



Control Panel

User Manual

Contents

Chapter 1 Unboxing Video	1
Chapter 2 Appearance	2
2.1 Packing List	2
2.2 Components Introduction	2
Chapter 3 Start Up	4
3.1 Download and Login the App	4
3.2 Activation	4
3.2.1 Activation with Wi-Fi	4
3.2.2 Activation with SIM	6
3.2.3 Activation with Ethernet	7
3.3 Unbind the Device	8
3.3.1 Unbind the Device from Your Own Account	8
3.3.2 Unbind the Device from Another Account	9
Chapter 4 Installation	11
4.1 Precaution	11
4.2 Installation	11
4.3 Installation FAQ	12
Chapter 5 Configuration	14
5.1 Set-up with App	14
5.1.1 Add Control Panel to the App	14
5.1.2 Add Peripheral to the Control Panel	14
5.1.3 Installation Wizard	15
5.1.4 Main Page	15
5.1.5 Area Management	16
5.1.6 User Management	17
5.1.7 System Settings	19

Control Panel User Manual

5.1.8 Network	20
5.1.9 Device Maintenance	22
5.1.10 Check Alarm Notification	22
Chapter 6 General Operations	23
6.1 Arming	23
6.2 Disarming	24
6.3 SMS Control	24
Chapter 7 Appendix	25
7.1 Specifications	25
7.2 Trouble Shooting	27
7.2.1 Communication Fault	27
7.2.2 Problems While Arming	28
7.3 Access Levels	28
7.4 Signaling	28
7.5 SIA and CID Code	30
7.6 User Privacy Statement	30
7.7 Legal Information	31
7.8 Symbol Conventions	32

Chapter 1 Unboxing Video

Watch the video to get the device general information.

Refer to the video for details:

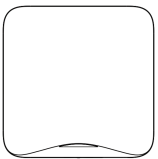
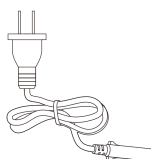

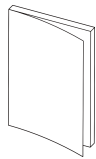
Refer to the link to see the high-definition video: <https://enpinfodata.hikvision.com/analysisQR/showQR/b722d26f>

Chapter 2 Appearance

2.1 Packing List

Unbox and check device and accessories.

Table 2-1 Packing List

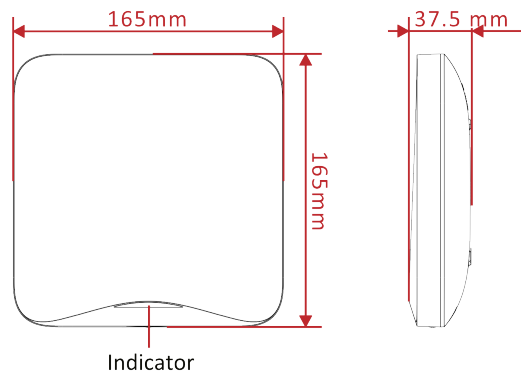
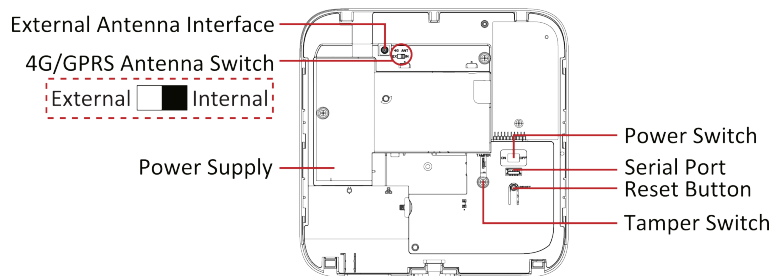
Control Panel	Power Adapter	Screws	Quick Start Guide
			

2.2 Components Introduction

Check components location and name for further use.

 **Note**

- Structures may differ in different models, please refer to the actual product.



Indicator Status	Control Panel Status
Solid Green	Powered on (station mode)
Flashing Green	AP Mode
Solid White	Connected to the cloud
Flashing white once, and flashing green twice	Unbinding Mode
Flashing white rapidly	Reset

Chapter 3 Start Up

3.1 Download and Login the App

Download the App and login the client before operating the control panel.

Steps

1. Scan the QR code below to download the App.



Figure 3-1 App QR Code

2. Register a new account if it is the first time you use the App.



Note

For details, see the user manual of the App.

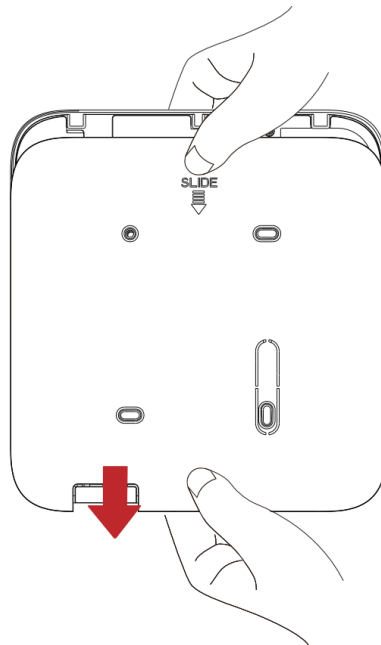
3. Run and login the App.


3.2 Activation

3.2.1 Activation with Wi-Fi

Steps

1. Slide to remove the rear cover.

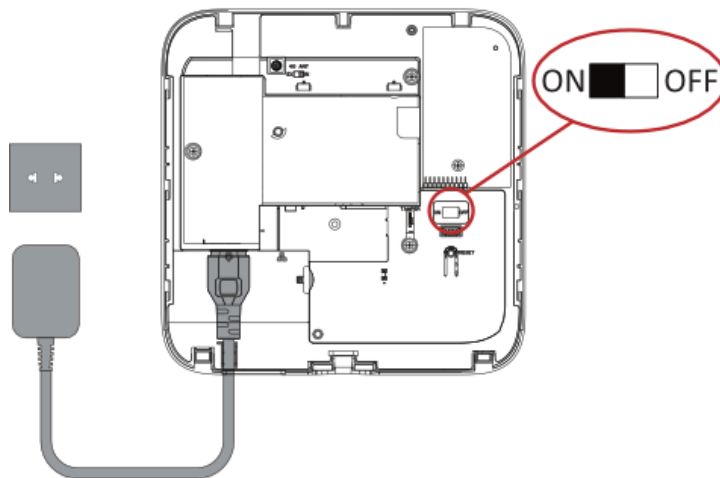


2. Open the App, tap  → **Scan QR Code** . Scan the QR code of the control panel. Or tap **Add Device Manually** and enter the serial No.

 **Note**

Make sure your phone is connected to your home Wi-Fi.

3. Connect to the power supply and turn on the power switch. After powered on, the green indicator flashes.

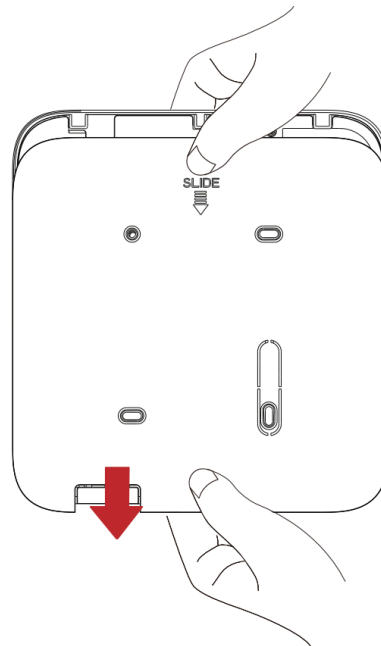


4. Operate according to the App prompts. Wait for the device to log in the cloud. The white indicator will remain on.

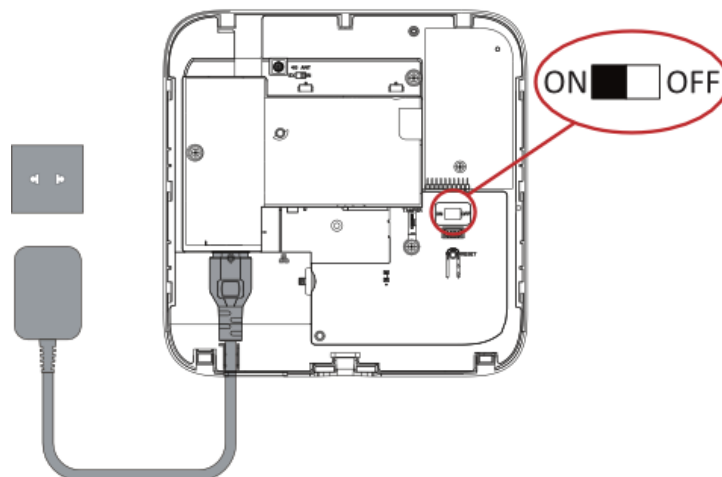
3.2.2 Activation with SIM

Steps

1. Slide to remove the rear cover.



2. Open the App, tap **+** → **Scan QR Code** . Scan the QR code of the control panel. Or tap **Add Device Manually** and enter the serial No.
3. Insert SIM card.
4. Connect to the power supply and turn on the power switch.

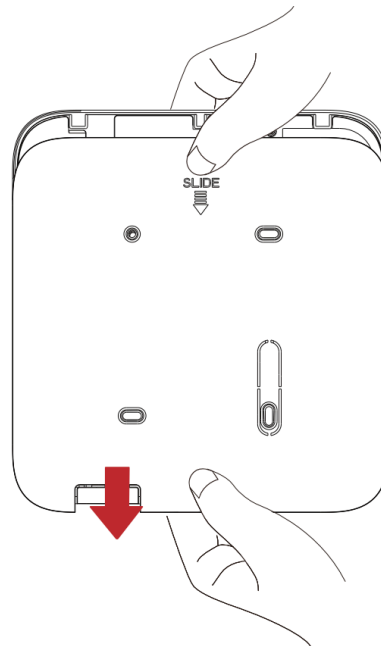


5. Wait for the device to log in the cloud. The white indicator will remain on.

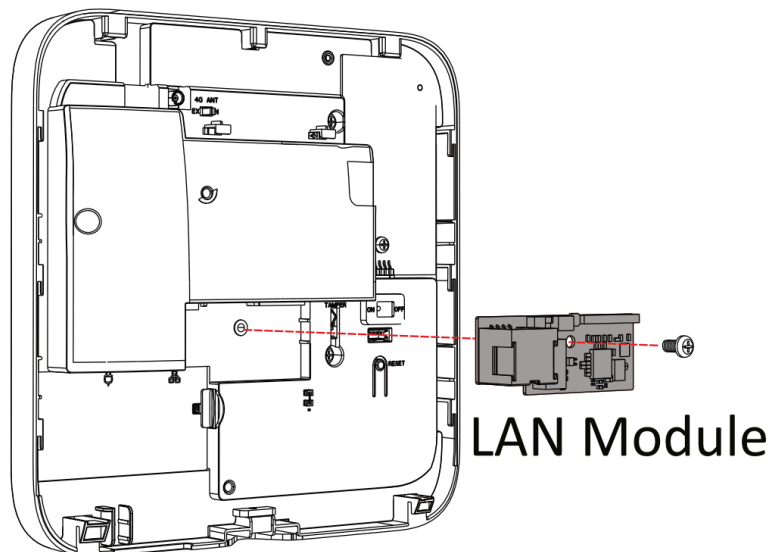
3.2.3 Activation with Ethernet

Steps

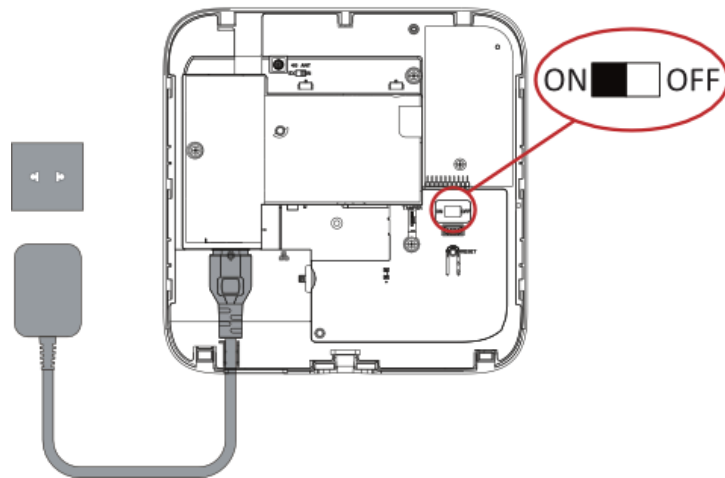
1. Slide to remove the rear cover.



2. Open the App, tap **+** → **Scan QR Code** . Scan the QR code of the control panel. Or tap **Add Device Manually** and enter the serial No.
3. Install the LAN module (sold separately), and connect the device to Ethernet with LAN.



4. Connect to the power supply and turn on the power switch.



5. Wait for the device to log in the cloud. The white indicator will remain on.

3.3 Unbind the Device

3.3.1 Unbind the Device from Your Own Account

When the device is bound to your own account, you can delete it directly.

Steps

1. On the home page, tap ... → **Settings** to enter the page.
2. Tap **Delete Device**.

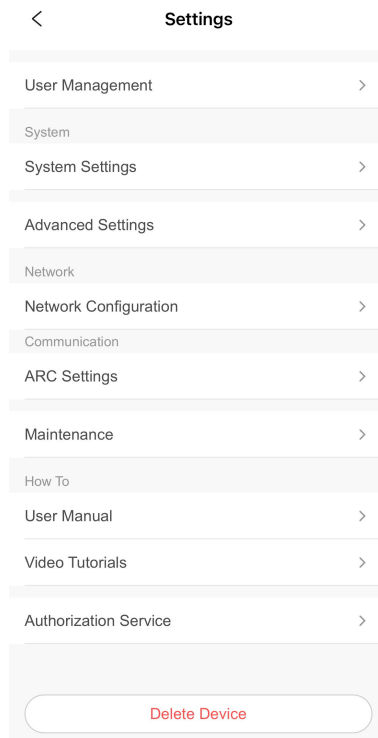


Figure 3-2 Delete Device

3.3.2 Unbind the Device from Another Account

Make sure the control panel is in your hands. The phone and device are on the same network segment.

Steps

1. Open the App, tap  → Scan QR Code .

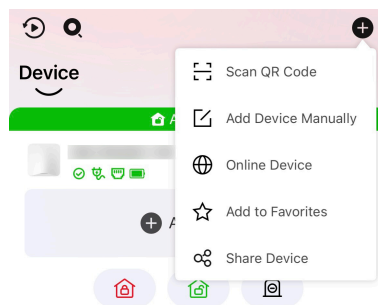


Figure 3-3 Add Device

2. Scan the QR code of the control panel. The page will prompt that the device has been added by another account.
3. Tap **Unbind Device**.

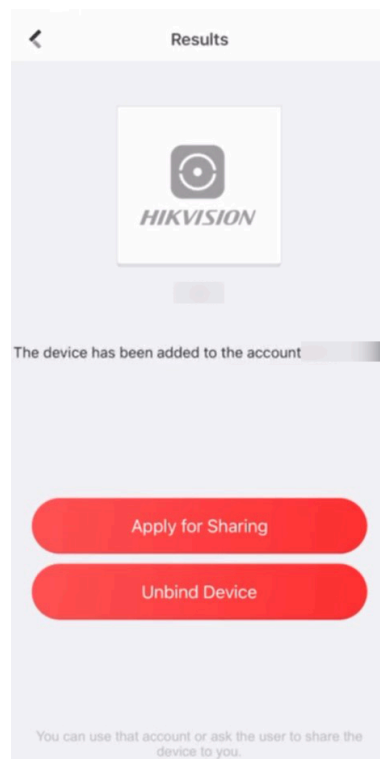


Figure 3-4 Unbind Device

4. Press and hold the reset button for more than 10 s.

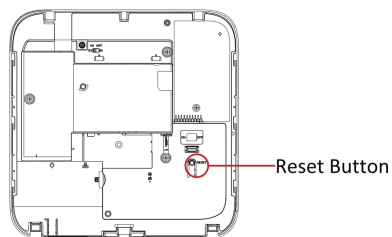


Figure 3-5 Reset Button

5. Check **Device Unbound**, and tap **Add Again** to add the device to your own account.

Chapter 4 Installation

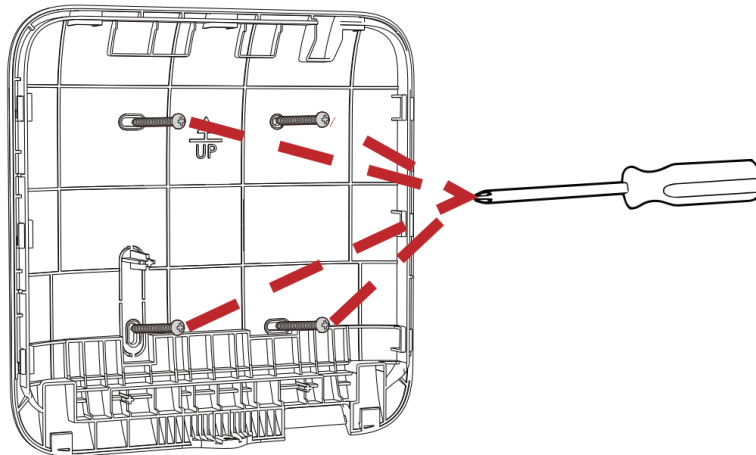
4.1 Precaution

1. Avoid installing the device on metal surfaces.
2. Avoid placing the device directly on the ground.
3. The device is not allowed to be wrapped in metal.
4. Avoid obstructions within 50 cm around the device, except for the installation surface.
5. Check the signal strength before installation and install the control panel according to the App prompts.
6. Vertical installation is recommended for devices.

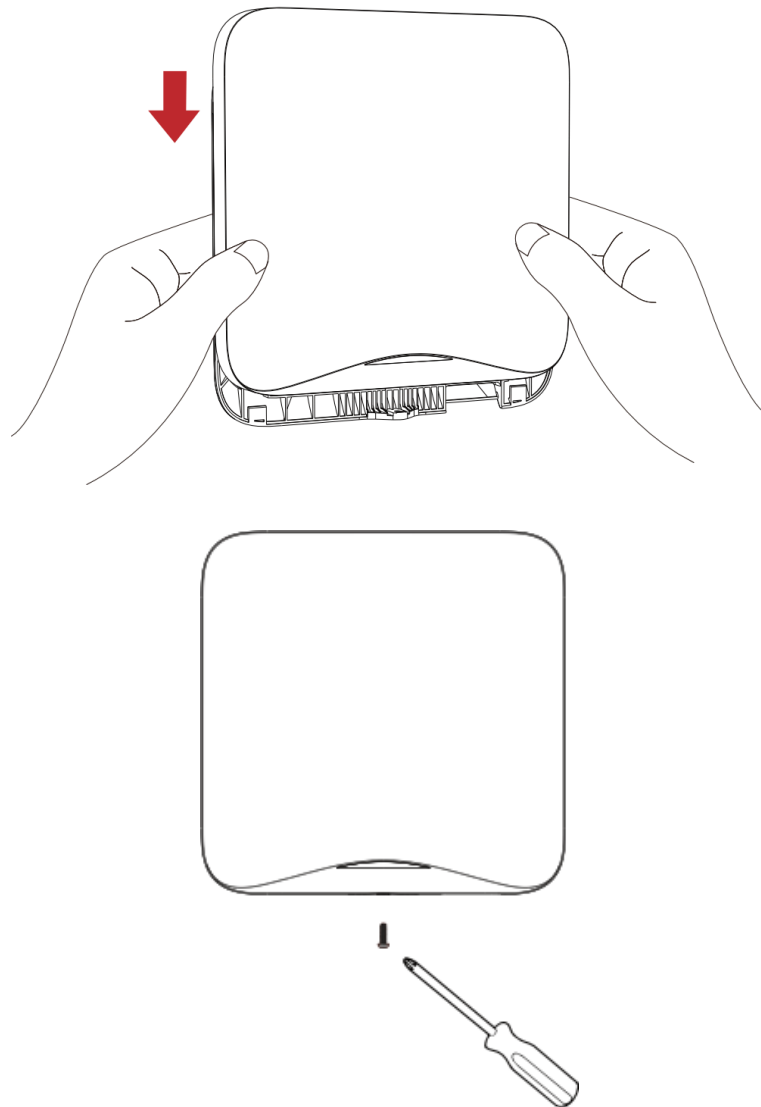
4.2 Installation

Steps

1. Break through the screw hole.
2. Fix the rear cover to the wall with 4 screws (4_KA3×25).



3. Install the front cover, and fix with the screw (sc-pb3×6-sus).



4.3 Installation FAQ

Question 1: Why is the signal normal during installation, but worse in actual use?

Answer: Check whether the working environment changes during installation and actual use. Such as obstruction caused by closed doors and windows.

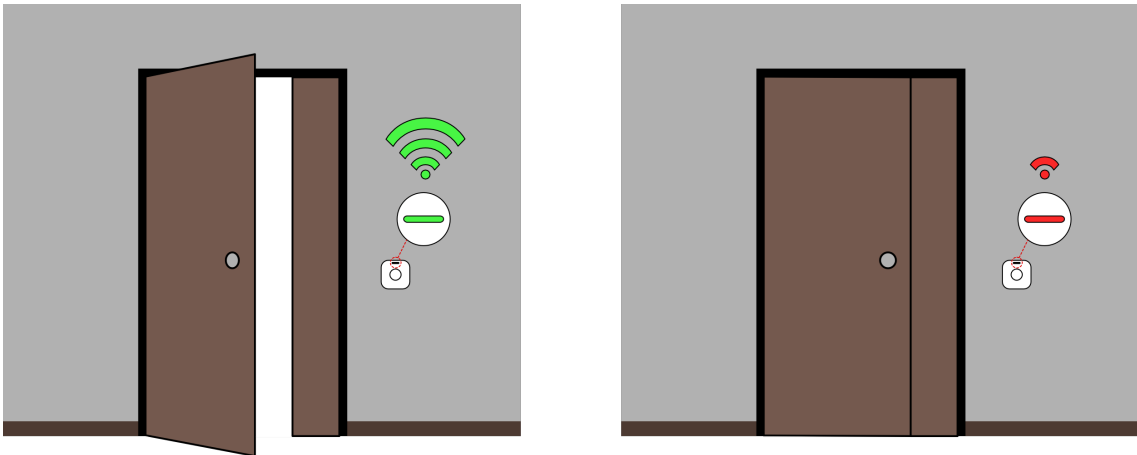


Figure 4-1 Installation FAQ

Question 2: After the installation is complete, the peripheral is offline.

Answer:

- Adjust the position of the control panel and check whether the signal strength is suitable for installation.
- Check whether to install devices according to the precautions.

Chapter 5 Configuration

5.1 Set-up with App

The operator can use the App to control the device, such as general arming/disarming operation, and user management etc.

5.1.1 Add Control Panel to the App

Add a control panel to the App before other operations.

Before You Start


The control panel has been activated.

Steps

1. Power on the control panel.
2. If you select adding method as **Scan QR Code**, Scan the QR code on the control panel.



Normally, the QR code is printed on the label stuck on the back cover of the control panel.

3. If you select adding method as **Add Device Manually**, enter the device information manually.
 - 1) Enter the device serial No. with the Hik-Connect Domain adding type.
 - 2) Tap  to search the device.
 - 3) Tap **Add** on the Results page.
 - 4) Enter the verification code and tap **OK**.
 - 5) After adding completed, enter the device alias and tap **Save**.

5.1.2 Add Peripheral to the Control Panel

Before You Start

Make sure the control panel is disarmed.

Steps

1. On the home page, tap the control panel to enter the Area page.
2. Tap **Device** → **Add Device** .
3. Select adding method.
 - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the control panel.



The QR code is usually on the back cover of the device.

- Tap **Batch Add** to enter the enrollment mode. Powered on peripherals nearby will be enrolled to the control panel automatically. Tap **Finish**.

5.1.3 Installation Wizard

You can test the installation environment for devices.

Steps

1. On the home page, tap ... → **Settings** → **Maintenance** → **Installation Wizard** to enter the page.
2. Tap + to enroll more peripherals.
3. Tap 🗑️ to delete enrolled peripherals.
4. Tap **Start Installation**, it will test the signal of control panel.
5. When the control panel is ready for installation, tap **Next**. Edit device name and language, and tap **OK**.
6. Tap peripherals in the list, check the installation environment and edit basic information.
7. Tap **Exit** to exit the installation mode.
8. Tap **Finish** to complete installation test.

5.1.4 Main Page

You can add shortcut, arm and disarm areas, view device status, etc.

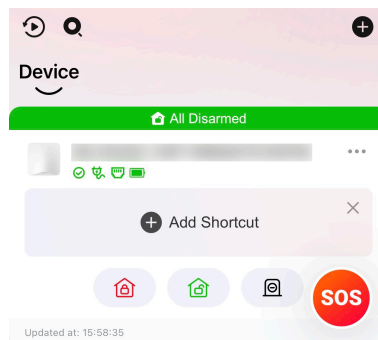


Figure 5-1 Main Page

Status

You can view the device status on the device list page.

Tap control panel, and tap **Device** to enter the device page. Tap control panel or peripherals to view detailed device status.

Shortcut


On the home page, tap **Add Shortcut** or tap ... → **Add Shortcut**.

Select area or device, and tap **Add**. The area or device will be shown on the device list page, you can operate the area or device quickly.


After adding, tap ... → **Manage Shortcuts** to view added shortcuts. Tap 🗑️ to delete the added shortcut. Tap + to add more shortcuts. Drag the icons to adjust the orders of added shortcuts.

Arming / Disarming / Silence Alarm

Arming

Tap  to arm the area. When someone intrudes into the detection area, the control panel will trigger alarm, and the system will upload alarm information.

Disarming



Tap  to disarm the area. When someone intrudes into the detection area, the system will not upload alarm information.

Silence Alarm

Tap  to mute alarms but the system will upload alarm information.

Panic Alarm

On the device list page, tap  to enter the Panic Alarm page.

Tap  , the device will emit the alarm sound. Tap  , the alarm sound will be muted.

5.1.5 Area Management

You can add new area, edit area information, link devices, etc.

Steps

1. On the home page, tap control panel to enter the Area page.

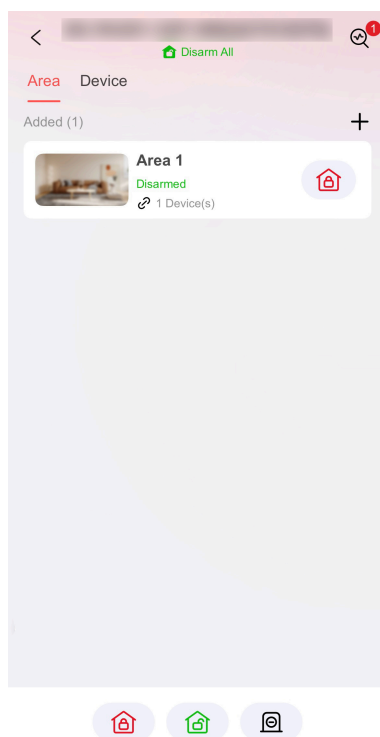




Figure 5-2 Area Management

2. Tap **+**, enter area name, and tap **OK**.
3. Tap  to set the area image.
4. Tap **Link to More Devices**, select devices and tap **OK**.
5. Tap **Area Details** and slide to enable **Add to Home Shortcut**, the area will be shown on the device list page.
6. Tap  to delete the area.

5.1.6 User Management

Add/Edit/Delete Users

The administrator and the installers can manage users. If you are the administrator, you can add, edit, and delete users, and assign different permissions to the newly-added users.

Steps

1. On the home page, tap **...** → **Settings** → **User Management** to enter the page.
2. Tap **Add**.
3. Enter **User Name** and **Phone Number**.
4. Select **User Property**.

Permanent

The user is permanently valid.

Valid Time Period

You can set the start date, start time, end date and end time. The user is only valid during the configured time period.

One-time User

The user's arming and disarming operation is only valid once.

5. Enter **Keypad Password** and **Duress Password**.
-



The keypad password +1 is the duress code. Use the duress code can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123457. If the keypad password is 123459, the duress code is 123450.

6. Select the linked area for the user.
7. Tap **Next**.
8. Set notification parameters, and tap **OK** to finish adding.

Push Notifications / SMS Notifications / Phone Call

When the enabled events occur, you can receive corresponding notification push, SMS messages or call.


Arm/Disarm Permission

Select areas to enable arm or disarm function.

9. Tap a user to edit the parameters.
-



Configuration items and user permission will vary according to the user type.

10. Tap a user and tap  to delete the user.
-



Admin, installer and manufacturer can not be deleted.

Keyfob Management

After adding keyfobs to the control panel, you can press keys to arm or disarm all the detectors added to specific area(s) of the control panel, and silence alarms.

Steps

1. On the home page, tap **...** → **Settings** → **User Management** to enter the page.
2. Tap a user to enter the configuration page.
3. Tap **Keyfob** → **Add**, scan the QR code of the keyfob or enter the serial No. and select type.
4. Tap a keyfob to edit the parameters.

Name

Edit device name.

User

Select linked user.

I/II Key

Select the function of configurable keys.

Deactivation

The selected part will be deactivated.

5. Optional: Tap **Delete** to delete the keyfob.

5.1.7 System Settings

System Settings

You can change language and select time zone.

Steps

1. On the home page, tap ... → **Settings** → **System Settings** to enter the page.
2. Select device language and time zone.
3. Tap **DST** and slide to enable. Set the start, end time and bias time for daylight saving time, and tap **OK**.

Advanced Settings

On the device list page, tap ... → **Settings** → **Advanced Settings** to enter the page.

Panel LED Display

Enable/Disable panel functional LED.

Fault Prompt on Arming

When the enabled faults occur on arming, you can receive prompts.

Panel-Server Polling Interval

The system will transfer information to the cloud every configured time.

Delay of Server Connection Failure

When the server connection failure occurs, the system will report fault after the configured time.

Panel Fault Check

The system will check the fault that is enabled after the configured time duration.

Tap **Save**.

5.1.8 Network


Wired Network

Steps

1. On the home page, tap ... → **Settings** → **Network Configuration** → **TCP/IP** to enter the page.
2. Set the parameters.
 - Automatic Settings: Enable **DHCP**.
 - Manual Settings: Disabled **DHCP** and set IP address, subnet mask, gateway address, DNS server address.
3. Tap **Save**.

Wi-Fi Configuration

Steps

1. On the home page, tap ... → **Settings** → **Network Configuration** → **Wi-Fi** to enter the page.
2. Tap a Wi-Fi in the list and tap **Connect** or **Disconnect**.
3. Tap  to refresh Wi-Fi list.
4. **Optional:** Tap **Manually Add Wi-Fi**, enter Wi-Fi name, password and select security mode. Tap **OK** to add the Wi-Fi to the list.

Cellular Data Network

Steps

1. On the home page, tap ... → **Settings** → **Network Configuration** → **Cellular Data Network** to enter the page.
2. Tap the SIM card, and slide to enable cellular network.
3. Set parameters.



You only need to set the parameter after changing the SIM card.

Access Number

Enter the number of the SIM card.

User Name / Password / APN / PIN

Ask the network carrier and enter the information.

Data Limit

Used Traffic This Month

The used data will be accumulated and displayed in this text box.

Traffic Threshold

Set the data threshold every month. If data usage is more than the configured threshold, an alarm will be triggered and uploaded to the alarm center and mobile client.

4. Tap **Network Test** to diagnose network connection.
5. Tap **Save**.

Alarm Receiving Center (ARC)

You can set the alarm receiving center's parameters and all alarms will be sent to the configured alarm center.

Steps

1. On the home page, tap ... → **Settings** → **ARC Settings** to enter the page.
2. Slide to enable the ARC and set parameters.

Protocol Type

Select as ADM-CID, SIA-DCS, *SIA-DCS, *ADM-CID or OTAP to set uploading mode.

Connection Mode

Select as TCP or UDP. UDP is recommended by the SIA DC-09 standard.

Communication Channel

Enable communication channels.

Address Type

Select as IP or domain name. Enter server address/domain name, port number and account code.

Polling Option

Enable and set the polling rate with the range from 10 to 3888000 seconds. The system will report fault if the time is over the limit. The status of device will be shown as offline.

Periodic Test

After enabling, you can set the time interval, setting how often to send a test event to the ARC to ensure the connection.

Retry Timeout Period

After the set time, the system will retry to connect to the cloud.

Push Notifications

Enabled events will trigger notifications.

GMT

Enable the Greenwich Mean Time.



3. Tap **Save**.

5.1.9 Device Maintenance

You can reboot, upgrade, test the device, etc.

Steps

1. On the home page, tap **...** → **Settings** → **Maintenance** to enter the page.
2. You can perform the following operations.

Operation	Description
Reboot Device	Tap Reboot Device to reboot the control panel.
<hr/>	
 Note	
It takes about 3 minutes to reboot the device.	
<hr/>	
Reset Device	Tap Reset Device → Reset Panel Partly , part of functions and parameters will be restored to factory default settings. Tap Reset Device → Reset Panel to Default , all functions and parameters will be restored to factory default settings.
Device Upgrade	Tap Device Upgrade to upgrade the control panel to the latest version.
Detector & Peripheral Upgrade	Tap Detector & Peripheral Upgrade → Upgrade to upgrade the peripherals to the latest version.
Walk Test	Tap Walk Test , slide to enable the function and view test results of different devices. Tap  to refresh test results.

5.1.10 Check Alarm Notification

When an alarm is triggered, and you will receive an alarm notification. You can check the alarm information from the mobile client.

Steps

1. Tap **Notifications** in the mobile client to enter the page.
All alarm notifications are listed in Notification page.
2. Tap an alarm and you can view the alarm details.

Chapter 6 General Operations

6.1 Arming

You can use keypad, keyfob, App to arm your system.

After the arming command is sending to control panel, the sytem will check the detector status. If the detector is in fault, you will need to choose whether to arm the system with fault.

While the system is armed, the control panel will prompt the result, and upload the arming report.

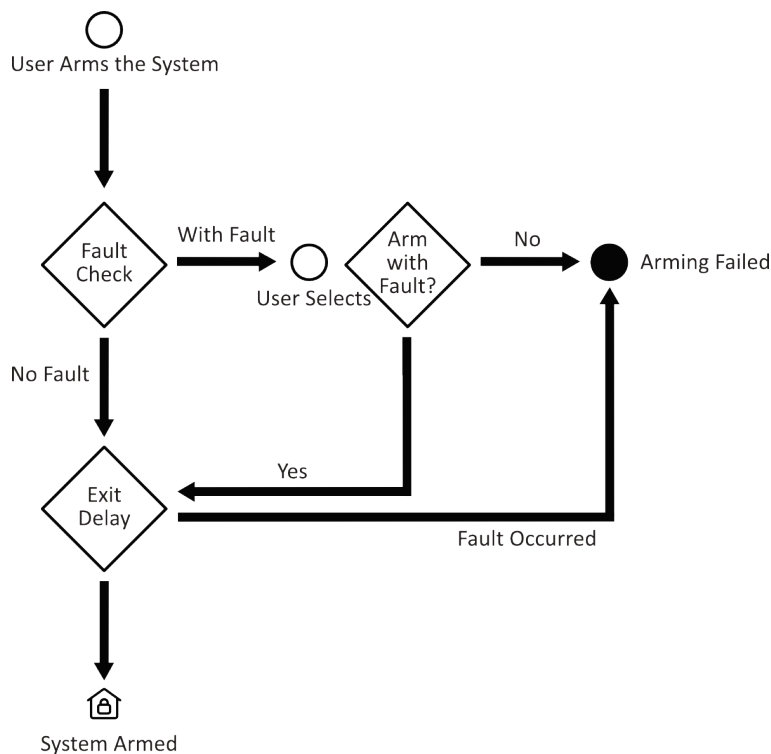


Figure 6-1 Arming Process

Access level of Arming

The user in level 2 or 3 has the permission to arm or partly arm the system.

Arming Indication

The arming/disarming indicator keeps solid blue for 5s.

Reason of Arming Failure

- Intrusion detector triggered (excepts the detector on the exit route).
- Panic alarm device triggered.
- Tampering alarm occurred.
- Communication exception

- Main power supply exception
- Backup battery exception
- Alarm receiving fault
- Sounder fault
- Low battery of the keyfob (when using keyfob to arm)
- Others

Arming with Fault

While the arming is stopped with fault, user in level 2 has the permission to arm the system with fault (forced arming).

Forced arming only takes effect on the current arming operation.

6.2 Disarming

You can disarm the system with keypad, keyfob, or App.

Disarming Indication

The system will report the disarming result after the operation completed.

Entry Delay Duration

Ensure that timer is no longer than 45 seconds in order to comply with EN50131-1.

6.3 SMS Control

You can control the security system with SMS, and the command is shown below.

SMS format for arming/disarming: {Command} + {Operation Type} + {Target}

Command: 2 digits, 00- Disarming, 01- Away arming

Operation type: 1- Area Operation

Target: No more than 3 digits, 0-Operation for all areas, 1-Operation for area 1(zone1), and the rest can be deduced by the analogy.

Chapter 7 Appendix

7.1 Specifications

Model		DS-PA201P-32WE	DS-PA201P-16WE	DS-PA201PG-32WE	DS-PA201PG-16WE	DS-PA201PS-32WE	DS-PA201PS-16WE
WE: 868 Mhz		DS-PA201P-32WB	DS-PA201P-16WB	DS-PA201PG-32WB	DS-PA201PG-16WB	DS-PA201PS-32WB	DS-PA201PS-16WB
WB: 433 Mhz		DS-PA201P-32WA	DS-PA201P-16WA	DS-PA201PG-32WA	DS-PA201PG-16WA	DS-PA201PS-32WA	DS-PA201PS-16WA
WA: 915 Mhz							
Capacity	ARC numbers	1					
	Installer; Admin; User	1; 1; 14					
	Areas	8	4	8	4	8	4
	Wireless zones	32	16	32	16	32	16
	Wireless keypads; Sounders; Keyfobs	4; 4; 16					
	Logs	1000					
Communication	Transmission technology	TRI-X 868.0 to 868.6 MHz 433.1 to 433.7 MHz 912.5 to 917.4 MHz					
	Transmission range (free space)	Up to 2000 m (868 Mhz) Up to 1200 m (433 Mhz) Up to 2000 m (915 Mhz)					
	Maximum effective	≤ 25 mW (868 MHz) ≤ 10 mW (433 MHz) ≤ 60 mW (915 MHz)					

Control Panel User Manual

Model WE: 868 Mhz WB: 433 Mhz WA: 915 Mhz		DS- PA201P- 32WE	DS- PA201P- 16WE	DS- PA201PG -32WE	DS- PA201PG -16WE	DS- PA201PS- 32WE	DS- PA201PS- 16WE
		DS- PA201P- 32WB	DS- PA201P- 16WB	DS- PA201PG -32WB	DS- PA201PG -16WB	DS- PA201PS- 32WB	DS- PA201PS- 16WB
		DS- PA201P- 32WA	DS- PA201P- 16WA	DS- PA201PG -32WA	DS- PA201PG -16WA	DS- PA201PS- 32WA	DS- PA201PS- 16WA
	radiated power						
	Radio signal modulation	2GFSK					
	Encryption	AES-128					
	Ethernet	1 8P8C socket					
	Ethernet speed	≤ 10 Mbps					
	Wi-Fi	802.11 b/g/n					
	Cellular	No	No	GPRS	GPRS	4G	4G
	Cellular Model	No	No	M25	M25	EC21	EC21
	Cellular bands	No	No	GSM850, EGSM900 DCS1800, PCS1900	GSM850, EGSM900 DCS1800, PCS1900	B1, B3, B7 , B8, B20, B28	B1, B3, B7 , B8, B20, B28
	SIM slots	No	No	1	1	1	1
Monitoring	LED indication	Yes					
	Upgrade OTA	Yes					
	Protocols	SIA-DCS/*SIA-DCS; ADM-CID/*ADM-CID; OTAP; Other proprietary protocols					
Power supply	Mains power	110 to 240 V~, 50/60 Hz					
	Mains power consumption	Max current: 0.2 A Quiescent current: 90 mA					

Model WE: 868 Mhz WB: 433 Mhz WA: 915 Mhz		DS-PA201P-32WE	DS-PA201P-16WE	DS-PA201PG-32WE	DS-PA201PG-16WE	DS-PA201PS-32WE	DS-PA201PS-16WE
		DS-PA201P-32WB	DS-PA201P-16WB	DS-PA201PG-32WB	DS-PA201PG-16WB	DS-PA201PS-32WB	DS-PA201PS-16WB
		DS-PA201P-32WA	DS-PA201P-16WA	DS-PA201PG-32WA	DS-PA201PG-16WA	DS-PA201PS-32WA	DS-PA201PS-16WA
	Built-in backup battery	Yes					
	Battery life	Up to 12 hours at normal temperature (The battery working time can be significantly reduced at low temperatures)					
Tamper	Tamper alarm	Yes					
Enclosure	Dimension (W × H × D)	165 × 165 × 37.5 mm					
	Weight	400 g	400 g	407 g	407 g	410 g	410 g
	Operating temperature	-10 °C to 55 °C (The battery can not be charged at temperature lower than 0 °C, please make sure the adapter is connected)					
	Operating humidity	10% to 90%					
	Shell material	Plastic					

7.2 Trouble Shooting

7.2.1 Communication Fault

IP Conflict

Fault Description:

IP that the panel automatically acquired or set is same as other devices, resulting in IP conflicts.

Solution:

Search the current available IP through ping. Change the IP address and log in again.

7.2.2 Problems While Arming

Failure in Arming (When the Arming Process is Not Started)

Fault Description:

When the panel is arming, prompt arming fails.

Solution:

The panel does not enable "forced arming", and when there is a fault in the zone, the arming will fail. Please turn on the "forced arming" enable, or restore the zone to the normal status.

7.3 Access Levels

Level	Description
1	Access by any person; for example the general public.
2	User access by an administrator; for example a system user.
3	User access by an installer; for example an alarm company professional.

Table 7-1 Permission of the Access Level

Permissions	User Level		
	Level 1	Level 2	Level 3
User Management	No	Yes	Yes ^a
System Management	No	Yes	Yes
Areas	Yes	Yes	Yes ^a
View devices	Yes	Yes	Yes ^a

 **Note**

^a By the condition of being accredited by user in level 2.

7.4 Signaling

Detection of ATP/ATS Faults

ATP (Alarm Transmission Path) faults will be detected when network interface of the control panel disconnected or the transmission path to the transceiver of receiving center located in ARC blocked somewhere in between. An ATS (Alarm Transmission System) fault will be reported when ATP faults are detected on both transmission paths.

ATP restore will be detected as soon as network interface connected and the transmission path to the transceiver of receiving center restored. ATS restore will be reported when ATP restore of any transmission path is detected.

The timing performance of detecting ATP faults and restores shows in the table below.

	TN	Maximum timing of detection
Primary ATP failure/restore	LAN/Wi-Fi	30 s
Secondary ATP failure/restore	GPRS	30 s
	3G/4G LTE	30 s (when primary ATP failed)

Signaling will be always transmitted from primary ATP when it is operational. Otherwise it will be automatically switched to secondary transmission path that is operational at the moment. Both primary and secondary ATP fault and restore events will be reported to ARC when there is an ATP left to work. They will also be recorded to mandatory log memory with capacity of 300 records allocated in non-volatile flash memory storage, as well as the ATS fault record. The detail of reports and log records are listed in the table below.

	Event code when signaling	Event log description
Primary ATP failure/restore	E351/R351	Main signalling path fault/ restored
Secondary ATP failure/restore	E352/R352	Backup signalling path fault/ restored
ATS failure/restore	N/A	ATS Failure/restored
Primary network interface failure/restore	E351/R351	Main signalling path fault/ restored
Secondary network interface failure/restore	E352/R352	Backup signalling path fault/ restored

ATS Category

While the alarm receiving center is enabled, the control panel will upload alarm report to the receiver center via the main path (LAN or Wi-Fi) or the back-up path (3G/4G). If the control panel is properly connected to the LAN or Wi-Fi, the main path is selected as the transmission path. If the main path connection is failed, the path will be switched to 3G/4G. And if the main path

connection is restored, the path will be switched back to LAN or Wi-Fi. The control panel checks the connection status continuously, and generates logs transmission fault for any of the path. While both of the paths are invalid, the control panel determines ATS fault.

7.5 SIA and CID Code

The code is for transmitting from the security control panel to ARC via DC09 protocol.

Read the table below to obtain the events corresponding to the CID code.

You can scan the QR code and download the CID table separately.



Figure 7-1 CID Table

7.6 User Privacy Statement

The debug or zhimakaimen command is used to control access to the file system to ensure device security. To obtain this permission, you can contact technical support.

The device has admin, installer, maintenance, operator account. You can use these accounts to access and configure the device.

Table 7-2 User Privacy Information Description

Password	The password for the device account, used to log in to the device.
User name	The user name for the device account, used to log in to the device.
Device IP and port	The device IP and port are used to support network service communication.
Log	Used to record information such as device operating status and operation records.
Database information	Used to record information.

7.7 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.

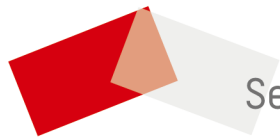
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION 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.

7.8 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.



See Far, Go Further