AX PRO

User Manual

Legal Information

About this Manual

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

Trademarks

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

Disclaimer

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

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

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

Data Protection

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

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

Symbol Conventions

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

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

Note

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

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 KIWA

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

EU Conformity Statement

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

	Warning 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.
	FCC Information Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: —Reorient or relocate the receiving antenna. —Increase the separation between the equipment and receiver. —Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. —Consult the dealer or an experienced radio/TV technician for help. This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body. FCC Conditions This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: 1. This device may not cause harmful interference. 2. This device must accept any interference received, including interference that may cause undesired operation.

Contents

Chapter 1 Installation Instruction

1.1 Typical Scene

Typical installation location of devices:

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

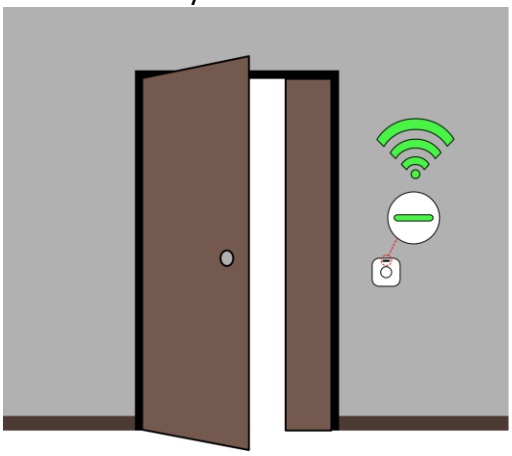
1.2 Precaution

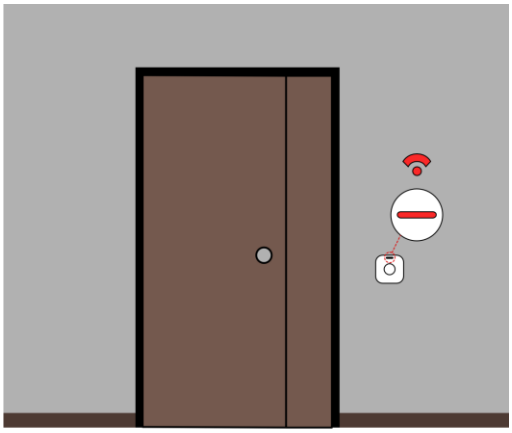
1. Avoid installing the device on metal surfaces.
2. Avoid placing the device directly on the ground.
3. The device is not allowed to be wrapped in metal.
4. Avoid obstructions within 50 cm around the device, except for the installation surface.
5. The repeater needs to be installed between the control panel and the peripheral.
6. Check the signal strength before installation and it is recommended to install the device at the green indicator location. (Do not wrap the detector with your hands when checking the signal strength.)
7. Vertical installation is recommended for devices.

1.3 Installation FAQ

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

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





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

Answer:
- Adjust the position of the control panel and check whether the signal strength is suitable for installation.
- Install a repeater between the offline peripheral and the control panel.
- Check whether to install devices according to the precautions.

Chapter 2 Introduction

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. The system is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- Innovative Tri-X 2-way wireless technology.
- Two-way communication with AES-128 encryption.
- Frequency-hopping spread spectrum (FHSS) is used to avoid interference, to prevent eavesdropping, and to enable code-division multiple access (CDMA) communications.
- Voice guide for alarm alert, system status indication, operation prompt, etc.
- Configuration via web client, mobile client, and Convergence Cloud.
- Pushes alarm notification via messages or phone calls.
- Views life videos from Hik-Connect and alarm video clips via emails, Hik-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.

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

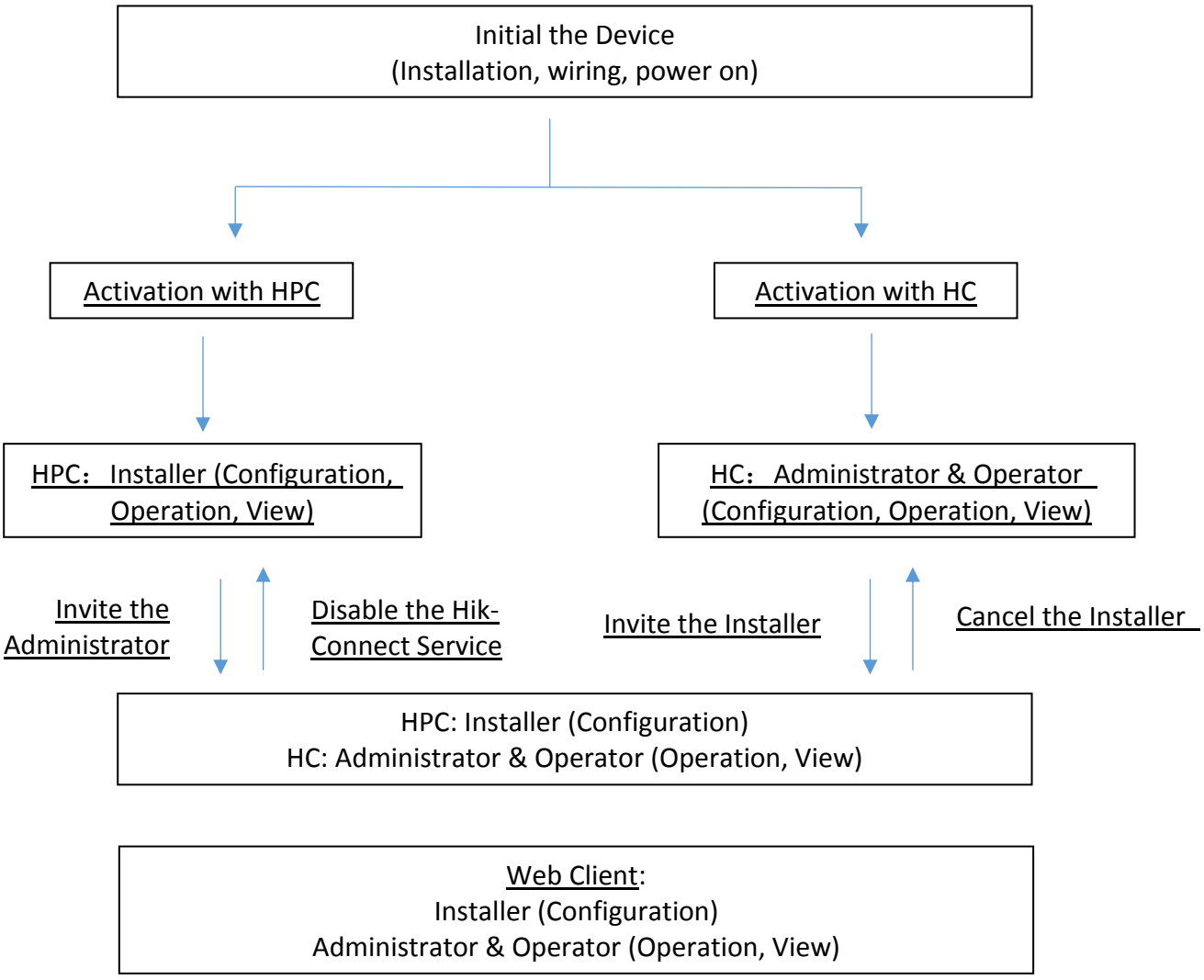
The AX PRO is suitable for the below notification requirements along with the required sounders

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

Chapter 3 Start Up

3.1 Authority Management

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



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

3.2 Activation

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

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

Step1 Create a site (Only for HPC)
Download 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.

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

Note

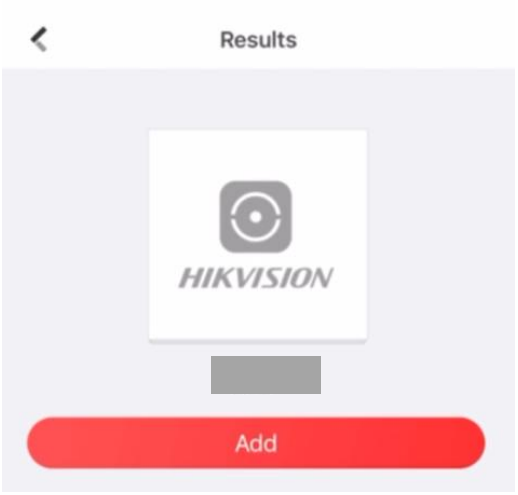
- While the device is powered on, the power LED turn green.
- Once the device connected to the network, the LED indicator turns green.
- Make sure the SIM card you insert can connect to the network.

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

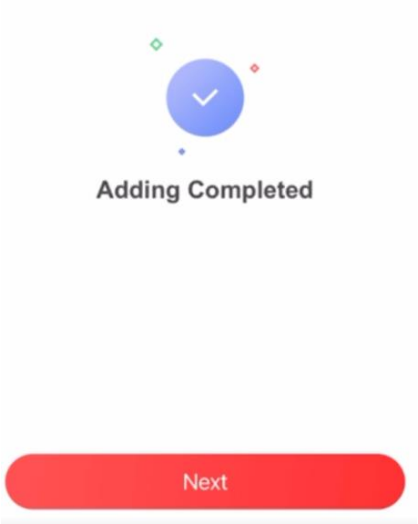
Note

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

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



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



The control panel will be added to the site (HPC) 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/Hik-Connect Service and local web client can be logged in with the Hik-ProConnect/Hik-Connect installer account.

Note

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

3.2.2 Activation with Wi-Fi

Step1 Create a site (Only for HPC)

Download 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.

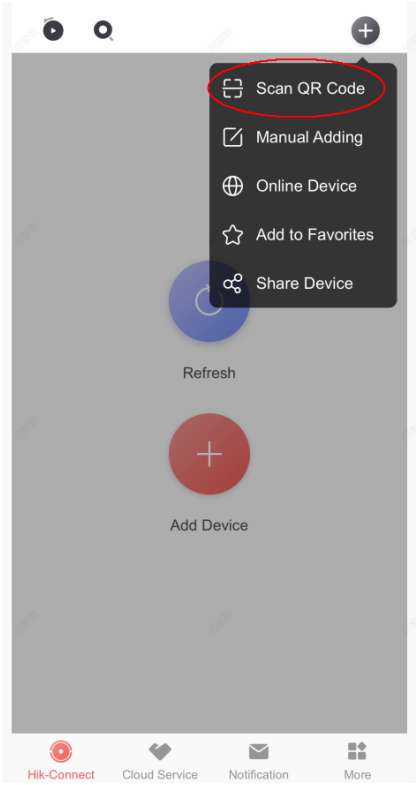
Step2 Configure the Network on APP

1. Download Hik-Connect/Hik-ProConnect and log in.

2. Power on the AX PRO.

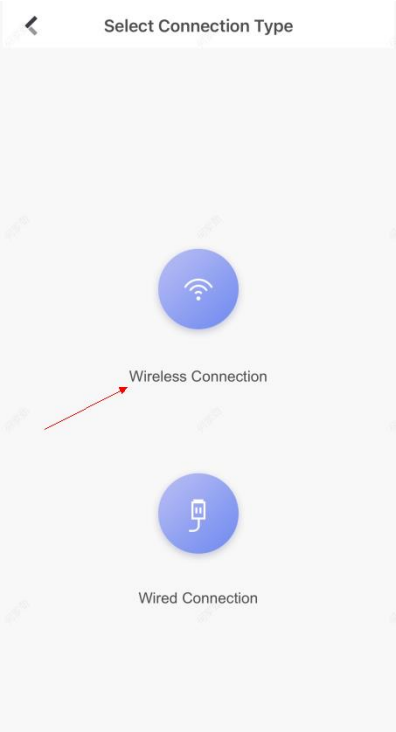
3. Connect your phone to your home Wi-Fi. Make sure that this Wi-Fi can access the Internet normally and the signal is stable.

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



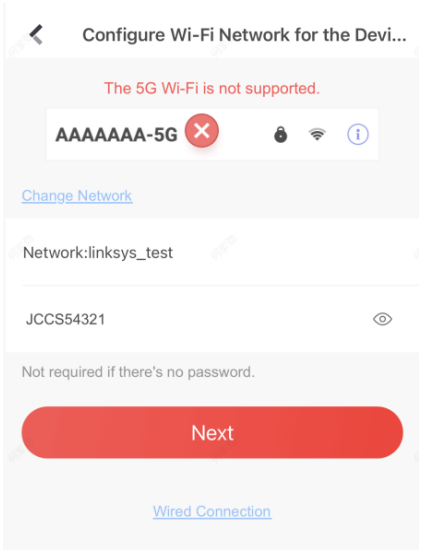
5. Scan the QR code on the back of the control panel and wait for the result.

6. Tap **Next**.
7. Tap **Wireless Connection**.



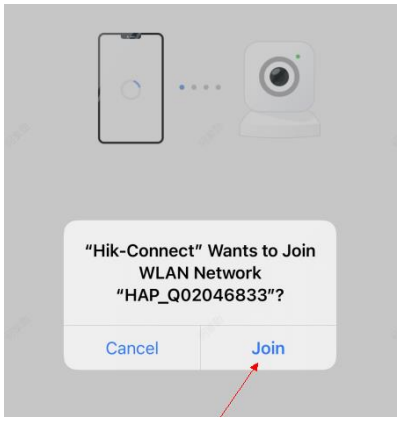
8. Check **The device is started**. And then tap **Next**.

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

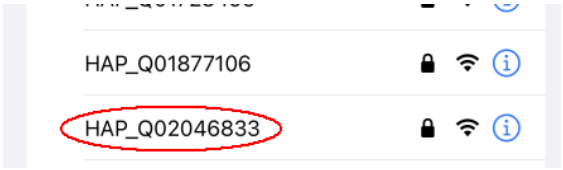


10. Tap **Connect to a Network**.

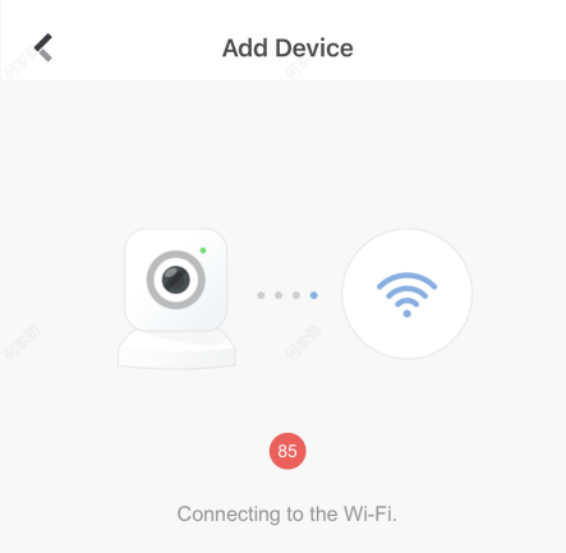
11. Tap **Join**. The mobile phone will disconnect the home Wi-Fi. After interacting information with the control panel, the mobile phone will automatically switch back to the home Wi-Fi.



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

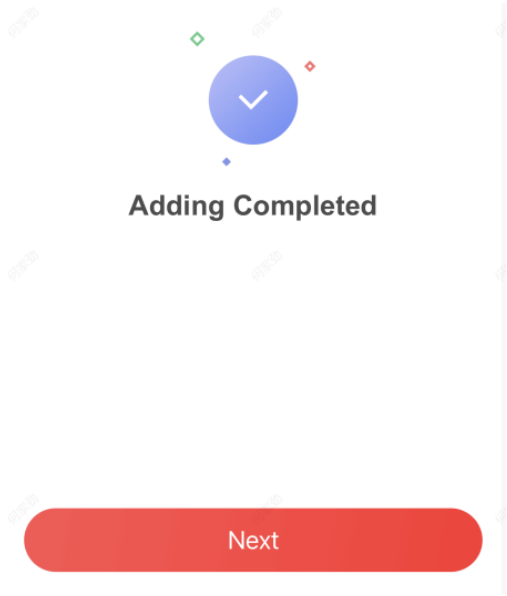


12. After the control panel broadcasts the "Exit hotspot mode", the following page will appear.

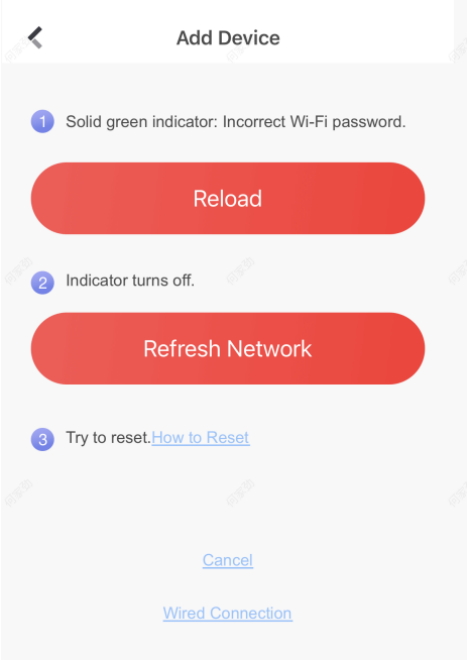


13. Wait for the device to join the home WiFi and log in the EZVIZ Cloud.

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

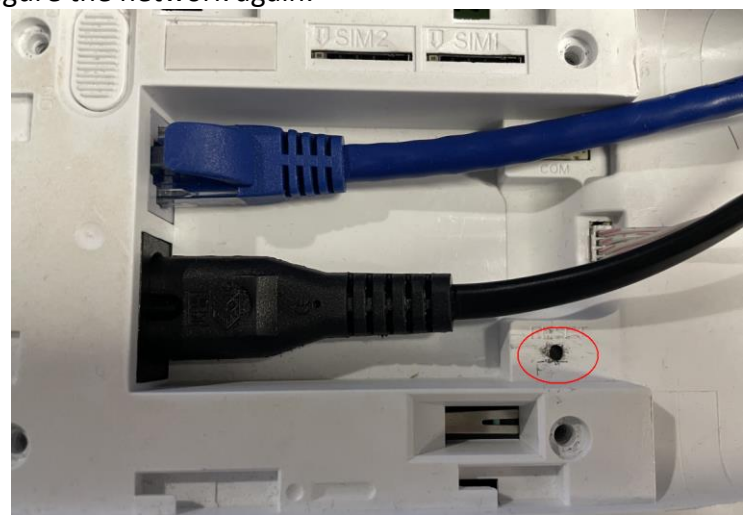


(2) When the home Wi-Fi signal is unstable, the control panel may not be connected to the EZVIZ Cloud before the countdown ends, and the following page will appear:



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

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



Note

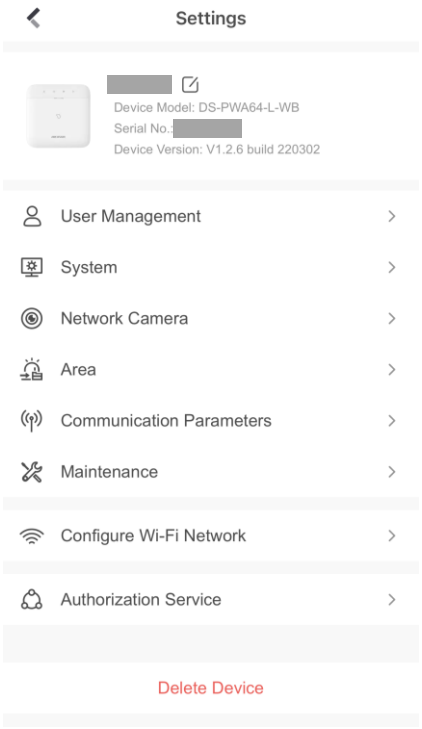
Once the device connected to the network, the LED indicator turns green.

3.3 Unbind the Device

3.3.1 Unbind the Device from Your Own Account

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

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

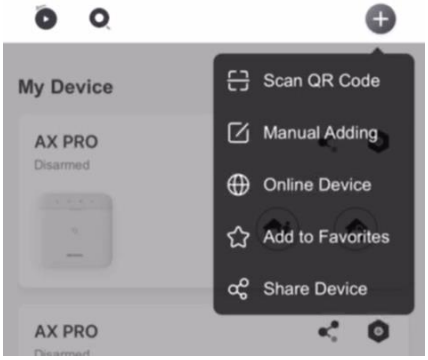


3.3.2 Unbind the Device from Another Account

Make sure the control panel is in your hands.

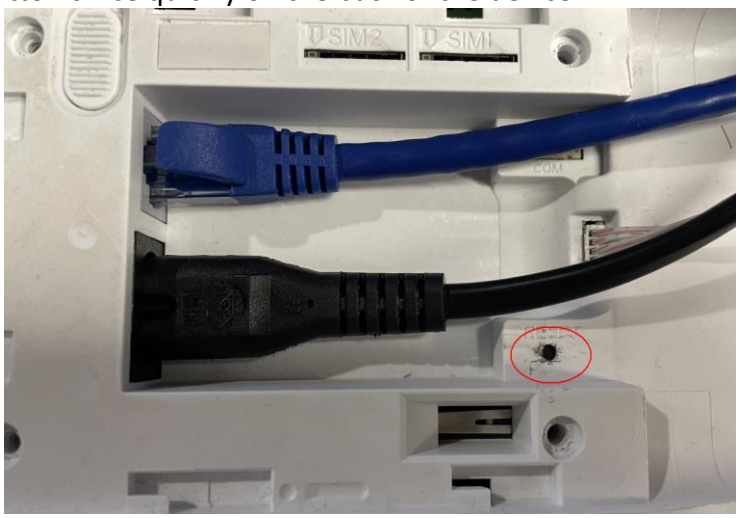
The phone and device are on the same network segment.

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

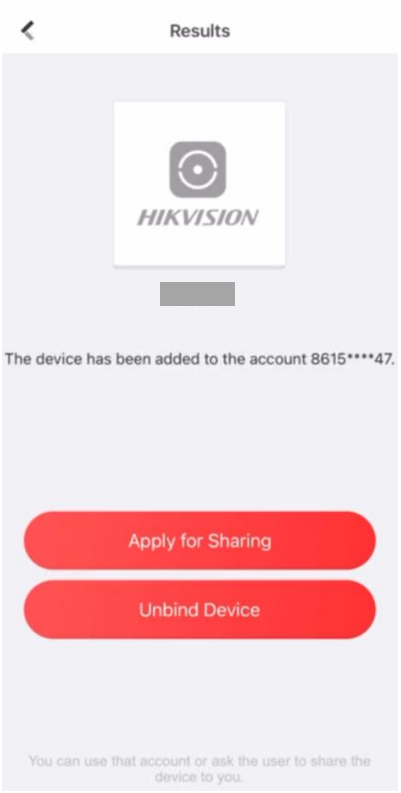


3. Scan the QR code on the label of the device.

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



5. Tap **Unbind Device**.



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

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

Chapter 4 User Management

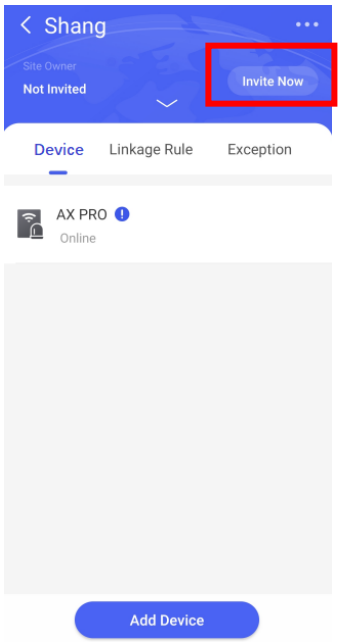
4.1 User Management

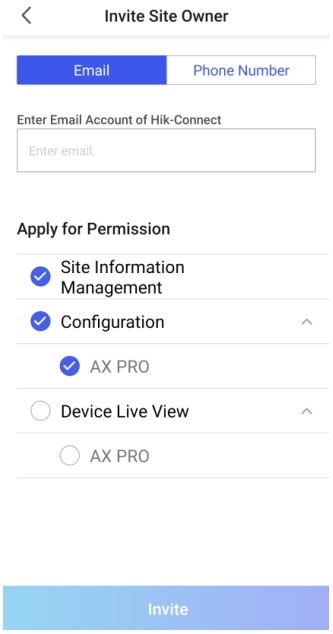
Note

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

4.1.1 Invite the Administrator

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.

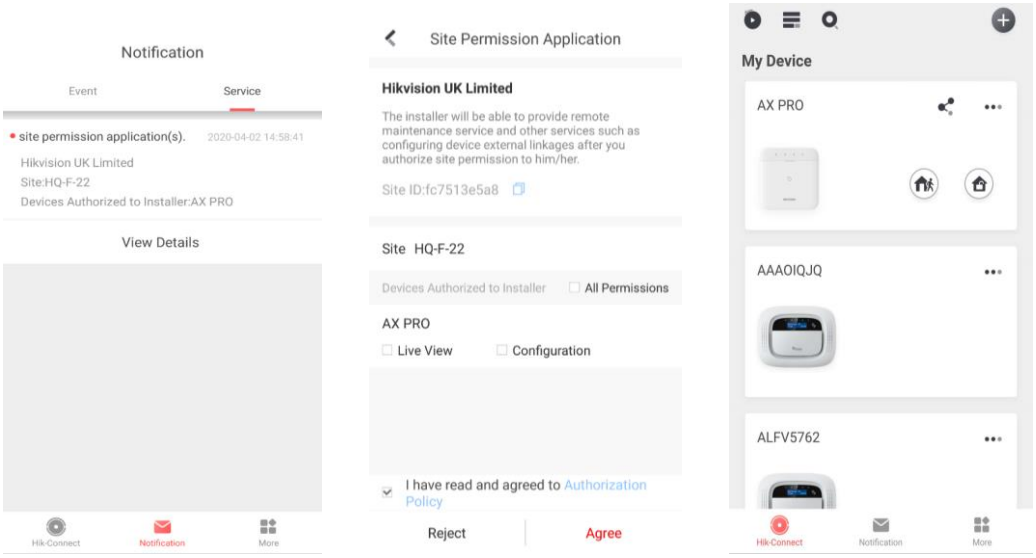
1. Press "**Invite Now**" Button and enter the email account or phone number account to transfer the site ownership to the administrator. At the same time, the installer will apply permissions from the site owner, such as configuration and management.
2. **Optional**: Check **Allow Me to Disable Hik-Connect Service**.

Note

- If the check-box is checked, after you hand over the Site to your customer and your customer approves the request, you can disable Hik-Connect service for devices that you rent to your customer without her/his authorization If Hik-Connect service is disabled, your customer cannot operate on these devices via the Hik-Connect Mobile Client.

3. 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.

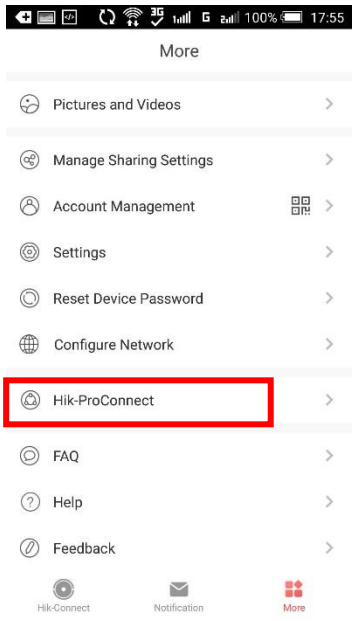
The administrator account will be added to the control panel, which could be used to login to Hik-Connect app and local web client.

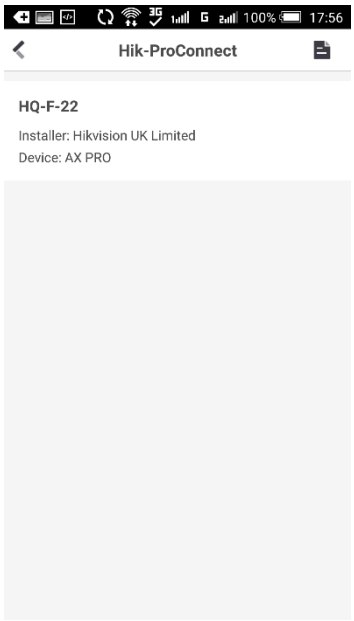


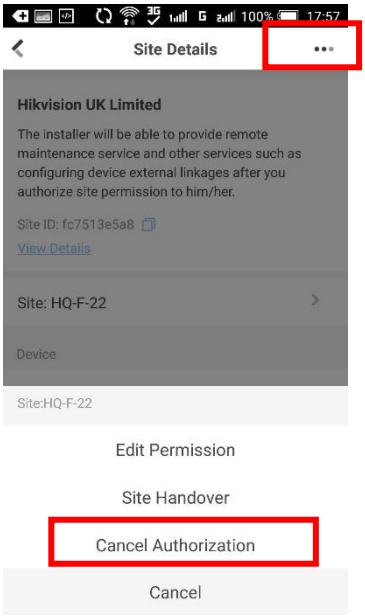
4.1.2 Cancel Installer Access

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.

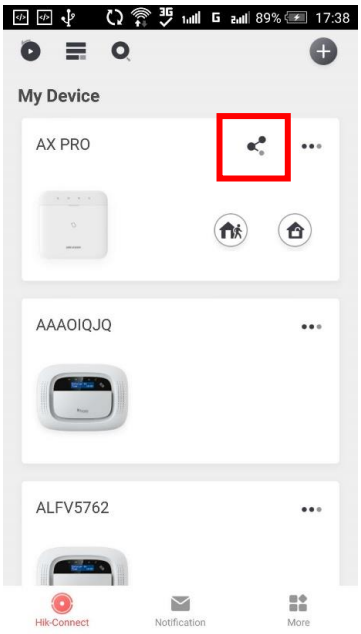


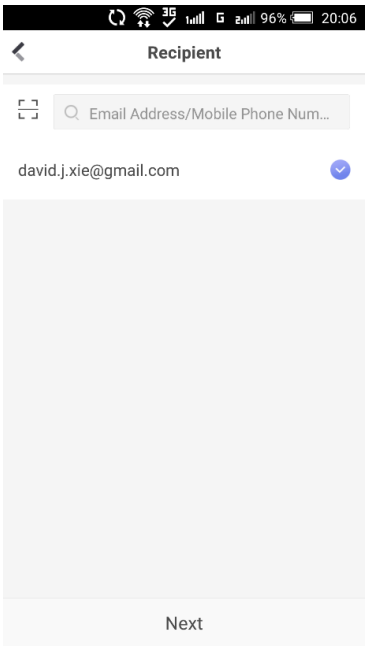


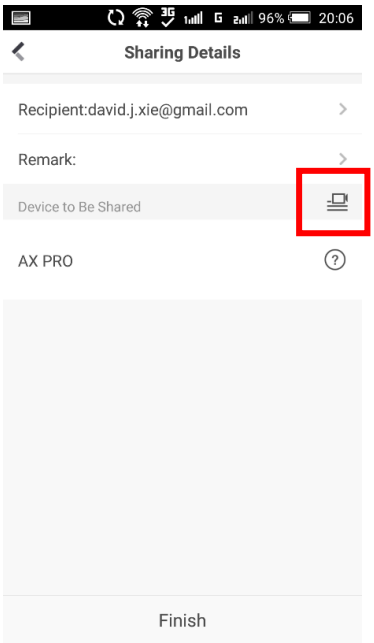


4.1.3 Add an Operator

The administrator can share the device to other operators.

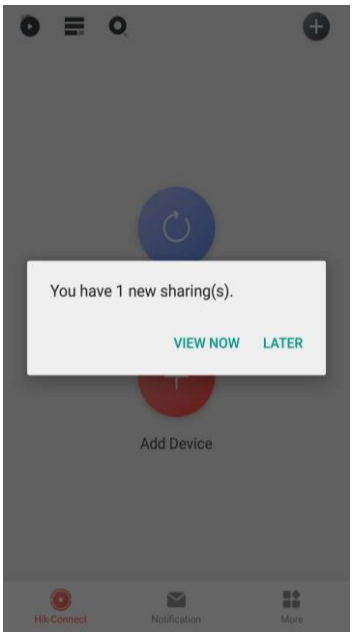


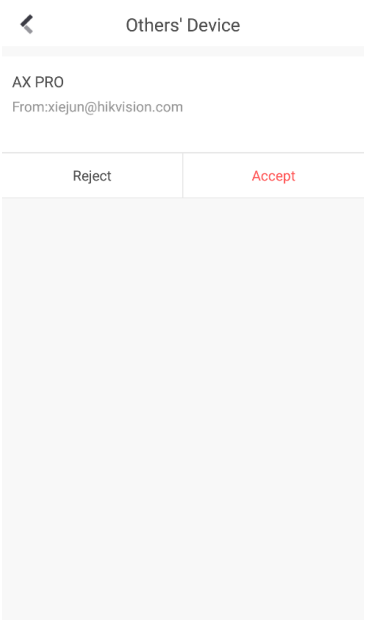


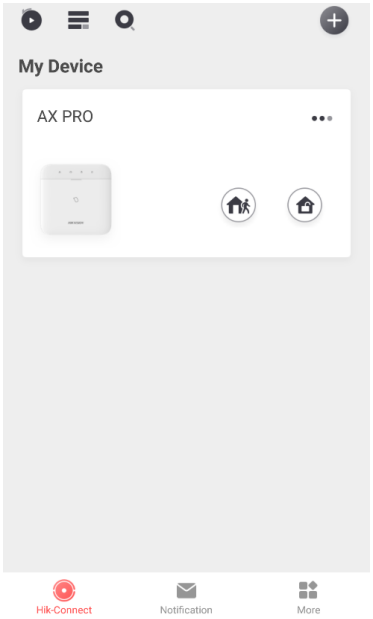


1. Tap the (share button) in the device list.
2. Enter the Hik-Connect account of the operator.

   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.

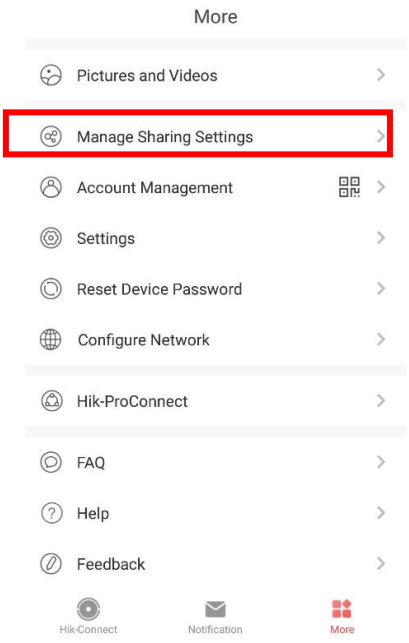
3. Accept the invitation, and the device will be listed in the device list.

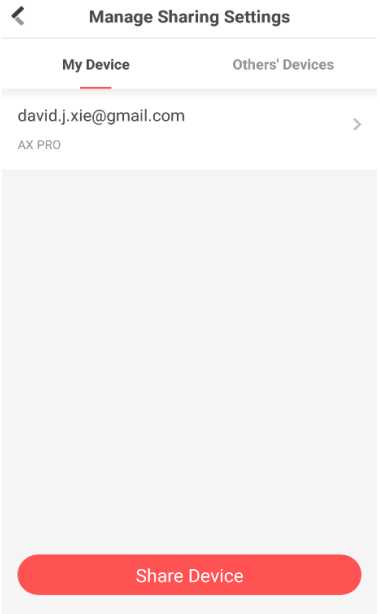
The operator account will be added to the control panel, which could be used to login to Hik-Connect app and local web client.

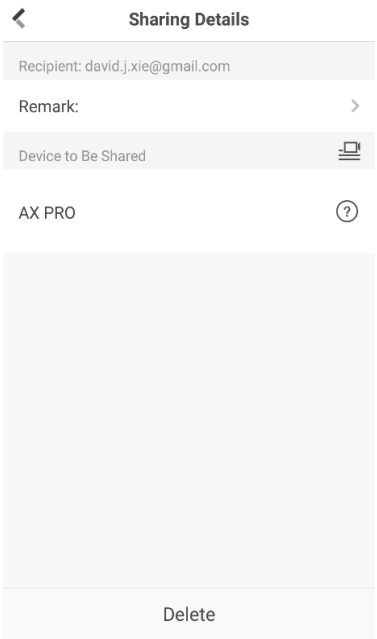
4.1.4 Delete an Operator

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.







4.1.5 Disable the Hik-Connect Service

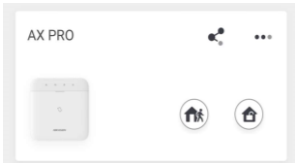
Note

- The site must be a rental site.
- The installer on the HPC side needs to check **Allow Me to Disable Hik-Connect Service** when inviting the administrator and the administrator on the HC side also accepts this option.

You can go to the **Device** tab to disable Hik-Connect service for one device or all devices in this Site by tapping or setting Hik-Connect Service switch to off. You can also delete the devices from the your customer's Hik-Connect account without her/his authorization.

4.1.6 Invite the Installer

1. In HC, tap in the device list



2. Tap **Share with Installer** and enter the email address.
3. Tap **OK**.
4. Tap → **Share with Installer** → **Share QR Code**
5. In HPC, select a site and tap **Add Device**.
6. Scan the QR Code.
7. In HC, the user will receive a device authorization application. Go to the application page and tap **Agree**.
8. Go to **Cloud Service** → **Device Authorization** → → **Authorize More Devices**
9. Select devices and permissions.
10. Tap **OK** and the devices will be authorized to the Installer and added to the Site.

4.2 Access Entries

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

different user roles with particular access level.

Access entries for Installers (Access Level 3)

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

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

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

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

Chapter 5 Configuration

5.1 Set-up with Hik-Proconnect

5.1.1 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

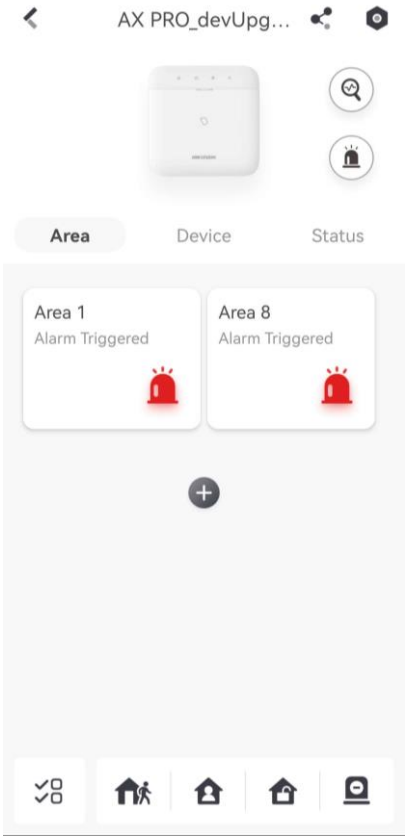
Add peripheral to the AX PRO.

Steps

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

Main Page

You can view faults, arm and disarm areas, view device status, etc.
On the device list page, tap the AX PRO and then log in to the device (if required) to enter the page.



Enable Alarm

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

View Faults

Tap to view faults.

Area Management

Tap **+** to add an area.

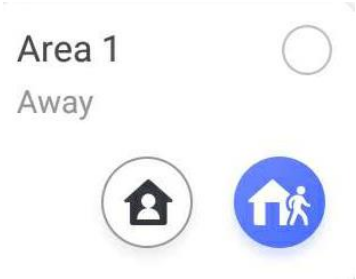
Tap Area to enter the area management page. Refers to ***Set Arming/Disarming Schedule*** for details.

Arm/Disarm the Area

Arm or disarm the area manually as you desired.

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

Operations for a Single Area



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

Operations for Multiple Areas

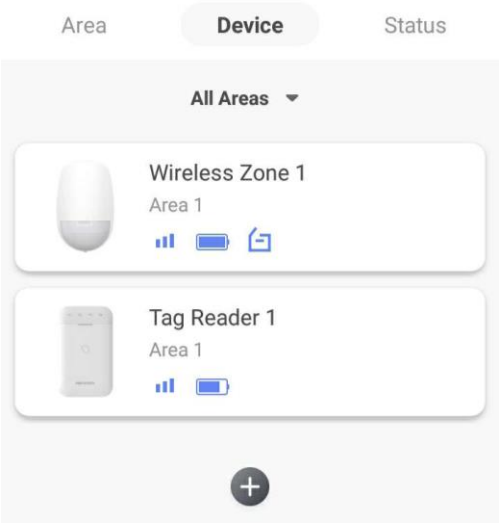
- **Select Areas**: Tap to select areas you want to operate. If you do not select areas, following operations will take effect for all areas.
- **Away Arming**: Tap to away arm selected areas. When all the people in the detection area leave, turn on the Away mode to arm all zones in all areas after the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

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

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

Zone Management

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



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

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

- 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.

Follow Zone

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

Note

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

Disabled Zone

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

24-Hour Zone

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

Timeout Zone

The zone activates all the time. The zone type is used to monitor and report the "ACTIVE" status of a zone, but it will only report and alarm this status after the programmed time has expired. (1 to 599) Seconds. It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

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.

Arm Mode

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

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

PD6662 is not enabled: You need to set the combined time interval.
When the first zone is triggered, the system will start timing after the zone is restored. If the second zone is triggered within the set time, both zones will give alarms. Otherwise, no alarm will be triggered.

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

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

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

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

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

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

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

Double knock

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

Sounder Delay Time

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

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 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.
Change Keypad Password	If the target user is an administrator, an installer, or an operator, you can tap the target user on the user list and then tap **Change Keypad Password** to set the keypad password to the target user.
Change Duress Password	If the target user is an administrator or an operator, you can tap the target user on the user list and then tap **Change Duress Password** to set the duress password to the target user. **Note** If under duress, you can enter the duress code on the 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 Card/Tag 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.
5. Optional: Tap a Tag to enter the Setting Page.
6. 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.

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

Note

Different linked users have different Tag permissions.

Operation Tag

You can swipe the Tag to arm or disarm.

Patrol Tag

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

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

Device Information

You can change language and select time zone.

Steps

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

4. Enable DST according to your needs.

DST

Daylight saving time (also called summer time) is the practice of advancing clocks during the lighter months so that evenings have more daylight and mornings have less.

System Management

Steps

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

Forced Auto Arm

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

Note

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

Forced Arming

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

System Status report

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

Voice Prompt

If the option is enabled, the AX PRO will enable the text voice prompt.
You can set detailed prompt: **Fault Prompt On Arming, Fault Prompt On Disarming, Fault Prompt When Armed, Fault Prompt When Disarmed, Voice Prompt On Alarm.**

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.

Alarm Duration

The time duration of the panel alarm.

Wireless Supervision Loss

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

Bypass on Re-Arm

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

Jamming Sensitivity Settings

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

Fault LED Stay On When Armed

When system is armed, the fault indicator is always on.

Arm LED Stay On

The arm LED is always on.

Hik-Connect Indicator

Enable the Hik-Connect indicator.

Motion Detector Restore

Motion detectors include all PIR detectors.

Power Save Mode

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

PD6662

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

Fault Check

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

Steps

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

Panel Battery Fault Check

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

LAN Fault Check

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

Wi-Fi Fault Check

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

Cellular Network Fault Check

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

Main Power Lost

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

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.

Steps

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

You can set the following parameters:

Arm with Fault

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

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.

3. Tap **Save**.

Enrollment Mode

Steps

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

2. Tap → **System** → **System Options** → **Enrollment Mode** to enter the page.
3. Tap **Enter the Enrollment Mode**. You can enroll the peripheral by triggering it.

Network Camera

Add Cameras to the AX PRO

Steps

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

Set Video Parameters

Steps

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

Stream Type

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

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Bitrate

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

Set Arming/Disarming Schedule

Steps

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

2. Tap → Area to enter the page.
3. Tap an area in the list, enable the area and select linked areas.
4. 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.

Note

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**.

Auto Arm Sound Prompt

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

Weekend Exception

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

Holiday Excepted

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.

Communication

Wired Network

Steps

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

Cellular Data Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Cellular Data Network Settings** to enter the page.
3. Enable **Cellular Data Network**.
4. Tap to select a SIM card. Tap **Parameter Configuration** → **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**.

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.

Push Notifications

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

Steps

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

Zone Alarm/Lid Opened

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.

Fire 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 operates the AX PRO.

Smart Alarm Event

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

5. Tap **Phone Call and SMS**.
6. Tap **+ Add Phone Number** to enter the phone number.
7. Tap the added phone number to enable **Phone Call** and **SMS** according to your need.
8. (For Phone Call) Set **Numbers of Calling**.
9. (For SMS) Set **Arming Permission**, **Disarming Permissio**n and **Alarm Clearing Permission** for areas.

General Hint

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

You can import **Common Voice.** When the alarm is triggered, your customized voice will be added at the beginning of the content of the phone dialed by the system.

Note

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

10. Check notifications.

Alarm Receiving Center (ARC)

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

Steps

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

Protocol Type

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

Companies

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

Address Type

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

port number and account code.

Transmission Mode

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

Retry Timeout Period

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

Attempts

Set the number of retry attempts.

Polling Option

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

Periodic Test

Enter the periodic test interval.

GMT

Enable the Greenwich Mean Time.

Cloud Service Settings

Steps

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

Auto

The 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.

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

5. Tap **Save**.

Notification by Email

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Notification by Emails** to enter the page.
3. Enable **Email**.
4. Enter the sender name, sender email address, SMTP server address, SMTP port, user name and password.
5. Select the encryption type as **None**, **SSL** or **TLS**.
6. Enable **Server Authentication**.
7. Enter receiver name and receiver email address. Tap **Test Receiver Email Address** to test whether the email address is correct.
8. Tap **Save**.

FTP Settings

Steps

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

FTP Type

Set the FTP type as preferred or alternated.

Protocol Type

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

Server Address and Port

The FTP server address and corresponding port.

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. Tap **Save**.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among

networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

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

Steps

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

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

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

Steps

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

   SIP

   The control panel will use ARC and SIP server.

   IP Receiver Pro

   The control panel will user cloud service.
4. Select a sounder and tap **Save**.

Device Maintenance

You can reboot the device.

Steps

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

5.1.2 Use 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.

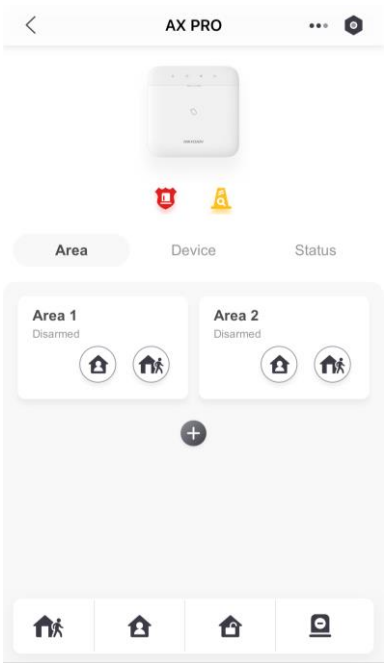
Click **Site** to enter the site list page, and then click the name of a site to enter site details page.

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.

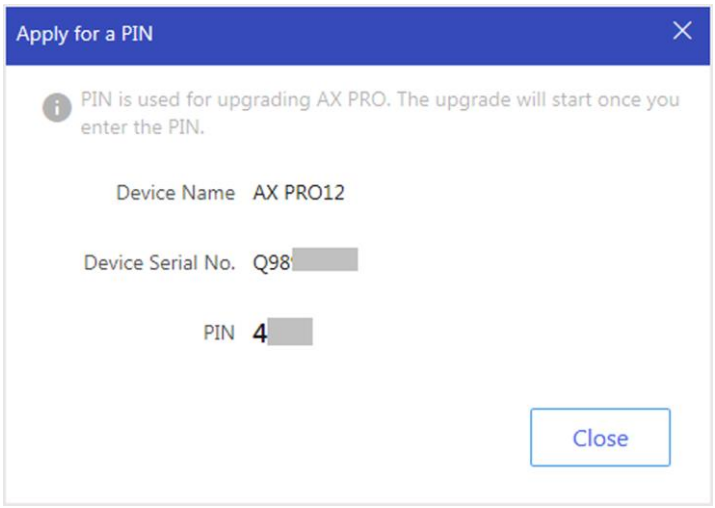
Note

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.

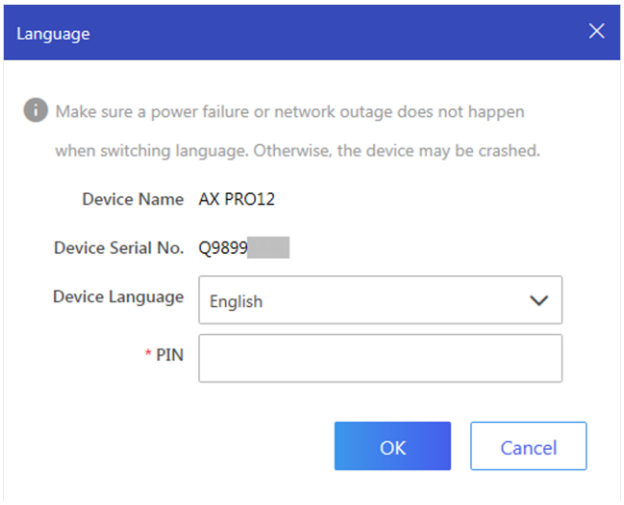


Switch Language

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.

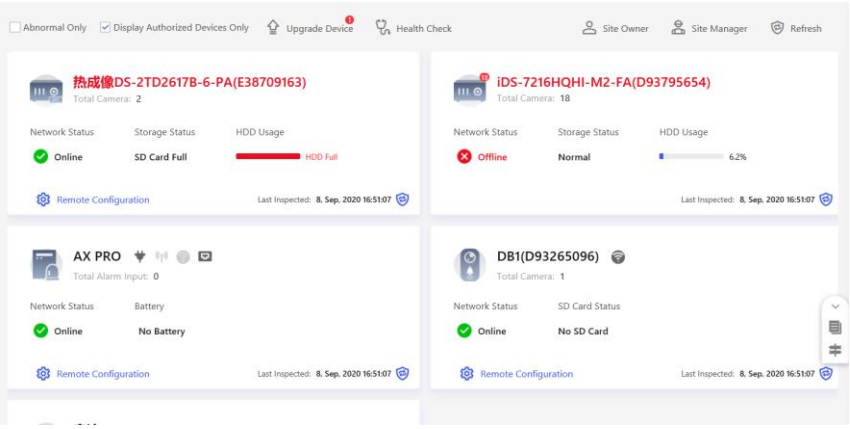


Health Monitoring

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

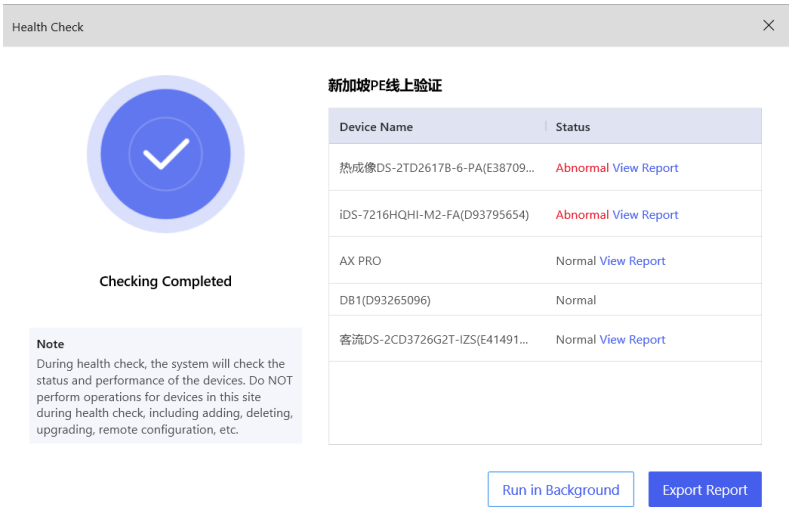
the page.

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.

5.2 Set-up with Hik-Connect

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

Download and Login the Mobile Client

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

Steps

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

Note

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

3. Run and login the client.

Add AX PRO to the Mobile Client

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

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.

Note

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

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

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

Add Peripheral to the AX PRO

Add peripheral to the AX PRO.

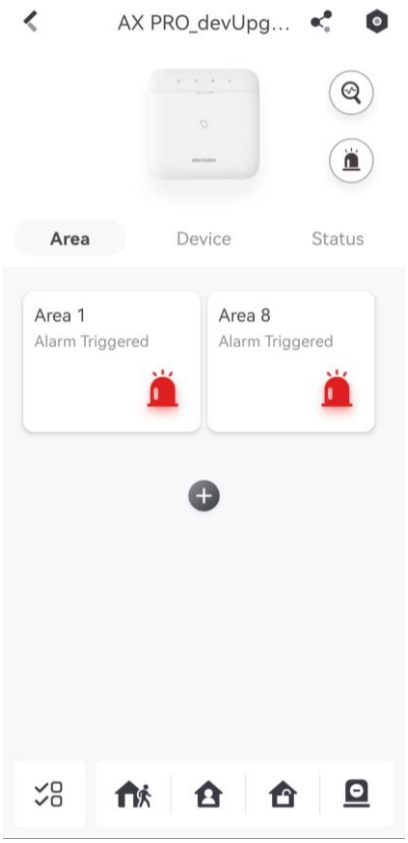
Steps

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

Main Page

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

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



Enable Alarm

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

View Faults

Tap to view faults.

Area Management

Tap **+** to add an area.

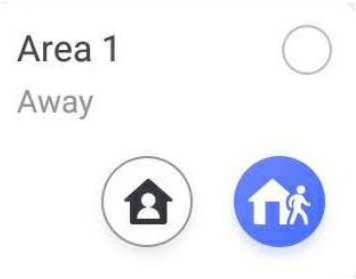
Tap Area to enter the area management page. Refers to ***Set Arming/Disarming Schedule*** for details.

Arm/Disarm the Area

Arm or disarm the area manually as you desired.

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

Operations for a Single Area



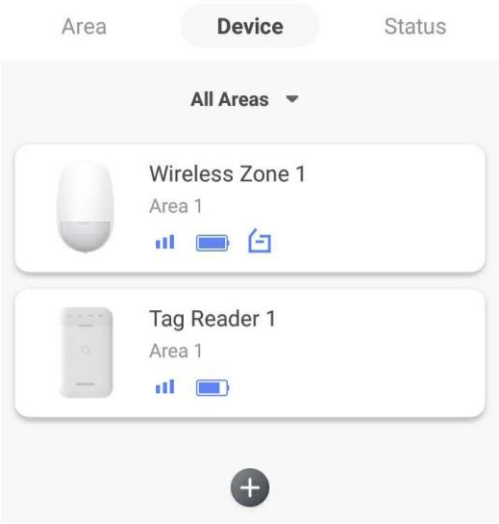
- **Away Arming**: Tap to away arm a single area. When all the people in the detection area leave, turn on the Away mode to arm all zones in the area after the defined dwell time.
- **Stay Arming:** Tap to stay arm a single area. When all the people stays inside the detection area, turn on the Stay mode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

Operations for Multiple Areas

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

Zone Management

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



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

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

- 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.

Follow Zone

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

Note

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

Disabled Zone

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

24-Hour Zone

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

Timeout Zone

The zone activates all the time. The zone type is used to monitor and report the "ACTIVE" status of a zone, but it will only report and alarm this status after the programmed time has expired. (1 to 599) Seconds. It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

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.

Arm Mode

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

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

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

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

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

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

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

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

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

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

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

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

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

Double knock

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

Sounder Delay Time

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

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

View Status

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

Bypass Zone

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

Before You Start

Link a detector to the zone.

Steps

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

Bypass Status

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

User Management

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

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

Steps

Note

There are 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 Information Page.
7. Optional: Perform the following operations if required.

User Permission	You can tap the target user on the user list and then tap to set the permissions authorized to the target user. **Note** Only the administrator can do such an operation.
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.
Change Keypad Password	If the target user is an administrator, an installer or an operator, you can tap the target user on the user list and then tap **Change Keypad Password** to set the keypad password to the target user.

Note

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

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

Note

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

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 Card/Tag and Wireless Keyfob of the user but you do not have permission to configure them.

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

Card/Tag Management

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

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.

Device Information

You can change language and select time zone.

Steps

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

DST

Daylight saving time (also called summer time) is the practice of advancing clocks during the lighter months so that evenings have more daylight and mornings have less.

System Management

Steps

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

Forced Auto Arm

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

Note

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

Forced Arming

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

System Status report

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

Voice Prompt

If the option is enabled, the AX PRO will enable the text voice prompt.
You can set detailed prompt: **Fault Prompt On Arming, Fault Prompt On Disarming, Fault Prompt When Armed, Fault Prompt When Disarmed, Voice Prompt On Alarm.**

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(lid opened alarm).

Alarm Duration

The time duration of the panel alarm.

Wireless Supervision Loss

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

Bypass on Re-Arm

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

Jamming Sensitivity Settings

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

Fault LED Stay On When Armed

When system is armed, the fault indicator is always on.

Arm LED Stay On

The arm LED is always on.

Hik-Connect Indicator

Enable the Hik-Connect indicator.

Motion Detector Restore

Motion detectors include all PIR detectors.

Power Save Mode

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

PD6662

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

Fault Check

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

Steps

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

Panel Battery Fault Check

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

LAN Fault Check

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

Wi-Fi Fault Check

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

Cellular Network Fault Check

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

alarm will be triggered.

Main Power Lost

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

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.

Steps

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

You can set the following parameters:

Arm with Fault

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

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.

3. Tap **Save**.

Enrollment Mode

Steps

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

Network Camera

Add, edit and delete network camera channels.

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 →**Network Camera** → **Network Camera Channel** to enter the page.
3. Tap **+ Add Channel**, and enter IP address, user name, password to add the channel.
4. Tap the Camera. You can view its parameters or tap **Delete** to delete it.
5. Tap to edit parameters.

Set Video Parameters

Steps

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

Stream Type

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

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Bitrate

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

Before Alarm

The recording time length before the alarm.

After Alarm

The recording time length after the alarm.

Set Arming/Disarming Schedule

Steps

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

4. 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.

Note

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**.

Auto Arm Sound Prompt

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

Weekend Exception

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

Holiday Excepted

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.

Communication

Wired Network

Steps

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

Cellular Data Network

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Cellular Data Network Settings** to enter the page.
3. Enable **Cellular Data Network**.
4. Tap to select a SIM card. Tap **Parameter Configuration** → **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**.

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.

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. Select an ARC or the APP.
4. Enable the target notification.

Zone Alarm/Lid Opened

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.

Fire 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 operates the AX PRO.

Smart Alarm Event

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

5. Tap **Phone Call and SMS**.
6. Tap **+ Add Phone Number** to enter the phone number.
7. Tap the added phone number to enable **Phone Call** and **SMS** according to your need.
8. (For Phone Call) Set **Numbers of Calling**.
9. (For SMS) Set **Arming Permission**, **Disarming Permissio**n and **Alarm Clearing Permission** for areas.

General Hint

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

Note

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

10. Check notifications.

Alarm Receiving Center (ARC)

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

Steps

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

Protocol Type

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

Companies

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

Address Type

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

port number and account code.

Transmission Mode

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

Retry Timeout Period

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

Attempts

Set the number of retry attempts.

Polling Option

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

Periodic Test

Enter the periodic test interval.

GMT

Enable the Greenwich Mean Time.

Cloud Service Settings

Steps

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

Auto

The 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.

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

5. Tap **Save**.

Notification by Email

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap → **Communication Parameters**→ **Notification by Emails** to enter the page.
3. Enable **Email**.
4. Enter the sender name, sender email address, SMTP server address, SMTP port, user name and password.
5. Select the encryption type as **None**, **SSL** or **TLS**.
6. Enable **Server Authentication**.
7. Enter receiver name and receiver email address. Tap **Test Receiver Email Address** to test whether the email address is correct.
8. Tap **Save**.

FTP Settings

Steps

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

FTP Type

Set the FTP type as preferred or alternated.

Protocol Type

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

Server Address and Port

The FTP server address and corresponding port.

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. Tap **Save**.

NAT

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among

networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

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

Steps

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

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

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

Steps

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

   SIP

   The control panel will use ARC and SIP server.

   IP Receiver Pro

   The control panel will user cloud service.
4. Select a sounder and tap **Save**.

Device Maintenance

You can reboot the device.

Steps

1. In the site, tap the AX PRO and then log in to the device (if required).
2. Tap →**Maintenance** → **Reboot Device**. to enter the maintenance page.
   The AX PRO will reboot.
3. Tap →**Maintenance** → **Device Upgrade** to check the system version.
   The AX PRO will upgrade to the latest version.
4. Optional: Tap →**Maintenance** → **Remote Log Collection** to enable the function.
   Remote Log Collection is for getting logs relating to the device. When this is enabled, our

technical support will be able to collect logs relating to the device remotely and upload them to our server for troubleshooting. You can set the validity period according to actual needs. This function will be disabled after the set validity period.

Wi-Fi Connection

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

Steps

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

Check Alarm Notification

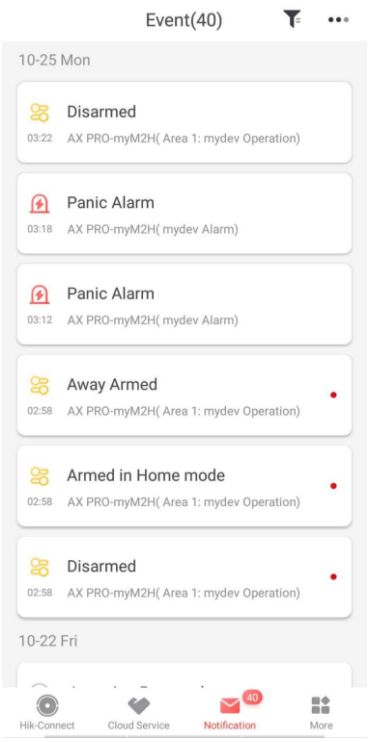
When an alarm is triggered, and you will receive an alarm notification. You can check the alarm information from the mobile client.

Before You Start

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

Steps

1. Tap **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.

5.3 Set-up with the Web Client

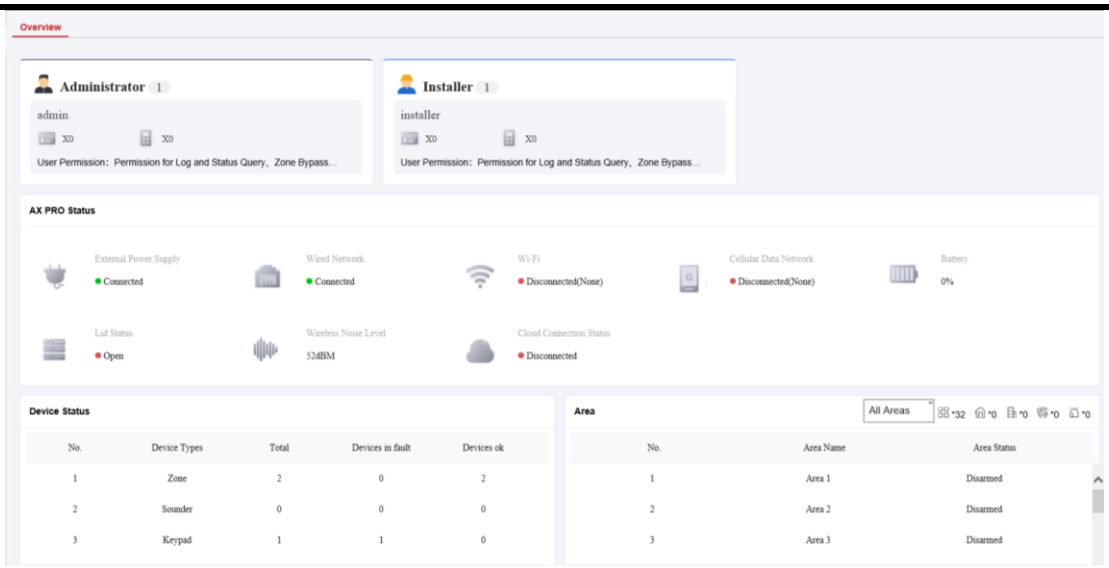
Steps

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

Note

- Only the administrator and the installer can login to the web client.
- The user name and the password are the ones when activating via Hik-Connect or Hik-ProConnect.

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



5.3.1 Communication Settings

Wired Network

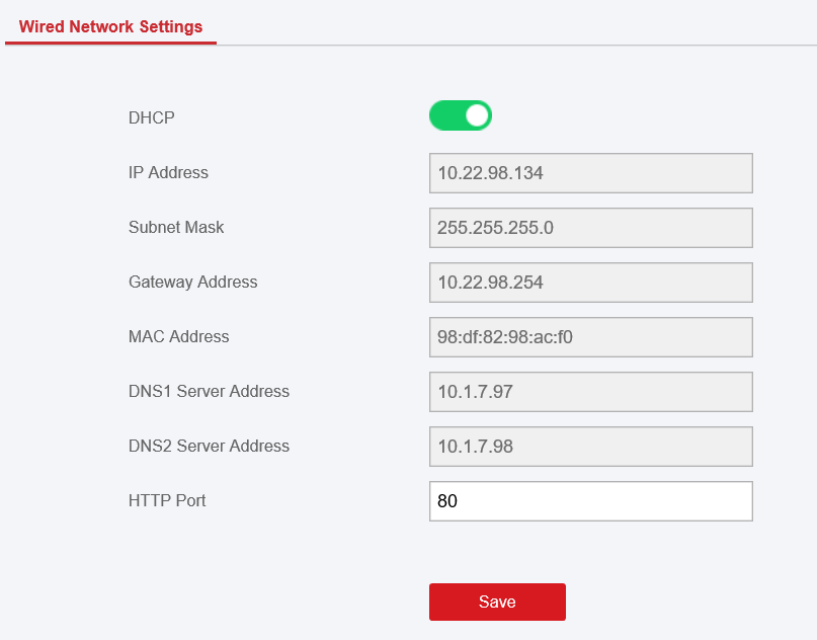
You can set the device IP address and other network parameters.

Steps

Note

Functions varied depending on the model of the device.

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



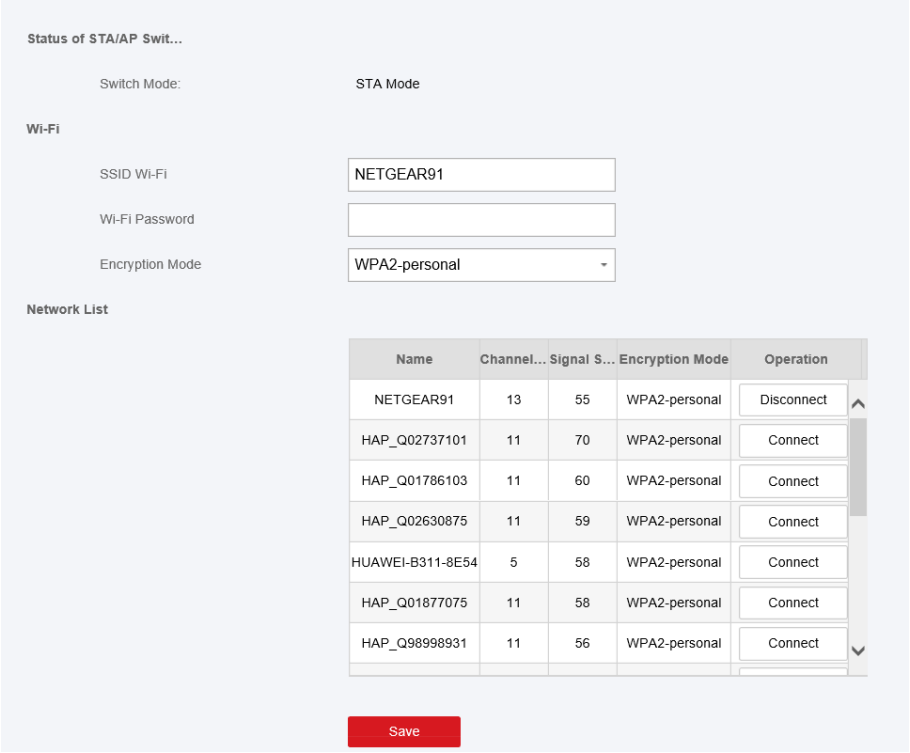
2. Set the parameters.
   - Automatic Settings: Enable **DHCP** and set the HTTP port.
   - Manual Settings: Disabled **DHCP** and set **IP Address**, **Subnet Mask**, **Gateway Address**, **DNS Server Address**.
3. **Optional**: Set correct DNS server address if the device needs to visit Hik-Connect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

Wi-Fi

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

Steps

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

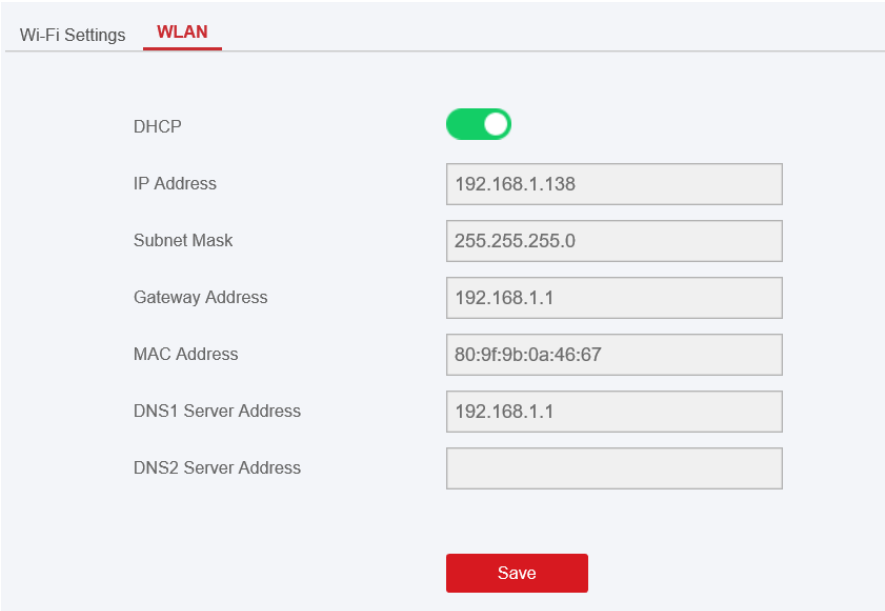


2. Connect to a Wi-Fi.

– 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**.

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



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

Note

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

5. Click **Save**.

Cellular Network

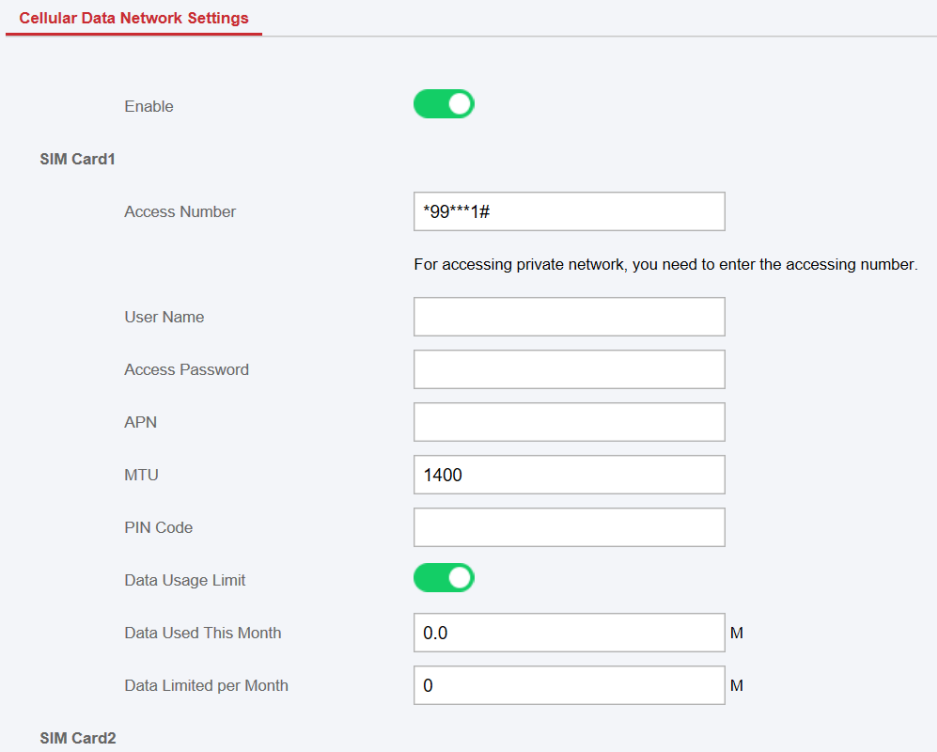
Set the cellular network parameters if you insert a SIM card inside the device. By using the cellular network, the device can upload alarm notifications to the alarm center.

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

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



Note

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

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

Access Number

Input the operator dialing number.

Note

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

User Name

Ask the network carrier and input the user name.

Access Password

Ask the network carrier and input the password.

APN

Ask the network carrier to get the APN information and 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.

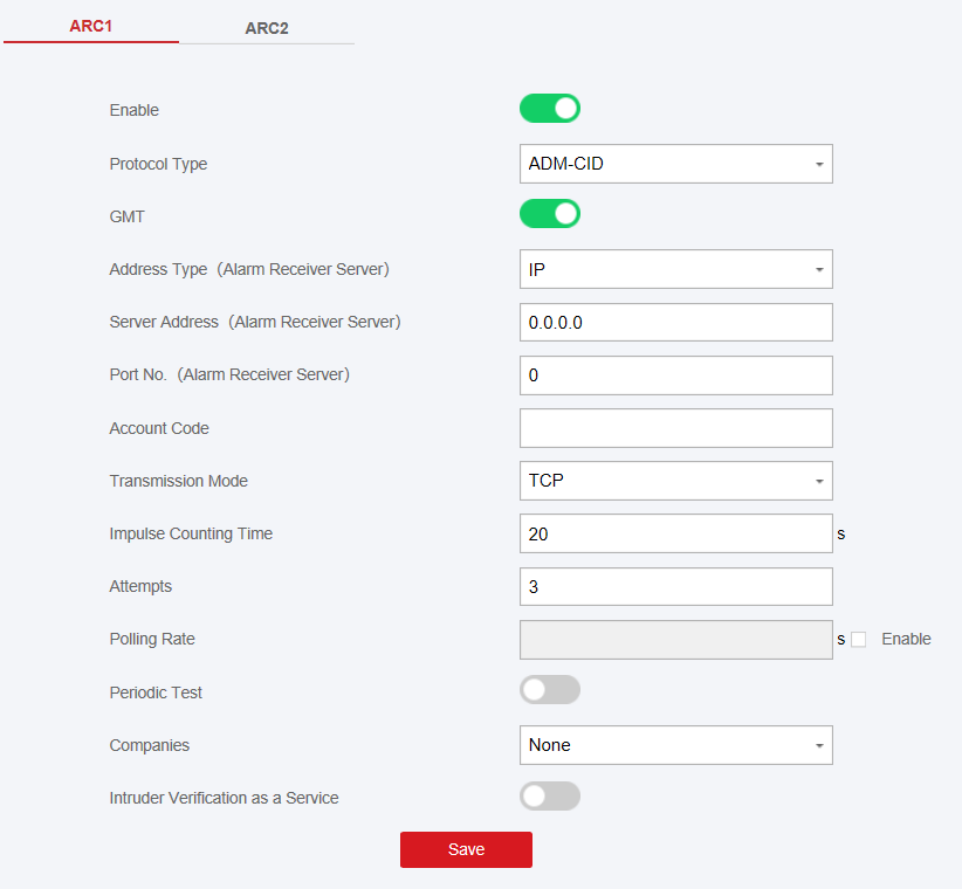
4. Click **Save**.

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** → **Alarm Receiving Center** to enter the Alarm Receiving Center page.



2. Select the **ARC** 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(ARC1) is enabled, you can set the alarm receiver center 2 as the **backup channel** and edit the channel parameters.

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

Note

Standard DC-09 Protocol

ADM-CID: The data presenting method of DC-09 is CID, which is not encrypted and only for uploading alarm report.

*ADM-CID: The data presenting method of DC-09 is CID, which is encrypted and only for uploading alarm report.

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

*SIA-DCS: The data presenting method of DC-09 is DCS (also called SIA protocol), which is encrypted and only for uploading alarm report.

ADM-CID or **SIA-DCS:** You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP address, port number, account code, impulse counting time, attempts, polling rate.

Note

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

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

Note

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

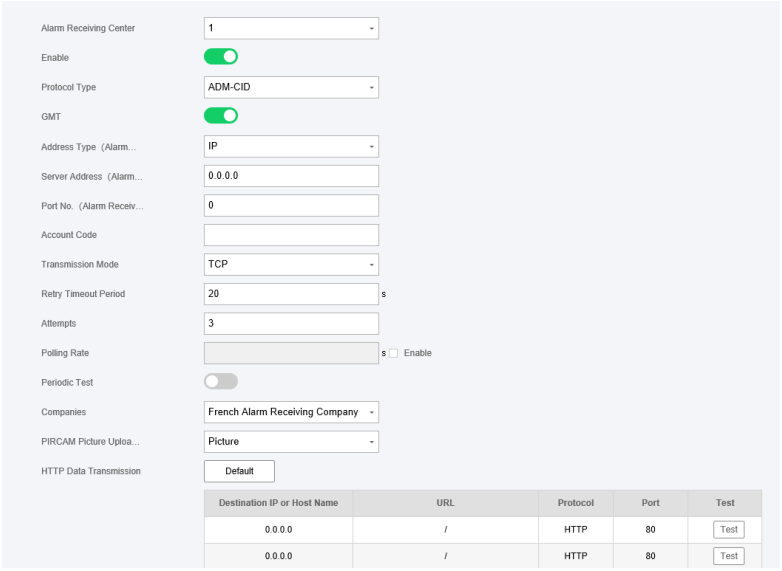
4. Click **Save**.

Use PIRCAM to Upload Pictures or Videos

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

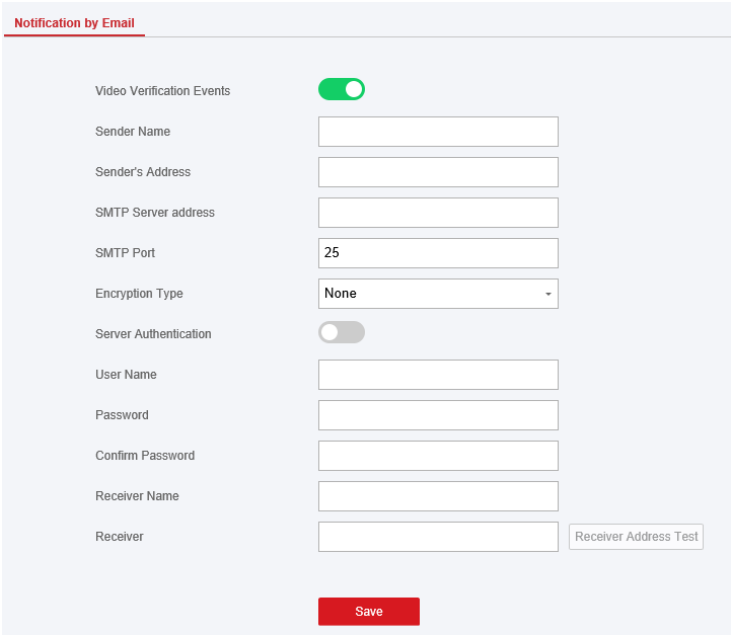
1. Upload Pictures
   You can choose to upload 1 to 20 pictures.

(1) Click **Communication** → **Alarm Receiving Center** to enter the page.
(2) Slide the slider to enable the selected alarm receiver center.
(3) Select the **Protocol Type** as **SIA-DCS**.
(4) Select the **Companies** as **French Alarm Receiving Company**.
(5) Click **Save**.



(6) Configure SMTP or FTP parameters.
   Configure SMTP parameters:
   Click **Communication** → **Notification by Email**.

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

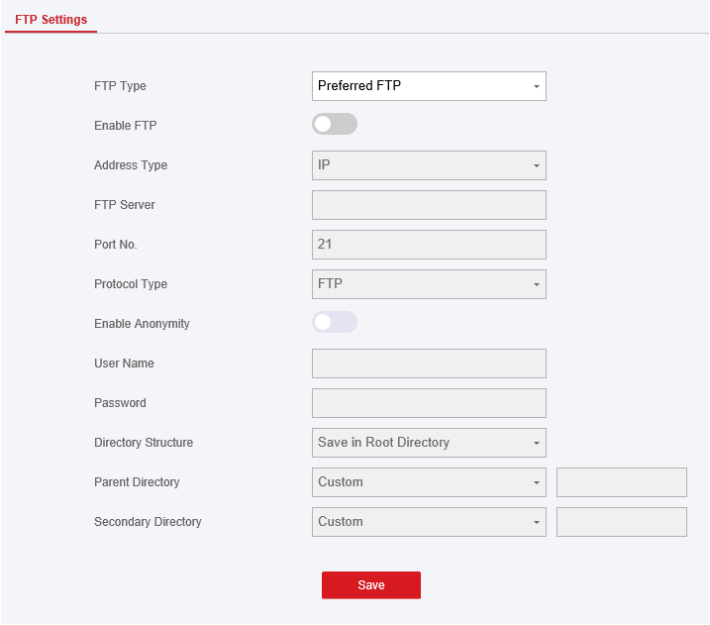


Configure FTP parameters:

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

Slide the slider to enable FTP and set corresponding parameters. For details, see FTP.

Click **Save**.



2. Upload Videos

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

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

   (2) Slide the slider to enable the selected alarm receiver center.

   (3) Select the **Protocol Type** as **SIA-DCS**.

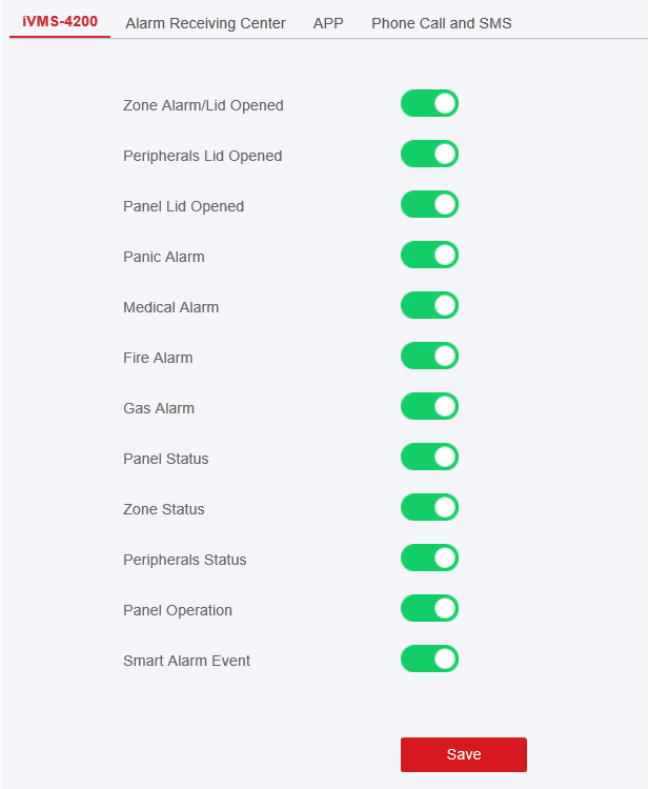
(4) Click **Save**.
(5) Configure SMTP or FTP parameters as same as Upload Photos.

Notification Push

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

Steps

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



2. Enable the target notification.

   Zone Alarm/Lid Opened

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

   Peripherals Lid Opened

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

   Panel Lid Opened

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

   Panic Alarm

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

Medical Alarm

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

Fire Alarm

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

Gas Alarm

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

Panel Status

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

Zone Status

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

Peripherals Status

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

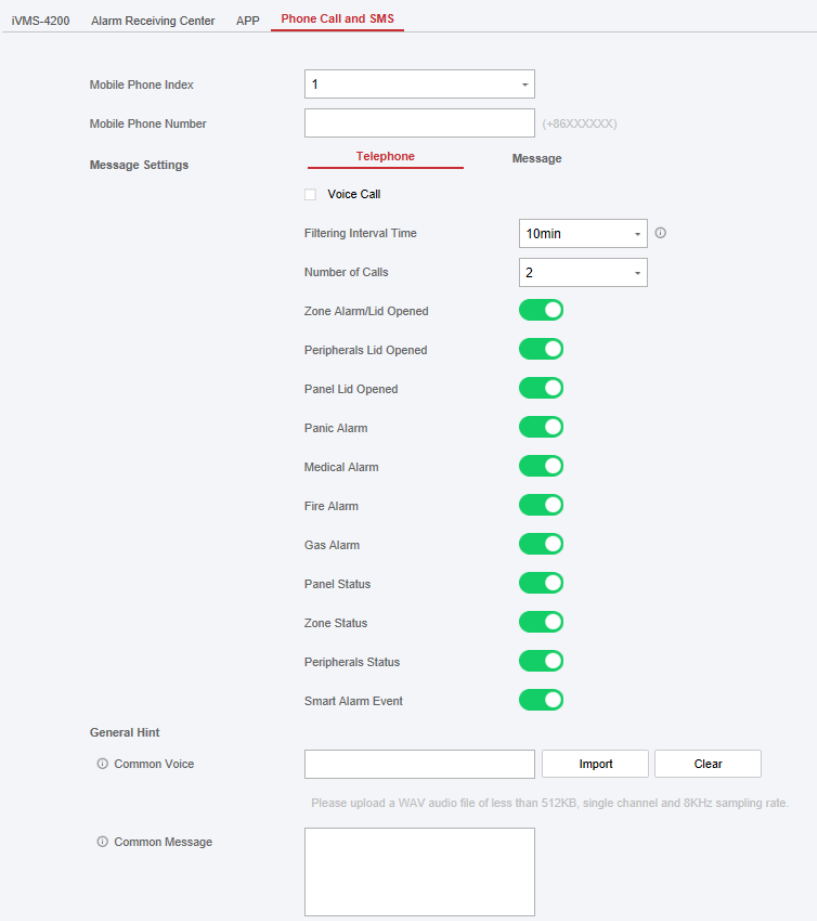
Panel Operation

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

Smart Alarm Event

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

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



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

General Hint

You can import **Common Voice.** When the alarm is triggered, your customized voice will be added at the beginning of the content of the phone dialed by the system.

Note

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

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

5. Click **Save**.

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

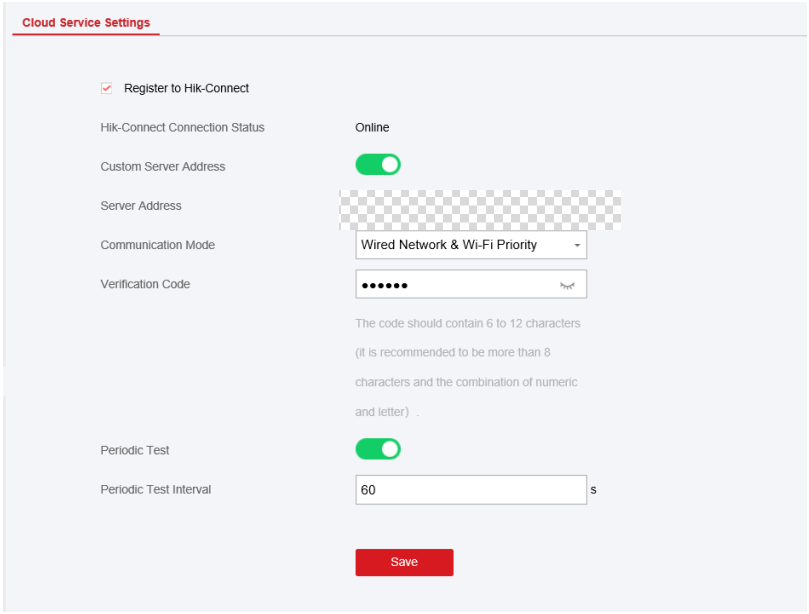
If you want to register the device to the mobile client for remote configuration, you should set the mobile client registration parameters.

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



2. 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).

3. Enable **Custom Server Address**.
   The server address is already displayed in the Server Address text box.

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

   Wired Network & Wi-Fi Priority

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

   Wired &Wi-Fi

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

   Cellular Data Network

   The system will select cellular data network only.
5. Optional: Change the verification code.

Note

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

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

Notification by Email

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

Steps

1. Click **Communication** → **Notification by Email** to enter the page.
2. Select **Email 1** or **Email 2**. (Email 2 is a backup for Email 1.)
3. Enable **Video Verification Events** and **Server Authentication**.
4. Enter the sender’s information.

Note

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

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

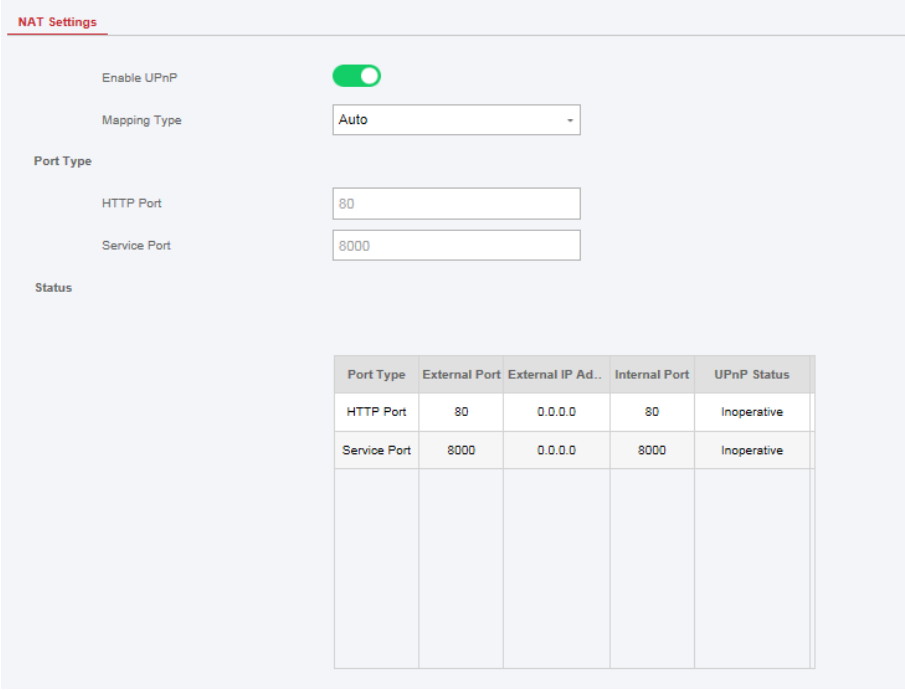
NAT

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

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

Steps

1. Click **Communication** → **NAT** to enter the page.



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

FTP

You can configure the FTP server to save alarm video.

Steps

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

FTP Type

Set the FTP type as preferred or alternated.

Protocol Type

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

FTP Server and Port No.

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.

Intercom Service

You can configure the Intercom service for an intercom sounder.

Before You Start

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

Steps

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

SIP

The control panel will use ARC and SIP server.

IP Receiver Pro

The control panel will user cloud service.

4. Select a sounder and click **Save**.

5.3.2 Device Management

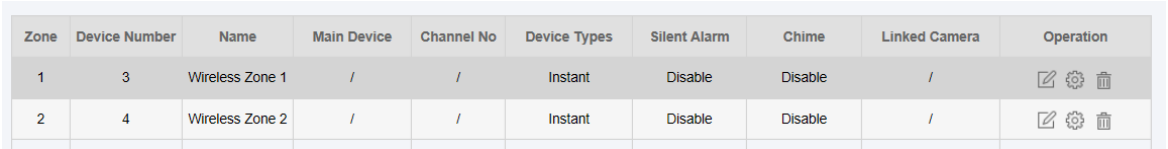
You can manage the enrolled peripherals including detector, sounder, keypad, etc. in this section.

Zone

You can set the zone parameters on the zone page.

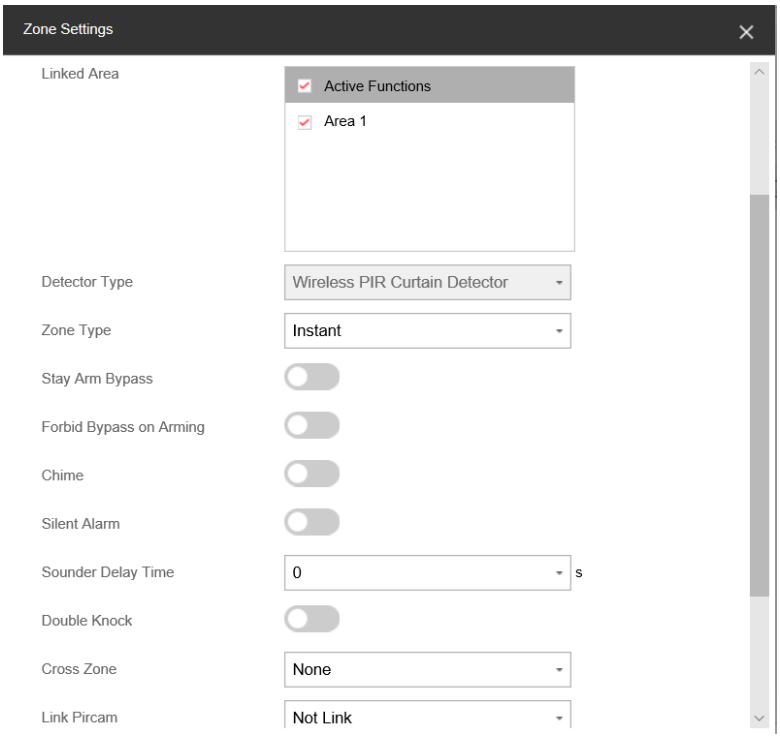
Steps

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



Zone	Device Number	Name	Main Device	Channel No	Device Types	Silent Alarm	Chime	Linked Camera	Operation
1	3	Wireless Zone 1	/	/	Instant	Disable	Disable	/	
2	4	Wireless Zone 2	/	/	Instant	Disable	Disable	/	

2. Select a zone and click 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.

Follow Zone

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

Keyswitch Zone

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

Note

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

Disabled Zone

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

24-hour Zone

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

Timeout Zone

The zone activates all the time. The zone type is used to monitor and report the "ACTIVE" status of a zone, but it will only report and alarm this status after the programmed time has expired. (1 to 599) Seconds. It can be used in places equipped with magnetic contacts that require access but for only a short period (e.g., fire hydrant box's door or another external security box door).

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.

Arm Mode

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

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

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

Stay Arm Bypass

The zone will be automatically bypassed in stay arming.

Cross Zone

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

Forbid Bypass on Arming

After enabled, you cannot bypass zones when arming.

Chime

Enable the doorbell. Usually used for door magnetic detectors.

Silent Alarm

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

Double knock

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

Sounder Delay Time

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

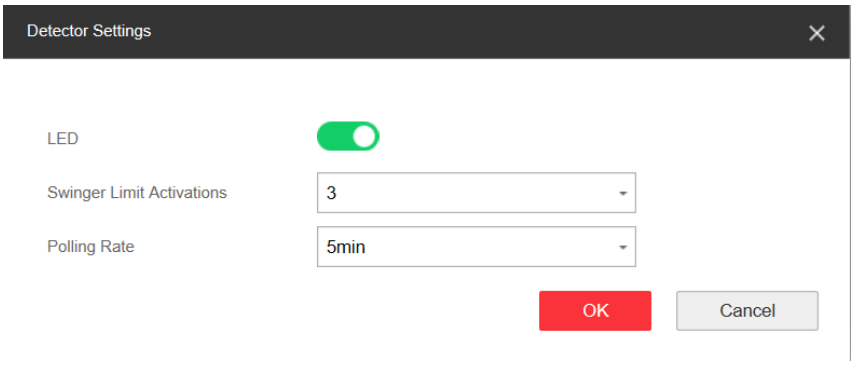
7. If required, link a PIRCAM or a camera for the zone.
8. Click **OK**.

Note

After adding the transmitter, you can click **Device** → **Zone** → **Enroll** to add a wired zone. Select the **Relate Mode** as Wired, the **Device Source** as Single or Multi Transmitter, the Channel and click **OK**.
After setting the zone, you can enter **Maintenance** → **Device Status** → **Zone Status** to view the zone status.

---

9. **Optional**: Click **Device** → **Zone** and click Detector Settings. You can set detector parameters.

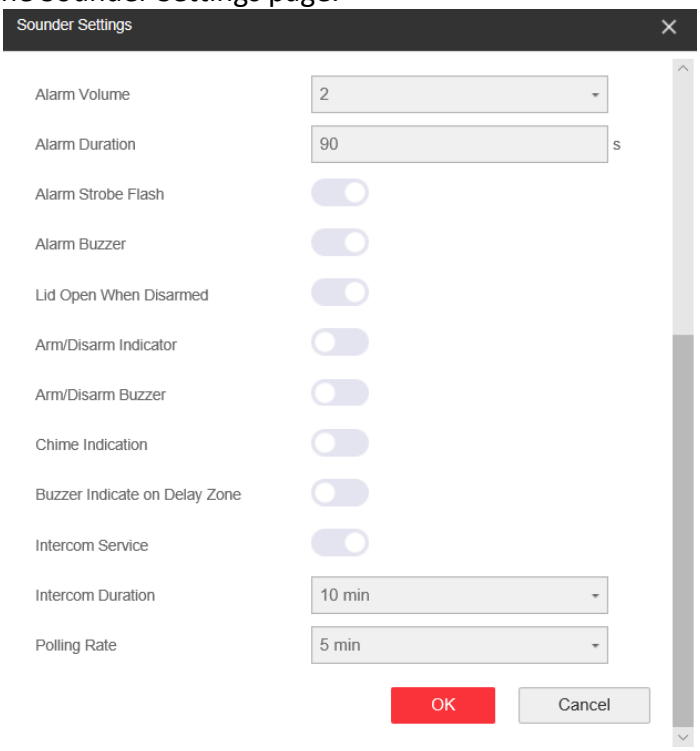


Sounder

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.



3. Set the alarm name, the volume and the duration.

Note

The available alarm volume range is from 0 to 3 (function varies according to the model of device).
The available alarm duration range is from 10 to 900 s.

4. Select the linked area.

Note

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

5. Select to enable **Alarm Strobe Flash, Alarm Buzzer**, **Lid Open When Disarmed**, **Arm/Disarm LED Indicator**, and **Arm/Disarm Buzzer**.

Alarm Strobe Flash

Enable alarm strobe light.

Alarm Buzzer

Enable alarm buzzer.

Lid Open When Disarmed

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

Arm/Disarm Indicator

Enable arm/disarm LED indicator.

Arm/Disarm Buzzer

Enable arm/disarm buzzer.

Chime Indicator

Enable chime.

Buzzer Indicator on Delay Zone

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

Intercom Service

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

6. Set the **Polling Rate**.
7. If required, enable **Enroll Wireless Sounder.**
8. Click **OK**.

Note

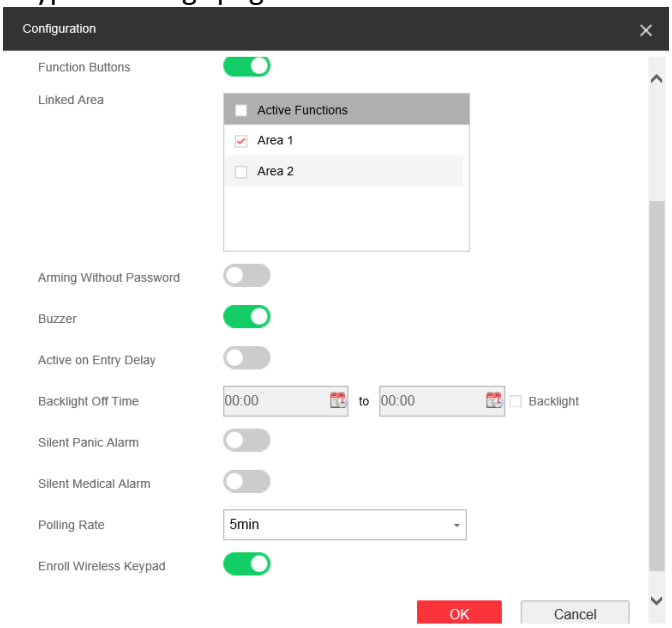
After the sounder is configured, you can click **Maintenance** → **Device Status** → **Sounder Status** to view the sounder status.

Keypad

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

Steps

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



3. Set the keypad name.
4. Enable the function of buzzer, silent panic alarm, silent medical alarm, and keypad button.
5. Enable the function of arming without password and active on entry delay.
6. Check the **Enable** check box of Back-light Off Time, and set the duration of light off.
7. Set the polling 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

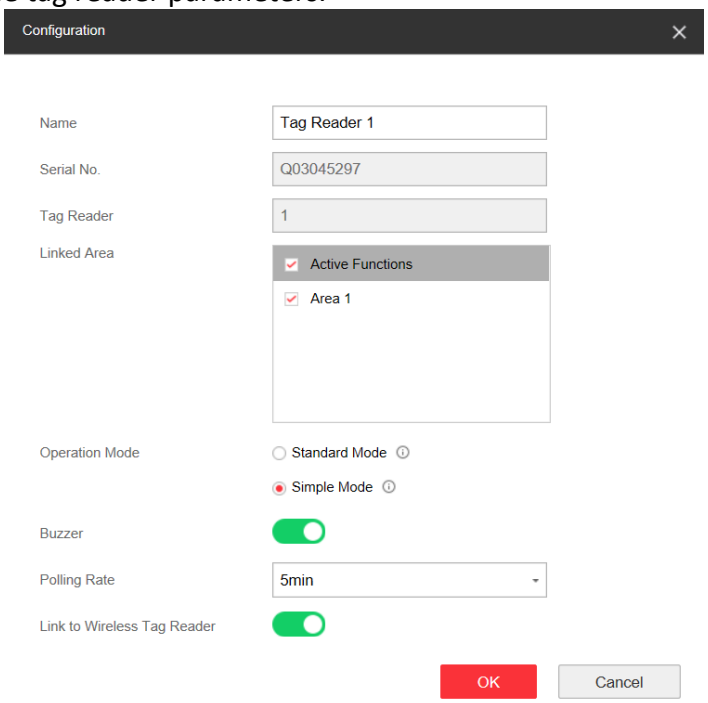
- After the keypad is configured, you can click **Maintenance** → **Device Status** → **Keypad Status** to view the keypad status.
- You can set the keypad password on the page of **User** → **User Management**→ **Operation**.

Tag Reader

You can set the parameters of the tag reader.

Steps

1. Click **Device** → **Automation** to enter the page.
2. Click **Enroll**, enter the serial No. to add a tag reader.
3. Click ⚙ to edit the tag reader parameters.



4. Edit device name.
5. Check linked areas.
6. Select operation mode.

Standard Mode

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

Simple Mode

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

7. Choose whether to enable the **Buzzer**. After disable the buzzer, there will be no beep when swiping the tag.
8. Set **Polling Rate**.

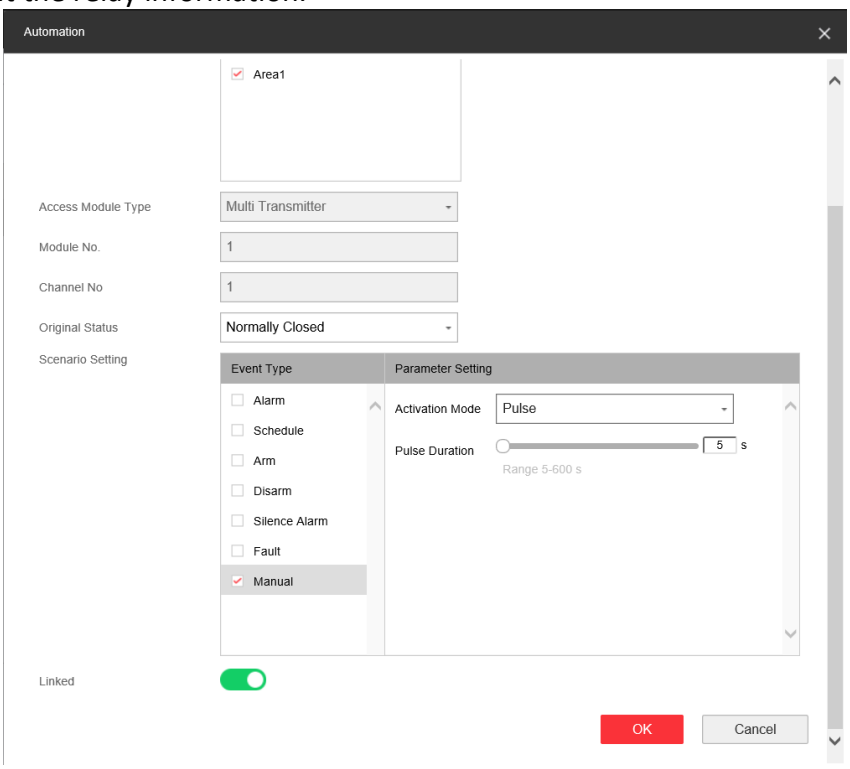
9. **Optional**: Enable **Link to Wireless Tag Reader**.
10. Click **OK**.

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.



- 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

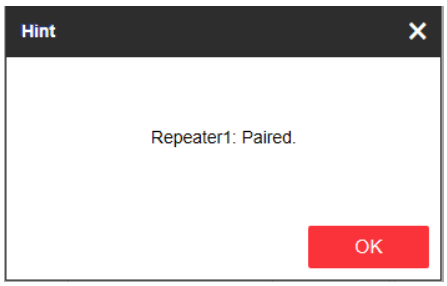
- Set the original status as Normally Closed or Normally Open.
- Set the event for being triggered.
- Set the activation after being triggered.
- Set whether to link to the relay output device or not. If the link is enabled, the device will be deleted.

Repeater

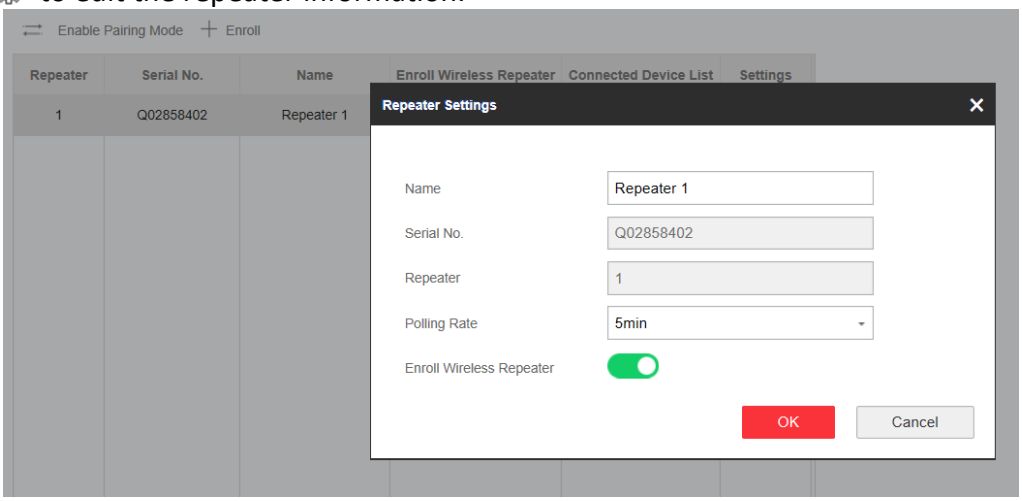
The repeater can amplify signals between the control panel and the peripherals.

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.

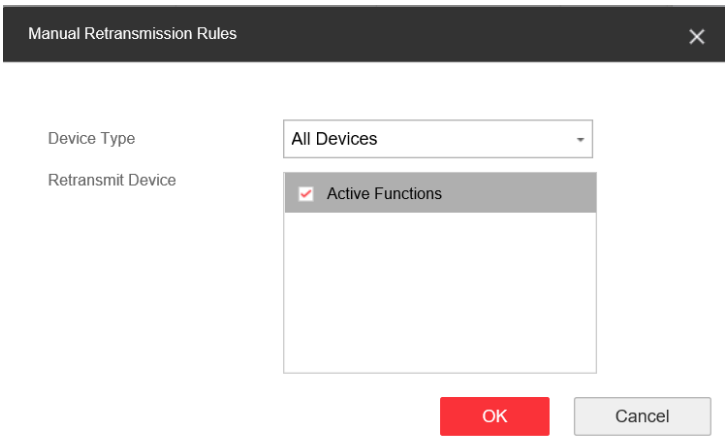


5. Click ⚙ to edit the repeater information.



- 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.

6. Click ⚙ to enter the Manual Retransmission Rules page.



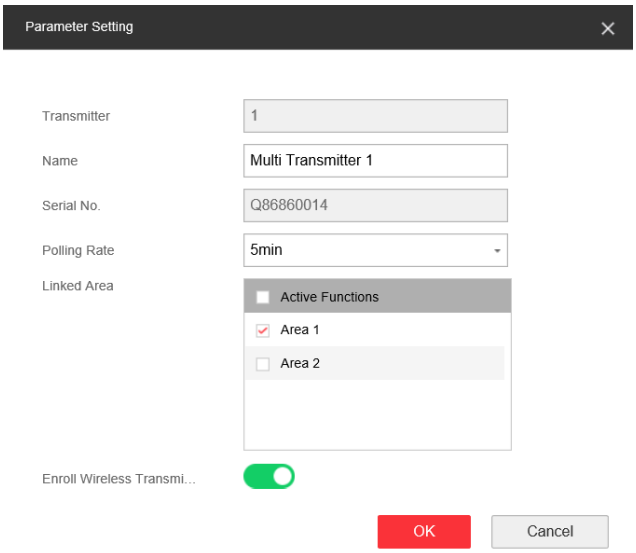
- Select the **Device Type**.
- Check **Active Functions**.
- Click **OK**, then the devices can be manually retransmitted.

Transmitter

You can set the parameters of the transmitter.

Steps

1. Click **Device** → **Transmitter** to enter the page.
2. Click **Enroll,** enter the Serial No. and select the device model to add a transmitter.
3. Click ⚙ to edit the transmitter information.



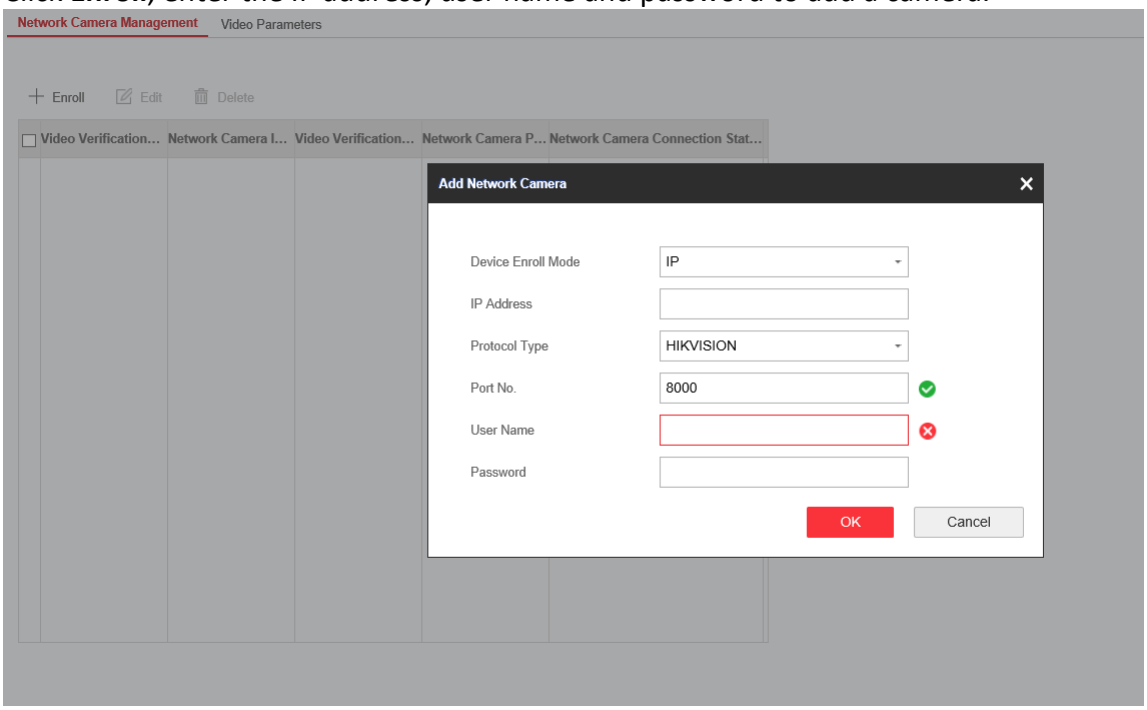
4. Set the name of the transmitter.
5. Set the polling rate of the transmitter.
6. Enable **Enroll Wireless Transmission**.
7. Click **OK**.

Network Camera

You can add network cameras in the system.

Steps

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



3. Click ⚙ to edit the camera information.

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

5.3.3 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. Click **Edit Linked Zone** and **Edit Linked Peripheral** to check linked zones or peripherals.
5. Click **Save** to complete the settings.

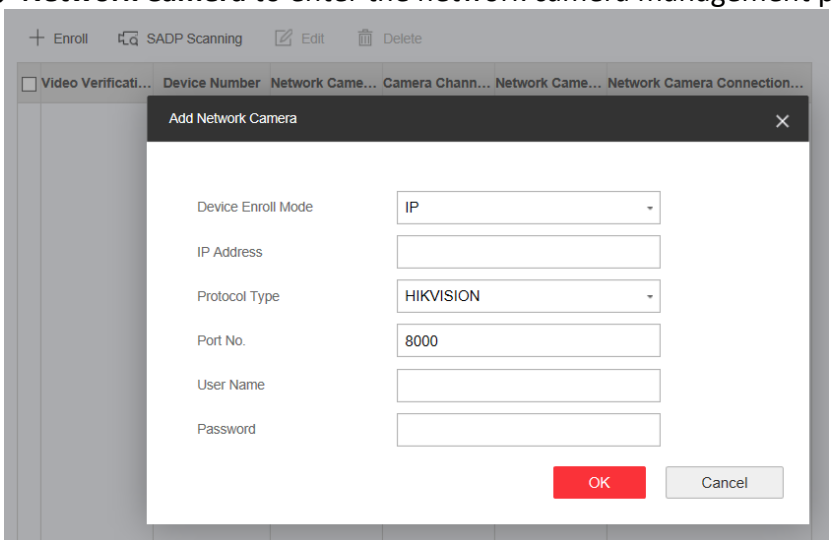
5.3.4 Video Management

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



2. Click **Enroll**, and enter the basic information of the camera, such as IP address and port No., and select the protocol type.
3. Enter the user name and password of the camera.

   SADP Scanning

   Scan all network cameras in the same LAN. A list will pop up after scanning. You can directly check to add cameras in the list.
4. Click **OK**.
5. **Optional**: Click **Edit** or **Delete** to edit or delete the selected camera.

Link a Camera with the Zone

Steps

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

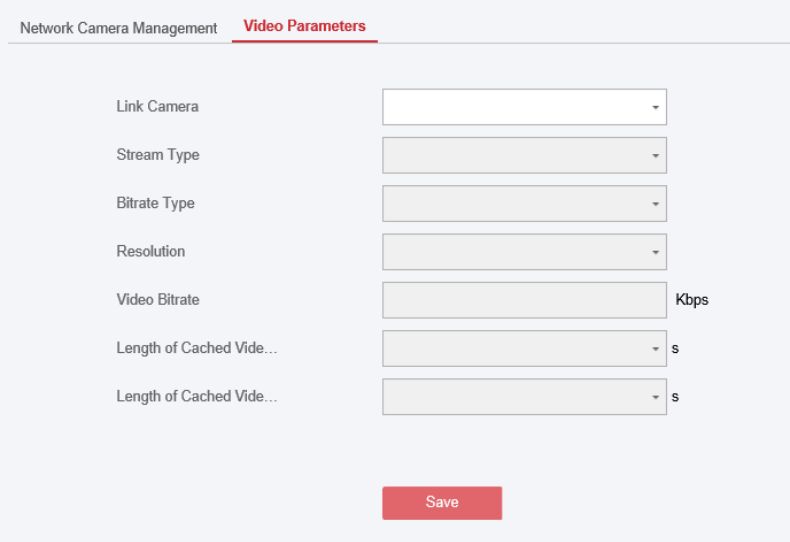
Note

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

Set Video Parameters

Steps

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



2. Select a camera and set the video parameters.

Stream Type

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

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Video Bitrate

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

5.3.5 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 **Enroll** and press any key on the keyfob.
3. Set the keyfob parameters.

   Name

   Customize a name for the keyfob.

   Permission Settings

   Check different items to assign permissions.

   Single Key Settings

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

   Combination Keys Settings

   Select from the drop-down list to set combination keys' functions.
4. Click **OK**.
5. Optional: Click to edit the keyfob information.
6. Optional: Delete a single keyfob or check multiple keyfobs and click **Delete** to delete the keyfobs in batch.

Note

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

Add/Edit/Delete Tag

You can add tag to the AX 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 **Enroll** 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.

5.3.6 Maintenance

Device Information

You can view device name and other information.

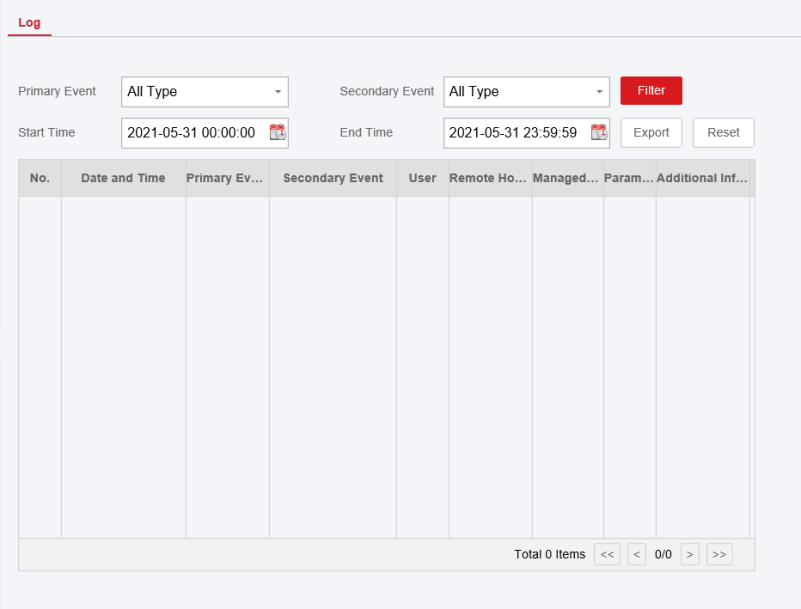
Click **Maintenance → Device Information** to enter the page.
You can view device model, device serial No., device firmware version, web version or click **About** → **View Licenses** to view the source software licenses.

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

Local Log Search

You can search the log on the device.

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



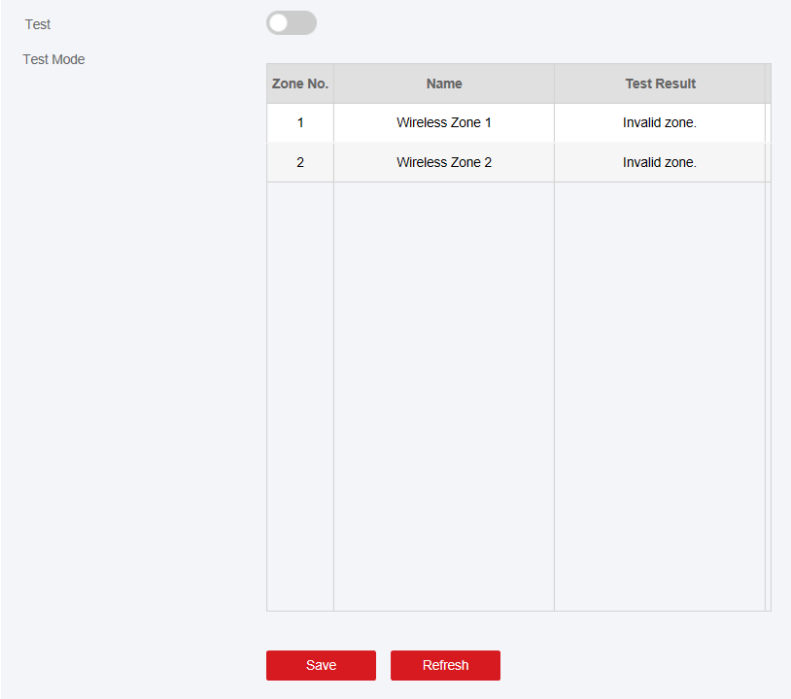
Select a primary event and a secondary event from the drop-down list, set the log start time and end time and click **Filter**. All filtered log information will be displayed in the list.
You can also click **Reset** to reset all search conditions.

Test

The AX PRO supports walk test function.

Steps

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



Note

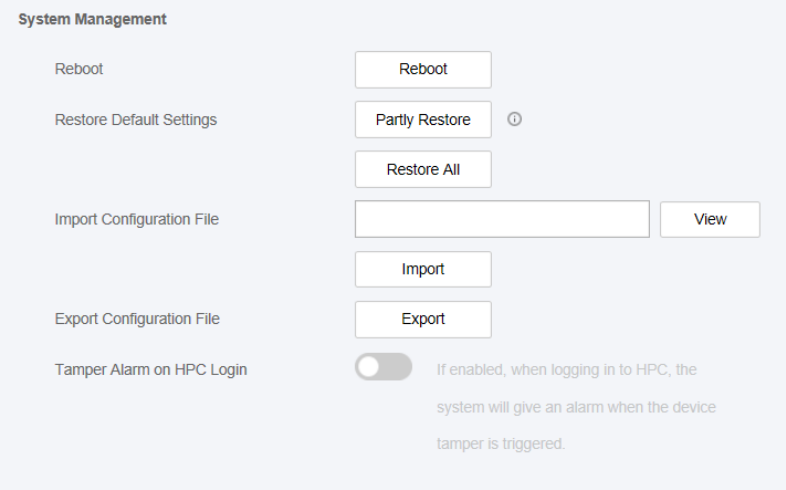
Only when all the detectors are without fault, you can enter the mode TEST mode.

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

System Maintenance

You can reboot the device, restore default settings, import/export configuration file, 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 **Maintenance→ Device Maintenance→ 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 device time zone information, user parameters, wired network, Wi-Fi network, HC information detector information, detector information enrolled in the zone and enrolled wireless peripheral information to default ones.

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

Import Configuration File

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

Export Configuration File

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

Exporting configuration file requires a password to be used for file encryption.

Tamper Alarm on HPC Login

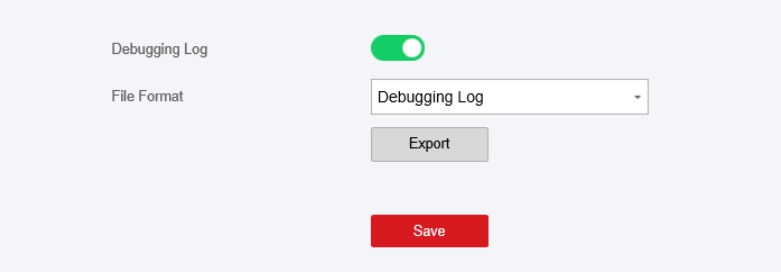
After this function is enabled, the device lid opened alarm (tamper alarm) takes effect when installer login. (By default, the lid opened alarm (tamper alarm) does not take effect when the installer login.)

Export File

You can export debugging file to the PC.

Steps

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



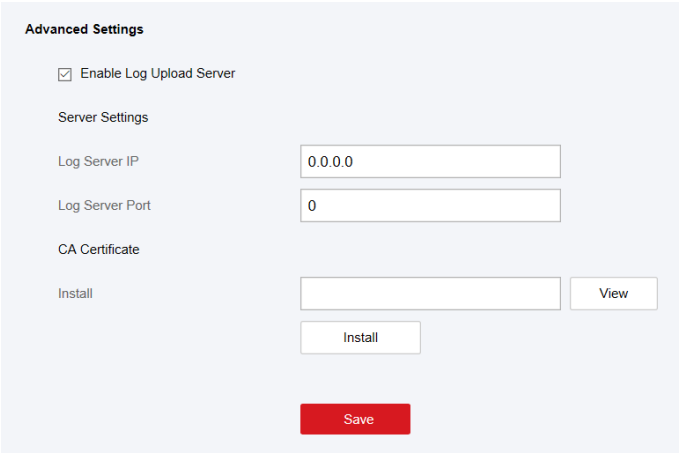
2. Slide to enable the function.
3. Click **Export** to save the debugging file in the PC.

Security Audit Log

You can add the Security Audit Server to the system, to receive the security audit exception logs (e.g., injection attack logs, XSS events) of encoding devices from the server, and trigger related alarms in the system.

Steps

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



3. Check **Enable Log Upload Server**.
4. Enter log server IP and port.

5. Click **View** to select a certificate.

Note

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

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

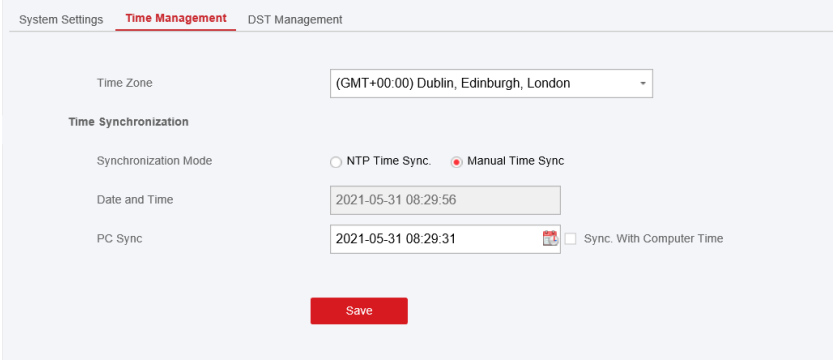
5.3.7 System Settings

Time Settings

You can set the device time zone, synchronize device time, and set the DST time. The device supports time synchronization via **Hik-Connect Guarding Vision** server.

Time Management

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



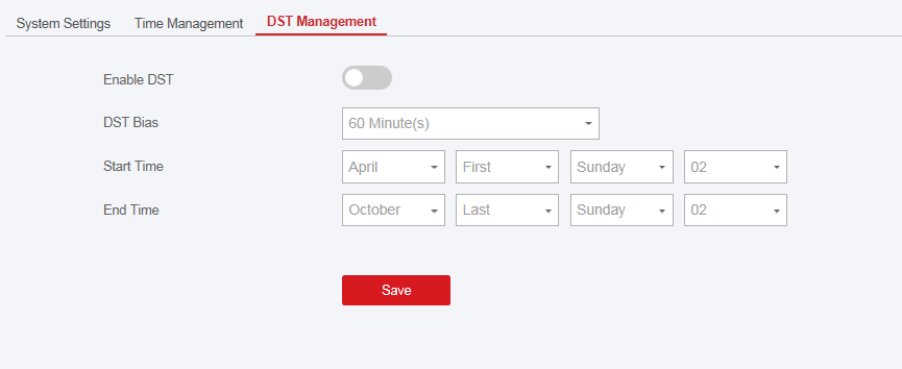
You can select a time zone from the drop-down list.
You can synchronize the device time manually with NTP. Check the check box of **NTP Time Sync.**, enter the server address and port No., and set the synchronization interval.
You can synchronize the device time manually. Or check **Sync. with Computer 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.

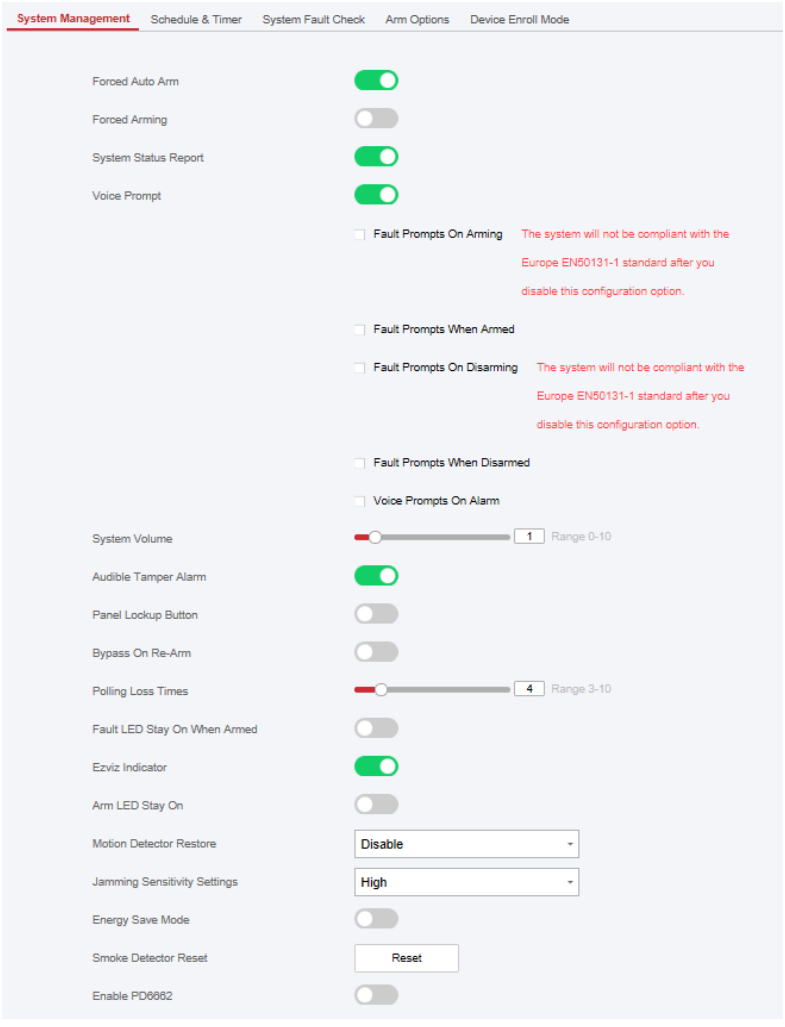


You can enable the DST and set the DST bias, DST start time, and DST end time.

Authority Management

Set the authority options.

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



Forced Auto Arm

After enabled, when the timed automatic arming starts, if there are an active faults in a zone,

the zone will be automatically bypass.

Note

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

Forced Arming

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

System Status report

If the option is enabled, the device will upload report automatically when the AX 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 LED Stay On When Armed

When system is armed, the fault indicator is always on.

Ezviz Indicator

Enable the Ezviz indicator.

Arm LED Stay On

The arm LED is always on.

Motion Detector Restore

Motion detectors include all PIR detectors.

Jamming Sensitivity Settings

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

Energy Save Mode

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

Enable PD6662

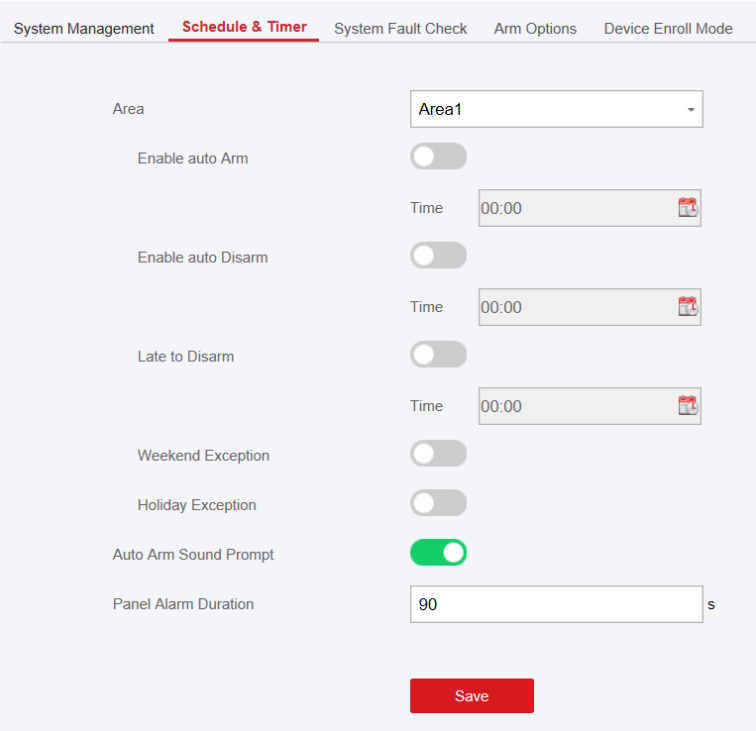
Enable PD6662 standard. Functions that do not meet the standard will not take effect.

Schedule and Timer Settings

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

Steps

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



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

Enable Auto Arm

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

Note

- The auto arming time and the auto disarming time cannot be the same.
- The buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.
- You can select to enable forced arming on the System Options page. While the function is

enabled, the system will be armed regardless of the fault.

Enable Auto Disarm

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

Note

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

Late to Disarm

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

Note

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

Weekend Exception

Enable the function and the zone will not be armed in the weekend.

Holiday Exception

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

Note

Up to 6 holiday groups can be set.

Auto Arm Sound Prompt

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

Panel Alarm Duration

The time duration of the panel alarm.

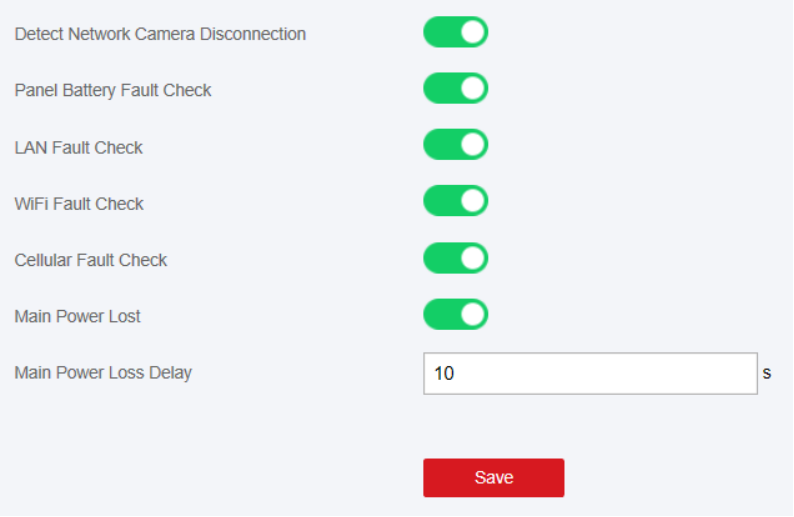
Note

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

5. Click **Save**.

Fault Check

The system determines whether to check the faults listed on the page. The system will only check the fault that is selected.
Click **System** → **System Options** → **System Fault Check** to enter the page.



Detect Network Camera Disconnection

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

Panel Battery Fault Check

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

LAN Fault Check

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

Wi-Fi Fault Check

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

Cellular Network Fault Check

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

Main Power Lost

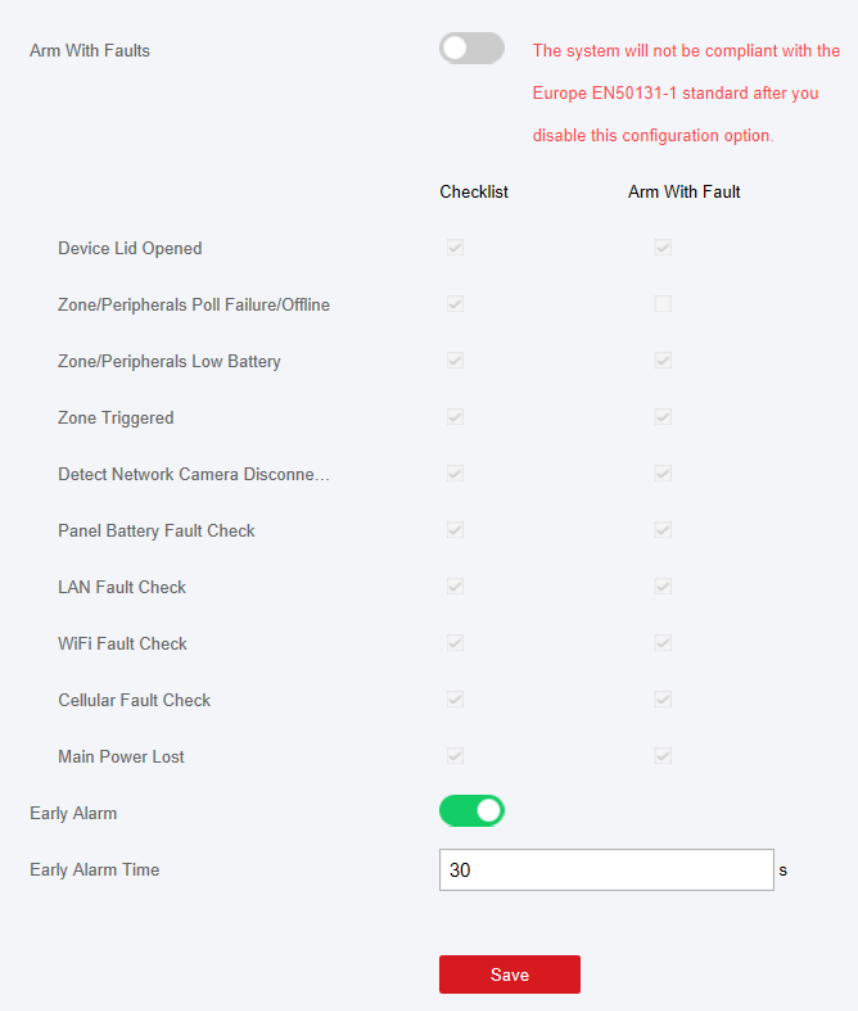
If the option is enabled, an alarm will be triggered when the main supply is disconnected.

Main Power Loss Delay

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

Arm Options

Set advanced authority parameters.
Click **System** → **System Options** →**Arm Options** to enter the Advanced Settings page.



You can set the following parameters:

Arm with Fault

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

Fault Checklist

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

Early Alarm

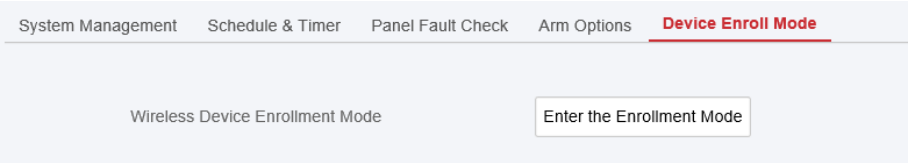
If you enable the function, when the zone is armed and the zone is triggered, the alarm will be triggered after the set delay time.

Note

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

Device Enroll Mode

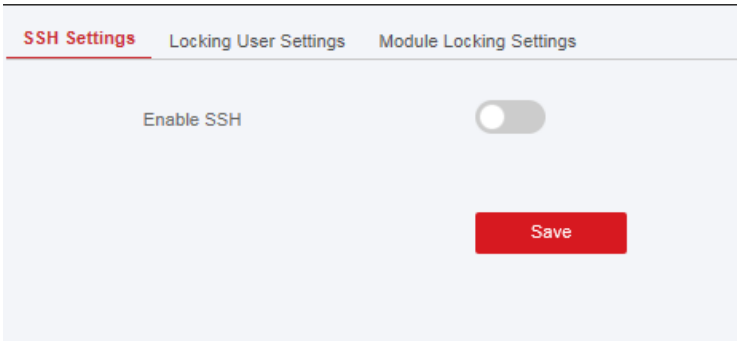
Click Enter the Enrollment Mode to make the panel enter the enroll mode.



Security Settings

SSH Settings

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



Locking User Settings

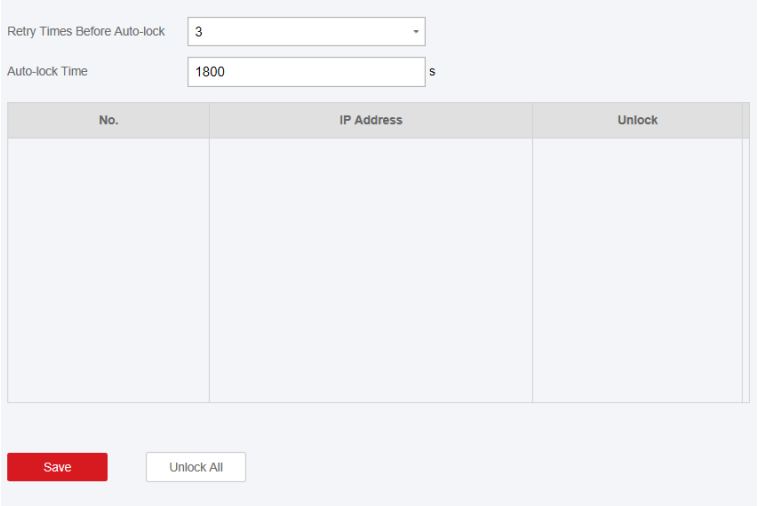
The device will be locked 90 s after 3 failed credential attempts (can be set in Retry Time before Auto-Lock) in a minute.
You can view the locked user or unlock a user and set the user locked duration.

Note

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

Steps

1. Click **System → System Security → User Lockout Attempts** to enter the Locking User Settings page.



2. Set the following parameters.

Retry Times before Auto-Lock

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

Note

The administrator has two more attempts than the configured value.

Auto-lock Time

Set the locking duration when the account is locked.

Note

The available locking duration is 5s to 1800s.

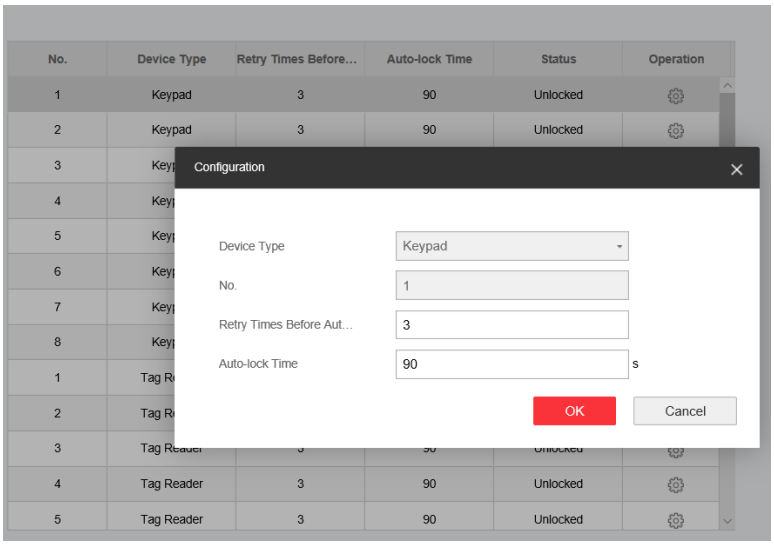
3. Click to unlock the account or click **Unlock All** to unlock all locked users in the list.
4. Click **Save**.

Module Lock Settings

Set the module locking parameters, including the Max Failure Attempts, and locked duration. The module will be locked for the programmed time duration, once the module authentication has failed for the amount of configured times.

Steps

1. Click **System** → **System Security** → **Module Locking Settings** to enter the Module Lock Settings page.



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

Retry Times before Auto-Lock

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

Auto-lock Time

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

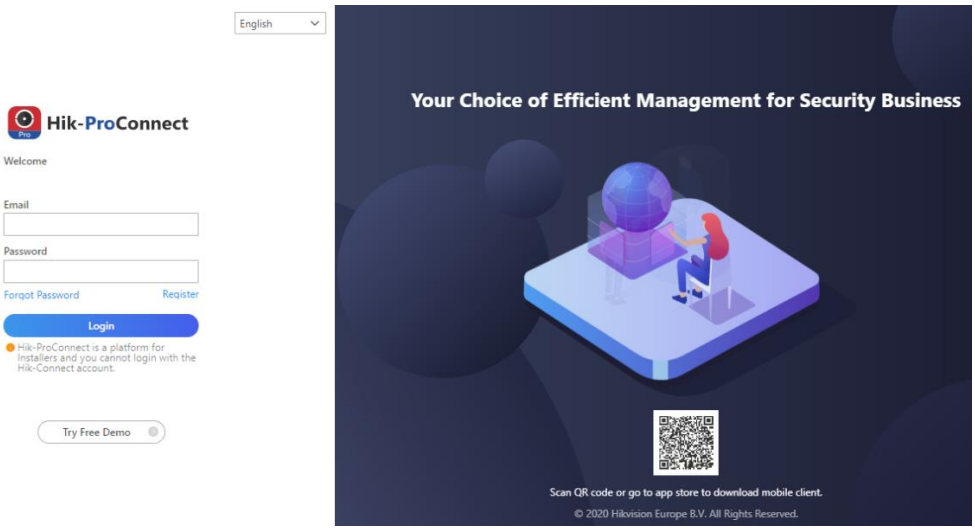
4. Click **OK**.
5. Optional: Click the **Lock** icon to unlock the locked module.

Device Upgrade

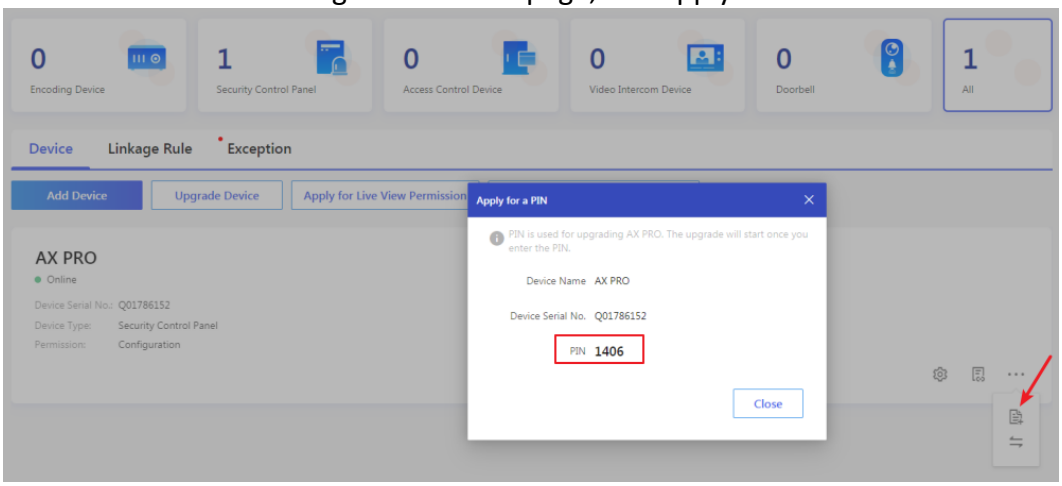
Get Manufacture PIN

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.

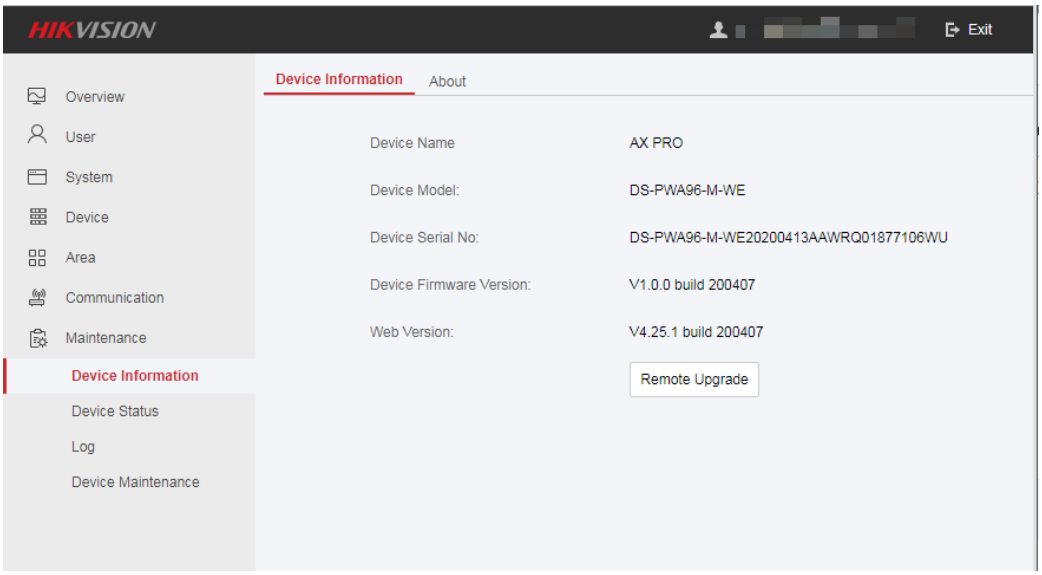


- **Get PIN from HIKVISION tech-support**
  It is better to use remote desktop to access the local web client of control panel. The PIN will be authorized according to the standard tech-support procedure.

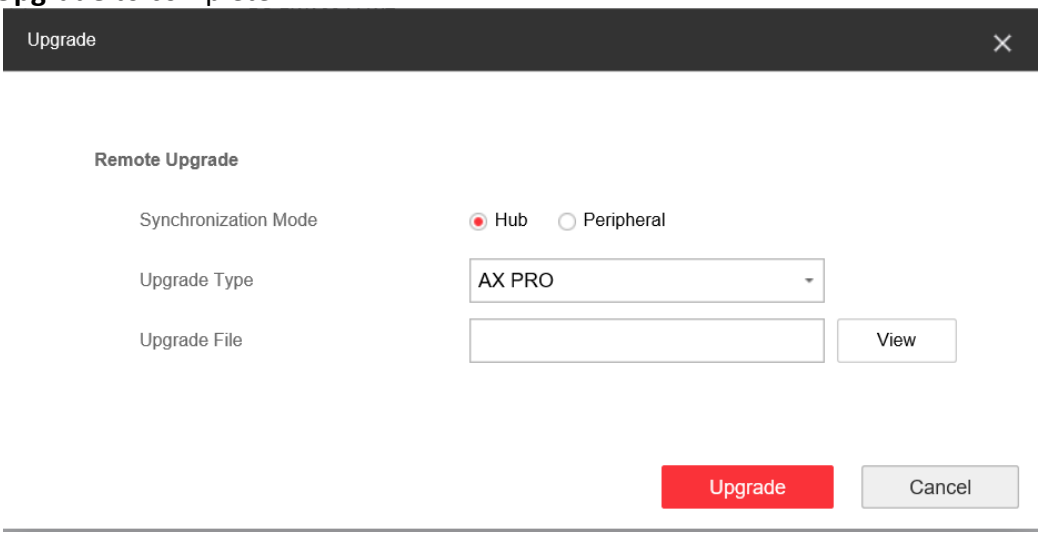
Firmware Upgrade

Steps:

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



3. Choose the hub or the peripheral for upgrade, and select the **Upgrade Type**.
4. Click **View** to find the firmware file with the name digicap.dav.
5. Click **Upgrade** to complete.

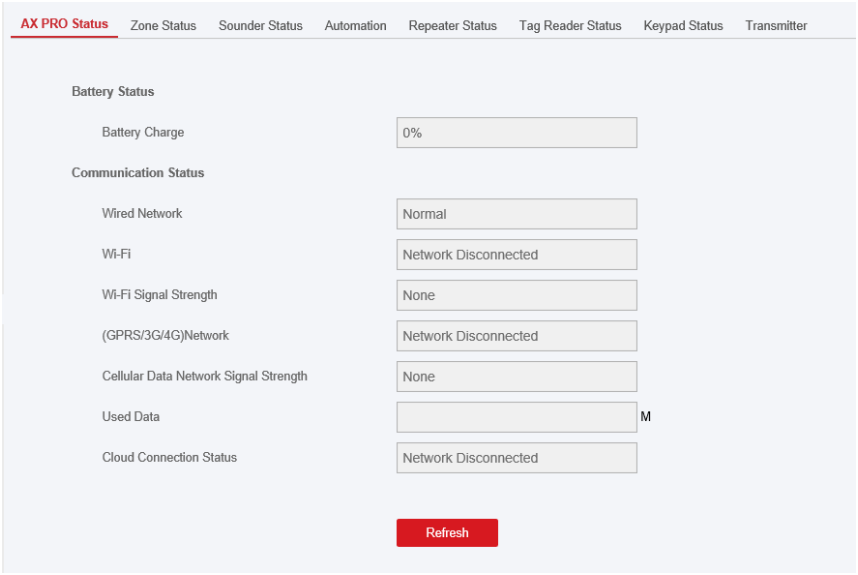


Note

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

5.3.8 Check Status

After setting the zone, repeater, and other parameters, you can view their status.
Click **Maintenance** → **Device Status**. You can view the status of AX PRO control panel, zone, sounder, automation, repeater, keypad, Tag reader, keyfob and transmitter.



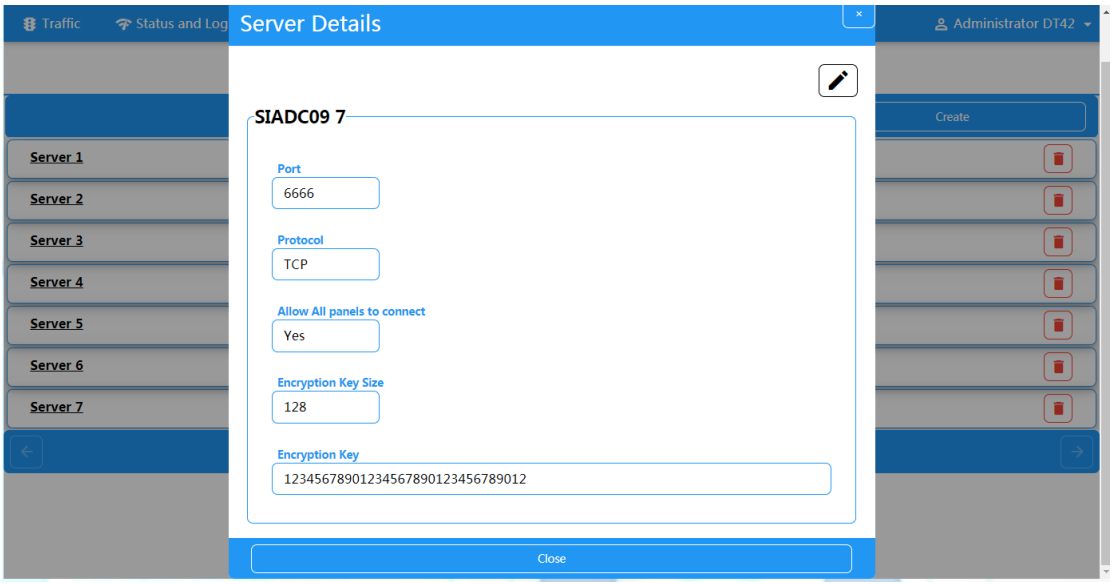
5.4 Report to ARC (Alarm Receiver Center)

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

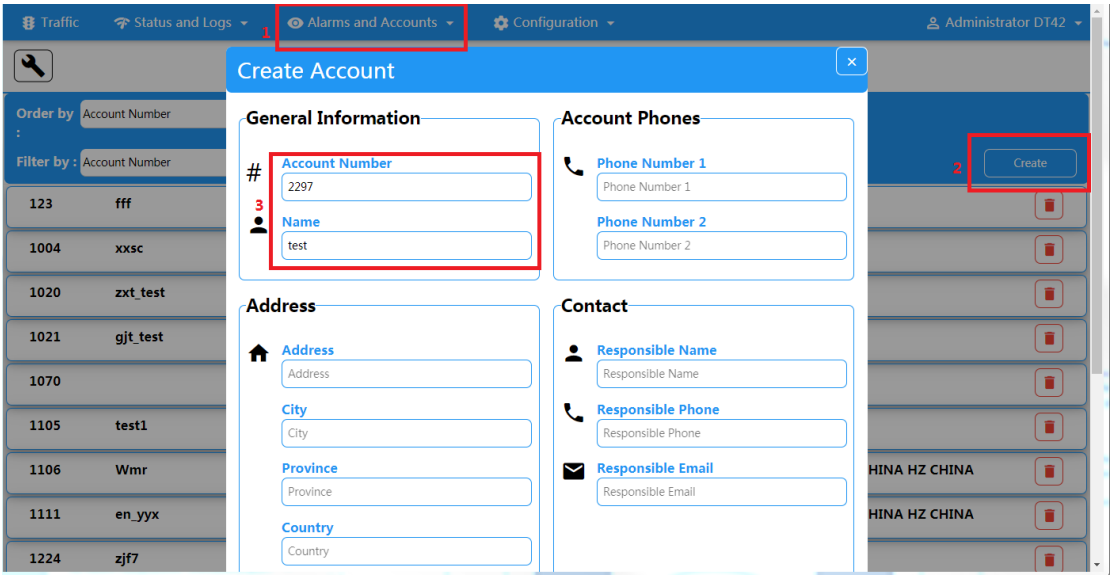
Steps:

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



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

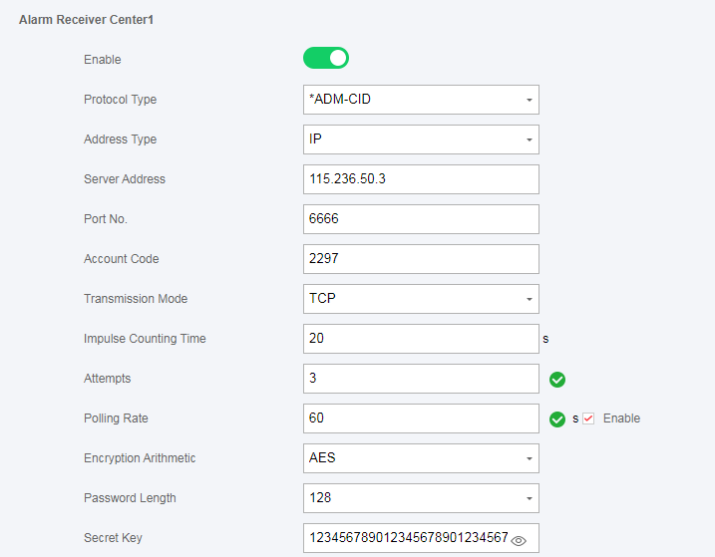
show below.



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**.



- = Protocol Setting =

Protocol Type — ADM-CID — SIA-DCS — *ADM-CID — *SIA-DCS Select token supported by the receiver in the ARC. Choose the token with "*" mark to

improve the communication security.

- **= Server Setting =**

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

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

- **= Account Setting =**

  - ***Account Code***

    Input the assigned account provided by the ARC.

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

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

    Both TCP and UDP are supported for transmission. UDP is recommended by the SIA DC-09 standard.
  - ***Connection Setting***
    - ***Impulse Counting Time / Retry Timeout Period***

      Setup the timeout period waiting for receiver to respond. Re-transmission will be arranged if the transceiver of receiving center is timeout.
    - ***Attempts***

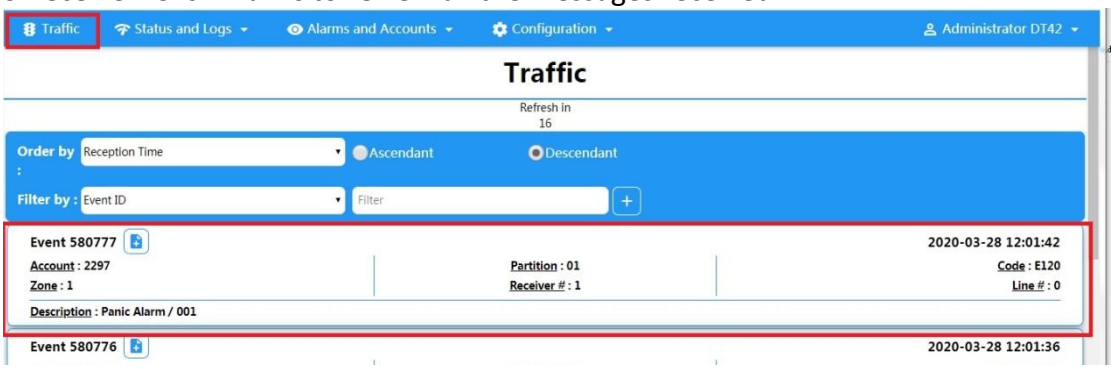
      Setup the maximum number that re-transmission will be tried.
    - ***Polling Rate***

      Setup the interval between 2 live polling if enable is checked.
  - ***Encryption Setting***
    - ***Encryption Arithmetic***
      - AES
    - ***Password Length***
      - 128
      - 192
      - 256
    - ***Secret Key***

      Setup the encryption key length and input the key provided by the ARC.

Signaling Test

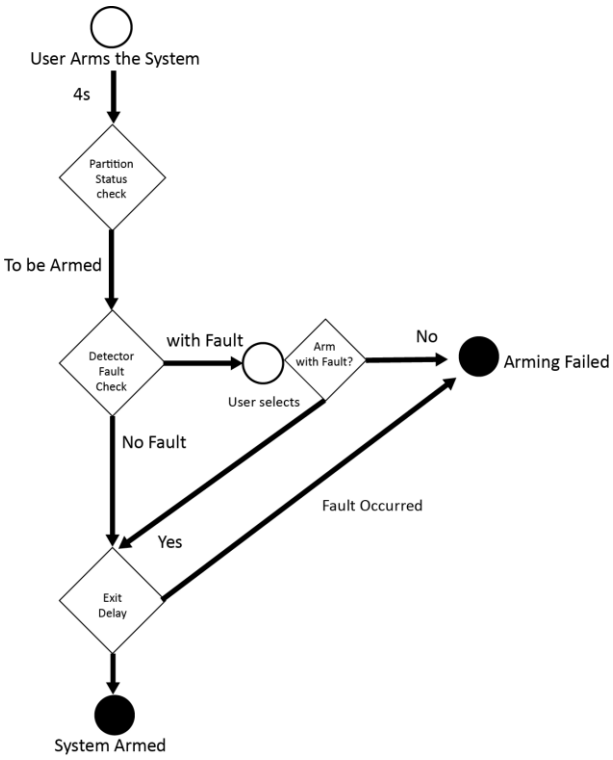
Activate a panic alarm from the control panel.
Login to Receiver. Click **Traffic** to review all the messages received.



Chapter 6 General Operations

6.1 Arming

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



Access level of Arming

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

Arming Indication

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

Reason of Arming Failure

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

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

Arming with Fault

While the arming is stopped with fault, user in level 2 has the permission to arm the system with fault (forced arming).
Forced arming only takes effect on the current arming operation.
The forced arming operation will be record in the event log.

6.2 Disarming

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

Disarming Indication

The arming/disarming indicator flashes 30s while the user successfully disarm the system through the entry/exit route.
The system will report the disarming result after the operation completed.

Entry Delay Duration

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

Early Alarm

If 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.

6.3 SMS Control

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

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

Command: 2 digits, 00- Disarming, 01- Away arming, 02- Stay arming, 03- Silencing alarm
Operation type: 1- Area Operation
Target: No more than 3 digits, 0-Operation for all areas, 1-Operation for area 1(zone1), and the rest can be deduced by the analogy.

A. Trouble Shooting

A.1 Communication Fault

A.1.1 IP Conflict

Fault Description:
IP that the panel automatically acquired or set is same as other devices, resulting in IP conflicts.
Solution:
Search the current available IP through ping. Change the IP address and log in again.

A.1.2 Web Page is Not Accessible

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

A.1.3 Hik-Connect is Offline

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

A.1.4 Network Camera Drops off Frequently

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

A.1.5 Failed to Add Device on APP

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

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

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

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

A.2 Mutual Exclusion of Functions

A.2.1 Unable to Enter Registration Mode

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

A.3 Zone Fault

A.3.1 Zone is Offline

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

A.3.2 Zone Tamper-proof

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

A.3.3 Zone Triggered/Fault

Fault Description:

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

A.4 Problems While Arming

A.4.1 Failure in Arming (When the 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	The system will immediately alarm when it detects triggering event after system armed. Audible Response Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Perimeter Zone	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and sounder. There is a configurable interval between alarm and sounder output, which allows you to check the alarm and cancel the sounder output during the interval. Voice Prompt: Zone X perimeter alarm.
Delayed Zone	The system provides you time to leave through or enter the defense area without alarm. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X alarm.
Follow Zone	The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X follow alarm.
24H Silence Zone	The zone activates all the time without any sound/sounder output when alarm occurs. Audible Response: No system sound (voice prompt or sounder).
Panic Zone	The zone activates all the time. Audible Response: Trigger the system sound and sounder. Voice Prompt: Zone X panic alarm.
Fire Zone	The zone activates all the time with sound/sounder output when alarm occurs.

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

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

Voice Prompt: Armed/Arming failed.

C. Output Types

Table C-1 Output Types

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

D. Event Types

Table D-1 Event Types

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

E. Access Levels

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

Table E-1 Permission of the Access Level

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

Note

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

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

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

F. Signalling

Detection of ATP/ATS Faults

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

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

	TN	Maximum timing of detection
Primary ATP failure/restore	LAN/WiFi	10 min
Secondary ATP failure/restore	GPRS	60 min
	3G/4G LTE	20 min (when primary ATP failed)

Signalling will be always transmitted from primary ATP when it is operational. Otherwise it will be automatically switched to secondary transmission path that is operational at the moment. Both primary and secondary ATP fault and restore events will be reported to ARC when there is an ATP left to work. They will also be recorded to mandatory log memory with capacity of 1000 records allocated in non-volatile flash memory storage, as well as the ATS fault record. The detail of reports and log records are listed in the table below.

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

ATS Category

The ATS category of AXPRO is DP2. While the alarm receiving center is enabled. The control panel will upload alarm report to the receiver center via the main path (LAN or Wi-Fi) or the back-up path (3G/4G). If the control panel is properly connected to the LAN or Wi-Fi, the main path is selected as the transmission path. If the main path connection is failed, the path will be switched to 3G/4G. And if the main path connection is restored, the path will be switched back to LAN or Wi-Fi. The control panel checks the connection status continuously, and generates logs transmission fault for any of the path. While both of the paths are invalid, the control panel determines ATS fault.

G. SIA and CID Code

Note

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

Table F-1 SIA and CID Code

SIA Code	CID Code	Description
MA	1100	Medical Alarm
MH	3100	Medical Alarm Restored
BA (Water Leak Detector: WA)	1130 (Water Leak Detector: 1154)	Burglary Alarm
BH (Water Leak Detector: WH)	3130 (Water Leak Detector: 3154)	Burglary Alarm Restored
FA (Heat Detector: KA)	1111 (Heat Detector: 1114)	Fire Alarm
FH (Heat Detector: KH)	3111 (Heat Detector: 3114)	Fire Alarm Restored
HA	1121	Duress alarm
HA	1122	Silent Panic Alarm
HH	3122	Silent Panic Alarm Restored
AA	1123	Audible Panic Alarm
CH	3123	Audible Panic Alarm Restored
	1133	24H Alarm
	3133	24H Alarm Restored
	1133	24H Alarm
	3133	24H Alarm Restored
BA	1130	Timeout Alarm
BH	3130	Timeout Alarm Restored
PA	1120	Audible Panic Alarm
PH	3120	Audible Panic Alarm Restored
BA	1130	Burglary Alarm
BH	3130	Burglary Alarm Restored
BA	1131	Perimeter Breached

SIA Code	CID Code	Description
BH	3131	Perimeter Restored
AD	1132	Interior Burglary Alarm
CK	3132	Interior Burglary Alarm Restored
BA (Water Leak Detector: WA)	1130 (Water Leak Detector: 1154)	24H Alarm
BH (Water Leak Detector: WH)	3130 (Water Leak Detector: 3154)	24H Alarm Restored
BA (Water Leak Detector: WA)	1130 (Water Leak Detector: 1154)	Burglary Alarm
BH (Water Leak Detector: WH)	3130 (Water Leak Detector: 3154)	Burglary Alarm Restored
TA	1137	Lid Opened
TR	3137	Lid Restored
BV	1139	Confirmed Alarm
BW	3139	Confirmed Alarm Restore
		BUS Open-circuit Alarm
		BUS Open-circuit Restored
AF	1142	BUS Short-circuit Alarm
CN	3142	BUS Short-circuit Restored
TA	1144	External Probe Disconnected
TR	3144	External Probe Connected
AG	1148	Device Motion Alarm
CO	3148	Device Motion Alarm Restored
	1149	Masking Alarm
	3149	Masking Alarm Restored
GA	1162	Gas Leakage Alarm
GH	3162	Gas Leakage Alarm Restored
AH	1207	Zone Early-Warning
CP	3207	Zone Early-Warning Dismissed
AT	1301	Mains Power Lost
AR	3301	Mains Power Restored

SIA Code	CID Code	Description
YT	1302	Battery Low
YR	3302	Battery Voltage Restored
ZY	1305	Reset to defaults
YM Transmitter battery missing ID range: 301~	1311 Transmitter battery missing ID range: 301~	Battery Disconnected
YR Transmitter battery missing ID range: 301~	3311 Transmitter battery missing ID range: 301~	Battery Reconnected
YI	1312	Overcurrent Protection Triggered
YJ	3312	Overcurrent Protection Restored
YP	1319	Overvoltage Protection Triggered
YQ	3319	Overvoltage Protection Restored
AI	1333	Expander Exception
CQ	3333	Expander Restored
AJ	1336	Printer Disconnected
CR	3336	Printer Connected
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
		Expander Low Voltage
		Normal Expander Voltage
YP	1301	Mains Power Lost
YQ	3301	Mains Power Restored
YM	1311	Battery Disconnected
YR	3311	Battery Reconnected
TA (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1144 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Lid Opened
TR (The serial number of output module starts from 1,	3144 (The serial number of output module starts from 1,	Lid Restored

SIA Code	CID Code	Description
of keypad starts from 101, of tag reader starts from 201)	of keypad starts from 101, of tag reader starts from 201)	
YP transmitter AC power down ID range: 301~	1301 transmitter AC power down ID range: 301~	Expander AC Power Loss
YQ transmitter AC power down ID range: 301~	3301 transmitter AC power down ID range: 301~	Expander AC Power Loss Restored
TA	1144	Lid Opened
TR	3144	Lid Restored
TA	1144	Lid Opened
TR	3144	Lid Restored
XL	1381	Device Offline
XC	3381	Device Restored
TA (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	1144 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Lid Opened
TR (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	3144 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Lid Restored
XT (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	1384 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Battery Low
XR (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	3384 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Battery Voltage Restored
XL (The serial number of output module starts from 1,	1381 (The serial number of output module starts from 1,	Device Offline

SIA Code	CID Code	Description
of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	
XC (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	3381 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Device Restored
LT	1351	Main Signalling Path Fault
LR	3351	Main Signalling Path Restored
LT	1352	Backup Signalling Path Fault
LR	3352	Backup Signalling Path Restored
AM	1354	Telephone Line Disconnected
CU	3354	Telephone Line Connected
AN	1382	BUS Supervision Fault
CV	3382	BUS Supervision Restored
TA	1144	Lid Opened
TR	3144	Lid Restored
		Zone Open-circuit Alarm
		Zone Short-circuit Alarm
OP	1401	Disarmed
CL	3401	Armed
OA	1403	Auto Disarmed
CA	3403	Auto Armed
BC	1406	Alarm Silenced
CW	3408	Instant Arming
CS	1409	Keyswitch Zone Disarming
OS	3409	Keyswitch Zone Arming
NL	3441	Armed in home mode
CX	3442	Forced Arming
		Turn On Output by Schedule

SIA Code	CID Code	Description
		Turn Off Output by Schedule
CT	1452	Late to Disarm
CD	1455	Auto Arming Failed
		Turning On Output Failed
		Turning Off Output Failed
		Auto Disarming Failed
		Network Change
QB	1570	Bypassed
QU	3570	Bypass Restored
AU	1574	Group Bypass
CZ	2574	Group Bypass Restored
AV	1601	Manual Report Test
RP	1602	Periodic Report Test
TS	1607	Walk Test Enabled
TE	3607	Walk Test Disabled
AW	1617	Telephone Connection Test
LB	1627	Programming mode
LX	1628	Exit Programming
BA	1131	Intrusion Detection
BH	3131	Intrusion Detection Restored
BA	1131	Cross-Zone Alarm
BH	3131	Cross-Zone Alarm Restored
		PIR Alarm
		PIR Alarm Restored
AY	1775	Sudden Increase of Sound Intensity Alarm
DE	3775	Sudden Increase of Sound Intensity Alarm Restored
AZ	1776	Sudden Decrease of Sound Intensity Alarm
DF	3776	Sudden Decrease of Sound Intensity Alarm Restored

SIA Code	CID Code	Description
		Audio Input Fault
		Audio Input Restored
BA	1131	Line Crossing Alarm
BH	3131	Line Crossing Alarm Restored
BA	1134	Region Entrance Detection
EA	1134	Alarm Restored
FA	1112	Fire Source Alarm
FH	3112	Fire Source Alarm Restored
KS	1158	High Temperature Pre-Alarm
KR	3158	High Temperature Pre-Alarm Restored
ZS	1159	Low Temperature Pre-Alarm
ZR	3159	Low Temperature Pre-Alarm Restored
KA	1158	High Temperature Alarm
KH	3158	High Temperature Alarm Restored
ZA	1159	Low Temperature Alarm
ZH	3159	Low Temperature Alarm Restored
EA	1134	Region Exiting Detection
PA (The user No. of keypad starts from 101, of keyfob starts from 901)	1120 (The user No. of keypad starts from 101, of keyfob starts from 901)	Audible Panic Alarm
FA	1110	Keypad/Keyfob Fire Alarm
		Keypad/Keyfob Burglary Alarm
CI	1454	Arming Failed
MA	1100	Keypad/Keyfob Medical Alarm
DK	1501	Keypad Locked
DO	3501	Keypad Unlocked
		Absence Alarm
BE	1910	Keypad Disconnected
DH	3910	Keypad Connected

SIA Code	CID Code	Description
BF	1911	KBUS Relay Disconnected
DI	3911	KBUS Relay Connected
		KBUS GP/K Disconnected
		KBUS GP/K Connected
		KBUS MN/K Disconnected
		KBUS MN/K Connected
DK	1501	Tag Reader Locked
DO	3501	Tag Reader Unlocked
BD	1865	Unregistered Tag
XL	1381	Device Offline
XC	3381	Device Restored
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
XL (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	1381 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Offline
XC (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	3381 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201)	Device Restored
XL	1381	Device Offline
XC	3381	Device Restored
BI	1918	Radar Transmitter Fault
DL	3918	Radar Transmitter Restored
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
NT	1350	Cellular Fault
NR	3350	Cellular Restored
NT	1350	SIM Card Exception
NR	3350	SIM Card Restored
NT	1350	Network Fault
NR	3350	Network Restored

SIA Code	CID Code	Description
XQ	1344	Jamming Detected
XH	3344	Jamming Restored
NT	1350	Data limitation Reached
XT	1384	Battery Low
XR	3384	Battery Voltage Restored
NT	1350	IP Address Already Used
NR	3350	Normal IP address
NT	1350	Network Fault
NR	3350	Network Restored
BA	1131	Motion Detection Alarm Started
BH	3131	Motion Detection Alarm Stopped
BJ	1941	Device Blocked
DM	3941	Device Blocking Alarm Restored
		Video Signal Loss
		Video Signal Restored
		Input/Output Format Unmatched
		Input/Output Format Restored
		Video Input Exception
		Video Input Restored
		Full HDD
		Free HDD
		HDD Exception
		HDD Restored
		Upload Picture Failed
BQ	1948	Email Sending Failed
BR	1949	Network Camera Disconnected
DS	3949	Network Camera Connected
		Duty Checking
		Post Response
BU	1962	Fire Alarm Consulting

SIA Code	CID Code	Description
DT	3962	Fire Alarm Consulting Over
BV	1963	Duress Alarm Consulting
DU	3963	Duress Alarm Consulting Over
BW	1964	Emergency Medical Alarm Consulting
DV	3964	Emergency Medical Alarm Consulting Over
DW	3250	Patrol Signing
BX	1970	BUS Query
BY	1971	BUS Registration
BZ	1973	Single-Zone Disarming
DX	3973	Single-Zone Arming
CA	1974	Single-Zone Alarm Cleared
CB	1306	Device Deleted
DY	3306	Device Enrolled
CC	1976	Business Consulting
DZ	3976	Business Consulting Over
CD	1306	Device Deleted
EA	3306	Device Enrolled
CE	1306	Device Deleted
EB	3306	Device Enrolled
CF	1306	Device Deleted
EC	3306	Device Enrolled
CG	1306 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Device Deleted
ED	3306 (The serial number of output module starts from 1, of keypad starts from 101, of tag reader starts from 201, of transmitter starts from 301)	Device Enrolled

SIA Code	CID Code	Description
JA	1461	Incorrect Password
NT	1350	Device Offline
YM	1311	Power Depletion

H. Communication Matrix and Operation Command

Please scan the OR code for communication matrix and operation command

AXPRO Communication Matrix

AXPRO Operation Command

User Privacy Statement

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

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

User Privacy Information Description

Password	The password for the device account, used to log in to the device.
Username	The username for the device account, used to log in to the device.
Device IP and port	The device IP and port are used to support network service communication. For details, refer to *Communication Matrix*.
Log	Used to record information such as device operating status and operation records.
Database information	Used to record information.