AX Security Control Panel

User Manual

UD11739B

Legal Information

User Manual

About this Manual

Please use this user manual under the guidance of professionals.

Trademarks

Disclaimer

Symbol Conventions

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

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

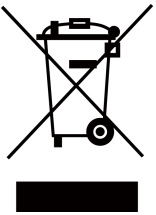
Regulatory Information

EN 50131-1:2009+A2:2017
EN 50131-3:2009
EN 50131-6:2017
EN 50131-5-3:2017
Security Grade: 2
Environmental Class: II

EU Conformity Statement

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

Contents

1 Installation Guide

1.1 Overview

1.1.1 System Description

AX wireless security control panel, containing 32 wireless zones, supports Wi-Fi, TCP/IP, and 3G/4G communication methods. It also supports ISAPI, Hik-Connect, DC09, and NAL2300, which is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- TCP/IP, Wi-Fi, and 3G/4G network
- Connects up to 32 wireless zones, 32 wireless outputs, 8 wireless keyfobs, 4 relays, 2 repeaters, and 2 sirens
- Supports up to 13 network users, including 1 installer, 1 administrator, 1 manufacturer, and 10 normal users
- Supports doorbell function: The detector rings like a doorbell when it is triggered in disarming status
- Voice prompt
- Wi-Fi settings in AP mode
- Configuration via Web client or mobile client
- Pushes alarm notification via messages or phone calls

Note

Only device containing 3G/4G communication method supports this function

- Views live videos and sends emails of alarm linked videos via mobile client
- Uploads reports to alarm center
- Long distance two-way communication with AES-128 encryption
- Supports LED indicator to indicates system status
- 4520 mAh lithium backup battery, supports up to 12 h power supply
- SIA-Contact ID protocol compatible

Note

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

1.1.2 Specification

DS-PW32-H(R)(S)(G)		
Wireless Device Connection	Alarm Input	32
	Alarm Output	32
	Siren	2
	Keyfob	8
	Partition	1

DS-PW32-H(R)(S)(G)		
Interaction	Audio Output	1, 1.5W
RF	RF Frequency	433/868MHz (depends on the model)
	RF Modulation	2GFSK
	RF Distance	800m (Open Area)
Wired Network	Ethernet	10M/100M Self-adaptive
Cellular Network	GPRS, 3/4G	Supports reporting push-notification to ARC & Cloud, text notification via SMS, and audio notification via phone call
Wi-Fi	Standard	802.11b/g/n
	Encryption	Supported
	Channel	2.4 G
Application & Protocol	Application	iVMS-4200, and mobile APP
	Protocol	SIA - Contact ID
User	IC Card	12
	User	13 (1 installer, 1 administrator, 1 manufacturer, and 10 general users)
Others	Power	5 VDC, 10 W
	Consumption (without HDD)	< 5.6 W
	Operation Temperature	–10 °C to 55 °C
	Operation Humidity	10% to 90%
	Shell Material	PC+ABS
	Dimension(WxHxD)	155 × 155 × 35mm
	Battery Power Supply	12 H

1.2 Appearance

Front Panel

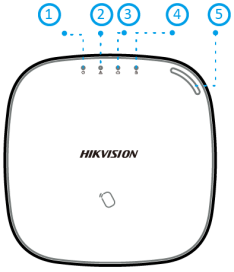


Figure 1-1 Front Panel

Table 1-1 Front Panel Description

No.	Indicator Name	Description
1	AC Power	Solid Green: Power on Off: Power off
2	Fault	Solid Orange: System disarmed Off: System armed **Note** You can set to indicate fault when arming * in the web client. *Not compliant the EN requirement.
3	Link	Solid Green: The panel is bound to Hik-connect account Off: The panel is not bound to Hik-connect account
4	Arm/Disarm	Solid Blue for 5 s: Armed **Note** You can set the arming indicator continuously on* when armed in the web client. *Not compliant the EN requirement. Off: Disarmed
5	Alarm	Flashing Red: Alarm Occurred Solid Red: Device Tampered Off: No Alarm

Component and Interface

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

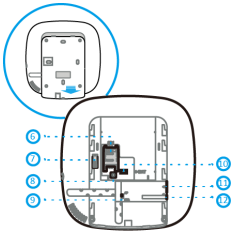


Figure 1-2 Component and Interface

Table 1-2 Rear Panel Description

Number	Description
6	SIM Card Slot **Note** The function of GPRS or 3G/4G (implemented with built-in SIM card slot) varies depends on the model of the device.
7	TAMPER
8	Reset Button
9	AP&STA Switch
10	Battery Connector
11	Network Interface
12	Power Interface

Function Button

The function button is on the side of the control panel.

Figure 1-3 Function Button

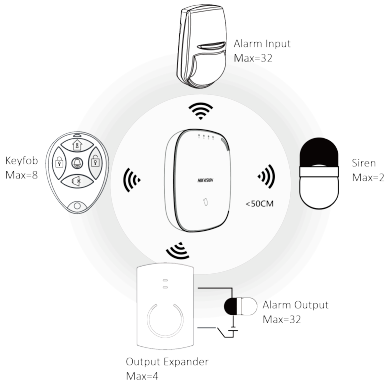
Use the function button to add wireless devices and check the RF signal.

1.3 Connection

You can connect peripheral device to the control panel loccally, via client software, web client, or mobile clien.

Note

Check the RF signal strentch before connection and peripheral device installation.While the control panel is not in the configuration mode, double press the function button, and trigger the wireless device (event alarm or tampering alarm). you can view the RF signal strength indication on the peripheral device.



Connect Locally

Note

Add card or keyfob via the web client before adding peripheral device for clearing tampering alarm.

While the control panel is not in the configuration mode, press the function button on the side of the control panel once and trigger a peripheral device.

Connect via Client Software

Add a control panel to the client software.

In the client software, click **Device Management → Remote Configuration → Wireless Device** . Select a zone/relay/siren and enter the **Settings** page. Input the device serial No. for connection.

Note

for details, refer to the chapter of *Configuration-Configure via Web Client-Alarm Settings*.

Connect via Web Client

In the web client, click **Wireless Device** . Select a zone/relay/siren and enter the **Settings** page. Input the device serial No. for connection.

Note

for details, refer to the chapter of *Configuration-Configure via Web Client-Alarm Settings*.

Connect via Mobile Client

Add a control panel to the mobile client.

On the control panel settings page, Click **+**, scan the QR code on the wirless device or enter the serial No. of the device.

Note

for details, refer to the chapter of*Configuration-Configuration via Mobile Client-Add Peripheral to the Control Panel.*

1.4 Installation

Steps

1. Loosen the screw on the rear cover. Slide down the rear cover and remove it from the control panel.

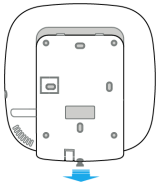


Figure 1-4 Remove the Rear Cover

2. Insert a SIM card into the SIM card slot.

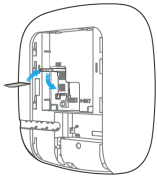


Figure 1-5 Insert SIM Card

3. Connect the battery to the control panel.

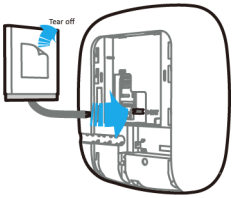


Figure 1-6 Connect the Battery

4. Connect the power adapter to the control panel and a power outlet. The power indicator turns green after about 30 s, which means that the device is powered on.

Note

The condition of no SIM card, no battery, AC power off, or network disconnected, will cause Control Panel Fault.

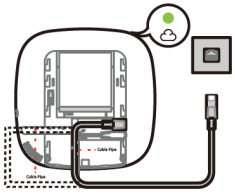


Figure 1-7 Power On

5. Connect the Ethernet cable to an internet outlet. While the device is added to a Hik-Connect account, the Link indicator turns green.

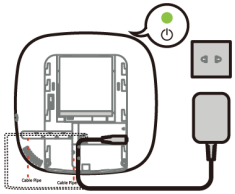


Figure 1-8 Connect to the Ethernet

6. Secure the rear cover to the installation position with the supplied screws. Attach the control panel on the rear cover, and tighten the rear cover screw to complete the installation.

Figure 1-9 Complete the Installation

Note

- Blue Star: Side Opening. If you need to route the cable though the botton of the panel, remove the sheet of the side opening.
- Red Star: TAMPER Screw. It is compulsory to secure the TAMPER screw.

1.5 Activation

In order to protect personal security and privacy and improve the network security level, you should activate the device the first time you connect the device to a network.

You can create an activation password to protect your device from logging in by other persons.

1.5.1 Activate Device via Web Browser

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

Before You Start

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

Steps

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

Note

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

2. Create and confirm the admin password.

Caution

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

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

4. Edit IP address of the device.

1) Enter IP address modification page. **Configuration → Network → TCP/IP**

2) Change IP address.

3) Save the settings.

1.5.2 Activate Device via iVMS-4200

is a PC client to manage and operate your devices. Security control panel activation is supported by the software.

Before You Start

- Get the client software from the supplied disk or the official website ***http://www.hikvision.com/en/*** . Install the software by following the prompts.
- The device and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.

2. Enter **Device Management** or **Online Device**.

3. Check the device status from the device list, and select an inactive device.

4. Click **Activate**.

5. Create and confirm the admin password of the device.

Caution

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

6. Click **OK** to start activation.

Device status will change to **Active** after successful activation.

7. Edit IP address of the device.

1) Select a device and click **Modify Netinfo** at **Online Device**.

2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.

3) Input the admin password of the device and click **OK** to complete modification.

1.5.3 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.

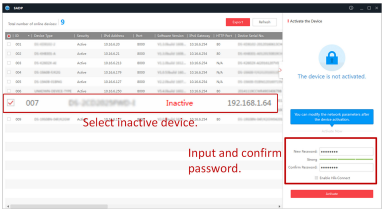
2. Find and select your device in online device list.

3. Input new password (admin password) and confirm the password.

Caution

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

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

1) Select the device.

2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.

3) Input the admin password and click **Modify** to activate your IP address modification.

1.6 Configuration

Configure the security control panel in the web client or the remote configuration page in client software.

1.6.1 Use the Client Software

Steps

1. Download, install and register to the client software.
2. Add device in **Control Panel → Device Management → Device** .

Note

Set the device port No. as 80.

Note

The user name and password when adding device are the activation user name and password.

3. Click Remote Configuration to enter the device configuration page after the device is completely added,

1.6.2 Use the Web Client

Steps

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

Note

When using mobile broswer, the default IP Address is 192.168.8.1. The device must be in the AP mode.

Note

When connectiing the network cable with computer directly, the default IP Address is 192.0.0.64

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

Note

Refer to *Activation* chapter for the details.

Network Settings

Wired Network

If the device is linked to the wired network, you can set the wired network parameters when you want to change the device IP address and other network parameters.

Steps

Note

The function is not supported by some device models.

1. In iVMS-4200 client software, enter the Device Management page.

2. Select the radar in the Device for Management list, click **Remote Configuration**.

3. Click **Communication Parameters → Wired Network Parameters** to enter the Wired Network Parameters page.

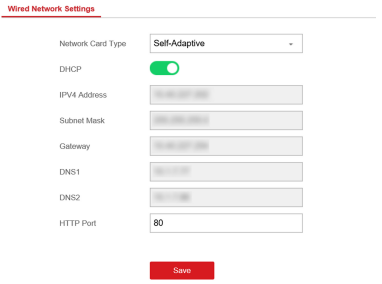


Figure 1-10 Wired Network Settings Page

4. 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**.

Note

By default, the HTTP port is 80, which is not editable.

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

6. Click **Save**.

Wi-Fi

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

Steps

1. Click **Communication Parameters → Wi-Fi Parameters** .

2. Click **Wi-Fi** to enter the Wi-Fi page.

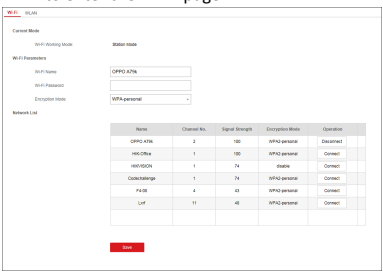


Figure 1-11 Wi-Fi Settings Page

3. Connect to a Wi-Fi.
   - Manually Connect: Input the Wi-Fi name and the Wi-Fi password, 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**.

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

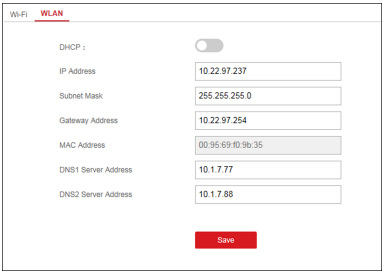


Figure 1-12 WLAN Settings Page

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

Note

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

6. Click **Save**.

Cellular Network

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

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

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

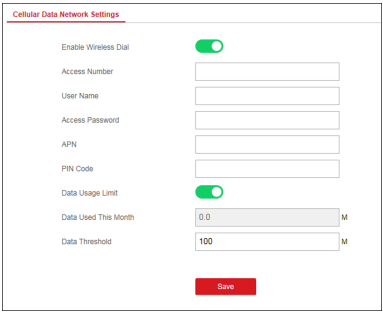


Figure 1-13 Cellular Data Network Settings Page

2. Enable Wireless Dial.
3. Set the cellular data network parameters.

Access Number

Input the operator dialing 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.

Data Used This Month

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

4. Click **Save**.

Hik-Connect

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

Before You Start

- Connect the device to the network via wired connection, dial-up connection, or Wi-Fi connection.
- Set the device IP address, subnet mask, gateway and DNS server in the LAN.

Steps

1. Click **Communication Parameters → Hik-Connect Registration Parameters** to enter the Hik-Connect Registration Settings page.

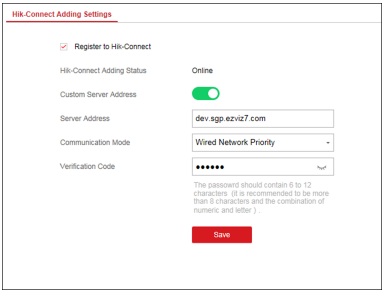


Figure 1-14 Hik-Connect Registration Settings Page

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

Note

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

You can view the device status that in the Hik-Connect server.

3. Enable **Custom Server Address**.

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

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

Auto

The system will select the communication mode automatically according to the sequence of wired network,

Wi-Fi network, and cellular data network. Only when the current network is disconnected, will the device connect to other network.

Wired Network Priority

The system will select wired network only.

Note

When the device supports cellular data network connection and the wired network is disconnected, it will connect to the cellular data network. When the wired network is restored, only if the cellular data network is disconnected, does the device connect to the wired 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 authentication password.

Note

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

6. Click **Save**.

EHome

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

Steps

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

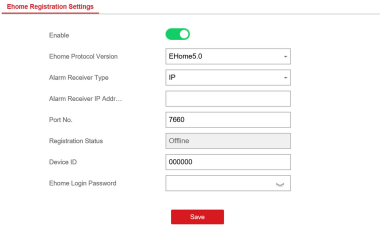


Figure 1-15 EHome Registeration

2. Slide the slider to enable EHome protocol.
3. Select the **Alarm Receiver Type** as **IP** or **Domain Name**.
4. Input IP address or domain name according to the alarm receiver type.
5. Input the port number for the protocol.

Note

By default, the port number for EHome is 7660.

6. Set an account, including the **Device ID** and **Ehome Login Password**.
7. Click **Save**.

Alarm Settings

Alarm Center

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

Steps

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

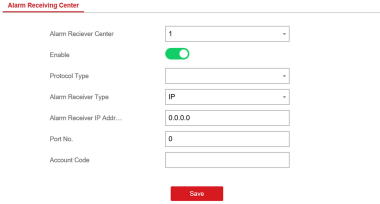


Figure 1-16 Alarm Receiving Center Parameters

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

Note

You can enable the **backup channel** when the **Alarm Receiver Center** is selected as **2**.

3. Select the **Protocol Type** as **ADM-CID**, **EHome**, **SIA-DCS**, ***SIA-DCS**, or ***ADM-CID** to set uploading mode.
   - **ADM-CID** or **SIA-DCS**

     You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, timeout, re-upload times and heartbeat interval.

     Note

     You should check **Enable** on the right of Heartbeat Interval line to edit the heartbeat interval.
   - **EHome**

     You do not need to set the EHome protocol parameters.
   - ***SIA-DCS** or ***ADM-CID**

     You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, timeout, re-upload times, heartbeat interval, encryption arithmetic, password length and secret key.

     Note

     You should check **Enable** on the right of Heartbeat Interval line to edit the heartbeat interval.
4. Click **Save**.

Notification Push

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

Steps

1. Click **Communication Parameters → Message Notification** .
2. Enable the target notification.

   Alarm and Tampering Event Notification

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

   Safety Event Notification

   The device will push notifications when fire alarm, gas alarm, or medical alarm is triggered.

   System Status Notification

   The device will push notifications when any status in the system is changed.

   Operation Event Notification

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

Note

If you want to send the alarm notifications to the mobile client, you should also set the **Mobile Phone Index**, **SIM Card No.**, and check the **Notification Type**.

Note

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

3. Click **Save**.

Zone

You can set the zone parameters on the zone page.

Steps

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

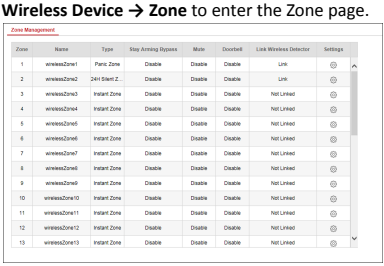


Figure 1-17 Zone Page

2. Select a zone and click ⚙ to enter the Zone Settings page.
3. Edit the zone name.
4. Select a zone type.

   Instant Zone

The system will immediately trigger an alarm when it detects triggering event after system armed. Detectors can be set as this type, which can be used in places such as supermarket.

Delayed Zone

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

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

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

Note

You can set the delayed time duration in **System → Schedule & Timer** .

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. It is usually set in the living room or hall with perimeter delayed zones at the same time.

Perimeter Zone

The system will immediately alarm when it detects triggering event after system armed. There is a configurable interval between alarm and siren output, which allows you to check the alarm and cancel the siren output during the interval time in case of false alarm. It is usually used in the perimeter area, such as doors and windows.

When the zone is armed, you can set the peripheral alarm delayed time in **System → Schedule & Timer** . You can also mute the siren in the delayed time.

24H Silent Zone

The zone activates all the time without any sound/siren output when alarm occurs. It is usually used in the sites equipped with panic button (e.g., bank, jewelry store).

Panic Zone

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

Fire Zone

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

Combustible Gas Zone

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

Medical Zone

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

Timeout Zone

The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. It is usually used in places equipped with magnetic contacts (e.g., fire hydrant box's door).

Shield Zone

Alarms will not be activated when the zone is triggered or tampered. It is usually used to disable faulty detectors .

5. Enable **Stay Arming Bypass**, **Doorbell**, or **Mute** according to your actual needs.

Note

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

6. Enable **Link Wireless Detector** , input the serial No., and set the linked camera No.

Note

868 Devices do not support inputting serial No.

7. Click **OK**.

Note

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

Alarm Schedule

You can set the delayed time duration for the delayed zone and the delayed time to exit the zone. You can also set the alarm schedule. The zone will be armed/disarmed according to the configured time schedule.

Steps

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

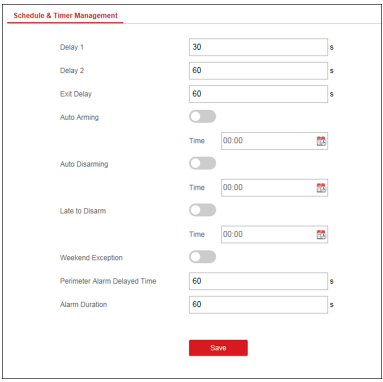


Figure 1-18 Schedule & Timer Page

2. Set time duration of **Delay 1**, **Delay 2**, or **Exit Delay** respectively.

Delay 1/Delay 2

If you have set the delayed zone, you can set the delayed time duration here.

Note

The available time duration rage is from 5s to 600s.

Exit Delay

If the you want to exit the zone without triggering the alarm, you can set the exit delay duration.

Note

The available time duration rage is from 5 s to 600 s.

3. **Optional:** Set the following parameters according to actual needs.

Auto Arming

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.

Auto Disarming

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 Operation Event Notification function in **Communication Parameters → Message Notification** before enabling the Late to Disarm function.

Weekend Exception

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

Perimeter Alarm Delayed Time

If you have set the perimeter zone, you can set the delayed time for the zone.

Note

The available time duration range is from 0 s to 600 s.

Alarm Duration

Set the time duration of the alarm.

Note

The available time duration range is from 5 s to 600 s.

4. Click **Save**.

Output

If you want to the link the device with a relay output to output the alarm, set the output parameters.

Steps

1. Click **Wireless Device → Output** to enter the Output page.

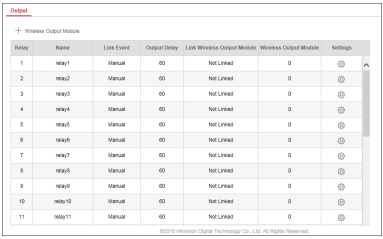


Figure 1-19 Output Page

2. Add a wireless output module.

1) Click **Wireless Output Module**.

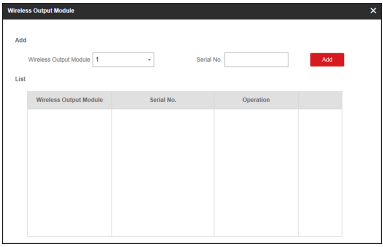


Figure 1-20 Wireless Output Module Settings

2) Select a wireless output module number from the drop-down list.

3) Input the serial No. of the wireless output module.

4) Click **Add**.

3. Click ⚙ and the Relay Settings window will pop up.

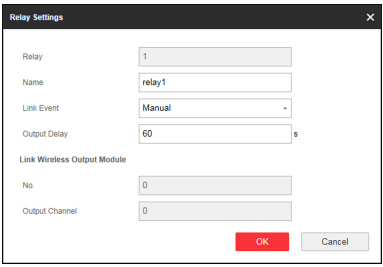


Figure 1-21 Relay Settings Page

4. Edit the relay name, select a link event, and set the output delay time duration.

Note

If the relay has linked to the wireless output module, the wireless output module information will be displayed in the Link Wireless Output Module area.

5. Click **OK**.

Note

After the relay is configured, you can click **Status → Relay** to view the output status.

Siren

If you want to link the security control panel to a siren to report an alarm when the alarm is triggered, you can set the siren parameters.

Steps

1. Click **Wireless Device → Siren** to enter the Siren page.

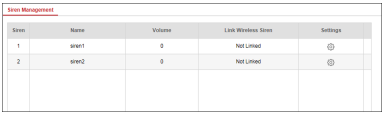


Figure 1-22 Siren Page

2. Click ⚙ to enter the Siren Settings page.
3. Set the siren name and the volume.

Note

The available siren volume range is from 0 to 3.

4. **Optional:** Enable **Link Wireless Siren** and set the siren serial No.

Note

Some detectors may not support this function.

5. Click **OK**.

Note

After the siren is configured, you can click **Status → Siren** to view the siren status.

Repeater

If the detector is far away from the control panel, set the repeater parameters to enlarge the signal.

Steps

1. Click **Wireless Device → Repeater** to enter the Repeater page.

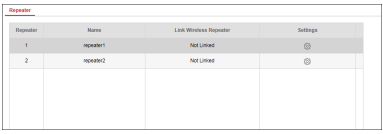


Figure 1-23 Repeater Page

2. Click ⚙ to set the repeater parameters.

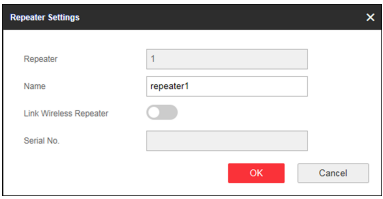


Figure 1-24 Repeater Settings

3. Edit the repeater's name.
4. Enable **Link Wireless Repeater** and input the repeater serial No.
5. Click **OK**.

Note

After setting the repeater, you can enter **Status → Repeater** to view the repeater status.

Video Management

You can add two network cameras to the wireless security control panel, 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 Security Control Panel

Steps

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

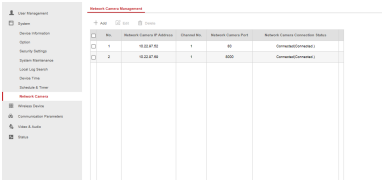


Figure 1-25 Network Camera Management

2. Click**Add**, and enter the basic information of the camera, such as camera name, IP address, and port No..
3. Enter the user name and password of the camera.
4. Click **Save**.

Note

You can add two network cameras for a wireless securty control panel.

1. **Optional:** Click**Edit**or**Delete**to edit or delete the selected camera.

Link a Camera with the Zone

Steps

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

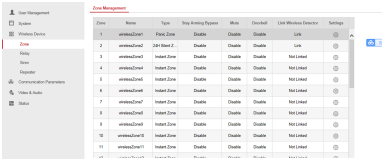


Figure 1-26 Zone Management

2. Select a zone needs video monitoring, and click the **Settings**icon.

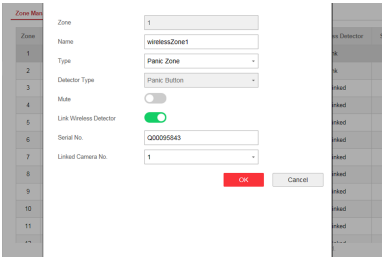


Figure 1-27 Zone Configuration

3. Select the **Linked Camera No.**.

4. Click**OK**.

Set Email to Receive Alarm Video

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

Steps

1. Click **Communication Parameters → Event Video Transfer via Email** to enter the page.

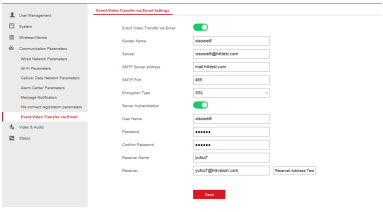


Figure 1-28 Event Video Transfer via Email

2. Click the block to enable the function.

3. Enter the sender's information.

4. Enter the receiver's information.

5. Click **Receiver Address Test** and make sure the address is correct.

6. Click **Save**.

Set Video Parameters

Steps

1. Click **Video & Audio → Event Video Parameters** to enter the page.

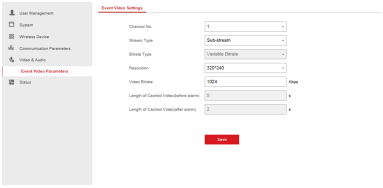


Figure 1-29 Video Settings

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.

Note

For network camera supporting sub-stream, SMS video uses sub-stream, and the configuration of main stream will not effect on the SMS video.

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.

Permission Management

Add/Edit/Delete User

Administrator can add user to the security control panel, edit the user information, or delete the user from the security control panel. You can also assign different permissions to the new user.

Steps

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

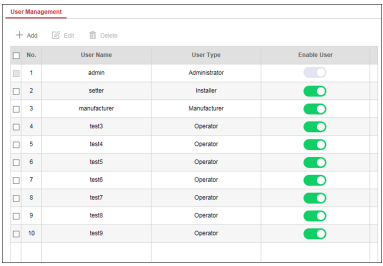


Figure 1-30 User Management Page

2. To compliant the EN requirement, slide the block to enable the setter and manufactuer .

Note

The default password of the setter is **setter12345**, and the default password of the manufactuer is **hik12345**.

3. Click **Add**.
4. Set the new user's information in the pop-up window, including the user type, the user name, and the password.

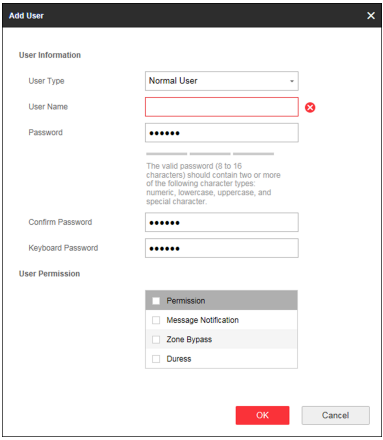


Figure 1-31 Add User Page

5. Check the checkboxes to set the user permission.

   The user can only operate the assigned permissions.

6. Click **OK**.
7. **Optional:** Enable the user in the Enable User column to allow the enabled user operating the device.
8. **Optional:** Select an user and click **Edit** and you can edit the user's information and permission.
9. **Optional:** Delete a single user or check multiple users and click **Delete** to delete users in batch.

Note

The admin and the setter cannot be deleted.

Add/Edit/Delete Card

You can add card to the security control panel and you can use the card to arm/disarm the zone. You can also edit the card information or delete the card from the security control panel.

Steps

1. Click **User Management → Card** to enter the Card Management page.

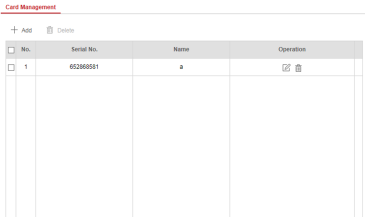


Figure 1-32 Card Management

2. Click **Add** and place a card on the card swiping area.
3. Customize a name for the card in the pop-up window.
4. Click **OK** and the card information will be displayed in the list.
5. **Optional:** Click and you can change the card name.
6. **Optional:** Delete a single card or check multiple cards and click **Delete** to delete cards in batch.

Add/Edit/Delete Keyfob

You can add keyfob to the security control panel and you can control the security control panel via the keyfob. You can also edit the keyfob information or delete the keyfob from the security control panel.

Steps

1. Click **User Management → Keyfob** to enter the Keyfob Management page.

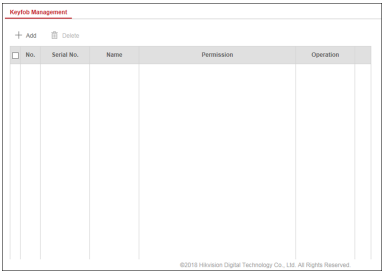


Figure 1-33 Keyfob Management

2. Click **Add** and press any key on the keyfob.
3. Set the keyfob parameters.

   Name

   Customize a name for the keyfob.

   Permission Settings

   Check different items to assign permissions.

   Single Key Settings

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

   Combination Keys Settings

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

4. Click **OK**.

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

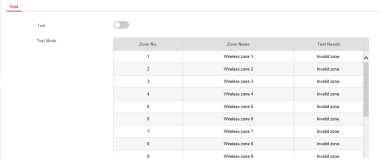
Maintenance

Test

The security control panel supports walk test function.

Steps

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



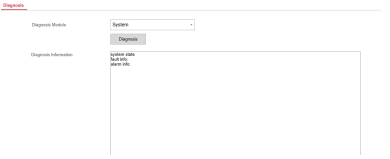
2. Check the **Test** check box to start walk test.
3. Trigger the detector in each zone.
4. Check the test result.

Diagnosis

The control panel supports diagnosis of system, alarm, wireless device, Wi-Fi, and cloud flatform

Steps

1. Enter **Maintenance → Diagnosis** .



2. Select system, alarm, wireless device, Wi-Fi, or cloud platform as the diagnosis module.
3. Click **Diagnosis** to start the operation.
4. View the diagnosis result in the information box.

System Settings

Authority Management

Set the authority options.

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

Set the following parameters as you desired.

Wireless Device Supervision

If the option is enabled, the system will detect the peripheral's heartbeat. If no peripheral's heartbeat detected, the system will upload an event.

Forced Arming

If the option is enabled and there's faults occurred in the zone, the zone will be bypassed automatically and then armed again.

Note

You should disable the arming function in the Advanced Settings page. Or the forced arming function cannot be valid.

System Fault Report

If the option is enabled, the device will upload the system fault report automatically.

Disable Function Key

If the option is enabled, all function keys will be disabled.

Detect Network Camera Disconnection

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

Battery Supervision

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

System Volume

The available system volume range is from 0 to 10.

Time Settings

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

Time Management

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

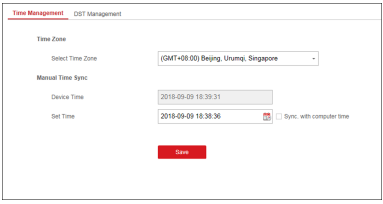


Figure 1-34 Time Management

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

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

DST Management

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

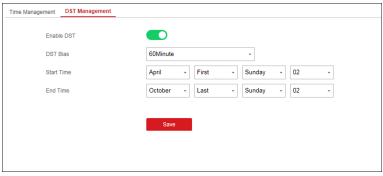


Figure 1-35 DST Management

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

SSH Settings

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

Click **System → Security → SSH Settings** to enter the SSH Settings page and you can enable or disable the SSH function.

Card Reader Lock Settings

Set the card reader locking parameters, including the max. failure attempts, and locked duration. The card reader will be locked after the card authentication failed for the configured times.

Steps

1. Click **System → Security → Card Reader Lock Settings** to enter the Card Reader Lock Settings page.
2. Set the following parameters.
   Max. Failure Attempts

   If the user continuously authentication failed for more than the configured times, the card readers will be locked.

   Locked Duration

   Set the locking duration when the card reader is locked. After the configured duration, the card reader will be unlocked.
3. Click **Save**.

Locking User Settings

Set user locking. You can view the locked user or unlock a user and set the user locked duration.

Steps

1. Click **System → Security → Locking User Settings** to enter the Locking User Settings page.
2. Set the following parameters.
   Max. Failure Attempts

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

   Note

   The administrator has two more attempts than the configured value.

   Locked Duration

   Set the locking duration when the account is locked.

   Note

   The available locking duration is 5s to 1800s.
3. Click 🔓 to unlock the account or click **Unlock All** to unlock all locked users in the list.
4. Click **Save**.

System Maintenance

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

Select the device and click **Remote Configuration** in iVMS-4200, or enter the device IP address in the address bar of the web browser. Click **System → System Maintenance** to enter the Upgrade and Maintenance page.

Figure 1-36 System Maintenance

Restart

Click **Reboot** to reboot the device.

Restore Default Settings

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

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

Import Parameters

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

Export Parameters

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

Upgrade File

Click **View** to select an upgrade file from the PC and click **Upgrade** to upgrade the device remotely.

Note

Do not power off when the device is upgrading.

Certificate Standard

Click **System → System Maintenance → Certificate Standard** to enter the certificate standard settings page.

You can switch between **EN Standard** and **General Standard** mode.

The device applies EN Standard by default.

Note

When you select **EN Standard**, the user permission and arming parameters will conform to the EN Standard.

Local Log Search

You can search the log on the device.

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

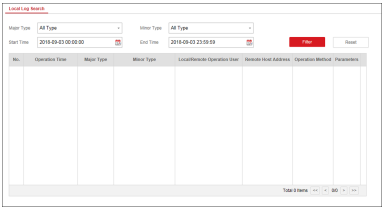


Figure 1-37 Local Log Search Page

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

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

Authority Advanced Settings

Set advanced authority parameters.

Click **System → Authority Management → Advanced Settings** to enter the Advanced Settings page.

You can set the following parameters:

Enable Arming

When you enable the function, during the device arming procedure, the system will check the configured fault checklist. When there is fault occurred during the arming procedure, the procedure will be stopped.

Fault Checklist

The system will check the checked faults in the fault checklist. The system will check the checked faults in the fault checklist during the arming procedure.

Enable Arming with Fault

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

Arming Indicator Keeps Light

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

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

Prompt Fault When Arming

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

Enable Early Alarm

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

Note

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

Delay

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

Check Status

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

Click **Status**. You can view the status of zone, relay, siren, battery, communication, and repeater.

- Zone: You can view the zone status, alarm status, detector battery capacity, and signal strength.
- Siren: You can view siren status, battery status, and signal strength.
- Relay: You can view relay status, battery status, and signal strength.
- Battery: You can view the battery charge.
- Communication: You can view the wired network mode, Wi-Fi status, Wi-Fi signal strength, cellular network status, used data, and cloud connection status.

1.6.3 Configuration via Mobile Client

Download and Login the Mobile Client

Download the Hik-Connect mobile client from Google Play (for Android) or App store (for iOS) and login the client before operating the security control panel.

Steps

1. Search and download Hik-Connect mobile client from Google Play (for Android) or App Store (for iOS).
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 Control Panel to the Mobile Client

Add a control panel to the mobile client before other operations.

Steps

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

     Note

     Normally, the QR code is printed on the label sticked on the back cover of the control panel.
   - Tap → **Manual Adding** to enter the Add Device page. Input the device serial No. with the Hik-Connect Domain adding type.
3. Connect to a network.

   1) Tap **Connect to a Network**.

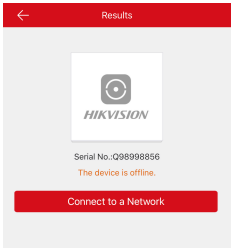


Figure 1-38 Connect to a Network Page

2) Tap **Wireless Connect** on the Select Connection Type page.

3) Follow the instructions on the Turn on Hotspot page and change the control panel to the AP mode. Tap **Next**.

Note

You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

4) Select a stable Wi-Fi for the device to connect and tap **Next**.

Note

Make sure the device and the mobile phone are connect to the same Wi-Fi.

4. Follow the instructions on the Device's Wi-Fi page and connect the mobile phone with the control panel via wireless connection.

Note

Select **HAP-Device Serial No.** as the hotspot and enter the hotspot password. By default, the password is ***AP + Device Verification Code***. The verification code is normally printed on the device label.

5. Return to the mobile client and create a device password for device activation.

Note

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

6. Optional: If you add the control panel by entering its serial No., you should enter the device verification code and tap **OK**.

Note

By default, the verification code is printed on the device label.

7. Follow the instructions and change the control panel to the Station mode. Tap **Next**.

Note

You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

8. When the control panel is adding completed, tap **Finish**.

   The control panel is listed on the Hik-Connect page.

AddPeripheral to the Control Panel

It is required to enter the activation name and the password login the control panel after it being added.

Before You Start

Make sure the control panel is disarmed.

Steps

Note

Some control panel models do not support add zones or wireless devices remotely. You should add them to the control panel directly. For details, see the user manual of the wireless device.

1. Tap to enter the Scan QR Code page.
2. Scan the peripheral's QR code to add the peripheral.
3. Select a peripheral type, and create a name for the peripheral.

Note

- When the adding peripheral is a detector, the detector will be linked to the zone. You can view the detector information in the Zone tab.
- Up to 32 detectors can be linked to the zone.

The added peripheral will be listed in the Zone tab or the Wireless Device tab.

Set Zone

After the detector is added, you can set the zone, including the zone name, the zone type, zone bypass, linked camera, stay/away status, the siren, and the silent zone. You can also view the detector serial No. and the detector type of the zone.

Steps

1. Tap a zone in the Partition page to enter the zone settings page.

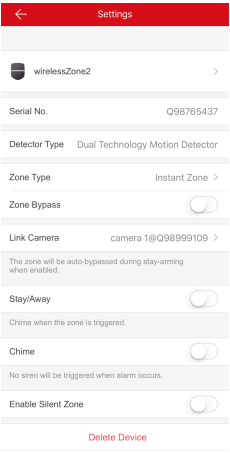


Figure 1-39 Zone Settings Page

2. Set the following parameters as you desired.

Zone Type

Select a zone type from the zone type list. You can tap **?** to view each zones' definition.

Zone Bypass

Enable the function and the zone will be bypassed. No alarm will be received while the zone is bypassed.

Link Camera

You can link the zone to cameras. When an alarm is triggered, you can monitor the zone via the linked cameras.

Stay/Away

Enable the function and the zone will be auto bypassed when the zone is in stay or away status.

Chime

Enable the function and the zone will be start audible alarm when it is triggered.

Enable Silent Zone

Enable the function and no siren will be triggered if an event or alarm occurs.

Add a Camera to the Zone

You can link a camera to the zone to monitor the zone. You can view the alarm videos when an alarm is triggered.

Before You Start

Make sure you have installed the camera in the target zone and the camera has connected the same LAN as the security control panel's.

Steps

1. Tap a security control panel on the Hik-Connect page and tap **Zone** to enter the zone list page.

2. Select a zone to enter the zone settings page.

3. Tap **Link Camera** to enter the Link Camera page.

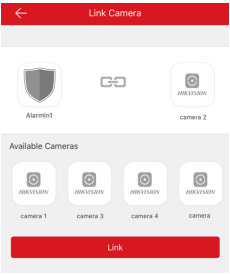


Figure 1-40 Link Camera Page

4. Select a camera in the available cameras, and tap **Link**.

The selected camera will be linked to the zone. The icon ⓟ will be displayed on the right of the zone in the zone list. Tap the icon to view the zone live video.

Set Arming/Disarming Schedule

Set the arming/disarming schedule to arm/disarm a particular zone automatically.

Tap a security control panel to enter the control page and tap ⚙ or ≡ to enter the Settings page.

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, and siren delay time.

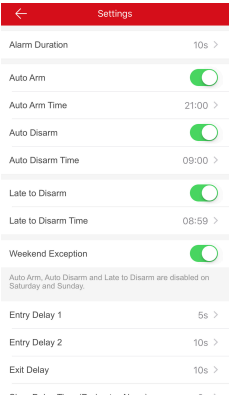


Figure 1-41 Arming or Disarming Schedule Page

Add Card

You can add card to the control panel. Use the card to arm, disarm, or clear alarm.

Steps

1. Select a control panel on the Hik-Connect page to enter the control panel management page.

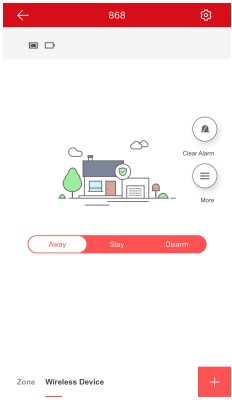


Figure 1-42 Control Panel Management Page

2. Tap → **Card/Tag Management** to enter the Card/Tag Management page.
3. Tap .
4. When hearing the voice prompt "Swipe Card", you should present the card on the control panel card presenting area.

   When hearing a beep sound, the card is recognized.
5. Create a card alias and tap **Finish**.

   Note

   The alias should contain 1 to 32 characters.

   The card is displayed in the Card/Tag Management page.

Add Keyfob

You can add keyfobs to the control panel and control partition arming/disarming status. You can also clear alarm when an alarm is triggered.

Steps

Note

Make sure the keyfob's frequency is the same as the control panel's.

1. Tap to enter the Add Keyfob page.
2. Follow the instruction on the page and press any key on the keyfob to add.
3. Create a name for the keyfob and tap **Finish**.

   The keyfob is listed in the Wireless Device page.
4. **Optional:** You can view the keyfob's serial No. and you can also delete it.

1.7 Input Types

Table 1-3 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 siren. 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 siren. There is a configurable interval between alarm and siren output, which allows you to check the alarm and cancel the siren 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 siren. 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 siren. Voice Prompt: Zone X follow alarm.
24H Silence Zone	The zone activates all the time without any sound/siren output when alarm occurs. Audible Response: No system sound (voice prompt or siren).
Panic Zone	The zone activates all the time. Audible Response: Trigger the system sound and siren. Voice Prompt: Zone X panic alarm.

Input Types	Operations
Fire Zone	The zone activates all the time with sound/siren output when alarm occurs. Audible Response: Trigger the system sound and siren. Voice Prompt: Zone X fire alarm.
Gas Zone	The zone activates all the time with sound/siren output when alarm occurs. Audible Response: Trigger the system sound and siren. 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 siren. Voice Prompt: Zone X medical alarm.
Timeout Zone	The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. Audible Response: Trigger the system sound and siren. Voice Prompt: Zone X alarm.
Disabled Zone	Alarms will not be activated when the zone is triggered or tampered. Audible Response: No system sound (voice prompt or siren).
Virtual Zone (Keypd/Keyfob)	The system will immediately alarm when it detects triggering event after system armed. Audible Response: Trigger the system sound and siren. 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 siren. Voice Prompt: Zone X tampered.

Input Types	Operations
Link	Trigger the linked device when event occurs. e.g. The output expander linked relays will be enabled when the control panel is armed.
Arm	When aremed: Voice prompt for fault.You can handle the fault according to the voice prompt. •System sound for arming with card or keyfob. •Voice prompt for fault.You can handle the fault according to the voice prompt. •Fault evnet displays on client. You can handle the fault via client software or mobile client. Voice Promt: Armed/Arming failed.

1.8 Output Types

Table 1-4 Output Types

Output Types	Active	Restore
Arming	Arm the control panel	after the configured output delay
Disarming	Disarm the control panel	after the configured output delay
Alarm	When alarm event occurs. The alarm output will be actived after the configured exit/ enter delay.	after the configured output delay, disarm the control panel or clear alarm
Manual Operation	Enable relays manually	Over the triggering time or disable the relays manually

1.9 Event Types

Table 1-5 Event Types

Evnet 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	×/√	√	×	×	×

1.10 Access Levels

Level	Description
1	Access by any person; for example the general public.
2	User access by an operator; for example customers (systems users).
3	User access by an engineer; for example an alarm company professional.
4	User access by the manufacturer of the equipment.

Table 1-6 Permission of the Access Level

Function	Permission			
	1	2	3[a]	4[b]
Arming	No	Yes	Yes	No
Disarming	No	Yes	Yes	No
Restoring/Clearing Alarm	No	Yes	Yes	No
Entering Walk Test Mode	No	Yes	Yes	No
Bypass(zone)/ Disabling/Force Arming	No	Yes	Yes	No
Adding/Changing Verification Code	No	Yes[d]	Yes[d]	Yes[d]
Adding/Editing Level 2 User and Verification Code	No	Yes	Yes	No
Adding/Editing Configuration Data	No	No	Yes	No
Replacing software and firmware	No	No	No	Yes

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 or level 4 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.

1.11 SIA and CID Code

Table 1-7 SIA and CID Code

SIA Code	CID Code	Description
BA	1130	Burglary Alarm
BH	3130	Burglary Alarm Restored
HA	1122	Silent Panic Alarm
HH	3122	Silent Panic Alarm Restored
NA	1780	Timeout Alarm
BH	3780	Timeout Alarm Restored
PA	1120	Panic Alarm
PH	3120	Panic Alarm Restored
BA	1131	Perimeter Alarm
BH	3131	Perimeter Alarm Restored
BA	1134	Entry/Exit Alarm
BH	3134	Entry/Exit Alarm Restored
TA	1137	Device Tampered
TR	3137	Device Tamper Restored
TA	1383	Detector Tampered
TR	3383	Detector Tamper Restored
TA	1321	Wireless Siren Tampered
TR	3321	Wireless Siren Tamper Restored
TA	1334	Wireless Repeater Tampered

SIA Code	CID Code	Description
TR	3334	Wireless Repeater Tamper Restored
ES	1341	Expander Tampered
EJ	3341	Expander Tamper Restored
/	1810	Keypad/Keyfob Panic Alarm
MA	1100	Medical Alarm
MH	3100	Medical Alarm Restored
GA	1151	Gas Leakage Alarm
GH	3151	Gas Leakage Alarm Restored
FA	1110	Fire Alarm
FH	3110	Fire Alarm Restored
OP	1401	Disarming
CL	3401	Away Arming
OA	1403	Auto Disarming
CA	3403	Auto Arming
BC	1406	Alarm Clearing
CL	3441	Stay Arming
CD	1455	Auto Arming Failed
BB	1570	Zone Bypassed
BU	3570	Zone Bypass Restored
CT	1452	Late to Disarm
AT	1301	AC Power Loss
AR	3301	AC Power Restored
YT	1302	Low System Battery

SIA Code	CID Code	Description
YR	3302	Low System Battery Restored
/	1925	Low Keyfob Battery
/	3925	Low Keyfob Battery Restored
/	1311	Battery Fault
/	3311	Battery Fault Restored
/	1862	Keypad Locked
/	3862	Keypad Unlocked
/	1607	Test Mode Entered
/	3607	Test Mode Exited
/	1305	Control Panel Reset
RN	1305	Control Panel Reset
UY	1321	Wireless Siren Disconnected
UJ	3321	Wireless Siren Connected
UY	1381	Wireless Detector Disconnected
UJ	3381	Wireless Detector Connected
XT	1384	Wireless Detector Low Voltage
XR	3384	Normal Wireless Detector Voltage
ET	1333	Expander Disconnected
ER	3333	Expander Connected

SIA Code	CID Code	Description
UY	1334	Wireless Repeater Disconnected
UJ	3334	Wireless Repeater Connected
NT	1352	Cellular Data Network Disconnected
NR	3352	Cellular Data Network Connected
NT	1352	SIM Card Exception
NR	3352	SIM Card Restored
NT	1352	Network Flow Exceeded
NT	1352	IP Address Conflicted
NR	3352	Normal IP address
NT	1352	Wired Network Exception
NR	3352	Normal Wired Network
YX	1351	Wi-Fi Communication Fault
YZ	3351	Wi-Fi Connected
XQ	1344	RF Signal Exception
XH	3344	Normal RF Signal
/	1306	Detector Deleted
/	3306	Detector Added
/	1306	Detector Deleted
/	3306	Detector Added

SIA Code	CID Code	Description
/	1306	Wireless Repeater Deleted
/	3306	Wireless Repeater Added
/	1306	Wireless Siren Deleted
/	3306	Wireless Siren Added

2 User Guide

2.1 System Description

AX wireless security control panel, containing 32 wireless zones, supports Wi-Fi, TCP/IP, and 3G/4G communication methods. It also supports ISAPI, Hik-Connect, DC09, and NAL2300, which is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- TCP/IP, Wi-Fi, and 3G/4G network
- Connects up to 32 wireless zones, 32 wireless outputs, 8 wireless keyfobs, 4 relays, 2 repeaters, and 2 sirens
- Supports up to 13 network users, including 1 installer, 1 administrator, 1 manufacturer, and 10 normal users
- Supports doorbell function: The detector rings like a doorbell when it is triggered in disarming status
- Voice prompt
- Wi-Fi settings in AP mode
- Configuration via Web client or mobile client
- Pushes alarm notification via messages or phone calls

Note

Only device containing 3G/4G communication method supports this function

- Views live videos and sends emails of alarm linked videos via mobile client
- Uploads reports to alarm center
- Long distance two-way communication with AES-128 encryption
- Supports LED indicator to indicates system status
- 4520 mAh lithium backup battery, supports up to 12 h power supply
- SIA-Contact ID protocol compatible

Note

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

2.2 Operations

You can use the client keyfob, card, client software, or mobile client to do arming, disarming, bypass, and zone disabling.

2.2.1 Arming

You can use keyfob, card, client software, mobile client to arm your system.

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

While the system is armed, the control panel will prompt the result in 5s, and upload the arming report.

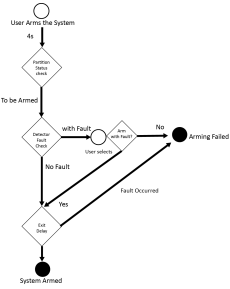


Figure 2-1 Arming Process

Access level of Arming

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

Arming Indication

The arming/disaring 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
- Mian power supply exception
- Backup battery exception
- Alarm receiving fault
- Siren 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).

Fored arming only taks effect on the current arming operation.

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

2.2.2 Disarming

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

Diarming 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

Set the entry delay duration within 45s to compliant the EN requirement.

Early Aalrm

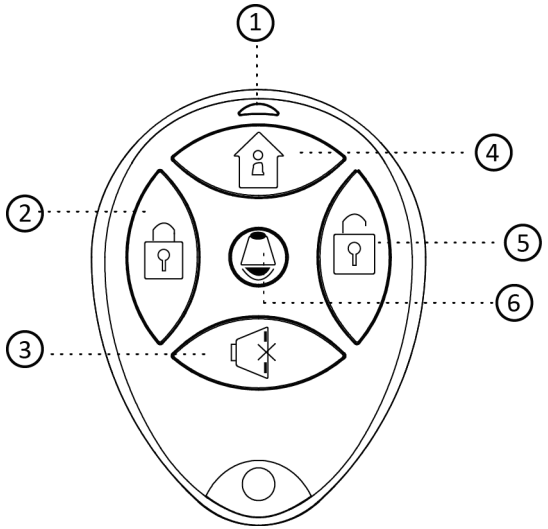
If either the intrusion or tampering alalrm occurrs on the enter/exit route when the control panel is in the status of entry delay, the control panel then enters the early alarm mode.

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

The control panel will reports the alarm only if the alarm event lasts over the duration of early alarm with the addition of enry delay.

2.2.3 Use the Keyfob

The keyfod is used for away arming, stay arming, disarming, panic alarm, and clearing alarm.



No.	Description
1	Indicator Green: Successful Operation Red: Press the Key
2	Away Arming
3	Clearing Alarm
4	Stay Arming
5	Disarming
6	Panic Alarm (Hold for 2 s)

The following table shows the keyfob operation and responded indications.

Keyfob Operation Result	Voice Prompt	Indication
Armed	Away/Stay Arming	Red LED Flashes Once
Arming Failed	Arming failed.	Green LED Flashes Once
Arming	Beep in the first 5 seconds. Fault promt after the beep for fault occurring	Green LED Flashes 9 Times
No Arming Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Fault Checking Finished	No Voice Prompt	Yellow LED Flashes 4 Times
Alarm Cleared	Alarm cleared	Green LED Flashes Once
No Permission for Clearing Alarm	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Disarmed	Disarmed	Green LED Flashes Once
No Disarming Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times
Panic Alarm Uploaded	Alarm Prompt	Green LED Flashes Once
No Panic Alarm Permission	Operation failed. The keyfob has no arming permission.	Yellow LED Flashes 4 Times

2.2.4 Use the Card

It is poissible to arm or disarm the system with the card.

While the system is not armed, present a valid card to the control panel to arm the system.

While the system is armed, present a valid card to the control panel to disarm the system.

The card operations and responding voice prompts are shown below.

Card Operation Result	Voice Prompt
Armed with Enrolled Card	Away/Stay Arming
Arming Failed with Enrolled Card	Arming Failed
Start Arming with Enrolled Card	Beep in the first 5 seconds. Fault promt after the beep for fault occurring
No Arming Permission for the Enrolled Card	No Voice Prompt
Fault Checking Finished with the Enrolled Card	No Voice Prompt
Disarming with Enrolled Card	Disarmed
No Disarming Permission for the Enrolled Card	No Voice Prompt
Unenrolled Card Operation	Invalid access

2.2.5 Use Mobile Client

AddPeripheral to the Control Panel

It is required to enter the activation name and the password login the control panel after it being added.

Before You Start

Make sure the control panel is disarmed.

Steps

Note

Some control panel models do not support add zones or wireless devices remotely. You should add them to the control panel directly. For details, see the user manual of the wireless device.

1. Tap to enter the Scan QR Code page.

2. Scan the peripheral's QR code to add the peripheral.

3. Select a peripheral type, and create a name for the peripheral.

Note

- When the adding peripheral is a detector, the detector will be linked to the zone. You can view the detector information in the Zone tab.
- Up to 32 detectors can be linked to the zone.

The added peripheral will be listed in the Zone tab or the Wireless Device tab.

Download and Login the Mobile Client

Download the Hik-Connect mobile client from Google Play (for Android) or App store (for iOS) and login the client before operating the security control panel.

Steps

1. Search and download Hik-Connect mobile client from Google Play (for Android) or App Store (for iOS).
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 Control Panel to the Mobile Client

Add a control panel to the mobile client before other operations.

Steps

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

     Note

     Normally, the QR code is printed on the label sticked on the back cover of the control panel.
   - Tap → **Manual Adding** to enter the Add Device page. Input the device serial No. with the Hik-Connect Domain adding type.
3. Connect to a network.

   1) Tap **Connect to a Network**.

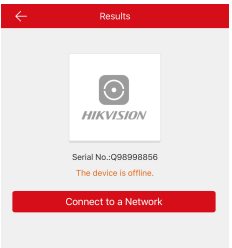


Figure 2-2 Connect to a Network Page

   2) Tap **Wireless Connect** on the Select Connection Type page.

3) Follow the instructions on the Turn on Hotspot page and change the control panel to the AP mode. Tap **Next**.

Note

You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

4) Select a stable Wi-Fi for the device to connect and tap **Next**.

Note

Make sure the device and the mobile phone are connect to the same Wi-Fi.

4. Follow the instructions on the Device's Wi-Fi page and connect the mobile phone with the control panel via wireless connection.

Note

Select **HAP-Device Serial No.** as the hotspot and enter the hotspot password. By default, the password is ***AP + Device Verification Code***. The verification code is normally printed on the device label.

5. Return to the mobile client and create a device password for device activation.

Note

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

6. Optional: If you add the control panel by entering its serial No., you should enter the device verification code and tap **OK**.

Note

By default, the verification code is printed on the device label.

7. Follow the instructions and change the control panel to the Station mode. Tap **Next**.

Note

You need to remove the rear panel of the device and the AP/STA switch is on the back of the device.

8. When the control panel is adding completed, tap **Finish**.

The control panel is listed on the Hik-Connect page.

Add Card

You can add card to the control panel. Use the card to arm, disarm, or clear alarm.

Steps

1. Select a control panel on the Hik-Connect page to enter the control panel management page.

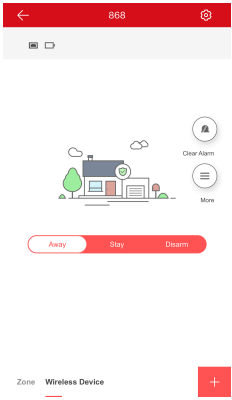


Figure 2-3 Control Panel Management Page

2. Tap → **Card/Tag Management** to enter the Card/Tag Management page.
3. Tap .
4. When hearing the voice prompt "Swipe Card", you should present the card on the control panel card presenting area.

   When hearing a beep sound, the card is recognized.
5. Create a card alias and tap **Finish**.

   Note

   The alias should contain 1 to 32 characters.

   The card is displayed in the Card/Tag Management page.

Add Keyfob

You can add keyfobs to the control panel and control partition arming/disarming status. You can also clear alarm when an alarm is triggered.

Steps

Note

Make sure the keyfob's frequency is the same as the control panel's.

1. Tap to enter the Add Keyfob page.
2. Follow the instruction on the page and press any key on the keyfob to add.
3. Create a name for the keyfob and tap **Finish**.

   The keyfob is listed in the Wireless Device page.
4. **Optional:** You can view the keyfob's serial No. and you can also delete it.

Arm/Disarm the Zone

Arm or disarm the zone manually as you desired.

Note

Axiom security control panel supports one partition.

On the Hik-Connect page, tap a security control device to enter the control panel management page. Tap **Away/Stay/Disarm** to control the partition's status.

You can also tap **Clear Alarm** to clear the alarm when an alarm is triggered.

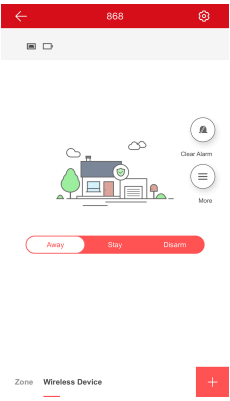


Figure 2-4 Control Panel Management Page

Bypass Zone

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

Before You Start

Link a detector to the zone.

Steps

1. Select a zone in the Zone tab of the Partition page.

2. Select a zone and enter the Settings page.

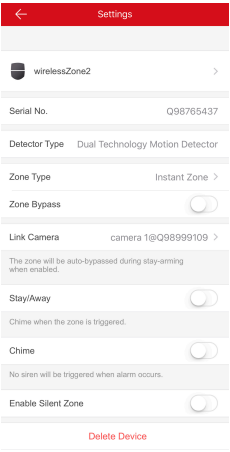


Figure 2-5 Zone Settings Page

3. Enable **Zone Bypass** and the zone will be in the bypass status.

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

Set Zone

After the detector is added, you can set the zone, including the zone name, the zone type, zone bypass, linked camera, stay/away status, the siren, and the silent zone. You can also view the detector serial No. and the detector type of the zone.

Steps

1. Tap a zone in the Partition page to enter the zone settings page.

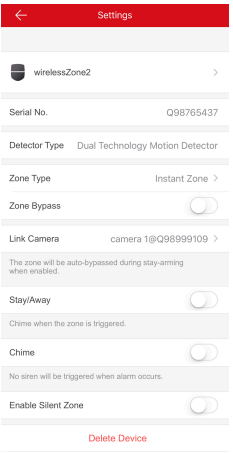


Figure 2-6 Zone Settings Page

2. Set the following parameters as you desired.

Zone Type

Select a zone type from the zone type list. You can tap **?** to view each zones' definition.

Zone Bypass

Enable the function and the zone will be bypassed. No alarm will be received while the zone is bypassed.

Link Camera

You can link the zone to cameras. When an alarm is triggered, you can monitor the zone via the linked cameras.

Stay/Away

Enable the function and the zone will be auto bypassed when the zone is in stay or away status.

Chime

Enable the function and the zone will be start audible alarm when it is triggered.

Enable Silent Zone

Enable the function and no siren will be triggered if an event or alarm occurs.

Set Arming/Disarming Schedule

Set the arming/disarming schedule to arm/disarm a particular zone automatically.

Tap a security control panel to enter the control page and tap or to enter the Settings page.

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, and siren delay time.

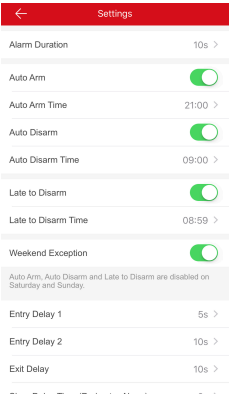


Figure 2-7 Arming or Disarming Schedule Page

Check System Status (Zone Status/Communication Status)

You can view the zone status and the communication status via the mobile client.

View Zone Status

In the Partition page, tap Zone to enter the Zone tab. You can view the each zone's status in the list.

Communication Mode

Tap to enter the control panel settings page. You can view the device communication status, including the battery, Ethernet network, Wi-Fi, mobile network, and data usage.

Check Alarm Notification

When an alarm is triggered, and the 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 **Message** in the Hik-Connect page to enter the Message page.

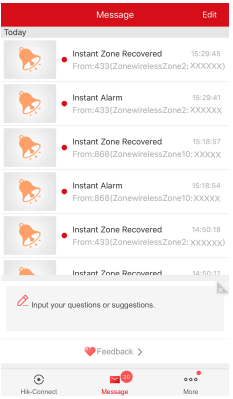


Figure 2-8 Message Page

All alarm notifications are listed in Message page.

2. Select an alarm and you can view the alarm details.

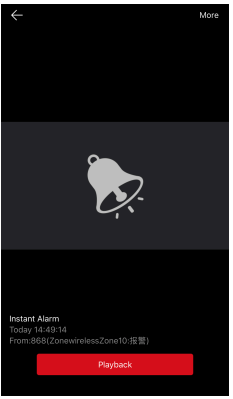


Figure 2-9 Alarm Notification Page

3. Optional: If the zone has linked a camera, you can view the playback when the alarm is triggered.

Add a Camera to the Zone

You can link a camera to the zone to monitor the zone. You can view the alarm videos when an alarm is triggered.

Before You Start

Make sure you have installed the camera in the target zone and the camera has connected the same LAN as the security control panel's.

Steps

1. Tap a security control panel on the Hik-Connect page and tap **Zone** to enter the zone list page.

2. Select a zone to enter the zone settings page.

3. Tap **Link Camera** to enter the Link Camera page.

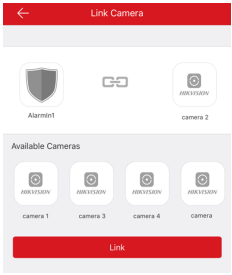


Figure 2-10 Link Camera Page

4. Select a camera in the available cameras, and tap **Link**.

The selected camera will be linked to the zone. The icon ⓟ will be displayed on the right of the zone in the zone list. Tap the icon to view the zone live video.

2.2.6 Use the Client Software

Steps

1. Download, install and register to the client software.

2. Add device in **Control Panel → Device Management → Device** .

Note

Set the device port No. as 80.

Note

The user name and password when adding device are the activation user name and password.

3. Click Remote Configuration to enter the device configuration page after the device is completely added,

Accessing the Operation Page

Control partitions and it's related zones in the **Security Control Panel** module.

Note

If there is no **Security Control Panel** displayed on the **Control Panel** page, click **Selecting Modules**, and select **Security Control Panel**

.

Partition Operation

In the **Security Control Panel**module, you can control the selected partition , such as away arming, stay arming, instant arming, disarming, clearing alarm, group bypass, and group bypass restoring.

Note

The wireless security control panel only have one partition.

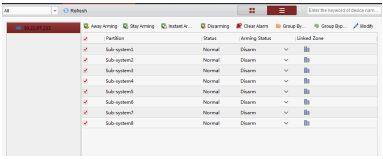


Figure 2-11 Partition Operation

Click**Edit**to edit the partition name and display options.

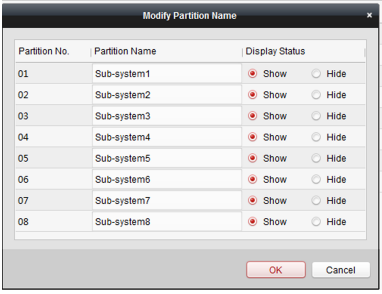


Figure 2-12 Editing Partition Information

Zone Operating

Click **Linked Zone**in the partition list of the **Security Control Module**. You can control the selected partition related zones, such as arming, disarming, bypass, or bypass restoring.

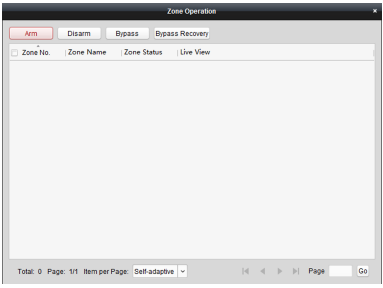


Figure 2-13 Zone Operation

2.2.7 Use the Web Client

Steps

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

Note

When using mobile broswer, the default IP Address is 192.168.8.1. The device must be in the AP mode.

Note

When connectiing the network cable with computer directly, the default IP Address is 192.0.0.64

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

Note

Refer to *Activation* chapter for the details.

Add/Edit/Delete Card

You can add card to the security control panel and you can use the card to arm/disarm the zone. You can also edit the card information or delete the card from the security control panel.

Steps

1. Click **User Management → Card** to enter the Card Management page.

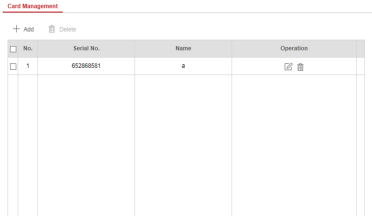


Figure 2-14 Card Management

2. Click **Add** and place a card on the card swiping area.
3. Customize a name for the card in the pop-up window.
4. Click **OK** and the card information will be displayed in the list.
5. **Optional:** Click ✎ and you can change the card name.
6. **Optional:** Delete a single card or check multiple cards and click **Delete** to delete cards in batch.

Add/Edit/Delete Keyfob

You can add keyfob to the security control panel and you can control the security control panel via the keyfob. You can also edit the keyfob information or delete the keyfob from the security control panel.

Steps

1. Click **User Management → Keyfob** to enter the Keyfob Management page.

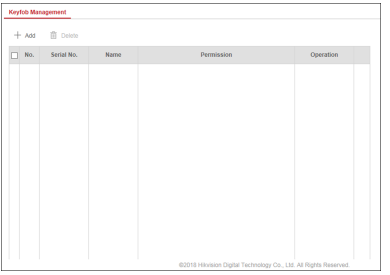


Figure 2-15 Keyfob Management

2. Click **Add** and press any key on the keyfob.
3. Set the keyfob parameters.
   Name

   Customize a name for the keyfob.

   Permission Settings

   Check different items to assign permissions.

   Single Key Settings

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

   Combination Keys Settings

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

Add/Edit/Delete User

Administrator can add user to the security control panel, edit the user information, or delete the user from the security control panel. You can also assign different permissions to the new user.

Steps

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

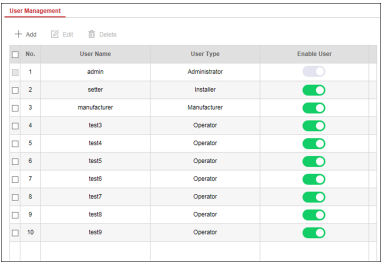


Figure 2-16 User Management Page

2. To compliant the EN requirement, slide the block to enable the setter and manufactuer .

Note

The default password of the setter is **setter12345**, and the default password of the manufactuer is **hik12345**.

3. Click **Add**.
4. Set the new user's information in the pop-up window, including the user type, the user name, and the password.

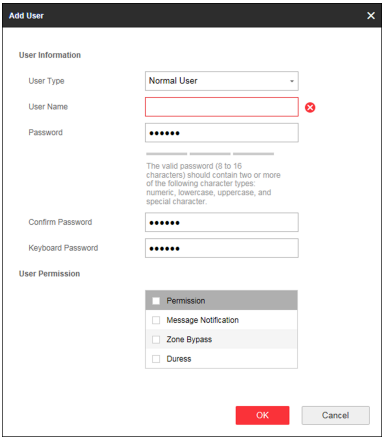


Figure 2-17 Add User Page

5. Check the checkboxes to set the user permission.

   The user can only operate the assigned permissions.
6. Click **OK**.
7. **Optional:** Enable the user in the Enable User column to allow the enabled user operating the device.
8. **Optional:** Select an user and click **Edit** and you can edit the user's information and permission.
9. **Optional:** Delete a single user or check multiple users and click **Delete** to delete users in batch.

Note

The admin and the setter cannot be deleted.

Check Status

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

Click **Status**. You can view the status of zone, relay, siren, battery, communication, and repeater.

- Zone: You can view the zone status, alarm status, detector battery capacity, and signal strength.
- Siren: You can view siren status, battery status, and signal strength.
- Relay: You can view relay status, battery status, and signal strength.

- Battery: You can view the battery charge.
- Communication: You can view the wired network mode, Wi-Fi status, Wi-Fi signal strength, cellular network status, used data, and cloud connection status.

2.3 Configuration

Configure the security control panel in the web client or the remote configuration page in client software.

2.3.1 Activation

In order to protect personal security and privacy and improve the network security level, you should activate the device the first time you connect the device to a network.

You can create an activation password to protect your device from logging in by other persons.

Activate Device via iVMS-4200

is a PC client to manage and operate your devices. Security control panel activation is supported by the software.

Before You Start

- Get the client software from the supplied disk or the official website ***http://www.hikvision.com/en/*** . Install the software by following the prompts.
- The device and the PC that runs the software should be in the same subnet.

Steps

1. Run the client software.
2. Enter **Device Management** or **Online Device**.
3. Check the device status from the device list, and select an inactive device.
4. Click **Activate**.
5. Create and confirm the admin password of the device.

   Caution

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

6. Click **OK** to start activation.

   Device status will change to **Active** after successful activation.

7. Edit IP address of the device.

   1) Select a device and click **Modify Netinfo** at **Online Device**.

   2) Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking **DHCP**.

   3) Input the admin password of the device and click **OK** to complete modification.

Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

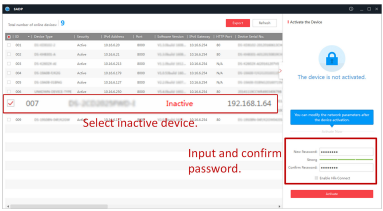
Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

Caution

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

4. Click **Activate** to start activation.



Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.

   1) Select the device.

   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.

   3) Input the admin password and click **Modify** to activate your IP address modification.

Activate Device via Web Browser

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

Before You Start

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

Steps

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

Note

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

2. Create and confirm the admin password.

Caution

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

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

4. Edit IP address of the device.

1) Enter IP address modification page. **Configuration → Network → TCP/IP**

2) Change IP address.

3) Save the settings.

2.3.2 Network Settings

Wired Network

If the device is linked to the wired network, you can set the wired network parameters when you want to change the device IP address and other network parameters.

Steps

Note

The function is not supported by some device models.

1. In iVMS-4200 client software, enter the Device Management page.

2. Select the radar in the Device for Management list, click **Remote Configuration**.

3. Click **Communication Parameters → Wired Network Parameters** to enter the Wired Network Parameters page.

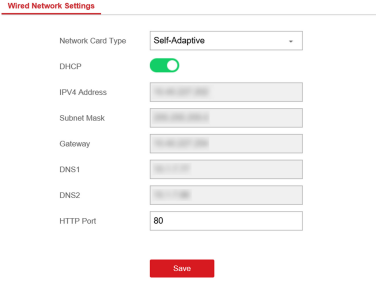


Figure 2-18 Wired Network Settings Page

4. 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**.

Note

By default, the HTTP port is 80, which is not editable.

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

6. Click **Save**.

Wi-Fi

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

Steps

1. Click **Communication Parameters → Wi-Fi Parameters** .

2. Click **Wi-Fi** to enter the Wi-Fi page.

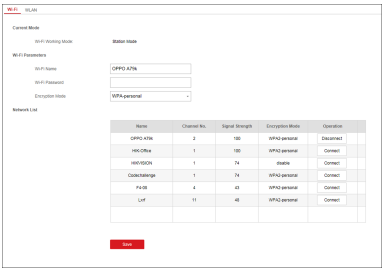


Figure 2-19 Wi-Fi Settings Page

3. Connect to a Wi-Fi.
   - Manually Connect: Input the Wi-Fi name and the Wi-Fi password, 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**.

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

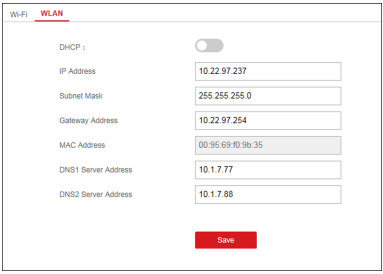


Figure 2-20 WLAN Settings Page

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

Note

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

6. Click **Save**.

Cellular Network

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

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

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

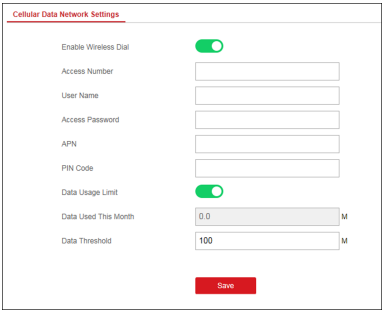


Figure 2-21 Cellular Data Network Settings Page

2. Enable Wireless Dial.

3. Set the cellular data network parameters.

Access Number

Input the operator dialing 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.

Data Used This Month

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

4. Click **Save**.

Hik-Connect

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

Before You Start

- Connect the device to the network via wired connection, dial-up connection, or Wi-Fi connection.
- Set the device IP address, subnet mask, gateway and DNS server in the LAN.

Steps

1. Click **Communication Parameters → Hik-Connect Registration Parameters** to enter the Hik-Connect Registration Settings page.

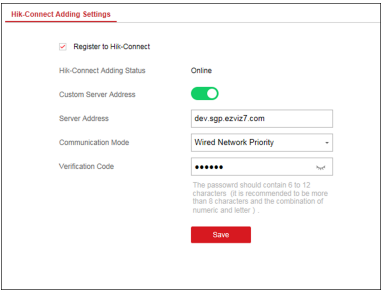


Figure 2-22 Hik-Connect Registration Settings Page

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

Note

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

You can view the device status that in the Hik-Connect server.

3. Enable **Custom Server Address**.

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

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

   Auto

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

   Wired Network Priority

   The system will select wired network only.

   Note

   When the device supports cellular data network connection and the wired network is disconnected, it will connect to the cellular data network. When the wired network is restored, only if the cellular data network is disconnected, does the device connect to the wired 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 authentication password.

Note

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

6. Click **Save**.

2.3.3 Alarm Settings

Alarm Center

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

Steps

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

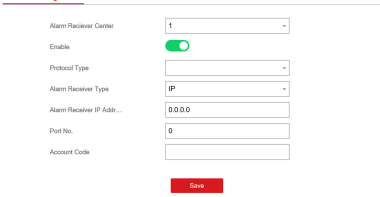


Figure 2-23 Alarm Receiving Center Parameters

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

Note

You can enable the **backup channel** when the **Alarm Receiver Center** is selected as **2**.

3. Select the **Protocol Type** as **ADM-CID**, **EHome**, **SIA-DCS**, ***SIA-DCS**, or ***ADM-CID** to set uploading mode.
   - **ADM-CID** or **SIA-DCS**

     You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, timeout, re-upload times and heartbeat interval.

     Note

     You should check **Enable** on the right of Heartbeat Interval line to edit the heartbeat interval.
   - **EHome**

     You do not need to set the EHome protocol parameters.
   - ***SIA-DCS** or ***ADM-CID**

You should select the **Alarm Receiver Type** as **IP** or **Domain name**, and enter the IP/domain name, port number, account code, timeout, re-upload times, heartbeat interval, encryption arithmetic, password length and secret key.

Note

You should check **Enable** on the right of Heartbeat Interval line to edit the heartbeat interval.

4. Click **Save**.

Notification Push

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

Steps

1. Click **Communication Parameters → Message Notification** .

2. Enable the target notification.

Alarm and Tampering Event Notification

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

Safety Event Notification

The device will push notifications when fire alarm, gas alarm, or medical alarm is triggered.

System Status Notification

The device will push notifications when any status in the system is changed.

Operation Event Notification

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

Note

If you want to send the alarm notifications to the mobile client, you should also set the **Mobile Phone Index**, **SIM Card No.**, and check the **Notification Type**.

Note

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

3. Click **Save**.

Zone

You can set the zone parameters on the zone page.

Steps

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

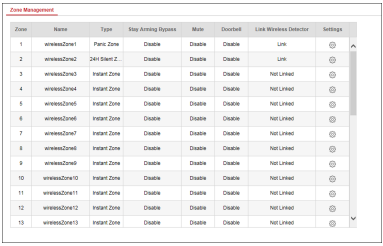


Figure 2-24 Zone Page

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

3. Edit the zone name.

4. Select a zone type.

Instant Zone

The system will immediately trigger an alarm when it detects triggering event after system armed. Detectors can be set as this type, which can be used in places such as supermarket.

Delayed Zone

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

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

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

Note

You can set the delayed time duration in **System → Schedule & Timer** .

Follow Zone

The zone acts as delayed zone when it detects triggering event during system Entry Delay, while it acts as instant zone otherwise. It is usually set in the living room or hall with perimeter delayed zones at the same time.

Perimeter Zone

The system will immediately alarm when it detects triggering event after system armed. There is a configurable interval between alarm and siren output, which allows you to check the alarm and cancel the siren output during the interval time in case of false alarm. It is usually used in the perimeter area, such as doors and windows.

When the zone is armed, you can set the peripheral alarm delayed time in **System → Schedule & Timer** . You can also mute the siren in the delayed time.

24H Silent Zone

The zone activates all the time without any sound/siren output when alarm occurs. It is usually used in the sites equipped with panic button (e.g., bank, jewelry store).

Panic Zone

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

Fire Zone

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

Combustible Gas Zone

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

Medical Zone

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

Timeout Zone

The zone activates all the time. It alarms when the event you defined does happen throughout a configurable period. It is usually used in places equipped with magnetic contacts (e.g., fire hydrant box's door).

Shield Zone

Alarms will not be activated when the zone is triggered or tampered. It is usually used to disable faulty detectors .

5. Enable **Stay Arming Bypass**, **Doorbell**, or **Mute** according to your actual needs.

Note

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

6. Enable **Link Wireless Detector** , input the serial No., and set the linked camera No.

Note

868 Devices do not support inputting serial No.

7. Click **OK**.

Note

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

Alarm Schedule

You can set the delayed time duration for the delayed zone and the delayed time to exit the zone. You can also set the alarm schedule. The zone will be armed/disarmed according to the configured time schedule.

Steps

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

Figure 2-25 Schedule & Timer Page

2. Set time duration of **Delay 1**, **Delay 2**, or **Exit Delay** respectively.

Delay 1/Delay 2

If you have set the delayed zone, you can set the delayed time duration here.

Note

The available time duration rage is from 5s to 600s.

Exit Delay

If the you want to exit the zone without triggering the alarm, you can set the exit delay duration.

Note

The available time duration rage is from 5 s to 600 s.

3. Optional: Set the following parameters according to actual needs.

Auto Arming

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.

Auto Disarming

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 Operation Event Notification function in **Communication Parameters → Message Notification** before enabling the Late to Disarm function.

Weekend Exception

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

Perimeter Alarm Delayed Time

If you have set the perimeter zone, you can set the delayed time for the zone.

Note

The available time duration range is from 0 s to 600 s.

Alarm Duration

Set the time duration of the alarm.

Note

The available time duration range is from 5 s to 600 s.

4. Click **Save**.

Output

If you want to the link the device with a relay output to output the alarm, set the output parameters.

Steps

1. Click **Wireless Device → Output** to enter the Output page.

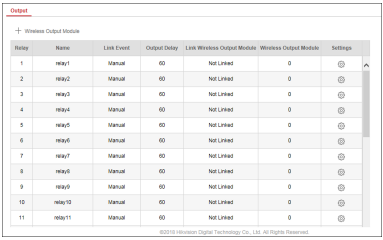


Figure 2-26 Output Page

2. Add a wireless output module.

1) Click **Wireless Output Module**.

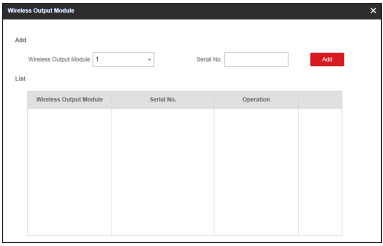


Figure 2-27 Wireless Output Module Settings

2) Select a wireless output module number from the drop-down list.

3) Input the serial No. of the wireless output module.

4) Click **Add**.

3. Click ⚙ and the Relay Settings window will pop up.

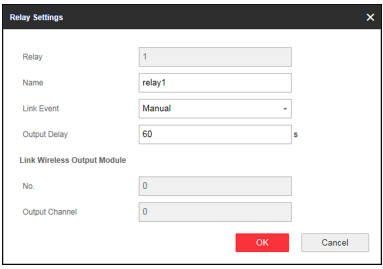


Figure 2-28 Relay Settings Page

4. Edit the relay name, select a link event, and set the output delay time duration.

Note

If the relay has linked to the wireless output module, the wireless output module information will be displayed in the Link Wireless Output Module area.

5. Click **OK**.

Note

After the relay is configured, you can click **Status → Relay** to view the output status.

Siren

If you want to link the security control panel to a siren to report an alarm when the alarm is triggered, you can set the siren parameters.

Steps

1. Click **Wireless Device → Siren** to enter the Siren page.

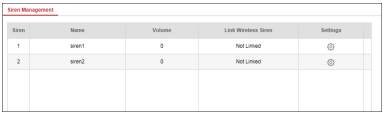


Figure 2-29 Siren Page

2. Click ⚙ to enter the Siren Settings page.

3. Set the siren name and the volume.

Note

The available siren volume range is from 0 to 3.

4. Optional: Enable **Link Wireless Siren** and set the siren serial No.

Note

Some detectors may not support this function.

5. Click **OK**.

Note

After the siren is configured, you can click **Status → Siren** to view the siren status.

Repeater

If the detector is far away from the control panel, set the repeater parameters to enlarge the signal.

Steps

1. Click **Wireless Device → Repeater** to enter the Repeater page.

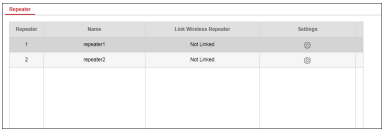


Figure 2-30 Repeater Page

2. Click ⚙ to set the repeater parameters.

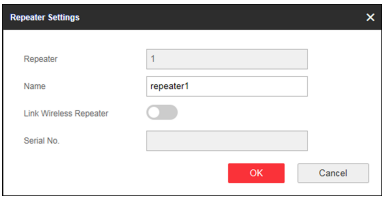


Figure 2-31 Repeater Settings

3. Edit the repeater's name.
4. Enable **Link Wireless Repeater** and input the repeater serial No.
5. Click **OK**.

Note

After setting the repeater, you can enter **Status → Repeater** to view the repeater status.

2.3.4 Video Management

You can add two network cameras to the wireless security control panel, 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 Security Control Panel

Steps

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

Figure 2-32 Network Camera Management

2. Click**Add**, and enter the basic information of the camera, such as camera name, IP address, and port No..
3. Enter the user name and password of the camera.
4. Click **Save**.

Note

You can add two network cameras for a wireless securty control panel.

1. **Optional:** Click**Edit**or**Delete**to edit or delete the selected camera.

Link a Camera with the Zone

Steps

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

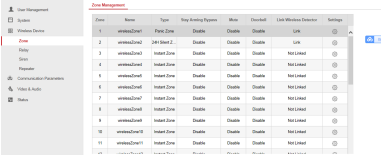


Figure 2-33 Zone Management

2. Select a zone needs video monitoring, and click the **Settings**icon.

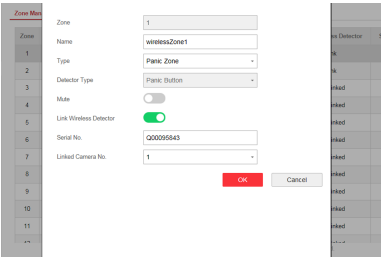


Figure 2-34 Zone Configuration

3. Select the **Linked Camera No.**.
4. Click**OK**.

Set Email to Receive Alarm Video

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

Steps

1. Click **Communication Parameters → Event Video Transfer via Email** to enter the page.

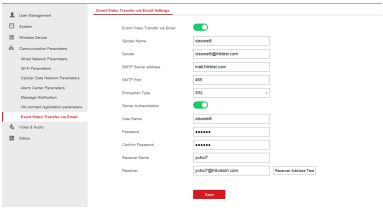


Figure 2-35 Event Video Transfer via Email

2. Click the block to enable the function.
3. Enter the sender's information.
4. Enter the receiver's information.
5. Click **Receiver Address Test** and make sure the address is correct.
6. Click **Save**.

Set Video Parameters

Steps

1. Click **Video & Audio → Event Video Parameters** to enter the page.

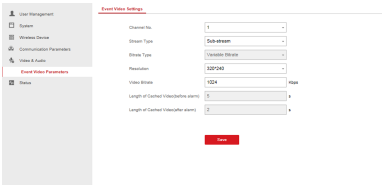


Figure 2-36 Video Settings

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.

Note

For network camera supporting sub-stream, SMS video uses sub-stream, and the configuration of main stream will not effect on the SMS video.

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.

2.3.5 System Settings

Time Settings

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

Time Management

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

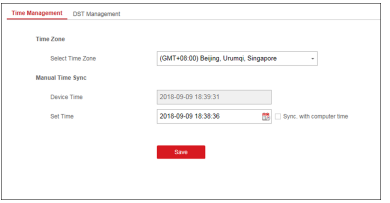


Figure 2-37 Time Management

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

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

DST Management

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

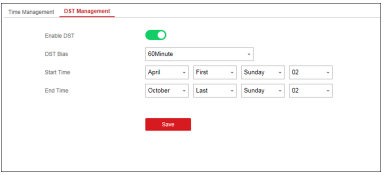


Figure 2-38 DST Management

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

SSH Settings

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

Click **System → Security → SSH Settings** to enter the SSH Settings page and you can enable or disable the SSH function.

Local Log Search

You can search the log on the device.

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

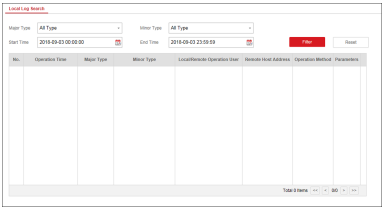


Figure 2-39 Local Log Search Page

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

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

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 Unaccessible.

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-connet 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 "AP" mode. Switch the panel to "station" mode, and then try to enter the registration mode again.

A.2.2 Unable to Enter RF Signal Query Mode

Fault Description:

Double-click the host function key, and the prompt button invalid.

Solution:

The panel is in "AP" mode. Solution: switch the panel to "station" mode, and then try to enter the RF signal query 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:

Recovery detector tamper-proof button.

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 port
  Defualt 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 name
  User name of Outlook and Hotmail require full names, and other email require a prefix before @.