AX PRO

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED “AS IS” AND “WITH ALL FAULTS AND ERRORS”. HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
YOU ACKNOWLEDGE THAT THE NATURE OF 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 INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

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

Data Protection

During the use of device, personal data will be collected, stored and processed. To protect data, the development of Hikvision devices incorporates privacy by design principles. For example, for device with facial recognition features, biometrics data is stored in your device with encryption method; for fingerprint device, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.

As data controller, you are advised to collect, store, process and transfer data in accordance with the applicable data protection laws and regulations, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and assessments of the effectiveness of your security controls.

Symbol Conventions

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

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

Note

- Please update firmware to the latest version.
- For installers, it is recommended to install and maintain devices via Hik-Partner Pro.

Regulatory Information

EN 50131-1:2006+A1:2009+A2:2017+A3:2020

EN 50131-3:2009

EN 50131-6:2017+A1:2021

EN 50131-5-3:2017

EN 50131-10:2014

EN 50136-2: 2013

SSF 1014

Security Grade (SG): 2

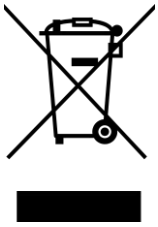
Environmental Class (EC) : II

Larmklass R, Miljöklass II

Certified by KIWA

Note EN50131 compliance labeling should be removed if non-compliant configurations are used.

EU Conformity Statement

CE	This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU
	2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info
	2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Contents

Chapter 1 Installation Instruction

1.1 Typical Scene

Figure 1-1. Typical Scene

Typical installation location of devices:

1. AX PRO Control Panel
2. Repeater
3. PIR Detector
4. Sounder
5. Magnetic Detector

1.2 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. The repeater needs to be installed between the control panel and the peripheral.
6. Check the signal strength before installation and it is recommended to install the device at the green indicator location. (Do not wrap the detector with your hands when checking the signal strength.)

7. Vertical installation is recommended for devices.

1.3 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.

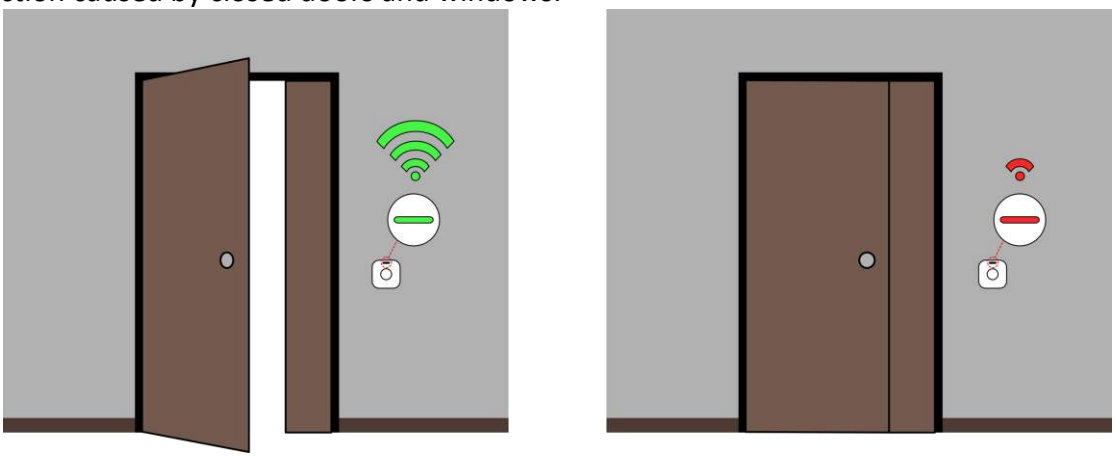


Figure 1-2. Installation FAQ

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.
- Install a repeater between the offline peripheral and the control panel.
- Check whether to install devices according to the precautions.

Chapter 2 Introduction

AX PRO is a wireless alarm system designed to protect premises required for proper protection from intrusion alarm. It supports LAN /Wi-Fi as the primary transmission network. The system is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- Innovative Tri-X 2-way wireless technology.
- Two-way communication with AES-128 encryption.
- Frequency-hopping spread spectrum (FHSS) is used to avoid interference, to prevent eavesdropping, and to enable code-division multiple access (CDMA) communications.
- Voice guide for alarm alert, system status indication, operation prompt, etc.
- Configuration via web client, mobile client, and Convergence Cloud.
- Pushes alarm notification via messages or phone calls.
- Views life videos from Hik-Connect and alarm video clips via emails, Hik-Partner Pro, and Hik-Connect.
- Uploads alarm reports to ARC.
- SIA-DC09 protocol, and supports both Contact ID and SIA data format.
- 4520 mAh lithium backup battery with 12 H standby duration.

<table>
<tr><td colspan="2" rowspan="2">Parameters</td><td colspan="2">AX PRO</td></tr>
<tr><td>64 Series</td><td>96 Series</td></tr>
<tr><td rowspan="2">Event logs</td><td>Mandatory</td><td colspan="2">1000</td></tr>
<tr><td>Total</td><td colspan="2">5000</td></tr>
<tr><td rowspan="5">ARC Signaling</td><td>ATS Category</td><td colspan="2">DP2</td></tr>
<tr><td>Primary Transmission Path</td><td colspan="2">LAN / WiFi</td></tr>
<tr><td>Secondary Transmission Path</td><td colspan="2">GPRS or 3G/4G LTE</td></tr>
<tr><td>Acknowledgement Operation[a]</td><td colspan="2">Pass-through</td></tr>
<tr><td>Protocols</td><td colspan="2">SIA-DC09[b], Contact ID, ISUP 5.0</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>a</td><td colspan="3">As per requirements defined in EN 50131-1:2006+A1:2009+A2:2017+A3:2020
AX Pro wireless control panel adopts pass-through mode of acknowledgement operation. Both positive and negative acknowledgement from the transceiver of receiving center will be recorded.
Event log description
Positive acknowledgement — ARC Uploaded
Negative acknowledgement — ARC Communication Failed</td></tr>
<tr><td>b</td><td colspan="3">AX Pro wireless control panel is compatible with SIA IP Reporting (UDP/TCP-2013) as per ANSI/SIA DC-09-2013: Internet Protocol Event Reporting. The control panel supports tokens (protocols) of ADM-CID and SIA-DCS defined in SIA DC-07-2001.04, which will be modified to insert a “*” before token name as *ADM-CID and *SIA-DCS when the data and timestamp of transmission message are AES encrypted. AES-128, AES-192 and AES-256 are all supported.</td></tr>
</table>

Note

ISUP5.0:

A privacy internet protocol that is used for accessing the third-party platform, which supports alarm report uploading, AX PRO management, and short video uploading.

The prioritization of the message and indications are the same. The AXPRO uploads messages and gives indications synchronously.

Standard DC-09 Protocol:

- ADM-CID: The data presenting method of DC-09 is CID, which is not encrypted and only for uploading alarm report.
- *ADC-CID: The data presenting method of DC-09 is CID, which is encrypted and only for uploading alarm report.
- SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is not encrypted and only for uploading alarm report.
- *SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is encrypted and only for uploading alarm report.

RSSI Instruction for Peripherals

With regards to EN 50131-5-3 4.2.2 Requirement for immunity to attenuation.

Signal Strength	RSSI Value	Indication	Remark
Strong	≥66	Green	Okay to install
Medium	50 to 65	Yellow	Not recommend to install, but can work
Weak	40 to 49	Red	Not okay to install, but can work most of time
Invalid	<40	Red (flash)	Not okay to install, cannot work normally

AX PRO Notification Options

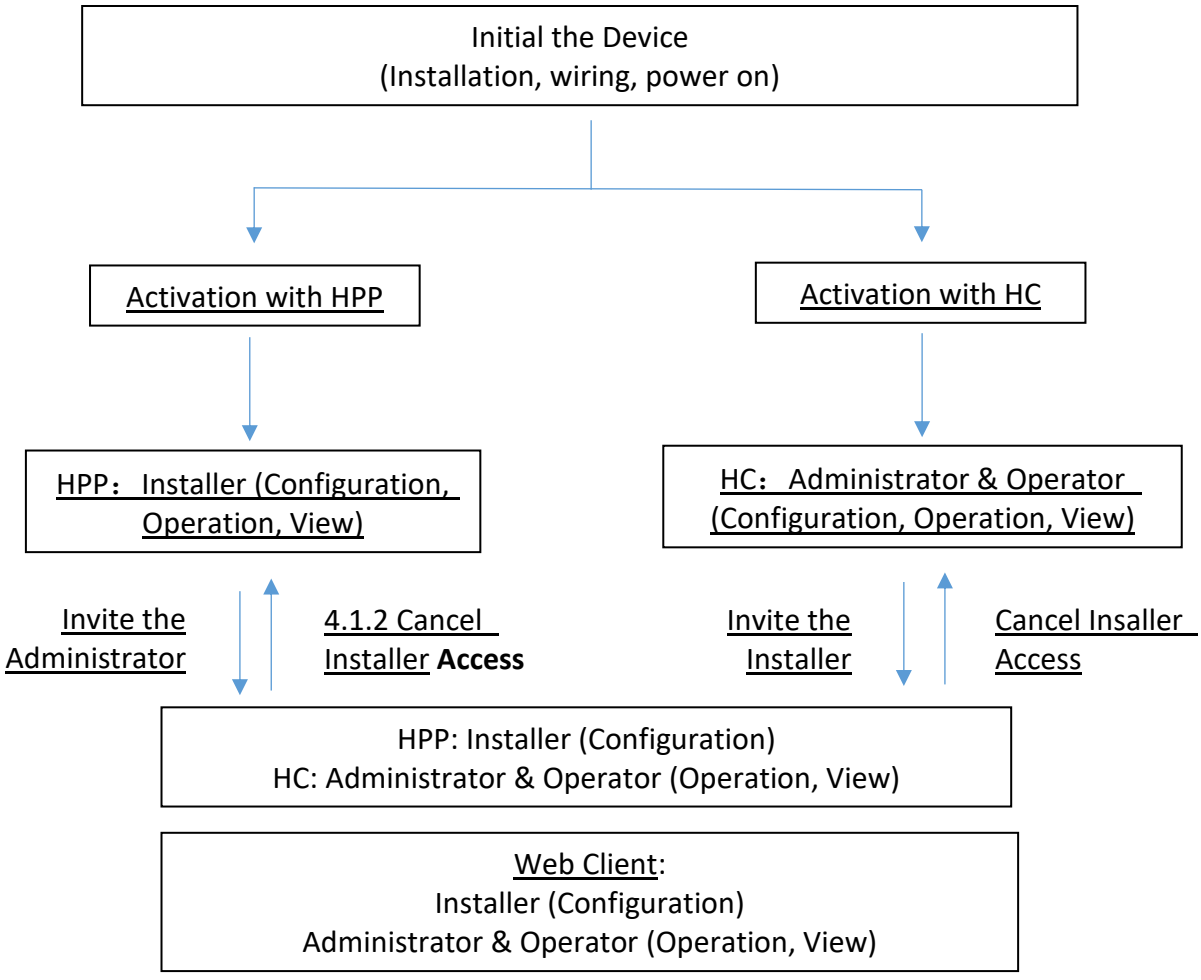
The AX PRO is suitable for the below notification requirements along with the required sounders

Notification equipment	I&HAS Grade 2		
	Options		
	C	E	F
Self-powered audible WD	2	1	Optional
ATS	DP1	Optional	DP2

Chapter 3 Start Up

3.1 Authority Management

You can use web browser, HPP (Hik-Partner Pro, APP) or HC (Hik-Connect, APP) to activate the device. After activation, you can manage the device by transferring permissions between APPs. You can also use the account and password of all accounts to log in to the WEB client to configure the device.



For more information, refers to ***Chapter 4 User Management***.

3.2 Activation

While initial the device with Hik-Partner Pro or Hik-Connect, the AX PRO should always be add to an installer account first. The installer account will invite and transfer ownership to the administrator account later after finishing all initial setup and test. Follow the steps below to initializing the wireless alarm system.
You can activate the device by Wi-Fi, LAN or SIM(4G/GPRS).

3.2.1 Activation with LAN/SIM(4G/GPRS)

Step1 Create a site (Only for HPP)
Download the Hik-Partner Pro and login with the installer account.

A site is the place where the alarm system deployed. Create a site where the device can be added to with it's site name and address. The owner of the site would be an end user, usually regarded as administrator.

Step2 Connect to the network.
Connect the device to the Ethernet with LAN or SIM, and power the device on.

Note

- While the device is powered on, the power LED turn green.
- Once the device connected to the network, the LED indicator turns green.
- Make sure the SIM card you insert can connect to the network.

Step3 Add Device
1. Open the site. (Only for HPP)

Note

While initial the device with Hik-Connect, you do not need to build a site first.

2. Tap **+** and scan the QR code on the label of the panel.
3. Tap **Add**.

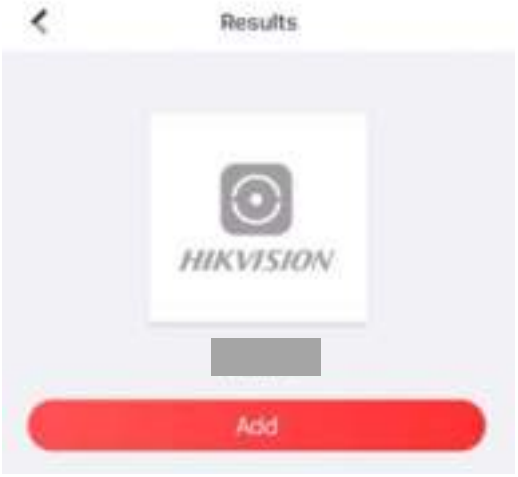


Figure 3-1. Add Device

4. Tap **Next**. You can edit parameters of the device or skip to use it directly.

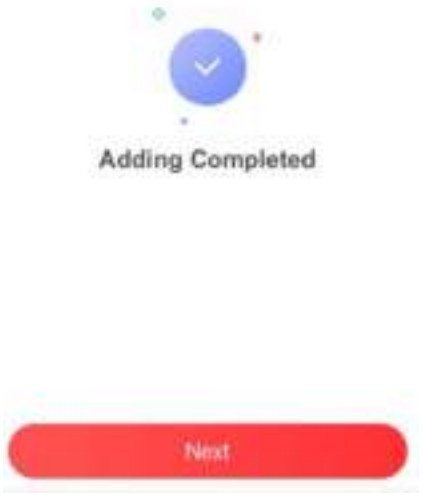


Figure 3-2. Adding Completed

The control panel will be added to the site (HPP) created and managed by the installer account, which also means that the installer account was created in the panel.

The installer now can perform configuration and tests of the panel before deploying. Both Hik-Partner Pro/Hik-Connect Service and local web client can be logged in with the Hik-Partner Pro/Hik-Connect installer account.

Note

While initial the device with Hik-connect, you do not need to build a site first. Download and login the App, and add the device by scanning QR code or enter the device serial No..

3.2.2 Activation with Wi-Fi

Step1 Create a site (Only for HPP)

Download the Hik-Partner Pro and login with the installer account.

A site is the place where the alarm system deployed. Create a site where the device can be added to with it's site name and address. The owner of the site would be an end user, usually regarded as administrator.

Step2 Configure the Network on APP

1. Download Hik-Connect/Hik-Partner Pro and log in.

2. Power on the AX PRO.

3. Connect your phone to your home Wi-Fi. Make sure that this Wi-Fi can access the Internet normally and the signal is stable.

4. Open the HC or HPP, click **+**, and select **Scan QR Code**.

Figure 3-3. Scan QR Code

5. Scan the QR code on the back of the control panel and wait for the result.

Figure 3-4. QR Code

Figure 3-5. Result

6. Tap **Next**.

7. Tap **Wireless Connection**.

Figure 3-6. Connection Type

8. Check **The device is started**. And then tap **Next**.

Figure 3-7. Device Is Started

9. The APP will automatically fill in the home Wi-Fi currently used by the mobile phone into the page, as shown in the figure below. After confirming the Wi-Fi password, tap **Next**.

Figure 3-8. Configure Wi-Fi

10. Tap **Connect to a Network**.

Figure 3-9. Connect to Network

11. Tap **Join**. The mobile phone will disconnect the home Wi-Fi. After interacting information with the control panel, the mobile phone will automatically switch back to the home Wi-Fi.

Figure 3-10. Join Wi-Fi

As shown in the figure above, during the information interacting, the Wi-Fi connected to the mobile phone named “HAP_serial number” (AX PRO serial number)

Figure 3-11. Serial Number

Figure 3-12. Wi-Fi

12. After the control panel broadcasts the "Exit hotspot mode", the following page will appear.

Figure 3-13. Connecting to Wi-Fi

13. Wait for the device to join the home Wi-Fi and log in the EZVIZ Cloud.

(1) When the home Wi-Fi signal is good, the control panel will successfully log in to EZVIZ Cloud and complete the binding before the countdown ends.

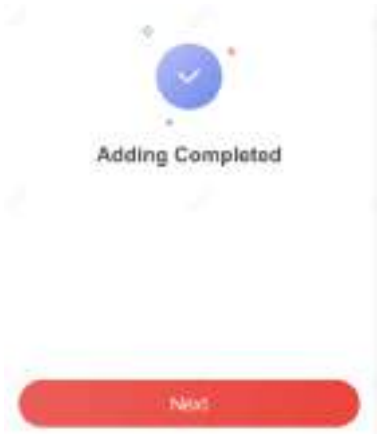


Figure 3-14. Adding Completed

(2) When the home Wi-Fi signal is unstable, the control panel may not be connected to the EZVIZ Cloud before the countdown ends, and the following page will appear:

Figure 3-15. Reload

If you make sure that the home Wi-Fi password is correct and quality is good, tap **Refresh Network**, the control panel will enter a new countdown. You can wait for the connection.

If you want to change the home Wi-Fi, you should change the home Wi-Fi connected to the mobile phone first, then press the **RESET** button on the back of the control panel (marked in the figure below). After hearing the voice of "Enter hotspot mode", tap **Reload**. The interface will jump back step 9, you can configure the network again.

Figure 3-16. Reset Button

Note

Once the device connected to the network, the LED indicator turns green.

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.

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap .
3. Tap **Delete Device**.

Figure 3-17. Settings

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.

1. Open HC and tap **+**.
2. Tap **Scan QR Code**.

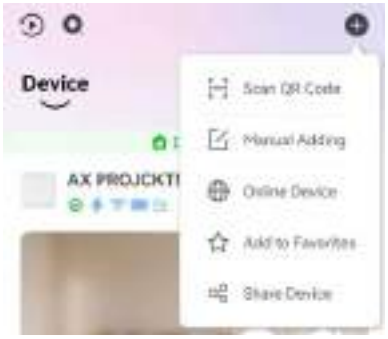


Figure 3-18. Scan QR Code

3. Scan the QR code on the label of the device.

Figure 3-19. QR Code

4. Press the **RESET** button twice quickly on the back of the device.

Figure 3-20. Reset Button

5. Tap **Unbind Device**.

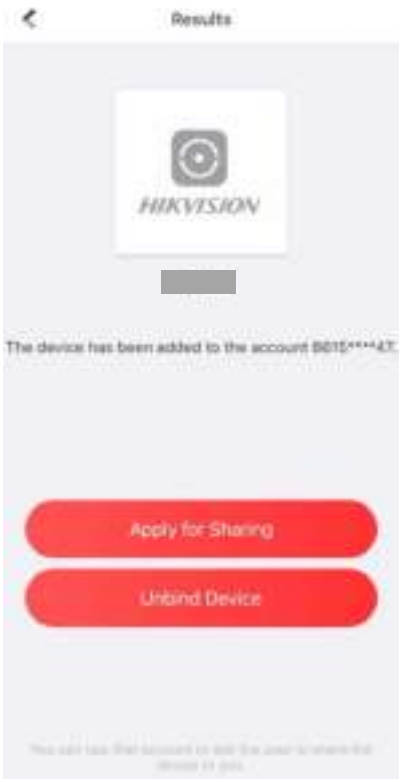


Figure 3-21. Unbind Device

5. Enter verification code and tap **Finish**.

Figure 3-22. Verification Code

The device is unbound from the account. You can add it to your account now.

Note

The maximum duration of unbinding mode is 3 minutes. After the timeout, the device will automatically exit the unbundling mode.

Chapter 4 User Management

4.1 User Management

Note

- The users can be created in clients.
- The name and password of network user (web client and APP user)can be 1 to 32 characters and 8 to 16 characters.

4.1.1 Invite the Administrator

After the initial configuration finished, the service provider in Hik-Partner Pro can transfer the device to the administrator on the Hik-Connect.

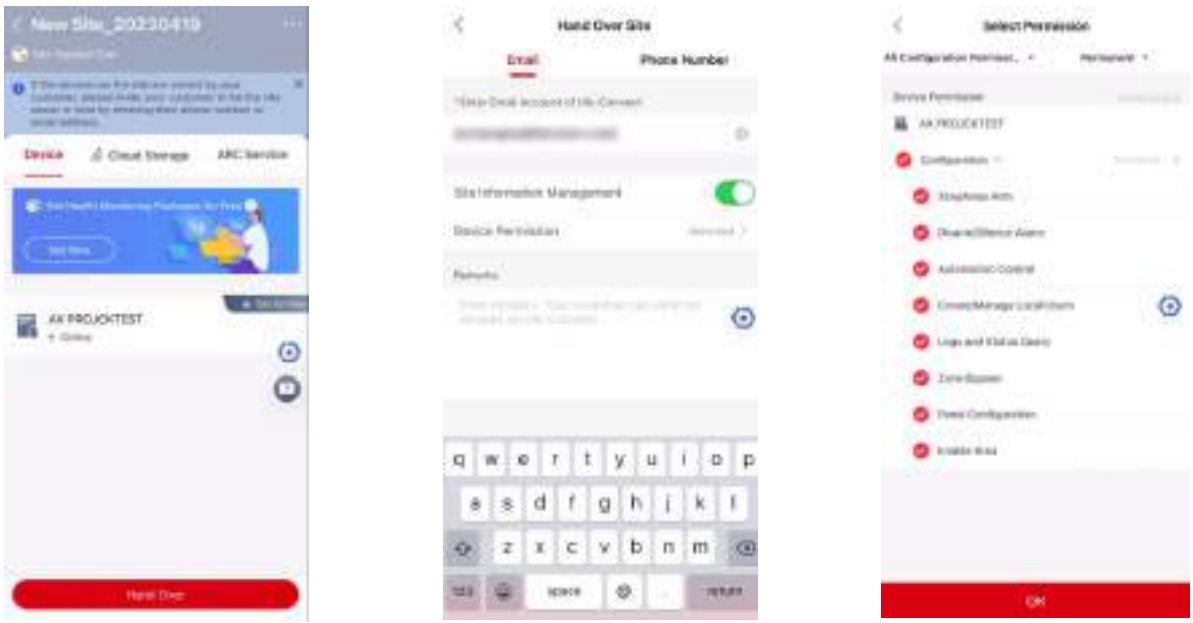


Figure 4-1. Hand Over

1. In the site, press **Hand Over**. There will be 2 methods:

   Transfer

   Transferring the device to the user, who will owns the device.

   Share

   Share the device to the user, who can only use the device.
2. Click **Transfer**.
3. Enter the recipient's email address or phone number.
4. Click **Device Permission**. You can select the configuration permissions that the recipient gets and the valid time.

5. Click **OK**.
6. Open the **Hik-Connect** APP and login with the administrator account. The installer service request will be pop-up or received at notification page.
7. Tap **Notification → Service** and tap the message to receive the request.
8. Tap **Agree**.
9. Set valid time and tap **Agree**. The device will be display in your device list.

The administrator account will be added to the control panel, which could be used to login to Hik-Connect app and local web client.

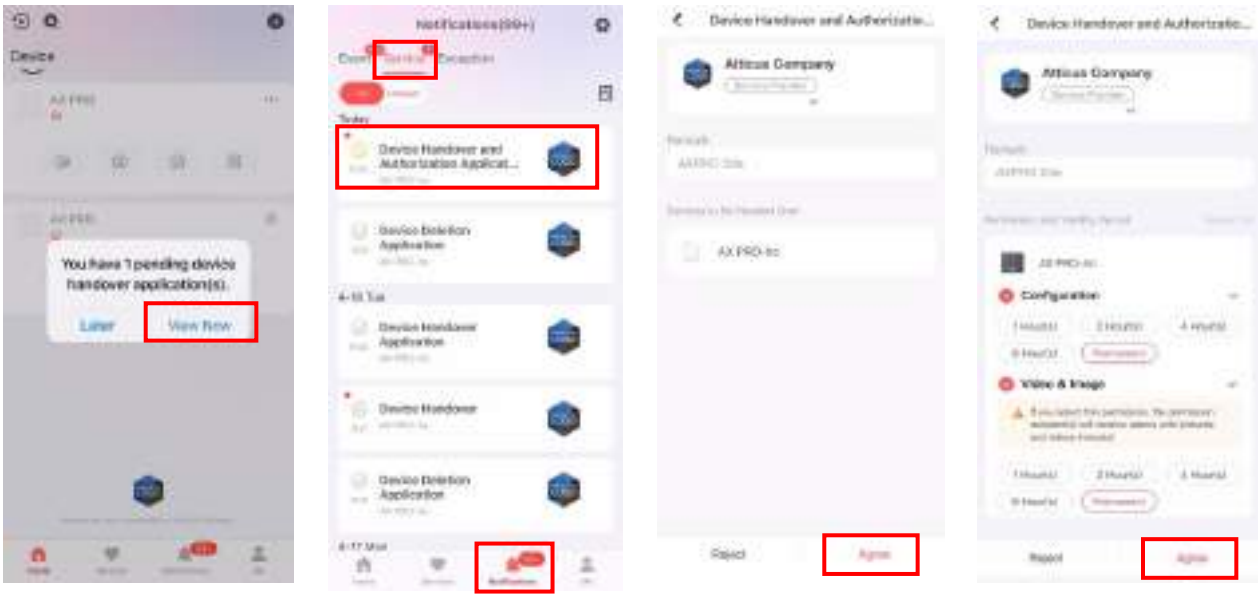


Figure 4-2. Accept Handover

4.1.2 Cancel Installer Access

The administrator can cancel the access authorization of the service provider.

1. Enter the **Service** page.
2. Tap the service provider.
3. Tap **··· → Cancel Authorization.**
4. Confirm the operation, and the authorization of the installer will be canceled. Once the authorization is canceled, the installer need to apply it again if any access requirement.

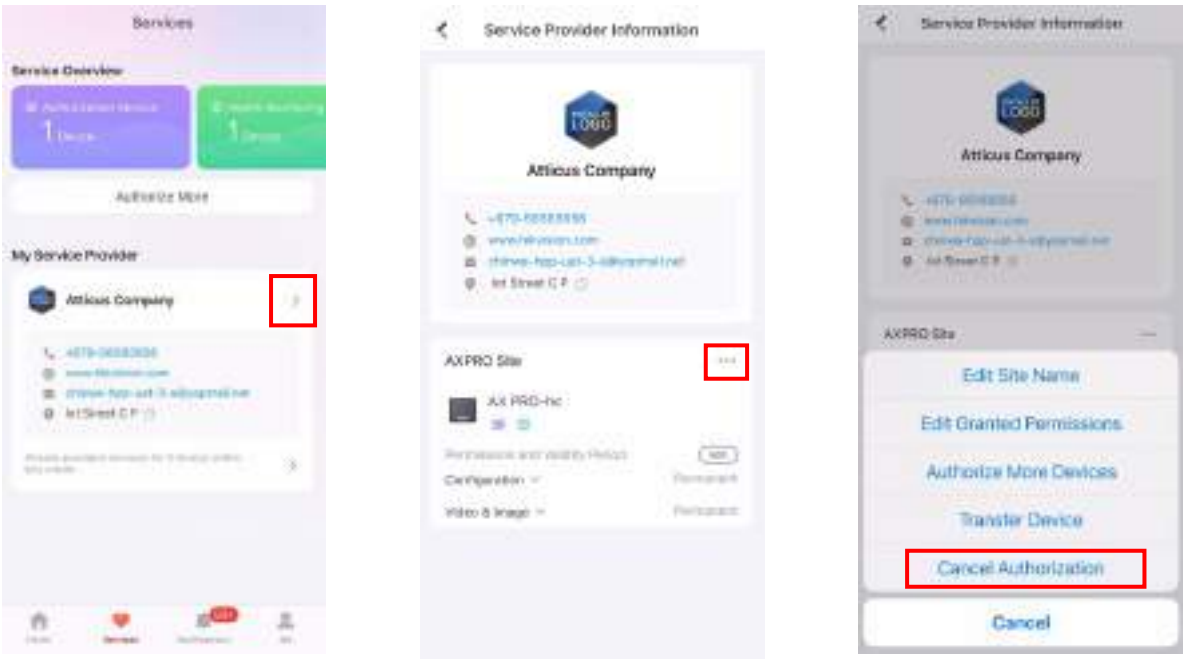


Figure 4-3. Cancel Authorization

4.1.3 Add an Operator

The administrator can share the device to other operators.

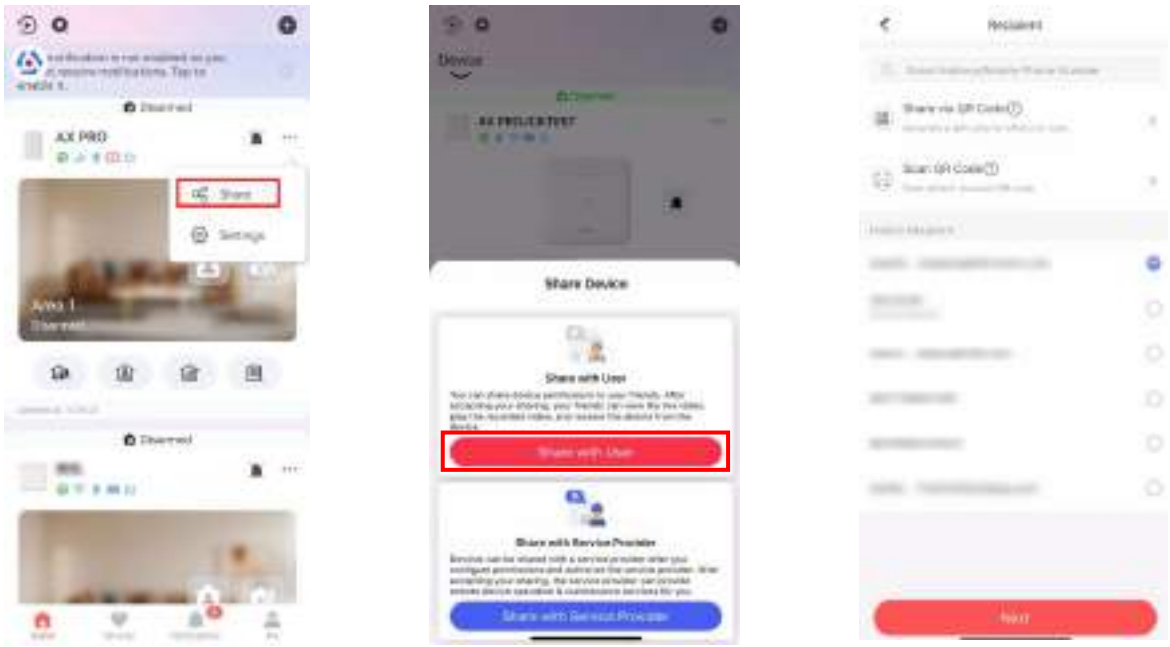


Figure 4-4. Share with User

1. Tap ··· → **Share** → **Share with User**.
2. Enter an operator account or select a history recipient.
   Administrator can also select which device to be shared.
3. A sharing message will be sent to the operator's account, and the operator can read the message in the notification page of Hik-Connect App.

The operator account will be added to the control panel, which could be used to login to Hik-Connect app and local web client.

4.1.4 Delete an Operator

Administrator user can delete an operator.

1. Enter the **Me** page and tap **Manage Sharing Settings**.
2. Delete the selected operator.

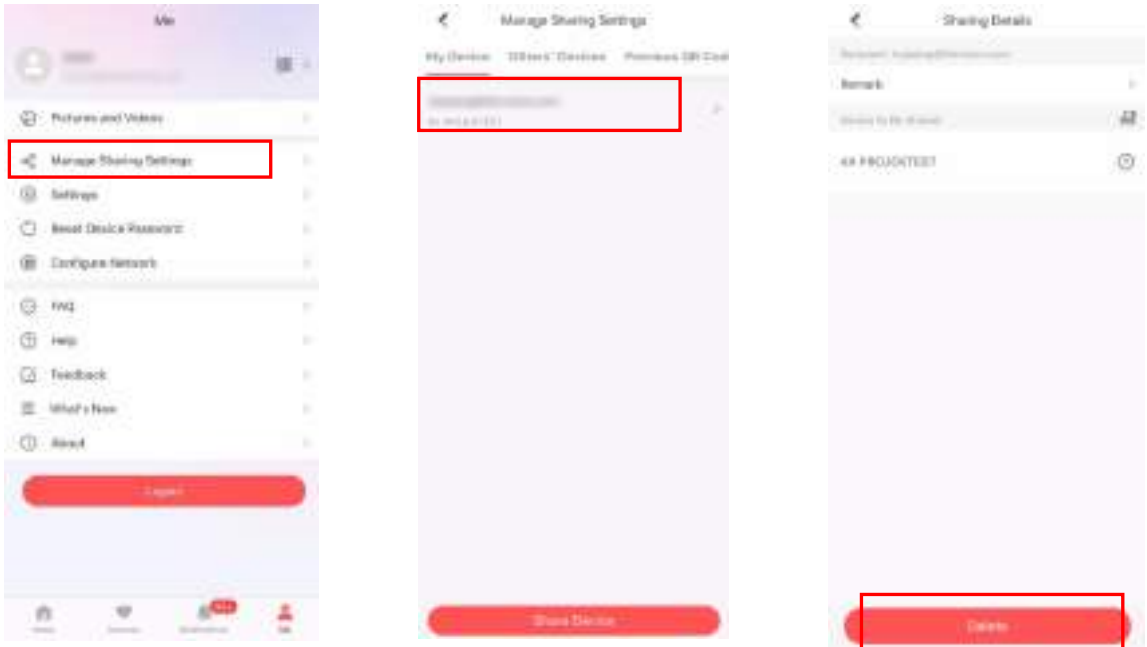


Figure 4-5. Manage Sharing Settings

4.1.5 Invite the Installer

The service provider on the Hik-Partner Pro APP is invited to control the device.

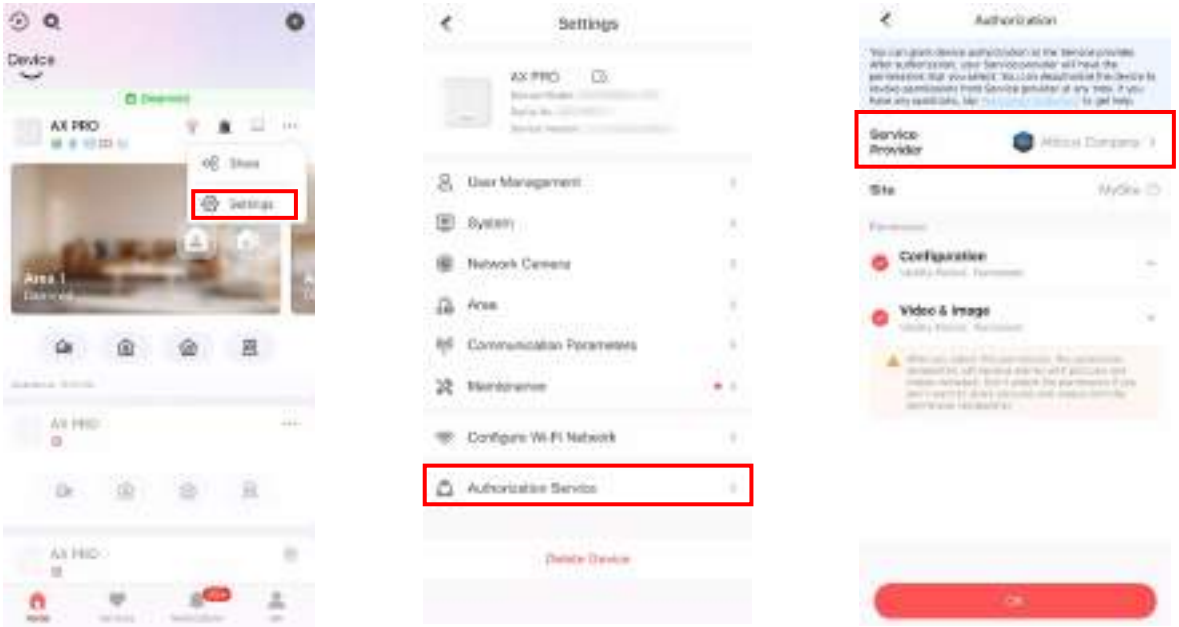


Figure 4-6. Invite the Installer

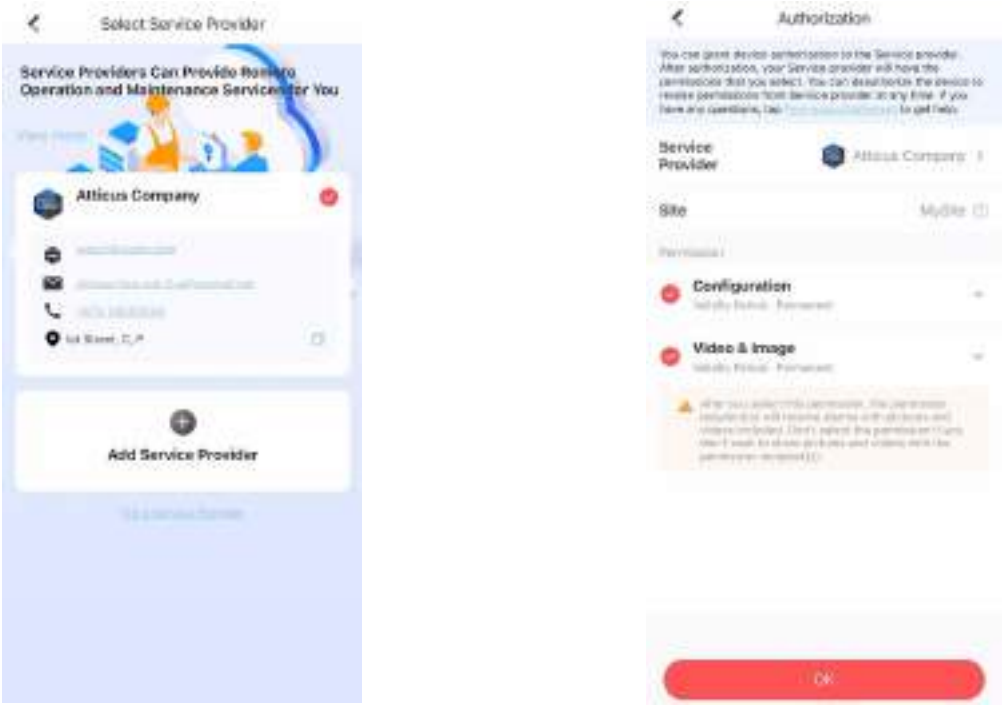


Figure 4-7. Invite the Installer2

1. Login Hik-Connect, tap ··· → **Settings**
2. Tap **Authorization Service**.
3. Tap **Service Provider**.
4. Select a service provider or add a new one.
5. Tap **OK** in authorization page.
6. Select configuration permission you want to send and tap **OK**.

4.2 Access Entries

The installer and operators of the AXPRO were assigned different access levels which define the system functions that an individual user can perform. Various user entries are provided for different user roles with particular access level.

Access entries for Installers (Access Level 3)

- **Hik-Partner Pro Service**
  Hik-Partner Pro is a service for installers that is used to manage customers' alarm systems located in various sites remotely. Control panels can be added to an installer account on the Hik-Partner Pro Service and be managed in sites.
- **Local Web Client**
  Visit the device IP address that can be found out with SADP tool. The installer can login with Hik-Partner Pro service account after the panel was added.
- **Other Entries**
  Keypad PINs and tags can be also assigned with installer user at particular access level to perform essential operations.

Access Entries for the Administrator and Operators (Access Level 2)

- **Hik-Connect Service**
  The Hik-Connect service can be used for end users to access and manage the devices.
- **Local Web Client (for the administrator)**
  As soon as the panel was added to the end user account on Hik-Connect Service, the Hik-Connect account can be used to login to the web client build in.

  Operators cannot login the web client.
- **Other Entries**
  Keypad PINs and tags can be also assigned with end user at particular access level to perform essential operations.

Chapter 5 Configuration

5.1 Set-up with Hik-Partner Pro

5.1.1 Use the Hik-Partner Pro APP

The installer can use the Hik-Partner Pro to configure the AX PRO, such as activation, device enrollment, etc.

Download and Login the Hik-Partner Pro

Download the Hik-Partner Pro mobile client and login the client before operating the AX PRO.

Steps

1. Download Hik-Partner Pro mobile client.
2. Optional: Register a new account if it is the first time you use the Hik-Partner Pro mobile client.

Note

- For details, see *User Manual of Hik-Partner Pro Mobile Client*.
- You need an invitation code for registration. Please ask technical supports.

3. Run and login the client.

Add AX PRO to the Mobile Client

Add AX PRO to the mobile client before other operations.

Steps

1. Power on the AX PRO.
2. Create or search a site.
   - Tap **+**, set site name, time zone, address, city, state/province/region and tap **OK** to create a site.
   - Enter site name in the search area and tap **Search Icon** to search a site.
3. Tap **Add Device**.
   - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the AX PRO.

     Note

     Normally, the QR code is printed on the label stuck on the back cover of the AX PRO.

   Tap **Manual Adding** to enter the Add Device page. Enter the device serial No. and verification code to add the device.
4. Activate the **Device**.

Add Peripheral to the AX PRO

Add peripheral to the AX PRO.

Steps

1. Select a site.
2. Select a control device (AX PRO).
3. Tap the **+** icon.
   – Scan the QR code on the peripheral.
   – Tap to enter the Manually Input page. Enter the device serial No. and select the device type to add the device.

Main Page

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

On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.

Figure 5-1. Main Page

Enable Alarm
Tap to select **Audible Panic Alarm** or **Silent Panic Alarm**.

View Faults
Tap to view faults.

Area Management
Tap **+** to add an area.
Tap Area to enter the area management page. Refers to ***Set Arming/Disarming Schedule*** for details.

Arm/Disarm the Area
Arm or disarm the area manually as you desired.
On the device list page, tap the AX PRO and then log in to the device (if required) to enter the Area page.

Operations for a Single Area

Figure 5-2. Single Area

- **Away Arming**: Tap to away arm a single area. When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time.
- **Stay Arming:** Tap to stay arm a single area. When all the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection set in all the zones of all areas.

Operations for Multiple Areas

Figure 5-3. Multiple Area Key

- **Select Areas**: Tap to select areas you want to operate. If you do not select areas, following operations will take effect for all areas.
- **Away Arming**: Tap to away arm selected areas. When all the people in the detection area leave, turn on the Away mode to arm all zones in all areas after the defined dwell time.
- **Stay Arming**: Tap to stay arm all areas. When the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony) set in all the zones of all areas. At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People

can move inside the area and alarm will not be triggered.

- **Disarming**: Tap to disarm all areas. In Disarm mode, all the zones of all areas will not trigger alarm, no matter alarm events happen or not.
- **Silence Alarm**: Tap to silent alarms for all areas.

Zone Management

1. Tap **Device** to view linked zones.

Figure 5-4. Device Page

2. Tap **+** to add a new zone.
3. Tap a zone to enter the management page. You can view device status (e.g. temperature, battery status, single strength, etc.).
4. Tap on the upper right corner to enter the zone settings page.
5. Select a zone type.

You can view the configurable zone types for various detectors through ***I. Detector Zone Types***.

Instant Zone

This Zone type will immediately trigger an alarm event when armed.

Delay Zone

-Exit Delay Time: Exit Delay provides you time to leave through the zone without alarm. You should confirm faults first, and then the zone is in arming process. If the delay zone is triggered within the exit delay time but it restores before the time ends, the alarm will not be triggered and the zone will be armed.

-Entry Delay Time: Entry Delay provides you time to enter the zone to disarm the system without alarm.

After triggering, if the zone is not disarmed or silenced before the entry delay time ends, the zone will alarm.

-Stay Arm Delay Time: Stay arming uses Stay Arm Delay Time to count down.
The system gives Entry/Exit delay time when it is armed or reentered. It is usually used in entrance/exit route (e.g. front door/main entrance), which is a key route to arm/disarm via operating keypad for users.

Note

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

Panic Zone

24-hour active zone, whether armed or not. Report panic alarm after triggering. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

Medical Alarm

24-hour active zone, whether armed or not. Report medical alarm after triggering.

Fire Zone

24-hour active zone, whether armed or not. Report fire alarm after triggering.

Gas Zone

24-hour active zone, whether armed or not. Report gas alarm after triggering.

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise.

Keyswitch Zone

Trigger Type:
-By Trigger Time: Change the arming and disarming status after each trigger. For example, in the disarmed status, if the zone is triggered, the linked area will be armed. Trigger the zone again and the area will be disarmed.
-By Zone Status: You need to choose to arm or disarm the linked area after the zone is triggered.
In the case of the lid opened alarm, the arming and disarming operation will not be triggered.

Disabled

Zone disabled ignoring any alarm event. It is usually used to disable faulty detectors.

24-hour Zone

The zone activates all the time with sound/light output when alarm occurs, whether it is armed or not. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Timeout Zone

The zone activates all the time. When this zone has been triggered or restored and exceeds the set time, an alarm will be generated.

It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).
-Not-Triggered Zone Alarm: If the zone is not triggered for the set time, it will alarm.
-Alarm on Zone Activated: If the zone is triggered for the set time, it will alarm.
-Retry Time Period: Set the timeout period.

6. Enable other parameters according to your actual needs.

Note

The supported functions vary depending on the zone types. Refer to the actual zone to set the function.

Arm Mode

If the zone is a public zone (the zone is belongs to more than one areas), you can set arm mode.
And: When all linked areas are armed, the zone will arm. When any of linked areas is disarmed, the zone will disarm.
Or: When any of the linked areas is armed, the zone will arm. When all linked areas are disarmed, the zone will disarm. When the zone is in alarm, the disarmed areas linked with the zone cannot be armed.

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

PD6662 is not enabled: You need to set the combined time interval.
When the first zone is triggered, the system will start timing after the zone is restored. If the second zone is triggered within the set time, both zones will give alarms. Otherwise, no alarm will be triggered.
If the first zone is not be restored, both zones will give alarms when the second zone is triggered, regardless of whether the set time has elapsed.
PD6662 is enabled: You need to set the combined time interval.
The first zone will give an alarm when triggered. If the first zone is not restored and the second zone is triggered, the system will report the alarm confirmation.
If the first zone is restored, the system will start timing. If the second zone is triggered within the set time, the system will report the alarm confirmation.
If the first zone is restored, the system will start timing. If the second zone is not triggered within the set time, no information will be reported.

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

After enabled, when an alarm is triggered, only the report will be uploaded and no sound is

emitted.

Double knock

After enabled, the time interval can be set. If the same detector is triggered twice or continuously in a period of time, the alarm will be triggered.

Sounder Delay Time

The sounder will be triggered immediately (0s) or after the set time.

Final Door Exit

Only magnetic contacts have this option.
After enabling, when the user use keypads or tag readers to arm:
-Arm With Faults is enabled: During the arming countdown, if the magnetic contact is triggered and then restored, the arming process will be terminated immediately after restoring, and the arming is completed.
-Arm With Faults is disabled: If the magnetic contact is triggered and then restored, the linked area immediately arms the delayed zone.

AM Mode

-Alarm Only When ARM: Anti-masking alarm will be triggered only when the zone is armed.
-Alarm Only When ARM or DISARM: Anti-masking alarm will be triggered whether the zone is armed or disarmed.

Warning Time Enable

Set the warning time. The warning time countdown will be triggered if the instant zone is triggered during entry delay or the system not be disarmed after entry delay ends. Local alarms are generated during the period, but no messages will be pushed.

Swinger Limit Activations

When the number of times the infrared detector is triggered exceeds the set value, the alarm will no longer be triggered. (Except for anti-masking alarms.).

Dual Zone (Wired Zone)

After enabled, when multi transmitter detects that the entire zone circuit of the local zone and the extended zone is open circuit, both zones trigger lid opened alarms.

7. If required, link a PIRCAM or a camera for the zone.
8. Click **OK**.

View Status

Tap **Status** to view peripherals' status.

Bypass Zone

When the area is armed, you can bypass a particular zone as you desired.

Before You Start

Link a detector to the zone.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the Area page.
2. Tap **Device**.
3. Tap a zone in the Device tab.
4. Tap to enter the Settings page.
5. Enable **Bypass** and the zone will be in the bypass status.

Bypass Status

The detector in the zone does not detect anything and you will not receive any alarm from the zone.

User Management

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

Note

There are three types of users for the AX PRO, including administrator (or owner), operator, and installer (or setter). Different types of users have different permissions for accessing the functionality of the AX PRO.

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the AX PRO page.
2. Tap to enter the Recipient Page.
3. Select a user to invite.
   - Scan QR code to invite a user.
   - Enter email address/mobile phone number to invite a user.
   - Select a user in the list.
4. Tap **Next** to invite the user.

Note

The recipient need to accept the invitation.

5. Tap → **User Management**.
6. Tap a user to enter the User Information Page.
7. Optional: Perform the following operations if required.

User Permission	You can tap the target user on the user list and then tap to set the permissions authorized to the target user.

Note

Only the administrator can do such an operation.

Linked Area

If the target user is an operator, tap the target user on the user list and then tap to set the area linked to the target user.

Note

Only the administrator can do such an operation.

Change Keypad Password

If the target user is an administrator, an installer or an operator, you can tap the target user on the user list and then tap **Change Keypad Password** to set the keypad password to the target user.

Note

The password (PIN code) is allowed to be 4 to 6 digits. No number is disallowed, with 10,000 to 100,000 differs, and no limit of the digit combination.
After you add one keypad, you can add PIN code (Keypad Password) in the user menu. When you click in the input box, there will be indication shows that 4 to 6 numbers allowed. This is the same for each user

Change Duress Password

If the target user is an administrator or an operator, you can tap the target user on the user list and then tap **Change Duress Password** to set the duress password to the target user.

Note

If under duress, you can enter the duress code on the keypad to arm and disarm area(s) and upload a duress alarm.

Card/Tag/Keyfob

An administrator, an installer or an operator can use cards/tags or keyfob.

Note

- Configuration items and user permission will vary according to the user type.
- You can view linked Card/Tag and Wireless Keyfob of the user.

8. Optional: (Only for the administrator) Click **+** to add a user.

Card/Tag Management

After adding cards/tags to the wireless AX PRO, you can swipe the card/tag to arm or disarm all the detectors added to specific area(s) of the AX PRO, and silence alarms.

Note

The tag ID/PIN is a 32 bit long integer, and the variant could be 42949672956.

Steps

1. Enter the site, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **User Management** to enter the page.
3. Tap a user to enter the configuration page.
3. Tap **+** to add a tag/keyfob.
4. When hearing the voice prompt "Swipe Tag", you should present the tag on the AX PRO tag presenting area.
   - When hearing a beep sound, the tag is recognized.
   - The tag will be displayed on the tag list
5. Optional: Tap a tag to enter the configuration page.
6. Tap to edit the tag name.

Note

- If you log in as an installer, skip this step. Editing tag name is only available to administrator.
- The name should contain 1 to 32 characters.

7. Slide **Enable Tag**.
8. Select a linked user.
9. Select the tag type

Note

Different linked users have different tag permissions.

Operation Tag

You can swipe the tag to arm or disarm.

Patrol Tag

When you swipe the tag, the system will upload a record.

10. Optional: Tap **Delete** to delete the tag.

Device Information

You can change language and select time zone.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System → Configuration** to enter the page.
3. Select device language and time zone.

System Management

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System → System Options → System Management** to enter the page.

Panel Sound Prompt

If the option is enabled, the AX PRO will enable the voice prompt.
-System Volume: The available system volume range is from 0 to 10.
-Fault Prompts When Armed: Voice prompt of faults when the system is armed.
-Fault Prompts When Disarmed: Voice prompt of faults when the system is disarmed.
-Alarm Prompts: Voice prompt of faults when an alarm is triggered.

Panel LED Display

Enable/Disable panel functional LED.

Arm LED/Cloud LED

Enable arm/cloud LED indicator.

Fault LED Stays On When Armed

After arming, the fault indicator remains on.

System Alarm Duration

Set linked alarm voice prompt lasting time.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Bypass on Re-Arm

While enabled, after the detector is bypassed, if its faults are restored and the linked area is armed, the detector will automatically arm.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Motion Detector Restore

Motion detectors include all PIR detectors.
-Disable: No automatic restore.
-Immediate After Alarm: Motion detectors automatically restores immediately after the

alarm and reports to Cloud (for APP) and ARC.
-After Disarm: Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC

Power Saving Mode

While enabled, the main power supply is off, Wi-Fi enters low power consumption, 4G closes, tag reading fails, LED off, and voice prompt off.

Panel Fault Check

The fault check here is only for the control panel in the normal status.
The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System** → **System Options** → **Panel Fault Check** to enter the page.

Report Delay

If the fault returns to normal within the delay duration, no fault will be reported.

IP Camera Disconnection

This option only appears if a camera has been added to AX PRO.
If the option is enabled, when the linked network camera is disconnected, an alarm will be triggered. The delay time of network camera disconnection detection is the same as that of LAN.

Battery Lost

If the option is enabled, when panel battery is disconnected, the device will upload events.

Low Battery

If the option is enabled, when panel battery is in low battery status, the device will upload events.

LAN Lost

If the option is enabled, when the wired network is disconnected or with other faults, the alarm will be triggered.

WiFi Lost

If the option is enabled, when the Wi-Fi is disconnected or with other faults, the alarm will be triggered.

Cellular Lost

If the option is enabled, when the cellular data network is disconnected or with other faults, the alarm will be triggered.

Panel Mains Power Lost

If the option is enabled, an alarm will be triggered when the control panel main supply is disconnected.

Arming Options

This function is for the whole alarm system, to inform the user of the current system status before arming. If it is enabled, there will be a fault prompt and confirmation process for tag readers, keypads, keyfobs, and APP. If it is not enabled, there will be no fault detection before arming.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System → System Options → Arming Options** to enter the page.

You can set the following parameters:

Fault Checklist when Arming

Check the faults in the checklist, and you can manually stop arming if fault occurs.

Fault Voice Prompts on Arming

The system will make voice prompts when arming.

Fault Voice Prompts on Disarming

The system will make voice prompts when disarming.

3. Tap **Save**.

Enrollment Mode

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System → System Options → Enrollment Mode** to enter the page.
3. Tap **Enter the Enrollment Mode**. You can enroll the peripheral by triggering it.

Regional Certification

Tap → **System → System Options → Regional Certificate** to enter the page.

PD6662 is applicable to the UK market. If this function is enabled, the arming function and alarm logic of the control panel will change.

PD6662

Enable PD6662 standard. Functions that do not meet the standard will not take effect.

Communication Fault Sending Delay

The delay time while the ATP communication fault reports to ARC.

Network Camera

Add Cameras to the AX PRO

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Network Camera** → **Network Camera Channel** to enter the page.
3. Tap **+** → **Add Channel/SADP Scanning**.

   SADP Scanning

   Scan all network cameras in the same LAN. A list will pop up after scanning. You can directly check to add cameras in the list.
4. Enter IP address, port, the user name and password of the camera.
5. Tap **Save Icon**.
6. Optional: tap **Edit** or **Delete** to edit or delete the selected camera.

Set Video Parameters

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Network Camera** → **Event Video Settings** to enter the page.
3. Select a camera and set the video parameters.

   Stream Type

   Main Stream: Being used in recording and HD preview, it has a high resolution, code rate and picture quality.
   Sub-Stream: It is used to transmit network and preview pictures as a video streaming with features of lower resolution, bit rate and picture quality.

   Bitrate Type

   Select the Bitrate type as constant or variable.

   Resolution

   Select the resolution of the video output.

   Bitrate

   The higher value corresponds to the higher video quality, but the better bandwidth is required.

   Before Alarm

   The recording time length before the alarm.

   After Alarm

   The recording time length after the alarm.

Set Arming/Disarming Schedule

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **Area** to enter the page.
3. Tap an area in the list, enable the area and select linked devices.
4. Set parameters:

Late to Disarm

Enable the function and set the time. If the alarm is triggered after the configured time, the person will be considered as late.

Auto Arm

Enable the function and set the arming start time. The zone will be armed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Force Arm When System has Faults:
While the function is enabled, faults will be ignored when the system is automatically armed.
-Count Down Sound Prompt:
After enabled, the buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.
After disabled, the buzzer will not beep before auto arming.

Auto Disarm

Enable the function and set the disarming start time. The zone will be disarmed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Weekend Exception:
Enable the function and the zone will not be armed in the weekend.
-Holiday Exception:
Enable the function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling. Up to 12 holiday groups can be set.

Communication

Wired Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).

2. Tap → **Communication Parameters→ Wired Network** to enter the page.
3. Set the parameters.
   – Automatic Settings: Enable **DHCP** and set the HTTP port.
   – Manual Settings: Disabled **DHCP** and set IP Address, Subnet Mask, Gateway Address, DNS Server Address.
4. **Optional**: Set correct DNS server address if the device needs to visit Hik-Connect server via a domain name.
5. Click **Save**.

Wi-Fi Configuration

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Wi-Fi Configuration** to enter the page.
3. Tap a Wi-Fi to connect in the list.

Cellular Data Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Cellular Data Network Settings** to enter the page.
3. Enable **Cellular Data Network**.
4. Tap to select a SIM card. Tap **Parameter Configuration** → and set parameters including the user name, access password, APN, MTU and PIN code.
5. Tap .
6. Enable **Data Usage Limit**.
7. Edit **Data Used This Month** and **Data Limited per Month**.

Access Number

Input the operator dialing number.

Note

Only the private network SIM card user needs to enter the access number.

User Name

Ask the network carrier and input the user name.

Access Password

Ask the network carrier and input the password.

APN

Ask the network carrier to get the APN information and input the APN information.

Data Limited per Month

You can enable the function and 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.

Data Used This Month

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

Push Notifications

When an alarm is triggered, if you want to send the alarm notification to the mobile phone, you can set the notification push parameters.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Push Notification(s)** to enter the page.
3. Enable the target notification.

Zone Alarm

The device will push notifications when the zone alarm is triggered or the zone lid opened is triggered or restored.

Note

You need to set event filtering interval time for phone calling.

Zone Alarm

The device will push notifications when the zone alarm (on web client, software client or mobile client) is triggered or the zone peripherals alarm is triggered or restored.

Peripherals Lid Opened

The device will push notifications when lid opened alarm of any peripheral is triggered or restored.

Panel Lid Opened

The device will push notifications when lid opened alarm of the control panel is triggered or restored.

Keypad/Keyfob/APP Panic Alarm

The device will push notifications when panic alarm on keypads/keyfobs/APP is triggered or restored.

Keypad/Keyfob Medical Alarm

The device will push notifications when medical alarm on keypads or keyfobs is triggered.

Keypad Fire Alarm

The device will push notifications when fire alarm on keypads is triggered or a user presses the fire alarm key on the keypad.

Panel Status (Power and Battery)

The device will push notifications when the control panel power/battery status is changed.

Panel Status (Communication)

The device will push notifications when the control panel communication status is changed.

Zone Status

The device will push notifications when any zone status is changed.

Peripherals Status

The device will push notifications when any peripheral status is changed.

Panel Operation

The device will push notifications when the user operate the control panel.

Smart Alarm Event

The device will push notifications when alarm is triggered in network cameras(using HIKVISION protocol).

PIRCAM Gif

The video and pictures generated by PIR cameras will be uploaded to the alarm receiving center.

Video Clips

The video and pictures generated by network cameras will be uploaded to the alarm receiving center.

5. Tap **APP** and check events. The selected events will be pushed in the APP as important alarms.

ARC Disconnection Report Delay

The device will push notifications when Alarm Receiving Center is disconnected.

6. Tap **Phone Call and SMS**.
7. Tap **+** to enter the phone number.
8. Tap the added phone number to enable **Phone Call** and **SMS** according to your need.

Note

Do not configure the phone number to the SIM card inserted in the device itself, otherwise abnormal charges will occur and the user will have to bear them.

(For Phone Call) Set number of calling when the phone is unanswered.
(For SMS) Set Arming Permission, Disarming Permission and Silence Alarm Permission for areas.

Common Message

You can enter message content. When the alarm is triggered, your customized content will be added at the beginning of the message sent by the system.

Common Voice

You can import a new audio. When the alarm is triggered, your customized voice will be added at the beginning of the content of the phone dialed by the system. You can also tap Clear to delete audios

---

Note

Only WAV format is supported, up to 512 KB and 15 s.

---

9. Check notifications.

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. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Alarm Receiving Center (ARC)** to enter the page.
3. Select an ARC and enable it.

Protocol Type

Select the Protocol Type as ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID, CSV-IP, FSK Module or RDC Module to set uploading mode.

Intruder Verification as a Service

When the control panel uploads the alarm information, it will return the picture and video address for you to view.

Companies

Select the support company as None, Hungary-Multi Alarm Receiving Company or French Alarm Receiving Company.

Address Type

Select the Address Type as IP Address and Domain Name. Enter server address/domain name, port number and account code.

Transmission Mode

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

Retry Timeout Period

After the selected time, the system will retry to transmit.

Attempts

Set the number of retry attempts.

Polling Option

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.

GMT

Enable the Greenwich Mean Time.

Cloud Service Settings

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Cloud Service Settings** to enter the page.
3. Select the **Communication Mode**.

   Auto

   The connection priority order from high to low is: wired network, Wi-Fi, cellular data network.

   Wired &Wi-Fi

   The system will select wired network first. If no wired network detected, it will select Wi-Fi network.

   Cellular Data Network

   The system will select cellular data network only.
4. Enable **Periodic Test**. Enter the periodic test interval.
5. Tap **Save**.

Notification by Email

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Notification by Emails** to enter the page.
3. Enable **Email 1**.
4. Enter the sender name, sender email address, SMTP server address, SMTP port, user name and password.

Note

It is recommended to use Gmail and Hotmail for sending mails.
Only if the zone is linked with a network camera, the alarm email will be attached with alarm video.

5. Select the encryption type as **None**, **SSL** or **TLS**.
6. Enable **Server Authentication**.
7. Enter receiver name and receiver email address. Tap **Test Receiver Email Address** to test whether the email address is correct.
8. Tap **Save**.
9. Optional: Configure **Email 2** in the same order. You can choose whether to set email 2 as a backup mailbox.

Note

Video and picture reviews will be sent to both mailboxes. If Email 2 is set as a backup mailbox, the system will push emails to Email 2 only if Email 1 fails to receive.

FTP Settings

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ FTP Settings** to enter the page.
3. Select **Preferred FTP** or **Alternated FTP**, and enable FTP.
4. Configure the FTP parameters

Protocol Type

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

Server Address & Port

The FTP server address and corresponding port.

User Name & Password/Enable Anonymity

The FTP user should have the permission to upload pictures. If the FTP server supports picture uploading by anonymous users, you can enable anonymous to hide your device information during uploading.

Directory Structure

The saving path of snapshots in the FTP server.

4. Tap **Save**.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

Enable the UPnP function, and you don't need to configure the port mapping for each port, and the device is connected to the Wide Area Network via the router.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ NAT** to enter the page.
3. Drag the slider to **Enable UPnP**.
4. **Optional**: Select the mapping type as **Manual** to set the HTTP port and the service port.
5. Click **Save** to complete the settings

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

You should enroll an intercom sounder first.
Only one sounder can be set as the intercom sounder.

Steps

1. Tap → **Communication Parameters**→ **Intercom Service** to enter the page.
2. Slide to enable the function.
3. Set intercom type.

   SIP

   The control panel will use ARC and SIP server.

   IP Receiver Pro

   The control panel supports intercom of cloud service and ISUP protocol.

   ISUP

   The control panel uses the ISUP protocol through the Hik-Central APP.
4. Select an intercom sounder and tap **Save**.

Device Maintenance

Walk Test

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap →**Maintenance** → **Device Maintenance** to enter the maintenance page.
3. Tap **Test**, and tap **Start Walk Test** to test the whether the device works properly or not.

Maintenance

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap →**Maintenance** →**Maintenance**.

   Tamper Alarm on HPP Login

   If enabled, an alarm will be triggered when the device is tampered after you log in to HPP.

   Reboot Device

   The AX PRO will reboot.

   Log

   View device logs.

Device Upgrade

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Maintenance** → **Device Upgrade** to upgrade the control panel, or tap → **Maintenance** → **Detector & Peripheral Upgrade** to upgrade detectors and peripherals.

Remote Log Collection

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Maintenance** → **Remote Log Collection** to enable the function.

Remote Log Collection is for getting logs relating to the device. When this is enabled, our technical support will be able to collect logs relating to the device remotely and upload then to our server for troubleshooting. You can set the validity period according to actual needs. This function will be disabled after the set validity period.

5.1.2 Use the Hik-Partner Pro Portal

For AX PRO security control panel, you can perform operations including arming/disarming area, silence alarm, bypassing zone etc., and remotely configure the control panel on the Portal. You can also apply for PIN (required for upgrading the firmware of AX PRO) and switch the language of AX PRO.

Click **Site** to enter the site list page, and then click the name of a site to enter site details page.

Remotely Operate AX PRO

Click the AX PRO to open the operation panel. And you can perform the following operations.

Table 4-3 Operation Description

Operation	Description
Stay Arm a Specific Area	Select the **Area** tab, and then click **Stay Arming** to stay arm the area.
Away Arm a Specific Area	Select the **Area** tab and then click **Away Arming**.
Disarm a Specific Area	Select the **Area** tab and then click **Disarm**.
Stay Arm Multiple Areas	Select the **Area** tab, and then select areas and click .
Away Arm Multiple Areas	Select the **Area** tab, and then select areas and click .
Disarm Multiple Areas	Select the **Area** tab, and then select areas and click .
Silence Alarms of Multiple Areas	Select the **Area** tab, and then select areas and click
Filter Peripheral Device by	Select the **Device** tab, and then click and select an area to

Operation	Description
Area	only display the peripheral devices linked to the selected area, or select **All** to display all the peripheral devices linked to all the areas.
Control Relay	Select the **Device** tab, and then select a wireless output expander to display the sirens linked to it, and then select siren(s) to enable/disable them.
Bypass Zone	Select the **Device** tab, and then select a zone (i.e., detector) and turn on the **Bypass** switch to bypass the zone.

Remotely Configure AX PRO

You can click ⚙ to enter the web page of the security control panel to configure the device.

Note

For details about security control panel configuration, see the user manual of the device.

Apply for a PIN

You can click • • • → 🖹 to open the Apply for a PIN window, and then PIN code will be displayed.

Figure 5-5. Apply for PIN

Switch Language

Note

You should have applied for a PIN.

You can click • • • → ⇆ to open the Language window, and then set the device language and enter the PIN.

Figure 5-6. Switch Language

Health Monitoring

1. Enter the Hik-Partner Pro Portal web site, and click **Health Monitoring** → **Health Status** to enter the page.

2. Select a site.

Figure 5-7. Health Monitoring

3. Click **Health Check**, and click **Check Now**.

When checking is completed, you can view the status and reports of devices. You can also

export the report.

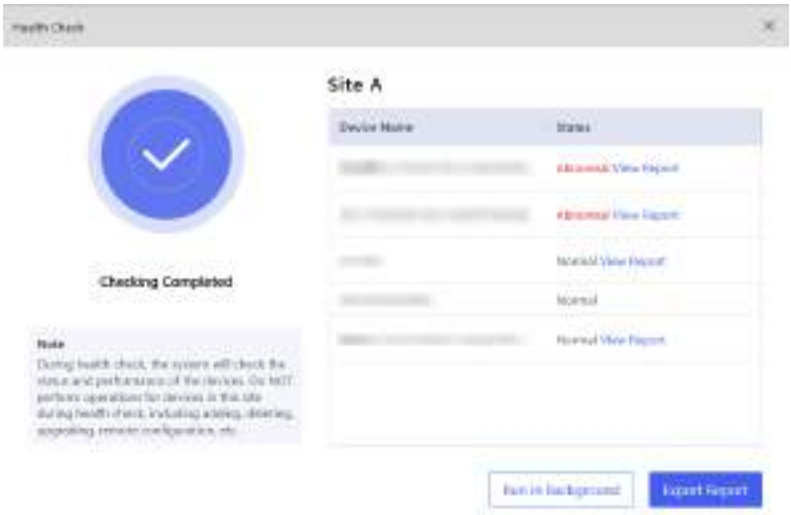


Figure 5-8. Checking Completed

4. Click to get the latest device status.

5.2 Set-up with Hik-Connect

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

Download and Login the Mobile Client

Download the Hik-Connect mobile client and login the client before operating the AX PRO.

Steps

1. Download Hik-Connect mobile client.
2. Optional: Register a new account if it is the first time you use the Hik-Connect mobile client.

Note

For details, see *User Manual of Hik-Connect Mobile Client*.

3. Run and login the client.

Add AX PRO to the Mobile Client

Add an AX PRO to the mobile client before other operations.

2. Select adding type.

Tap **+** → **Scan QR Code** to enter **Steps**

1. Power on the AX PRO.

the Scan QR code page. Scan the QR code on the AX PRO.

Note

Normally, the QR code is printed on the label stuck on the back cover of the AX PRO.

Tap **+** → **Manual Adding** to enter the Add Device page. Enter the device serial No. with the Hik-Connect Domain adding type.

3. Tap to search the device.
4. Tap **Add** on the Results page.
5. Enter the verification code and tap **OK**.
6. After adding completed, enter the device alias and tap **Save**.
7. Optional: Tap → **Delete Device** to delete the device.
8. Optional: Tap → to edit the device name.

Add Peripheral to the AX PRO

Add peripheral to the AX PRO.

Steps

1. Select a control device (AX PRO).
2. Tap **+** .
   - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the peripheral.
   - Tap to enter the Manually Input page. Enter the device serial No. and select the device type to add the device.

Main Page

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

On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.

Figure 5-9. Main Page

Enable Alarm

Tap to select **Audible Panic Alarm** or **Silent Panic Alarm**.

View Faults

Tap to view faults.

Area Management

Tap **+** to add an area.

Tap Area to enter the area management page. Refers to ***Set Arming/Disarming Schedule*** for details.

Arm/Disarm the Area

Arm or disarm the area manually as you desired.

On the device list page, tap the AX PRO and then log in to the device (if required) to enter the Area page.

Operations for a Single Area

Figure 5-10. Single Area

- **Away Arming**: Tap to away arm a single area. When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time.
- **Stay Arming:** Tap to stay arm a single area. When all the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection set in all the zones of all areas.

Operations for Multiple Areas

Figure 5-11. Multiple Area Key

- **Select Areas**: Tap to select areas you want to operate. If you do not select areas, following operations will take effect for all areas.
- **Away Arming**: Tap to away arm selected areas. When all the people in the detection area leave, turn on the Away mode to arm all zones in all areas after the defined dwell time.
- **Stay Arming**: Tap to stay arm all areas. When the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony) set in all the zones of all areas. At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.
- **Disarming**: Tap to disarm all areas. In Disarm mode, all the zones of all areas will not trigger alarm, no matter alarm events happen or not.
- **Silent Alarm**: Tap to silent alarms for all areas.

Zone Management

1. Tap **Device** to view linked zones.

Figure 5-12. Device Page

2. Tap **+** to add a new zone.
3. Tap a zone to enter the management page. You can view device status (e.g. temperature, battery status, single strength, etc.).
4. Tap on the upper right corner to enter the zone settings page.
5. Select a zone type.

You can view the configurable zone types for various detectors through ***I. Detector Zone Types***.

Instant Zone

This Zone type will immediately trigger an alarm event when armed.

Delay Zone

-Exit Delay Time: Exit Delay provides you time to leave through the zone without alarm. You should confirm faults first, and then the zone is in arming process. If the delay zone is triggered within the exit delay time but it restores before the time ends, the alarm will not be triggered and the zone will be armed.

-Entry Delay Time: Entry Delay provides you time to enter the zone to disarm the system without alarm.
After triggering, if the zone is not disarmed or silenced before the entry delay time ends, the zone will alarm.

-Stay Arm Delay Time: Stay arming uses Stay Arm Delay Time to count down.
The system gives Entry/Exit delay time when it is armed or reentered. It is usually used in entrance/exit route (e.g. front door/main entrance), which is a key route to arm/disarm via operating keypad for users.

Note

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

Panic Zone

24-hour active zone, whether armed or not. Report panic alarm after triggering. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

Medical Alarm

24-hour active zone, whether armed or not. Report medical alarm after triggering.

Fire Zone

24-hour active zone, whether armed or not. Report fire alarm after triggering.

Gas Zone

24-hour active zone, whether armed or not. Report gas alarm after triggering.

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise.

Keyswitch Zone

Trigger Type:

-By Trigger Time: Change the arming and disarming status after each trigger. For example, in the disarmed status, if the zone is triggered, the linked area will be armed. Trigger the zone again and the area will be disarmed.

-By Zone Status: You need to choose to arm or disarm the linked area after the zone is triggered.

In the case of the lid opened alarm, the arming and disarming operation will not be triggered.

Disabled

Zone disabled ignoring any alarm event. It is usually used to disable faulty detectors.

24-hour Zone

The zone activates all the time with sound/light output when alarm occurs, whether it is armed or not. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Timeout Zone

The zone activates all the time. When this zone has been triggered or restored and exceeds the set time, an alarm will be generated.

It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

-Not-Triggered Zone Alarm: If the zone is not triggered for the set time, it will alarm.

-Alarm on Zone Activated: If the zone is triggered for the set time, it will alarm.

-Retry Time Period: Set the timeout period.

6. Enable other parameters according to your actual needs.

Note

The supported functions vary depending on the zone types. Refer to the actual zone to set the function.

Arm Mode

If the zone is a public zone (the zone is belongs to more than one areas), you can set arm mode.

And: When all linked areas are armed, the zone will arm. When any of linked areas is disarmed, the zone will disarm.

Or: When any of the linked areas is armed, the zone will arm. When all linked areas are disarmed, the zone will disarm. When the zone is in alarm, the disarmed areas linked with the zone cannot be armed.

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

PD6662 is not enabled: You need to set the combined time interval.

When the first zone is triggered, the system will start timing after the zone is restored. If the second zone is triggered within the set time, both zones will give alarms. Otherwise, no alarm will be triggered.

If the first zone is not be restored, both zones will give alarms when the second zone is triggered, regardless of whether the set time has elapsed.

PD6662 is enabled: You need to set the combined time interval.

The first zone will give an alarm when triggered. If the first zone is not restored and the second zone is triggered, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is triggered within the set time, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is not triggered within the set time, no information will be reported.

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

After enabled, when an alarm is triggered, only the report will be uploaded and no sound is emitted.

Double knock

After enabled, the time interval can be set. If the same detector is triggered twice or continuously in a period of time, the alarm will be triggered.

Sounder Delay Time

The sounder will be triggered immediately (0s) or after the set time.

Final Door Exit

Only magnetic contacts have this option.
After enabling, when the user use keypads or tag readers to arm:
-Arm With Faults is enabled: During the arming countdown, if the magnetic contact is triggered and then restored, the arming process will be terminated immediately after restoring, and the arming is completed.
-Arm With Faults is disabled: If the magnetic contact is triggered and then restored, the linked area immediately arms the delayed zone.

AM Mode

-Alarm Only When ARM: Anti-masking alarm will be triggered only when the zone is armed.
-Alarm Only When ARM or DISARM: Anti-masking alarm will be triggered whether the zone is armed or disarmed.

Warning Time Enable

Set the warning time. The warning time countdown will be triggered if the instant zone is triggered during entry delay or the system not be disarmed after entry delay ends. Local alarms are generated during the period, but no messages will be pushed.

Swinger Limit Activations

When the number of times the infrared detector is triggered exceeds the set value, the alarm will no longer be triggered. (Except for anti-masking alarms.).

Dual Zone (Wired Zone)

After enabled, when multi transmitter detects that the entire zone circuit of the local zone and the extended zone is open circuit, both zones trigger lid opened alarms.

7. If required, link a PIRCAM or a camera for the zone.
8. Click **OK**.

View Status

Tap **Status** to view peripherals' status.

Bypass Zone

When the area is armed, you can bypass a particular zone as you desired.

Before You Start

Link a detector to the zone.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the Area page.
2. Tap **Device**.
3. Tap a zone in the Device tab.
4. Tap  to enter the Settings page.
5. Enable **Bypass** and the zone will be in the bypass status.

Bypass Status

The detector in the zone does not detect anything and you will not receive any alarm from the zone.

User Management

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

Note

There are three types of users for the AX PRO, including administrator (or owner), operator, and installer (or setter). Different types of users have different permissions for accessing the functionality of the AX PRO.

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the AX PRO page.
2. Tap to enter the Recipient Page.
3. Select a user to invite.
   - Scan QR code to invite a user.
   - Enter email address/mobile phone number to invite a user.
   - Select a user in the list.
4. Tap **Next** to invite the user.

Note

The recipient need to accept the invitation.

5. Tap → **User Management**.
6. Tap a user to enter the User Information Page.
7. Optional: Perform the following operations if required.

User Permission	You can tap the target user on the user list and then tap to set the permissions authorized to the target user. **Note** Only the administrator can do such an operation.
Linked Area	If the target user is an operator, tap the target user on the user list and then tap to set the area linked to the target user. **Note** Only the administrator can do such an operation.

Change Keypad Password	If the target user is an administrator, an installer or an operator, you can tap the target user on the user list and then tap **Change Keypad Password** to set the keypad password to the target user. **Note** The password (PIN code) is allowed to be 4 to 6 digits. No number is disallowed, with 10,000 to 100,000 differs, and no limit of the digit combination. After you add one keypad, you can add PIN code (Keypad Password) in the user menu. When you click in the input box, there will be indication shows that 4 to 6 numbers allowed. This is the same for each user
Change Duress Password	If the target user is an administrator or an operator, you can tap the target user on the user list and then tap **Change Duress Password** to set the duress password to the target user. **Note** If under duress, you can enter the duress code on the keypad to arm and disarm area(s) and upload a duress alarm.
Card/Tag/Keyfob	An administrator, an installer or an operator can use cards/tags or keyfob.

Note

- Configuration items and user permission will vary according to the user type.
- You can view linked Card/Tag and Wireless Keyfob of the user.

8. Optional: (Only for the administrator) Click **+** to add a user.

Card/Tag Management

After adding cards/tags to the wireless AX PRO, you can swipe the card/tag to arm or disarm all the detectors added to specific area(s) of the AX PRO, and silence alarms.

Note

The tag ID/PIN is a 32 bit long integer, and the variant could be 42949672956.

Steps

1. Enter the site, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **User Management** to enter the page.
3. Tap a user to enter the configuration page.
3. Tap **+** to add a tag/keyfob.
4. When hearing the voice prompt "Swipe Tag", you should present the tag on the AX PRO tag presenting area.
   - When hearing a beep sound, the tag is recognized.
   - The tag will be displayed on the tag list
5. Optional: Tap a tag to enter the configuration page.
6. Tap to edit the tag name.

Note

- If you log in as an installer, skip this step. Editing tag name is only available to administrator.
- The name should contain 1 to 32 characters.

7. Slide **Enable Tag**.
8. Select a linked user.
9. Select the tag type

Note

Different linked users have different tag permissions.

Operation Tag

You can swipe the tag to arm or disarm.

Patrol Tag

When you swipe the tag, the system will upload a record.

10. Optional: Tap **Delete** to delete the tag.

Device Information

You can change language and select time zone.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System** → **Configuration** to enter the page.
3. Select device language and time zone.

System Management

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System → System Options → System Management** to enter the page.

Panel Sound Prompt

If the option is enabled, the AX PRO will enable the voice prompt.
-System Volume: The available system volume range is from 0 to 10.
-Fault Prompts When Armed: Voice prompt of faults when the system is armed.
-Fault Prompts When Disarmed: Voice prompt of faults when the system is disarmed.
-Alarm Prompts: Voice prompt of faults when an alarm is triggered.

Panel LED Display

Enable/Disable panel functional LED.

Arm LED/Cloud LED

Enable arm/cloud LED indicator.

Fault LED Stays On When Armed

After arming, the fault indicator remains on.

System Alarm Duration

Set linked alarm voice prompt lasting time.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Bypass on Re-Arm

While enabled, after the detector is bypassed, if its faults are restored and the linked area is armed, the detector will automatically arm.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Motion Detector Restore

Motion detectors include all PIR detectors.
-Disable: No automatic restore.
-Immediate After Alarm: Motion detectors automatically restores immediately after the alarm and reports to Cloud (for APP) and ARC.
-After Disarm: Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC

Power Saving Mode

While enabled, the main power supply is off, Wi-Fi enters low power consumption, 4G closes, tag reading fails, LED off, and voice prompt off.

Panel Fault Check

The fault check here is only for the control panel in the normal status.
The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System** → **System Options** → **Panel Fault Check** to enter the page.

Report Delay

If the fault returns to normal within the delay duration, no fault will be reported.

IP Camera Disconnection

This option only appears if a camera has been added to AX PRO.
If the option is enabled, when the linked network camera is disconnected, an alarm will be triggered. The delay time of network camera disconnection detection is the same as that of LAN.

Battery Lost

If the option is enabled, when panel battery is disconnected, the device will upload events.

Low Battery

If the option is enabled, when panel battery is in low battery status, the device will upload events.

LAN Lost

If the option is enabled, when the wired network is disconnected or with other faults, the alarm will be triggered.

WiFi Lost

If the option is enabled, when the Wi-Fi is disconnected or with other faults, the alarm will be triggered.

Cellular Lost

If the option is enabled, when the cellular data network is disconnected or with other faults, the alarm will be triggered.

Panel Mains Power Lost

If the option is enabled, an alarm will be triggered when the control panel main supply is disconnected.

Arming Options

This function is for the whole alarm system, to inform the user of the current system status before arming. If it is enabled, there will be a fault prompt and confirmation process for tag readers,

keypads, keyfobs, and APP. If it is not enabled, there will be no fault detection before arming.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System** → **System Options** → **Arming Options** to enter the page.

You can set the following parameters:

Fault Checklist when Arming

Check the faults in the checklist, and you can manually stop arming if fault occurs.

Fault Voice Prompts on Arming

The system will make voice prompts when arming.

Fault Voice Prompts on Disarming

The system will make voice prompts when disarming.

3. Tap **Save**.

Enrollment Mode

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **System** → **System Options** → **Enrollment Mode** to enter the page.
3. Tap **Enter the Enrollment Mode**. You can enroll the peripheral by triggering it.

Regional Certification

Tap → **System** → **System Options** → **Regional Certificate** to enter the page.

PD6662 is applicable to the UK market. If this function is enabled, the arming function and alarm logic of the control panel will change.

PD6662

Enable PD6662 standard. Functions that do not meet the standard will not take effect.

Communication Fault Sending Delay

The delay time while the ATP communication fault reports to ARC.

Network Camera

Add Cameras to the AX PRO

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Network Camera** → **Network Camera Channel** to enter the page.

3. Tap **+ → Add Channel/SADP Scanning**.

SADP Scanning

Scan all network cameras in the same LAN. A list will pop up after scanning. You can directly check to add cameras in the list.

4. Enter IP address, port, the user name and password of the camera.
5. Tap **Save Icon**.
6. Optional: tap **Edit** or **Delete** to edit or delete the selected camera.

Set Video Parameters

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Network Camera → Event Video Settings** to enter the page.
3. Select a camera and set the video parameters.

Stream Type

Main Stream: Being used in recording and HD preview, it has a high resolution, code rate and picture quality.
Sub-Stream: It is used to transmit network and preview pictures as a video streaming with features of lower resolution, bit rate and picture quality.

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Bitrate

The higher value corresponds to the higher video quality, but the better bandwidth is required.

Before Alarm

The recording time length before the alarm.

After Alarm

The recording time length after the alarm.

Set Arming/Disarming Schedule

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **Area** to enter the page.
3. Tap an area in the list, enable the area and select linked devices.
4. Set parameters:

Late to Disarm

Enable the function and set the time. If the alarm is triggered after the configured time, the person will be considered as late.

Auto Arm

Enable the function and set the arming start time. The zone will be armed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Force Arm When System has Faults:
While the function is enabled, faults will be ignored when the system is automatically armed.
-Count Down Sound Prompt:
After enabled, the buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.
After disabled, the buzzer will not beep before auto arming.

Auto Disarm

Enable the function and set the disarming start time. The zone will be disarmed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Weekend Exception:
Enable the function and the zone will not be armed in the weekend.
-Holiday Exception:
Enable the function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling. Up to 12 holiday groups can be set.

Communication

Wired Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Wired Network** to enter the page.
3. Set the parameters.
   – Automatic Settings: Enable **DHCP** and set the HTTP port.
   – Manual Settings: Disabled **DHCP** and set IP Address, Subnet Mask, Gateway Address, DNS Server Address.
4. **Optional**: Set correct DNS server address if the device needs to visit Hik-Connect server via a domain name.
5. Click **Save**.

Wi-Fi Configuration

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Wi-Fi Configuration** to enter the page.
3. Tap a Wi-Fi to connect in the list.

Cellular Data Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Cellular Data Network Settings** to enter the page.
3. Enable **Cellular Data Network**.
4. Tap to select a SIM card. Tap **Parameter Configuration** → and set parameters including the user name, access password, APN, MTU and PIN code.
5. Tap .
6. Enable **Data Usage Limit**.
7. Edit **Data Used This Month** and **Data Limited per Month**.

Access Number

Input the operator dialing number.

Note

Only the private network SIM card user needs to enter the access number.

User Name

Ask the network carrier and input the user name.

Access Password

Ask the network carrier and input the password.

APN

Ask the network carrier to get the APN information and input the APN information.

Data Limited per Month

You can enable the function and 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.

Data Used This Month

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

Push Notifications

When an alarm is triggered, if you want to send the alarm notification to the mobile phone, you

can set the notification push parameters.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Push Notification(s)** to enter the page.
3. Enable the target notification.

Zone Alarm

The device will push notifications when the zone alarm is triggered or the zone lid opened is triggered or restored.

Note

You need to set event filtering interval time for phone calling.

Zone Alarm

The device will push notifications when the zone alarm (on web client, software client or mobile client) is triggered or the zone peripherals alarm is triggered or restored.

Peripherals Lid Opened

The device will push notifications when lid opened alarm of any peripheral is triggered or restored.

Panel Lid Opened

The device will push notifications when lid opened alarm of the control panel is triggered or restored.

Keypad/Keyfob/APP Panic Alarm

The device will push notifications when panic alarm on keypads/keyfobs/APP is triggered or restored.

Keypad/Keyfob Medical Alarm

The device will push notifications when medical alarm on keypads or keyfobs is triggered.

Keypad Fire Alarm

The device will push notifications when fire alarm on keypads is triggered or a user presses the fire alarm key on the keypad.

Panel Status (Power and Battery)

The device will push notifications when the control panel power/battery status is changed.

Panel Status (Communication)

The device will push notifications when the control panel communication status is changed.

Zone Status

The device will push notifications when any zone status is changed.

Peripherals Status

The device will push notifications when any peripheral status is changed.

Panel Operation

The device will push notifications when the user operate the control panel.

Smart Alarm Event

The device will push notifications when alarm is triggered in network cameras(using HIKVISION protocol).

PIRCAM Gif

The video and pictures generated by PIR cameras will be uploaded to the alarm receiving center.

Video Clips

The video and pictures generated by network cameras will be uploaded to the alarm receiving center.

5. Tap **APP** and check events. The selected events will be pushed in the APP as important alarms.

ARC Disconnection Report Delay

The device will push notifications when Alarm Receiving Center is disconnected.

6. Tap **Phone Call and SMS**.
7. Tap **+** to enter the phone number.
8. Tap the added phone number to enable **Phone Call** and **SMS** according to your need.

Note

Do not configure the phone number to the SIM card inserted in the device itself, otherwise abnormal charges will occur and the user will have to bear them.

(For Phone Call) Set number of calling when the phone is unanswered.
(For SMS) Set Arming Permission, Disarming Permission and Silence Alarm Permission for areas.

Common Message

You can enter message content. When the alarm is triggered, your customized content will be added at the beginning of the message sent by the system.

Common Voice

You can import a new audio. When the alarm is triggered, your customized voice will be added at the beginning of the content of the phone dialed by the system. You can also tap Clear to delete audios

Note

Only WAV format is supported, up to 512 KB and 15 s.

9. Check notifications.

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. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Alarm Receiving Center (ARC)** to enter the page.
3. Select an ARC and enable it.

Protocol Type

Select the Protocol Type as ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID, CSV-IP, FSK Module or RDC Module to set uploading mode.

Intruder Verification as a Service

When the control panel uploads the alarm information, it will return the picture and video address for you to view.

Companies

Select the support company as None, Hungary-Multi Alarm Receiving Company or French Alarm Receiving Company.

Address Type

Select the Address Type as IP Address and Domain Name. Enter server address/domain name, port number and account code.

Transmission Mode

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

Retry Timeout Period

After the selected time, the system will retry to transmit.

Attempts

Set the number of retry attempts.

Polling Option

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.

GMT

Enable the Greenwich Mean Time.

Cloud Service Settings

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ Cloud Service Settings** to enter the page.
3. Select the **Communication Mode**.

Auto

The connection priority order from high to low is: wired network, Wi-Fi, cellular data network.

Wired &Wi-Fi

The system will select wired network first. If no wired network detected, it will select Wi-Fi network.

Cellular Data Network

The system will select cellular data network only.

4. Enable **Periodic Test**. Enter the periodic test interval.
5. Tap **Save**.

Notification by Email

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Notification by Emails** to enter the page.
3. Enable **Email 1**.
4. Enter the sender name, sender email address, SMTP server address, SMTP port, user name and password.

Note

It is recommended to use Gmail and Hotmail for sending mails.
Only if the zone is linked with a network camera, the alarm email will be attached with alarm video.

5. Select the encryption type as **None**, **SSL** or **TLS**.
6. Enable **Server Authentication**.
7. Enter receiver name and receiver email address. Tap **Test Receiver Email Address** to test whether the email address is correct.
8. Tap **Save**.
9. Optional: Configure **Email 2** in the same order. You can choose whether to set email 2 as a backup mailbox.

Note

Video and picture reviews will be sent to both mailboxes. If Email 2 is set as a backup mailbox, the system will push emails to Email 2 only if Email 1 fails to receive.

FTP Settings

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **FTP Settings** to enter the page.

3. Select **Preferred FTP** or **Alternated FTP**, and enable FTP.
4. Configure the FTP parameters

Protocol Type

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

Server Address & Port

The FTP server address and corresponding port.

User Name & Password/Enable Anonymity

The FTP user should have the permission to upload pictures. If the FTP server supports picture uploading by anonymous users, you can enable anonymous to hide your device information during uploading.

Directory Structure

The saving path of snapshots in the FTP server.

4. Tap **Save**.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

Enable the UPnP function, and you don't need to configure the port mapping for each port, and the device is connected to the Wide Area Network via the router.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters→ NAT** to enter the page.
3. Drag the slider to **Enable UPnP**.
4. **Optional**: Select the mapping type as **Manual** to set the HTTP port and the service port.
5. Click **Save** to complete the settings

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

You should enroll an intercom sounder first.
Only one sounder can be set as the intercom sounder.

Steps

1. Tap → **Communication Parameters→ Intercom Service** to enter the page.
2. Slide to enable the function.
3. Set intercom type.

SIP

The control panel will use ARC and SIP server.

IP Receiver Pro

The control panel supports intercom of cloud service and ISUP protocol.

ISUP

The control panel uses the ISUP protocol through the Hik-Central APP.

4. Select an intercom sounder and tap **Save**.

Device Maintenance

You can reboot the device.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Maintenance** → **Reboot Device**. to enter the maintenance page.
   The AX PRO will reboot.
3. Tap → **Maintenance** → **Device Upgrade** to upgrade the control panel, or tap → **Maintenance** → **Detector & Peripheral Upgrade** to upgrade detectors and peripherals.
4. Optional: Tap → **Maintenance** → **Remote Log Collection** to enable the function.
   Remote Log Collection is for getting logs relating to the device. When this is enabled, our technical support will be able to collect logs relating to the device remotely and upload them to our server for troubleshooting. You can set the validity period according to actual needs. This function will be disabled after the set validity period.

Wi-Fi Connection

You can make the AX PRO connect to Wi-Fi through APP.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap → **Configure Wi-Fi Network**.
3. Follow the instructions on the page and change the AX PRO to the AP mode. Tap **Next**.
4. Select a stable Wi-Fi for the device to connect.
5. Back to configuration page to enter the Wi-Fi password and tap **Next**.
6. Tap **Connect to a network** and wait for connection.
   After the connection is completed, the AX PRO will prompt to exit AP mode and automatically switch to STA mode.

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.

Before You Start

- Make sure you have linked a zone with a detector.
- Make sure the zone is not bypassed.
- Make sure you have not enabled the silent zone function.

Steps

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

Figure 5-13. Notification Page

3. **Optional**: If the zone has linked a camera, you can view the playback when the alarm is triggered.
4. **Optional**: Tap to search events by dates or devices.

5.3 Set-up with the Web Client

Steps

1. Connect the device to the Ethernet.
2. Search the device IP address via the client software or the SADP software.
3. Enter the searched IP address in the address bar.
4. Use the activation user name and password to login.

Note

The user name and the password are the ones when activating via Hik-Connect or Hik-Partner Pro.

You can view the device, area, zone and so on status on the overview page.

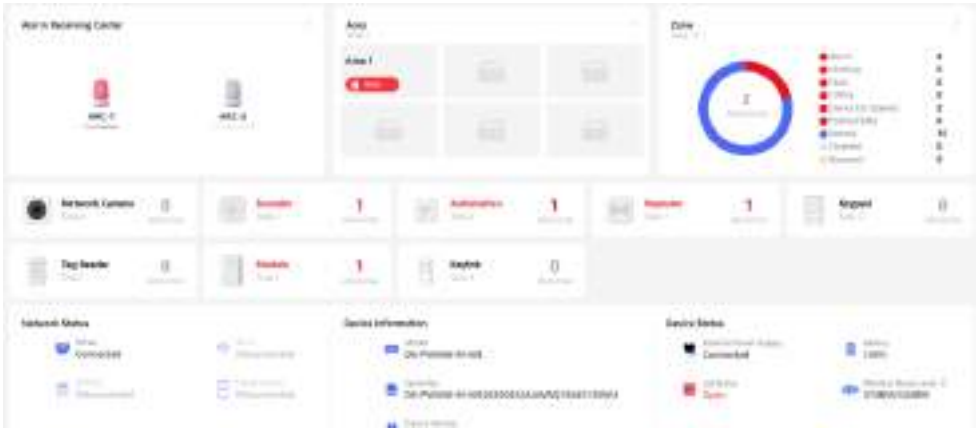


Figure 5-14. Web Main Page

5.3.1 User Management

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

Note

There are three types of users for the AX PRO, including administrator (or owner), operator, and installer (or setter). Different types of users have different permissions for accessing the functionality of the AX PRO.

Add User

Steps

1. Click **User Management** to enter the page.
2. Click **+Add**.
3. Configure the user parameters in the pop-up window on the right.

   Disposable User

   -Permanent: Permanent use. Configurable with full user permission.
   -One-Time User: Expired after arming or disarming once, or automatically expires after 24 hours. No duress code permission. No keyfobs and tags permission.

   Duress Code

   After entering the duress code, the system will upload the duress alarm to the alarm receiving center. No audible or visual alarm.
4. Click **Save** to add the user.

Edit User

Steps

1. Click **User Management** to enter the page.
2. Click to the right of a user to edit user parameters.

   User Parameters

   You can configure linked areas, the keypad password, the duress code and user permissions.

   Keyfob&Tag

   You can add, delete, enable or disable keyfobs and tags.
3. Click **Save**.

Delete User

Steps

1. Click **User Management** to enter the page.
2. Click to the right of a user to delete user parameters. You can also check users in the list and click **Delete** to delete users in batch.

Note

The administrator and the installer cannot be deleted.

5.3.2 Device Management

You can edit areas and manage the enrolled devices including detector, sounder, keypad, etc. in this section.

Area

You can set the area parameters on the page.

Steps

1. Click **Device Management** → **Area** to enter the page.
2. Click to the right of an area to enter the **Basic Information** page. Set parameters according to your actual needs.

Figure 5-15. Area

Late to Disarm Notification

Enable the function and set the time. If the alarm is triggered after the configured time, the person will be considered as late.

Enable Auto Arm

Enable the function and set the arming start time (Time Schedule). The zone will be armed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Force Arm When System has Faults:

While the function is enabled, faults will be ignored when the system is automatically armed.

-Count Down Sound Prompt:

After enabled, the buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.

After disabled, the buzzer will not beep before auto arming.

Enable Auto Disarm

Enable the function and set the disarming start time(Time Schedule). The zone will be disarmed according to the configured time.

Note

The auto arming time and the auto disarming time cannot be the same.

-Weekend Exception:
Enable the function and the zone will not be armed in the weekend.
-Holiday Exception:
Enable the function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling. Up to 12 holiday groups can be set.

3. Click **Save**.
4. Go to **Linked Zone/Detector** page and **Linked Peripheral** page to edit linkages of the area.

Device Enroll Mode

Click **Device Management** → **Mount Device** → **Device Enroll Mode** to enter the page. Slide the switch to enable the enrollment mode.

Zone

You can set the zone parameters on the zone page.

Steps

1. Click **Device Management → Mount Device → Zone** to enter the page.
   – Click ⚙ to view main device, channel No., zone type, silent alarm status, chime status, linked areas and linked cameras.
   – Click 📈 to view device status, battery status, signal strength, temperature & humidity and version.

Figure 5-16. Zone

2. Click **+Add** to add a zone.

Note

After adding a transmitter, you can add a wired zone.

3. Select a zone and click ✎ to enter the configuration page.

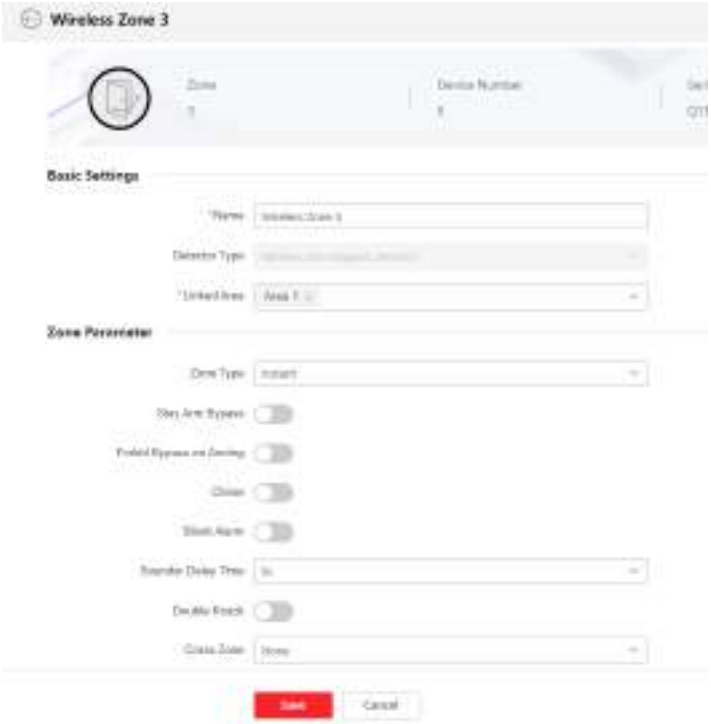


Figure 5-17. Zone Settings

4. Edit the zone name.
5. Check linked areas.

Note

- Only enabled areas will be listed.
- The newly added peripheral is linked to area 1 by default.

6. Select a zone type.

You can view the configurable zone types for various detectors through ***I. Detector Zone Types***.

Instant Zone

This Zone type will immediately trigger an alarm event when armed.

Delay Zone

-Exit Delay Time: Exit Delay provides you time to leave through the zone without alarm. You should confirm faults first, and then the zone is in arming process. If the delay zone is triggered within the exit delay time but it restores before the time ends, the alarm will not be triggered and the zone will be armed.

-Entry Delay Time: Entry Delay provides you time to enter the zone to disarm the system without alarm.
After triggering, if the zone is not disarmed or silenced before the entry delay time ends, the zone will alarm.

-Stay Arm Delay Time: Stay arming uses Stay Arm Delay Time to count down.

The system gives Entry/Exit delay time when it is armed or reentered. It is usually used in entrance/exit route (e.g. front door/main entrance), which is a key route to arm/disarm via operating keypad for users.

Note

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

Panic Zone

24-hour active zone, whether armed or not. Report panic alarm after triggering. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

Medical Alarm

24-hour active zone, whether armed or not. Report medical alarm after triggering.

Fire Zone

24-hour active zone, whether armed or not. Report fire alarm after triggering.

Gas Zone

24-hour active zone, whether armed or not. Report gas alarm after triggering.

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise.

Keyswitch Zone

Trigger Type:

-By Trigger Time: Change the arming and disarming status after each trigger. For example, in the disarmed status, if the zone is triggered, the linked area will be armed. Trigger the zone again and the area will be disarmed.

-By Zone Status: You need to choose to arm or disarm the linked area after the zone is triggered.

In the case of the lid opened alarm, the arming and disarming operation will not be triggered.

Disabled Zone

Zone disabled ignoring any alarm event. It is usually used to disable faulty detectors.

24-hour Zone

The zone activates all the time with sound/light output when alarm occurs, whether it is armed or not. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Timeout Zone

The zone activates all the time. When this zone has been triggered or restored and exceeds the set time, an alarm will be generated.

It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

-Not-Triggered Zone Alarm: If the zone is not triggered for the set time, it will alarm.

-Alarm on Zone Activated: If the zone is triggered for the set time, it will alarm.

-Retry Time Period: Set the timeout period.

7. Enable other parameters according to your actual needs.

Note

The supported functions vary depending on the zone types. Refer to the actual zone to set the function.

Arm Mode

If the zone is a public zone (the zone is belongs to more than one areas), you can set arm mode.

And: When all linked areas are armed, the zone will arm. When any of linked areas is disarmed, the zone will disarm.

Or: When any of the linked areas is armed, the zone will arm. When all linked areas are disarmed, the zone will disarm. When the zone is in alarm, the disarmed areas linked with the zone cannot be armed.

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

PD6662 is not enabled: You need to set the combined time interval.

When the first zone is triggered, the system will start timing after the zone is restored. If the second zone is triggered within the set time, both zones will give alarms. Otherwise, no alarm will be triggered.

If the first zone is not be restored, both zones will give alarms when the second zone is triggered, regardless of whether the set time has elapsed.

PD6662 is enabled: You need to set the combined time interval.

The first zone will give an alarm when triggered. If the first zone is not restored and the second zone is triggered, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is triggered within the set time, the system will report the alarm confirmation.

If the first zone is restored, the system will start timing. If the second zone is not triggered within the set time, no information will be reported.

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

After enabled, when an alarm is triggered, only the report will be uploaded and no sound is emitted.

Double knock

After enabled, the time interval can be set. If the same detector is triggered twice or

continuously in a period of time, the alarm will be triggered.

Sounder Delay Time

The sounder will be triggered immediately (0s) or after the set time.

Final Door Exit

Only magnetic contacts have this option.
After enabling, when the user use keypads or tag readers to arm:
-Arm With Faults is enabled: During the arming countdown, if the magnetic contact is triggered and then restored, the arming process will be terminated immediately after restoring, and the arming is completed.
-Arm With Faults is disabled: If the magnetic contact is triggered and then restored, the linked area immediately arms the delayed zone.

AM Mode

-Alarm Only When ARM: Anti-masking alarm will be triggered only when the zone is armed.
-Alarm Only When ARM or DISARM: Anti-masking alarm will be triggered whether the zone is armed or disarmed.

Warning Time Enable

Set the warning time. The warning time countdown will be triggered if the instant zone is triggered during entry delay or the system not be disarmed after entry delay ends. Local alarms are generated during the period, but no messages will be pushed.

Swinger Limit Activations

When the number of times the infrared detector is triggered exceeds the set value, the alarm will no longer be triggered. (Except for anti-masking alarms.).

Dual Zone (Wired Zone)

After enabled, when multi transmitter detects that the entire zone circuit of the local zone and the extended zone is open circuit, both zones trigger lid opened alarms.

8. If required, link a PIR camera or a camera for the zone.
9. Click **Save**.

Network Camera

You can add network cameras in the system.

Steps

1. Click **Device Management → Mount Device → Network Camera** to enter the page.
2. Click **+Add** to add a camera.

SADP Scanning

Scan all network cameras in the same LAN. A list will pop up after scanning. You can directly check to add cameras in the list.

3. Click to edit camera parameters.

Video Verification Report

Enable to report alarm video. When the control panel uploads the alarm information, it will

return the picture and video address for you to view. The number of channels that can be enabled depends on the device model.

4. Click to edit video parameters.

Stream Type

-Main Stream: Being used in recording and HD preview, it has a high resolution, code rate and picture quality.

-Sub-Stream: It is used to transmit network and preview pictures as a video streaming with features of lower resolution, bit rate and picture quality.

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Video Bitrate

The higher value corresponds to the higher video quality, but the better bandwidth is required.

Post-record/Pre-record

Set the recording video time before and after the alarm.

5. Click **Save**.

Sounder

The sounder is enrolled to the AX PRO via the wireless receiver module, and the 868 Mhz wireless sounder can be enrolled to the hybrid AX PRO via the wireless receiver that is at the address of 9.

Steps

1. Click **Device Management → Mount Device → Sounder** to enter the page.
   - Click to view the sounder type, linked areas and alarm volume.
   - Click to view the device status, battery status, device temperature, signal strength, main power status and version.
2. Click **+Add** to add a sounder.
3. Click to edit sounder parameters.

Figure 5-18. Sounder Settings

Linked Area

Only enabled areas will be listed.

The newly added peripheral is linked to area 1 by default.

Alarm Volume

The available alarm volume range is from 0 to 3 (function varies according to the model of device).

Alarm Strobe Flash

Enable alarm strobe light.

Alarm Duration

The available alarm duration range is from 10 to 900 s.

Alarm Buzzer

Enable alarm buzzer.

Lid Open When Disarmed

When the linked area is disarmed, there is a lid opened alarm triggered by a peripheral, and the sounder will also be triggered.

Arm/Disarm Indicator

Enable arm/disarm LED indicator.

Arm/Disarm Buzzer

Enable arm/disarm buzzer.

Buzzer Indicator on Delay Zone

When the area entry delay or exit delay, in addition to the control panel, the sounder will also give an alarm.

Polling Rate

Sets the interval at which the system requires the device to return a report. If the device

takes longer than the **Polling failure Times to determine offline** to reply, the system will report faults and the status of device will be shown as offline.

Intercom Service

Enable intercom service. Only one sounder can enable this function.

4. Click **Save**.

Automation

You can set the parameters of the relay outputs that is enrolled to the AX PRO.

Steps

1. Click **Device Management → Mount Device → Automation** to enter the page.
   – Click to view the main device, channel number, linked areas and linked events.
   – Click to view the device status, device temperature, voltage, current, power load, energy consumed, signal strength and version.
2. Click **+Add** to add a relay output device.
3. Click to edit the device parameters.

Linked Area

Only enabled areas will be listed.
The newly added peripheral is linked to area 1 by default.

Original Status

Set the device original status to normally open or normally closed.

Tamper Input

When enabled, the tamper-proof function of the device can be detected (if available).

Voltage Protection

When enabled, an exception event will be reported when the voltage is too high or too low.

For Linked Event:

Event Type

Set the status of the device when various events are triggered.

Activation Mode

-Pulse: The device changes to contact status after the trigger and restores to original status after the set pulse duration.
-Latch: The device changes to the contact status after the trigger and does not restore the original status.

Contact Status

Set the device status after being triggered.

4. Click **Save**.

Repeater

The repeater can amplify signals between the control panel and the peripherals.

Steps

1. Click **Device Management → Mount Device → Repeater** to enter the page.
   - Click ⚙ to view the serial number and linked device number.
   - Click 📈 to view the device status, battery status, signal strength, main power and version.
2. Click **+Add** to add a repeater.
3. Click **Enable Paring Mode(Cam-X)** to make the repeater enter the mode of device paring. When the distance between the peripheral and the control panel is far, the repeater can be used as a transfer station for pairing. The pairing mode lasts for 3 minutes and cannot be interrupted. After the pairing is successful, a list of connected devices will be displayed.
4. Click ✎ to edit the repeater parameters.

Figure 5-19. Repeater Settings

5. Click ⚙ to enter the **Manual Retransmission Rules** page.

Figure 5-20. Manual Retransmission Rules

6. Select devices in the list and click **OK**, and then the devices can be manually retransmitted.

Module/Transmitter

You can set the parameters of the transmitter.

Steps

1. Click **Device Management → Mount Device → Module** to enter the page.
   - Click ⚙ to view the serial number and linked device number.
   - Click 📈 to view the device status, battery status, signal strength, main power and version.

2. Click **+Add** to add a module.
3. Click to edit the device parameters.

Linked Area

Only enabled areas will be listed.
The newly added peripheral is linked to area 1 by default.

4. Click **Save**.

Keypad

You can set the parameters of the keypad that is enrolled to the AX PRO.

Steps

1. Click **Device Management → Mount Device → Keypad** to enter the page.
   - Click to view the linked areas, function buttons, alarm buzzer and button buzzer status.
   - Click to view the device status, temperature, battery status, signal strength and version.
2. Click **+Add** to add a keypad.
3. Click to edit the keypad parameters.

Figure 5-21. Keypad Settings

Linked Area

Only enabled areas will be listed.
The newly added peripheral is linked to area 1 by default.

Function Buttons

After disabling, fire alarm, medical alarm and panic alarm button will not work.

Arming Without Password

You can directly press the arm button to arm without entering a password.

Keypad Awake Time

If the keypad has no action within the set time, it will sleep automatically.

Active on Entry Delay

When enabled, the keypad can be used during the entry delay.

Chime Indication

Enable chime.

Area Status

Display area status and alarm information in the keypad main page.

Remote Arm/Disarm Indication

Enable the remote arm/disarm LED indication.

Polling Rate

Sets the interval at which the system requires the device to return a report. If the device takes longer than the **Polling failure Times to determine offline** to reply, the system will report faults and the status of device will be shown as offline.

Backlight

Enable the keypad backlight. You can configure the time schedule when the backlight is off.

Alarm Buzzer/Button Buzzer

Enable the alarm buzzer/button buzzer.

Silent Panic Alarm/Silent Medical Alarm

Panic alarm/Medical alarm do not sound.

Text1/Text2

The text displayed on the main page when waking up. Customizable content.

4. Click **Save**.

Tag Reader

You can set the parameters of the tag reader.

Steps

1. Click **Device Management → Mount Device → Tag Reader** to enter the page.
2. Click **+Add** to add a tag reader.
3. Click  to edit the tag reader parameters.

Figure 5-22. Tag Reader Settings

Linked Area

Only enabled areas will be listed.
The newly added peripheral is linked to area 1 by default.

Operation Mode

-Standard Mode: Area selection and fault confirmation are supported when arming or disarming. You should set the authorization method.
-Simple Mode: No Area selection and fault confirmation when swiping tag to arm or disarm.

Polling Rate

Sets the interval at which the system requires the device to return a report. If the device takes longer than the **Polling failure Times to determine offline** to reply, the system will report faults and the status of device will be shown as offline.

4. Click **Save**.

Keyfob

You can add keyfob to the AX PRO and control the AX PRO via the keyfob. You can also edit the keyfob information or delete the keyfob from the AX PRO.

Steps

1. Click **Device Management → Mount Device → Keyfob** to enter the page.
2. Click **+Add** to add a keyfob.
3. Click to edit the keyfob parameters.

Enable

Enable the keyfob or not.

Linked Area

Only enabled areas will be listed.
The newly added peripheral is linked to area 1 by default.

Button Configuration

Configure the functions of single keys and key combinations.

4. Click **Save**.

5.3.3 System

System Settings

You can view device information and configure device time.

Basic Information

Click **Configuration → System → System Settings → Basic Settings**
You can edit the device name and view device information here.

Time Settings

You can set the device time zone, synchronize device time, and set the DST time. The device supports time synchronization via Hik-Connect server.
Click **Configuration → System → System Settings → Time Settings** to enter the page.

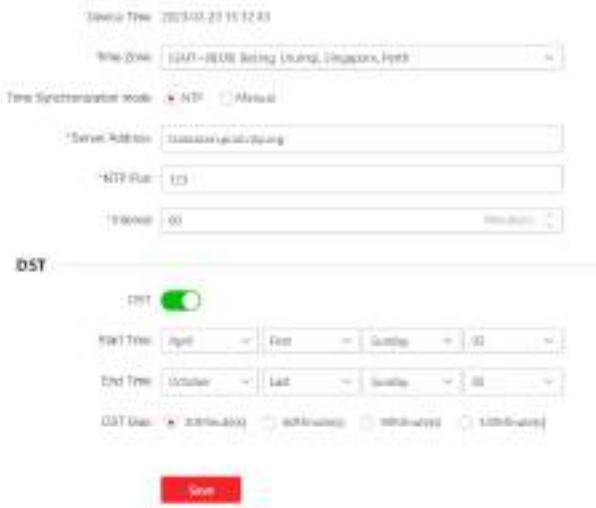


Figure 5-23. Time Settings

Time Zone

Select a time zone from the drop-down list.

Time Synchronization mode

-NTP: Set the server address, NTP port and interval. The system will automatically synchronize the time with the server.
-Manual: Set the system time manually or click **Sync. with Computer Time** to synchronize the device time with the computer time.

DST

Set the start, end date and bias time for daylight saving time.

Click **Save**.

Control Panel Options

Option Management

Set the authority options.

Click **Configuration → System → Control Panel Option → Option Management** to enter the page.

Figure 5-24. Option Management

Panel Sound Prompt

Enable/Disable sound prompt. Set the sound volume and trigger events.

Panel LED Display

Enable/Disable panel functional LED.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm. Regardless of whether it is enabled or not, the tamper alarm will be normally pushed to Cloud (for APP) and ARC.

Bypass on Re-Arm

While enabled, the bypassed zone will back to arm if fault restored.

Jamming Sensitivity Settings

The device will detect RF interference and push messages when the RF interference interferes with communication. You can adjust the detection sensitivity.

Motion Detector Restore

Motion detectors include all PIR detectors.

-Disable: No automatic restore.

-Immediate After Alarm: Motion detectors automatically restores immediately after the alarm and reports to Cloud (for APP) and ARC.

-After Disarm: Motion detectors automatically restores after disarming and reports to Cloud (for APP) and ARC.

Energy Save Mode

While enabled, the main power supply is off, Wi-Fi enters low power consumption, 4G closes, tag reading fails. LED is off, and voice prompt is off.

Panel Lockup Button

All functions of AX PRO will be frozen after it is enabled. This function can only be enabled by users with installer permission.

Click **Save**.

Panel Fault Check

The fault check here is only for the control panel in the normal status.
The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.
Click **Configuration → System → Control Panel Option → Panel Fault Check** to enter the page.

Figure 5-25. Panel Fault Check

Report Delay

If the fault returns to normal within the delay duration, no fault will be reported.

Battery Lost

If the option is enabled, when battery is disconnected, the device will upload events.

Low Battery

If the option is enabled, when battery is in low battery status, the device will upload events.

LAN Lost

If the option is enabled, when the wired network is disconnected or with other faults, the alarm will be triggered.

Wi-Fi Lost

If the option is enabled, when the Wi-Fi is disconnected or with other faults, the alarm will be triggered.

Cellular Lost

If the option is enabled, when the cellular data network is disconnected or with other faults,

the alarm will be triggered.

Panel Main Power Lost

If the option is enabled, an alarm will be triggered when the control panel main supply is disconnected.

To compliant the EN 50131-3, the report dealy duration should be 10 s.

Click **Save**.

Arming Options

This function is for the whole alarm system, to inform the user of the current system status before arming. If it is enabled, there will be a fault prompt and confirmation process for tag readers, keypads, keyfobs, and APP. If it is not enabled, there will be no fault detection before arming.

Click **Configuration → System → Control Panel Option → Arming Options** to enter the page.

Figure 5-26. Arming Options

You can set the following parameters:

Fault Checklist when Arming

The system will check if the device has the faults in the checklist during the arming process.

Fault Voice Prompts on Arming

The system will make voice prompts when arming.

Fault Voice Prompts on Disarming

The system will make voice prompts when disarming.

Regional Certification

Click **Configuration → System → Control Panel Option → Regional Certificate** to enter the page.

PD6662 is applicable to the UK market. If this function is enabled, the arming function and alarm logic of the control panel will change.

PD6662

Enable PD6662 standard. Functions that do not meet the standard will not take effect.

Communication Fault Sending Delay

The delay time while the ATP communication fault reports to ARC.

Network Configuration

TCP/IP

You can set the device IP address and other network parameters.

Steps

Note

Functions varied depending on the model of the device.

1. Click **Configuration → Network → Network Configuration → TCP/IP** to enter the page.

Figure 5-27. TCP/IP

2. Set the parameters.
   - Automatic Settings: Enable **DHCP**.
   - Manual Settings: Disabled **DHCP** and set other parameters.
3. Click **Save**.

Wi-Fi

Steps

1. Click **Configuration → Network → Network Configuration → Wi-Fi** to enter the page. You can view STA/AP Switch Status here.
2. Set the parameters.
   - Automatic Settings: Enable **DHCP**.
   - Manual Settings: Disabled **DHCP** and set other parameters.
3. Click **Save**.

Cellular Data Network

Set the cellular network parameters if you insert a SIM card inside the device. By using the cellular network, the device can upload alarm notifications to the alarm center.

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

5. Click **Configuration → Network → Network Configuration → Cellular Data Network** to enter the page.

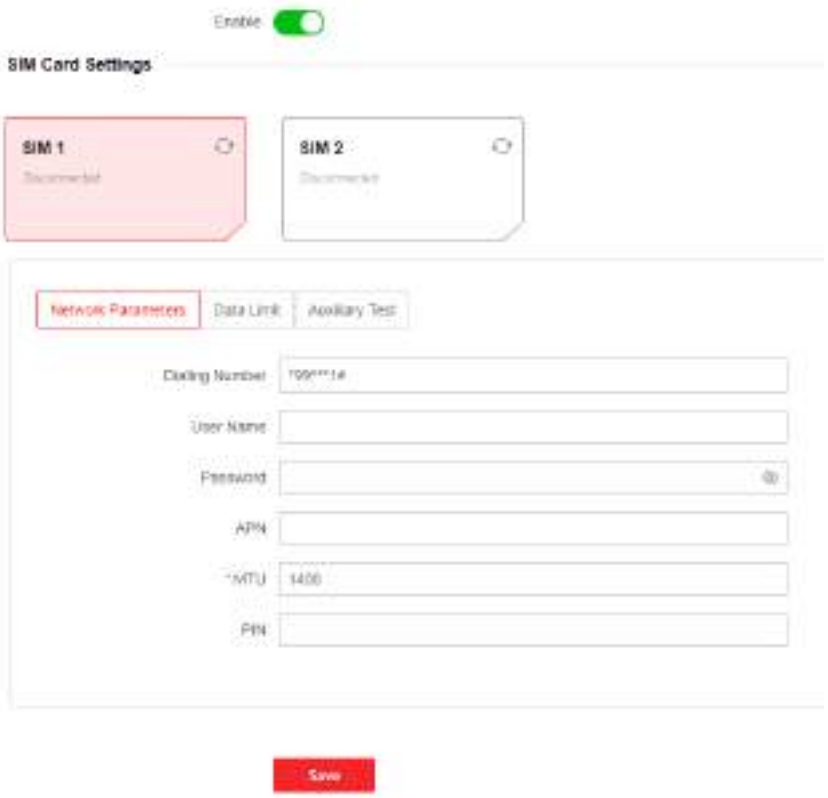


Figure 5-28. Cellular Data Network

6. Enable the function.
7. Set the cellular data network parameters.

Dialing Number

Enter the operator dialing number.

Note

Only the private network SIM card user needs to enter the dialing number.

User Name

Ask the network carrier and enter the user name.

Password

Ask the network carrier and enter the password.

APN

Ask the network carrier to get the APN information.

Data Limit

You can enable the function and set the data threshold every month.

Used Traffic This Month

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

Traffic Threshold

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

Network Connection Test

Click **Test** to check network connection status.

8. Click **Save**.

Network Service

HTTP(S)

Click **Configuration → Network → Network Service → HTTP(S)** to enter the page.
You can set HTTP port here.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.
Enable the UPnP function, and you don’t need to configure the port mapping for each port, and the device is connected to the Wide Area Network via the router.

1. Click Configuration → Network → Network Service → NAT to enter the page.

Port Mapping Mode

-Auto: Get the port number automatically.
-Manual: You need to enter external ports.

2. Click **Save**.

Device Access

If you want to enroll the device to the mobile client for remote configuration, you should set the mobile client enrollment parameters.

Before You Start

- Connect the device to the network via wired connection, dial-up connection, or Wi-Fi connection.

- Set the device IP address, subnet mask, gateway and DNS server in the LAN.

Steps

1. Click **Configuration → Network → Device Access** to enter the page.

Figure 5-29. Device Access

2. Drag the slider to enable the function.

Note

By default, the device Hik-Connect service is enabled.

You can view the device status in the Hik-Connect server (www.hik-connect.com).

3. The server address is already displayed in the Server Address box, or you can check **Custom** to edit it.
4. Optional: Change the verification code.

Note

- By default, the verification code is displayed in the text box.
- The verification code should contain 6 to 12 letters or digits. For security reasons, an 8-character password is suggested, which containing two or more of the following character types: uppercases, lowercases, and digits.

5. Select a network mode from the drop-down list according to the actual needs.

Auto

The connection priority order from high to low is: wired network, Wi-Fi, cellular data network.

Wired &Wi-Fi

The system will select wired network first. If no wired network detected, it will select Wi-Fi network.

Cellular Data Network

The system will select cellular data network only.

6. Enable **Periodic Test**. Enter the periodic test interval.

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.

7. Click **Save**.

Alarm Receiving Center

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

Steps

1. Click **Configuration → Alarm Communication → Alarm Receiving Cente**r to enter the page.

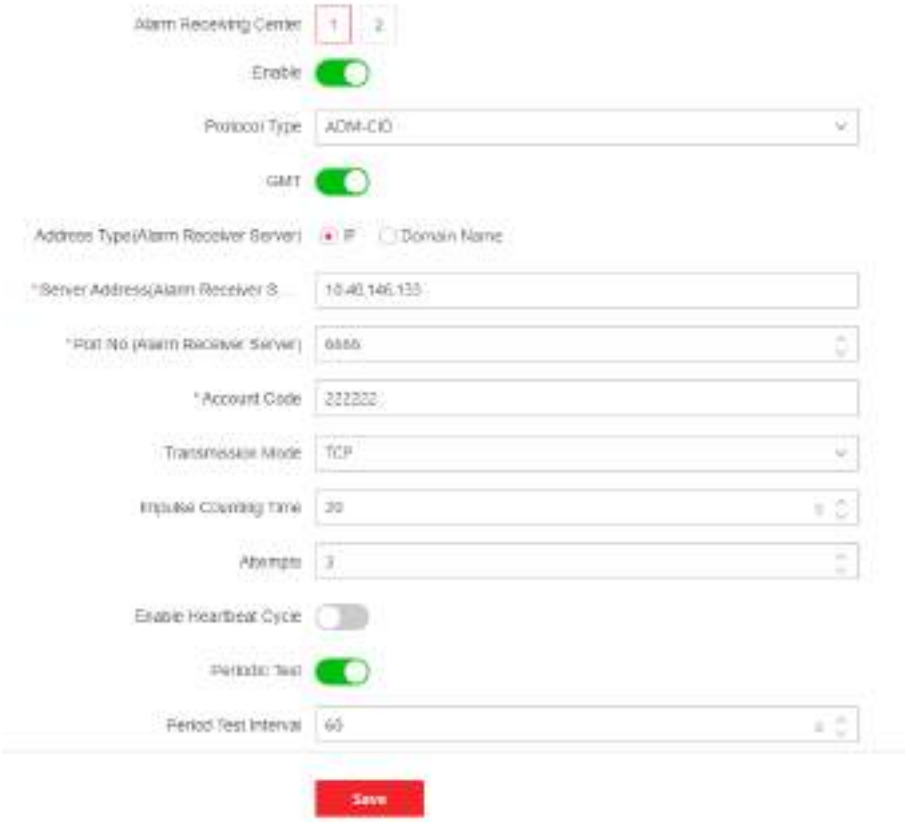


Figure 5-30. Alarm Receiving Center

2. Select the **Alarm Receiving Center** as **1** or **2** for configuration, and slide the slider to enable the selected alarm receiving center.

Note

Only if the alarm receiving center 1(ARC1) is enabled, you can set the alarm receiver center 2 as the **backup channel** and edit the channel parameters.

3. Select the Protocol Type as ADM-CID, ISUP, SIA-DCS, *SIA-DCS, *ADM-CID, CSV-IP, FSK Module or RDC Module to set uploading mode.

Note

Standard DC-09 Protocol
ADM-CID: The data presenting method of DC-09 is CID, which is not encrypted and only for uploading alarm report.
*ADM-CID: The data presenting method of DC-09 is CID, which is encrypted and only for uploading alarm report.
SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is not encrypted and only for uploading alarm report.
*SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is encrypted and only for uploading alarm report.

- **ADM-CID** or **SIA-DCS:** You should select the **Address Type** as **IP** or **Domain name**, and set the server address, port number, account code, impulse counting time, attempts, polling rate.
- **ISUP, CSV-IP, FSK and RDC:** You do not need to set the protocol parameters.
- ***SIA-DCS** or ***ADM-CID** You should select the **Address Type** as **IP** or **Domain name**, and set the server address, port number, account code, impulse counting time, attempts, encryption arithmetic, password length and secret key.

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.

4. Click **Save**.

Use PIRCAM to Upload Pictures or Videos

You can enable the PIRCAM function to upload pictures or videos.

1. Upload Pictures
   You can choose to upload 1 to 20 pictures.
   (1) Click **Configuration → Alarm Communication → Alarm Receiving Cente**r to enter the page.
   (2) Slide the slider to enable the selected alarm receiving center.
   (3) Select the **Protocol Type** as **SIA-DCS**.
   (4) Select the **Companies** as **French Alarm Receiving Company**.
   (5) Select to upload videos or pictures
   (6) Click **Save**.

Figure 5-31. Upload Video and Picture

2. Configure SMTP parameters:
   (1) Click **Configuration → Alarm Communication → Notification by Email**.
   (2) Slide to enable the function and set corresponding parameters. For details, see Notification by Email. Click **Save**.
3. Configure FTP parameters:
   (1) Click **Configuration → Alarm Communication → FTP** to enter the page.
   (2) Slide to enable FTP and set corresponding parameters. For details, see FTP. Click **Save**.
4. Upload Videos
   In this condition, when the PIRCAM is set to catch more than two pictures, videos will be uploaded.
   (1) Click **Configuration → Alarm Communication → Alarm Receiving Center** to enter the page.
   (2) Slide the slider to enable the selected alarm receiver center.
   (3) Select the **Protocol Type** as **SIA-DCS**.
   (4) Click **Save**.
   (5) Configure SMTP or FTP parameters as same as Upload Photos.

Event Notification

When an alarm is triggered, if you want to send the alarm notification to the client, alarm center, cloud or mobile phone, you can set the notification push parameters.

Alarm Receiving Center

Steps

1. Click **Configuration → Alarm Communication → Event Notification → Alarm Receiving Center**.

Figure 5-32. ARC(Notification)

2. Select one alarm receiving center.
3. Enable the target notification.

Zone Alarm

The device will push notifications when the zone alarm (on web client, software client or mobile client) is triggered or the zone peripherals alarm is triggered or restored.

Peripherals Lid Opened

The device will push notifications when lid opened alarm of any peripheral is triggered or restored.

Panel Lid Opened

The device will push notifications when lid opened alarm of the control panel is triggered or restored.

Keypad/Keyfob/APP Panic Alarm

The device will push notifications when panic alarm on keypads/keyfobs/APP is triggered or restored.

Keypad/Keyfob Medical Alarm

The device will push notifications when medical alarm on keypads or keyfobs is triggered.

Keypad Fire Alarm

The device will push notifications when fire alarm on keypads is triggered or a user presses the fire alarm key on the keypad.

Panel Status (Power and Battery)

The device will push notifications when the control panel power/battery status is changed.

Panel Status (Communication)

The device will push notifications when the control panel communication status is changed.

Zone Status

The device will push notifications when any zone status is changed.

Peripherals Status

The device will push notifications when any peripheral status is changed.

Panel Operation

The device will push notifications when the user operate the control panel.

Smart Alarm Event

The device will push notifications when alarm is triggered in network cameras(using HIKVISION protocol).

PIRCAM Gif

The video and pictures generated by PIR cameras will be uploaded to the alarm receiving center.

Video Clips

The video and pictures generated by network cameras will be uploaded to the alarm receiving center.

4. Click **Save**.

APP

Steps

1. Click **Configuration → Alarm Communication → Event Notification → APP**.
2. You need to set if it is important alarm. Refer to *Alarm Receiving Center* for detailed event description.

Important Alarm

When the APP is in silent mode, the push items set as important alarm will still play the corresponding voice prompts. Fire, medical, and panic alarms are configured as important alarms by default.

ARC Disconnection Report Delay

The device will push notifications when Alarm Receiving Center is disconnected.

Note

This configuration item is valid only when ARC is configured as ISUP protocol.

Figure 5-33. APP(Notification)

3. Click **Save**.

Phone Call and SMS

Send the alarm notifications to phones.

Steps

1. Click **Configuration → Alarm Communication → Event Notification → Phone Call and SMS**.
2. Click **+Add**.
3. Enter the phone number that receives the notification. You can set the system to send the alarm notifications through **Voice Call** or **SMS**.

Note

Do not configure the phone number to the SIM card inserted in the device itself, otherwise abnormal charges will occur and the user will have to bear them.

Filtering Interval Time

The interval between calls for the same alarm.

Dialing Time

The number of times the system repeatedly dials when the call is unanswered.

Push Event Type

Refer to *Alarm Receiving Center* for detailed event description.

4. Click **Save** to add the phone number.
5. Set contents of the voice call and SMS.

Common Voice

When the alarm is triggered, your customized voice will be added at the beginning of the content of the phone dialed by the system.

Common Message

When the alarm is triggered, your customized content will be added at the beginning of the message sent by the system.

Notification by Email

You can send the alarm video or event to the configured email.

Steps

1. Click **Configuration → Alarm Communication → Notification by Email** to enter the page.
2. Select and enable Email **1**.
3. Enable **Server Authentication**.
4. Enter the sender's information.

Note

- It is recommended to use Gmail and Hotmail for sending mails.
- Only if the zone is linked with a network camera, the alarm email will be attached with alarm video.

5. Enter the receiver's information.
6. Click **Receiver Address Test** and make sure the address is correct.
7. Click **Save**.
8. Optional: Configure Email **2** in the same order. You can choose whether to set email 2 as a backup mailbox.

Note

Video and picture reviews will be sent to both mailboxes. If Email 2 is set as a backup mailbox, the system will push emails to Email 2 only if Email 1 fails to receive.

FTP

You can configure the FTP server to save alarm video.

Steps

1. Click **Configuration → Alarm Communication → FTP** to enter the page.
2. Configure the FTP parameters

FTP Type

Set the FTP type as main used or alternated.

Protocol Type

FTP and SFTP are selectable. The files uploading is encrypted by using SFTP protocol.

Server Address and Port

The FTP server address and corresponding port.

Anonymity

The FTP user should have the permission to upload pictures. If the FTP server supports picture uploading by anonymous users, you can enable Anonymity to hide your device information during uploading. Otherwise, you should enter user information.

Directory Structure

The saving path of snapshots in the FTP server.

3. Click **Save**.

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

You should enroll an intercom sounder first.
Only one sounder can be set as the intercom sounder.

Steps

1. Click **Configuration → Alarm Communication → Intercom Service** to enter the page.
2. Slide to enable the function.
3. Set intercom type.

   SIP

   The control panel will use ARC and SIP server.

   IP Receiver Pro

   The control panel supports intercom of cloud service and ISUP protocol.

   ISUP

   The control panel uses the ISUP protocol through the Hik-Central APP.
4. Set parameters.

   Alarm Verify Priority

   Select picture or audio first.
5. Select a sounder and click **Save**.

5.3.4 Maintenance and Security

Maintenance

Restart

Click **Maintenance and Security → Maintenance → Restart** to enter the page.
Click **Restart** to restart the device.

Control Panel Upgrade

1. Click **Maintenance and Security → Maintenance → Control Panel Upgrade** to enter the page.
2. Click  to find the firmware file with the name digicap.dav.
3. Click **Upgrade** to complete.

Detector & Peripheral Upgrade

1. Click **Maintenance and Security → Maintenance → Detector & Peripheral Upgrade** to enter the page.
2. Select the Upgrade Type and the Peripheral.
3. Click  to find the firmware upgrade file.

4. Click **Upgrade** to complete.

Note

Both of the users and configuration information will be retained after upgrade finished.

System Maintenance

You can restore default settings, import configuration file, or export device parameters.
Click **Maintenance and Security → Maintenance →Backup and Reset** to enter the page.

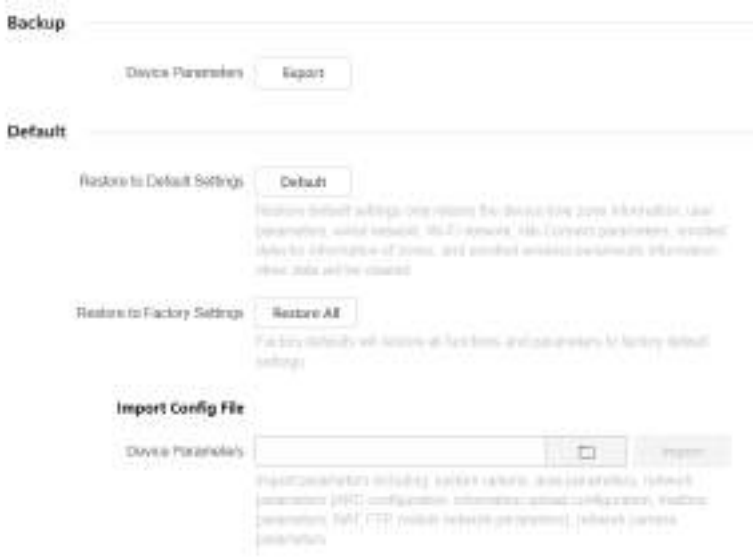


Figure 5-34. Backup and Reset

Export Configuration File

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

Restore to Default Settings

Click **Default** will restore all parameters except for device time zone information, user parameters, wired network, Wi-Fi network, HC information detector information, detector information enrolled in the zone and enrolled wireless peripheral information.

Restore to Factory Settings

Click **Restore All** to restore all parameters to the factory settings.

Import Configuration File

Click to select configuration file from the PC and click **Import** to import configuration parameters to the device.

Local

You can search the log on the device.
Click **Maintenance and Security → Maintenance → Log** to enter the page.

Figure 5-35. Log

Select a primary event and a sub type from the drop-down list, set the log start time and end time and click **Search**. All found log information will be displayed in the list.
You can also click **Reset** to reset all search conditions.

Security Audit Log

You can add the Security Audit Server to the system. The device will upload web logs to the server.

Steps

1. Click **Maintenance and Security → Maintenance → Security Audit Log** to enter the page.

Figure 5-36. Security Audit Log

2. Slide **Enable Log Upload Server**.
3. Enter log server IP and port.
4. Click to select a certificate.

Note

Formats include ca.crt, ca-chan.crt, private.txt are allowed.

5. Click **Import**.
6. Click **Save**.

Walk Test

The AX PRO supports walk test function.

Steps

1. Enter **Maintenance and Security → Maintenance → Walk Test** to enable the function.

Note

Only when all the detectors are without fault, you can enter the mode TEST mode.

2. Slide **Enable**.
3. Trigger the detector in each zone.
4. Click **Refres**h and check test results.

Device Debugging

You can export debugging file to the PC.

Steps

1. Click **Maintenance and Security → Maintenance → Export File** to enter the page.
2. Slide to enable functions.

   SSH

   Enable or disable SSH (Secure Shell) according to your actual needs.

   Debugging Log

   Enable the function and click **Export** to export serial logs.

   Tamper Alarm on HPP Login

   After this function is enabled, the device lid opened alarm (tamper alarm) takes effect when installer login. (By default, the lid opened alarm (tamper alarm) does not take effect when the installer login.)
3. Click **Sav**e.

Security

Enable or disable SSH (Secure Shell) according to your actual needs.
Click **System** → **System Security** → **SSH Settings** to enter the SSH Settings page and you can enable or disable the SSH function.

User Lockout Attempts

The device will be locked 90 s after 3 failed credential attempts (can be set in Retry Times Before Auto-Lock) in a minute.
You can view the locked user or unlock a user and set the user locked duration.

Note

To compliant the EN requirement, the system will only record the same log 3 times continuously.

Steps

1. Click **Maintenance and Security → Maintenance → User Lockout Attempts** to enter the page.

Figure 5-37. User Lockout Attempts

2. Set parameters.

Retry Times Before Auto-Lock

If the user continuously input the incorrect password for more than the configured times, the account will be locked.

Note

The administrator has two more attempts than the configured value.

Auto-lock Time

Set the locking duration when the account is locked.

Note

The available locking duration is 5s to 1800s.

3. Click to unlock the account or click **Unlock All** to unlock all locked users in the list.
4. Click **Save**.

Module Lock Settings

Set the module locking parameters, including the Retry Times before Auto-Lock, and locked duration. The module will be locked for the programmed time duration, once the module authentication has failed for the amount of configured times.

Steps

1. Click **Maintenance and Security → Maintenance → Module Locking Settings** to enter the page.
2. Select a module from the list, and click .

Figure 5-38. Module Locking Settings

3. Set the following parameters of the selected module.

Retry Times before Auto-Lock

If a user continuously tries to authentication a password for more than the configured attempts permitted, the keypad will be locked for the programmed duration.

Auto-lock Time

Set the locking duration when the keypad is locked. After the configured duration, the keypad will be unlocked.

4. Click **Save**.

5.4 Report to ARC (Alarm Receiving Center)

AX PRO wireless control panel is designed with transceiver built in following the guidance of EN 50131-10 and EN 50136-2. Category DP2 is provided with primary network interface of LAN/WiFi and secondary network interface of GPRS or 3G/4G LTE. ATS (Alarm Transmission system) is designed to always use LAN/Wi-Fi network interface when available to save mobile data usage. The secondary network interface provides resilience and reliability during mains power failure.

Setup ATS in Transceiver of Receiving Center

Steps:

1. Login to the web client of the alarm receiver.
2. Click **Configuration→ IP Reception**, and create a receiving server as shown below.

Figure 5-39. IP Reception

3. Click **Alarms and Accounts→ Accounts Management**, and assign an account for the panel as show below.

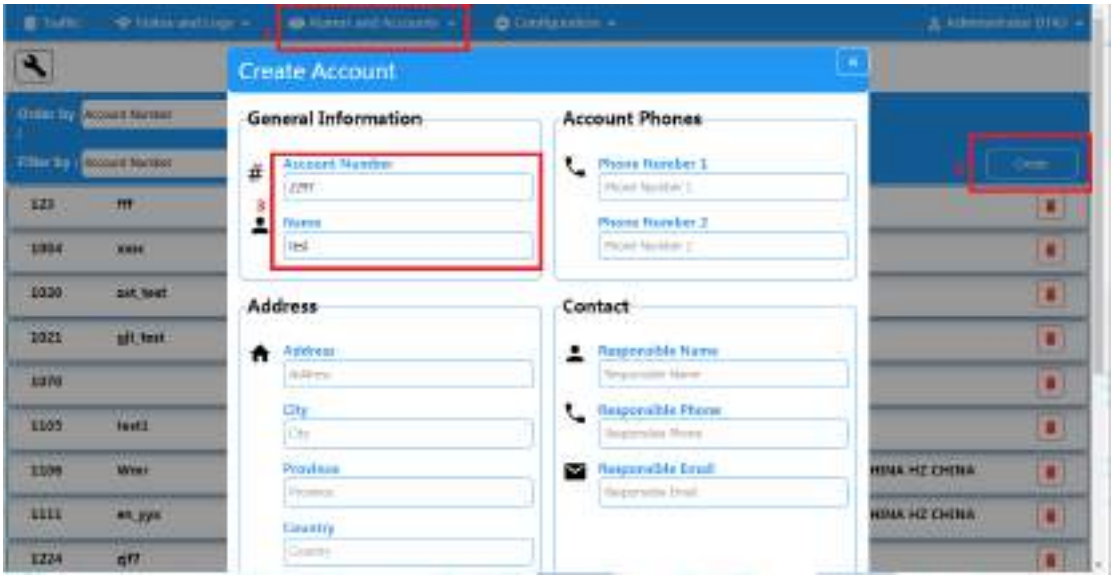


Figure 5-40. Account Management

Setup ATS in Transceiver of the Panel

Steps:

1. Login using installer account from local web client.
2. Click **Communication→ Alarm Receiving Center (ARC)**, and enable **Alarm Receiving Center 1**.

Figure 5-41. ARC1

- **= Protocol Setting =**

  Protocol Type

  — ADM-CID
  — SIA-DCS
  — *ADM-CID
  — *SIA-DCS

  Select token supported by the receiver in the ARC. Choose the token with "*" mark to improve the communication security.

- **= Server Setting =**

  - ***Address Type***
    — IP
    — Domain Name
  - ***Server Address / Domain Name***
  - ***Port No.***

    Input IP address or domain name by which the transceiver of receiving center could be reached. Input port number of the server provided by the ARC

- **= Account Setting =**

  - ***Account Code***

    Input the assigned account provided by the ARC.

- **= SIA DC-09 Protocol Setting =**

  - ***Transmission Mode***
    — TCP
    — UDP

    Both TCP and UDP are supported for transmission. UDP is recommended by the SIA DC-09

standard.

- *Connection Setting*
  - *Impulse Counting Time / Retry Timeout Period*
    Setup the timeout period waiting for receiver to respond. Re-transmission will be arranged if the transceiver of receiving center is timeout.
  - *Attempts*
    Setup the maximum number that re-transmission will be tried.
  - *Polling Rate*
    Setup the interval between 2 live polling if enable is checked.
- *Encryption Setting*
  - *Encryption Arithmetic*
    — AES
  - *Password Length*
    — 128
    — 192
    — 256
  - *Secret Key*
    Setup the encryption key length and input the key provided by the ARC.

Signaling Test

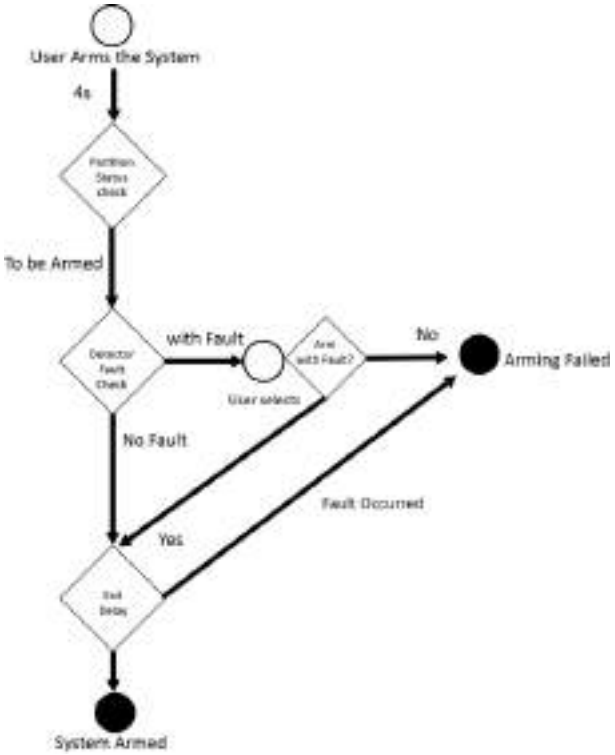
Activate a panic alarm from the control panel.
Login to Receiver. Click **Traffic** to review all the messages received.

Figure 5-42. Traffic

Chapter 6 General Operations

6.1 Arming

You can use keypad, keyfob, Tag, client software, mobile client to arm your system.
After the arming command is sending to AX PRO, the system 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 AX PRO will prompt the result in 5s, and upload the arming report.



Arming

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
- 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.
The forced arming operation will be record in the event log.

6.2 Disarming

You can disarm the system with keypad, keyfob, tag, client software, or mobile client.

Disarming Indication

The arming/disarming indicator flashes 30s while the user successfully disarm the system through the entry/exit route.
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.

Early Alarm

If the first instant zone is triggered when the AX PRO is in the status of entry delay, the AX PRO then enters the early alarm mode.
The early alarm duration can be set (> 30s).
The AX PRO will reports the alarm only if the alarm event lasts over the duration of early alarm with the addition of entry delay.

6.3 SMS Control

You can control the security system with SMS, and the command is shown below.
SMS format for Arming/disarming/silencing alarm:

{Command} + {Operation Type} + {Target}

Command: 2 digits, 00- Disarming, 01- Away arming, 02- Stay arming, 03- Silencing alarm
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.

A. Trouble Shooting

A.1 Communication Fault

A.1.1 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.

A.1.2 Web Page is Not Accessible

Fault Description:
Use browser to access web pages and display Inaccessible.
Solutions:
1. Check whether the network cable is loose and the panel network is abnormal.
2. The panel port has been modified. Please add a port to the web address for further access.

A.1.3 Hik-Connect is Offline

Fault Description:
The web page shows that the Hik-Connect is offline.
Solution:
Network configuration of the panel is error, unable to access extranet.

A.1.4 Network Camera Drops off Frequently

Fault Description:
System reports multiple event logs of IPC disconnection and connection.
Solution:
Check whether the network communication or camera live view is proper.

A.1.5 Failed to Add Device on APP

Fault Description:
When using APP to add devices, it is prompted that the device fails to be added, the device could not be found, etc.
Solution:

Check the web page: whether the Hik-Connect is offline.

A.1.6 Alarm Information is Not Reported to APP/4200/Alarm Center

Fault Description:
After the alarm is triggered, the app/4200/ alarm center does not receive the alarm message.
Solution:
"Message push" - "alarm and tamper-proof notice" is not enabled. You should enable "alarm and tamper-proof notice".

A.2 Mutual Exclusion of Functions

A.2.1 Unable to Enter Registration Mode

Fault Description:
Click the panel function key, and prompt key invalid.
Solution:
The panel is in "Hotspot" mode. Switch the panel to "station" mode, and then try to enter the registration mode again.

A.3 Zone Fault

A.3.1 Zone is Offline

Fault Description:
View status of zones which displays offline.
Solution:
Check whether the detector reports undervoltage. Replace the detector battery

A.3.2 Zone Tamper-proof

Fault Description:
View status of zones which displays tamper-proof.
Solution:
Make tamper-proof button of the detector holden.

A.3.3 Zone Triggered/Fault

Fault Description:

View status of zones which displays triggered/fault.
Solution:
Reset the detector.

A.4 Problems While Arming

A.4.1 Failure in Arming (When the forced arming is not enabled)

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.

A.5 Operational Failure

A.5.1 Failed to Enter the Test Mode

Fault Description:
Failed to enable test mode, prompting "A fault in the zone".
Solution:
Zone status, alarm status or zone power is abnormal.

A.5.2 The Silence Alarm Operation on the Panel Does Not Produce the Silence Alarm Report

Fault Description:
The alarm clearing operation on the panel does not produce the alarm clearing report.
Solution:
In the absence of alarm, no report will be uploaded for arm clearing.

A.6 Mail Delivery Failure

A.6.1 Failed to Send Test Mail

Fault Description:
when configure the mail information, click "test inbox" and prompt test fails.

Solution:
Wrong configuration of mailbox parameters. Please edit the mailbox configuration information, as shown in table 1/1.

A.6.2 Failed to Send Mail during Use

Fault Description:
Check the panel exception log. There is "mail sending failure".
Solution:
The mailbox server has restricted access. Please log in to the mailbox to see if the mailbox is locked.

A.6.3 Failed to Send Mails to Gmail

Fault Description:
The receiver's mailbox is Gmail. Click "Test Inbox" and prompt test fails.
1. Google prevents users from accessing Gmail using apps/devices that do not meet their security standards.
Solution:
Log in to the website (https://www.google.com/settings/security/lesssecureapps), and "start using access of application not safe enough". The device can send mails normally.
2. Gmail does not remove CAPTCHA authentication.
Solution: Click the link below, and then click "continue"
(https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Failed to Send Mails to QQ or Foxmail

Fault Description:
The receiver's mailbox is QQ or foxmail. Click "Test Inbox" and prompt test fails.
1. Wrong QQ account or password.
Solution:
the password required for QQ account login is not the password used for normal login. The specific path is: Enter the email account → device → account → to generate the authorization code, and use the authorization code as the login password.
2. SMTP login permission is needed to open.

A.6.5 Failed to Send Mails to Yahoo

Fault Description:
The receiver's mailbox is yahoo. Click "test inbox" and prompt test fails.
1. The security level of mailbox is too high.
Solution:
Go to your mail account and turn on "less secure sign-in".

A.6.6 Mail Configuration

Table A-1 Mail Configuration

Mail Type	Mail Server	SMTP Port	Protocols Supported
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Note

About mail configuration:

- SMTP portDefault to use port 25 without encryption, or using port 465 if SSL/TLS is used.
  Port 587 is mainly used for STARTTLS protocol mode.
  The STARTTLS protocol mode that is usually used by default when selecting TLS.
- User nameUser name of Outlook and Hotmail require full names, and other email require a prefix before @.

B. Input Types

Table B-1 Input Types

Input Types	Operations
Instant Zone	The system will immediately alarm when it detects triggering event after system armed. Audible Response Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Perimeter Zone	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. There is a configurable interval between alarm and sounder output, which allows you to check the alarm and cancel the sounder output during the interval. Voice Prompt: Zone X perimeter alarm.
Delayed Zone	The system provides you time to leave through or enter the zone without alarm. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Follow Zone	The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X follow alarm.
24H Silence Zone	The zone activates all the time without any sound/sounder output when alarm occurs. Audible Response: No system sound (voice prompt or sounder).
Panic Zone	The zone activates all the time. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X panic alarm.
Fire Zone	The zone activates all the time with sound/sounder output when alarm occurs.

Input Types	Operations
	Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X fire alarm.
Gas Zone	The zone activates all the time with sound/sounder output when alarm occurs. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X gas alarm.
Medical Zone	The zone activates all the time with beep confirmation when alarm occurs. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X medical alarm.
Timeout Zone	The zone activates all the time. The zone type is used to monitor and report the "ACTIVE" status of a zone, but it will only report and alarm this status after the programmed time has expired (1 to 599) seconds.
Disabled Zone	Alarms will not be activated when the zone is triggered or tampered. Audible Response: No system sound (voice prompt or sounder).
Virtual Zone (Keypad/Keyfob)	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. Voice Prompt: Buzzer beeps.
Tamper Alarm	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X tampered.
Link	Trigger the linked device when event occurs. e.g. The output expander linked relays will be enabled when the AX PRO is armed.
Arm	When armed: Voice prompt for fault. You can handle the fault according to the voice prompt. ● System sound for arming with Tag or keyfob. ● Voice prompt for fault. You can handle the fault according to the voice prompt.

Fault event displays on client. You can handle the fault via client software or mobile client.

Voice Prompt: Armed/Arming failed.

C. Output Types

Table C-1 Output Types

Output Types	Active	Restore
Arming	Arm the AX PRO	After the configured output delay
Disarming	Disarm the AX PRO	After the configured output delay
Alarm	When alarm event occurs. The alarm output will be activated after the configured exit/enter delay.	After the configured output delay, disarm the AX PRO or silence alarm
Zone Linkage	When alarm event occurs, the linked relay will output alarm signal.	After the configured output duration
Manual Operation	Enable relays manually	Over the triggering time or disable the relays manually

D. Event Types

Table D-1 Event Types

Event Types	Custom	Default 1 (client software notification)	Default 2 (alarm receiving center 1/2)	Default 3 (mobile client)	Default 4 (telephone)
Alarm and Tamper	×/√	√	√	√	√
Life Safety Event	×/√	√	√	√	√
System Status	×/√	√	×	×	×
Panel Management	×/√	√	×	×	×

E. Access Levels

Level	Description
1	Access by any person; for example the general public.
2	User access by an operator and administrator; for example customers (systems users).
3	User access by an installer; for example an alarm company professional.

Table E-1 Permission of the Access Level

Function	Permission		
	1	2	3
Arming	No	Yes	Yes
Disarming	No	Yes	Yes
Restoring/Clearing Alarm	No	Yes	Yes
Entering Walk Test Mode	No	Yes	Yes
Bypass(zone)/Disabling/Force Arming	No	Yes	Yes
Adding/Changing Verification Code	No	Yes[d]	Yes[d]
Adding/Editing Level 2 User and Verification Code	No	Yes	Yes
Adding/Editing Configuration Data	No	No	Yes
Replacing software and firmware	No	No	No

Note

[a] By the condition of being accredited by user in level 2.
[b]By the condition of being accredited by user in level 2 and level 3.
[d]Users can only edit their own user code.

- The user level 2 can assign the login permission of the controller to the user level 3 in the settings page.
- The user level 2 should assign permissions to the user level 3 if the user level 3 wants to login the controller remotely.
- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.

- When the controller is bypassed, the user level 3 can login the controller without the permission assignment of the user level 2.
- The user level 4 can login the controller only when the user level 2 or level 3 has assigned permissions to the user level 4.

F. Signalling

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/WiFi	10 min
Secondary ATP failure/restore	GPRS	60 min
	3G/4G LTE	20 min (when primary ATP failed)

Signalling 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 1000 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 signalling	Event log description
Primary ATP failure/restore	E351/R351	LAN Path Failed/LAN Path Recovery
Secondary ATP failure/restore	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery
ATS failure/restore	N/A	ATS Failed
Primary network interface failure/restore	E351/R351	LAN Path Failed/LAN Path Recovery
Secondary network interface failure/restore	E352/R352	Mobile Net Path Failed/Mobile Net Path Recovery

ATS Category

The ATS category of AXPRO is DP2. 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.

G. SIA and CID Code

Note

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.

Control Panel	AX PRO			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Lid Opened	Alarm	1137	TA	1137
Lid Closed	Alarm	3137	TR	3137
AC Power Down	Status	1301	AT	1301
AC Power Restored	Status	3301	AR	3301
Battery Low	Status	1302	YT	1302
Battery Voltage Restored	Status	3302	YR	3302
Battery Fault	Status	1311	YT	1310
Battery Fault Restored	Status	3311	YR	3310
Battery Disconnected	Status	1311	YM	1311
Battery Reconnected	Status	3311	YR	3311
Main Signalling Path ATP Fault	Status	1351	LT	1351
Main Signalling Path ATP Restored	Status	3351	LR	3351
Backup Signalling ATP Path Fault	Status	1352	LT	1352
Backup Signalling ATP Path Restored	Status	3352	LR	3352
Disarmed	Operation	1401	OP	1401
Away Armed	Operation	3401	CL	3401
Stay Armed	Operation	3441	NL	3441
Disarmed	Operation	1401	OP	1401
Auto Disarmed	Operation	1403	OA	1403
Auto Armed	Operation	3403	CA	3403

Walk Test Enabled	Operation	1607	TS	1607
Walk Test Disabled	Operation	3607	TE	3607
Enter Programming	Operation	1627	LB	1627
Exit Programming	Operation	1628	LX	1628
Cellular Data Network Exception	Status	1350	NT	1920
Cellular Data Network Connected	Status	3350	NR	3920
SIM Card Exception	Status	1350	NT	1921
SIM Card Detected	Status	3350	NR	3921
Wi-Fi Disconnected	Status	1350	NT	1922
Wi-Fi Connected	Status	3350	NR	3922
RF Signal Excpetion	Status	1344	XQ	1923
RF Signal Restored	Status	3344	XH	3923
IP Conflict	Status	1350	NT	1930
IP Conflict Restored	Status	3350	NR	3930
Wired Network Fault	Status	1350	NT	1931
Wired Network Connected	Status	3350	NR	3931
Power Running Out	Status	1311	YM	1318
Reset to Defaults	Operation	1305	ZY	1305
Alarm Silenced	Operation	1406	BC	1406
Late to Disarm	Status	1452	CT	1452
Auto Arming Failed	Operation	1455	CD	1455
Arming Failed	Operation	1454	CI	1822
Data limitation Reached	Status	1350	NT	1924
Sending Email Failed	Status	1948	BQ	1948
Unregistered Tag Operation	Status	1865	B D	1865
Duress Alarm	Operation	1121	HA	1121
Patrol Signing	Operation	3250	DW	3965

Network Camera

Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Timeout Alarm	Alarm	1130	BA	1126
Timeout Alarm Restored	Alarm	3130	BH	3126
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Entry Alarm	Alarm	1134	BA	1779
Exit Alarm	Alarm	1134	EA	1785
Intrusion Detection	Alarm	1131	BA	1759

Intrusion Detection Restored	Alarm	3131	BH	3759
Line Crossing Alarm	Alarm	1131	BA	1778
Line Crossing Alarm Restored	Alarm	3131	BH	3778
Fire Source Alarm	Alarm	1112	FA	1780
Fire Source Alarm Restored	Alarm	3112	FH	3780
High Temperature Pre-Alarm	Alarm	1158	KS	1781
High Temperature Pre-Alarm Restored	Alarm	3158	KR	3781
Low Temperature Pre-Alarm	Alarm	1159	ZS	1782
Low Temperature Pre-Alarm Restored	Alarm	3159	ZR	3782
High Temperature Alarm	Alarm	1158	KA	1783
High Temperature Alarm Restored	Alarm	3158	KH	3783
Low Temperature Alarm	Alarm	1159	ZA	1784
Low Temperature Alarm Restored	Alarm	3159	ZH	3784
Motion Detection Alarm Started	Alarm	1131	BA	1940
Motion Detection Alarm Ended	Alarm	3131	BH	3940
Network Camera Disconnected	Status	1949	BR	1949
Network Camera Connected	Status	3949	DS	3949

APP	Hik-Connect			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Panic Alarm	Alarm	1120	PA	1129
Silent Panic Alarm	Alarm	1120	PA	1127

Peripheral				
Single Input Transmitter	DS-PM1-I1-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Device Motion Alarm	Alarm	1148	AG	1148
Device Motion Alarm Restored	Alarm	3148	CO	3148
Masking Alarm	Alarm	1149	BA	1149
Masking Alarm Restored	Alarm	3149	BH	3149
Peripheral Undervoltage	Status	1384	XT	1347
Peripheral Undervoltage Restored	Status	3384	XR	3347
Peripheral Offline	Status	1381	XL	1348
Peripheral Online	Status	3381	XC	3348
Peripheral Deleted	Operation	1306	CG	1980
Peripheral Enrolled	Operation	3306	ED	3980

Multi IO transmitter	DS-PM1-I16O2-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Battery Disconnected	Status	1311	YM	1311
Battery Reconnected	Status	3311	YR	3311
Power Output Short Circuit	Status	1312	YI	1328
Power Output Short Circuit Restored	Status	3312	YJ	3328
Expander AC Power Down	Status	1301	YP	1342
Expander AC Power Restored	Status	3301	YQ	3342
Peripheral Lid Opened	Alarm	1144	TA	1346
Peripheral Lid Closed	Alarm	3144	TR	3346
Peripheral Undervoltage	Status	1384	XT	1347
Peripheral Undervoltage Restored	Status	3384	XR	3347
Peripheral Offline	Status	1381	XL	1348
Peripheral Online	Status	3381	XC	3348
Sensor Fault	Status	1380	FT	1380
Sensor Fault Restored	Status	3380	FJ	3380
Peripheral Deleted	Operation	1306	CG	1980
Peripheral Enrolled	Operation	3306	ED	3980

Wireless Repeater	DS-PR1-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Battery Fault	Status	1311	YT	1310
Battery Fault Restored	Status	3311	YR	3310
Repeater Battery Low	Status	1384	XT	1337
Repeater Battery Voltage Restored	Status	3384	XR	3337
Repeater AC Power Down	Status	1301	YP	1339
Repeater AC Power Restored	Status	3301	YQ	3339
Repeater Battery Disconnected	Status	1311	YM	1340
Repeater Battery Reconnected	Status	3311	YR	3340
Repeater Lid Opened	Alarm	1144	TA	1343
Repeater Lid Closed	Alarm	3144	TR	3343
Repeater Offline	Status	1381	XL	1917
Repeater Online	Status	3381	XC	3917
Repeater Deleted	Operation	1306	CE	1978
Repeater Enrolled	Operation	3306	EB	3978

Smart Plug	DS-PSP1-WE, DS-PSP1-EU-WE, DS-PSP1-UK-WE, DS-PSP1-IT-WE, DS-PSP1-US-WB, DS-PSP1-AU-WB
Wireless Output Module	DS-PM1-O1H-WE, DS-PM1-O1L-WE

Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Overcurrent Protection Triggered	Status	1312	YI	1312
Overcurrent Protection Restored	Status	3312	YJ	3312
Overvoltage Protection Triggered	Status	1319	YP	1319
Overvoltage Protection Restored	Status	3319	YQ	3319
Expander Offline	Status	1381	XL	1916
Expander Online	Status	3381	XC	3916
Expander Deleted	Operation	1306	CD	1977
Expander Enrolled	Operation	3306	EA	3977

Wireless Output Module	DS-PM1-O1L-WE

Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Expander Lid Opened	Alarm	1144	TA	1341
Expander Lid Closed	Alarm	3144	TR	3341
Expander Offline	Status	1381	XL	1916
Expander Online	Status	3381	XC	3916
Expander Deleted	Operation	1306	CD	1977
Expander Enrolled	Operation	3306	EA	3977

Sounder	
Wireless External Sounder	DS-PS1-E-WE

Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Expander AC Power Down	Status	1301	YP	1342
Expander AC Power Restored	Status	3301	YQ	3342
Sounder Lid Opened	Alarm	1144	TA	1344
Sounder Lid Closed	Alarm	3144	TR	3344
Sounder Offline	Status	1381	XL	1345
Sounder Online	Status	3381	XC	3345
Sounder Battery Low	Status	1384	XT	1919
Sounder Battery Voltage Restored	Status	3384	XR	3919
Sounder Deleted	Operation	1306	CF	1979

Sounder Enrolled	Operation	3306	EC	3979

Wireless External Sounder	DS-PS1-EV-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Motion Detection Alarm	Alarm	1148	AG	1148
Motion Detection Alarm Restored	Alarm	3148	CO	3148
Expander AC Power Down	Status	1301	YP	1342
Expander AC Power Restored	Status	3301	YQ	3342
Sounder Lid Opened	Alarm	1144	TA	1344
Sounder Lid Closed	Alarm	3144	TR	3344
Sounder Offline	Status	1381	XL	1345
Sounder Online	Status	3381	XC	3345
Sounder Battery Low	Status	1384	XT	1919
Sounder Battery Voltage Restored	Status	3384	XR	3919
Sounder Deleted	Operation	1306	CF	1979
Sounder Enrolled	Operation	3306	EC	3979
Vibration Alarm	Alarm	1133	BA	1125
Vibration Alarm Restored	Alarm	3133	BH	3125
Drilling Alarm	Alarm	1750	IA	1750
Drilling Alarm Restored	Alarm	3750	IR	3750

Wireless Internal Sounder	DS-PS1-I-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Sounder Lid Opened	Alarm	1144	TA	1344
Sounder Lid Closed	Alarm	3144	TR	3344
Sounder Offline	Status	1381	XL	1345
Sounder Online	Status	3381	XC	3345
Sounder Battery Low	Status	1384	XT	1919
Sounder Battery Voltage Restored	Status	3384	XR	3919
Sounder Deleted	Operation	1306	CF	1979
Sounder Enrolled	Operation	3306	EC	3979

Wireless Internal Sounder	DS-PS1-II-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Expander AC Power Dowm	Status	1301	YP	1342
Expander AC Power Restored	Status	3301	YQ	3342

Sounder Lid Opened	Alarm	1144	TA	1344
Sounder Lid Closed	Alarm	3144	TR	3344
Sounder Offline	Status	1381	XL	1345
Sounder Online	Status	3381	XC	3345
Sounder Battery Low	Status	1384	XT	1919
Sounder Battery Voltage Restored	Status	3384	XR	3919
Sounder Deleted	Operation	1306	CF	1979
Sounder Enrolled	Operation	3306	EC	3979

Wireless Keypad	DS-PK1-E-WE, DS-PK1-LT-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Peripheral Lid Opened	Alarm	1144	TA	1346
Peripheral Lid Closed	Alarm	3144	TR	3346
Peripheral Undervoltage	Status	1384	XT	1347
Peripheral Undervoltage Restored	Status	3384	XR	3347
Peripheral Offline	Status	1381	XL	1348
Peripheral Online	Status	3381	XC	3348
Keypad Locked	Status	1501	DK	1862
Keypad Unlocked	Status	3501	DO	3862
Peripheral Deleted	Operation	1306	CG	1980
Peripheral Enrolled	Operation	3306	ED	3980
Duress Alarm	Operation	1121	HA	1121
Incorrect Password	Status	1461	JA	1467
Keypad/Keyfob Panic Alarm	Alarm	1120	PA	1810
Keypad/Keyfob Fire Alarm	Alarm	1110	FA	1811
Keypad/Keyfob Medical Alarm	Alarm	1100	MA	1847
Unregistered Tag	Operation	1865	B D	1865

Wireless Tag Reader	DS-PT1-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Peripheral Lid Opened	Alarm	1144	TA	1346
Peripheral Lid Closed	Alarm	3144	TR	3346
Peripheral Undervoltage	Status	1384	XT	1347
Peripheral Undervoltage Restored	Status	3384	XR	3347
Peripheral Offline	Status	1381	XL	1348
Peripheral Online	Status	3381	XC	3348
Tag Reader Locked	Status	1501	DK	1864

Tag Reader Unlocked	Status	3501	DO	3864
Peripheral Deleted	Operation	1306	CG	1980
Peripheral Enrolled	Operation	3306	ED	3980
Unregistered Tag	Status	1865	B D	1865
Patrol Signing	Operation	3250	DW	3965

Wall Switch	DS-PM1-O1H-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Expander Offline	Status	1381	XL	1916
Expander Online	Status	3381	XC	3916
Expander Deleted	Operation	1306	CD	1977
Expander Enrolled	Operation	3306	EA	3977

Wireless Keyfob	DS-PKF1-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Keyfob Undervoltage	Status	1384	XT	1925
Keyfob Undervoltage Restored	Status	3384	XR	3925
Keypad/Keyfob Panic Alarm	Alarm	1120	PA	1810
Keypad/Keyfob Medical Alarm	Alarm	1100	MA	1847

Detector				
Emergency Button	DS-PDEBP1-EG2-WE, DS-PDEBP2-EG2-WE, DS-PDEB1-EG2-WE, DS-PDEB2-EG2-WE, DS-PDEB1-EG2-WE(B), DS-PDEB2-EG2-WE(B)			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Medical Alarm	Alarm	1100	MA	1100
Medical Alarm Restored	Alarm	3100	MH	3100
Panic Alarm	Alarm	1120	PA	1129
Panic Alarm Restored	Alarm	3120	PH	3129
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914

Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Wireless Magnet Detector	DS-PDMC-EG2-WE, DS-PDMCS-EG2-WE, DS-PDMCK-EG2-WE

Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Panic Alarm	Alarm	1120	PA	1129
Panic Alarm Restored	Alarm	3120	PH	3129
Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Keyswitch Zone Disarmed	Operation	1409	CS	1309
Keyswitch Zone Armed	Operation	3409	OS	3409
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

External Detector	DS-PDC10AM-EG2-WE, DS-PDC10DM-EG2-WE, DS-PDMCX-E-WE, DS-PDTT15AM-LM-WE

PIR Camera	DS-PDPC12P-EG2-WE, DS-PDPC12PF-EG2-WE, DS-PDPC12P-EG2-WE(B), DS-PDPC12PF-EG2-WE(B)			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Masking Alarm (Only for DS-PDC10AM-EG2-WE/DS-PDC10DM-EG2-WE/DS-PDTT15AM-LM-WE)	Alarm	1149	BA	1149
Masking Alarm Restored (Only for DS-PDC10AM-EG2-WE/DS-PDC10DM-EG2-WE/DS-PDTT15AM-LM-WE)	Alarm	3149	BH	3149
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Wireless Photoelectric Smoke Detector	DS-PDSMK-S-WE, DS-PDSMK-E-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Fire Alarm	Alarm	1111	FA	1110
Fire Alarm Restored	Alarm	3111	FH	3110

Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Heat Detector	DS-PDHT-E-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Fire Alarm	Alarm	1114	KA	1114
Fire Alarm Restored	Alarm	3114	KH	3114
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

PIR Detector				
Wireless PIR Detector	DS-PDP15P-EG2-WE, DS-PDPG12P-EG2-WE, DS-PDC15-EG2-WE, DS-PDCL12-EG2-WE, DS-PDP18-HM-WE			
Wireless Dual-Technology Detector	DS-PDD12P-EG2-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Timeout Alarm	Alarm	1130	BA	1126
Timeout Alarm Restored	Alarm	3130	BH	3126

Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

R3 Wireless 180° Panoramic Outdoor Detector	DS-PDQP15AM-LM-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
External Module Disconnected	Status	1144	TA	1144
External Module Connected	Status	3144	TR	3144
Expander AC Power Down	Status	1301	YP	1342
Expander AC Power Restored	Status	3301	YQ	3342
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383

Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Temperature Detector	DS-PDTPH-E-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
External Module Disconnected	Status	1144	TA	1144
External Module Connected	Status	3144	TR	3144
High Temperature Alarm	Alarm	1158	KA	1783
High Temperature Alarm Restored	Alarm	3158	KH	3783
Low Temperature Alarm	Alarm	1159	ZA	1784
Low Temperature Alarm Restored	Alarm	3159	ZH	3784
Temperature Exception Alarm	Alarm	1153	KT	1786
Temperature Exception Alarm Restored	Alarm	3153	KJ	3786
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915

Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Water Leak Detector	DS-PDWL-E-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Water Leakage Alarm	Alarm	1154	WA	1154
Water Leakage Alarm Restored	Alarm	3154	WH	3154
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Glass Break Detector	DS-PDBG8-EG2-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134

Delay Alarm Restored	Alarm	3134	BH	3134
Confirmed Alarm	Alarm	1139	BV	1139
Confirmed Alarm Restored	Alarm	3139	BW	3139
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

Wireless Triple Signal Detector	DS-PDTT15AM-LM-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Instant Alarm	Alarm	1130	BA	1103
Instant Alarm Restored	Alarm	3130	BH	3103
Burglary Alarm	Alarm	1130	BA	1130
Burglary Alarm Restored	Alarm	3130	BH	3130
24H Alarm	Alarm	1130	BA	1133
24H Alarm Restored	Alarm	3130	BH	3133
Delay Alarm	Alarm	1134	BA	1134
Delay Alarm Restored	Alarm	3134	BH	3134
External Module Disconnected	Status	1144	TA	1144
External Module Connected	Status	3144	TR	3144
Masking Alarm	Alarm	1149	BA	1149
Masking Alarm Restored	Alarm	3149	BH	3149
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975

Detector Enrolled	Operation	3306	DY	3975

Wireless CO Detector	DS-PDCO-E-WE			
Event Description	Event Type	CID Code/STD Code	SIA Code	HIK Code
Gas Leakage Alarm	Alarm	1162	GA	1151
Gas Leakage Alarm Restored	Alarm	3162	GH	3151
Detector Lid Opened	Alarm	1144	TA	1383
Detector Lid Closed	Alarm	3144	TR	3383
Bypassed	Alarm	1570	QB	1570
Bypass Restored	Alarm	3570	QU	3570
Wireless Detector Offline	Status	1381	XL	1914
Wireless Detector Online	Status	3381	XC	3914
Wireless Detector Battery Low	Status	1384	XT	1915
Wireless Detector Battery Voltage Restored	Status	3384	XR	3915
Detector Deleted	Operation	1306	CB	1975
Detector Enrolled	Operation	3306	DY	3975

H. User Privacy Statement

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.

User Privacy Information Description

Password	The password for the device account, used to log in to the device.
Username	The username 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. For details, refer to *Communication Matrix*.
Log	Used to record information such as device operating status and operation records.
Database information	Used to record information.

I. Detector Zone Types

This table is applicable to detectors of version 1.2.8, to show the configurable zone types of various detectors.

Detector	Available Zone Type
Wireless PIR Detector	PIR Camera & Wireless Triple Signal AM Detector: Instant/Delay/Follow/24 Hour/Disabled
	Others: Instant/Delay/Follow/Timeout/24 Hour/Disabled
Wireless DT Detector	Instant/Delay/Follow/Timeout/24 Hour/Disabled
Wireless Magnetic Contact	Instant/Delay/Follow/24 Hour/Panic/Timeout/ Keyswitch/Disabled
Wireless Emergency Button	Panic/Medical Zone/disabled
Outdoor Detector	Instant/Delay/Follow/Timeout/24 Hour/Disabled
Temperature & Humidity Detector	Instant/Delay/24 Hour/Disabled
Wireless Glass Break Detector	Instant/Delay/Follow/24 Hour/Disabled
Wireless Smoke Detector	Fire/Disabled
Wireless Water Leak Detector	Instant/Delay/24 Hour/Disabled
Wireless Heat Detector	Fire/Disabled
Wireless CO Detector	Gas/Disabled


See Far, Go Further