



AX HYBRID PRO

User Manual

Legal Information

©2022 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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-ProConnect.

Regulatory Information

EN 50131-3:2009

EN 50131-10:2014

EN 50136-2:2013

Security Grade (SG): 2

EN 50136-1:2012+A1:2018

Environmental Class (EC) : II


EN 50131-6:2017

SP4





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

EN 50130-4:2011+A1:2014

EN 50130-5:2011

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

EU Conformity Statement

	<p>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</p>
 	<p>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</p>
	<p>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</p>

Contents

Chapter 1 Introduction	7
System Description.....	7
Chapter 2 Start Up.....	9
Activate the Device with WEB	9
Chapter 3 Configuration	10
3.1 Set-up with the Web Client.....	10
3.1.1 Communication Settings	11
3.1.2 Device Management	25
3.1.3 Area Settings	34
3.1.4 Video Management.....	34
3.1.5 Permission Management	36
3.1.6 Maintenance.....	38
3.1.7 System Settings	42
3.1.8 Check Status	51
3.2 Report to ARC (Alarm Receiver Center)	51
Setup ATS in Transceiver of Receiving Center.....	52
Setup ATS in Transceiver of the Panel.....	52
Signaling Test.....	54
Chapter 4 General Operations	55
4.1 Access Entries	55
4.2 Arming	55
4.3 Disarming.....	57
4.4 SMS Control	57
A. Trouble Shooting.....	58
A.1 Communication Fault.....	58
A.1.1 IP Conflict	58
A.1.2 Web Page is Not Accessible.....	58
A.1.3 Hik-Connect is Offline	58
A.1.4 Network Camera Drops off Frequently.....	58

A.1.5 Failed to Add Device on APP	58
A.1.6 Alarm Information is Not Reported to APP/4200/Alarm Center.....	59
A.2 Mutual Exclusion of Functions	59
A.2.1 Unable to Enter Enrollment Mode	59
A.3 Zone Fault.....	59
A.3.1 Zone is Offline	59
A.3.2 Zone Tamper-proof	59
A.3.3 Zone Triggered/Fault	59
A.4 Problems While Arming	60
A.4.1 Failure in Arming (When the Arming Process is Not Started).....	60
A.5 Operational Failure	60
A.5.1 Failed to Enter the Test Mode	60
A.5.2 The Alarm Clearing Operation on the Panel Does Not Produce the Alarm Clearing Report	60
A.6 Mail Delivery Failure	60
A.6.1 Failed to Send Test Mail	60
A.6.2 Failed to Send Mail during Use.....	61
A.6.3 Failed to Send Mails to Gmail.....	61
A.6.4 Failed to Send Mails to QQ or Foxmail	61
A.6.5 Failed to Send Mails to Yahoo	61
A.6.6 Mail Configuration	62
B. Input Types	63
C. Output Types	66
D. Event Types	67
E. Access Levels	68
F. Signalling.....	70
Detection of ATP/ATS Faults.....	70
ATS Category.....	70
G. SIA and CID Code	71
H. Communication Matrix and Operation Command.....	79

Chapter 1 Introduction

System Description

AX HYBRID PRO control panel is a wired intrusion control panel with wireless detectors & peripherals access capability. It is the first control panel that supports high-speed Speed-X Bus, which is a creative technology and is used to transmit verification video/picture from PIR-CAM. Besides, this hybrid control panel supports customized voice library, which is designed for users to upload customized voice files. These voice files will be played via alarm phone call when alarm triggered. As for basic functions, it supports Wi-Fi, PSTN, TCP/IP and GPRS/3G/4G communication methods. It also supports Hik-ProConnect, Hik-Connect, Hik IP Receiver, Hik IP Receiver Pro and Hik-Central, which is applicable to the scenarios of market, hotel, supermarket, warehouse, office, house (especially with cables pre-installed), etc.

 **Note**

ISUP5.0: a privacy internet protocol that is used for accessing the third-party platform, which supports alarm report uploading, AX HYBRID PRO management, and short video uploading. The prioritization of the message and indications are the same. The AXPRO uploads messages and gives indications synchronously.

 **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.

*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.

Chapter 2 Start Up

Activate the Device with WEB

Use web browser to activate the device. Use SADP software or PC client to search the online device to get the IP address of the device, and activate the device on the web page.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Open a web browser and enter the IP address of the device.

Note

If you connect the device with the PC directly, you need to change the IP address of your PC to the same subnet as the device. The default IP address of the device is 192.0.0.64.

2. Create and confirm the admin password. (The default user name of **admin** account is **admin**.)

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Click **OK** to complete activation.

Note

- The default user name of **admin** account is **admin**.
 - You should login the admin account first to enable the installer and the maintenance.
 - The default password of the **installer** is **installer12345**, and the default password of the **maintenance** is **hik12345**. These password will have to be changed when first connected.
-

Chapter 3 Configuration

3.1 Set-up with the Web Client

Steps

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



Note

Only the admin and the installer can login to the web client.

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

The screenshot displays the 'Overview' page of the web client. At the top, there are navigation tabs: Overview, Area Control, Zone Control, and Peripheral Control. Below these are three user status cards for Administrator (1), Installer (1), and Operator (1). The Administrator card shows 'admin' with 0 active sessions and permissions for Log and Status Query, Zone Bypass, and Arm. The Installer card shows 'installer' with 1 active session and permissions for Log and Status Query, Zone Bypass, and Rem. The Operator card shows '11' with 0 active sessions and permissions for Arm and Disarm. Below the user cards is the 'AX Hybrid PRO Status' section, which includes indicators for External Power Supply (Connected), Wired Network (Connected), Wi-Fi (Disconnected/None), Battery (0%), Lid Status (Open), and Cloud Connection Status (Disconnected). At the bottom, there are two tables: 'Device Status' and 'Area'. The 'Device Status' table lists 5 device types: Zone (2 total, 0 in fault, 2 ok), Sounder (1 total, 0 in fault, 1 ok), Keypad (1 total, 0 in fault, 1 ok), Keyfob (1 total, 0 in fault, 1 ok), and Automation (2 total, 0 in fault, 2 ok). The 'Area' table lists 2 areas: Area 1 (Disarmed) and Area 2 (Disarmed).

No.	Device Types	Total	Devices in fault	Devices ok
1	Zone	2	0	2
2	Sounder	1	0	1
3	Keypad	1	0	1
4	Keyfob	1	0	1
5	Automation	2	0	2

No.	Area Name	Area Status
1	Area 1	Disarmed
2	Area 2	Disarmed

3.1.1 Communication Settings

Wired Network

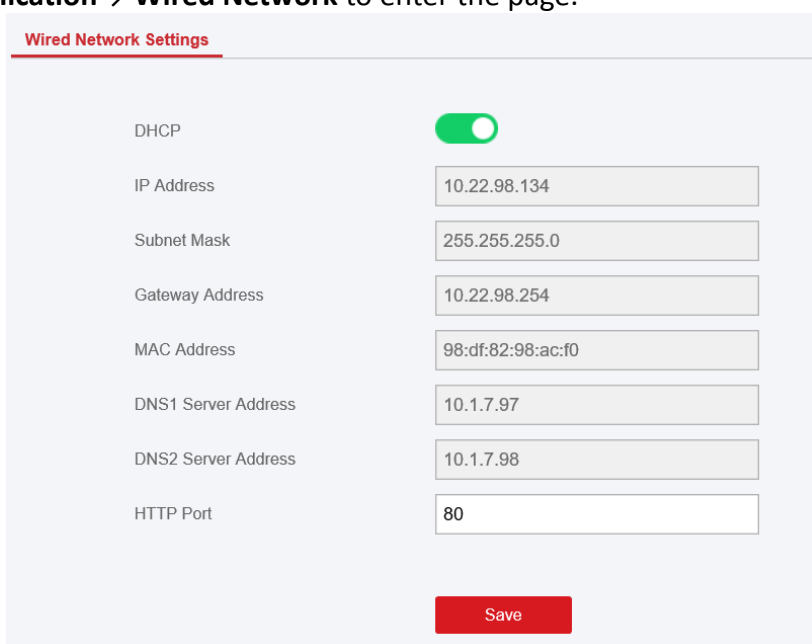
You can set the device IP address and other network parameters.

Steps



Functions varied depending on the model of the device.

1. Click **Communication** → **Wired Network** to enter the page.



2. 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**.
3. **Optional**: Set correct DNS server address if the device needs to visit Hik-Connect server via a domain name.
4. Click **Save**.

Wi-Fi

You can set the Wi-Fi parameters if there are secure and credible Wi-Fi networks nearby.

Steps

1. Click **Communication** → **Wi-Fi** to enter the Wi-Fi page.

Status of STA/AP Swit...

Switch Mode: STA Mode

Wi-Fi

SSID Wi-Fi: NETGEAR91

Wi-Fi Password:

Encryption Mode: WPA2-personal

Network List

Name	Channel...	Signal S...	Encryption Mode	Operation
NETGEAR91	13	55	WPA2-personal	Disconnect
HAP_Q02737101	11	70	WPA2-personal	Connect
HAP_Q01786103	11	60	WPA2-personal	Connect
HAP_Q02630875	11	59	WPA2-personal	Connect
HUAWEI-B311-8E54	5	58	WPA2-personal	Connect
HAP_Q01877075	11	58	WPA2-personal	Connect
HAP_Q98998931	11	56	WPA2-personal	Connect

Save

2. Connect to a Wi-Fi.

- Manually Connect: Enter the **SSID Wi-Fi** and **Wi-Fi Password**, select **Encryption Mode** and click **Save**.
- Select from Network List: Select a target Wi-Fi from the Network list. Click **Connect** and enter Wi-Fi password and click **Connect**.

3. Click **WLAN** to enter the WLAN page.

Wi-Fi Settings **WLAN**

DHCP

IP Address: 192.168.1.138

Subnet Mask: 255.255.255.0

Gateway Address: 192.168.1.1

MAC Address: 80:9f:9b:0a:46:67

DNS1 Server Address: 192.168.1.1

DNS2 Server Address:

Save

4. Set **IP Address**, **Subnet Mask**, **Gateway Address**, and **DNS Server Address**.

 **Note**

If enable DHCP, the device will gain the Wi-Fi parameters automatically.

5. Click **Save**.

Cellular Network

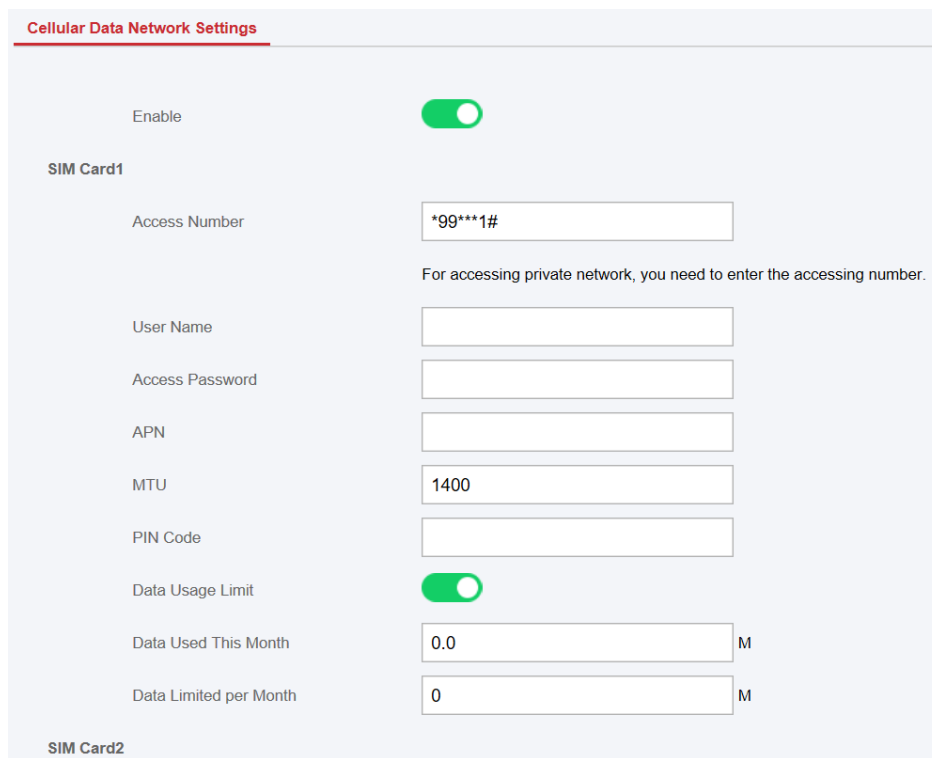
Set the cellular network parameters if you insert a SIM card inside the device. By using the cellular network, the device can upload alarm notifications to the alarm center.

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

1. Click **Communication** → **Cellular Data Network** to enter the Cellular Data Network Settings page.



The screenshot shows the 'Cellular Data Network Settings' page. At the top, the title 'Cellular Data Network Settings' is underlined in red. Below the title, there is a section for 'SIM Card1'. The 'Enable' toggle is turned on (green). The 'Access Number' field contains '*99***1#'. Below this field, a note states: 'For accessing private network, you need to enter the accessing number.' Other fields include 'User Name', 'Access Password', 'APN', 'MTU' (set to 1400), 'PIN Code', 'Data Usage Limit' (turned on), 'Data Used This Month' (0.0 M), and 'Data Limited per Month' (0 M). A section for 'SIM Card2' is visible at the bottom of the page.

 **Note**

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

2. Enable the function.
3. Set the cellular data network parameters.

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 enter the APN information.

Data Usage Limit

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.

4. Click **Save**.

Alarm Center

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

Steps

1. Click **Communication** → **Alarm Receiving Center** to enter the Alarm Receiving Center page.

Alarm Receiving Center

ARC1 ARC2 **ARC3** ARC4

Enable	<input checked="" type="checkbox"/>
Connection Type	IP
Protocol Type	ADM-CID
GMT	<input checked="" type="checkbox"/>
Address Type (Alarm Receiver Server)	IP
Server Address (Alarm Receiver Server)	0.0.0.0
Port No. (Alarm Receiver Server)	1
Account Code	
Transmission Mode	TCP
Impulse Counting Time	20 s
Attempts	3
Polling Rate	<input type="checkbox"/> Enable
Periodic Test	<input type="checkbox"/>
Companies	None

2. Select the **ARC1** or **ARC3** for configuration, and slide the slider to enable the selected alarm receiver center.

 **Note**

Only if the alarm receiver center 1/3 is enabled, you can set the alarm receiver center 2/4 as the **backup channel** and edit the channel parameters.

3. Select the **Protocol Type** as **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, ***ADM-CID**, or **CSV-IP** 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 enter the Server address, port number, account code, impulse counting time, attempts, polling rate, etc.

 **Note**

Set the polling rate with the range from 10 to 3888000 seconds.

ISUP, CSV-IP: 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 enter the IP address, port number, account code, impulse counting time, attempts, polling rate, encryption arithmetic, password length, etc.

 **Note**

Set the polling rate with the range from 10 to 3888000 seconds.

1. 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 **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) Select the **Companies** as **French Alarm Receiving Company**.
- (5) Click **Save**.

Enable
 Connection Type: IP
 Protocol Type: SIA-DCS
 GMT
 Address Type (Alarm Receiver Server): IP
 Server Address (Alarm Receiver Server): 0.0.0.0
 Port No. (Alarm Receiver Server): 1
 Account Code:
 Transmission Mode: TCP
 Impulse Counting Time: 20 s
 Attempts: 3
 Polling Rate: s Enable
 Periodic Test:
 Companies: French Alarm Receiving Company
 PIRCAM Picture Upload Mode: Picture
 HTTP Data Transmission: Default

Destination IP or Host Name	URL	Protocol	Port	Test
0.0.0.0	/	HTTP	80	<input type="button" value="Test"/>
0.0.0.0	/	HTTP	80	<input type="button" value="Test"/>

(6) Configure SMTP or FTP parameters.

Configure SMTP parameters:

Click **Communication** → **Notification by Email**.

Enable **Video Verification Events** and set corresponding parameters. For details, see Notification by Email. Click **Save**.

Notification by Email

Video Verification Events
 Sender Name:
 Sender's Address:
 SMTP Server address:
 SMTP Port: 25
 Encryption Type: None
 Server Authentication:
 User Name:
 Password:
 Confirm Password:
 Receiver Name:
 Receiver:

Configure FTP parameters:

Click **Communication** → **FTP** to enter the FTP Settings page.

Slide the slider to enable FTP and set corresponding parameters. For details, see [FTP](#). Click **Save**.

2. Upload Videos

In this condition, when the PIRCAM is set to catch more than two pictures, videos will be uploaded.

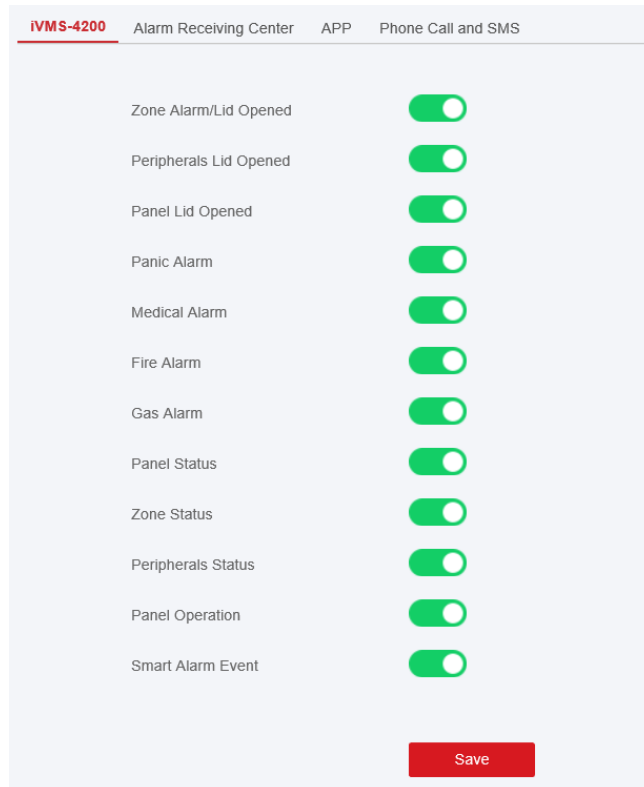
- (1) Click **Communication** → **Alarm Receiving Center** to enter the Alarm Receiving Center page.
- (2) Slide the slider to enable the selected alarm receiver center.
- (3) Select the **Protocol Type** as **SIA-DCS**.
- (4) Click **Save**.
- (5) Configure SMTP or FTP parameters as same as Upload Photos.

Notification Push

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.

Steps

1. Click **Communication** → **Event Types Notification**.



2. Enable the target notification.

Zone Alarm/Lid Opened

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.

Panic Alarm

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

Medical Alarm

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

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.

Gas Alarm

The device will push notifications when gas alarm on keypads is triggered.

Panel Status

The device will push notifications when the control panel system 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.

3. **Optional:** For **Alarm Receiving Center**, you need to select center number before settings.
4. **Optional:** If you want to send the alarm notifications to the mobile client, you should set **Phone Call and SMS** parameters.

- (1) Set the **Mobile Phone Index** and **Mobile Phone Number**.

- (2) Check **Voice Call** on **Telephone** page.
- (3) Select time of **Filtering Interval Time** and **Number of Calls**.
- (4) Check **SMS** on **Message** page.
- (5) Select areas that have arming, disarming or alarm clearing permission.

General Hint

You can import **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.



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

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

5. Click **Save**.
-



For mobile phone notification:

- You need to press * to finish the call.
 - It is required to add control code when entering the mobile phone number.
-

Cloud Service

If you want to register the device to the mobile client for remote configuration, you should set the mobile client registration 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 **Communication** → **Cloud Service** to enter the Hik-Connect Registration Settings page.

2. Check **Register to Hik-Connect**.



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. Enable **Custom Server Address**.

The server address is already displayed in the Server Address text box.

4. Select a communication mode from the drop-down list according to the actual device communication method.

Wired Network & Wi-Fi Priority

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.

5. Optional: Change the verification code.



- 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.
-

6. Enable **Periodic Test**. Enter the periodic test interval.
7. Click **Save**.

Notification by Email

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

Steps

1. Click **Communication** → **Notification by Email** to enter the page.
2. Enable **Video Verification Events** and **Server Authentication**.
3. 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.

4. Enter the receiver's information.
5. Click **Receiver Address Test** and make sure the address is correct.
6. Click **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. Click **Communication** → **NAT** to enter the page.

NAT Settings

Enable UPnP

Mapping Type

Port Type

HTTP Port

Service Port

Status

Port Type	External Port	External IP Ad..	Internal Port	UPnP Status
HTTP Port	80	0.0.0.0	80	Inoperative
Service Port	8000	0.0.0.0	8000	Inoperative

2. Drag the slider to enable UPnP.
3. **Optional:** Select the mapping type as **Manual** and set the HTTP port and the service port.
4. Click **Save** to complete the settings

FTP

You can configure the FTP server to save alarm video.

Steps

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

FTP Type

Set the FTP type as preferred or alternated.

FTP Protocol

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

Server and Port

The FTP server address and corresponding port.

User Name and Password

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

Directory Structure

The saving path of snapshots in the FTP server.

3.1.2 Device Management

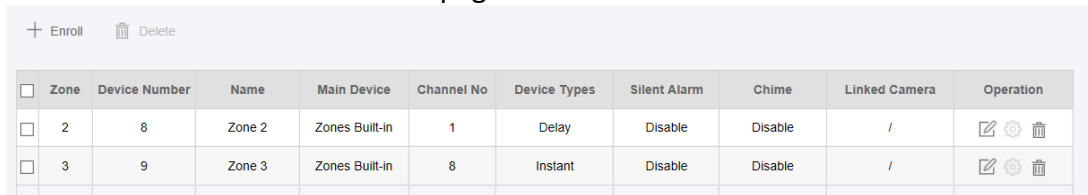
You can manage the enrolled peripherals including detector, sounder, keypad, etc. in this section.

Zone

You can set the zone parameters on the zone page.

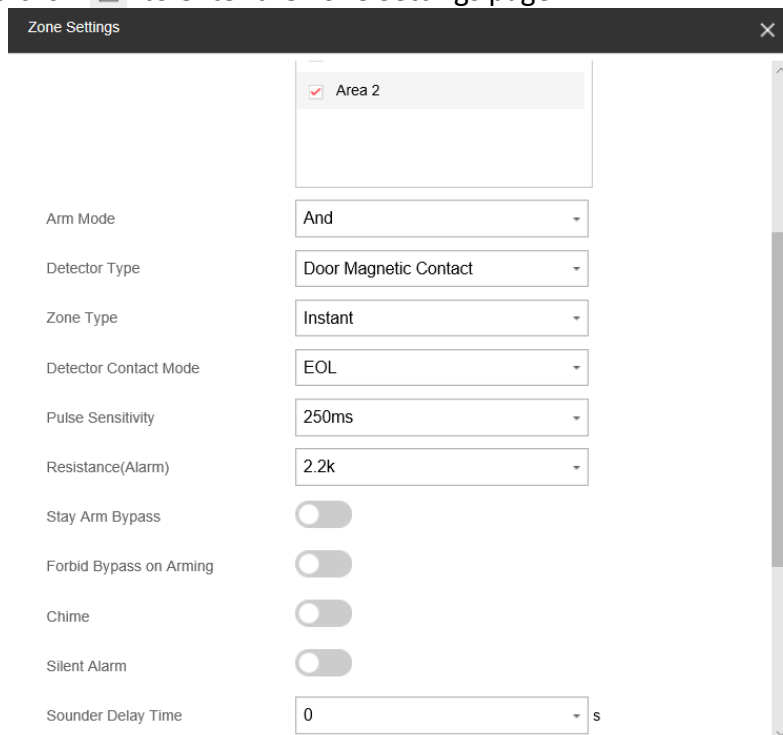
Steps

1. Click **Device** → **Zone** to enter the Zone page.



<input type="checkbox"/>	Zone	Device Number	Name	Main Device	Channel No	Device Types	Silent Alarm	Chime	Linked Camera	Operation
<input type="checkbox"/>	2	8	Zone 2	Zones Built-in	1	Delay	Disable	Disable	/	
<input type="checkbox"/>	3	9	Zone 3	Zones Built-in	8	Instant	Disable	Disable	/	

2. Select a zone and click to enter the Zone Settings page.



Zone Settings

Area 2

Arm Mode: And

Detector Type: Door Magnetic Contact

Zone Type: Instant

Detector Contact Mode: EOL

Pulse Sensitivity: 250ms

Resistance(Alarm): 2.2k

Stay Arm Bypass:

Forbid Bypass on Arming:

Chime:

Silent Alarm:

Sounder Delay Time: 0 s

3. Edit the zone name.

4. Check linked areas.

Note

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

5. (If more than one area is selected) Set **Arm Mode**.

And

When all the selected areas are armed, the zone will arm.

Or

When any of the selected areas is armed, the zone will arm

6. Select a zone type.

Instant Zone

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

Delay Zone

Exit Delay: Exit Delay provides you time to leave through the defense area without alarm.

Entry Delay: Entry Delay provides you time to enter the defense area to disarm the system without alarm.

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 keyboard for users.

Note

- You can set 2 different time durations in **System Options** → **Schedule & Timer**.
 - Ensure that timer is no longer than 45 seconds in order to comply with EN50131-1.
 - You can set Stay Arm Delay Time for the delay zone.
-

Panic Zone

The zone activates all the time. It is usually used in the sites equipped with panic button, smoke detector and glass-break detector.

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

The linked area will arm after being triggered, and disarm after being restored. In the case of the tampering alarm, the arming and disarming operation will not be triggered.

Note

Two trigger types (by trigger times and by zone status) can be selected for the zone. If the zone status type is selected, set the trigger operation (trigger arming/disarming).

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/siren output when alarm occurs. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

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. 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).

Fire Zone

The zone activates all the time with sound or sounder output when alarm occurs. It is usually used in fire hazardous areas equipped with smoke detectors and temperature sensors.

Gas Zone

The zone activates all the time with sound or sounder output when alarm occurs. It is usually used in areas equipped with gas detectors (e.g., the kitchen).

Medical Zone

The zone activates all the time with beep confirmation when alarm occurs. It is usually used in places equipped with medical emergency buttons.

7. Enable other functions according to your detector types and actual needs.



Note

The configurable functions vary in different detectors and zones. Refer to the actual zone to set the function.

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

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.

Dual Zone

After enable the dual zone, one zone can be expanded to two zones.

Sounder Delay Time

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

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


 **Note**

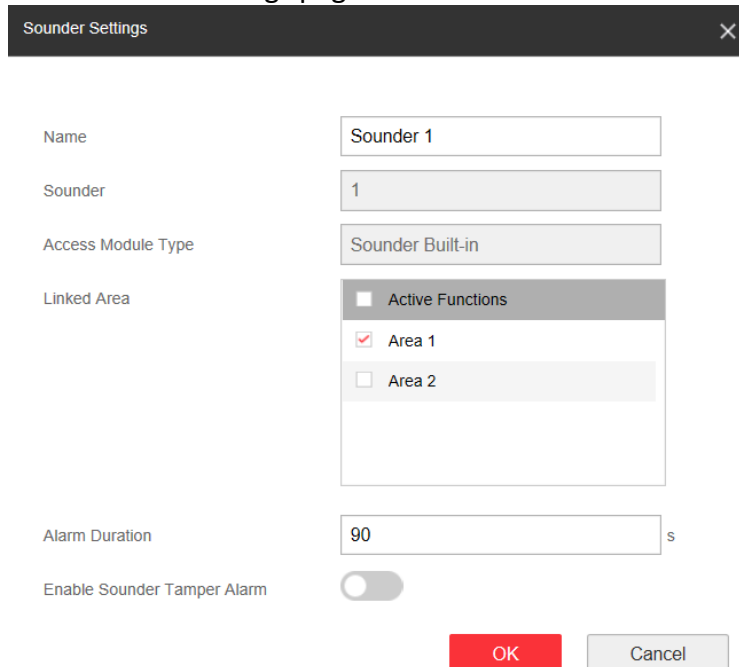
After setting the zone, you can enter **Maintenance** → **Device Status** → **Zone Status** to view the zone status.

Sounder

Set sounder parameters.

Steps

1. Click **Device** → **Sounder** to enter the Sounder page.
2. Click  to enter the Sounder Settings page.



Sounder Settings

Name: Sounder 1

Sounder: 1

Access Module Type: Sounder Built-in

Linked Area:

- Active Functions
- Area 1
- Area 2

Alarm Duration: 90 s

Enable Sounder Tamper Alarm:

OK Cancel

3. Set the sounder name and alarm duration.
4. Check the linked area.

 **Note**

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

6. Enable **Sounder Tamper Alarm**.
7. Click **OK**.


Note

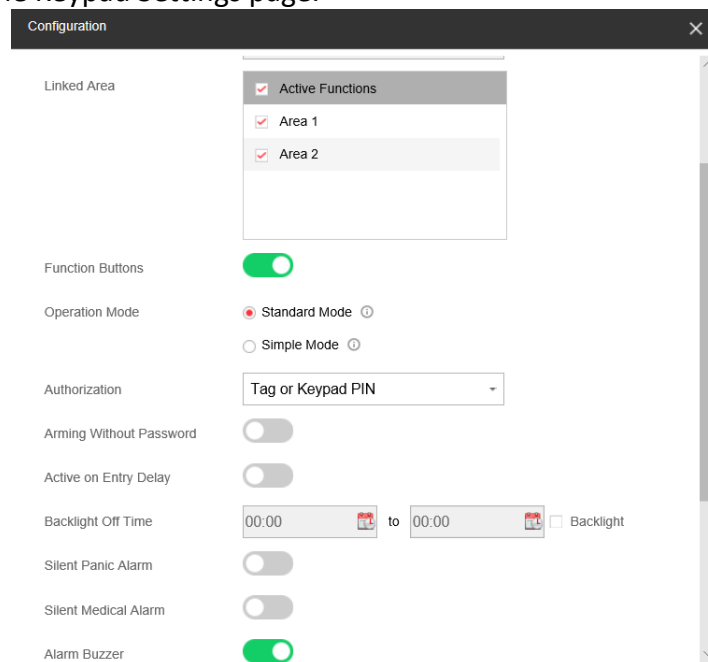
After the sounder is configured, you can click **Maintenance** → **Device Status** → **Sounder Status** to view the sounder status.

Keypad

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

Steps

1. Click **Device** → **Keypad** to enter the page.
2. Click  to enter the Keypad Settings page.



3. Set the keypad name.
4. Check linked areas.
5. Select the keypad mode.
6. Enable the function according to your actual needs.

Authorization

Only standard mode has this function. You can select the authorization method.

Active on Entry Delay

When someone enters the delay zone, the screen and backlight of the keypad will be on. This function can indicate the keypad position for those who enter the delay zone at night.

Keypad Arming Light

Enable the arming indicator of the keypad.

 **Note**

- Only enabled areas will be listed.
 - The newly added peripheral is linked to area 1 by default.
 - For detailed information, refers to the keypad user manual.
-

7. Click **OK**.


 **Note**

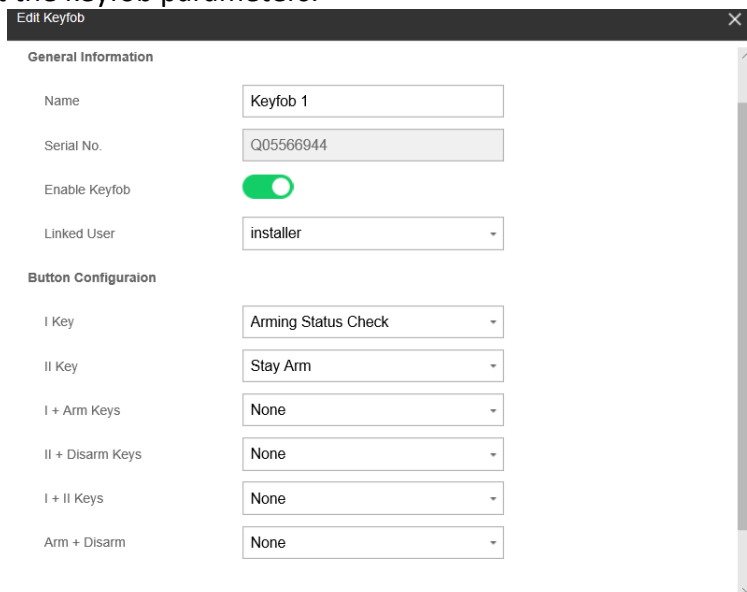
- After the keypad is configured, you can click **Maintenance** → **Device Status** → **Keypad Status** to view the keypad status.
 - You can set the keypad password on the page of **User** → **User Management** → **Operation**.
-

Keyfob

You can set the parameters of the keyfob.

Steps

1. Click **Device** → **Keyfob** to enter the page.
2. Click **Enroll** to add a keyfob.
3. Click  to edit the keyfob parameters.




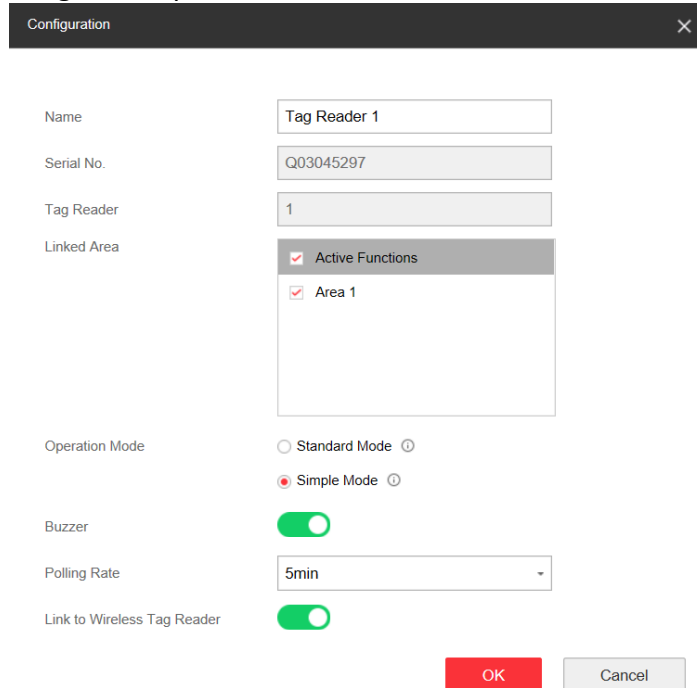
4. Enable the keyfob.
5. Select a linked user.
6. Configure the functions of the buttons according to your actual needs.
7. Click **OK**.

Tag Reader

You can set the parameters of the tag reader.

Steps

8. Click **Device** → **Automation** to enter the page.
9. Click **Enroll**, enter the serial No. to add a tag reader.
10. Click  to edit the tag reader parameters.



The screenshot shows a 'Configuration' dialog box with the following fields and options:

- Name:** Tag Reader 1
- Serial No.:** Q03045297
- Tag Reader:** 1
- Linked Area:** A list containing 'Active Functions' and 'Area 1', both of which are checked.
- Operation Mode:** Radio buttons for 'Standard Mode' (unselected) and 'Simple Mode' (selected).
- Buzzer:** A green toggle switch that is turned on.
- Polling Rate:** A dropdown menu set to '5min'.
- Link to Wireless Tag Reader:** A green toggle switch that is turned on.

At the bottom right of the dialog are two buttons: a red 'OK' button and a grey 'Cancel' button.

11. Edit device name.
12. Check linked areas.
13. Select operation mode.

Standard Mode

Area selection and fault confirmation are supported when swiping tag to arm or disarm.

Simple Mode


No Area selection and fault confirmation when swiping tag to arm or disarm.

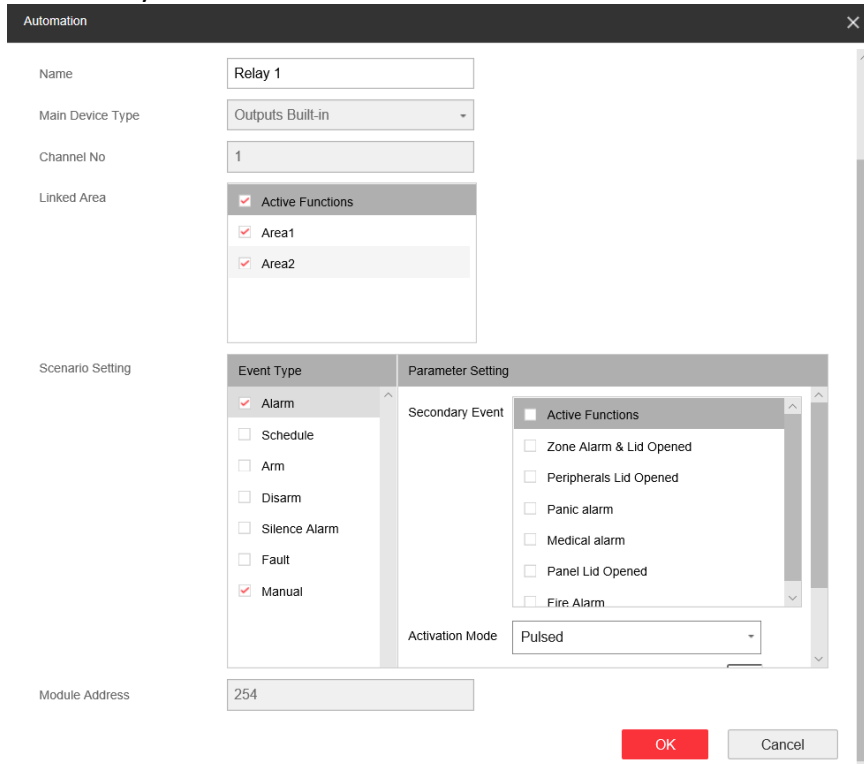
14. Choose whether to enable the **Buzzer**. After disable the buzzer, there will be no beep when swiping the tag.
15. Set **Polling Rate**.
16. **Optional:** Enable **Link to Wireless Tag Reader**.
17. Click **OK**.

Automation

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

Steps

1. Click **Device** → **Automation** to enter the page.
2. Click **Enroll**, enter the serial No. and select the main device type, main device name, channel to add a relay output device.
3. Click  to edit the relay information.



The screenshot shows the 'Automation' configuration window. It has a title bar with a close button. The main area is divided into several sections:

- Name:** Relay 1
- Main Device Type:** Outputs Built-in
- Channel No:** 1
- Linked Area:** A list with checkboxes for 'Active Functions', 'Area1', and 'Area2'. All are checked.
- Scenario Setting:** A list with checkboxes for 'Alarm', 'Schedule', 'Arm', 'Disarm', 'Silence Alarm', 'Fault', and 'Manual'. 'Alarm' and 'Manual' are checked.
- Secondary Event:** A list with checkboxes for 'Active Functions', 'Zone Alarm & Lid Opened', 'Peripherals Lid Opened', 'Panic alarm', 'Medical alarm', 'Panel Lid Opened', and 'Fire Alarm'. 'Active Functions' is checked.
- Activation Mode:** Pulsed
- Module Address:** 254

At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Select the modified output No.
5. Set the relay name.
6. Select the linked area.

Note

- Only enabled areas will be listed.
 - The newly added peripheral is linked to area 1 by default.
 - The function varies according to different relay types
-

7. Set event type and its parameters:

Secondary Event

The sub-event type of alarm, arm, disarm and fault event.

Activation Mode

Latched: Continue the output until the relay is manually closed or opened.

Pulsed: The relay will be closed/open after the set duration.

Contact Status

Normally Open: Under normal conditions, the relay is open. When the event is triggered, the relay will be closed.

Normally Closed: Under normal conditions, the relay is closed. When the event is triggered, the relay will be open.

Schedule

You can set the close/open time for the relay.

8. Click **OK**.

Network Camera

You can add network cameras in the system.

Steps

1. Click **Device** → **Camera** to enter the page.
2. Click **Enroll**, enter the IP address, user name and password to add a camera.

3. Click  to edit the camera information.

You can also click **Edit** to edit the camera, or click **Delete** to delete the 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.

Module

Set module parameters.

Steps

1. Click **Device** → **Module** to enter the page.

2. Click  edit the paramters.
3. Select linked areas.
4. Enable **AUX** according to your needs. It will enable the auxiliary power output of the module.
5. Click **OK**.

3.1.3 Area Settings

Basic Settings

You can link zones to the selected area.

Steps

1. Click **Area** → **Basic Settings** to enter the page.
2. Select an area.
3. Check **Enable**.
4. Check the check box in front of the zone to select zones for the area.
5. Click **Save** to complete the settings.

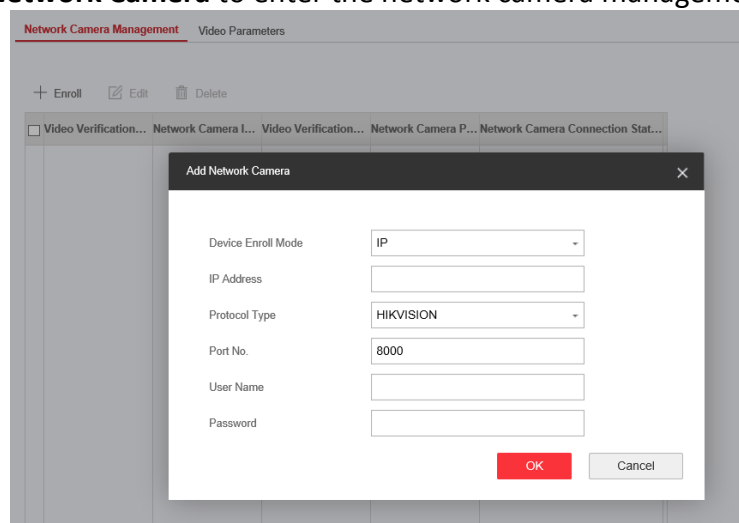
3.1.4 Video Management

You can add network cameras (4 for DS-PHA64-LP /2 for DS-PHA48-EP) to the AX HYBRID PRO , and link the camera with the selected zone for video monitoring. You can also receive and view the event video via client and Email.

Add Cameras to the AX HYBRID PRO

Steps


1. Click **Device** → **Network Camera** to enter the network camera management page.



2. Click **Enroll**, and enter the basic information of the camera, such as IP address and port No., and select the protocol type.
3. Enter the user name and password of the camera.
4. Click **OK**.
5. Optional: Click **Edit** or **Delete** to edit or delete the selected camera.

Link a Camera with the Zone

Steps

1. Click **Device** → **Zone** to enter the configuration page.
2. Select a zone that you wish to include video monitoring, and click .
3. Select the **Link Camera**.
4. Click **OK**.

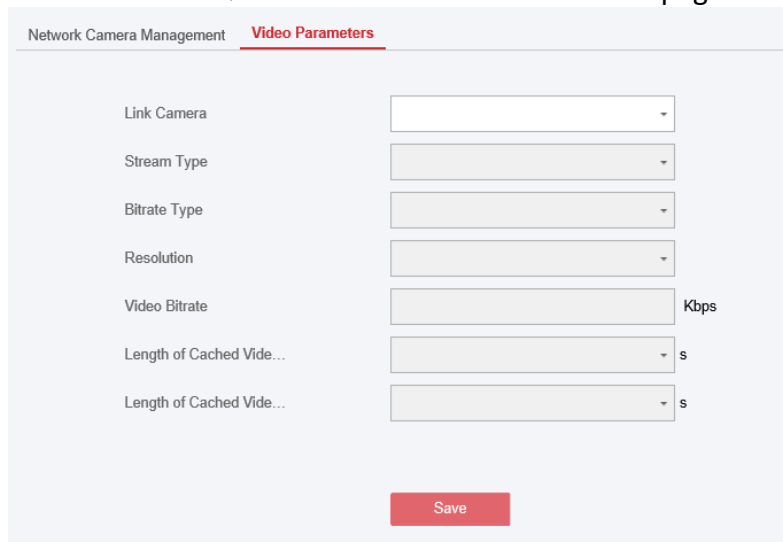
Note

Only if the zone is linked with a network camera, the alarm email will be attached with alarm video.

Set Video Parameters

Steps

1. Click **Device** → **Network Camera** → **Video Parameters** to enter the page.



2. 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.

Video Bitrate

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

3.1.5 Permission Management

Add/Edit/Delete Keyfob

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

Steps

1. Click **Device** → **Keyfob** to enter the Keyfob Management page.
2. Click **Enroll** and press any key on the keyfob.
3. Set the keyfob parameters.

Name

Customize a name for the keyfob.

Permission Settings


Check different items to assign permissions.

Single Key Settings

Select from the drop-down list to set I key and II key's functions

Combination Keys Settings

Select from the drop-down list to set combination keys' functions.

4. Click **OK**.
5. Optional: Click  to edit the keyfob information.
6. Optional: Delete a single keyfob or check multiple keyfobs and click **Delete** to delete the keyfobs in batch.

 **Note**

The communication of wireless devices like keyfob was identified by the SN number, which will be encrypted during transmission. The SN number was leading with character Q to Z, and following 8 digits, like Q02235774. Allowing for a maximum number of 100,000,000 (10 to the power of 8 [digits]).

Add/Edit/Delete Tag

You can add tag to the AX HYBRID PRO and you can use the Tag to arm/disarm the zone. You can also edit the tag information or delete the tag from the AX HYBRID PRO .

 **Note**

The communication of tag was identified by the SN number, which will be encrypted during transmission. The SN number was leading with 32 digits, and there are at most 4,294,967,296 SN numbers can be identified.

Steps

1. Click **Device** → **Tag** to enter the management page.
2. Click **Enroll** and place a tag on the tag area of the keypad.
3. Customize a name for the tag in the pop-up window.
4. Select the tag type and tag linked area.
5. Select the permission for the tag.


 **Note**

You should allocate at least a permission for the tag.

6. Click **OK** and the tag information will be displayed in the list.

 **Note**

The Tag supports at least 20-thousand serial numbers.

7. Optional: Click  and you can change the tag name.
8. Optional: Delete a single tag or check multiple tags and click **Delete** to delete tags in batch.

3.1.6 Maintenance

Device Information

You can view device name and other information.

Click **Maintenance** → **Device Information** to enter the page.

You can view device model, device serial No., device firmware version, web version or click **About** → **View Licenses** to view the source software licenses.

You can go to **System** → **System settings** to change the device name.

Local Log Search

You can search the log on the device.

Click **Maintenance** → **Log** to enter the Local Log Search page.

No.	Date and Time	Primary Ev...	Secondary Event	User	Remote Ho...	Managed...	Param...	Additional Inf...
-----	---------------	---------------	-----------------	------	--------------	------------	----------	-------------------

Select a major type and a minor type from the drop-down list, set the log start time and end time and click **Filter**. All filtered log information will be displayed in the list.

You can also click **Reset** to reset all search conditions.

Test

The AX HYBRID PRO supports walk test function.

Steps

1. Enter **Maintenance** → **Device Maintenance** → **Test** to enable the function.

Test Maintenance Export File Security Audit Log

Test

Test Mode

Zone No.	Name	Test Result
1	Zone 2	Invalid zone.
2	Zone 3	Invalid zone.

Save Refresh


 **Note**

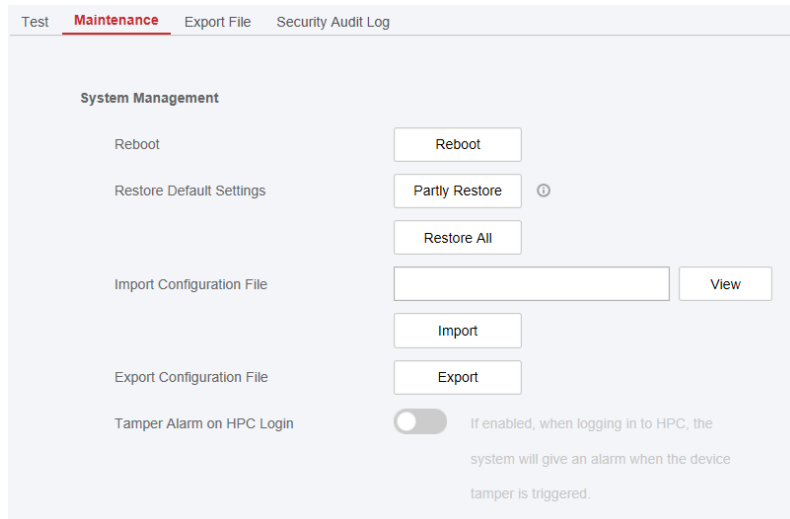
Only when all the detectors are without fault, you can enter the mode TEST mode.

2. Enable **Test** to start walk test.
3. Click **Save** to complete the settings.
4. Trigger the detector in each zone.
5. Check the test result.

System Maintenance

You can reboot the device, restore default settings, import/export configuration file.

Select the device and click  in the client software, or enter the device IP address in the address bar of the web browser. Click **Maintenance** → **Device Maintenance** → **Maintenance** to enter the page.



Reboot

Click **Reboot** to reboot the device.

Restore Default Settings

Click **Partly Restore** to restore all parameters except for admin user information, wired network, Wi-Fi network, detector information, and peripheral information to default ones. Click **Restore All** to restore all parameters to the factory settings.

Import Configuration File

Click **View** to select configuration file from the PC and click **Import Configuration File** to import configuration parameters to the device. Importing configuration file requires entering the password set at the time of exporting.

Export Configuration File

Click **Export Configuration File** to export the device configuration parameters to the PC. Exporting configuration file requires a password to be used for file encryption.

Tamper Alarm on HPC 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.)

Export File

You can export debugging file to the PC.

Steps

1. Click **Maintenance** → **Device Maintenance** → **Export File** to enter the page.

The screenshot shows a web interface with a navigation bar containing 'Test', 'Maintenance', 'Export File' (highlighted in red), and 'Security Audit Log'. Below the navigation bar, there are two rows of settings: 'Debugging Log' with a green toggle switch turned on, and 'File Format' with a dropdown menu showing 'Debugging Log'. Below these settings are two buttons: a grey 'Export' button and a red 'Save' button.

2. Check the check box to enable the function.
3. Click **Export** to save the debugging file in the PC.

Security Audit Log

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

Steps

2. Click **System Maintenance** → **Device Maintenance** → **Security Audit Log** to enter the page.

The screenshot shows the 'Advanced Settings' page. At the top, there is a section 'Advanced Settings' with a checked checkbox 'Enable Log Upload Server'. Below this is the 'Server Settings' section with two input fields: 'Log Server IP' containing '0.0.0.0' and 'Log Server Port' containing '0'. The 'CA Certificate' section has an 'Install' button and a 'View' button. At the bottom of the page is a red 'Save' button.

3. Check **Enable Log Upload Server**.
4. Enter log server IP and port.
5. Click **View** to select a certificate.

Note

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

6. Click **Install**.
7. Click **Save**.

3.1.7 System Settings

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 Guarding Vision** server.

Time Management

Click **System** → **System Settings** → **Time Management** to enter the Time Management page.

System Settings **Time Management** DST Management

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

Time Synchronization

Synchronization Mode: NTP Time Sync Manual Time Sync

Date and Time: 2021-05-31 08:29:56

PC Sync: 2021-05-31 08:29:31 Sync. With Computer Time

Save

You can select a time zone from the drop-down list.

You can synchronize the device time automatically with NTP. Check the check box of **NTP Time Sync.**, enter the server address and port No., and set the synchronization interval.

You can synchronize the device time manually. Or check **Sync. with Computer Time** to synchronize the device time with the computer time.

Note

While you synchronize the time manually or with the computer time, the system records the log “SDK Synchronization”.

DST Management

Click **System** → **System Settings** → **DST Management** to enter the Time Management page.

System Settings Time Management **DST Management**

Enable DST:

DST Bias: 60 Minute(s)

Start Time: April First Sunday 02

End Time: October Last Sunday 02

Save

You can enable the DST and set the DST bias, DST start time, and DST end time.

Authority Management

Set the authority options.

Click **System** → **System Options** → **System Management** to enter the page.

System Management | Schedule & Timer | System Fault Check | Arm Options | Device Enroll Mode

Forced Auto Arm

Forced Arming

System Status Report

Audible Tamper Alarm

Panel Lockup Button

Bypass On Re-Arm The bypassed zone will back to arm if fault restored.
The system will not be compliant with the Europe EN50131-1 standard after you enable this configuration option.

Enable PD6662

Communication Fault Sending Delay s
The configuration is for the delay time while the ATP communication fault reports to ARC.

PD6662 configuration

Keypad logout min

Save

Forced Auto Arm

After enabled, when the timed automatic arming starts, if there are an active faults in a zone, the zone will be automatically bypass.

Note

You should disable the arming function in the Advanced Settings page. Or the AX HYBRID PRO arming with fault function cannot be valid.

Forced Arming

After enabled, when manual arming starts, if there are an active faults in a zone, the zone will be automatically bypass.

System Status report

If the option is enabled, the device will upload report automatically when the AX HYBRID PRO status is changed.

Audible Tamper Alarm

While enabled, the system will alert with buzzer for the tamper alarm.

Panel Lockup Button

Enable/disable the lockup button for the control panel.

Bypass on Re-Arm

While enabled, the zone with fault will be bypassed automatically when re-arming.

Enable PD6662

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

Keypad Logout

Keypad logout time. If the keypad does not be operated beyond the set time, the user will log out automatically.

Schedule and Timer Settings

You can set the alarm schedule. The zone will be armed/disarmed according to the configured time schedule.

Steps

1. Click **System** → **System Options** → **Schedule & Timer** to enter the Schedule & Timer page.

The screenshot shows the 'Schedule & Timer' configuration page. At the top, there are navigation tabs: 'System Management', 'Schedule & Timer' (highlighted), 'System Fault Check', 'Arm Options', and 'Device Enroll Mode'. The main content area is divided into several sections:

- Area:** A dropdown menu set to 'Area1'.
- Enable auto Arm:** A toggle switch that is currently turned off. Below it is a 'Time' field set to '00:00' with a calendar icon.
- Enable auto Disarm:** A toggle switch that is currently turned off. Below it is a 'Time' field set to '00:00' with a calendar icon.
- Late to Disarm:** A toggle switch that is currently turned off. Below it is a 'Time' field set to '00:00' with a calendar icon.
- Weekend Exception:** A green toggle switch that is turned on. Below it are checkboxes for 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', 'Saturday', and 'Sunday'. 'Saturday' and 'Sunday' are checked.
- Holiday Exception:** A green toggle switch that is turned on. Below it is a 'Holiday 1' field with two date pickers set to '02-15' and a range separator '-'. There are 'x' and '+' icons next to the date pickers.
- Panel Alarm Duration:** A text input field containing the number '90' and a unit 's'.

At the bottom center, there is a red 'Save' button.

2. Select an area.
3. Set the following parameters according to actual needs.

Enable 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.

- The buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.
 - You can select to enable forced arming on the System Options page. While the function is enabled, the system will be armed regardless of the fault.
-

Enable 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.
-

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.

Note

You should enable the Panel Management Notification function in **Communication Parameters** → **Event Communication** before enabling the Late to Disarm function.

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.

Note

Up to 6 holiday groups can be set.

Panel Alarm Duration

The time duration of the panel alarm.

Note

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

5. Click **Save**.

Fault Check

The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.

Click **System** → **System Options** → **System Fault Check** to enter the page.

Detect Network Camera Disconnection	<input checked="" type="checkbox"/>
Panel Battery Fault Check	<input checked="" type="checkbox"/>
LAN Fault Check	<input checked="" type="checkbox"/>
WiFi Fault Check	<input checked="" type="checkbox"/>
Cellular Fault Check	<input checked="" type="checkbox"/>
Main Power Lost	<input checked="" type="checkbox"/>
AC Power Loss Delay	<input type="text" value="10"/> s

Save

Detect Network Camera Disconnection

If the option is enabled, when the linked network camera is disconnected, an alarm will be triggered.

Panel Battery Fault Check

If the option is enabled, when battery is disconnected or out of charge, the device will upload events.

LAN Fault Check

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

Wi-Fi Fault Check

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

Cellular Network Fault Check

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

Main Power Lost

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

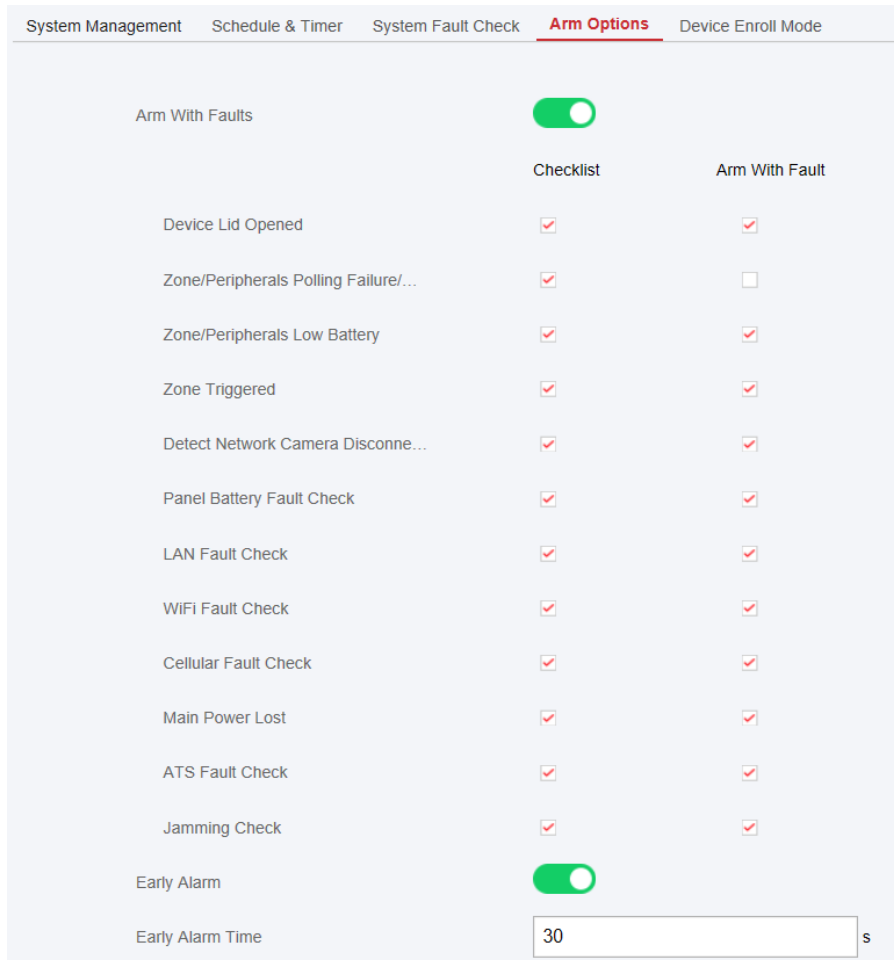
Main Power Loss Delay

The system checks the fault after the configured time duration after AC power down. To compliant the EN 50131-3, the check time duration should be 10 s.

Arm Options

Set advanced authority parameters.

Click **System** → **System Options** → **Arm Options** to enter the Advanced Settings page.



You can set the following parameters:

Arm with Fault

Check the faults in the Enable Arming with Fault list, and the device will not stop the arming procedure when faults occurred.

Fault Checklist

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

Early Alarm

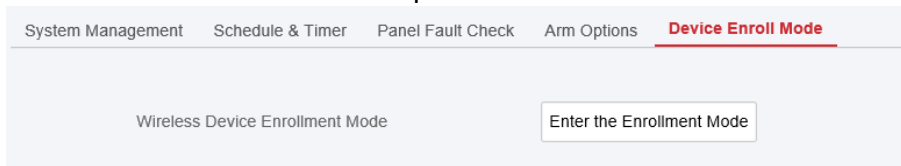
If you enable the function, when the zone is armed and the zone is triggered, the alarm will be triggered after the set delay time.

Note

The early alarm will be taken effect only after the delayed zone is triggered.

Device Enroll Mode

Click Enter the Enrollment Mode to make the panel enter the enroll mode.

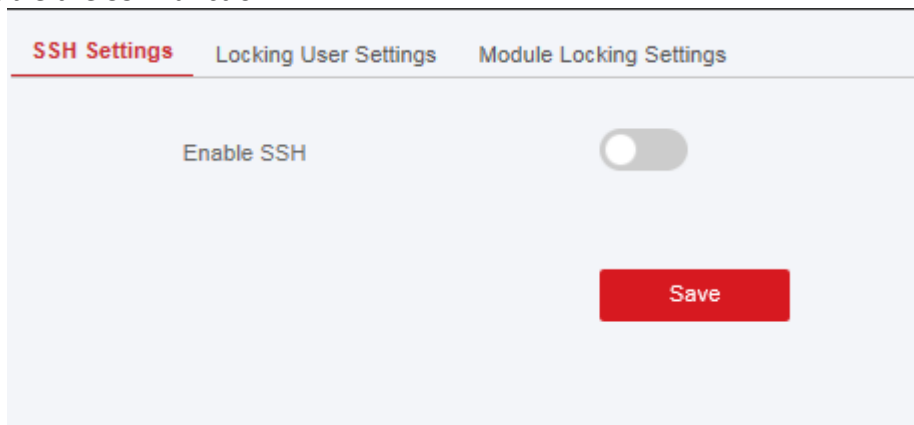


Security Settings

SSH Settings

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.



Locking User Settings

The device will be locked 90 s after 3 failed credential attempts (can be set in Retry Time 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 **System** → **System Security** → **User Lockout Attempts** to enter the Locking User Settings page.

SSH Settings **User Lockout Attempts** Module Locking Settings

Retry Times Before Aut...

Auto-lock Time s

No.	IP Address	Unlock

2. Set the following 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.

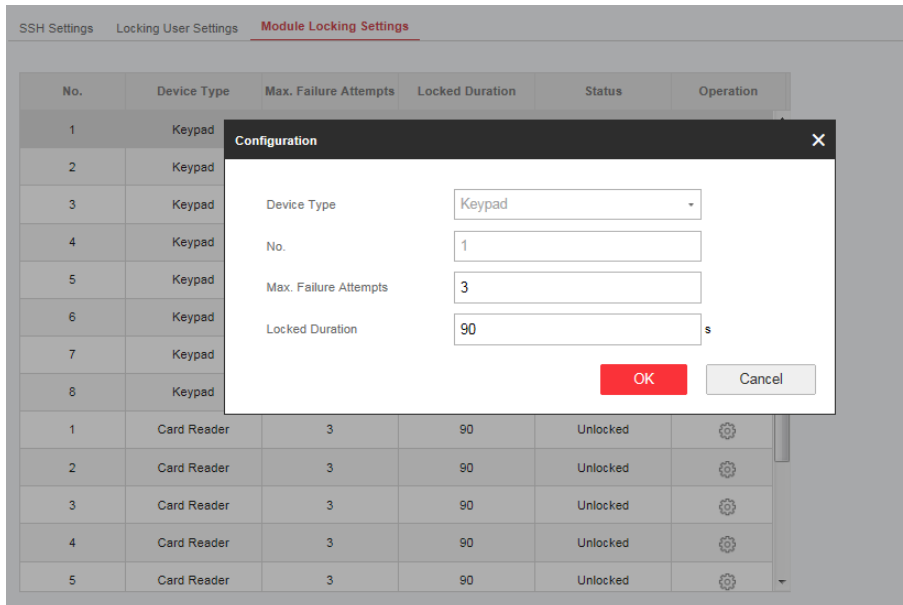
4. Click **Save**.

Module Lock Settings

Set the module locking parameters, including the Max Failure Attempts, 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 **System** → **System Security** → **Module Locking Settings** to enter the Module Lock Settings page.



2. Select a module from the list, and click the icon.
3. Set the following parameters of the selected module.

Max. Failure Attempts

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.

Locked Duration

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

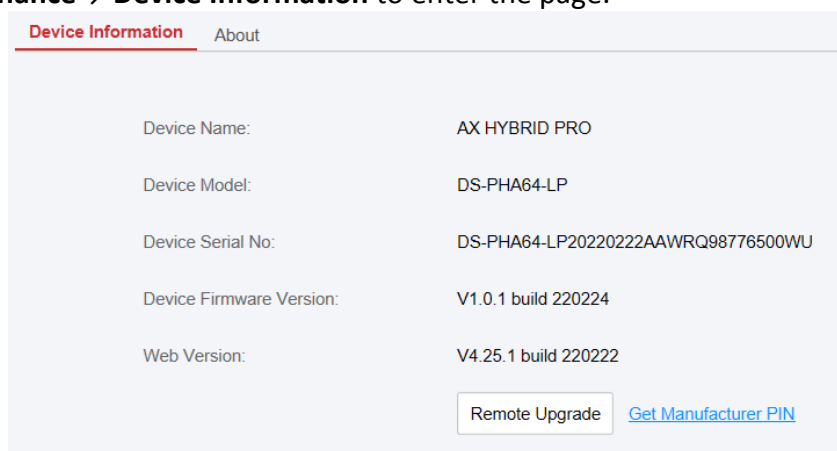
4. Click **OK**.
5. Optional: Click the **Lock** icon to unlock the locked module.

Device Upgrade

Only installer can upgrade the device on web client.

Steps:

1. Click **Maintenance** → **Device Information** to enter the page.



2. Click **Get Manufacturer PIN** to view the PIN.
3. Click **Remote Upgrade** and enter the PIN.
4. Click **OK** to complete.

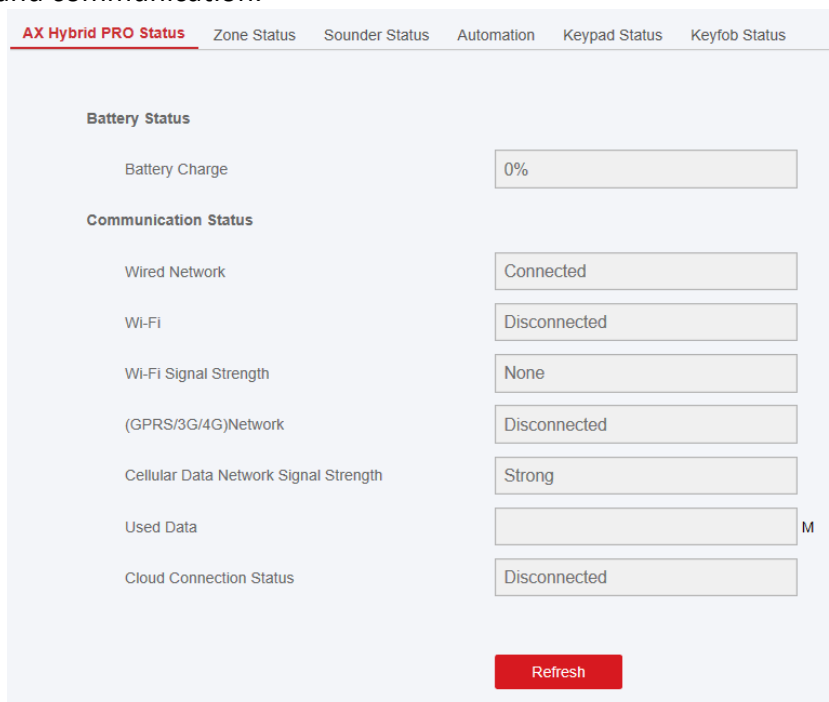
 **Note**

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

3.1.8 Check Status

After setting the zone, repeater, and other parameters, you can view their status.

Click **Maintenance** → **Device Status**. You can view the status of zone, relay, sounder, keypad, Tag reader, battery, and communication.



The screenshot shows the 'AX Hybrid PRO Status' page with several tabs: 'AX Hybrid PRO Status' (selected), 'Zone Status', 'Sounder Status', 'Automation', 'Keypad Status', and 'Keyfob Status'. The 'Battery Status' section shows 'Battery Charge' at 0%. The 'Communication Status' section shows: 'Wired Network' (Connected), 'Wi-Fi' (Disconnected), 'Wi-Fi Signal Strength' (None), '(GPRS/3G/4G)Network' (Disconnected), 'Cellular Data Network Signal Strength' (Strong), 'Used Data' (empty field with 'M' next to it), and 'Cloud Connection Status' (Disconnected). A red 'Refresh' button is at the bottom.

- Zone: You can view the zone status, alarm status, detector battery capacity, and signal strength.
- Sounder: You can view sounder status, battery status, and signal strength.
- Output: You can view relay status, battery status, and signal strength.
- Keypad: You can view keypad status, battery status, and signal strength.
- Repeater: You can view repeater working status.
- Tag Reader: You can view Tag reader status, battery status, and signal strength.
- Transmitter: You can view Transmitter status, battery status, and signal strength.

3.2 Report to ARC (Alarm Receiver Center)

AX HYBRID 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.

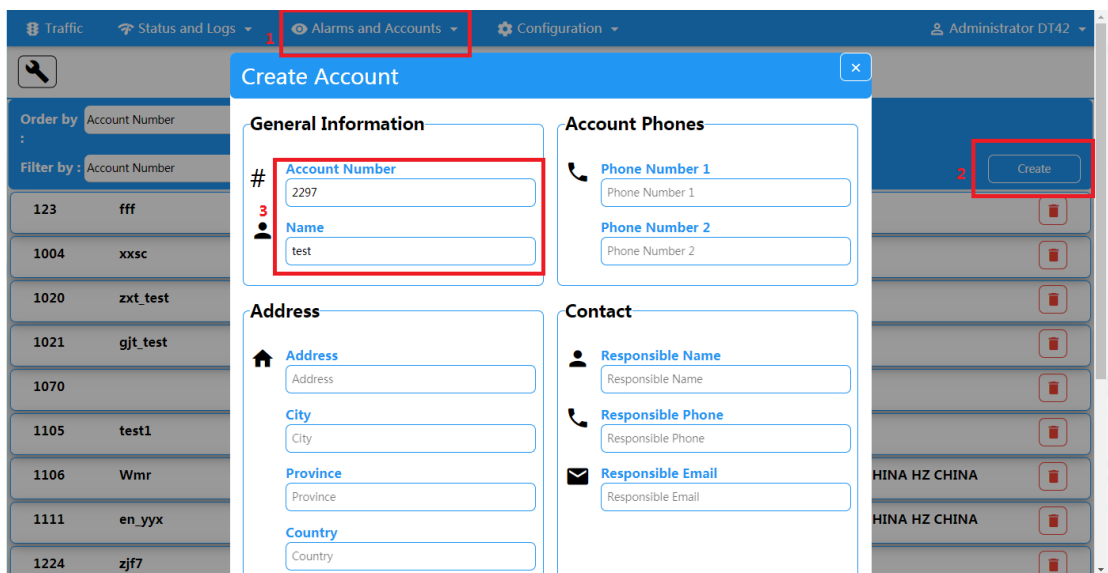
Setup ATS in Transceiver of Receiving Center

Steps:

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



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



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**.

Alarm Receiver Center1

Enable

Protocol Type *ADM-CID

Address Type IP

Server Address 115.236.50.3

Port No. 6666

Account Code 2297

Transmission Mode TCP

Impulse Counting Time 20 s

Attempts 3 ✓

Polling Rate 60 ✓ s Enable

Encryption Arithmetic AES

Password Length 128

Secret Key 123456789012345678901234567

● = 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.

The screenshot shows a web interface for monitoring traffic. The top navigation bar includes 'Traffic', 'Status and Logs', 'Alarms and Accounts', and 'Configuration'. The main header is 'Traffic' with a 'Refresh in 16' indicator. Below the header, there are controls for 'Order by' (Reception Time) and 'Filter by' (Event ID). A table of events is displayed, with one event highlighted by a red box:

Event 580777	Account : 2297	Zone : 1	Partition : 01	Receiver.# : 1	Code : E120	Line.# : 0	2020-03-28 12:01:42
Description : Panic Alarm / 001							
Event 580776							2020-03-28 12:01:36

Chapter 4 General Operations

4.1 Access Entries

The installer and operators of the AX HYBRID PRO 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-ProConnect Service**
Hik-ProConnect 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-ProConnect 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-ProConnect 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.

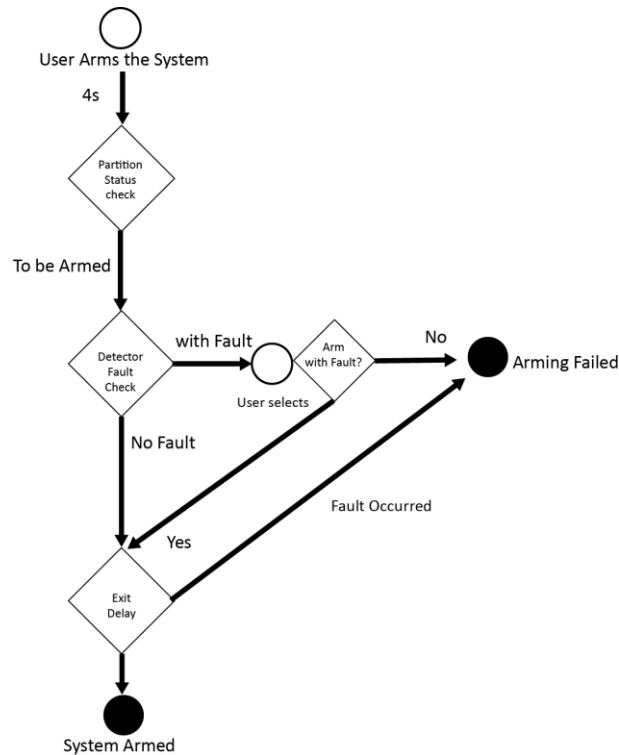
Access Entries for the Administrator and Operators (Access Level 2)

- **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.

4.2 Arming

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



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.
- Lid opened (tamper) 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.

4.3 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 either the intrusion or tampering alarm occurs on the enter/exit route when the AX HYBRID PRO is in the status of entry delay, the AX HYBRID PRO then enters the early alarm mode.

The early alarm duration can be set (> 30s).

The AX HYBRID PRO will reports the alarm only if the alarm event lasts over the duration of early alarm with the addition of entry delay.

4.4 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 Enrollment 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 enrollment 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 Arming Process is Not Started)

Fault Description:

When the panel is arming, prompt arming fails.

Solution:

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

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 Alarm Clearing Operation on the Panel Does Not Produce the Alarm Clearing 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	<p>The system will immediately alarm when it detects triggering event after system armed.</p> <p>Audible Response Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X alarm.</p>
Perimeter Zone	<p>The system will immediately alarm when it detects triggering event after system armed.</p> <p>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.</p> <p>Voice Prompt: Zone X perimeter alarm.</p>
Delayed Zone	<p>The system provides you time to leave through or enter the defense area without alarm.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X alarm.</p>
Follow Zone	<p>The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X follow alarm.</p>
24H Silence Zone	<p>The zone activates all the time without any sound/sounder output when alarm occurs.</p> <p>Audible Response: No system sound (voice prompt or sounder).</p>
Panic Zone	<p>The zone activates all the time.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X panic alarm.</p>
Fire Zone	<p>The zone activates all the time with sound/sounder output when alarm occurs.</p>

Input Types	Operations
	<p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X fire alarm.</p>
Gas Zone	<p>The zone activates all the time with sound/sounder output when alarm occurs.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X gas alarm.</p>
Medical Zone	<p>The zone activates all the time with beep confirmation when alarm occurs.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X medical alarm.</p>
Timeout Zone	<p>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.</p>
Disabled Zone	<p>Alarms will not be activated when the zone is triggered or tampered.</p> <p>Audible Response: No system sound (voice prompt or sounder).</p>
Virtual Zone (Keypad/Keyfob)	<p>The system will immediately alarm when it detects triggering event after system armed.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Buzzer beeps.</p>
Tamper Alarm (Lid Opened Alarm)	<p>The system will immediately alarm when it detects triggering event after system armed.</p> <p>Audible Response: Trigger the system sound and sounder.</p> <p>Voice Prompt: Zone X tampered.</p>
Link	<p>Trigger the linked device when event occurs.</p> <p>e.g. The output expander linked relays will be enabled when the AX HYBRID PRO is armed.</p>
Arm	<p>When armed: Voice prompt for fault. You can handle the fault according to the voice prompt.</p> <ul style="list-style-type: none"> ● System sound for arming with Tag or keyfob. ● Voice prompt for fault. You can handle the fault according to the voice prompt.

Input Types	Operations
	<p>Fault event displays on client. You can handle the fault via client software or mobile client.</p> <ul style="list-style-type: none">● Voice Prompt: Armed/Arming failed.

C. Output Types

Table C-1 Output Types

Output Types	Active	Restore
Arming	Arm the AX HYBRID PRO	After the configured output delay
Disarming	Disarm the AX HYBRID 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 HYBRID 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	x/v	√	√	√	√
Life Safety Event	x/v	√	√	√	√
System Status	x/v	√	x	x	x
Panel Management	x/v	√	x	x	x

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.

^bBy the condition of being accredited by user in level 2 and level 3.

^dUsers 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 below is for transmitting from the security control panel to ARC via DC09 protocol.

Table F-1 SIA and CID Code

SIA code	CID code	Description
MA	1100	Medical Alarm
MH	3100	Medical Alarm Restored
BA	1130	Burglary Alarm
BH	3130	Burglary Alarm Restored
FA	1110	Fire Alarm
FH	3110	Fire Alarm Restored
HA	1121	Duress alarm
HA	1122	Silent Panic Alarm
HH	3122	Silent Panic Alarm Restored
	1133	24H Alarm
	3133	24H Alarm Restored
	1133	24H Alarm
	3133	24H Alarm Restored
NA	1780	Timeout Alarm
BH	3780	Timeout Alarm Restored
PA	1120	Audible Panic Alarm
PH	3120	Audible Panic Alarm Restored
BA	1130	Burglary Alarm
BH	3130	Burglary Alarm Restored
BA	1131	Perimeter Breached
BH	3131	Perimeter Restored
		Interior Burglary Alarm
		Interior Burglary Alarm Restored
BA	1133	24H Alarm
BH	3133	24H Alarm Restored
BA	1134	Burglary Alarm
BH	3134	Burglary Alarm Restored
TA	1137	Lid Opened
TR	3137	Lid Restored
BV	1139	Confirmed Alarm
BW	3139	Confirmed Alarm Restore
		BUS Open-circuit Alarm

SIA code	CID code	Description
		BUS Open-circuit Restored
		BUS Short-circuit Alarm
		BUS Short-circuit Restored
ES	1380	External Probe Disconnected
EJ	3380	External Probe Connected
	1148	Device Motion Alarm
	3148	Device Motion Alarm Restored
	1149	Masking Alarm
	3149	Masking Alarm Restored
GA	1151	Gas Leakage Alarm
GH	3151	Gas Leakage Alarm Restored
		Zone Early-Warning
		Zone Early-Warning Dismissed
AT	1301	Mains Power Lost
AR	3301	Mains Power Restored
YT	1302	Battery Low
YR	3302	Battery Voltage Restored
RN	1305	Reset to defaults
YM	1311	Battery Disconnected
YR	3311	Battery Reconnected
YI	1312	Overcurrent Protection Triggered
YJ	3312	Overcurrent Protection Restored
YP	1319	Overvoltage Protection Triggered
YQ	3319	Overvoltage Protection Restored
		Expander Exception
		Expander Restored
		Printer Disconnected
		Printer Connected
XT	1338	Battery Low
XR	3338	Battery Voltage Restored
		Expander Low Voltage
		Normal Expander Voltage
AT	1342	Mains Power Lost
AR	3342	Mains Power Restored
YM	1311	Battery Disconnected
YR	3311	Battery Reconnected
ES (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Lid Opened

SIA code	CID code	Description
EJ (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Lid Restored
		Expander AC Power Loss
		Expander AC Power Loss Restored
TA	1334	Lid Opened
TR	3334	Lid Restored
TA	1321	Lid Opened
TR	3321	Lid Restored
UY	1321	Device Offline
UJ	3321	Device Restored
ES (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Lid Opened
EJ (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3341 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Lid Restored
XT	1338	Battery Low
XR	3338	Battery Voltage Restored
ET (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Offline
ER (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Restored
LT	1351	Main Signalling Path Fault
LR	3351	Main Signalling Path Restored

SIA code	CID code	Description
LT	1352	Backup Signalling Path Fault
LR	3352	Backup Signalling Path Restored
		Telephone Line Disconnected
		Telephone Line Connected
		BUS Supervision Fault
		BUS Supervision Restored
TA	1383	Lid Opened
TR	3383	Lid Restored
		Zone Open-circuit Alarm
		Zone Short-circuit Alarm
OP	1401	Disarmed
CL	3401	Armed
OA	1403	Auto Disarmed
CA	3403	Auto Armed
BC	1406	Alarm Silenced
		Instant Arming
CS	1409	Keyswitch Zone Disarming
OS	3409	Keyswitch Zone Arming
CL	3441	Armed in home mode
		Forced Arming
		Turn On Output by Schedule
		Turn Off Output by Schedule
CT	1452	Late to Disarm
CD	1455	Auto Arming Failed
		Turning On Output Failed
		Turning Off Output Failed
		Auto Disarming Failed
		Network Change
BB	1570	Bypassed
BU	3570	Bypass Restored
		Group Bypass
		Group Bypass Restored
		Manual Report Test
RP	1602	Periodic Report Test
TS	1607	Walk Test Enabled
TE	3607	Walk Test Disabled
		Telephone Connection Test
LB	1627	Programming mode
LX	1628	Exit Programming
BA	1131	Intrusion Detection
BH	3131	Intrusion Detection Restored
BA	1131	Cross-Zone Alarm

SIA code	CID code	Description
BH	3131	Cross-Zone Alarm Restored
		PIR Alarm
		PIR Alarm Restored
		Sudden Increase of Sound Intensity Alarm
		Sudden Increase of Sound Intensity Alarm Restored
		Sudden Decrease of Sound Intensity Alarm
		Sudden Decrease of Sound Intensity Alarm Restored
		Audio Input Fault
		Audio Input Restored
BA	1131	Line Crossing Alarm
BH	3131	Line Crossing Alarm Restored
BA	1134	Region Entrance Detection
FA	1112	Fire Source Alarm
FH	3112	Fire Source Alarm Restored
KS	1158	High Temperature Pre-Alarm
KR	3158	High Temperature Pre-Alarm Restored
ZS	1159	Low Temperature Pre-Alarm
ZR	3159	Low Temperature Pre-Alarm Restored
KA	1158	High Temperature Alarm
KH	3158	High Temperature Alarm Restored
ZA	1159	Low Temperature Alarm
ZH	3159	Low Temperature Alarm Restored
EA	1134	Region Exiting Detection
PA (The user No. of keyfob starts from 201)	1120 (The user No. of keyfob starts from 201)	Audible Panic Alarm
		Audible Panic Alarm
		Audible Panic Alarm
		Audible Panic Alarm
FA	1110	Keypad/Keyfob Fire Alarm
		Keypad/Keyfob Burglary Alarm
CI	1454	Arming Failed
MA (If triggered by a keyfob, the text message contains user information)	1100	Keypad/Keyfob Medical Alarm

SIA code	CID code	Description
DK	1501	Keypad Locked
DO	3501	Keypad Unlocked
		Absence Alarm
		Keypad Disconnected
		Keypad Connected
		KBUS Relay Disconnected
		KBUS Relay Connected
		KBUS GP/K Disconnected
		KBUS GP/K Connected
		KBUS MN/K Disconnected
		KBUS MN/K Connected
DK	1501	Tag Reader Locked
DO	3501	Tag Reader Unlocked
		Unregistered Tag
UY	1381	Device Offline
UJ	3381	Device Restored
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
ET (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Offline
ER (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3333 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Restored
UY	1334	Device Offline
UJ	3334	Device Restored
		Radar Transmitter Fault
		Radar Transmitter Restored
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
NT	1350	Cellular Fault
NR	3350	Cellular Restored
NT	1350	SIM Card Exception
NR	3350	SIM Card Restored

SIA code	CID code	Description
NT	1350	Network Fault
NR	3350	Network Restored
XQ	1344	Jamming Detected
XH	3344	Jamming Restored
NT	1350	Data limitation Reached
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
NT	1350	IP Address Already Used
NR	3350	Normal IP address
NT	1350	Network Fault
NR	3350	Network Restored
BA	1131	Motion Detection Alarm Started
BH	3131	Motion Detection Alarm Stopped
		Device Blocked
		Device Blocking Alarm Restored
		Video Signal Loss
		Video Signal Restored
		Input/Output Format Unmatched
		Input/Output Format Restored
		Video Input Exception
		Video Input Restored
		Full HDD
		Free HDD
		HDD Exception
		HDD Restored
		Upload Picture Failed
		Email Sending Failed
		Network Camera Disconnected
		Network Camera Connected
		Duty Checking
		Post Response
		Fire Alarm Consulting
		Fire Alarm Consulting Over
		Duress Alarm Consulting
		Duress Alarm Consulting Over
		Emergency Medical Alarm Consulting
		Emergency Medical Alarm Consulting Over
	3250	Patrol Signing

SIA code	CID code	Description
		BUS Query
		BUS Registration
		Single-Zone Disarming
		Single-Zone Arming
		Single-Zone Alarm Cleared
	1306	Device Deleted
	3306	Device Enrolled
		Business Consulting
		Business Consulting Over
	1306	Device Deleted
	3306	Device Enrolled
	1306	Device Deleted
	3306	Device Enrolled
	1306	Device Deleted
	3306	Device Enrolled
	1306	Device Deleted
	3306	Device Enrolled

H. Communication Matrix and Operation Command

Please scan the QR code for communication matrix and operation command



AX HYBRID PRO Communication Matrix

AX HYBRID PRO Operation Command

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.
User name	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 <i>Communication Matrix</i> .
Log	Used to record information such as device operating status and operation records.
Database information	Used to record information.

