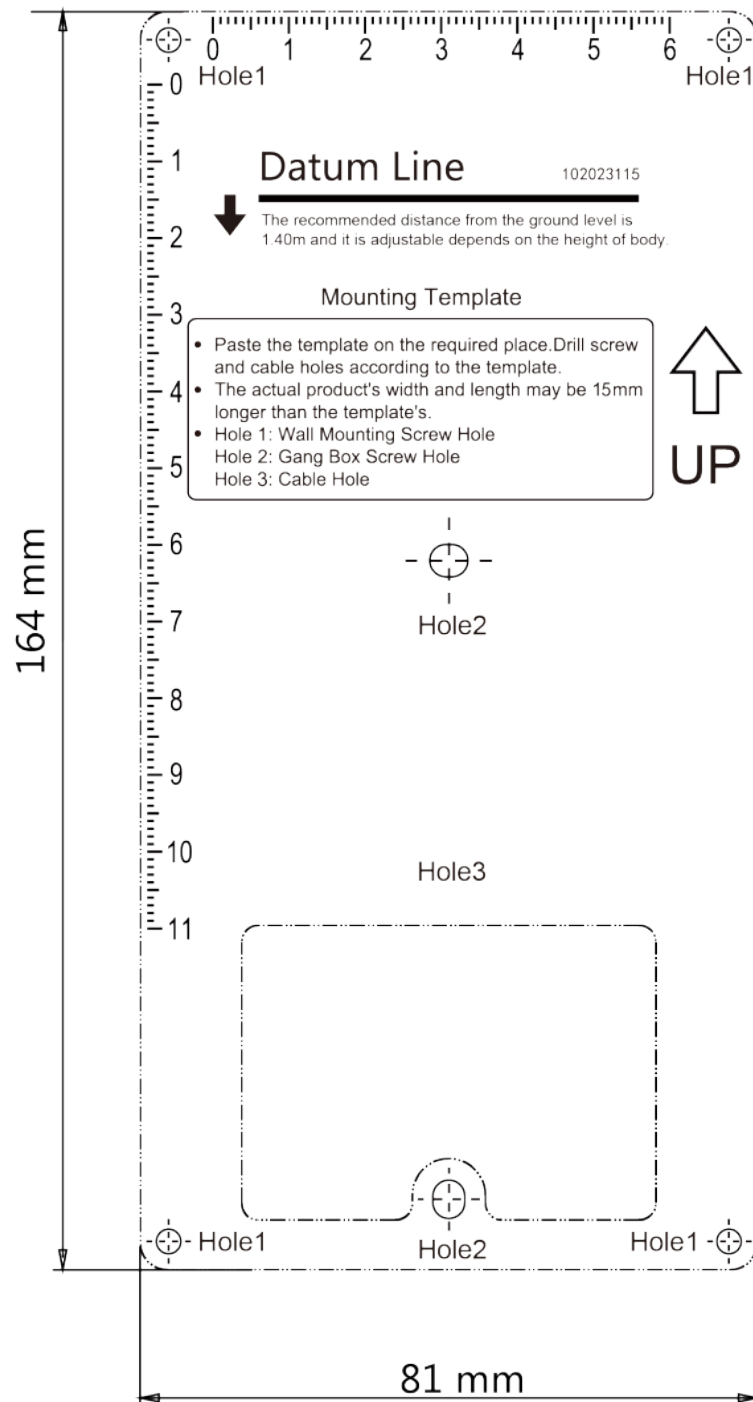


Figure 3-8 Mounting Template

Note

The suggested size of hole is 175 mm × 84 mm × 19 mm.

2. Secure the gang box into the hole with 4 screws.

3. Insert the device to the gang box. Secure the device with 4 supplied screws.
4. Fix the cover onto the device with the screw.

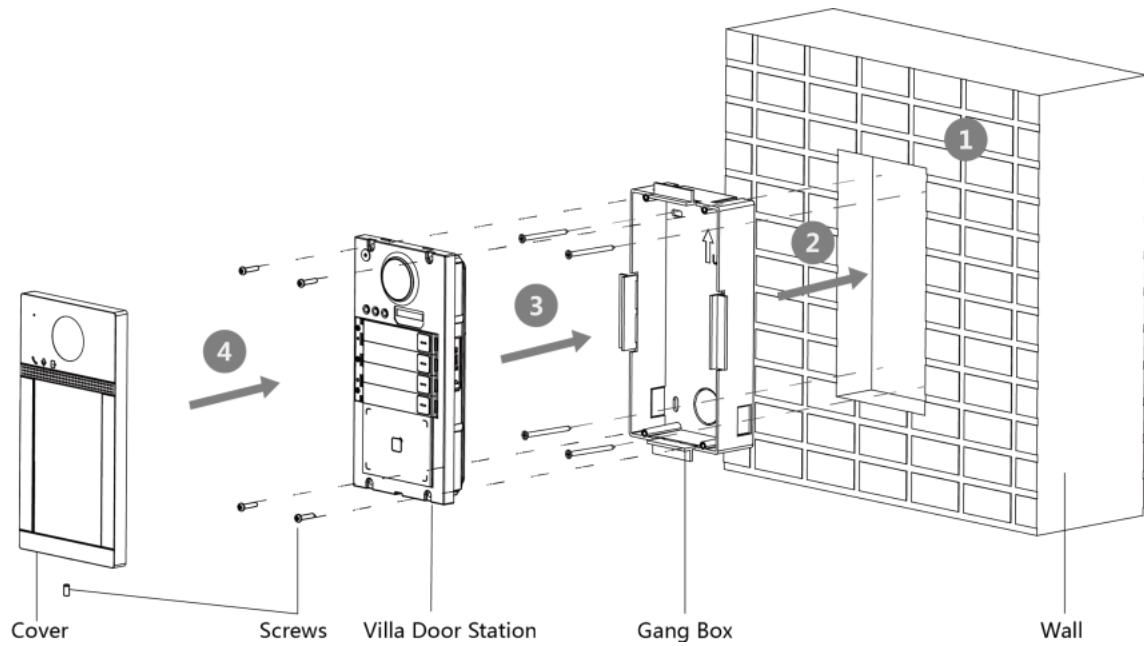


Figure 3-9 Flush Mounting without Protective Shield

Chapter 4 Activation

4.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

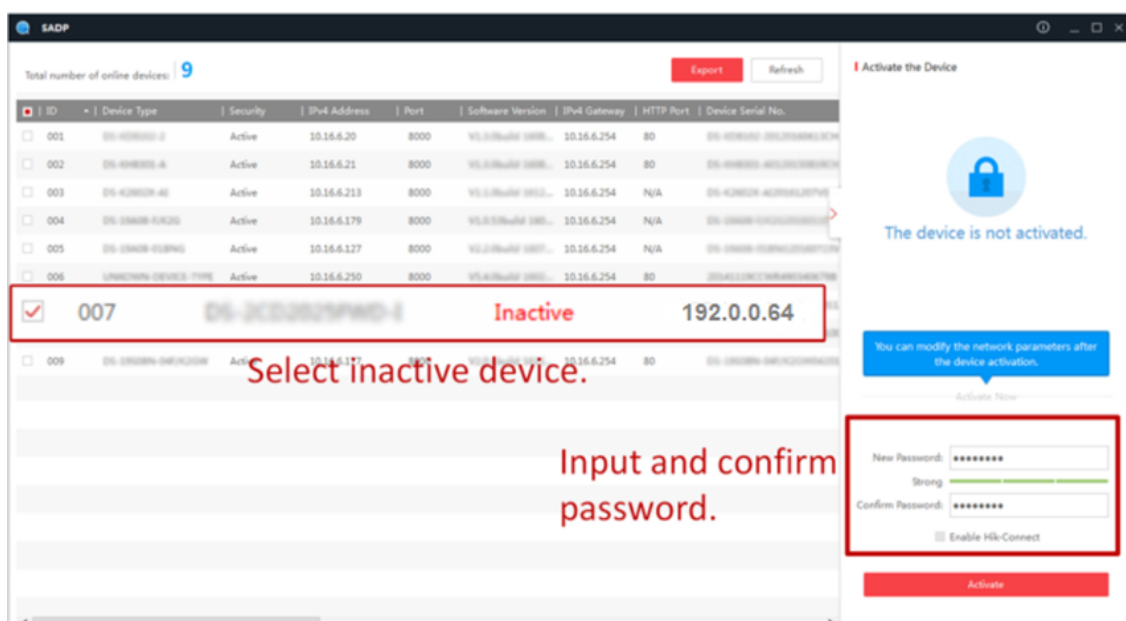
1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.



Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including 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 **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

- 1) Select the device.
- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

4.2 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.
-



Note

- 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.
 - The username cannot be the same as the password. Password cannot be inverted write of user name.
 - 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.
 - Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
-

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.

4.3 Activate Device via Client Software

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

Default parameters of door station are as follows:

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

Steps

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

Note

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

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

Note

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

4.4 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 **Guarding Vision** client software.

Steps

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


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.

Chapter 5 Quick Operation via Web Browser

5.1 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.

5.2 Time Settings

Click  in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** 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.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

5.3 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.

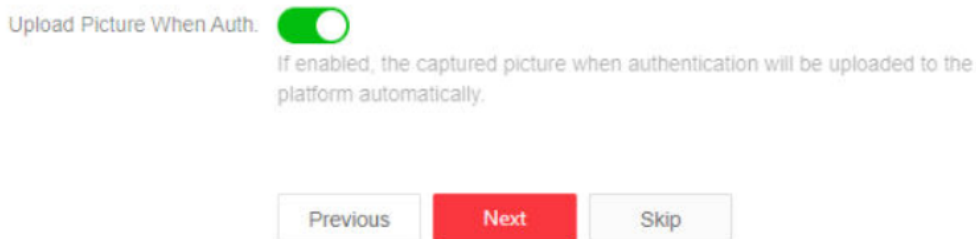


Figure 5-1 Privacy Settings


Upload Picture When Auth.

Upload the pictures when authenticating to the platform automatically.

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

5.4 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. Click **Add Card** to enter the Card No. and select the property of the card.


Note

Up to 5 cards can be supported.

4. Click **Complete** to complete the settings.
-

5.5 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.**

Device Type

The device can be used as a door station or doorphone. 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.

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 6 Operation via PC Web

6.1 Login Web Browser

You can log into the Web browser for device configuration.

Steps

1. Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
2. Enter the device user name and the password. Click **Login** to login to the page.

6.2 Forget Password

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

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 the server email address 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.

6.3 Overview

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

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, Card, and Event capacity.

6.4 Person Management

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

Add Basic Information

Click **Person** → **+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 Validity Period

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

Set the authentication type. You can choose from cards and pin configuration.

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

Add Card

Click **Person** → **+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.

Generate PIN

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

You can click **Auto Generate** to get a random pin.

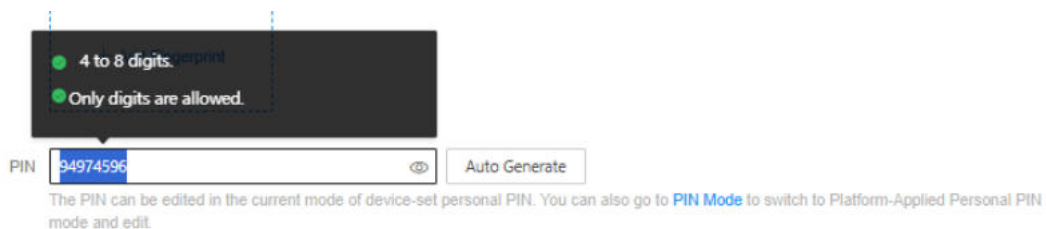
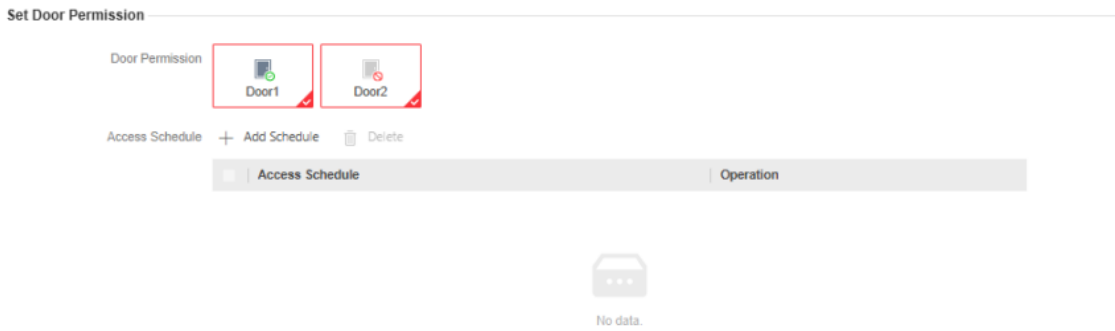


Figure 6-2 PIN

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

Set Door Permission

You can add schedule and door permission for each person.



Note

Just select an access schedule from your saved template and click **OK**.

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

6.5 Search Event

Click **Access Control** → **Event Search** to enter the page.

No.	Employee ID	Name	Card No.	Event Types	Time	Operation
1	--	--	--	Device Powering On	2022-07-06 09:32:04 00:00	--
2	--	--	--	Door Locked	2022-07-06 09:32:04 00:00	--
3	--	--	--	Device Tampered	2022-07-06 09:32:07 00:00	--
4	--	--	--	Authentication via Fingerprint Failed	2022-07-06 09:32:21 00:00	--
5	--	--	--	The password mismatches.	2022-07-06 09:54:24 00:00	--
6	--	--	--	The password mismatches.	2022-07-06 10:04:54 00:00	--
7	--	--	--	Network Disconnected	2022-07-06 10:05:05 00:00	--
8	--	--	--	Network Recovered	2022-07-06 10:05:08 00:00	--
9	--	--	--	Local Login	2022-07-06 10:06:06 00:00	--
10	--	--	--	Remote Login	2022-07-06 10:07:21 00:00	--
11	--	--	--	Remote Login	2022-07-06 10:12:50 00:00	--
12	--	--	--	Remote Login	2022-07-06 10:14:59 00:00	--
13	--	--	--	Remote Login	2022-07-06 10:20:46 00:00	--
14	--	--	--	Remote Login	2022-07-06 10:25:30 00:00	--
15	--	--	--	Remote Login	2022-07-06 10:37:30 00:00	--
16	--	--	--	Local Login	2022-07-06 10:40:55 00:00	--
17	--	--	--	Remote Login	2022-07-06 10:47:01 00:00	--
18	--	--	--	Remote Login	2022-07-06 11:05:29 00:00	--

Figure 6-3 Search Event

Enter the search conditions, including the event type, 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.

6.6 Device Management

You can manage the linked device on the page.

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



Figure 6-4 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.

Refresh

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

Synchronize

Click **Synchronize**, enable **synchronize** and click **OK** to synchronize parameters for activated devices.



Note

After enabling Sync. Parameters, activated devices will synchronize parameters. Inactivated devices will synchronize parameters whether enabling Sync. Parameters or not.

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.

6.7 Configuration

6.7.1 View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc.

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

You can view the device name, device No., language, model, serial No., version, number of channels, IO input, IO output, lock, alarm input, alarm output, and device capacity, etc. Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

6.7.2 Set Time

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

Click **System and Maintenance** → **System 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 6-5 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.


6.7.3 Set DST

Steps

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

6.7.4 Change Administrator's Password

Steps

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

Note

- 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.
 - The username cannot be the same as the password. Password cannot be inverted write of user name.
 - 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.
 - Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
-

6.7.5 Online Users

The information of users logging into the device is shown.

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

6.7.6 Set Secure Door Control Unit Parameters via PC Web

You can set secure door control unit parameters.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Access Configuration** → **Secure Door Control Unit** .
2. View secure door control unit status.
3. You can enable **Auto Binding**.



If the function is enabled, the connected secure door control unit will be automatically bound to the door station and cannot be used for other door stations.

6.7.7 Set I/O Parameters

You can set I/O Parameters on PC Web.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Access Configuration** → **I/O Settings** .
2. Select Input 2 as **Disable** or **Door Status**. Select Input 3 and Input 4 as **Disable** or **Exit Button**.



The Input 1 is **Door Status** by default.

3. Select Output 2 as **Disable**, **Mechanical Doorbell** or **Electric Lock**.



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

6.7.8 View Device Arming/Disarming Information

View device arming type and arming IP address.

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

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

6.7.9 Network Settings

Set Basic Network Parameters

Click **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **TCP/IP** .

TCP/IP

dhcp

*IPv4 Address

*IPv4 Subnet Mask

*IPv4 Default Gateway

IPv6 Mode Manual dhcp Route Advertisement

[View Route Advertisement](#)

IPv6 Address

IPv6 Subnet Prefix Length

IPv6 Default Gateway

Mac Address

MTU

*Alarm Center IP

*Alarm Host Port

DNS Server

Preferred DNS Server

Alternate DNS Server

Save

Figure 6-6 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.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Enter **IPv6 Address**, **IPv6 Prefix Length**, and **IPv6 Default Gateway**. Consult the network administrator for required information.

Device Hotspot

Only some models support this function.

Steps

1. Click **Network → Network Settings → Device Hotspot** .

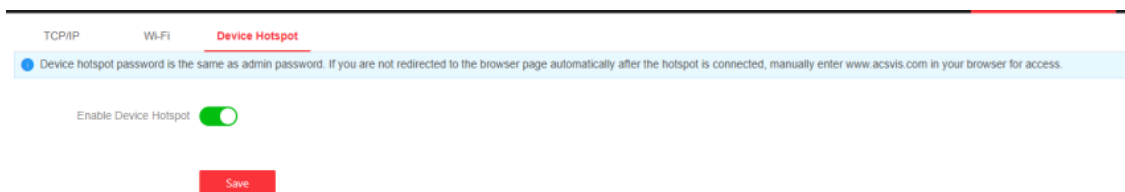


Figure 6-7 Device Hotspot

2. Slide to enable/disable device hotspot.

Note

Device hotspot password is the same as admin password. If you are not redirected to the browser page automatically after the hotspot is connected, manually enter www.acsvis.com in your browser for access.

3. Click **Save**.

Wi-Fi Settings

Some models support Wi-Fi function.

Steps

1. Click **System Configuration → Network → Network Settings → Wi-Fi** to enter the settings page.

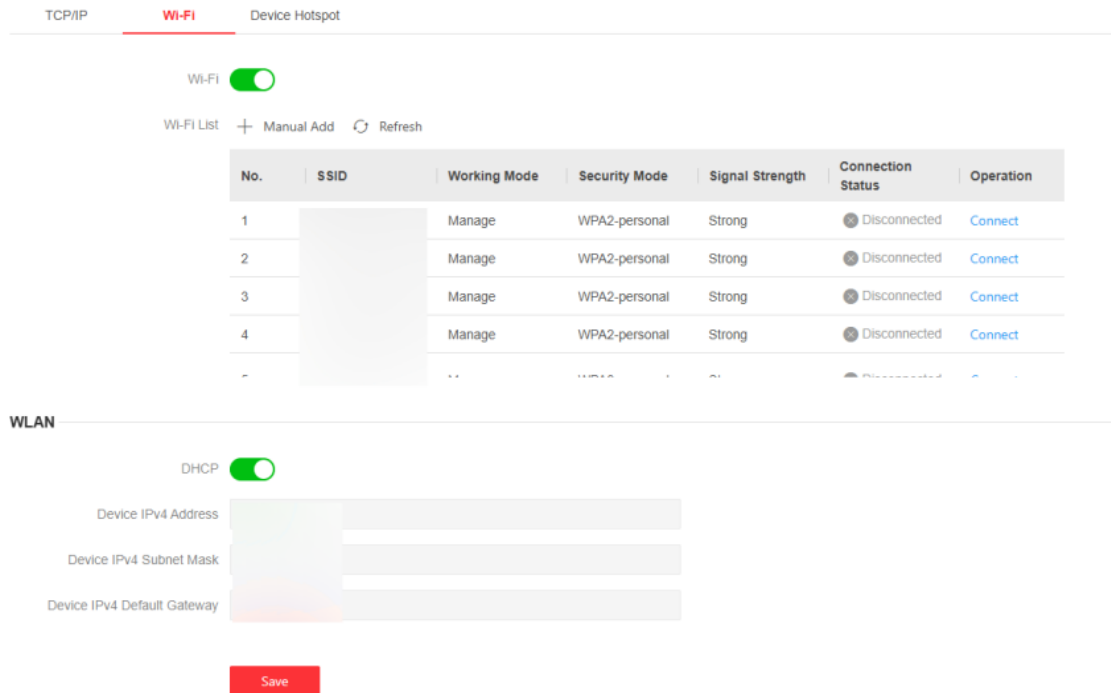


Figure 6-8 Wi-Fi

2. Enable **Wi-Fi**.
3. Click **+ Manual Add**, and set corresponding parameters and **Password** of the Wi-Fi.
 - 1) Enter the **SSID**.
 - 2) Select **Security Mode**.
 - 3) Click **Save**.
 - 4) **Optional**: Click **Refresh** to get the present information.
4. Click **Connect**.

Set Port Parameters

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

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

RTSP

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

Click **System 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 **System Configuration** → **Network** → **Device Access** → **Guarding Vision** to enter the settings page.



Guarding Vision 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. Enter the verification code.
6. Bind an account.
Binding via Code: Use the App to scan the QR code at the back of your device to bind the account.
7. Click **Save** to enable the settings.

FTP Settings

You can configure FTP (File Transfer Protocol) parameters.

Steps

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

HTTP(S) RTSP **FTP** WebSocket(s)

Enable FTP

Server Type

*Server IP Address

*Port

Anonymous

*User Name

*Password

*Password Confirm

Directory Structure

Parent Directory

Child Directory

*Delimiter

Named Item

Named Item

Named Element

Figure 6-9 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 VoIP

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

Steps

1. Click **System Configuration** → **Network** → **Device Access** → **VoIP** .
2. Slide to **Enable VoIP Gateway**.
3. Enter **Server IP Address** and **Server Port**.
4. Enter **Register User Name** and **Registration Password**.
5. Set **Expiry Time**. The range is 15 to 99 min.
6. Slide to **Enable P2P** according to your actual need.
7. Click **Save**.
8. 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.

6.7.10 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **System and Maintenance** → **System 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 6-10 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 **System and Maintenance** → **System Configuration** → **Video/Audio** → **Audio** .

Stream Type Main Stream Sub-stream

Audio Encoding G.711ulaw

Input Volume 7

Output Volume 7

Audio Sampling Rate 8 KHz

Figure 6-11 Audio Settings Page

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

Slide to enable **Unlocking Sound** according to your actual need.

Check then click < or > to enable or disable **SIP Audio Encoding**.



You can drag icon ≡ to adjust the order of the encoding.

Click **Save** to save the settings.

6.7.11 Adjust Display Settings

You can adjust image parameters, video parameters, supplement parameters, backlight, beauty etc..

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **Display Settings**.
2. Configure the parameters to adjust the image.

Video Adjustment

Set the video frame rate when performing live view remotely. After changing the video 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

- You can enable or disable the BLC function.
If enabled, you can choose BLC as **Center, UP, Down, Left** or **Right**.
- You can 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.

Day/Night Switch

You can choose Day/Night Switch as Auto, Schedule Switch, Night or Daytime mode.

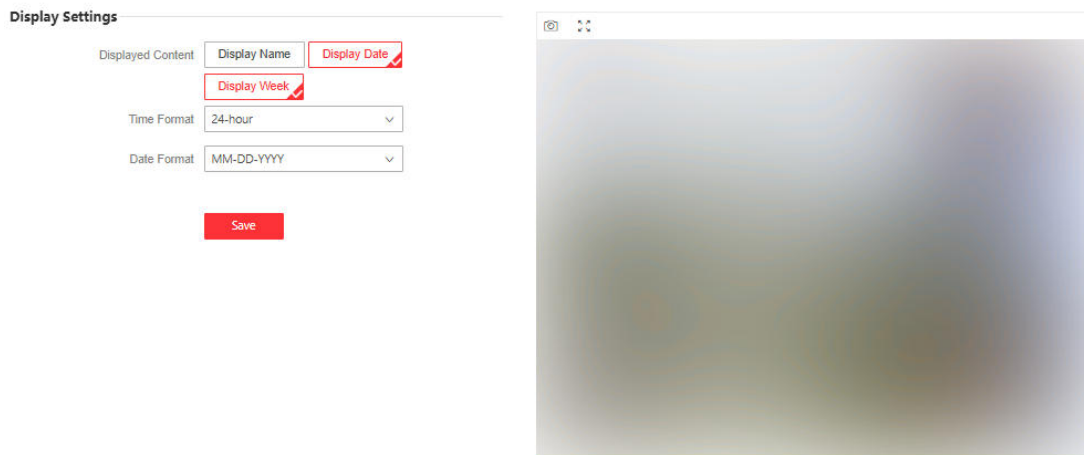
When choose Day/Night Switch as Auto, you also need to select **Sensitivity** range from 1 to 7.

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

OSD Configuration

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **OSD Configuration** .
2. At **Displayed Content**, you can click to choose what to display.

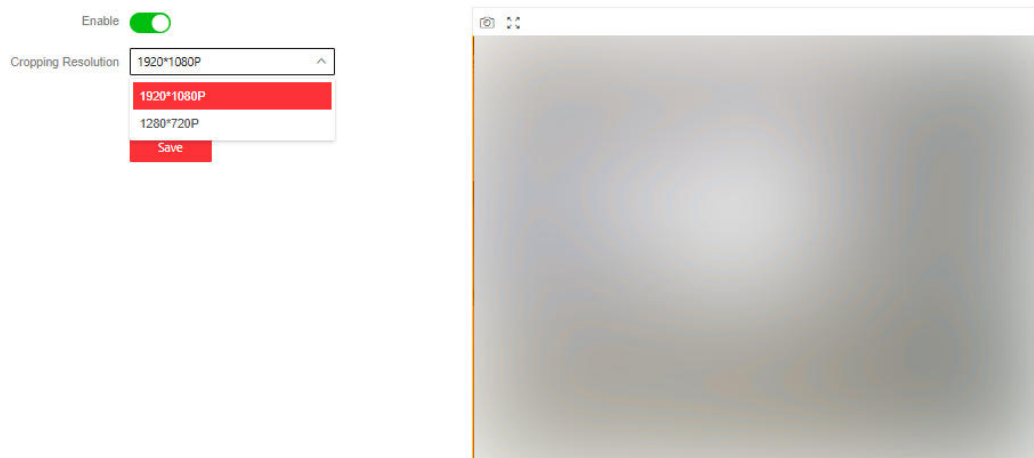


3. You can also choose **Time Format** and **Date Format** according to your actual needs.

Target Cropping

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **Target Cropping** .
2. Slide to enable this function.



3. Select a **Select a Cropping Resolution..**

Note

Cropping resolution is the main stream resolution after target cropping.

4. Click **Save**.

Note

Some models support target cropping. Refer to the actual device for details.

This function is mutually exclusive with some functions. After enabling target cropping, some functions will fail. Refer to the actual device for details.

6.7.12 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 **System and Maintenance** → **System Configuration** → **Event** → **Event Detection** → **Motion** .

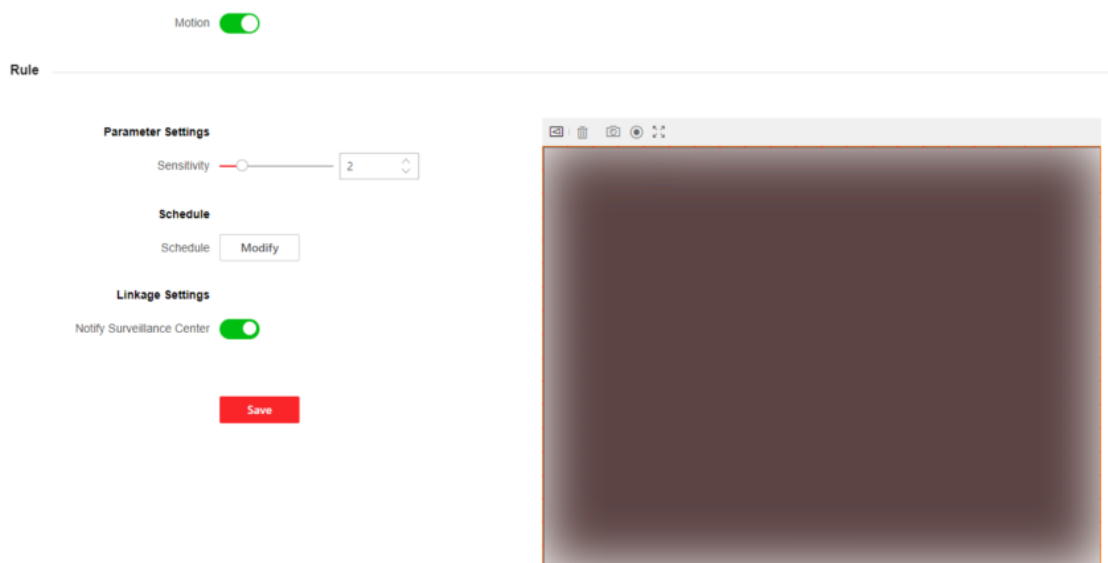


Figure 6-12 Motion Detection

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 6-13 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.

6.7.13 Access Control Settings

Set Access Schedule

You can name and add new access template on this page.

Steps

1. Click **Access Control** → **Time Schedule** → **Access Schedule** to enter this page.

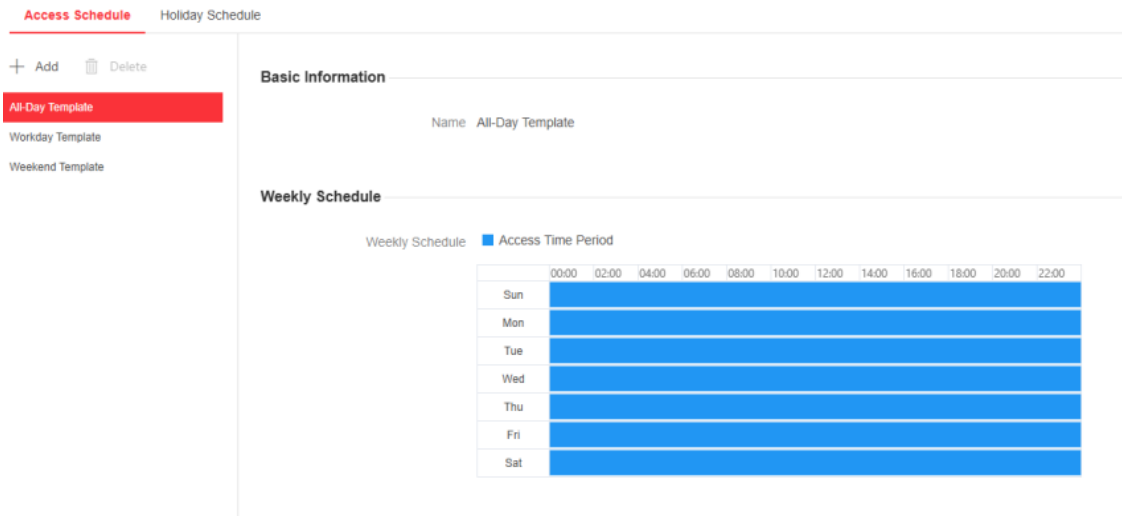


Figure 6-14 Access Schedule

2. Click **+Add**. Then you can edit the name of the schedule.
3. Drag cursor on corresponding timestamp to map valid access period.
4. You can also click **Quick Operation** to apply existing template.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save** to save your settings.

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Access control** → **Time Schedule** → **Holiday Schedule** → **+Add** .



Figure 6-15 Holiday Schedule Template

2. Enter holiday name in the right column.
3. Set Start Date and End Date.
4. Drag cursor on corresponding timestamp to map valid holiday period.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save**.

Set Door Parameters

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

Door No.

*Door Name

Open Duration s

Relay Reverse Open Disable

Figure 6-16 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.

Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Click **Access Control** → **Privacy Settings** to enter this page.

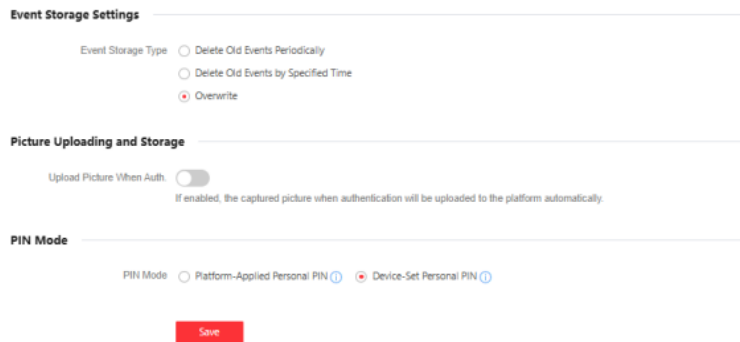


Figure 6-17 Privacy Settings

Upload Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform. Tap **Save** to complete the 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.

Card Settings

Choose card types to enable.

Go to **Access Control** → **Access Control** → **Card Settings** .

Slide to enable card types and click **Save** to save the settings.

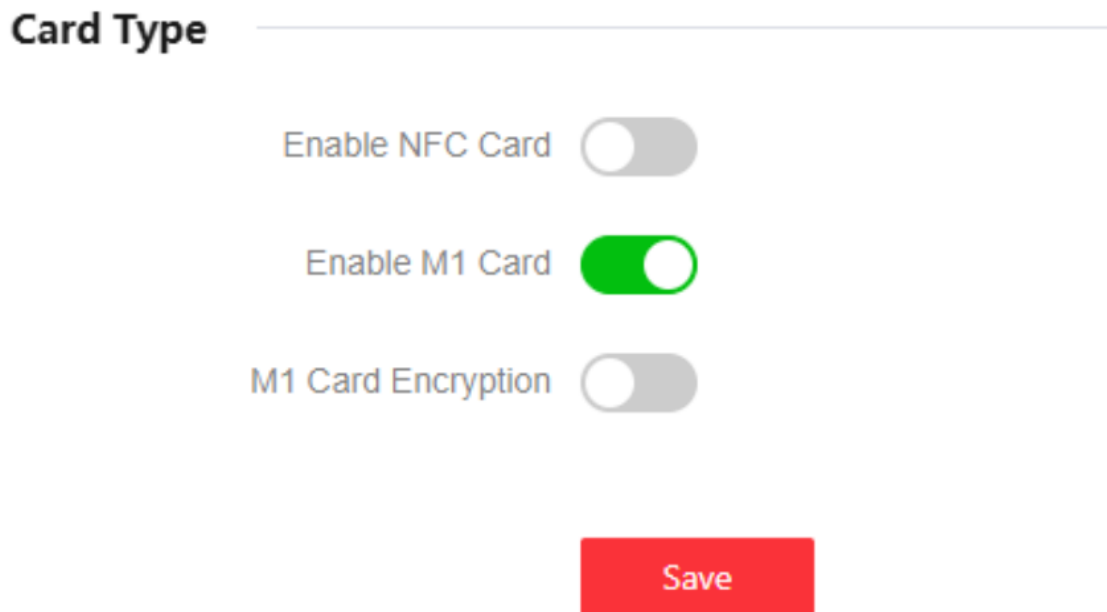


Figure 6-18 Card Type

Enable M1 Card

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

Note

The function of Enable M1 Card is enabled by default.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Enable NFC Card

If enabled, the device will actively detect and process communication requests from NFC cards.

6.7.14 Video Intercom Settings

Device No. Settings

Steps

1. Click **Video 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 6-19 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.

Registration Password: []

Main Station IP: 0.0.0.0

Private Server IP: 0.0.0.0

Enable Protocol 1.0:

Save

Figure 6-20 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 **Video Intercom** → **Call Parameters** → **Call Settings** .

The screenshot shows a web interface for 'Call Settings'. It contains two input fields. The first is labeled 'Max. Communication Time' and has the value '90' with a small 's' and up/down arrows to its right. The second is labeled 'Max. Message Duration' and has the value '30' with a small 's' and up/down arrows to its right. Below these fields is a red rectangular button with the word 'Save' in white text.

Figure 6-21 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 **Video Intercom** → **Call Parameters** → **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.

Call Priority

Steps

1. Click **Video Intercom** → **Call Parameters** → **Call Priority** to enter the settings page.

Call Priority	Call Type	Ring Duration
Priority1	<input checked="" type="checkbox"/> Platform <input checked="" type="checkbox"/> Indoor Station <input type="checkbox"/> Telephone Gateway	60 <input type="text"/>
Priority2	<input type="checkbox"/> Platform <input type="checkbox"/> Indoor Station <input checked="" type="checkbox"/> Telephone Gateway	60 <input type="text"/>
Priority3	<input type="checkbox"/> Platform <input type="checkbox"/> Indoor Station <input type="checkbox"/> Telephone Gateway	60 <input type="text"/>

The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Save

Figure 6-22 Call Priority

2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.

Note

The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Press Button to Call

Steps

1. Click **Video Intercom** → **Call Parameters** → **Press Button to Call** to enter the settings page.
2. Fill in the room No. of the indoor station in the blank of the Button Setting column.
3. Link Time Schedule: Select time schedule plan from the drop-down list. For more information about the time schedule plan,
4. Click **Save** to enable the settings.

Number Settings

Link the room No. and SIP numbers.

Click **Video Intercom** → **Call Parameters** → **Number Settings** to enter the page.



Figure 6-23 Number Settings

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

6.8 Maintenance and Security

6.8.1 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 **System and Maintenance** → **Maintenance** → **Protocol Testing** .

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

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

6.8.2 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 be displayed in **PING Result**.

6.8.3 Upgrade and Maintenance

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


Reboot Device

Click **System and Maintenance** → **Maintenance** → **Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **System and Maintenance** → **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 Guarding Vision and network, when there is a new installation package in Guarding Vision, you can click **Upgrade** after Online Update to upgrade the device system.




Note

Do not power off during the upgrading.

Sub Device Upgrade

Click **System and Maintenance** → **Maintenance** → **Upgrade** .

Set Upgrade Settings as **RS-485 Card Reader**, and select a card reader.

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

Restore Parameters

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

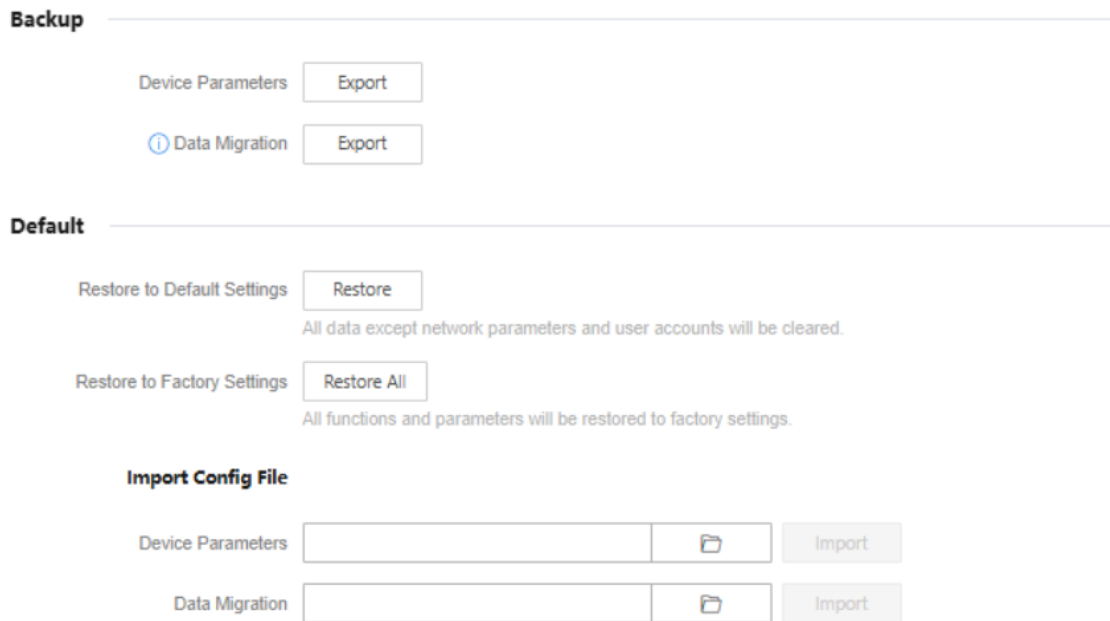


Figure 6-24 Back up and Reset

Device Parameters

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

Note

You can import the exported device parameters to another device.

Data Migration

Click **Export** to migrate user information and configuration details to other devices.

The information and data include door station configuration data, advertisement information, ringtone and etc.

Import

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

6.8.4 Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance** → **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 click **Export** to export log.

Capture Network Packet

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

6.8.5 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance** → **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.

6.8.6 Certificate Management

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



Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

1. Go to **System and Maintenance** → **Safe** → **Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

The created certificate is displayed in the **Certificate Details** area.

The certificate will be saved automatically.

6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
 - 1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.

- 2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import CA Certificate** 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 7 Configuration via Client Software

7.1 Device Management

Device management includes device activation, adding device, editing device, and deleting device, and so on.

After running the Guarding Vision, video intercom devices should be added to the client software for remote configuration and management.

7.1.1 Add Online Device

Before You Start

Make sure the device to be added is in the same subnet with your computer. Otherwise, please edit network parameters first.

Steps

1. Click **Online Device** to select an active online device.
2. Click **Add**.
3. Enter corresponding information, and click **Add**.

7.1.2 Add Device by IP Address

Steps

1. Click **+Add** to pop up the adding devices dialog box.
2. Select **IP/Domain** as **Adding Mode**.
3. Enter corresponding information.
4. Click **Add**.

7.1.3 Add Device by IP Segment

You can add many devices at once whose IP addresses are among the IP segment.

Steps


1. Click **+Add** to pop up the dialog box.
2. Select **IP Segment** as **Adding Mode**.
3. Enter corresponding information, and click **Add**.

7.2 Live View via Door Station

Steps

1. On the main page of the client software, click **Main View** to enter the Live View page.
2. In the left list of the window, double-click the device IP or click the play icon to live view.
3. **Optional:** On the Live View page, control-click and select **Capture** to get the picture of the live view.

7.3 Organization Management

On the main page of the Client Software, click  **PersonalManagement** to enter the configuration page.

7.3.1 Add Organization


Steps

1. In the organization list on the left, click **+Add**.
2. Enter the **Organization Name** as desired.
3. Click **OK** to save the adding.
4. **Optional:** 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) Then the added organization will be the sub-organization of the upper-level organization.

Note

Up to 10 levels of organizations can be created.

7.3.2 Modify and Delete Organization

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

You can select an organization, and click **X** 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.
-

7.4 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 2,000 persons can be added.
 - Up to 5 cards can be added to each person.
-

7.4.1 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 editable.

2. Set basic person information.

- 1) Enter basic information: name, tel, birthday details, effective period and email address.
-

Note

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

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

Note

The picture should be in *.jpg format.

Click Upload Select the person picture from the local PC to upload it to the client.

Click Take Phone Take the person's photo with the PC camera.

Click Remote Collection Take the person's photo with the collection device.

3. Issue the card for the person.

- 1) Click **Credential** → **Card** .
- 2) Click **+** to pop up the Add Card dialog.
- 3) Select **Normal Card** as **Card Type**.
- 4) Enter the **Card No.**
- 5) Click **Read** and the card(s) will be issued to the person.

4. Link the device to the person.

- 1) Set the linked devices.
-

Linked Device

You can bind the indoor station to the person.



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.

- 2) Click **OK** to save the settings.
5. Click **Add** to save the settings.

7.4.2 Modify and Delete Person

Select the person and click **Edit** to open the editing person dialog.

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



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

7.4.3 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.

7.4.4 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.
 - 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**.
- 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.

7.4.5 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 from Device** to pop up the dialog box.
 3. The added device will be displayed.
 4. Click to select the device and then click **Get** to start getting the person information from the device.
-

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.
-

7.4.6 Issue Card in Batch

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

Steps

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

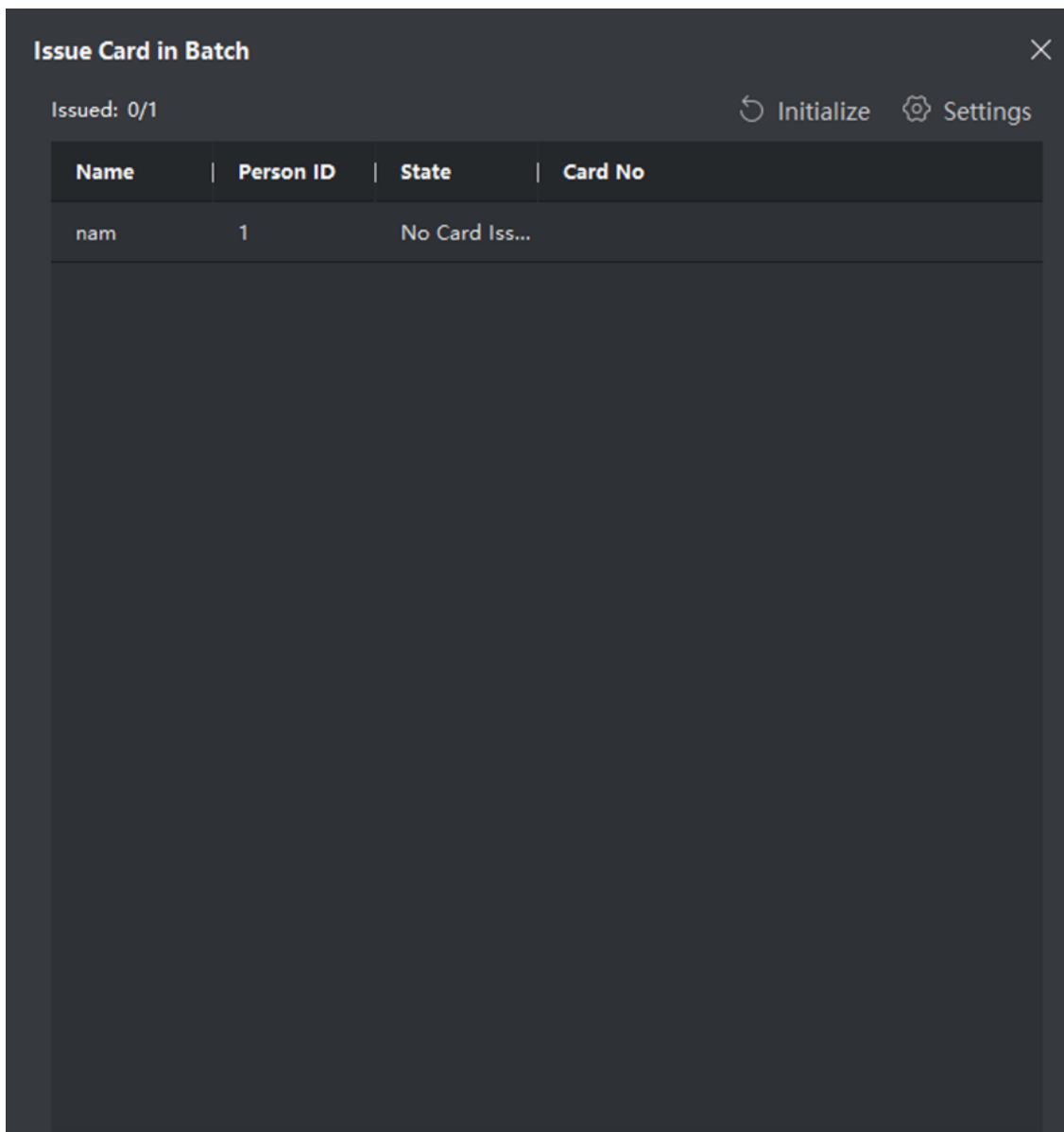


Figure 7-1 Issue Card in Batch

2. Click **Settings**.

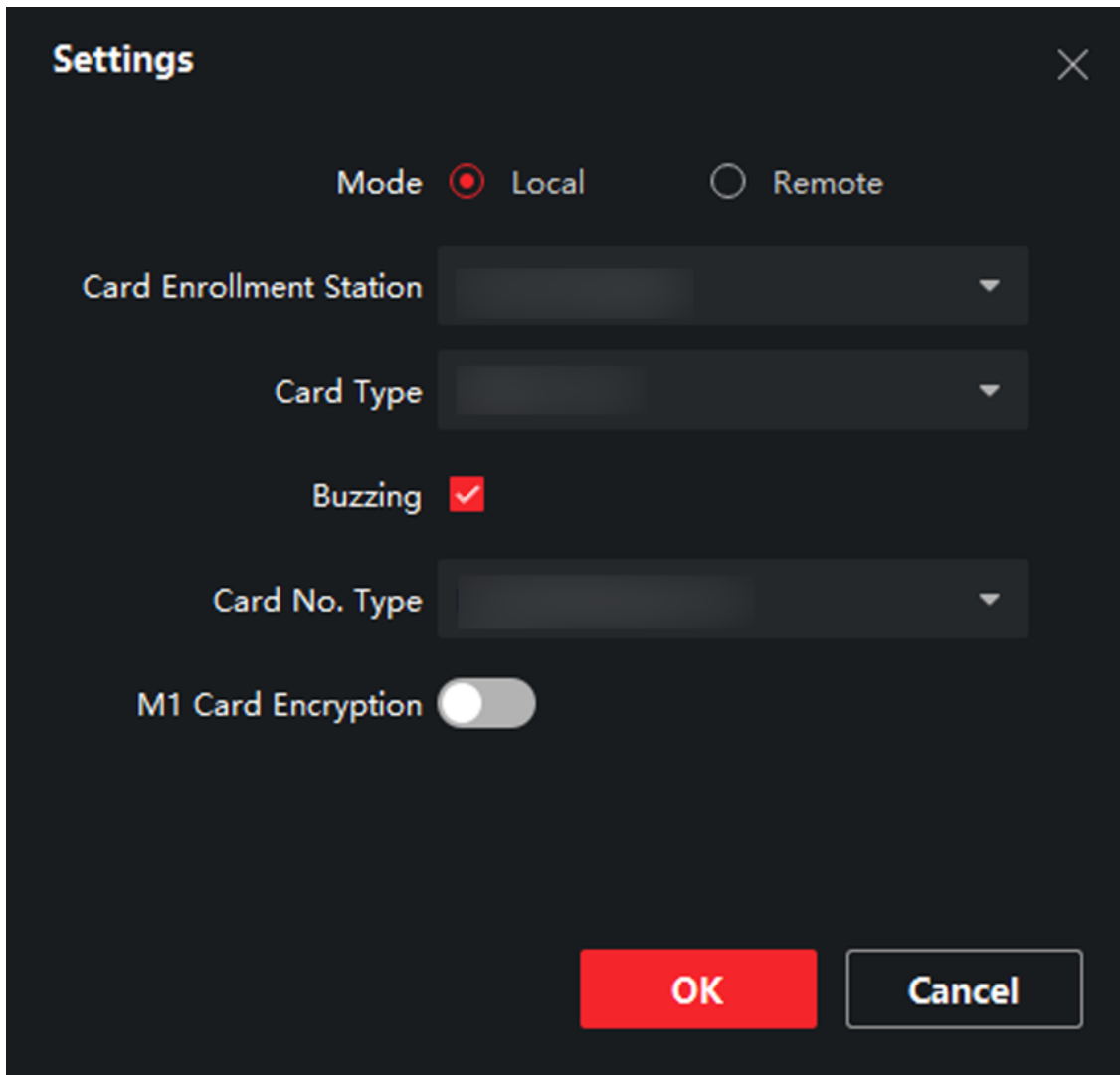


Figure 7-2 Card Settings

3. Select **Card Type** and **Card No. Type**.
4. Click **OK** to save the settings.

Result

After issuing the card to the person, the person and card information will display in the Person(s) with Card Issued list.


7.5 Video Intercom Settings

The Video Intercom Management module provides the function of video intercom, checking call logs and managing notice via the Guarding Vision 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.


On the main page, click  **AccessControlInfo** → **Video Intercom** → **Video Intercom** on the left bar to enter the Video Intercom page.

7.5.1 Receive Call from Door Station

Steps

1. Select the client software in the page to start calling the client and an incoming call dialog will pop up in the client software.
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 **Hang Up** to hang up.

Adjust the Volume of Microphone

Click  to adjust the volume of 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 Guarding Vision can be set from 120s to 600s via the Remote Configuration of indoor station.
 - The maximum speaking duration between door station and Guarding Vision can be set from 90s to 120s via the Remote Configuration of door station.
-

7.5.2 Release Notice

You can create different types of notices and send them to the residents. Four notice types are available, including Advertising, Property, Alarm and Notice Information.

Before You Start

Make sure the person has been added to the client.

Steps

1. On the video intercom settings page, click **Notice** to enter the page.
2. Click **+Add** to pop up the adding dialog box.
3. Select the person according to your needs.
4. Edit the **Subject, Type** and **Information**.
5. Click **View** to select the picture.
6. Click **Send**.



Note

- Up to 63 characters are allowed in the Subject field.
 - Up to 6 pictures in the JPGE format can be added to one notice. And the maximum size of one picture is 512KB.
 - Up to 1023 characters are allowed in the Information field.
-

7.5.3 Search Video Intercom Information

Search Call Logs

Steps

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

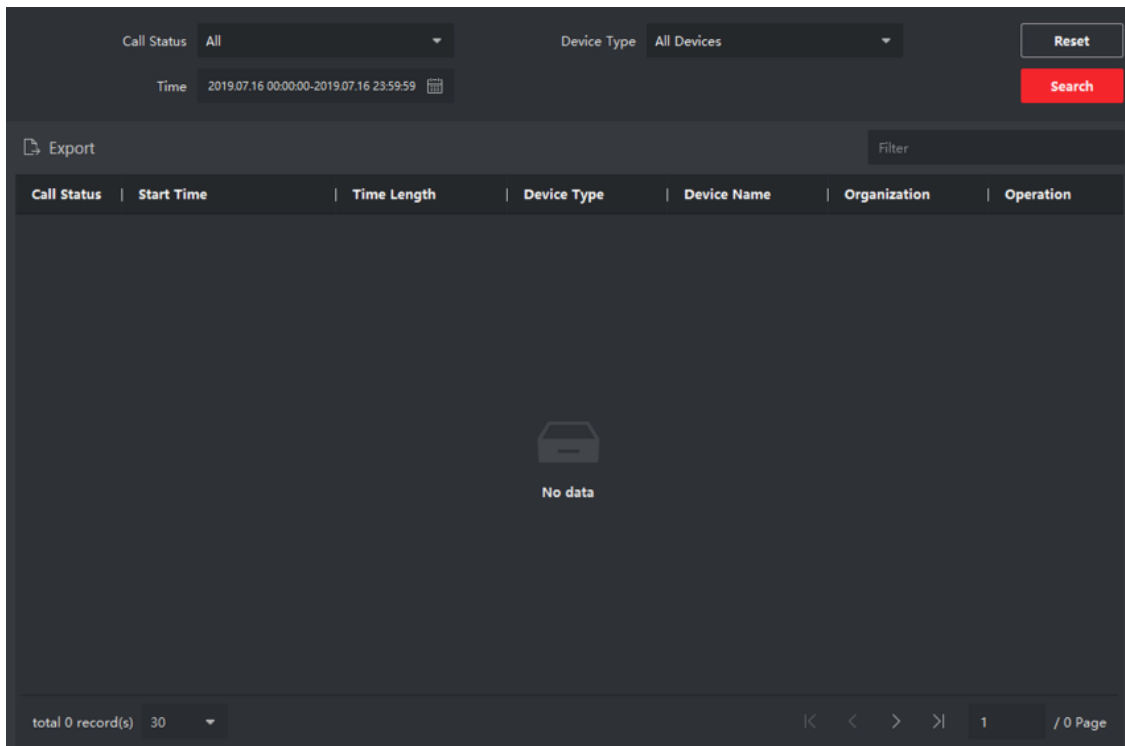


Figure 7-3 Search Call Logs

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 the time icon 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 Notice

Steps

1. On the Video Intercom page, click **Notice** to enter the page.
2. Set the search conditions, including notice type, start time and end time.

Type

Select **Advertising Information, Property Information, Alarm Information** or **Notice Information** as **Type** according to your needs.

Start Time/End Time


Click the time icon 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 the matched notice will display on this page.
4. **Optional:** Click **Export** to export the notices to your PC.

7.5.4 Upload Armed Information

Steps

1. On the main page, click upper right  → **Tool** → **DeviceGuard** to enter the page.
2. Enable to arm or disarm the device.

Note

- While device has been added to the client software, the device armed by default.
- When the device is armed, the alarm logs upload to the client software automatically.
- Click **Alarm Application** → **Event Search** to search the alarm logs.

-
3. **Optional:** Click **Arm All** or **Disarm All** to arm or disarm all the device.

Chapter 8 Video Intercom Operation

8.1 Call Resident

You can press the call button of the door station to call resident.



Note

- Make sure you have added contacts to the device.
 - Make sure you have configured the room No. for the call button. For more details, please refer to: **Press Button to Call**
-

8.2 Unlock Door

After issuing card, you can swipe card on the card reading area to unlock the door.

You can swipe card on the card reading area to unlock the door.



Note

Make sure you have issued cards for the device.

- Issue card via Client Software:
 - **Add Person**
 - **Issue Card in Batch**
 - Issue card via web client:
-

