



AX PRO

User Manual

Legal Information

©2020 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.

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.

Regulatory Information

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

EN 50131-3:2009

EN 50131-6:2017

EN 50131-5-3:2017

EN 50131-10: 2014

EN 50136-2: 2013

Security Grade (SG): 2

Environmental Class (EC) : II




DP2



Certified by Telefication



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>

	<p>Warning</p> <p>This is a class A product. In a domestic environment this product may cause radio inter-ference in which case the user may be required to take adequate measures.</p>
	<p>FCC Information</p> <p>Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.</p> <p>FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:</p> <ul style="list-style-type: none"> —Reorient or relocate the receiving antenna. —Increase the separation between the equipment and receiver. —Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. —Consult the dealer or an experienced radio/TV technician for help. <p>This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.</p> <p>FCC Conditions</p> <p>This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:</p> <ol style="list-style-type: none"> 1. This device may not cause harmful interference. 2. This device must accept any interference received, including interference that may cause undesired operation.

Contents

Chapter 1 Introduction	9
1.1 System Description	9
1.2 Specification	10
1.3 Appearance.....	14
Chapter 2 Start Up.....	17
2.1 Initial the Device	17
2.2 Install the Device	18
Chapter 3 User Management	20
3.1 User Management	20
3.1.1 Invite the Administrator.....	20
3.1.2 Cancel Installer Access	21
3.1.3 Add an Operator	22
3.1.4 Delete an Operator	23
3.2 Access Entries	23
Chapter 4 Configuration	25
4.1.Set-up with Hik-Proconnect.....	25
4.1.1 Use the Hik-Proconnect APP	25
4.1.2 User the Hik-ProConnect Portal	37
4.2 Set-up with Hik-Connect	41
4.3 Set-up with the Web Client.....	49
4.3.1 Communication Settings	50
4.3.2 Device Management	63
4.3.3 Area Settings	73
4.3.4 Video Management.....	75
4.3.5 Permission Management	76
4.3.6 Maintenance	78
4.3.7 System Settings	79
4.3.8 Check Status.....	92
4.4 Report to ARC (Alarm Receiver Center)	93

Setup ATS in Transceiver of Receiving Center	93
Setup ATS in Transceiver of the Panel.....	94
Signalling Test	95
Chapter 5 General Operations.....	97
5.1 Arming	97
5.2 Disarming.....	98
5.3 SMS Control	98
A. Trouble Shooting.....	99
A.1 Communication Fault	99
A.1.1 IP Conflict.....	99
A.1.2 Web Page is Not Accessible	99
A.1.3 Hik-Connect is Offline	99
A.1.4 Network Camera Drops off Frequently	99
A.1.5 Failed to Add Device on APP.....	99
A.1.6 Alarm Information is Not Reported to APP/4200/Alarm Center	100
A.2 Mutual Exclusion of Functions.....	100
A.2.1 Unable to Enter Registration Mode	100
A.3 Zone Fault.....	100
A.3.1 Zone is Offline.....	100
A.3.2 Zone Tamper-proof.....	100
A.3.3 Zone Triggered/Fault	100
A.4 Problems While Arming.....	101
A.4.1 Failure in Arming (When the Arming Process is Not Started)	101
A.5 Operational Failure.....	101
A.5.1 Failed to Enter the Test Mode.....	101
A.5.2 The Alarm Clearing Operation on the Panel Does Not Produce the Alarm Clearing Report	101
A.6 Mail Delivery Failure.....	101
A.6.1 Failed to Send Test Mail.....	101
A.6.2 Failed to Send Mail during Use	102
A.6.3 Failed to Send Mails to Gmail	102
A.6.4 Failed to Send Mails to QQ or Foxmail.....	102

A.6.5 Failed to Send Mails to Yahoo	102
A.6.6 Mail Configuration	103
B. Input Types.....	104
C. Output Types	107
D. Event Types	108
E. Access Levels	109
F. Signalling	111
Detection of ATP/ATS Faults.....	111
ATS Category	111
G. SIA and CID Code.....	112

Chapter 1 Introduction

1.1 System Description

AX Pro is a wireless alarm system designed to protect premises required for proper protection from intrusion alarm. It supports LAN /Wi-Fi as the primary transmission network, and GPRS/3G/4G LTE as the secondary transmission network. The system is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

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

Ordering

Model	Description
DS-PWA64-L-WE	Supports Ethernet/Wi-Fi, and GPRS
DS-PWA96-M-WE	Supports Ethernet/Wi-Fi, 3G/4G LTE, and IC Card

1.2 Specification

		AX PRO	
		64 Series	96 Series
Capacity	Areas	16	32
	Zones	Up to 64	Up to 96
	Outputs		
	Tag Readers	Up to 8	Up to 8
	Keypads		
	Sounders	4	6
	Repeaters	2	4
	Keyfobs	32	48
	Tags	32	48
	Tag Reader built-in	×	√
User	Installer	1	1
	Administrator	1	1
	Normal Users	30	46
Wireless technical characteristics	RF Frequency	868 Mhz(865 Mhz for PIR-Camera Detector) /433 Mhz	
	Wireless type	2-way wireless	
	Wireless Security	Frequency Hoping 128 AES Encryption	
Functional Features	Voice Prompts	√	√
	Voice Prompt Language	English, Italian, Spanish, French, Russian, Portuguese, Germany, Polish	
	Web Client	√	√
	Diagnostics	√	√
	SMS Notification	√	√
	Voice Call Notification	√	√
	Event Log Records	5000 including 1000 mandatory ^a	
	PIR Camera Support	√	√
IVaaS Storage	×	4 clips x 7 sec	
Communication interfaces	Ethernet	10/100 Mbps self-adaptive	
	Wi-Fi	802.11b/g/n (2.4GHz)	
	GPRS	√	×
	3G/4G LTE	×	√
	SIM slot	Single	Dual
ARC Signaling	ATS Category ^a	DP2	
	Primary Transmission Path	LAN / WiFi	
	Secondary Transmission Path	GPRS or 3G/4G LTE	
	Acknowledgement Operation ^a	Pass-through	

	Protocols	SIA-DC09 ^b , ISUP 5.0					
Cloud Services	Hik-ProConnect Service	√	√				
	Hik-Connect Service	√	√				
Automation	Wall-Switch	√	√				
	Relay Module	√	√				
	Smart Plug	√	√				
Power Supply	PS Type ^c	Type A					
	Mains Input	~ 100-240V 50/60Hz 0.3A(Max)					
	Battery Capacity ^d	4520 mAh					
	Battery Standby ^e	Up to 12 hrs					
	Battery Type	Built-in rechargeable Lithium-ion polymer battery Model: 765965					
	Current Consumption	With an alarm: 405mA Without an alarm: 340mA					
	Current when on Battery	340 mA					
	Recharge Period	4 hrs to 80%					
	Low Voltage Message	3.55 V					
Service	No user service parts inside						
Environmental Requirements	Operating Temperature	-10°C to 50°C - 10°C to +40°C (Certified temperature)					
	Relative Humidity	10% ~ 90% noncondensing					
Size & Weight	Dimension (W×H×D)	170.0 mm (6.7") × 170.0 mm (6.7") × 38.6 mm (1.5")					
	Weight	557.5 g (19.7 oz)					
Approvals	EN 50131	SG 2 EC II					
	CE	√					
	Rohs/Reach/WEEE	√					
a	<p>As per requirements defined in EN 50131-1:2006+A1:2009+A2:2017 AX Pro wireless control panel adopts pass-through mode of acknowledgement operation. Both positive and negative acknowledgement from the transceiver of receiving center will be recorded.</p> <p style="text-align: center;">Event log description</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>Positive acknowledgement</td> <td>ARC Uploaded</td> </tr> <tr> <td>Negative acknowledgement</td> <td>ARC Communication Failed</td> </tr> </table>			Positive acknowledgement	ARC Uploaded	Negative acknowledgement	ARC Communication Failed
Positive acknowledgement	ARC Uploaded						
Negative acknowledgement	ARC Communication Failed						

b	AX Pro wireless control panel is compatible with SIA IP Reporting (UDP/TCP-2013) as per ANSI/SIA DC-09-2013: Internet Protocol Event Reporting. The control panel supports tokens (protocols) of ADM-CID and SIA-DCS defined in SIA DC-07-2001.04, which will be modified to insert a "*" before token name as *ADM-CID and *SIA-DCS when the data and timestamp of transmission message are AES encrypted. AES-128, AES-192 and AES-256 are all supported.
c	As per EN 50131-1:2006+A1:2009+A2:2017, 9.1 Types of power supply
d	Nominal value. Actual capacity may vary slightly. The actual battery capacity for each individual device may be slightly above or below the nominal battery capacity. Removing the battery may cause damage to the device. To replace or repair the battery, please contact your installer.
e	In the condition of Wi-Fi connected, GPRS/3G/4G LTE connected, ARC connected (polling interval: 1800 s), 8 inputs and 1 keypad accessed, and cloud service accessed.

 **Note**

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

 **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.

RSSI Instruction for Peripherals

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

Signal Strength	RSSI Value	Indication	Remark
-----------------	------------	------------	--------

Strong	>120	Green	OK to install
Medium	81 to 120	Yellow	OK to install
Weak	60 to 80	Red	Not recommend to install, but can work
Invalid	0 to 59	Red (flash)	Not OK to install, cannot work normally

 **Note**

Install peripherals only if the signal strength is above 80. For getting a much better system, install at 120 and above.

AX PRO Notification Options

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

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

1.3 Appearance

Front Panel

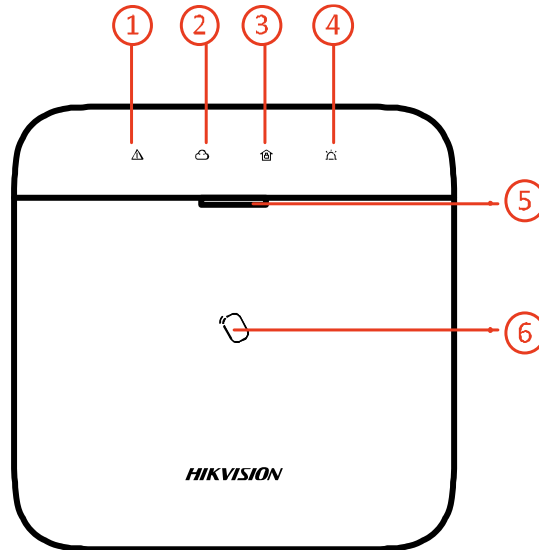




Table 1-2 Front Panel Description

No.	Name	Description
1	Alert Indicator	<p>Solid Orange: In the disarming status, the LED indicates alarm (such as panic alarm, zone alarm, tampering alarm, etc.) and fault (such as operation fault, connection fault, etc.)</p> <hr/> <p>Note</p> <ul style="list-style-type: none"> The indicator or voice notifications will not response to any operation made by level 1 users. Notifications will only response when level 1 user presents or uses a valid tag or keyfob. The device will prompt detailed alarm or fault information while the authorized users disarm the system.
2	Link Indicator	<p>Solid Green: The panel is bound to Hik-connect account</p> <p>Off: The panel is not bound to Hik-connect account</p>
3	Arm/Disarm Indicator	<p>Solid Blue for 5 s: Armed</p> <p>Green Flashes Twice: Disarmed</p>

No.	Name	Description
		<hr/>  Note If the function of Arming Indicator Keeps Light is enable, the LED keeps solid blue when armed, and off when disarmed. The function does not compliant with EN standard. <hr/>
4	Alarm Indicator	Flashing Red: Alarm Occurred Solid Red: Device Tampered Off: No Alarm
5	Power Indicator	Solid Green: Power on Off: Power off
6	Tag Present Area	<hr/>  Note The function varies according to the model of device. <hr/>

Component and Interface

Remove the rear cover, and some of the components and interfaces are on the rear panel.

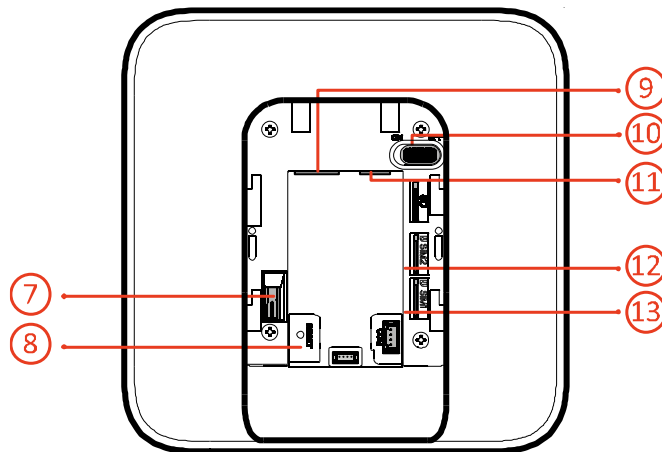





Table 1-3 Rear Panel Description

Number	Description
7	Tamper Switch
8	Reset Button

Number	Description
	<hr/>  Note Restart the device, the power LED flashes 3 times, and hold the reset button for 5 s. The voice prompt indicates the operation result. Press the button to switch the STA and Hotspot mode. <hr/>
9	Power Interface
10	Power Switch
11	Network Interface
12	SIM Card Slot 1 <hr/>  Note The function of GPRS or 3G/4G (implemented with built-in SIM card slot) varies depends on the model of the device. <hr/>
13	SIM card Slot 2 <hr/>  Note The function of GPRS or 3G/4G (implemented with built-in SIM card slot) varies depends on the model of the device. <hr/>

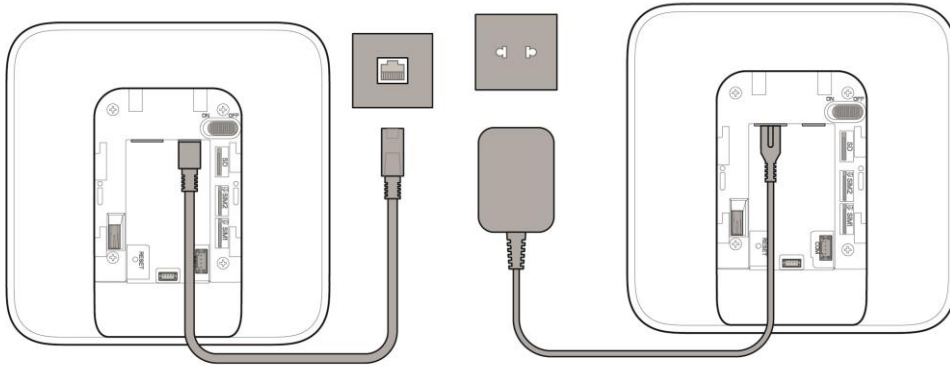
Chapter 2 Start Up

2.1 Initial the Device

While initial the device with Hik-ProConnector, the AX Pro should always be add to an installer account first. The installer account will invite and transfer ownership to the administrator account later after finishing all initial setup and test. Follow the steps below to initializing the wireless alarm system.

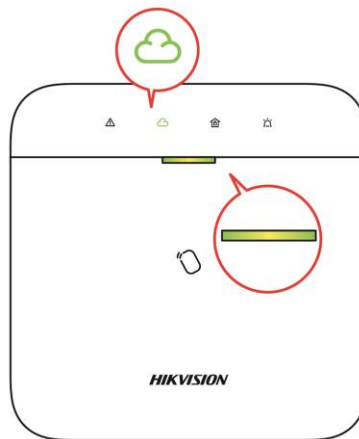
1. Connect to the network.

Connect the device to the Ethernet, and power the device on.



Note

While the device is powered on, the power LED and link LED turn green.



2. Create a site

Open the Hik-ProConnect and login with the installer account.

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

3. Add Device

Open the site. Tap **Add Device** and scan the QR code on the label of the panel.

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

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

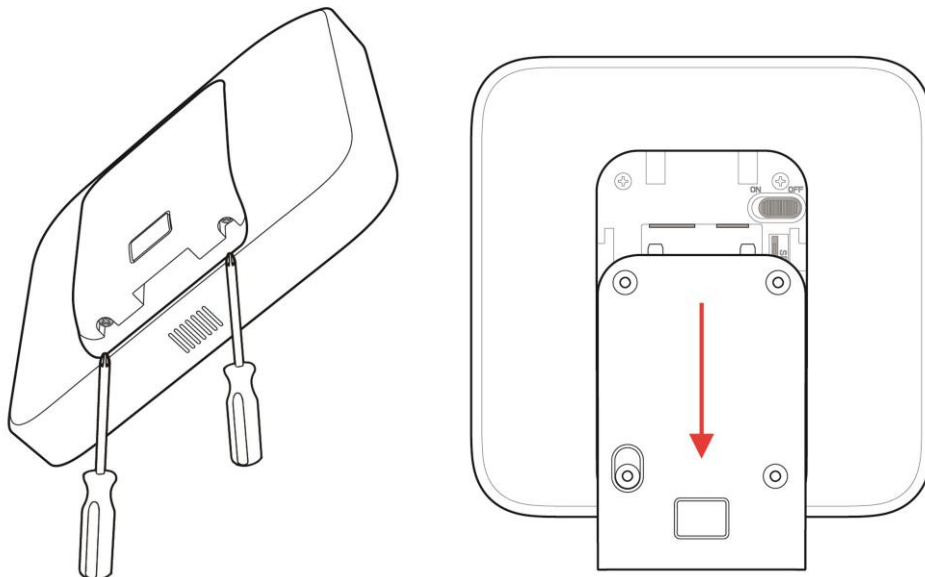
Note

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

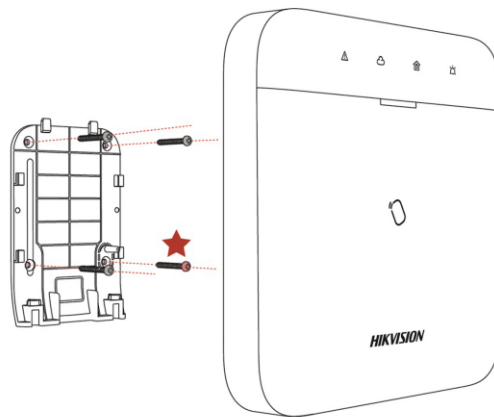
2.2 Install the Device

Steps

1. Loosen the screw on the rear cover. Slide down the rear cover and remove it from the AX PRO.



2. Secure the rear cover to the installation position with the supplied screws. Attach the AX PRO on the rear cover, and tighten the rear cover screw to complete the installation.



 **Note**

- Red Star: TAMPER Screw. It is compulsory to secure the TAMPER screw.
- No adjustments are required.
- For use within the supervised premises only.

 **Note**

Check the RF signal strength before connection and peripheral device installation. You can view the RF signal strength indication on the peripheral device.

Chapter 3 User Management

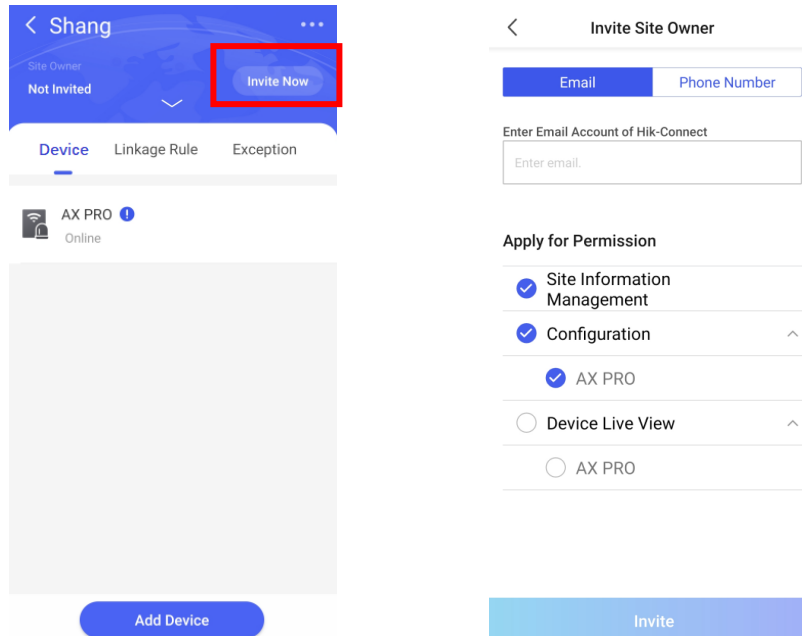
3.1 User Management

Note

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

3.1.1 Invite the Administrator

The administrator was known as site owner in Hik-ProConnect Service.

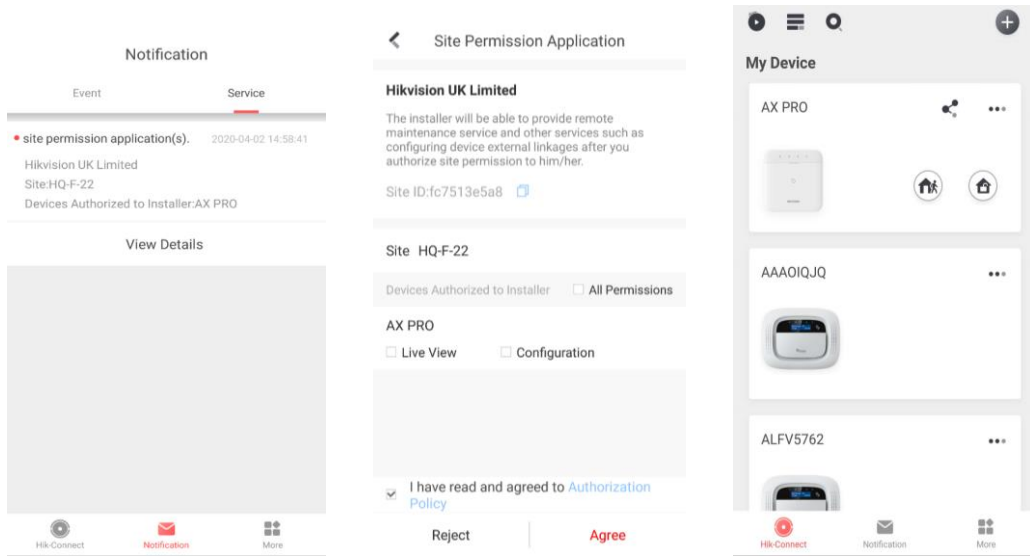


After the initial configuration finished, the installer shall invite the site owner and apply permission of site management and device configuration from the administrator account. The administrator account would be an end user account in the Hik-Connect Service.

Press “Invite Now” Button and enter the email account or phone number account to transfer the site ownership to the administrator. At the same time, the installer will apply permissions from the site owner, such as configuration and management.

Open the Hik-Connect app and login with the administrator account. The installer service request will be received at notification page. Open the notification detail to accept the installer service and setup permissions. The control panel and other devices in the site will be displayed at your device list.

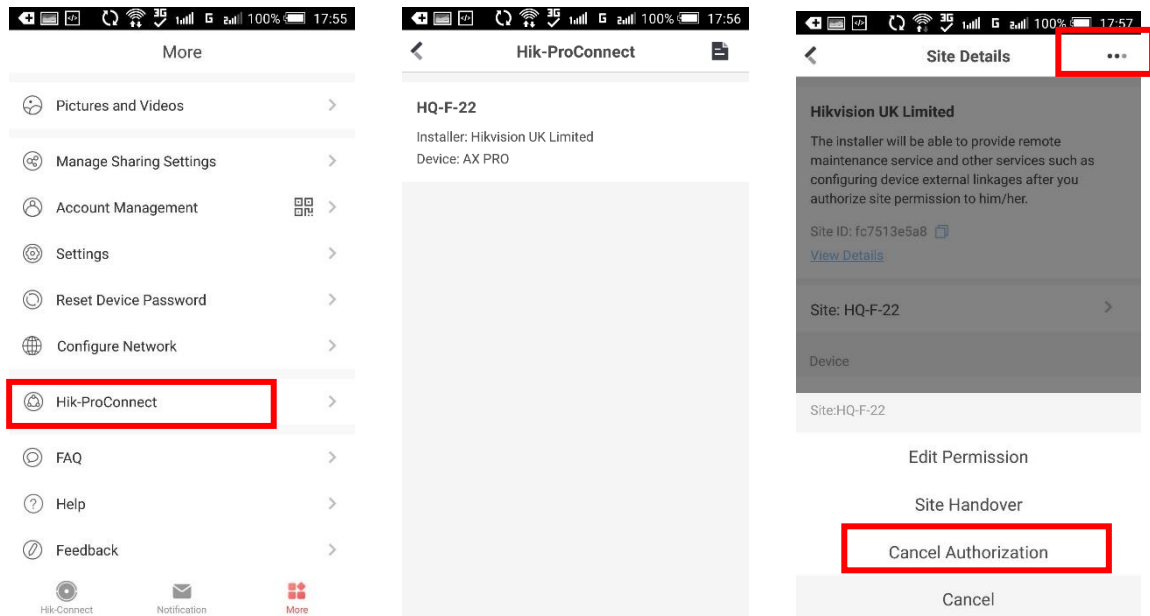
The administrator account will be added to the control panel, which could be used to login to Hik-Connect app and local web client.



3.1.2 Cancel Installer Access

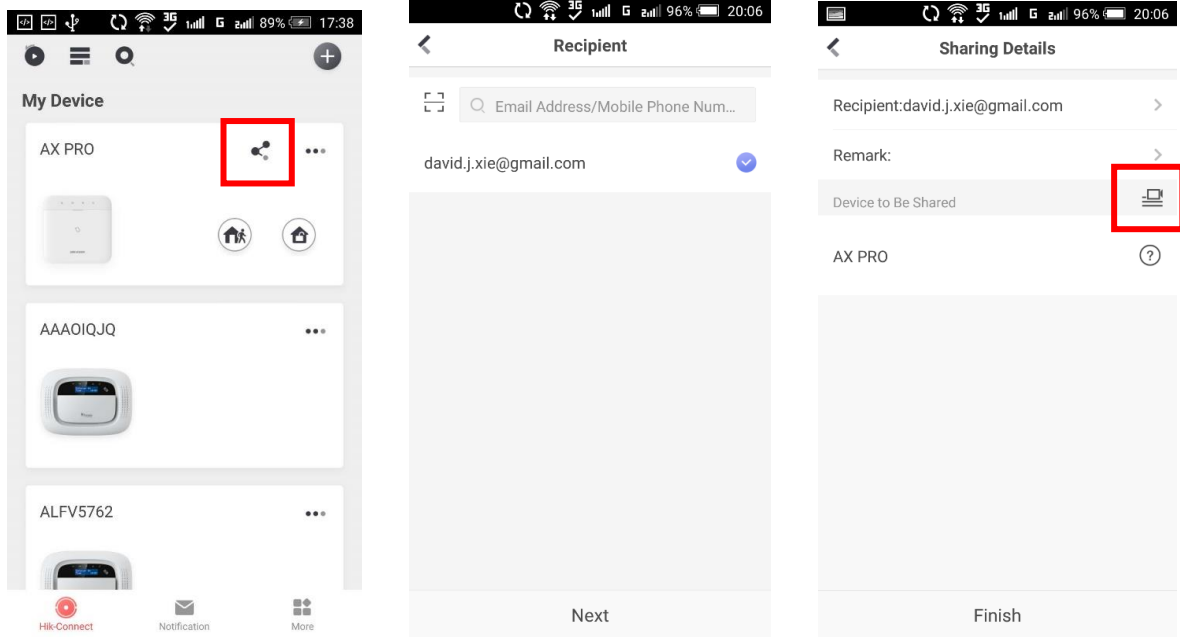
The administrator can cancel the access authorization of the installer.


1. Enter the page **More** and tap **Hik-ProConnect**. All sites that managed by the Hik-ProConnect Service are listed on the page.
2. Tap the option button at the top-right corner of the site details page, and tap **Cancel Authorization** in the prompt menu.
3. Confirm the operation, and the authorization of the installer will be canceled. Once the authorization is canceled, the installer need to apply it again if any access requirement.



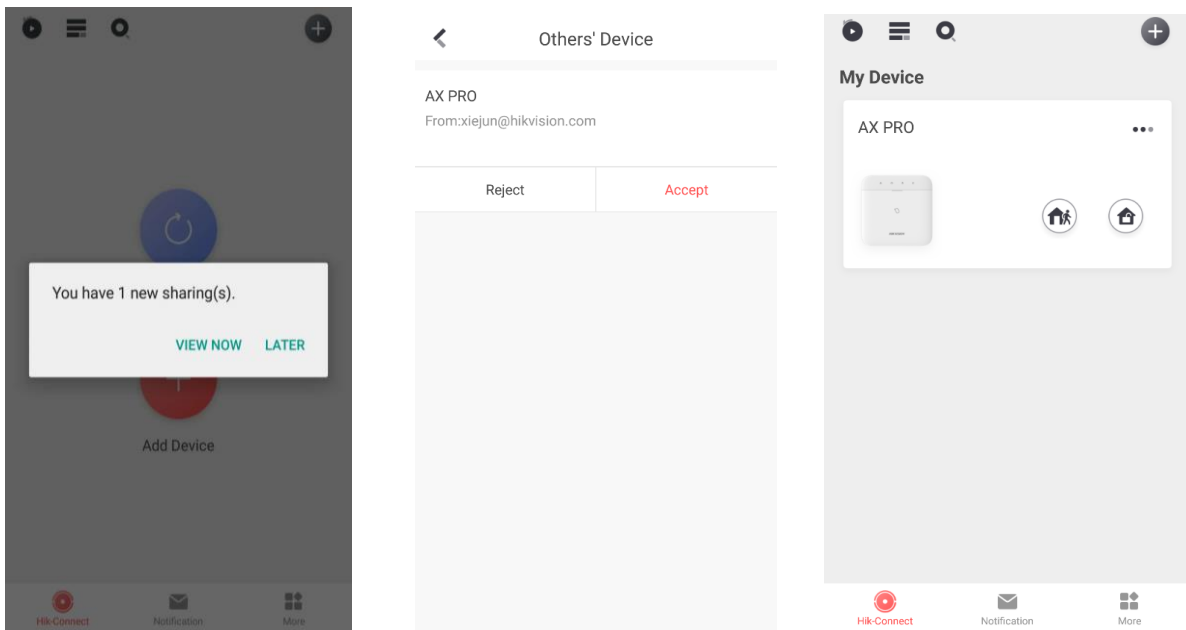
3.1.3 Add an Operator

The administrator can share the device to other operators.



1. Tap the  (share button) in the device list.
2. Enter the Hik-Connect account of the operator.

Administrator can also select which device to be shared.



A sharing message will be sent to the operator's account, and the operator can read the message in the Hik-Connect app.

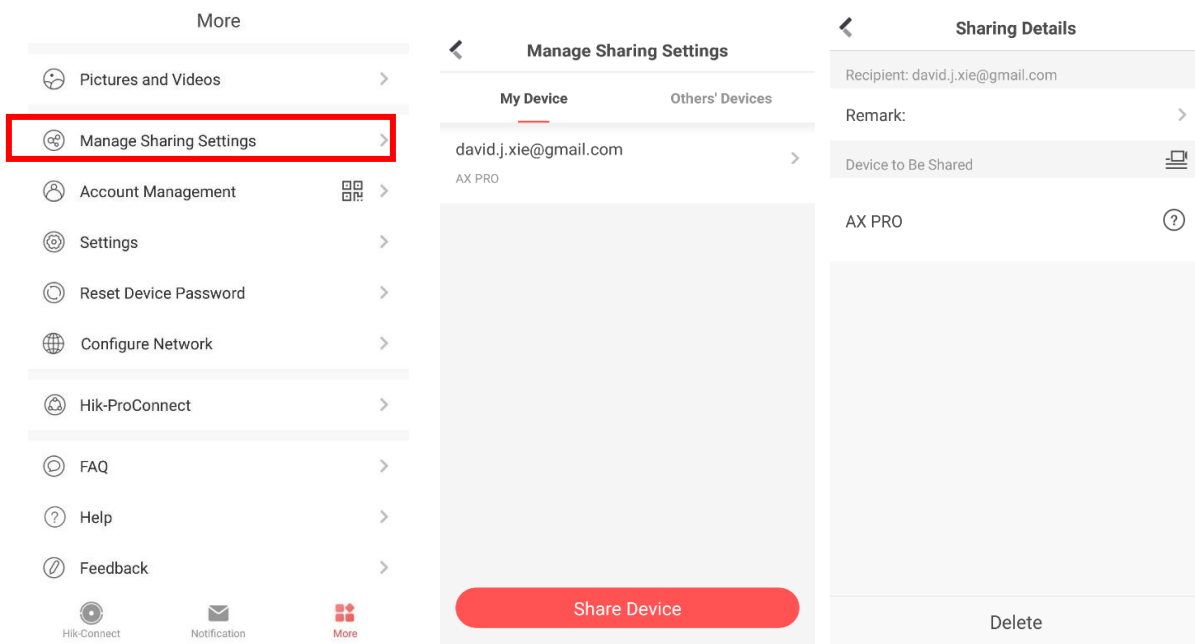
3. Accept the invitation, and the device will be listed in the device list.

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

3.1.4 Delete an Operator

Administrator user can delete an operator.

1. Enter the page **More** and tap **Manage Sharing Settings**.
2. Delete the selected operator or remove it from the device.



3.2 Access Entries

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

Access entries for Installers (Access Level 3)

- **Hik-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.
- **Legacy 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.
- **Legacy entries**
Keypad PINs and tags can be also assigned with end user at particular access level to perform essential operations.

Chapter 4 Configuration

4.1.Set-up with Hik-Proconnect

4.1.1 Use the Hik-Proconnect APP

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

Download and Login the Hik-ProConnect

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

Steps

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

Note

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

3. Run and login the client.

Add AX PRO to the Mobile Client

Add AX PRO to the mobile client before other operations.

Steps

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

Note

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

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

4. Activate the **Device**.

Add Peripheral to the AX PRO

Add peripheral to the AX PRO.

Steps

1. Select a site.
2. Select a control device (AX PRO).
3. Tap the + icon.
 - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the peripheral.
 - Tap **Manual Adding** to enter the Add Device page. Enter the device serial No. and verification code to add the device.

User Management

The installers (user of Hik-ProConnect) can manage users. If you are the administrator, you can add, edit, and delete users, and assign different permissions to the newly-added users.

Steps


Note

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

1. Enter the site, tap the AX PRO and then log in to the device (if required) to enter the AX PRO page.
 2. Tap **Next** to invite the user.
-

Note

The recipient need to accept the invitation.

3. Tap  → **User Management** → **User**.
4. Tap a user to enter the User Management page.
5. Optional: Perform the following operations if required.

User Permission

You can tap the target user on the user list and then tap **Edit Icon** to set the permissions authorized to the target user.

Note

Only the administrator can do such an operation.

Set Linked Areas

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

 **Note**

Only the administrator can do such an operation.

Edit Keypad Password

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

Edit Duress Password

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

 **Note**

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

Automation Control

An administrator, an installer or an operator can control the relay module, wall switch and smart plug.

 **Note**

- Configuration items and user permission will vary according to the user type.
 - You can view linked cards/tags and keyfobs of the user but you do not have permission to configure them.
-


Card/Tag Management

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

 **Note**

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

Steps

1. Enter the site, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap  → **User Management** → **Card/Tag** to enter the Tag Management page.
3. Tap **+** to add a Tag.
4. When hearing the voice prompt "Swipe Tag", you should present the Tag on the AX PRO Tag presenting area.
 - When hearing a beep sound, the Tag is recognized.

- The Tag will be displayed on the Tag page.
- Optional: Tap a Tag to enter the Setting Page.
 - Tap **Edit Icon** to edit the Tag name.

 **Note**

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

- Slide **Enable Tag**.
- Select a linked user.
- Select the Tag type

 **Note**

Different linked users have different Tag permissions.

Operation Tag

You can swipe the Tag to arm or disarm.

Patrol Tag

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

- Optional: Tap **Delete** to delete the Tag.

System Settings

System Configuration

You can set the device time zone and set the DST time.

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

Tap  → **System** → **Configuration** to enter the configuration page.


You can tap to select a time zone.

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

System Options

Set the system options.

Option Management

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

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

Forced Auto Arm

If the option is enabled and there are active faults in a zone, the zone will be bypassed automatically.

System Status Report

Switch for uploading system reports.

Voice Prompt

If the option is enabled, the AX PRO will enable the text voice prompt.

Audible Tamper Alarm

If the option is enabled, the system will alert with buzzer for the tamper alarm.

If the option is disabled, peripherals will report lid opened, but not link to alarms.

System Volume

The available system volume range is from 0 to 10.

Panel Lockup Button

If the option is enabled, the installer can use the lockup button function to lock the AX PRO.

After locking, users can not operate the device and receive messages.

Panel Alarm Duration

Set the time duration of the panel alarms.


Polling Loss Times

Set the maximum duration for polling loss. The system will report fault if the duration is over the limit.

Bypass on Re-Arm

The bypassed zone will back to arm if fault restored.

Fault Check

In the site, tap the AX PRO. Tap  → **System** → **System Options** → **Panel Fault Check** to enter the page.

Detect Network Camera Disconnection

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

Battery Fault Check

If the option is enabled, when battery is disconnected or out of charge, the device will not 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.

AC Power Down Check Time

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.

System Instructions

In the site, tap the AX PRO and then log in to the device (if required). Tap  → **System** → **System Options** → **System Instructions** to enter the page.

Arm with Fault

If the option is enabled, when there is a fault during the arming procedure, you can stop arming manually.

Checklist

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

Arm with Fault Checklist

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

Arm LED Stay On

If the device applies EN standard, by default, the function is disabled. In this case, if the device is armed, the LED will be solid blue for 5 s. And if the device is disarmed, the LED will flash 5 times. When the function is enabled, if the device is armed, the LED will be on all the time. And if the device is disarmed, the LED will be off.

Fault Prompts On Arming

If the device applies EN standard, by default, the function is disabled. In this case, the device will not prompt faults during the arming procedure.

Fault Prompts On Disarming

If the device applies EN standard, by default, the function is disabled. In this case, the device will not prompt faults during the disarming 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 delay time.

Early Alarm Time

When the early alarm function is enabled, you should set the early alarm time. The alarm will be

triggered after the configured early alarm time.


Enrollment Method

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap  → **System** → **System Options** → **Enrollment Method** to enter the page.
3. Tap **Enter the Enrollment Mode**.
4. Follow the instructions on the page to add a device.
5. Tap **Exit the Enrollment Mode**.

Network Camera


Add Cameras to the AX PRO

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap  → **IPC** → **IPC management** to enter the page.
3. Tap **Add**.
4. Enter IP address, port, the user name and password of the camera.
5. Tap **Save Icon**.
6. Optional: tap **Edit** or **Delete** to edit or delete the selected camera.

Set Video Parameters

Steps

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

Stream Type

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

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

Bitrate Type

Select the Bitrate type as constant or variable.


Resolution

Select the resolution of the video output.

Video Bitrate

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

Set Arming/Disarming Schedule

1. Set the arming/disarming schedule to arm/disarm a particular zone automatically.
2. In the site, tap the AX PRO and then log in to the device (if required).
3. Tap  → Area to enter the page.
4. Tap an area in the list, enable the area and select linked areas.
5. Enable the auto arm/disarm function and set the auto arm time/auto disarm time. You can also set the late to disarm time, entry delay time, exit delay time, sounder delay time, weekend exception and excepted holiday.

Auto Arm

Enable the area to automatically arm itself in a specific time point.

Auto Arm Time

Set the schedule for the area to automatically arm itself.

Auto Disarm

Enable the area to automatically disarm itself in a specific time point.

Auto Disarm Time

Set the schedule for the area to automatically disarm itself.

Late to Disarm

Enable the device to push a notification to the phone or tablet to remind the user to disarm the area when the area is still armed after a specific time point.



You should enable the Panel Management Notification function on the Web Client of **Communication Parameters** → **Event Communication** before enabling the Late to Disarm function.

Late to Disarm Time

Set the time point mentioned in **Late to Disarm**.

Weekend Exception

If enabled, **Auto Arm**, **Auto Disarm**, and **Late to Disarm** are disabled on the weekend.

Excepted Holiday

Enable the function and the zone will not be armed/disarmed in the holiday. You should set the holiday schedule after enabling.




Up to 6 holiday groups can be set.

Communication

Cellular Data Network

Enter a short description of your task here (optional).


Steps

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

Push Notifications

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

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap  → **Communication Parameters** → **Push Notification(s)** to enter the page.
3. Tap **Phone Call** and **SMS**.
4. Tap **+** or **+ Add Phone Number** to enter the phone number.
5. Tap the added phone number to enable **Phone Call** and **SMS** according to your need.
6. (For Phone Call) Set **Numbers of Calling**.
7. (For SMS) Set **Arming Permission**, **Disarming Permission** and **Alarm Clearing Permission** for areas.
8. Check notifications.

Zone Alarm/Lid Notification

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

Note

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

Peripherals Lid Opened

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

Panel Lid Opened

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

Panic Alarm

The device will push notifications when panic alarm is triggered or restored by zones, keypads or keyfobs.

Medical Alarm

The device will push notifications when medical alarm is triggered.

Gas Alarm

The device will push notifications when gas alarm 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 the 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 AX PRO.


Smart Alarm Notification

The device will push notifications when the alarm is triggered in thermal cameras.

Alarm Receiving Center (ARC)

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

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap  → **Communication Parameters** → **Alarm Receiving Center (ARC)** to enter the page.
3. Select an ARC and enable it.
4. Select the **Protocol Type** as **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, or ***ADM-CID** to set uploading mode.

ADM-CID or SIA-DCS

You should select the **Address Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, transmission mode, retry timeout period, attempts, polling option and period test.

Note

Set the period test interval with the range from 10 seconds to 24 hours.

ISUP

You do not need to set the ISUP protocol parameters.

***SIA-DCS or *ADM-CID**

You should select the **Address Type** as **IP** or **Domain name**, and enter the IP/domain name,

port number, account code, transmission mode, retry timeout period , attempts, polling option, encryption arithmetic, password length, secret key and period test.

Note

Set the period test interval with the range from 10 seconds to 24 hours.


For encryption arithmetic: The panel support encryption format for information security according to DC-09, AES-128, AES-192 and AES-256 are supported when you configure the alarm center.

For the secret key: When you use an encrypted format of DC-09, a key should be set when you configure the ARC. The key would be issued offline by ARC, which would be used to encrypt the message for substitution security.

Device Maintenance

You can reboot the device.

Steps

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

Device Management


Enter a short description of your concept here (optional).

This is the start of your concept.

Zone

You can set the zone parameters on the zone page.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap a zone in the **Device** tab.
3. Tap .
4. Tap **Edit Icon** the zone name.
5. Select a zone type.

Instant Zone

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

Delayed 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.

If the zone is a delayed zone, you can set Enter delay/Exit delay parameters.

Follow Zone

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

24h Silent Panic Zone

This zone type is active 24hrs, it is used for Panic or HUD (Hold Up Devices) not smoke sensors or break glass detectors.

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.

Fire Zone

The zone activates all the time with sound/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/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.

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)

Key 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.

Disabled Zone

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

6. Enable **Stay Arm Bypass, Chime, Double Knock, Silent Alarm** and other functions according to your actual needs.

 **Note**


- Some zones do not support the function. Refer to the actual zone to set the function.
 - Different zone types have different parameters.
-

7. Set the polling rate.
8. Optional: Tap **Delete** to delete the device.

Keypad

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


Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap a keypad in the **Device** tab.
3. Tap .
4. Tap **Edit Icon** the keypad name.
5. Enable **Enable Keyfob**.
6. Select linked users.
7. Tap **Function Key Settings** to set functions for single keys and combination keys.
8. Optional: Tap **Delete** to delete the device.

Sounder

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


Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap a sounder in the **Device** tab.
3. Tap .
4. Tap **Edit Icon** the sounder name.
5. Select linked areas.
6. Set alarming lasting time and alarm volume.
7. Enable arming/disarming LED, arming/disarming buzzer, alarm indicator according to actual needs.
8. Set heartbeat cycle.
9. Optional: Tap **Delete** to delete the device.

4.1.2 User the Hik-ProConnect Portal

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






Pro.

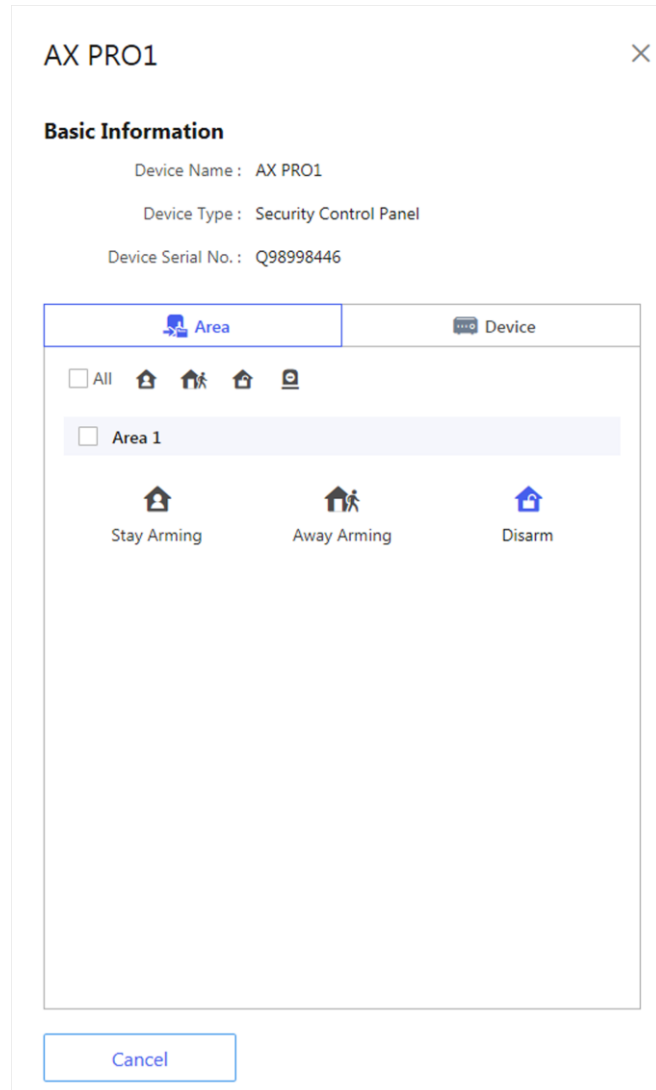
Click  **Site** to enter the site list page, and then click the name of a site to enter site details page.

Remotely Operate AX Pro


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

Table 4-3 Operation Description

Operation	Description
Stay Arm a Specific Area	Select the Area tab, and then click Stay Arming to stay arm the area.
Away Arm a Specific Area	Select the Area tab and then click Away Arming .
Disarm a Specific Area	Select the Area tab and then click Disarm .
Stay Arm Multiple Areas	Select the Area tab, and then select areas and click  .
Away Arm Multiple Areas	Select the Area tab, and then select areas and click  .
Disarm Multiple Areas	Select the Area tab, and then select areas and click  .
Silence Alarms of Multiple Areas	Select the Area tab, and then select areas and click  .
Filter Peripheral Device by Area	Select the Device tab, and then click  and select an area to only display the peripheral devices linked to the selected area, or select All to display all the peripheral devices linked to all the areas.
Control Relay	Select the Device tab, and then select a wireless output expander to display the sirens linked to it, and then select siren(s) to enable/disable them.
Bypass Zone	Select the Device tab, and then select a zone (i.e., detector) and turn on the Bypass switch to bypass the zone.





Remotely Configure AX Pro

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

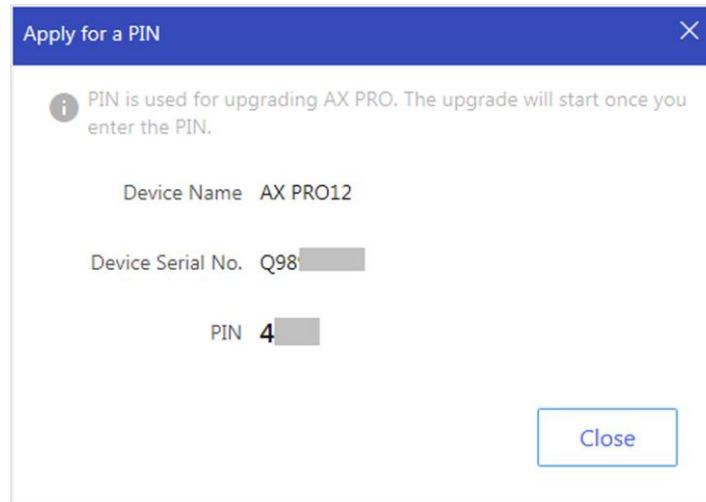
Note

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

Apply for a PIN

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

displayed.



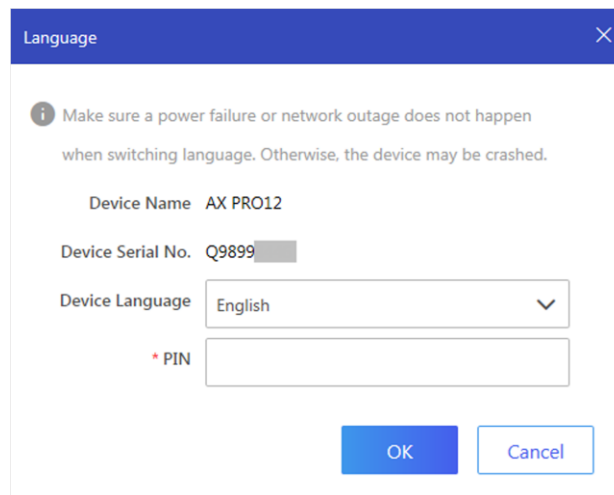
Switch Language



Note

You should have applied for a PIN.

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

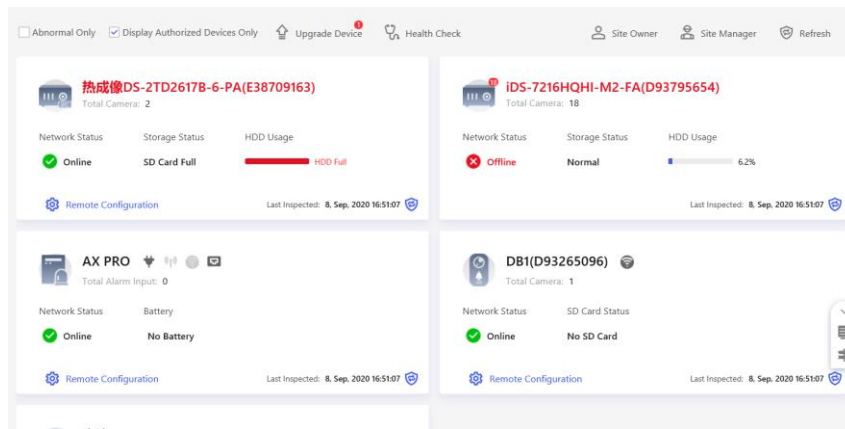


Health Monitoring

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

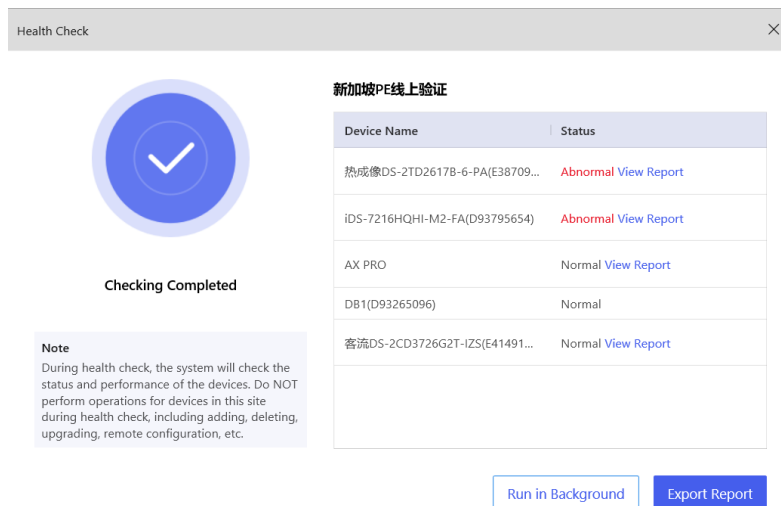
the page.


2. Select a site.



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

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



4. Click  to get the latest device status.

4.2 Set-up with Hik-Connect

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

Download and Login the Mobile Client

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

Steps

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



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

3. Run and login the client.

Add AX PRO to the Mobile Client

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





Steps

1. Power on the AX PRO.
2. Select adding type.
 - Tap + → **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the AX PRO.



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

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

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

Add Peripheral to the AX PRO

Add peripheral to the AX PRO.



Steps

1. Select a control device (AX PRO).
2. Tap + .
 - Tap **Scan QR Code** to enter the Scan QR code page. Scan the QR code on the peripheral.
 - Tap **Manual Adding** to enter the Add Device page. Enter the device serial No. and verification code to add the device.

Card/Tag Management

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

Steps

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

Note

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

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

Note

Different linked users have different tag permissions.

Operation Tag

You can swipe the tag to arm or disarm.

Patrol Tag

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

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

User Management


The administrator and the installers can manage users. If you are the administrator, you can add,

edit, and delete users, and assign different permissions to the newly-added users.

Steps


Note

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

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

Note

The recipient need to accept the invitation.

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

User Permission

You can tap the target user on the user list and then tap **Edit Icon** to set the permissions authorized to the target user.

Note

Only the administrator can do such an operation.

Set Linked Areas

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

Note

Only the administrator can do such an operation.

Edit Keypad Password

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

 **Note**

The password (PIN code) is allowed to be 4 to 6 digits. No number is disallowed, with 10,000 to 100,000 differs, and no limit of the digit combination.

After you add one keypad, you can add PIN code (Keypad Password) in the user menu. When you click in the input box, there will be indication shows that 4 to 6 numbers allowed. This is the same for each user

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

 **Note**

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

Automation Control An administrator, an installer or an operator can control the relay module, wall switch and smart plug.

 **Note**

- Configuration items and user permission will vary according to the user type.
 - You can view linked Tags/tags and keyfobs of the user but you do not have permission to configure them.
-

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


Bypass Zone

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

Before You Start

Link a detector to the zone.

Steps

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

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

Arm/Disarm the Area





Arm or disarm the area manually as you desired.

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

Operations for a Single Area

- **Away Arming:** Tap any area to away arm a single area. When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time.
- **Disarm:** Tap **Away Arming Icon** in any area to disarm a single area. In Disarm mode, all the zones in the area will not trigger alarm, no matter alarm events happen or not.

Operations for All Areas

- **Away:** Tap  to away arm all areas. When all the people in the detection area leave, turn on the Away mode to arm all zones in all areas after the defined dwell time.
- **Stay:** Tap  to stay arm all areas. When the people stays inside the detection area, turn on the Stay mode to arm all the perimeter burglary detection (such as perimeter detector, magnetic contacts, curtain detector in the balcony) set in all the zones of all areas. At the meantime, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and alarm will not be triggered.
- **Disarm:** Tap  to disarm all areas. In Disarm mode, all the zones of all areas will not trigger alarm, no matter alarm events happen or not.
- **Silence Alarm:** Tap  to silence alarms for all areas. Clear all the alarms triggered by the all the zones of all the areas.

Check Alarm Notification

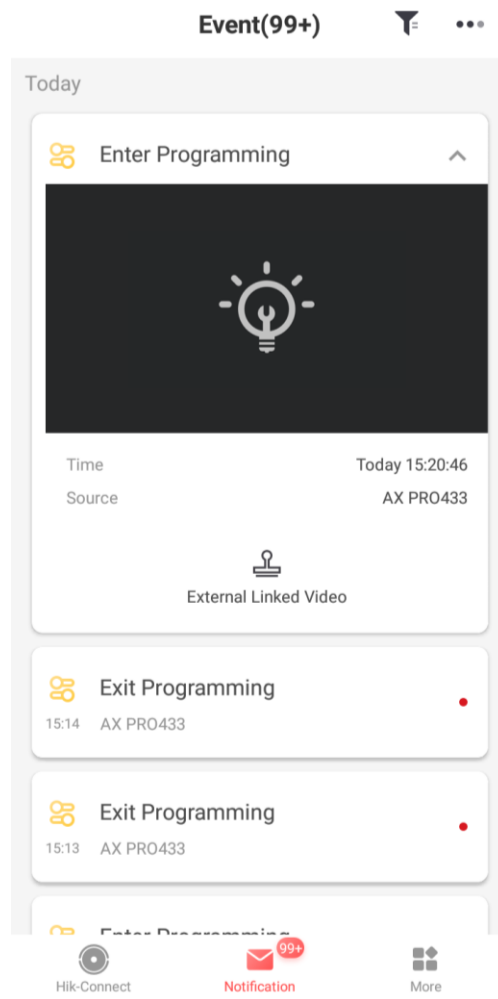
When an alarm is triggered, and you will receive an alarm notification. You can check the alarm information from the mobile client.


Before You Start

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

Steps

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




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

Wi-Fi Connection

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

Steps


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

After the connection is completed, the AX PRO will prompt to exit AP mode and automatically switch to STA mode.

Device Maintenance

You can reboot the device.

Steps

1. On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.
2. Tap  → **Maintenance** → **Reboot Device**.
The AX PRO will reboot.

4.3 Set-up with the Web Client

Steps

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

Note

- When using mobile browser, the default IP Address is 192.168.8.1.
 - When connecting the network cable with computer directly, the default IP Address is 192.0.0.64.
-

4. Use the activation user name and password to login.

Note

- Refer to *Activation* chapter for the details.
 - Only the administrator 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 a web client. At the top, there are two user status cards: 'Administrator' (1) and 'Installer' (1). Below these is the 'Control Panel Status' section, which includes indicators for External Power Supply (Connect), Wired Network (Normal), Wi-Fi (Network Disconnected), Cellular Data Network (Network Disconnected), Battery (100%), and Chassis Status (Open). There are also indicators for Wireless Average (28dBm) and Cloud Connection (Normal). The bottom section is divided into two tables: 'Device Status' and 'Partition'. The 'Device Status' table shows 3 rows of data for Zone, Siren, and Keypad. The 'Partition' table shows 3 rows of data for Partition 1, 2, and 3, all with a status of 'Disarm'.

No.	Type	Total	Abnormal Number	Normal Number
1	Zone	4	4	0
2	Siren	1	1	0
3	Keypad	0	0	0

No.	Partition Name	Partition Status
1	Partition 1	Disarm
2	Partition 2	Disarm
3	Partition 3	Disarm

4.3.1 Communication Settings


Wired Network

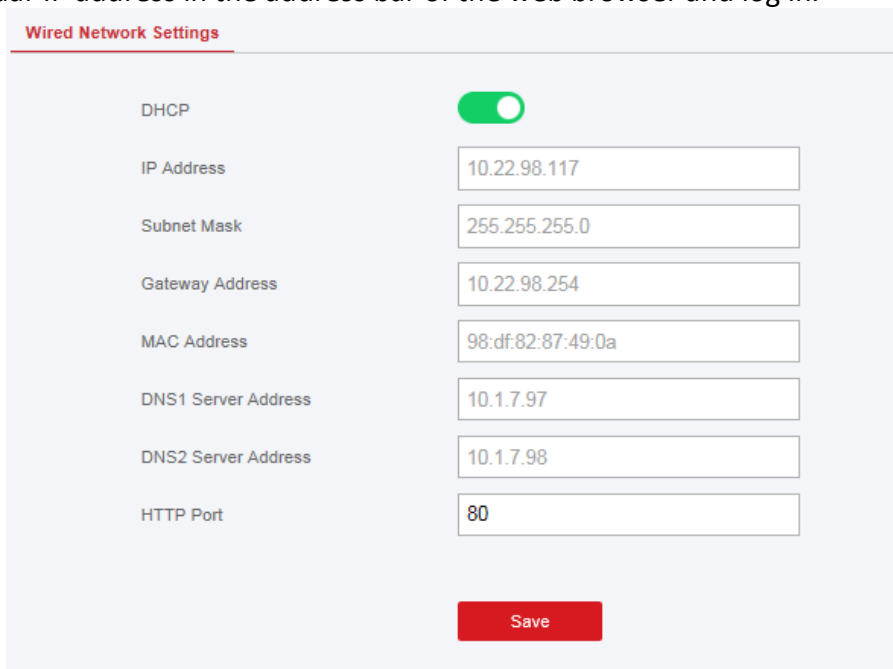
You can set the device IP address and other network parameters.

Steps



Functions varied depending on the model of the device.

1. In the client software, select the device on the **Device Management** page and click , or enter the radar IP address in the address bar of the web browser and log in.



DHCP	<input checked="" type="checkbox"/>
IP Address	<input type="text" value="10.22.98.117"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="10.22.98.254"/>
MAC Address	<input type="text" value="98:df:82:87:49:0a"/>
DNS1 Server Address	<input type="text" value="10.1.7.97"/>
DNS2 Server Address	<input type="text" value="10.1.7.98"/>
HTTP Port	<input type="text" value="80"/>

Save

2. Click **Communication Parameters** → **Ethernet** to enter the page.

3. Set the parameters.

Automatic Settings: Enable **DHCP** and set the HTTP port. Manual Settings: Disabled **DHCP** and set **IP Address, Subnet Mask, Gateway Address, DNS Server Address**.

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

5. Click **Save**.

Wi-Fi

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

Steps

1. Click **Communication Parameters** → **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: Input 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 input Wi-Fi password and click **Connect**.

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

Wi-Fi Settings **WLAN**

DHCP:

IP Address: 192.168.1.29

Subnet Mask: 255.255.255.0

Gateway Address: 192.168.1.1

MAC Address: ec:9c:32:5a:43:40

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

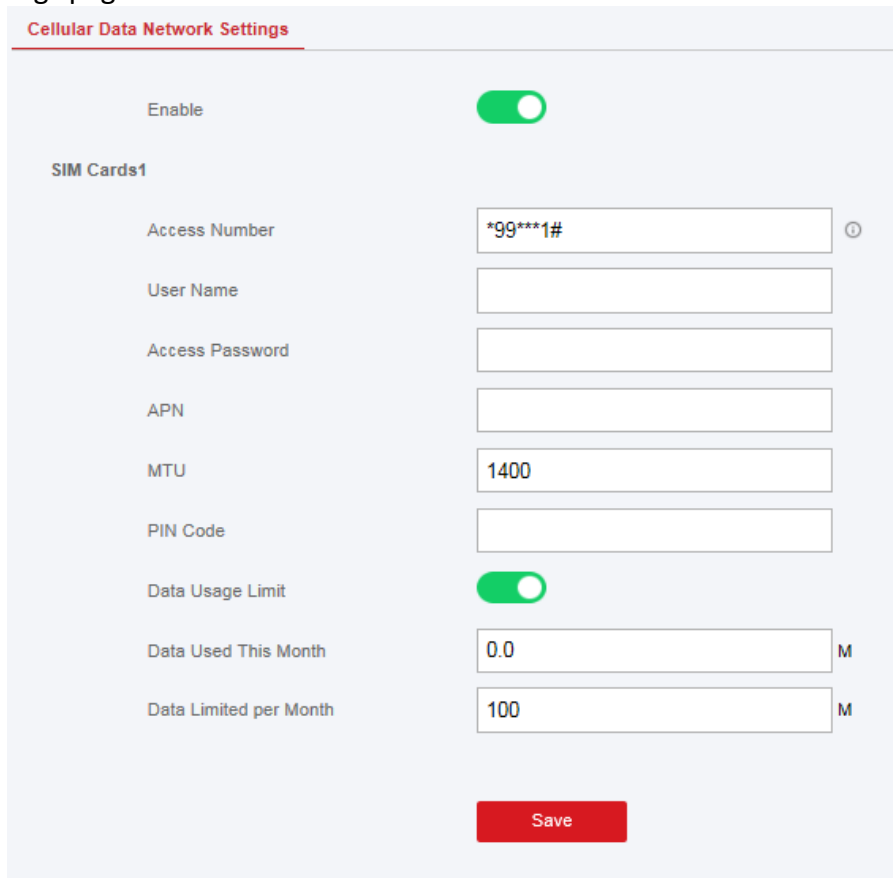
Set the cellular network parameters if you insert a SIM card inside the device. By using the cellular network, the device can upload alarm notifications to the alarm center.

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

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



2. Enable Wireless Dial.
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 input 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 Parameters** → **Alarm Receiving Center** to enter the Alarm Receiving Center page.

Alarm Receiving Center

Alarm Receiver Center1

Enable	<input checked="" type="checkbox"/>
Protocol Type	*SIA-DCS
Address Type	Domain Name
Domain Name	tyu
Port No.	0
Account Code	yyu
Transmission Mode	TCP
Retry Timeout Period	20 s
Attempts	3
Heartbeat Interval	<input type="text"/> s <input type="checkbox"/> Enable
Encryption Arithmetic	AES
Password Length	256
Secret Key	<input type="text"/>

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

Note

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

- Select the **Protocol Type** as **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, or ***ADM-CID** 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.

*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.

ADM-CID or **SIA-DCS** You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, timeout, re-upload times and

heartbeat interval.

 **Note**

Set the heartbeat interval with the range from 10 to 3888000 seconds.

ISUP You do not need to set the ISUP protocol parameters.

***SIA-DCS** or ***ADM-CID** You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, retry timeout period , attempts, heartbeat interval, encryption arithmetic, password length and secret key.

 **Note**

Set the heartbeat interval with the range from 10 to 3888000 seconds.

For encryption arithmetic: The panel support encryption format for information security according to DC-09, AES-128, AES-192 and AES-256 are supported when you configure the alarm center.

For the secret key: When you use an encrypted format of DC-09, a key should be set when you configure the ARC. The key would be issued offline by ARC , which would be used to encrypt the message for substitution security.

4. Click **Save**.

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 Parameters** → **Event Types Notification** .

iVMS-4200 Alarm Receiving Center APP Phone Call and SMS

Zone Alarm/Lid Opened	<input checked="" type="checkbox"/>
Peripherals Lid Opened	<input checked="" type="checkbox"/>
Panel Lid Opened	<input checked="" type="checkbox"/>
Panic Alarm	<input checked="" type="checkbox"/>
Medical Alarm	<input checked="" type="checkbox"/>
Fire Alarm	<input checked="" type="checkbox"/>
Gas Alarm	<input checked="" type="checkbox"/>
Panel Status	<input checked="" type="checkbox"/>
Zone Status	<input checked="" type="checkbox"/>
Peripherals Status	<input checked="" type="checkbox"/>
Panel Operation	<input checked="" type="checkbox"/>
Smart Alarm Event	<input checked="" type="checkbox"/>

Save

2. Enable the target notification.

 **Note**

If you want to send the alarm notifications to the mobile client, you should also set the **Mobile Phone Index**, **Mobile Phone Number** , and check the **Notification Type**.

 **Note**

For message notification in alarm receiving center, select the center index before settings.

3. Click **Save**.

Result

Table 4-1 Options of Notifications

Option	Notification
iVMS-4200	Zone alarm & Lid Opened Wireless Device Lid Opened Tamper Notification Panic Alarm Notification Medical Alarm Notification Gas Alarm Notification Fire Alarm Notification Panel Management Notification System Status Notification Detector Status Notification Wireless Device Status Notification
Alarm Receiver Center	Alarm Receiver Center 1&2 Zone alarm & Lid Opened Wireless Device Lid Opened Tamper Notification Panic Alarm Notification Medical Alarm Notification Gas Alarm Notification Fire Alarm Notification Panel Management Notification System Status Notification Detector Status Notification Wireless Device Status Notification
Cloud	Zone alarm & Lid Opened Wireless Device Lid Opened Tamper Notification Panic Alarm Notification Medical Alarm Notification

Option	Notification
	Gas Alarm Notification Fire Alarm Notification Panel Management Notification System Status Notification Detector Status Notification Wireless Device Status Notification
Mobile Phone	Mobile Phone Index 1 to 8 Mobile Phone Number Notification Type SMS & Voice Call Check Box Zone alarm & Lid Opened (Set Filter Time) Number of Calls Wireless Device Lid Opened Tamper Notification Panic Alarm Notification Medical Alarm Notification Gas Alarm Notification Fire Alarm Notification Panel Management Notification System Status Notification Detector Status Notification Wireless Device Status Notification

 **Note**

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 Parameters** → **Cloud Service Settings** to enter the Hik-Connect Registration Settings page.

Cloud Service Settings

Register to Hik-Connect

Hik-Connect Connection Status: Offline

Custom Server Address:

Server Address:

Communication Mode: Wired Network & Wi-Fi Priority

Verification Code:

The code should contain 6 to 12 characters (it is recommended to be more than 8 characters and the combination of numeric and letter)

Save

2. Click **Communication Parameters** → **Guarding Vision Registration** to enter the Guarding Vision Registration Settings page.
3. Check **Register to Hik-Connect**.

Note

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

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

4. Check **Register to Guarding Vision**.

Note

By default, the device Guarding Vision service is enabled.

You can view the device status in the Guarding Vision server (www.guardingvision.com).

5. Enable **Custom Server Address**.

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

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

Auto

The system will select the communication mode automatically according to the sequence of, wired network, Wi-Fi network, and cellular data network. Only when the current network is disconnected, will the device connect to other network.

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.

7. Optional: Change the authentication password.
-

Note

- By default, the authentication password is displayed in the text box.
 - The authentication password 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.
-

8. 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. Click the block to enable the function of sending video verification event .
 3. Enter the sender's information.
-

Note

It is recommended to use Gmail and Hotmail for sending mails.

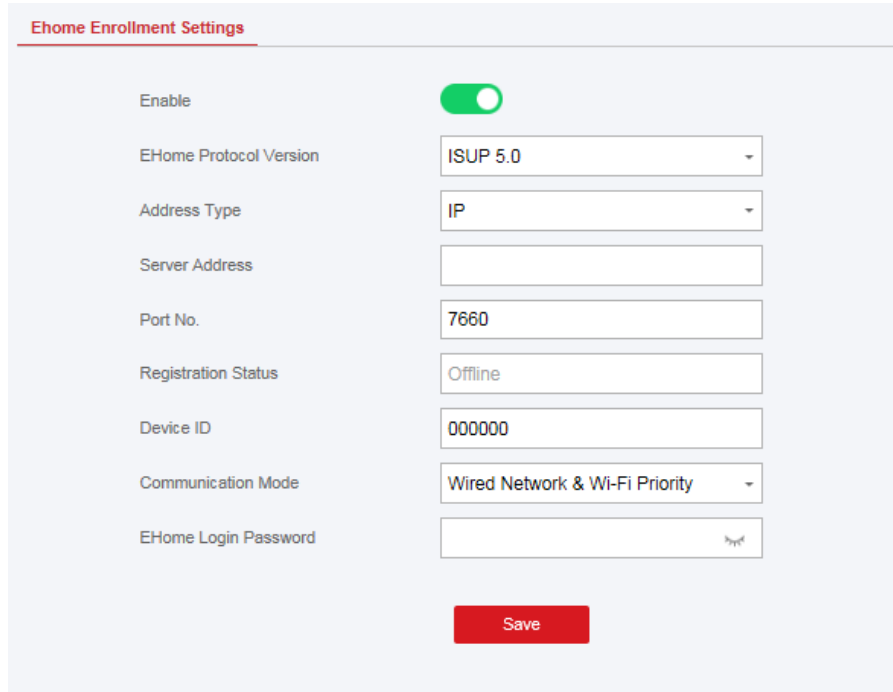
4. Enter the receiver's information.
5. Click **Receiver Address Test** and make sure the address is correct.
6. Click **Save**.

ISUP

In this section, you can create an ISUP account, and edit the IP address/domain name, port number.

Steps

1. Click **Communication Parameters** → **ISUP Registration** to enter the ISUP Registration Settings page.



The screenshot shows the 'Ehome Enrollment Settings' page. It contains the following fields and controls:

- Enable:** A green toggle switch is turned on.
- EHome Protocol Version:** A dropdown menu set to 'ISUP 5.0'.
- Address Type:** A dropdown menu set to 'IP'.
- Server Address:** An empty text input field.
- Port No.:** A text input field containing '7660'.
- Registration Status:** A text input field containing 'Offline'.
- Device ID:** A text input field containing '000000'.
- Communication Mode:** A dropdown menu set to 'Wired Network & Wi-Fi Priority'.
- EHome Login Password:** An empty password input field with a visibility icon.

A red 'Save' button is located at the bottom center of the form.

2. Slide the slider to enable ISUP protocol.
3. Select the **Address Type** as **IP** or **Domain Name**.
4. Enter IP address or domain name according to the address type.
5. Enter the port number for the protocol.

Note

By default, the port number for ISUP is 7660.

6. Set an account, including the **Device ID** and **ISUP Login Password**.
7. Select **Communication Mode**.

Auto

The system will select the communication mode automatically according to the sequence of, wired network, Wi-Fi network, and cellular data network. Only when the current network is disconnected, will the device connect to other network.

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.

8. 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 Parameters** → **NAT** to enter the page.

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**

4. Set the HTTP port and the service port.

5. 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 Address 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.

4.3.2 Device Management

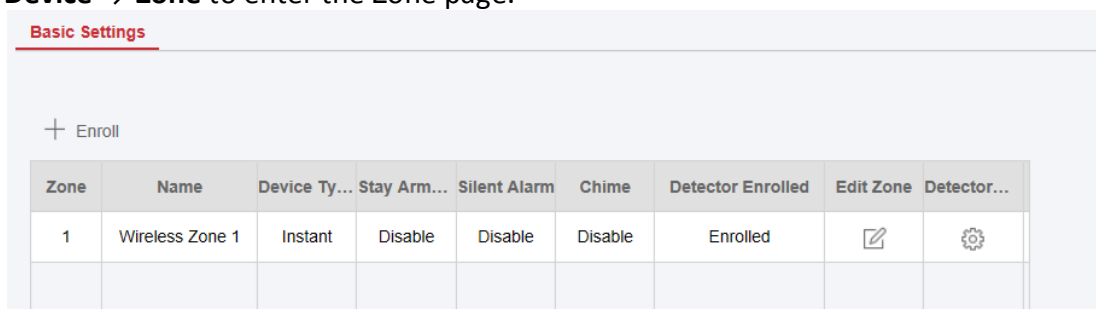
You can manage the enrolled peripherals including detector, sounder, keypad, etc. in this section.



Zone

You can set the zone parameters on the zone page.

Steps

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



Zone	Name	Device Ty...	Stay Arm...	Silent Alarm	Chime	Detector Enrolled	Edit Zone	Detector...
1	Wireless Zone 1	Instant	Disable	Disable	Disable	Enrolled		

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

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. 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.

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 Hours 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.

6. Enable **Cross zone, Silent Alarm, etc.** according to your actual needs.
-

Note

Some zones do not support the function. Refer to the actual zone to set the function.

7. Set the **Sounder Delay Time**. The sounder will be triggered immediately or after the set time.
 8. If required, link a camera for the zone.
 9. Enable **Detector Enrolled**, enter the serial No., and set the linked camera No.
 10. Click **OK**.
-

Note

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

11. Click **Detector Settings** to enter the Detector Settings page.

Detector Settings

Primary Contact

LED

Primary Contact

External Contact

Enable

External Contact Type

Polling Rate

OK Cancel


 **Note**

it is not allowed to turn off the contact for EN compliance.

Sounder

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

Steps

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

Sounder	<input type="text" value="1"/>
Name	<input type="text" value="Sounder 1"/>
Volume	<input type="text" value="2"/>
Enroll Wireless Sounder	<input checked="" type="checkbox"/>
Serial No.	<input type="text" value="Q00007031"/>
Area	<div><input checked="" type="checkbox"/> Active Functions <input checked="" type="checkbox"/> Area1 <input checked="" type="checkbox"/> Area2 <input checked="" type="checkbox"/> Area3</div>
Sounder Type	<input type="text" value="Internal"/>
Alarm LED Indicator	<input checked="" type="checkbox"/>
Alarm Buzzer	<input checked="" type="checkbox"/>
Arm/Disarm LED Indicator	<input checked="" type="checkbox"/>
Arm/Disarm Buzzer	<input type="checkbox"/>
Polling Rate	<input type="text" value="5min"/>
Alarm Duration	<input type="text" value="90"/> s

3. Set the sounder name and the volume.

 **Note**

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

4. Enable **Enroll Wireless Sounder** and set the sounder serial No.

5. Select the linked area.

 **Note**

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

6. Select to enable **Alarm LED Indicator**, **Alarm Buzzer**, **Arm/Disarm LED Indicator**, and **Arm/Disarm Buzzer**.
 7. Set the **Polling Rate** and **Alarm Duration**.
 8. Click **OK**.
-


 **Note**

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

Keypad

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

Steps

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

Name	<input type="text" value="keypad 1"/>
Serial No.	<input type="text" value="Q00000204"/>
Keypad	<input type="text" value="1"/>
Function Buttons	<input checked="" type="checkbox"/>
Linked Area	<div style="border: 1px solid gray; padding: 5px;"> <input type="checkbox"/> Active Functions <input type="checkbox"/> Area 6 <input type="checkbox"/> Area 23 <input type="checkbox"/> Area 32 </div>
Arming Without Password	<input type="checkbox"/>
Buzzer	<input checked="" type="checkbox"/>
Backlight Off Time	<input type="text" value="08:00"/> to <input type="text" value="20:00"/> <input type="checkbox"/> Backlight
Silent Panic Alarm	<input type="checkbox"/>
Silent Medical Alarm	<input type="checkbox"/>
Polling Rate	<input type="text" value="2min"/>
Enroll Wireless Keypad	<input checked="" type="checkbox"/>

3. Set the keypad name.
4. Check the check box to enable the function of buzzer, silent panic alarm, silent medical alarm, and keypad button.
5. Check the check box to enable the function of arming without password.
6. Check the **Enable** check box of Back-light Off Time, and set the duration of light off.
7. Set the rolling rate.
8. Select the keypad linked area.

 **Note**

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

9. Set whether to cancel the enrollment of the keypad or not. If the link is enabled, the device will be deleted.
10. Click **OK**.


Note

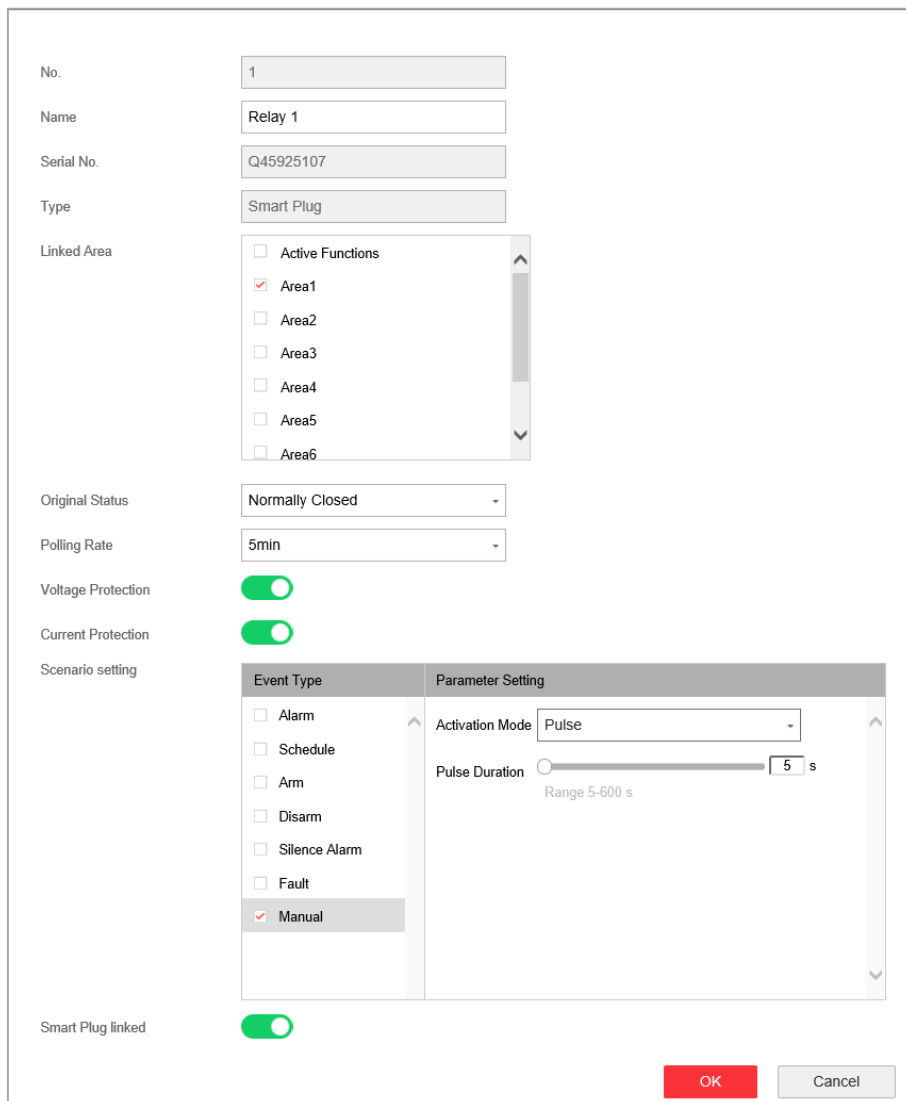
- After the keypad is configured, you can click **Status** → **Keypad** to view the keypad status.
 - You can set the keypad password on the page of **User Management** → **User** → **Operation**.
-

Automation

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

Steps

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



The screenshot shows a configuration window for a relay output device. The fields are as follows:

- No.: 1
- Name: Relay 1
- Serial No.: Q45925107
- Type: Smart Plug
- Linked Area: Active Functions, Area1, Area2, Area3, Area4, Area5, Area6
- Original Status: Normally Closed
- Polling Rate: 5min
- Voltage Protection:
- Current Protection:
- Scenario setting:

Event Type	Parameter Setting
<input type="checkbox"/> Alarm	Activation Mode: Pulse
<input type="checkbox"/> Schedule	Pulse Duration: 5 s (Range 5-600 s)
<input type="checkbox"/> Arm	
<input type="checkbox"/> Disarm	
<input type="checkbox"/> Silence Alarm	
<input type="checkbox"/> Fault	
<input checked="" type="checkbox"/> Manual	
- Smart Plug linked:

Buttons: OK, Cancel

- Set the name of the relay output device.

- Select the linked area for output.

Note

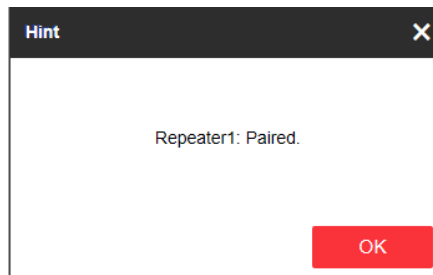
- Only enabled areas will be listed.
 - The newly added peripheral is linked to area 1 by default.
 - The function varies according to different relay types
-
- Set the original status as Normally Closed or Normally Opened.
 - Set the Polling rate.
 - Set whether to protect voltage/current or not.
 - Set the event for being triggered.
 - Set the activation after being triggered.
 - Set whether to link to the relay output device or not. If the link is enabled, the device will be deleted.


Repeater

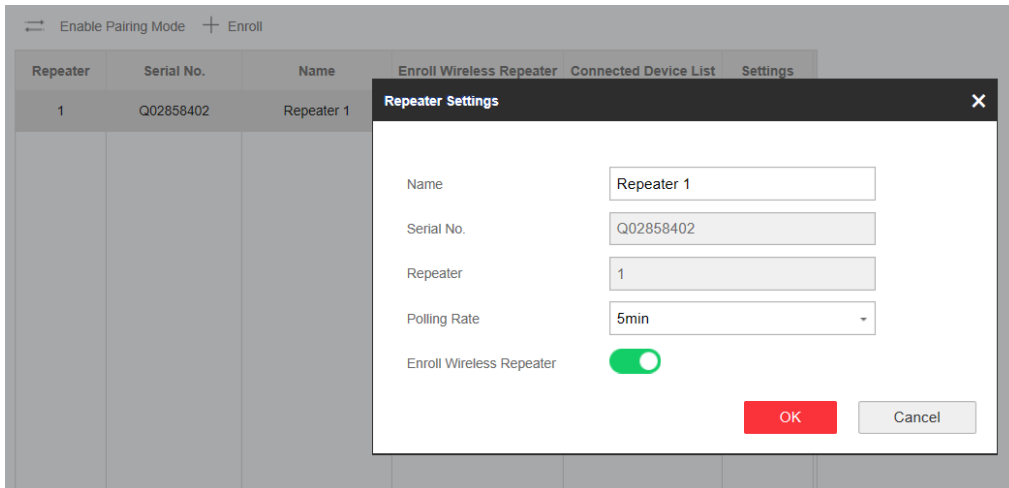
The repeater can amplify signals between the control panel and the peripherals.

Steps

1. Click **Device** → **Repeater** to enter the page.
2. Click **Enroll**, enter the serial No. and select the device type to add a repeater.
3. Click **Enter Paring Mode** to make the repeater enter the mode of device paring.
4. When the distance between the peripheral and the control panel is far, the repeater can be used as a transfer station for pairing. The pairing mode lasts for 3 minutes and cannot be interrupted. After the pairing is successful, a list of connected devices will be displayed.



5. Click  to edit the repeater information.



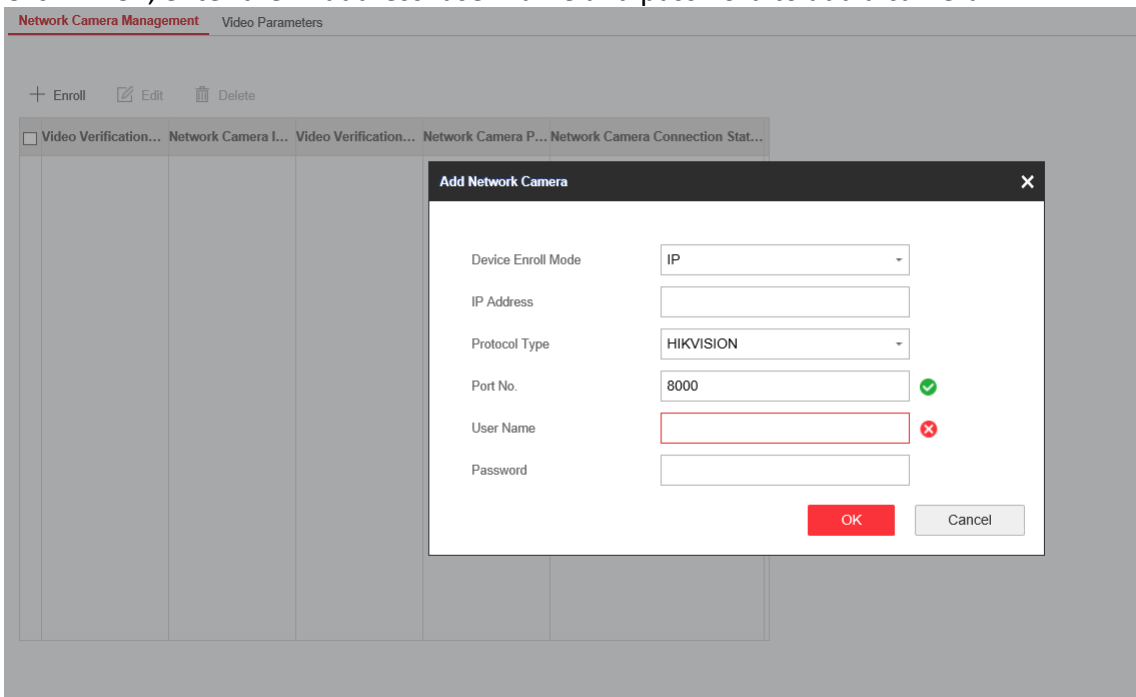
- Set the name of the repeater.
- Set the polling rate of the repeater.
- Set whether to cancel the enrollment of the repeater or not. If the link is enabled, the device will be deleted.

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.

4.3.3 Area Settings

Basic Settings

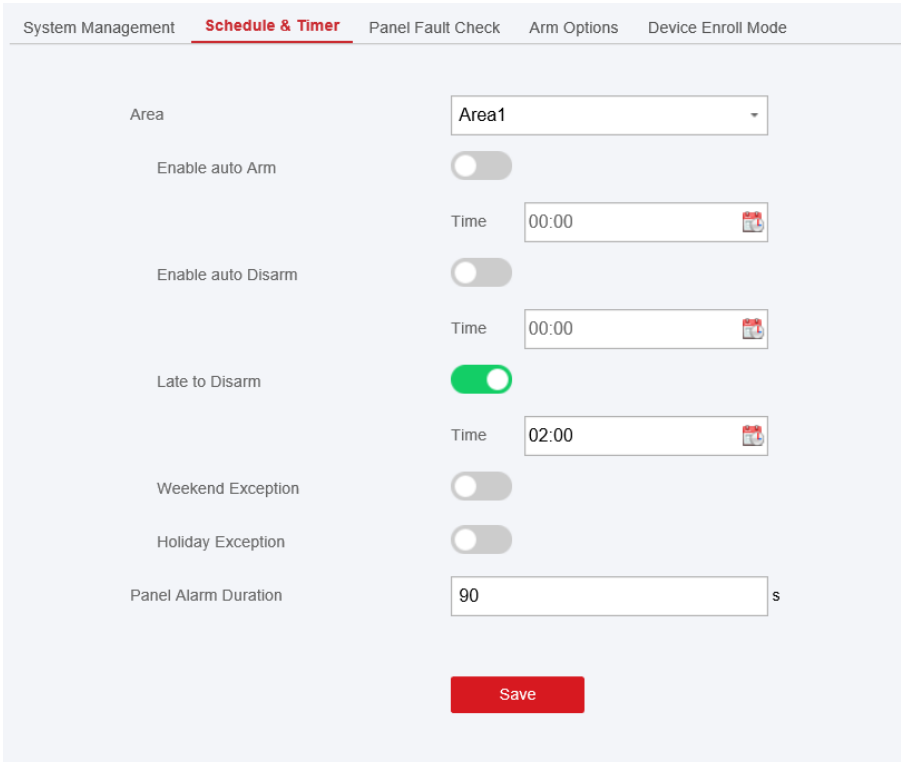
You can link zones to the selected area.

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.

Schedule and Timer Settings

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



The screenshot shows the 'Schedule & Timer' configuration page for 'Area1'. The page has a navigation bar with tabs: 'System Management', 'Schedule & Timer' (selected), 'Panel Fault Check', 'Arm Options', and 'Device Enroll Mode'. The settings are as follows:

Setting	Value
Area	Area1
Enable auto Arm	Off
Time	00:00
Enable auto Disarm	Off
Time	00:00
Late to Disarm	On
Time	02:00
Weekend Exception	Off
Holiday Exception	Off
Panel Alarm Duration	90 s

A red 'Save' button is located at the bottom of the form.

Steps

1. Click **System** → **System Options** → **Schedule & Timer** to enter the Schedule & Timer page.
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.
 - If the public area is enabled, the area 1 does not support auto arming.
-

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.
 - If the public area is enabled, the area 1 does not support auto disarming.
-

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**.

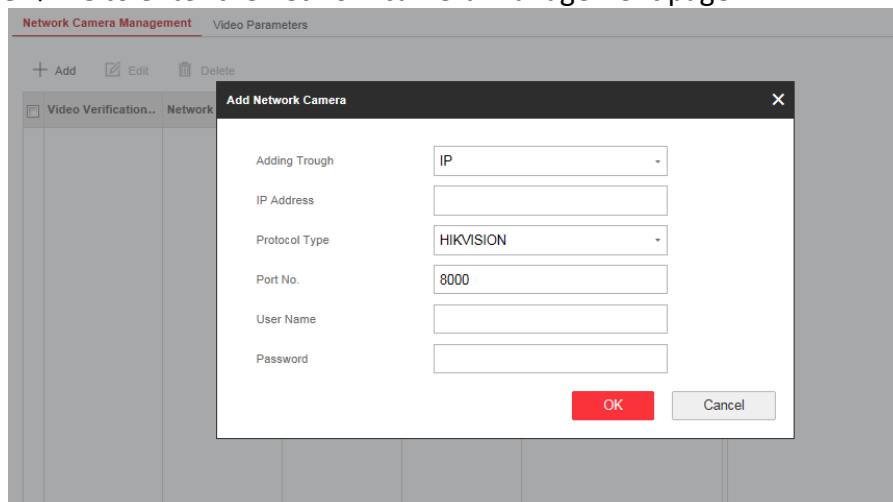
4.3.4 Video Management

You can add two network cameras to the AX 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 PRO

Steps

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



The screenshot shows a web interface titled "Network Camera Management" with a sub-tab "Video Parameters". A modal dialog box titled "Add Network Camera" is open, containing the following fields and values:

Field	Value
Adding Trough	IP
IP Address	
Protocol Type	HIKVISION
Port No.	8000
User Name	
Password	

Buttons: OK (red), Cancel (grey).

2. Click **Add**, 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 the .

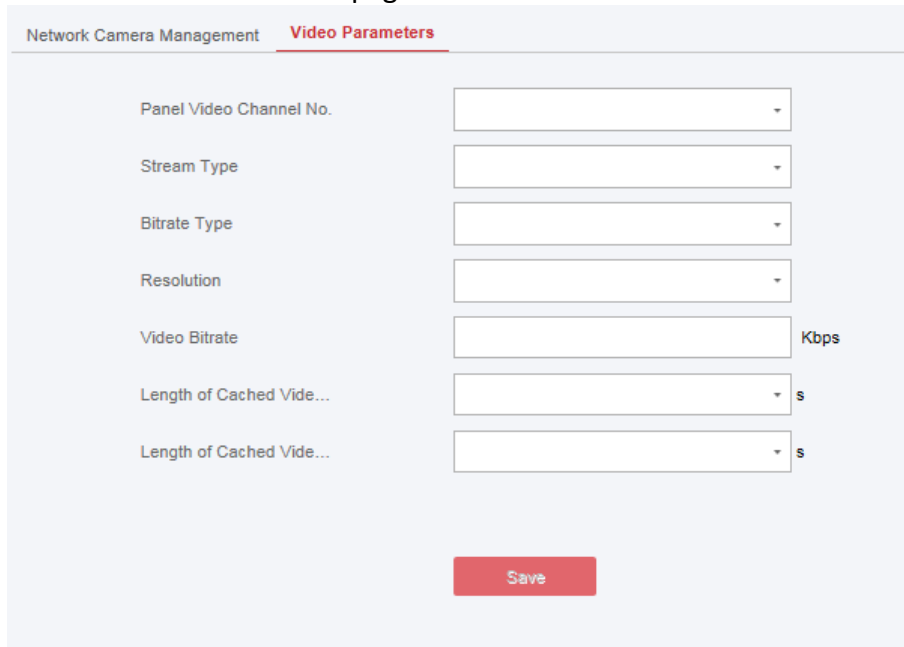
3. Select the **Panel Video Channel No.**.

4. Click **OK**.

Set Video Parameters

Steps

1. Click **Device** → **IPC** → **Video** to enter the page.



The screenshot shows a web interface for configuring video parameters. At the top, there are two tabs: "Network Camera Management" and "Video Parameters", with the latter being active. Below the tabs, there are seven configuration fields, each with a label and a dropdown menu:

- Panel Video Channel No. (dropdown)
- Stream Type (dropdown)
- Bitrate Type (dropdown)
- Resolution (dropdown)
- Video Bitrate (input field) with "Kbps" label to its right
- Length of Cached Vide... (dropdown) with "s" label to its right
- Length of Cached Vide... (dropdown) with "s" label to its right

At the bottom center of the form is a red "Save" button.

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.

4.3.5 Permission Management

Add/Edit/Delete Keyfob

You can add keyfob to the AX PRO and you can control the AX PRO via the keyfob. You can also

edit the keyfob information or delete the keyfob from the AX PRO.

Steps

1. Click **Device** → **Keyfob** to enter the Keyfob Management page.
2. Click **Add** 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 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 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 **Add** and place a Tag on the Tag area of the AX PRO.
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.

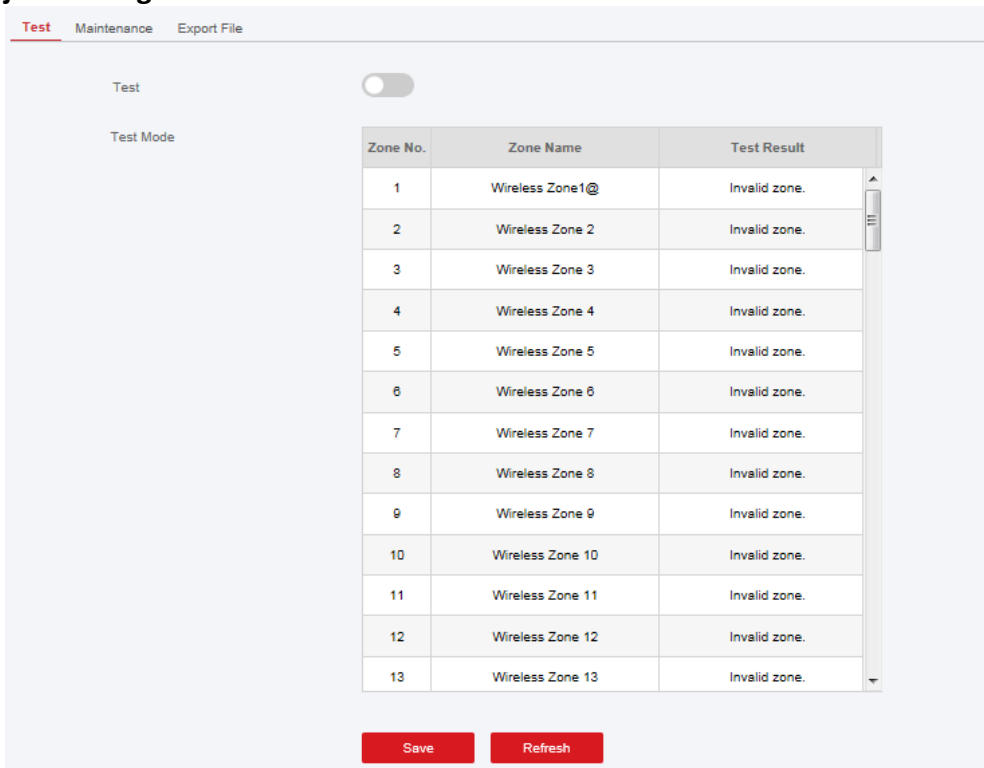
4.3.6 Maintenance

Test

The AX PRO supports walk test function.

Steps

1. Enter **Project Management** → **Maintain** → **Test** → to enable the function.



The screenshot displays the 'Test' interface. At the top, there are tabs for 'Test', 'Maintenance', and 'Export File'. Below the tabs, there is a 'Test' toggle switch (currently off) and a 'Test Mode' label. The main area contains a table with the following data:

Zone No.	Zone Name	Test Result
1	Wireless Zone1@	Invalid zone.
2	Wireless Zone 2	Invalid zone.
3	Wireless Zone 3	Invalid zone.
4	Wireless Zone 4	Invalid zone.
5	Wireless Zone 5	Invalid zone.
6	Wireless Zone 6	Invalid zone.
7	Wireless Zone 7	Invalid zone.
8	Wireless Zone 8	Invalid zone.
9	Wireless Zone 9	Invalid zone.
10	Wireless Zone 10	Invalid zone.
11	Wireless Zone 11	Invalid zone.
12	Wireless Zone 12	Invalid zone.
13	Wireless Zone 13	Invalid zone.

At the bottom of the interface, there are two red buttons: 'Save' and 'Refresh'.

Note

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

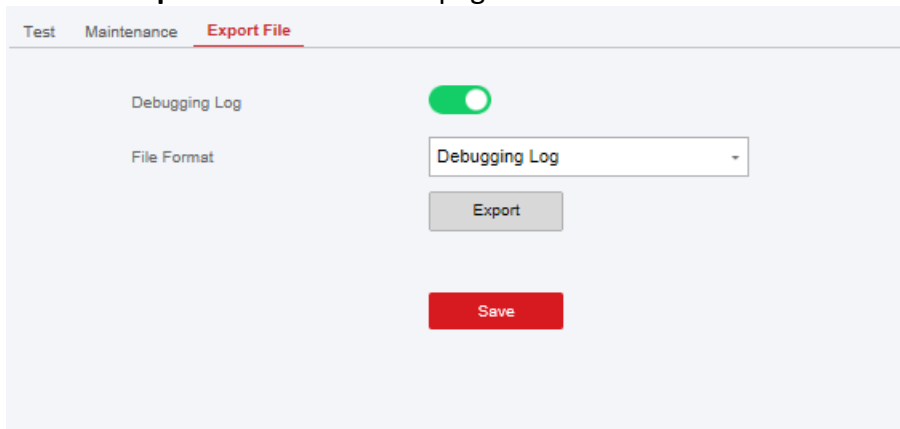
2. Check the **Test** check box to start walk test.
3. Click **Save** to complete the settings.
4. Trigger the detector in each zone.
5. Check the test result.

Export File

You can export debugging file to the PC.

Steps

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



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

4.3.7 System Settings

Authority Management

Set the authority options.

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

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

Forced Auto Arm	<input type="checkbox"/>
System Status Report	<input checked="" type="checkbox"/>
Voice Prompt	<input checked="" type="checkbox"/>
System Volume	<input type="range" value="3"/> 3 Range 0-10
Audible Tamper Alarm	<input checked="" type="checkbox"/>
Panel Lockup Button	<input type="checkbox"/>
Bypass On Re-Arm	<input type="checkbox"/>
Polling Loss Times	<input type="range" value="4"/> 4 Range 3-10

Save

Forced Auto Arm

If the option is enabled and there are active faults in a zone, the zone will be bypassed automatically when arming.

Note

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

System Status report

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

Voice Prompt

If the option is enabled, the AX PRO will enable the text voice prompt.

System Volume

The available system volume range is from 0 to 10.

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.

Polling Loss Times

Set the maximum duration for polling loss. The system will report fault if the duration is over the limit.

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** → **Fault Check** to enter the page.

System Management	Schedule & Timer	Panel Fault Check	Arm Options	Device Enroll Mode
Detect Network Camera Disconnection	<input checked="" type="checkbox"/>			
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"/>			
AC Power Loss Delay	<input type="text" value="10"/>	s		
<input type="button" value="Save"/>				

Detect Network Camera Disconnection

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

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.

AC 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.

System Management	Schedule & Timer	Panel Fault Check	Arm Options	Device Enroll Mode
Arm With Faults		<input checked="" type="checkbox"/>		
	Checklist	Arm With Fault		
Device Lid Opened	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Zone/Peripherals Poll Failure/Offline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Zone/Peripherals Low Battery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Zone Triggered	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Main Power Lost	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
Communication Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Arm LED Stay On	<input type="checkbox"/>			
Fault Prompts On Arming	<input type="checkbox"/>			
Fault Prompts On Disarming	<input checked="" type="checkbox"/>			
Early Alarm	<input checked="" type="checkbox"/>			
Early Alarm Time	<input type="text" value="30"/>		s	
<input type="button" value="Save"/>				

You can set the following parameters:

Enable Arming 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.

Arm LED Stay On

If the device applies EN standard, by default, the function is disabled. In this case, if the device is armed, the indicator will be solid blue for 5 s. And if the device is disarmed, the indicator will flash 5 times.

When the function is enabled, if the device is armed, the indicator will be on all the time. And if the device is disarmed, the indicator will be off.

Fault Prompt On Arming/Disarming

If the device applies EN standard, by default, the function is disabled. In this case, the device will not prompt faults during the arming/disarming procedure.

Enable 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.

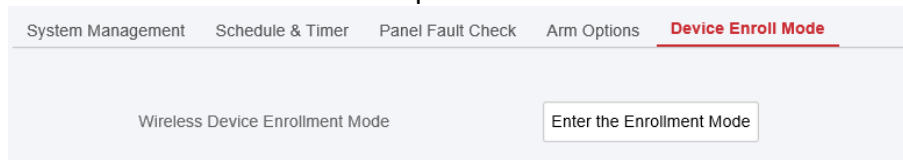


Note

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.



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** to enter the Time Management page.

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

You can synchronize the device time manually 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.

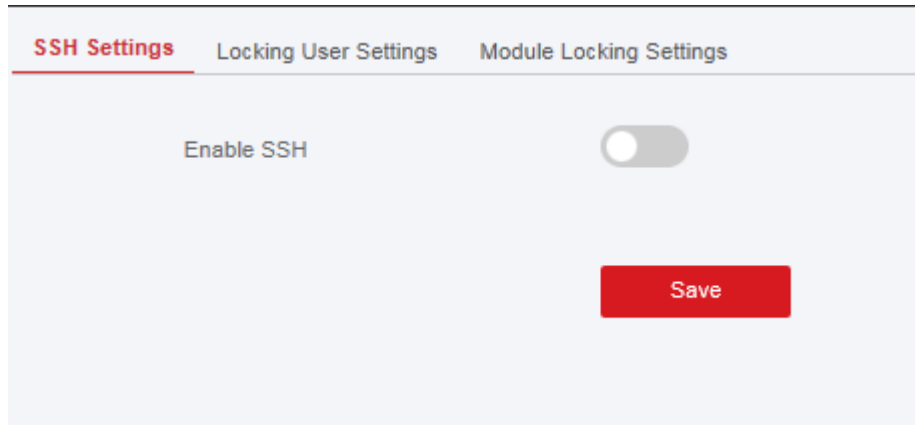
You can enable the DST and set the DST bias, DST start time, and DST end time.

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.

Locked Duration

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**.

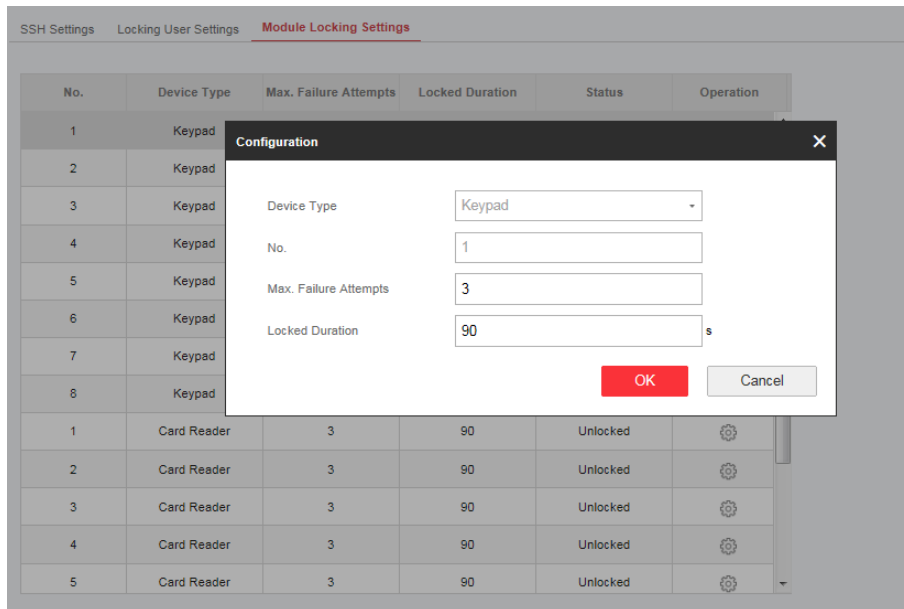
Module Lock Settings


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

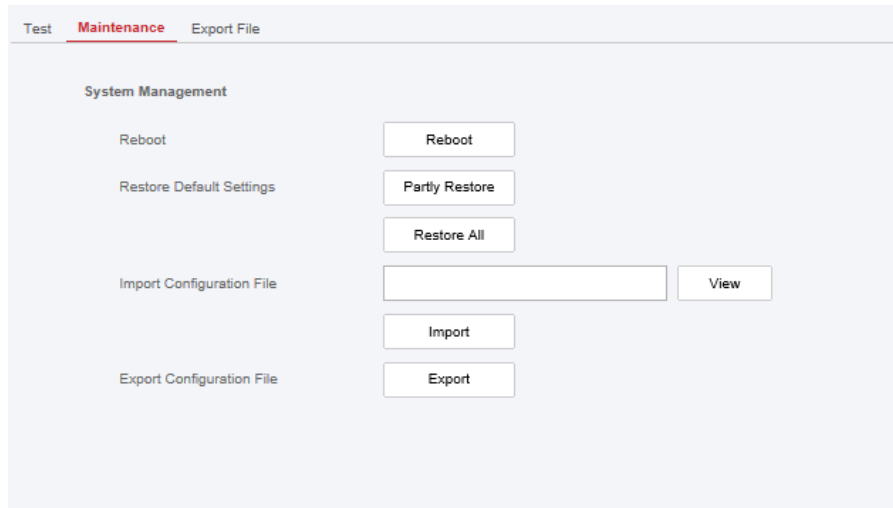
Set the locking duration when the keypad is locked. After the configured duration, the keypad will be unlocked.

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

System Maintenance

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

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

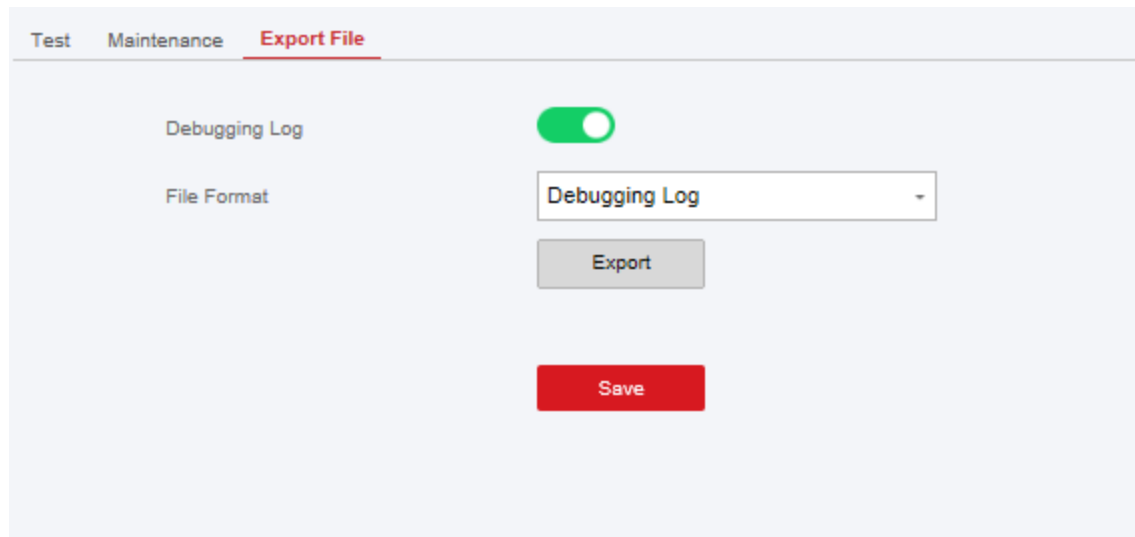
Click **View** to select configuration file from the PC and click **Import Configuration File** to import configuration parameters to the device. Importing configuration file requires entering the password set at the time of exporting.

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.

Export File

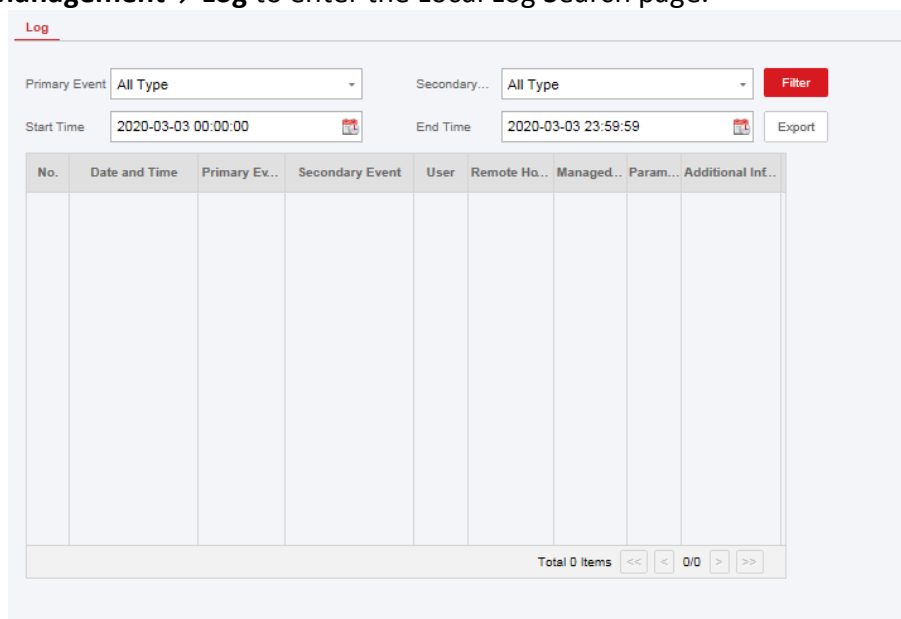
Click **Project Management**→ **Maintain**→ **Export File**
Enable **Debugging Log** to enable the function.



Select file type needs to be exported.
Click Export to export the file.

Local Log Search

You can search the log on the device.
Click **Project Management**→ **Log** to enter the Local Log Search page.



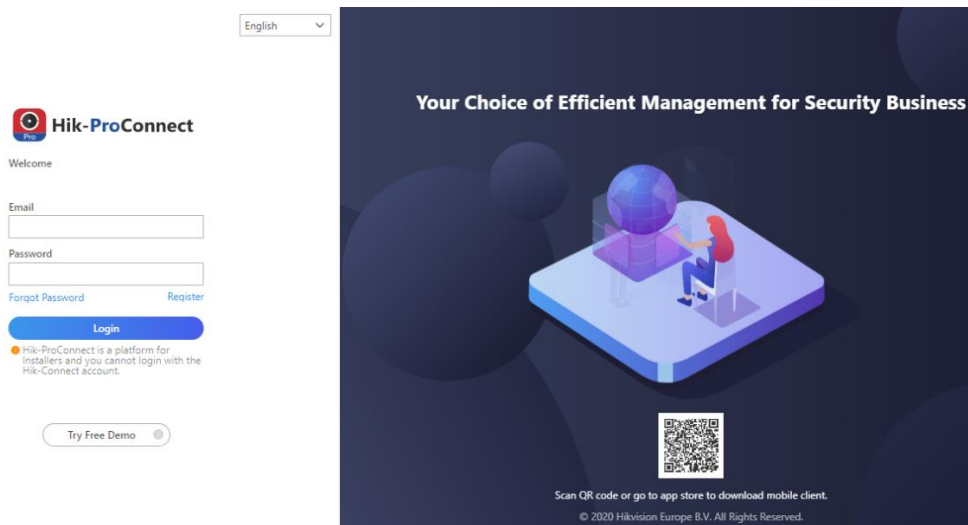
Select a major type and a minor type from the drop-down list, set the log start time and end time and click **Filter**. All filtered log information will be displayed in the list.
You can also click **Reset** to reset all search conditions.

Device Upgrade

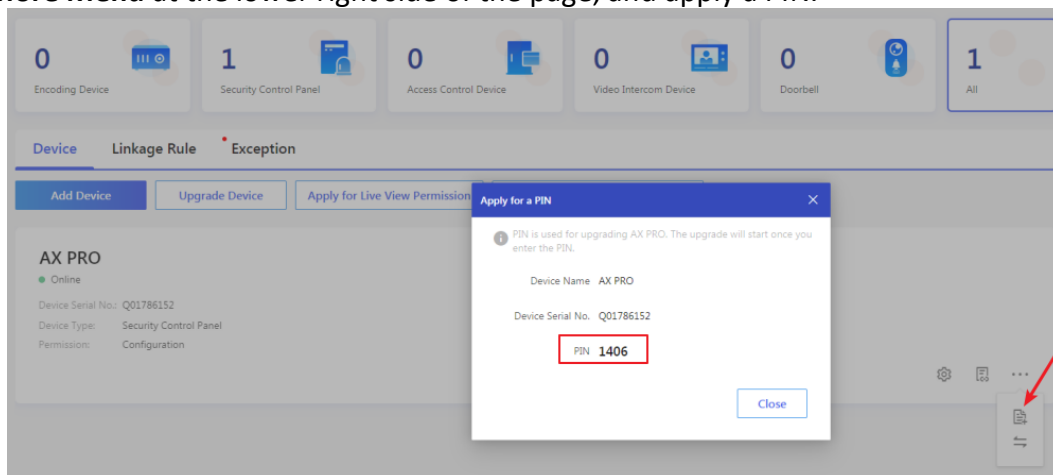
Get Manufacture PIN

To upgrade the device, a manufacture PIN is needed for authentication. The manufacture PIN can only get from the Hik-ProConnect service, which means that the installer, who authorized by administrator at access level 2, has authorized the access at level 4. The manufacture PIN can only work once.

- **Get PIN from Hik-ProConnect Service**



Login with the installer account and enter the page of the device to be upgraded. Click **More Menu** at the lower right side of the page, and apply a PIN.



- **Get PIN from HIKVISION tech-support**

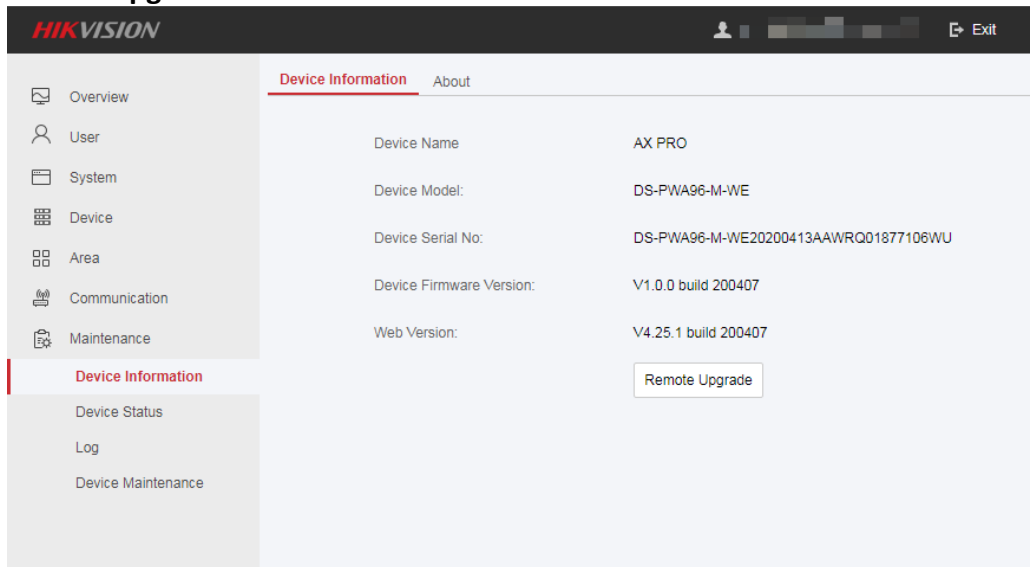
It is better to use remote desktop to access the local web client of control panel. The PIN

will be authorized according to the standard tech-support procedure.

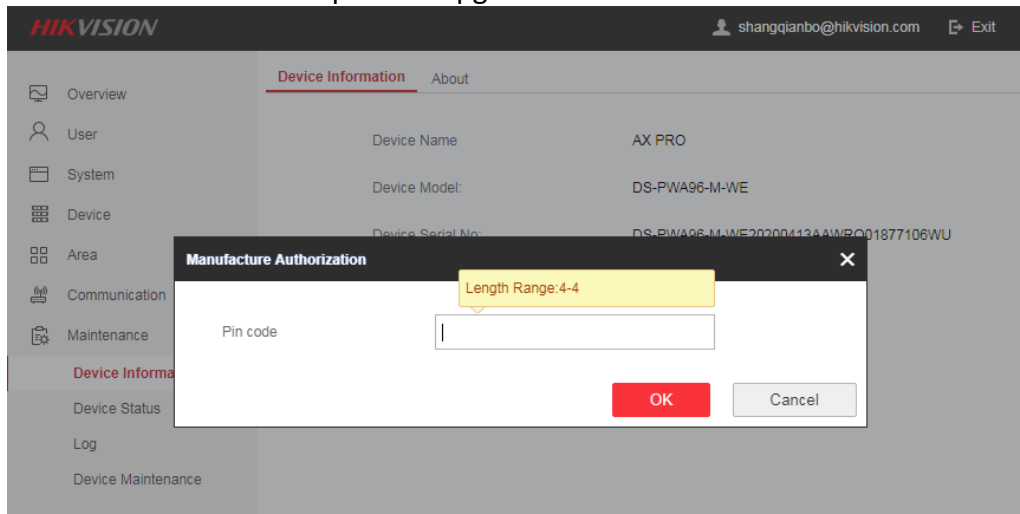
Firmware Upgrade

Steps:

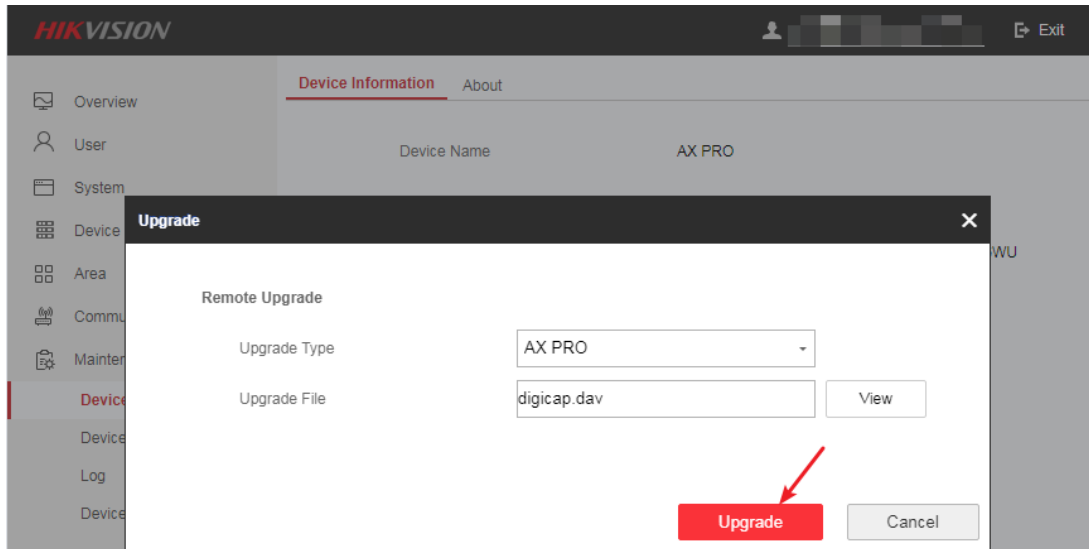
1. Click **Maintenance**→ **Device Information** to enter the page.
2. Click **Remote Upgrade**.



3. Enter the manufacture PIN to open the upgrade interface.



4. Click **View** to find the firmware file with the name digicap.dav.
5. Click **Upgrade** to complete.

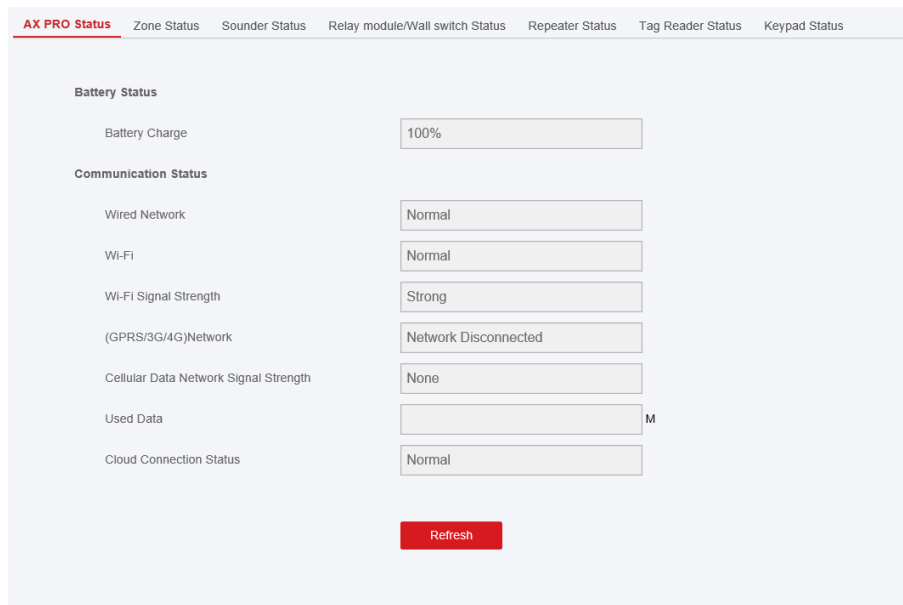


Note

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

4.3.8 Check Status

After setting the zone, repeater, and other parameters, you can view their status. Click **Status**. You can view the status of zone, relay, sounder, keypad, Tag reader, battery, and communication.



- 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.

4.4 Report to ARC (Alarm Receiver Center)

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

Setup ATS in Transceiver of Receiving Center

Steps:

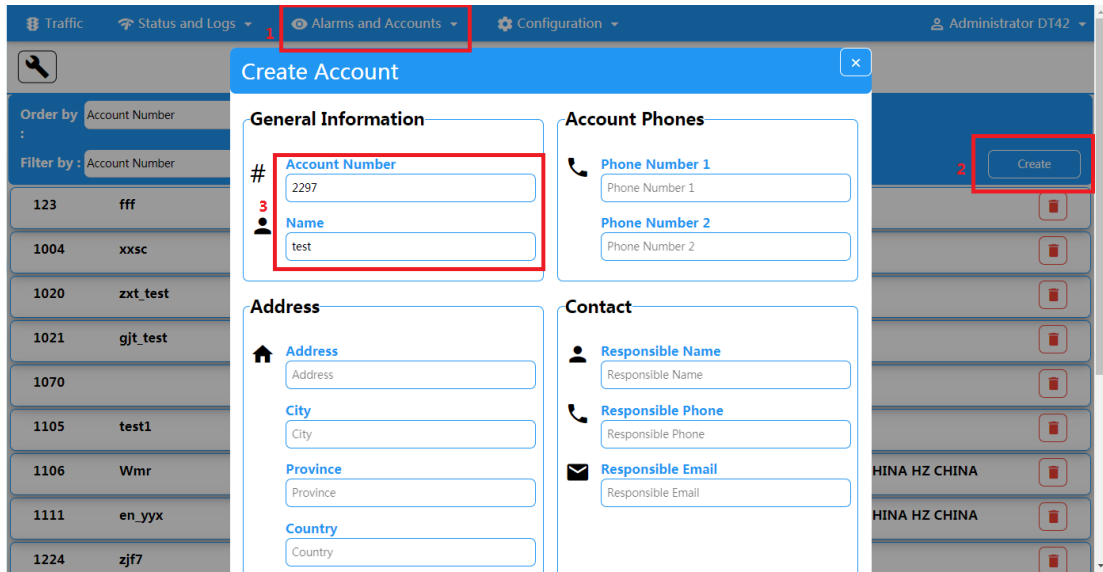
1. Login to the web client of the alarm receiver.
2. Click **Configuration**→ **IP Reception**, and create a receiving server as shown below.

The screenshot displays the 'Server Details' configuration interface. On the left, a sidebar lists servers from 'Server 1' to 'Server 7'. The main area shows the configuration for 'SIADC09 7'. The configuration form includes the following fields:

- Port:** 6666
- Protocol:** TCP
- Allow All panels to connect:** Yes
- Encryption Key Size:** 128
- Encryption Key:** 12345678901234567890123456789012

A 'Close' button is located at the bottom of the configuration form. The top of the interface shows navigation options like 'Traffic', 'Status and Log', and a user profile 'Administrator DT142'.

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

Address Type

Server Address

Port No.

Account Code

Transmission Mode

Impulse Counting Time s

Attempts

Polling Rate Enable

Encryption Arithmetic

Password Length

Secret Key

- = 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 <ul style="list-style-type: none">○ 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 <ul style="list-style-type: none">○ Encryption Arithmetic — AES○ Password Length — 128 — 192 — 256○ Secret Key Setup the encryption key length and input the key provided by the ARC.

Signalling 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 application interface with a blue header bar. The header contains several menu items: 'Traffic' (highlighted with a red box), 'Status and Logs', 'Alarms and Accounts', and 'Configuration'. The user name 'Administrator DT42' is visible in the top right corner.

Traffic

Refresh in 16

Order by: Reception Time (dropdown), Ascendant (radio), Descendant (radio)

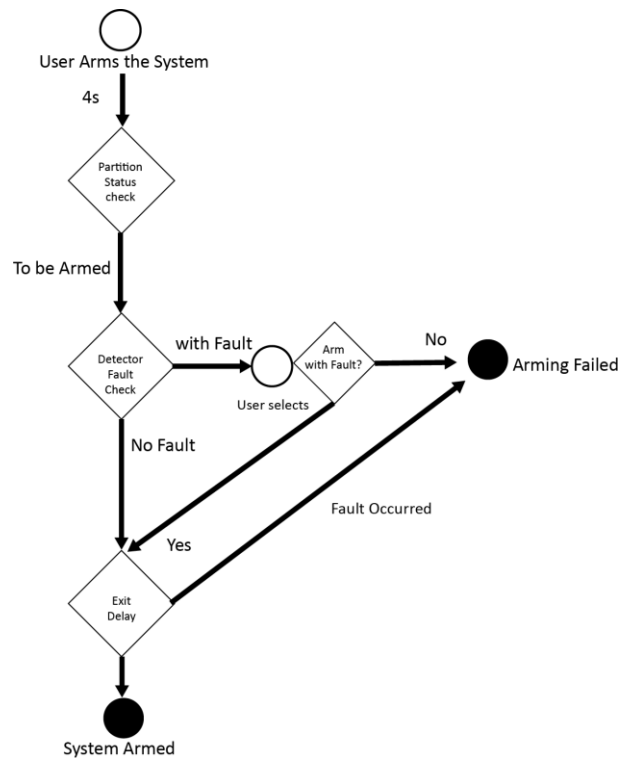
Filter by: Event ID (dropdown), Filter (input), + (button)

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

Chapter 5 General Operations

5.1 Arming

You can use keypad, keyfob, Tag, client software, mobile client to arm your system. After the arming command is sending to AX PRO, the system will check the detector status. If the detector is in fault, you will need to choose whether to arm the system with fault. While the system is armed, the AX PRO will prompt the result in 5s, and upload the arming report.



Access level of Arming

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

Arming Indication

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

Reason of Arming Failure

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

- Backup battery exception
- Alarm receiving fault
- Sounder fault
- Low battery of the keyfob
- Others

Arming with Fault

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

Forced arming only takes effect on the current arming operation.

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

5.2 Disarming

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

Disarming Indication

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

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

Entry Delay Duration

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

Early Alarm

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

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

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

5.3 SMS Control

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

SMS format for Arming/disarming/silencing alarm:

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

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

Operation type: 1- Area Operation

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

A. Trouble Shooting

A.1 Communication Fault

A.1.1 IP Conflict

Fault Description:

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

Solution:

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

A.1.2 Web Page is Not Accessible

Fault Description:

Use browser to access web pages and display Inaccessible.

Solutions:

1. Check whether the network cable is loose and the panel network is abnormal.
2. The panel port has been modified. Please add a port to the web address for further access.

A.1.3 Hik-Connect is Offline

Fault Description:

The web page shows that the Hik-Connect is offline.

Solution:

Network configuration of the panel is error, unable to access extranet.

A.1.4 Network Camera Drops off Frequently

Fault Description:

System reports multiple event logs of IPC disconnection and connection.

Solution:

Check whether the network communication or camera live view is proper.

A.1.5 Failed to Add Device on APP

Fault Description:

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

Solution:

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

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

Fault Description:

After the alarm is triggered, the app/4200/ alarm center does not receive the alarm message.

Solution:

"Message push" - "alarm and tamper-proof notice" is not enabled. You should enable "alarm and tamper-proof notice".

A.2 Mutual Exclusion of Functions

A.2.1 Unable to Enter Registration Mode

Fault Description:

Click the panel function key, and prompt key invalid.

Solution:

The panel is in "Hotspot" mode. Switch the panel to "station" mode, and then try to enter the registration mode again.

A.3 Zone Fault

A.3.1 Zone is Offline

Fault Description:

View status of zones which displays offline.

Solution:

Check whether the detector reports undervoltage. Replace the detector battery

A.3.2 Zone Tamper-proof

Fault Description:

View status of zones which displays tamper-proof.

Solution:

Make tamper-proof button of the detector holden.

A.3.3 Zone Triggered/Fault

Fault Description:

View status of zones which displays triggered/fault.

Solution:

Reset the detector.

A.4 Problems While Arming

A.4.1 Failure in Arming (When the 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	<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 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.

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

Voice Prompt: Armed/Arming failed.

C. Output Types

Table C-1 Output Types

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

D. Event Types

Table D-1 Event Types

Event Types	Custom	Default 1 (client software notification)	Default 2 (alarm receiving center 1/2)	Default 3 (mobile client)	Default 4 (telephone)
Alarm and Tamper	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

Table F-1 SIA and CID Code

SIA Code	CID Code	Description
BA	E130	Burglary Alarm
BH	R130	Burglary Alarm Restored
HA	E122	Silent Panic Alarm
HH	R122	Silent Panic Alarm Restored
NA	E780	Timeout Alarm
BH	R780	Timeout Alarm Restored
PA	E120	Panic Alarm
PH	R120	Panic Alarm Restored
BA	E131	Perimeter Alarm
BH	R131	Perimeter Alarm Restored
BA	E134	Entry/Exit Alarm
BH	R134	Entry/Exit Alarm Restored
TA	E137	Device Tampered
TR	R137	Device Tamper Restored
TA	E383	Detector Tampered
TR	R383	Detector Tamper Restored
TA	E321	Wireless Sounder Tampered
TR	R321	Wireless Sounder Tamper Restored
TA	E334	Wireless Repeater Tampered
TR	R334	Wireless Repeater Tamper Restored
ES	E341	Expander or Wireless Device Tampered
EJ	R341	Expander or Wireless Device Tamper Restored
PA	E120	Keypad/Keyfob Panic Alarm

SIA Code	CID Code	Description
MA	E100	Medical Alarm
MH	R100	Medical Alarm Restored
GA	E151	Gas Leakage Alarm
GH	R151	Gas Leakage Alarm Restored
FA	E110	Fire Alarm
FH	R110	Fire Alarm Restored
OP	E401	Disarming
CL	R401	Away Arming
OA	E403	Auto Disarming
CA	R403	Auto Arming
BC	E406	Alarm Clearing
CL	R441	Stay Arming
CD	E455	Auto Arming Failed
BB	E570	Zone Bypassed
BU	R570	Zone Bypass Restored
CT	E452	Late to Disarm
AT	E301	AC Power Loss
AR	R301	AC Power Restored
YT	E302	Low System Battery
YR	R302	Low System Battery Restored
XT	E384	Low Keyfob Battery
XR	R384	Low Keyfob Battery Restored
YM	E311	Battery Fault
YR	R311	Battery Fault Restored
DK	E501	Keypad Locked
DO	R501	Keypad Unlocked
TS	E607	Test Mode Entered
TE	R607	Test Mode Exited
RN	E305	AX PRO Reset

SIA Code	CID Code	Description
UY	E321	Wireless Sounder Disconnected
UJ	R321	Wireless Sounder Connected
UY	E381	Wireless Detector Disconnected
UJ	R381	Wireless Detector Connected
XT	E384	Wireless Detector Low Voltage
XR	R384	Normal Wireless Detector Voltage
ET	E333	Expander or Wireless Device Disconnected
ER	R333	Expander or Wireless Device Connected
UY	E334	Wireless Repeater Disconnected
UJ	R334	Wireless Repeater Connected
NT	E352	Cellular Data Network Disconnected
NR	R352	Cellular Data Network Connected
NT	E352	SIM Card Exception
NR	R352	SIM Card Restored
NT	E352	Network Flow Exceeded
NT	E351	IP Address Conflicted
NR	R351	Normal IP address
NT	E351	Wired Network Exception
NR	R351	Normal Wired Network
NT	E351	Wi-Fi Communication Fault
NR	R351	Wi-Fi Connected
XQ	E344	RF Signal Exception
XH	R344	Normal RF Signal

SIA Code	CID Code	Description
/	E306	Expander Deleted
/	R306	Expander Added
/	E306	Detector Deleted
/	R306	Detector Added
/	E306	Wireless Repeater Deleted
/	R306	Wireless Repeater Added
/	E306	Wireless Sounder Deleted
/	R306	Wireless Sounder Added
BA	E130	Burglary Alarm
BH	R130	Burglary Alarm Restored
XT	E338	Low Wireless Device Battery
XR	R338	Low Wireless Device Battery Restored
LB	E627	Programming Mode Entered
LX	E628	Programming Mode Exited
CI	E454	Arming Failed
/	R250	Patrol
/	E306	Wireless Device Deleted
/	R306	Wireless Device Added
XT	E384	Low Wireless Sounder Battery
XR	R384	Low Wireless Sounder Battery Restored
NT	E351	Wired Network/Wi-Fi ATP Failed
NR	R351	Wired Network/Wi-Fi ATP Restored
NT	E352	Cellular Network ATP Failed
NR	R352	Cellular Network ATP Restored
CS	1409	Key Zone Disarmed
OS	3409	Key Zone Armed

