AX Security Control Panel

Legal Information

About this Manual

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

Trademarks

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

Disclaimer

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

PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

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 EN 50131-10: 2014 EN 50136-2: 2013	Security Grade (SG): 2 Environmental Class (EC) : II telefication Certified by Telefication

Note

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

EU Conformity Statement

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

Contents

Chapter 1 Introduction

1.1 System Description

AX wireless security control panel, containing 32 wireless zones, supports Wi-Fi, TCP/IP, and GPRS/3G/4G communication methods. It also supports ISAPI, Hik-Connect, and DC-09, which is applicable to the scenarios of market, store, house, factory, warehouse, office, etc.

- TCP/IP, Wi-Fi, and GPRS/3G/4G network
- Connects up to 32 wireless zones, 4 wireless outputs, 8 wireless keyfobs, 32 relays and 4 sirens
- Supports up to 13 network users, including 1 installer, 1 administrator, 1 manufacturer, and 10 normal users

Note

The default password of the **installer** is **installer12345**, and the default password of the **manufacturer** is **hik12345**. These codes will have to be changed when first connected.

- 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 GPRS/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 3 times continuously.

- The device will be locked 90 s after 3 failed credential attempts in a minute

Ordering

Model	Description
DS-PWA32-HSR (Black/White)	supports Ethernet/ WI-FI, 3G/4G, and IC Card
DS-PWA32-HGR (Black/White)	supports Ethernet/ WI-FI, GPRS, and IC Card
DS-PWA32-HR (Black/White)	supports Ethernet/ WI-FI and IC Card
DS-PWA32-HS (Black/White)	supports Ethernet/ WI-FI, and 3G/4G
DS-PWA32-HG (Black/White)	supports Ethernet/ WI-FI, and GPRS
DS-PWA32-H (Black/White)	supports Ethernet/ WI-FI

1.2 Specification

DS-PW32-H(R)(S)(G)		
Wireless Device Connection	Alarm Input	32
	Alarm Output	32
	Siren	4
	Keyfob	8
	Keypad	4
	Tag reader	4
	Partition	4
Interaction	Audio Output	1, 1.5W
RF	RF Frequency	433/868MHz (depends on the model)
	RF Modulation	GFSK
	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

DS-PW32-H(R)(S)(G)		
	Encryption	Supported
	Channel	2.4 G
Application & Protocol	Application	iVMS-4200, and Hik-Connect
	Protocol	RCT protocol: DC-09(ADM-CID)/ DC-09(SIA-DCS) EHome
User	IC Card	12 (only for model with -R)
	User	12 (1 installer, 1 administrator, 1 manufacturer, and 10 general users)
Communication	Mode of operation	Pass-through
Logs	Stored in the FLASH (over-write protected)	4700 max log entries of which 1000 are mandatory
Power Supply	Type	A
	Model	Mains powered AC/DC adapter Shenzhen Honor Electronic Co Ltd ADS-12B-06 05010E Input 100-240V 50/60Hz Max 0.3A Output 5V DC 2.0A Center positive
	Low voltage message	3.55 V
	Output	No outputs
	Current when on battery	300mA
Battery	Type	Rechargeable Lithium-ion polymer battery Model: 765965 Nominal Voltage: 3.8V Capacity: 4520mAh 17.176Wh 24 hours to recharge to 80%
Service	No user serviceable parts inside	
Others	Power	5 VDC, 10 W
	Current	Alarm current: 300mA Non-alarm current: 240mA
	Consumption (without HDD)	< 5.6 W

DS-PW32-H(R)(S)(G)		
	Operation Temperature	–10 °C to 55 °C
	Operation Humidity	10% to 90%
	Shell Material	PC+ABS
	Dimension(W x H x D)	155 × 155 × 35 mm
	Weight	410 g
	Battery Power Supply	12 H

Note

Ehome5.0: a privacy internet protocol that is used for accessing the third-party platform, which supports alarm report uploading, security control panel management, and short video uploading.

Note

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

1.3 ATS Category

Table 1-2 ATS Category

Category	Model
DP2	DS-PWA32-HSR DS-PWA32-HS DS-PWA32-HGR DS-PWA32-HG
SP4	DS-PWA32-HR DS-PWA32-H

Note

If the ATP fault is detected, the control panel will generate and report logs. If the ATS fault is detected, the control panel will generate and report logs, indicates the fault with Alert LED (solid orange), and prompts fault details when the system is disarmed by authorized users.
DP2: While the alarm receiving center is enabled. The control panel will upload alarm report to the receiver center via the main path (LAN or Wi-Fi) or the back-up path (3G/4G). If the control panel is properly connected to the LAN or Wi-Fi, the main path is selected as the transmission path. If the main path connection is failed, the path will be switched to 3G/4G. And if the main path connection is restored, the path will be switched back to LAN or Wi-Fi. The control panel checks the connection status continuously, and generates logs transmission fault for any of the path. While both of the paths are invalid, the control panel determines ATS fault.
SP: Control panel can only upload report via LAN or Wi-Fi. While the connection is failed, the control panel determines ATS fault and stores the event log.
You can check the fault information in the control panel logs.

1.4 Appearance

Front Panel

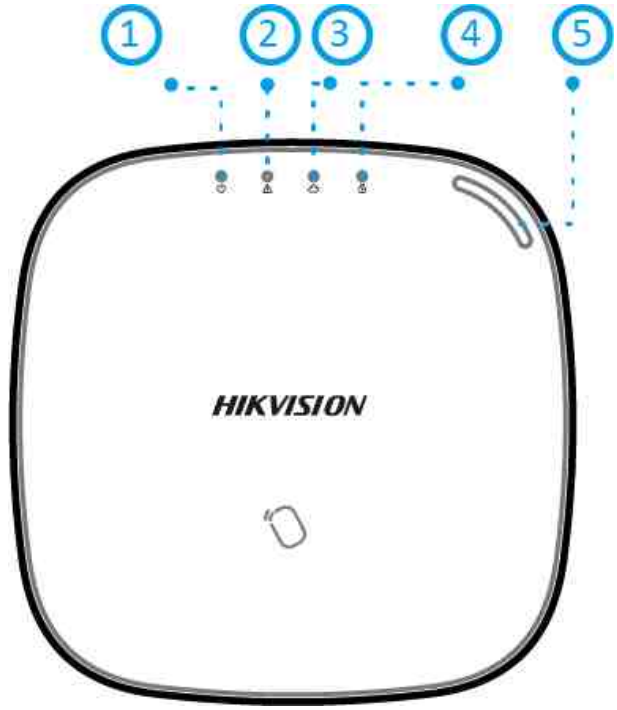


Figure 1-1 Front Panel

Table 1-3 Front Panel Description

No.	Indicator Name	Description
1	AC Power	Solid Green: Power on Off: Power off
2	Alert	Solid Orange: In the disarming status,the LED indicates alarm (such as panic alarm, zone alarm, tampering alarm, etc.) and fault (such as operation fault, connection fault, etc.) **Note** Voice notifications that are not allowed to be indicated/heard to level 1 users will only be heard when presented with a valid tag or keyfob. The device will prompt detailed alarm or fault information while authorized users disarm the system. 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.

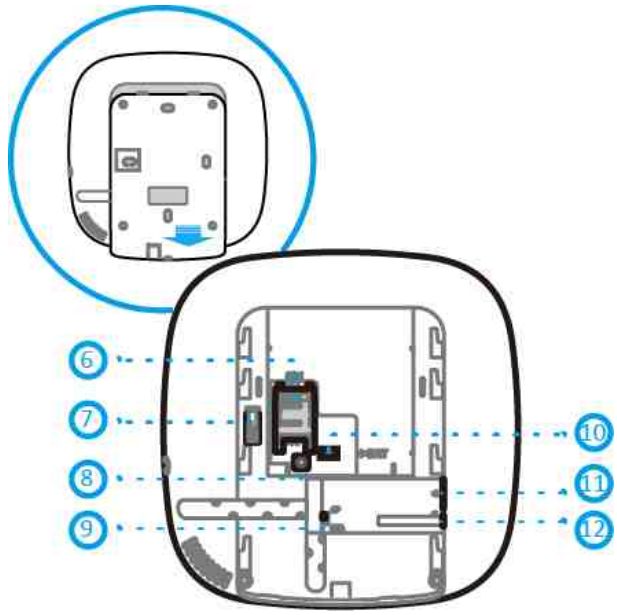


Figure 1-2 Component and Interface

Table 1-4 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.
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.
While the control panel is not in the configuration mode, double press the function button, and you can check the RF signal strength on the peripheral device.

Result	RSSI	Action
Strong	Over 160	OK to install
Medium	80 to 160	OK to install
Weak	0 to 79	Please see the note below.
Invalid	-	Not OK to install

Note

Only install peripherals when the signal strength is 100 or above. For much better system, install at 120 and above.

Chapter 2 Connection

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

Note

Check the RF signal strength before connection and peripheral device installation. While the control panel is not in the registration 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.

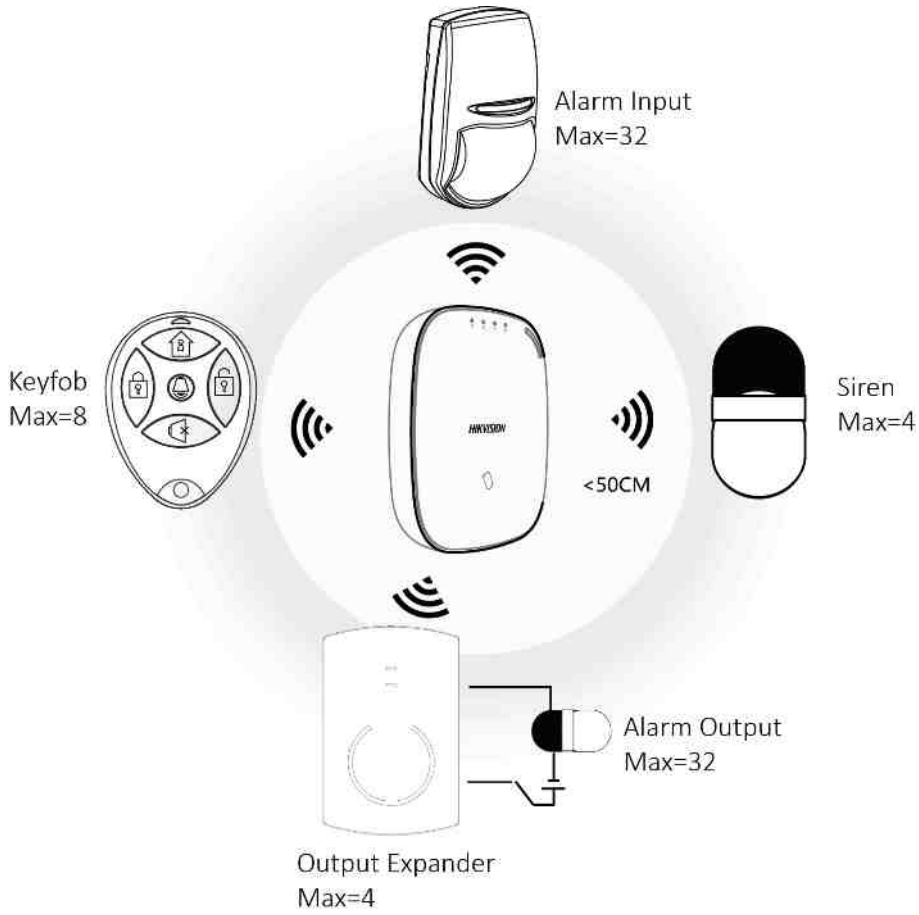


Figure 2-1 Connection

Connect Locally

Note

Add the card or keyfob via the web client before adding peripheral device for clearing tampering alarm.
The distance between the control panel and wireless device should be less than 50 cm.

While the control panel is not in the registration 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** → → **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 wireless 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.*

Chapter 3 Installation

Steps

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

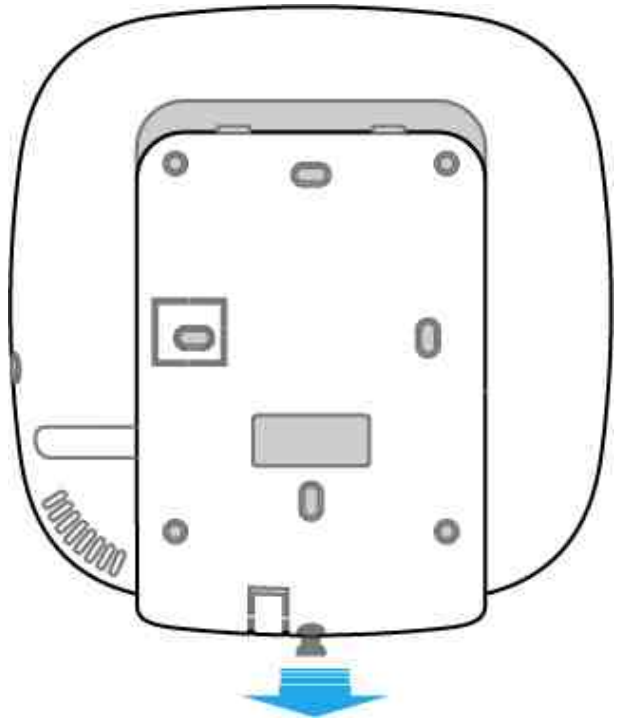


Figure 3-1 Remove the Rear Cover

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

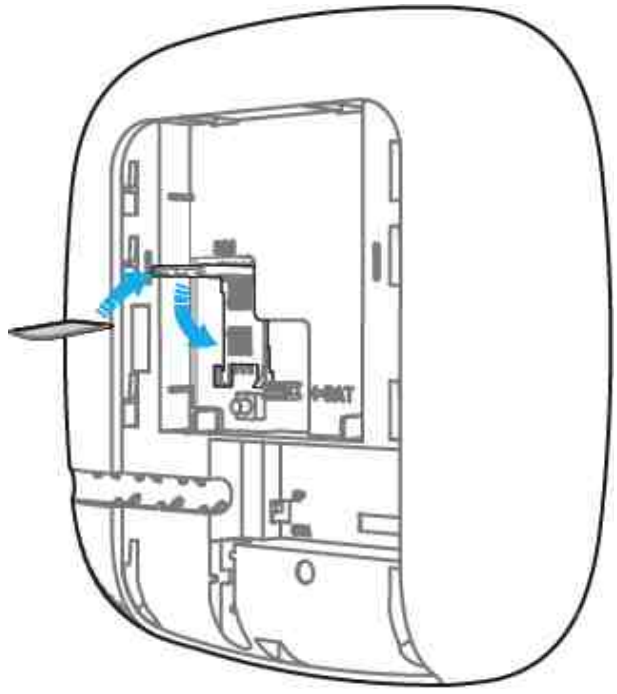


Figure 3-2 Insert SIM Card

Caution

Please ensure that the SIM card is tested as there might be communication issues with some providers.

3. Connect the battery to the control panel.

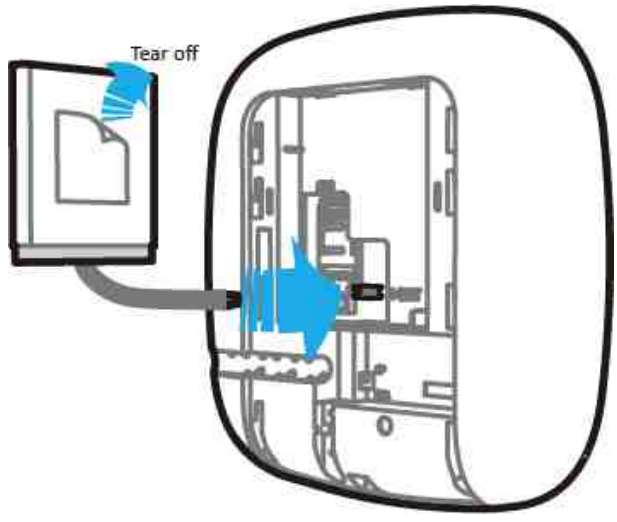


Figure 3-3 Connect the Battery

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

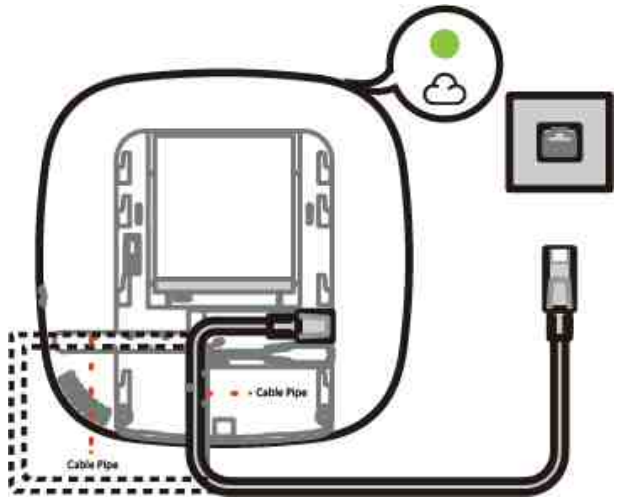


Figure 3-4 Power On

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

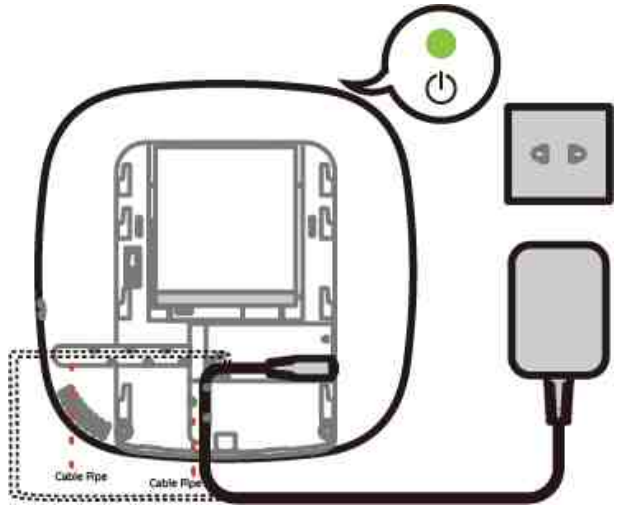


Figure 3-5 Connect to the Ethernet

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 3-6 Complete the Installation

Note

- Blue Star: Side Opening. If you need to route the cable though the bottom of the panel, remove the sheet of the side opening.
- Red Star: TAMPER Screw. It is compulsory to secure the TAMPER screw.
- No adjustments are required.
- For use within the supervised premises only.

Chapter 4 Configuration

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

4.1 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.

4.1.1 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.
   2) Change IP address.
   3) Save the settings.

4.1.2 Activate Device via Client Software

Before You Start

- Get the iVMS-4200 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**.
3. Click **Online Device**.
4. Check the device status from the online device list, and select an inactive device.
5. Click **Activate**.
6. 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.

7. Click **OK** to start activation.

   Device status will change to **Active** after successful activation.
8. Edit IP address of the device.
   1) Select a device and click on the online device list.
   2) Change the device IP address to the same subnet with your computer and set port number as 80.
   3) Enter the admin password of the device and click **OK** to complete modification.
9. **Optional:** Check the device on the online device list and click **Add** to add the device to the device list.

4.1.3 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.

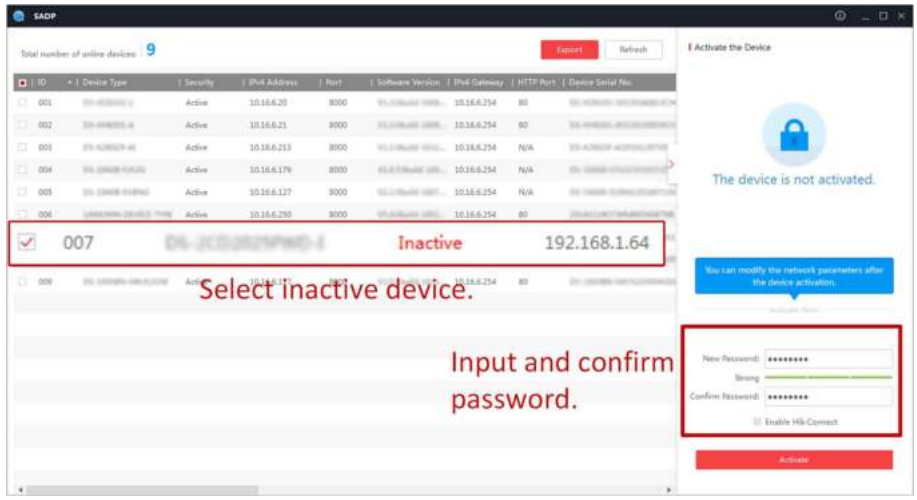
Steps

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.

4.2 Use the Client Software

Steps

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

Note

- Set the device port No. as 80.
- The user name and password when adding device are the activation user name and password.

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

4.3 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 browser, the default IP Address is 192.168.8.1. The device must be in the AP mode.

Note

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

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

Note

Refer to *Activation* chapter for the details.

4.3.1 Communication 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 the client software, enter the **Device Management** page.
2. Select the device in the Device for Management list, click **Remote Configuration**.
3. Click **Communication Parameters → Ethernet** to enter the Wired Network Parameters page.

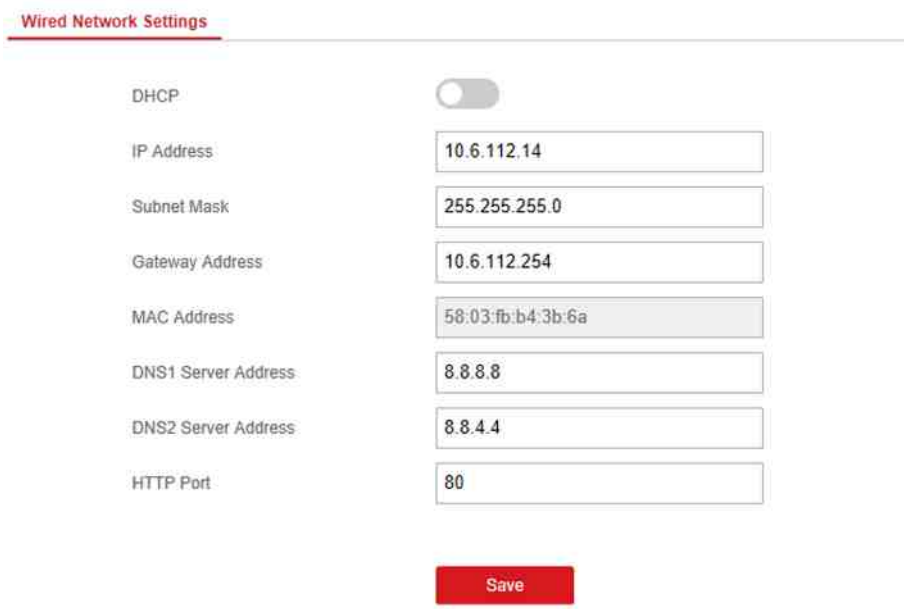


Figure 4-1 Wired Network Settings Page

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.
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** to enter the Wi-Fi page.

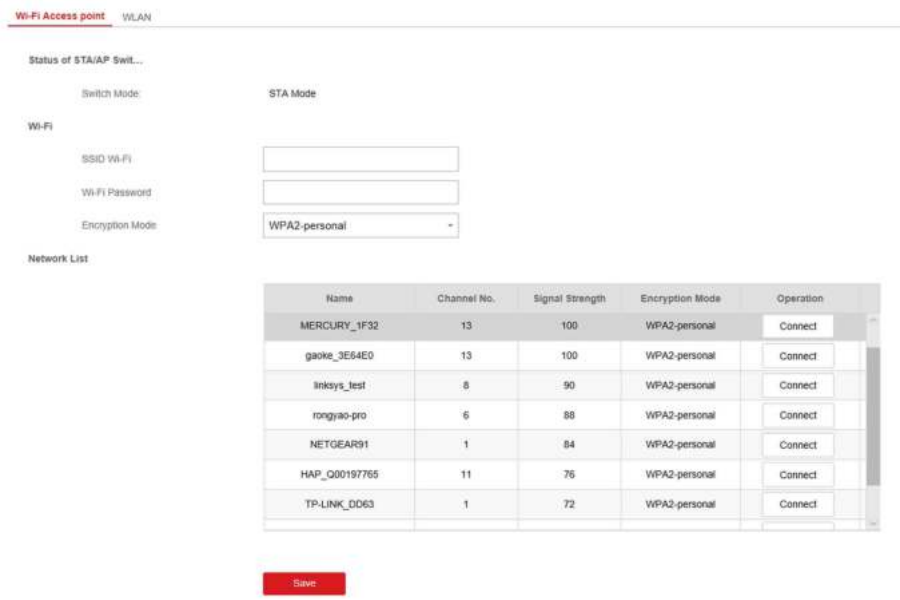


Figure 4-2 Wi-Fi Settings Page

2. Connect to a Wi-Fi.
   - Manually Connect: Input the **SSID Wi-Fi** and **Wi-Fi Password**, select **Encryption Mode** and click **Save**.
   - Select from Network List: Select a target Wi-Fi from the Network list. Click **Connect** and input Wi-Fi password and click **Connect**.
3. Click **WLAN** to enter the WLAN page.

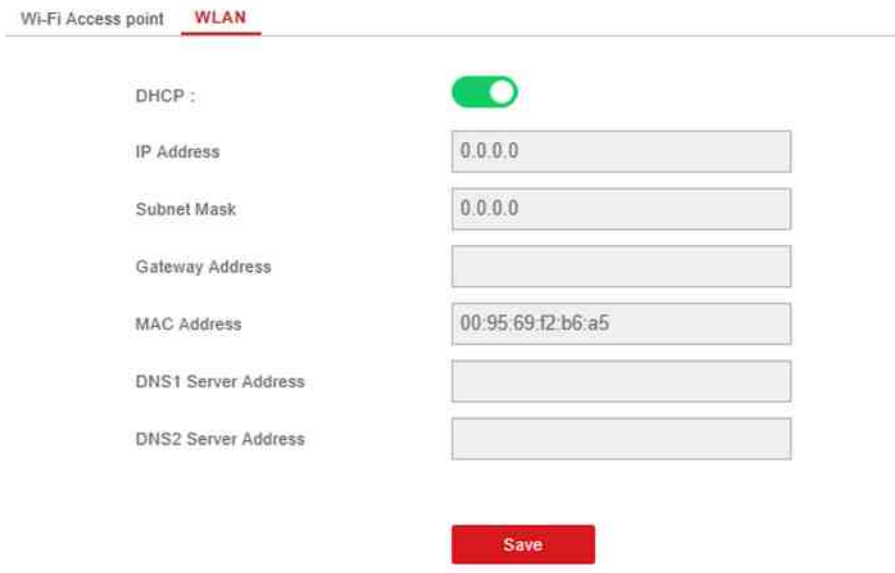


Figure 4-3 WLAN Settings Page

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

Note

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

5. Click **Save**.

Cellular Network

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

Before You Start

Insert a SIM card into the device SIM card slot.

Steps

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

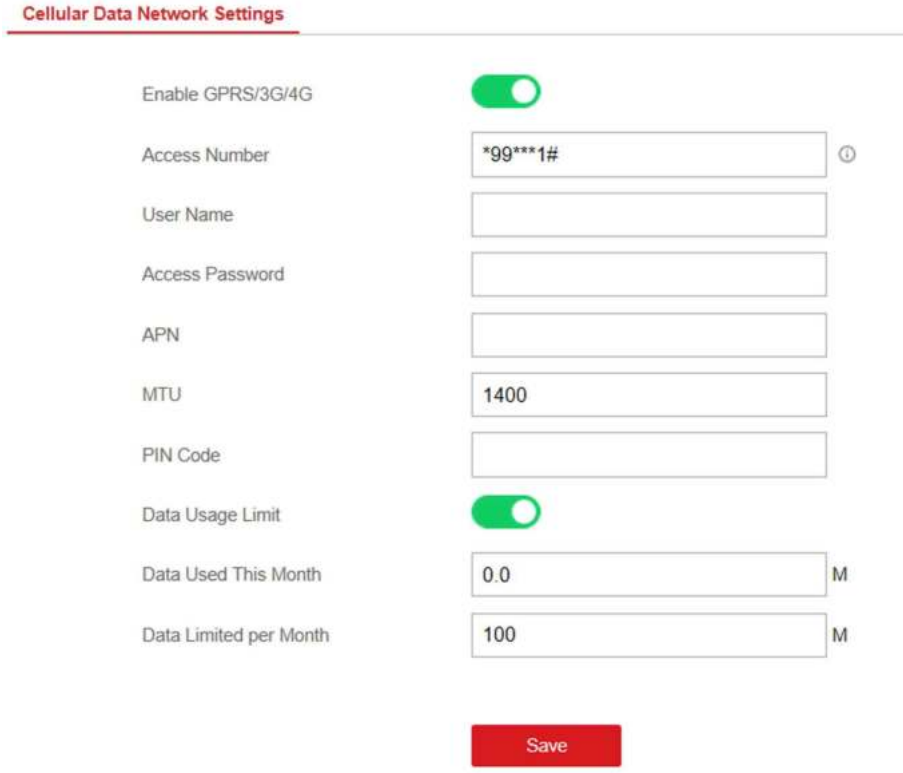


Figure 4-4 Cellular Data Network Settings Page

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 and mobile client.

Data Used This Month

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

4. Click **Save**.

Alarm Center

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

Steps

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

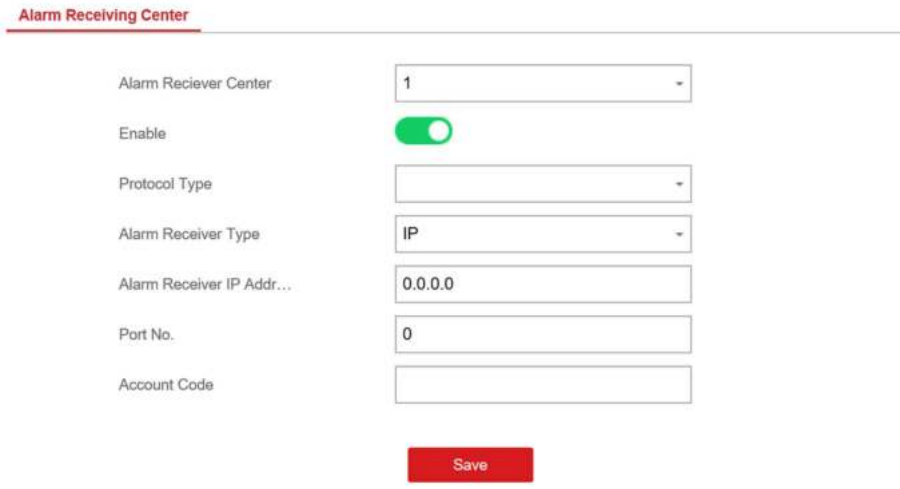


Figure 4-5 Alarm Receiving Center Parameters

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

Note

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

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

Note

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

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

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

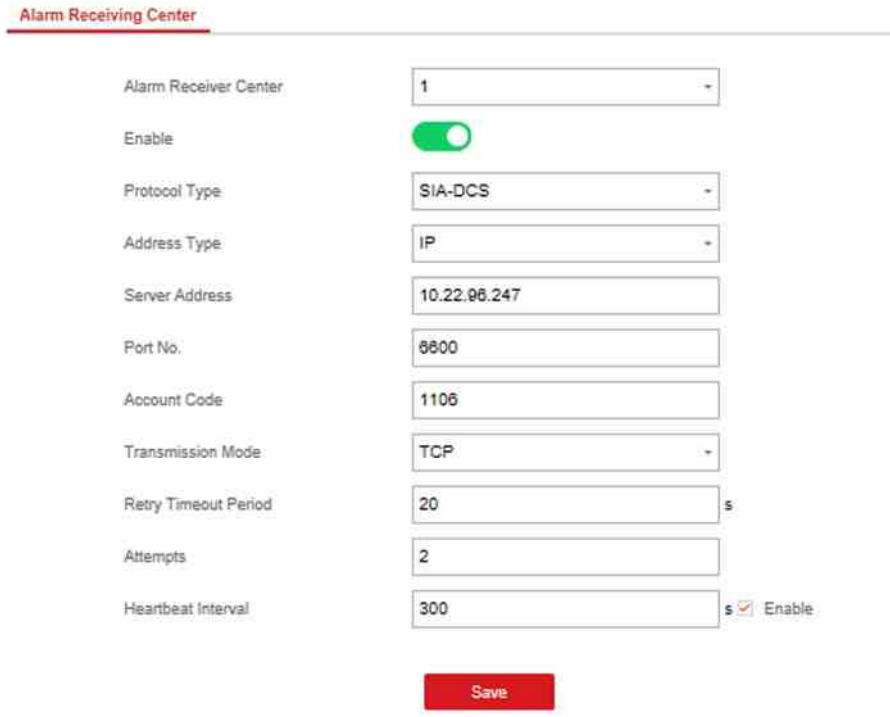


Figure 4-6 SIA-DCS

Note

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

- **EHome**

  You do not need to set the EHome protocol parameters.

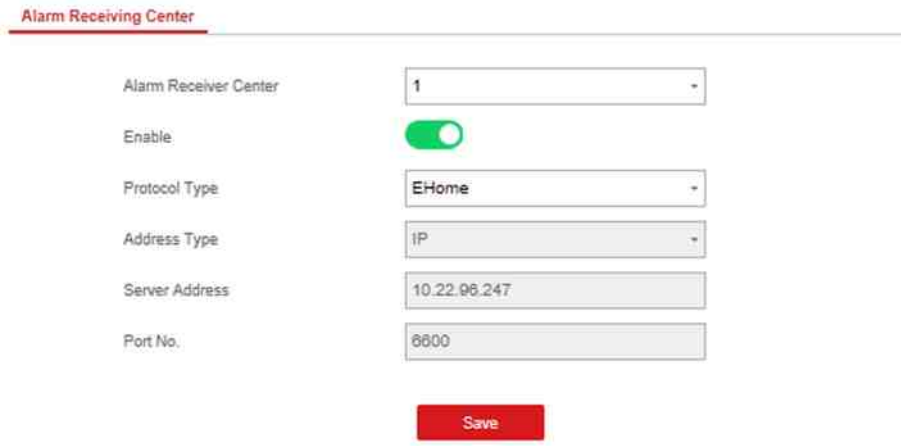


Figure 4-7 EHome

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

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

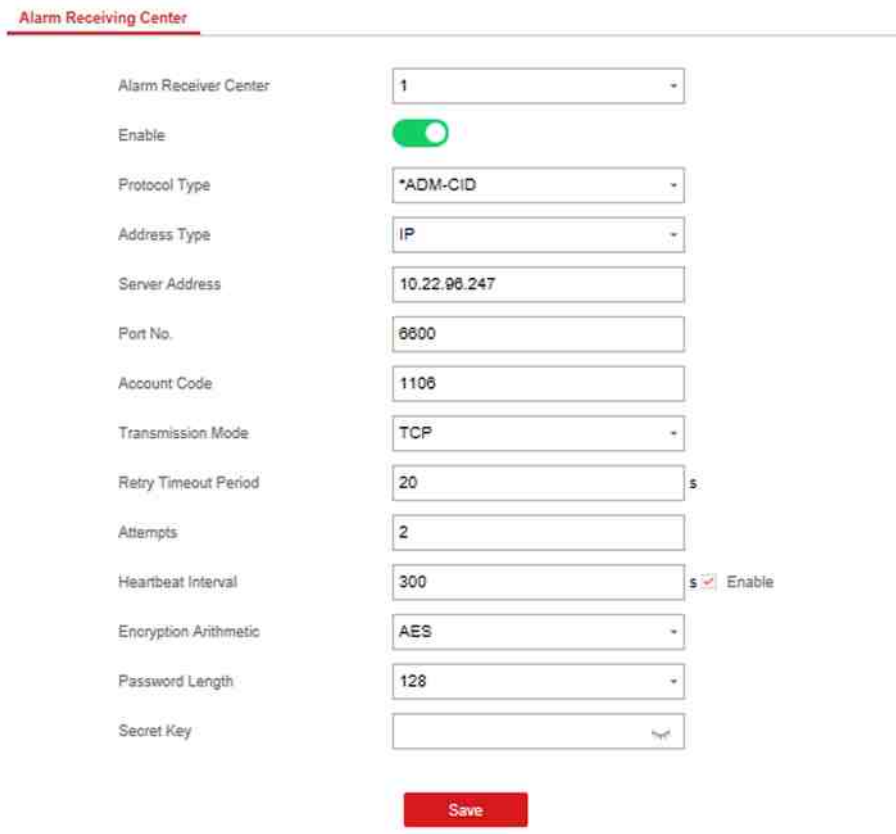


Figure 4-8 *ADM-CID

Note

Set the heartbeat interval with the range from 10 to 3888000 seconds.
For encryption arithmetic: The panel support encryption format for information security according to DC-09, AES-128, AES-192 and AES-256 are supported when you configure the alarm center.
For the secret key: When you use an encrypted format of DC-09, a key should be set when you configure the ARC. The key would be issued offline by ARC , which would be used to encrypt the message for substitution security.

4. Click **Save**.

Notification Push

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

Steps

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

Alarms and Tampers

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

Life Safety Alarms

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

Maintenance and Faults

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

Panel Management 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**, **Mobile Phone Number** , and check the **Notification Type**.

Note

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

3. Click **Save**.

Result

Table 4-1 Options of Notifications

Option	Notification
iVMS-4200	Alarms and Tampers Life Safety Alarms Maintenance and Faults Panel Management Notification
Alarm Receiver Center	Alarm Receiver Center 1&2 Alarms and Tampers Life Safety Alarms Maintenance and Faults Panel Management Notification
Cloud	Alarms and Tampers Life Safety Alarms Maintenance and Faults Panel Management Notification
Mobile Phone	Mobile Phone Index 1 to 6 Mobile Phone Number

Option	Notification
	Notification Type SMS & Voice Call Check Box Alarms and Tampers Life Safety Alarms Maintenance and Faults

Mobile Client Registration

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

Before You Start

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

Steps

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

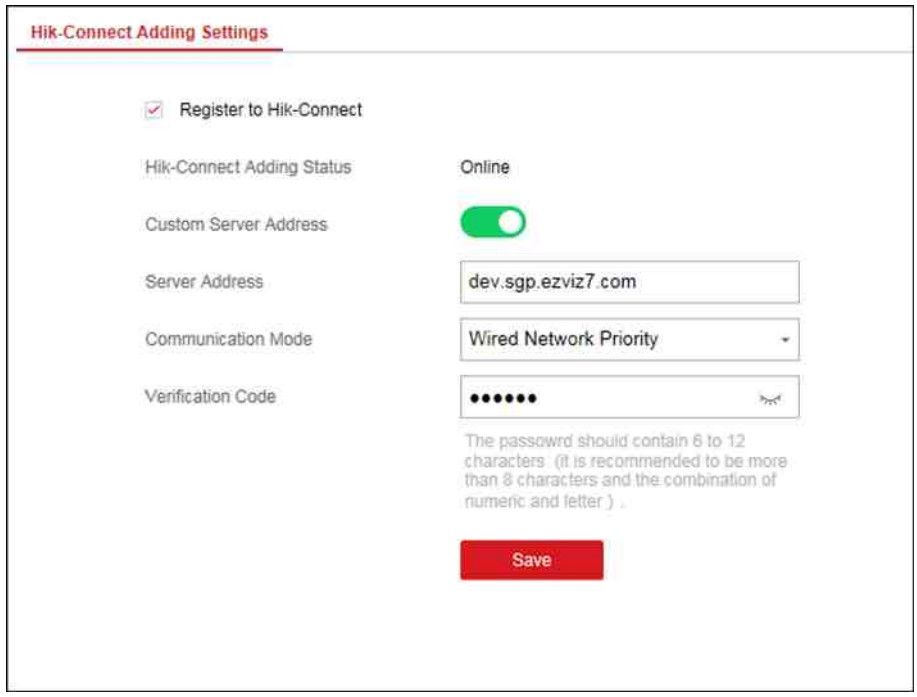


Figure 4-9 Hik-Connect Registration Settings Page

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

Note

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

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

3. Enable **Custom Server Address**.

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

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

   Auto

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

   Wired Network & Wi-Fi Priority

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

   Wired &Wi-Fi

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

   Cellular Data Network

   The system will select cellular data network only.

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 Registration** to enter the Ehome Registration Settings page.

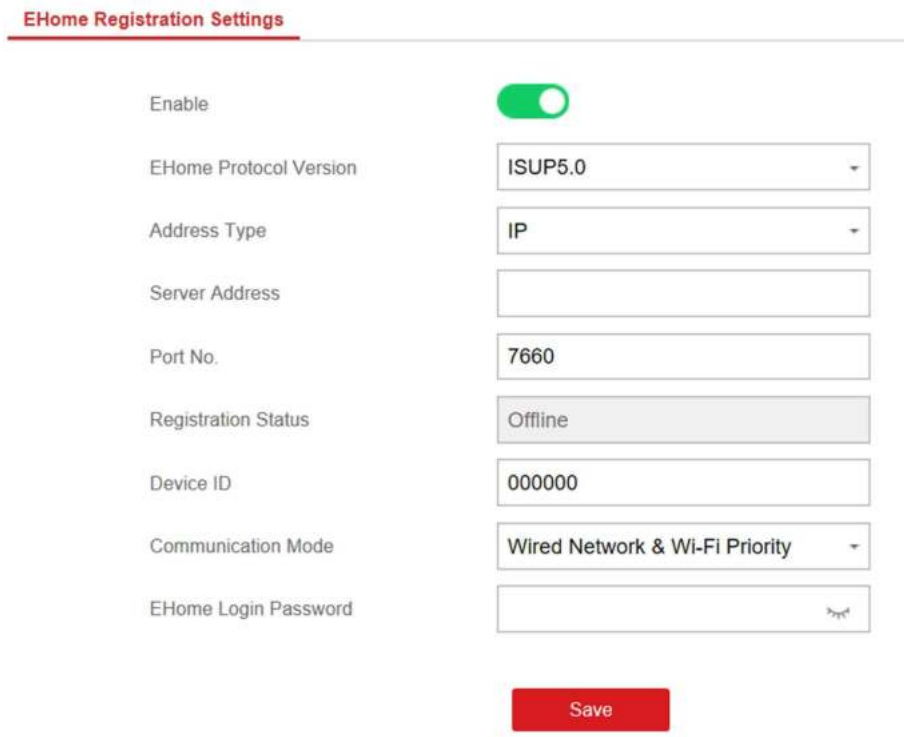


Figure 4-10 EHome Registration

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

Note

By default, the port number for EHome is 7660.

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

Auto

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

Wired Network & Wi-Fi Priority

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

Wired &Wi-Fi

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

Cellular Data Network

The system will select cellular data network only.

8. Click **Save**.

NAT

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

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

Steps

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

Figure 4-11 NAT Settings

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

4.3.2 Device Management

Zone

You can set the zone parameters on the zone page.

Steps

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

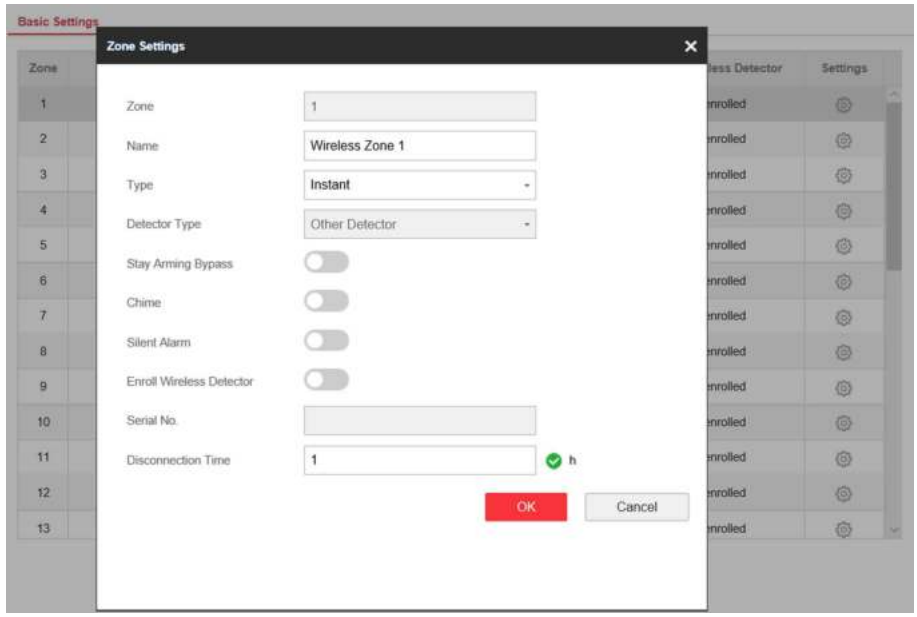


Figure 4-12 Zone Page

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

Instant Zone

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

Delayed Zone

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

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

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

Note

You can set 2 different time durations in **Partition Management → Schedule & Timer** . Ensure that timer is no longer than 45 seconds in order to comply with EN50131-1.

Follow Zone

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

Perimeter Zone

The system will immediately alarm when it detects a triggering event after the system is armed. There is a configurable interval timer between the alarm activation and siren output "Siren Delay Time (Perimeter Alarm) 0 to 600 Seconds". This option allows you to check the alarm and cancel the siren output during the interval time in case of false alarm.

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

Silent Panic Zone

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

Panic Zone

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

Fire Zone

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

Gas Zone

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

Key Zone

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

Disabled Zone

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**, **Chime**, or **Silent Alarm** according to your actual needs.

Note

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

6. Enable **Enroll Wireless Detector**, enter the serial No., and set the linked camera No.

Note

868 Devices do not support inputting serial No.

7. Set the **Disconnection Time**, and the system determines connection fault if the disconnected duration of the device is longer than the configured value.
8. Click **OK**.

Note

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

Note

Under the System Options of the Engineer Axiom Web platform there is an option called Early Alarm, this must be disabled for Sweden.

Output

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

Steps

1. Click **Device Management → Relay** to enter the Output page.
2. Add a wireless output module.
   1) Click **Wireless Output Module**.

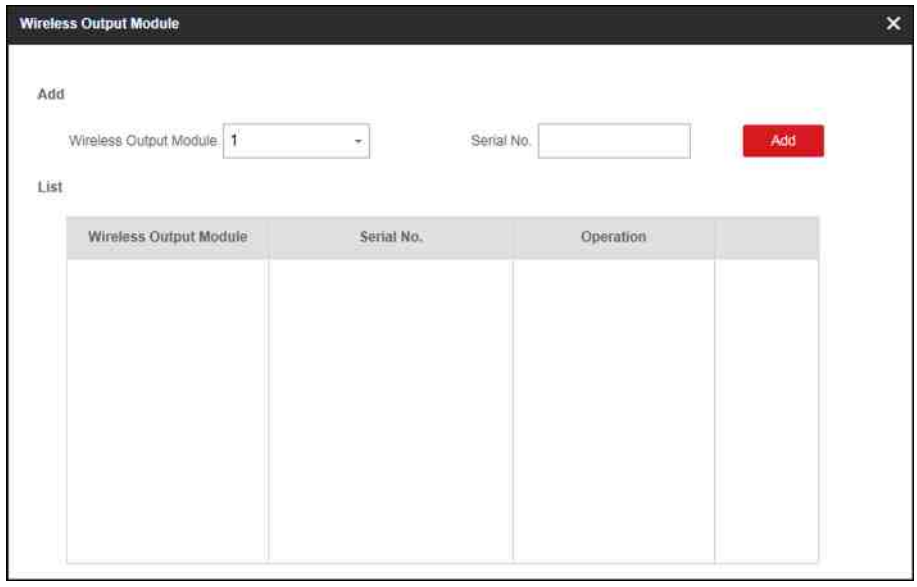


Figure 4-13 Wireless Output Module Settings

   2) Select a wireless output module number from the drop-down list.
   3) Input the serial No. of the wireless output module.

Note

The device in 868 MHZ may not support adding with serial No..

4) Click **Add**.

3. Click and the Output Settings window will pop up.

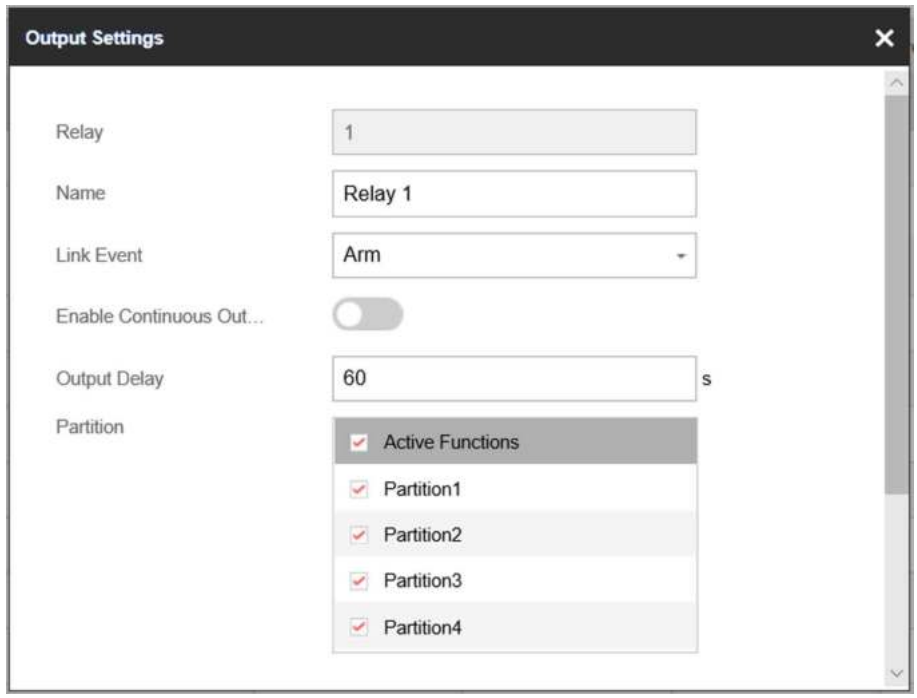


Figure 4-14 Output Settings

4. Edit the relay name and select a link event.

Note

You should set different parameters according to different linked events.

5. Enable **Enable Continuous Output** or set the output delay time.

Note

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

6. Check **Event Sub-Type** (Only for **Alarm** event).

7. Check partitions linked to the relay. (**Zone** and **Manual** event do not have this parameter.)

8. Click **OK**.

Note

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

Siren

The siren is enrolled to the control panel via the wireless receiver module, and the 868 Mhz wireless siren can be enrolled to the hybrid control panel via the wireless receiver that is at the address of 9.

Steps

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

Figure 4-15 Siren Page

2. Click ⚙ to enter the Siren Settings page.

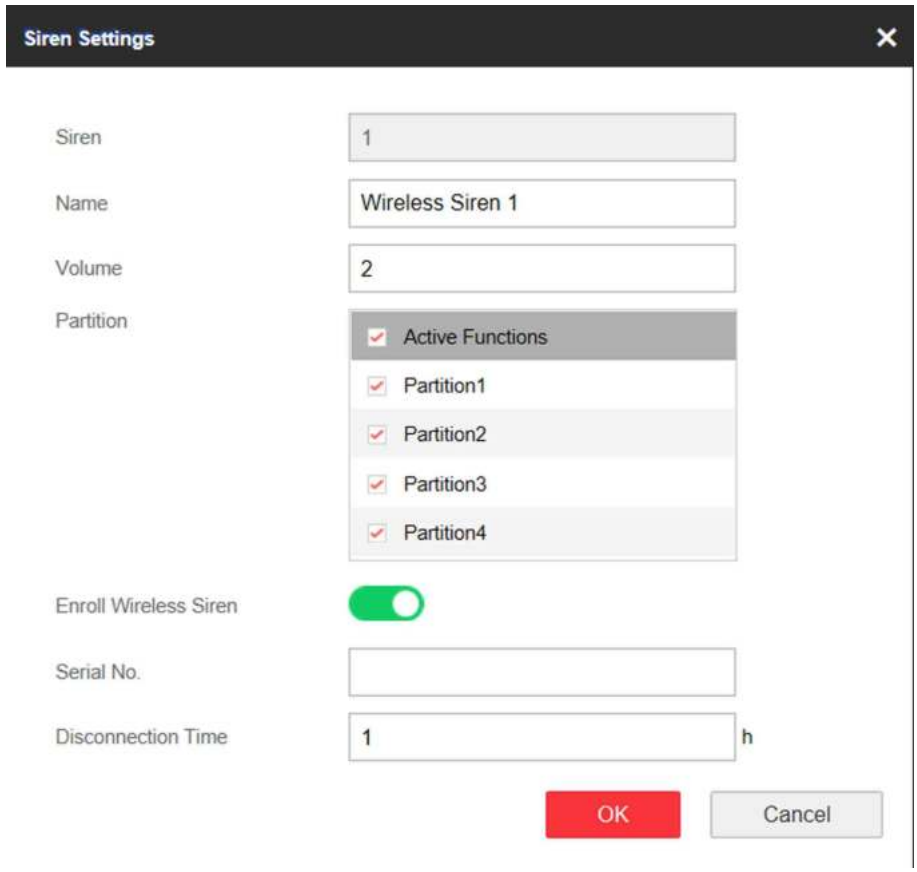


Figure 4-16 Siren Settings

3. Set the siren name and the volume.

Note

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

4. Check linked partitions.
5. **Optional:** Enable **Enroll Wireless Siren** and set the siren serial No.

Note

The siren in 868 MHZ may not support this function.

6. Set the **Disconnection Time**, and the system determines connection fault if the disconnected duration of the device is longer than the configured value.
7. Click **OK**.

Note

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

Keypad

You can set the parameters of the keypad that is enrolled to the control panel.

Steps

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

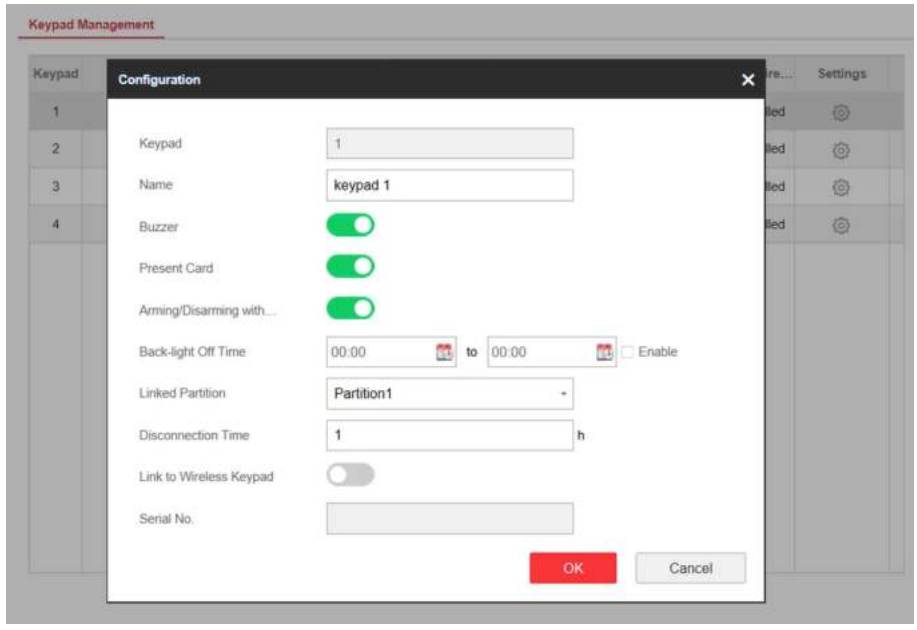


Figure 4-17 Keypad Settings Page

3. Set the keypad name.

4. Check the check box to enable the function of buzzer, presenting card, and arming/disarming with keypad.
5. Check the **Enable** check box of Back-light Off Time, and set the duration of light off.
6. Select the keypad linked partition.
7. **Optional:** Enable **Link to Wireless Keypad** and set the serial No.

Note

The keypad in 868 MHZ may not support this function.

8. Set the **Disconnectin Time**, and the system determins connection fault if the disconnected duration of the device is longer than the configured value.
9. Click **OK**.

Note

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

Card Reader

You can set the parameters of the card reader that is enrolled to the control panel.

Steps

1. Click **Device Management → Card Reader** to enter the page.

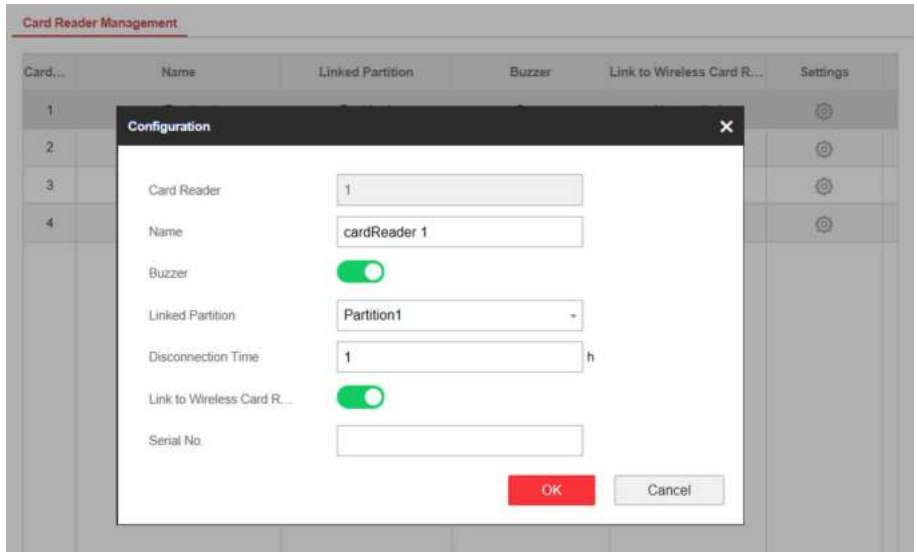


Figure 4-18 Card Reader Settings

2. Click ⚙ to enter the reader settings page.
3. Set the card reader name.
4. Enable **Buzzer**.
5. Select the keypad linked partition.

6. Set the **Disconnection Time**, and the system determines connection fault if the disconnected duration of the device is longer than the configured value.
7. **Optional:** Enable **Link to Wireless Card Reader** and set the serial No.

Note

The card reader in 868 MHZ may not support this function.

8. Click **OK**.

Note

- All zones are added to the partition 1 by default
- After the keypad is configured, you can click **Status → Keypad** to view the keypad status.

4.3.3 Partition Settings

Basic Settings

You can link zones to the selected partition.

Steps

1. Click **Partition Management → Basic Settings** to enter the page.

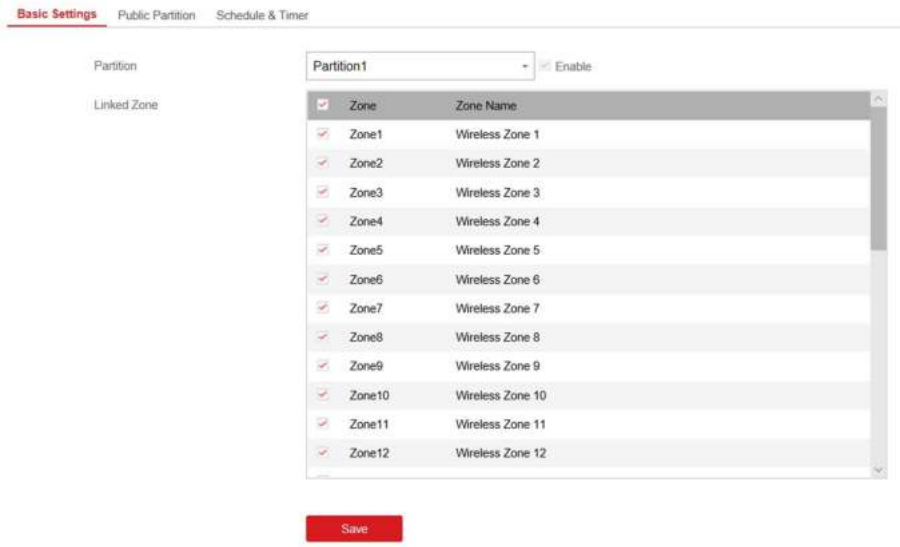


Figure 4-19 Partition Basic Information Management Page

2. Select a partition.
3. Check **Enable**.
4. Check the check box in front of the zone to select zones for the partition.
5. Click **Save** to complete the settings.

Public Partition Settings

Definition Public partition is considered a special one which can be shared to other partitions. It is usually applied to manage or control the public area related with other areas controlled by other partitions in one building.

Steps

1. Click **Partition Management → Public Partition** to enter the page.

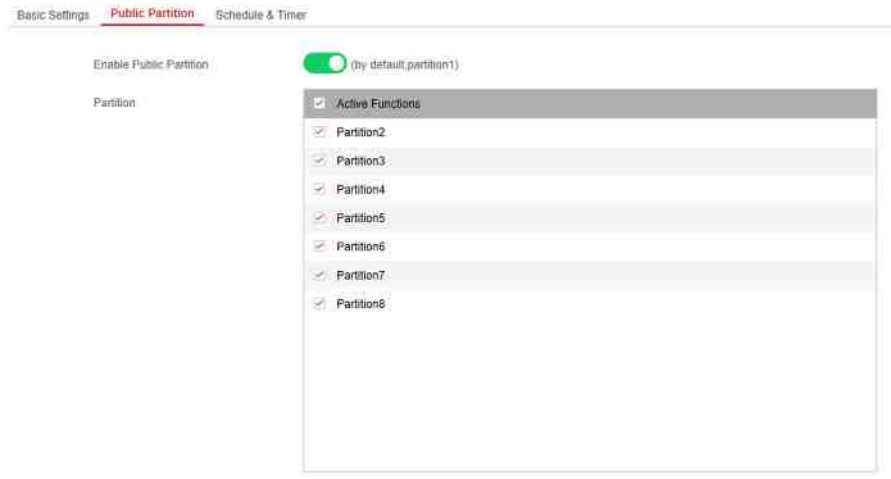


Figure 4-20 Public Partition Settings

2. Check the checkbox to enable the public partition function.

Note

the default public partition is partition 1

3. Select partition(s) to link to the public partition in the list.

Note

It is required to select at least a partition to link to the public paritition.

4. Click **Save** to set the partition as public partition.

Schedule and Timer Settings

You can set the **Entry Delay 1** & **Entry Delay 2** time duration for the delayed zone type and the Exit Delay 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 **Partition Management → Schedule & Timer** to enter the Schedule & Timer page.

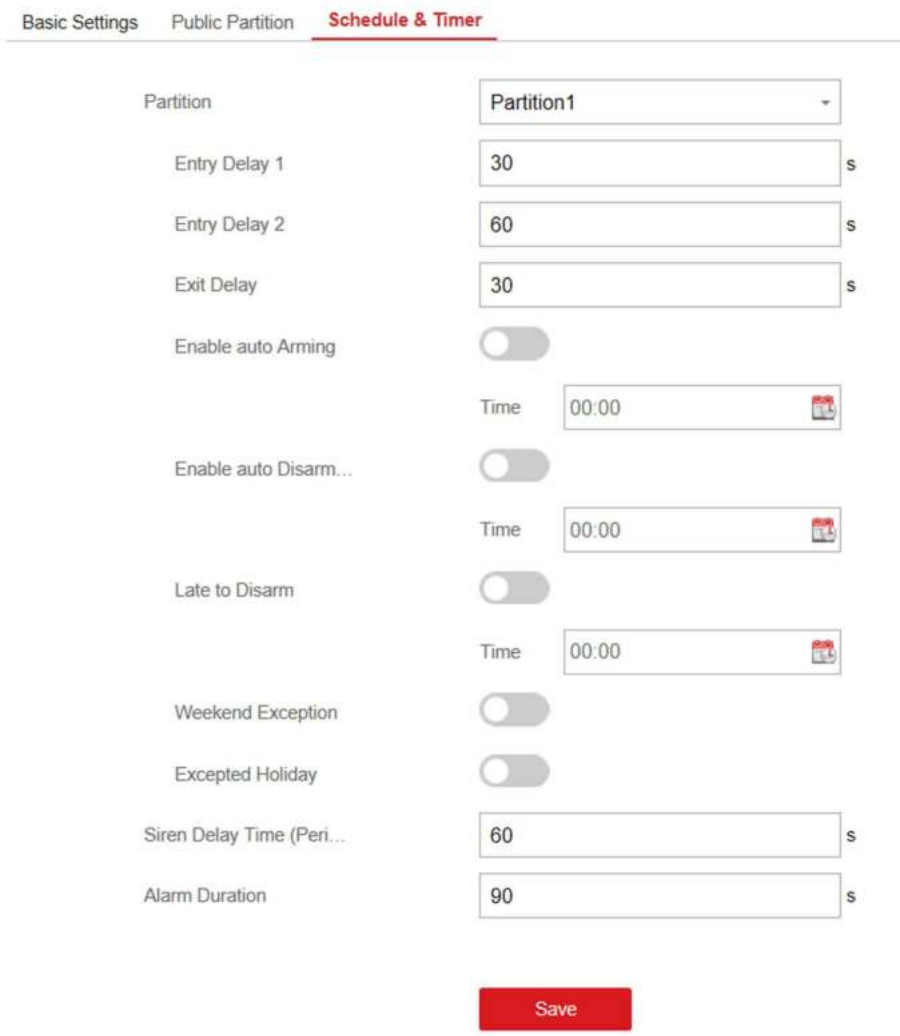


Figure 4-21 Schedule & Timer Settings

2. Select a partition.
3. Set time duration of **Entry Delay 1**, **Entry Delay 2**, or **Exit Delay** respectively.

Entry Delay 1/Entry Delay 2

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

Note

The available time duration range is from 1 s to 600 s.

Exit Delay

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

Note

The available time duration range is from 1 s to 600 s.

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

Enable 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.
- The buzzer beeps slowly 2 minutes before the auto arming starts, and beeps rapidly 1 minute before the auto arming starts.
- You can select to enable forced arming on the System Options page. While the function is enabled, the system will be armed regardless of the fault.
- If the public partition is enabled, the partition 1 dose not support auto arming.

Enable 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.
- If the public partition is enabled, the partition 1 dose not support auto disarming.

Late to Disarm

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

Note

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

Weekend Exception

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

Excepted Holiday

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

Note

Up to 6 holiday groups can be set.

Siren Delay Time (Perimeter Alarm)

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

If you have set the perimeter zone, you can set the time duration of the alarm.

Note

The available time duration range is from 1 s to 900 s.

5. Click **Save**.

4.3.4 Video Management

You can add two network cameras to the 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.

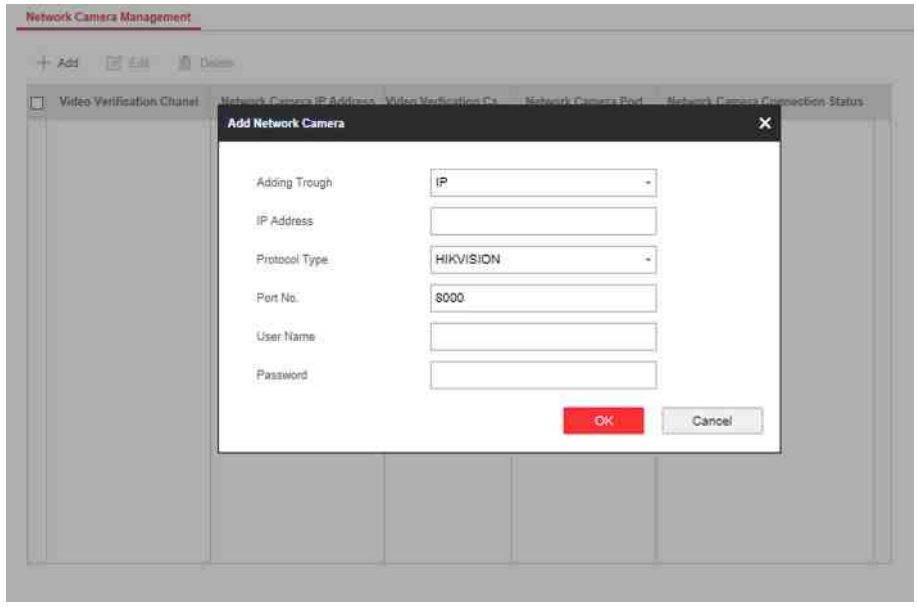


Figure 4-22 Network Camera Management

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

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

Link a Camera with the Zone

Steps

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

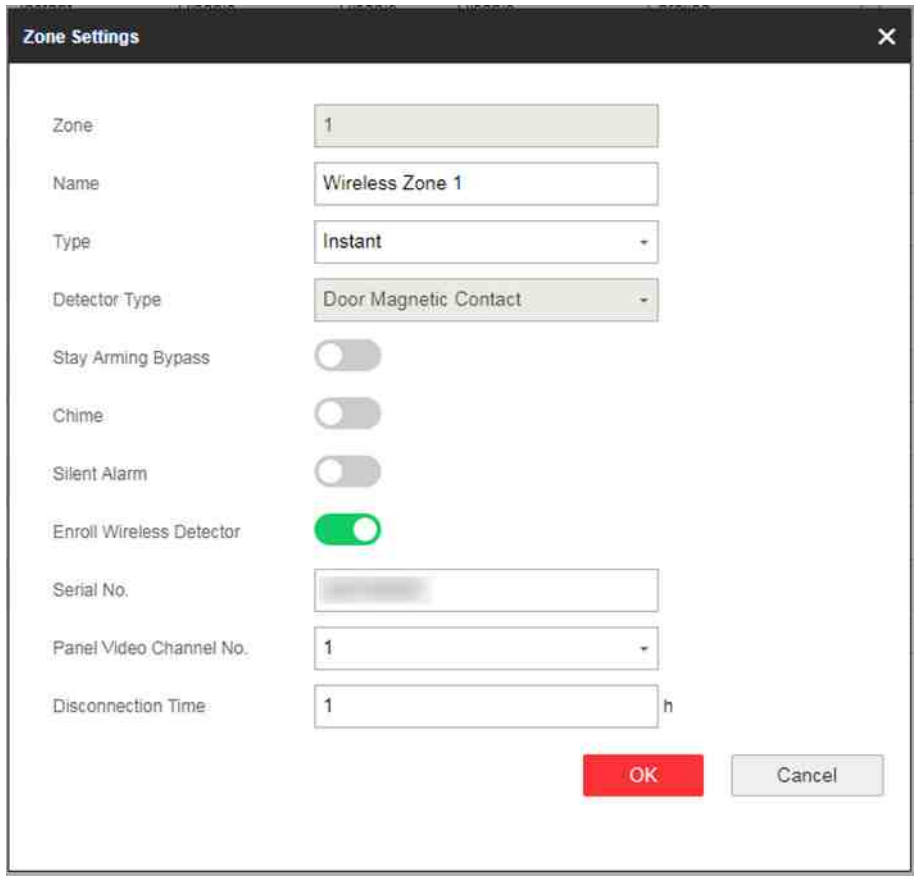


Figure 4-23 Zone Settings

3. Select the **Panel Video Channel 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 → Video Verification Events** to enter the page.

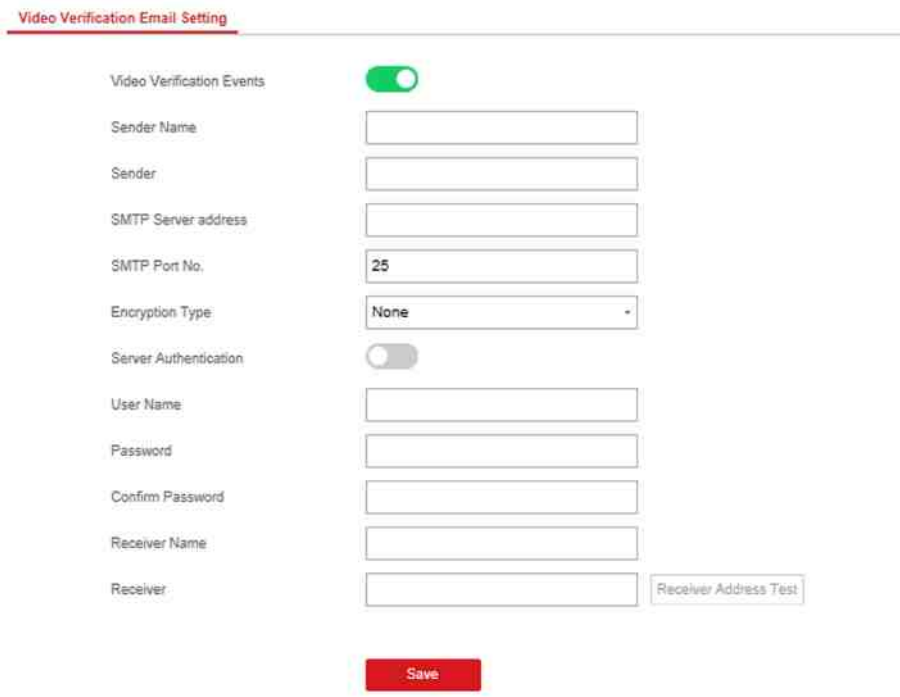


Figure 4-24 Set Email to Receive Alarm Video

2. Click the block to enable the function.
3. Enter the sender's information.

Note

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

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

Set FTP to Save Video

You can configure the FTP server to save alarm video.

Steps

1. Click **Communication Parameters → FTP** to enter the page.

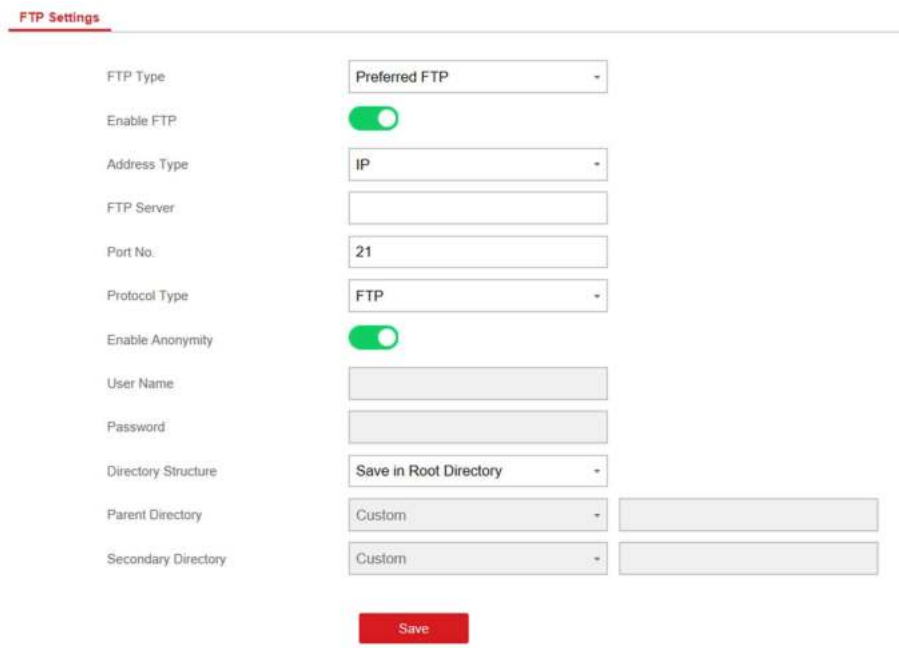


Figure 4-25 FTP Settings

2. Select **FTP Type**.
3. Drag the slider to enable FTP.
4. Select address type as **Domain Name** or **IP**.
5. Enter the domain name or FTP server.
6. Enter port number, user name and password.
7. **Optional:** Drag the slider to enable anonymity.
8. Set **Directory Structure** as the saving path of snapshots in the FTP server.
9. Click **Save**.

Set Video Parameters

Steps

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

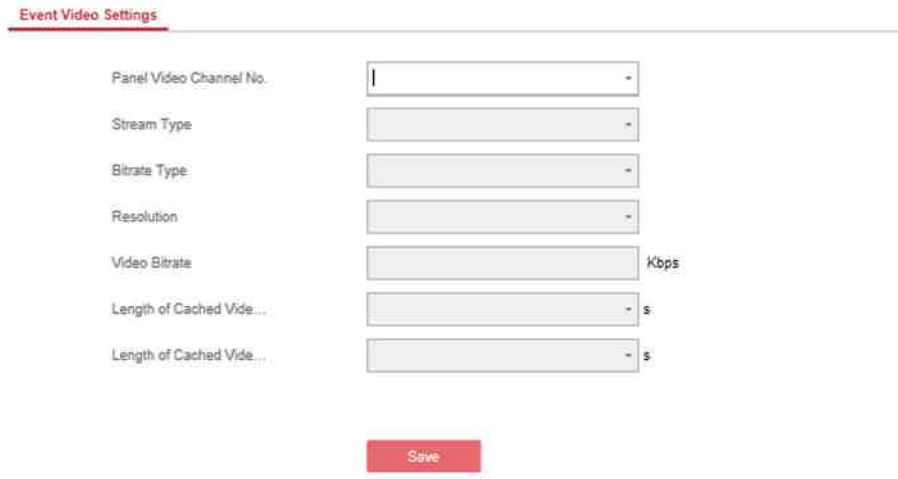


Figure 4-26 Video Settings

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.

Bitrate Type

Select the Bitrate type as constant or variable.

Resolution

Select the resolution of the video output.

Video Bitrate

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

4.3.5 Permission Management

Add/Edit/Delete 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.

2. To compliant the EN requirement, slide the block to enable the installer and manufacturer .

Note

- The default password of the **installer** is **installer12345**, and the default password of the **manufacturer** is **hik12345**. These codes will have to be changed when first connected.
- The Italian user name of admin is **admin**.

Table 4-2 User Name of Installer

Language	User Name	Language	User Name
English	installer	Russian	монтажник
Italian	installatore	French	installateur
Polish	instalator	Spanish	instalador
German	errichter	Portuguese	instalador
Turkish	kurulumcu	Czech	technik

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.

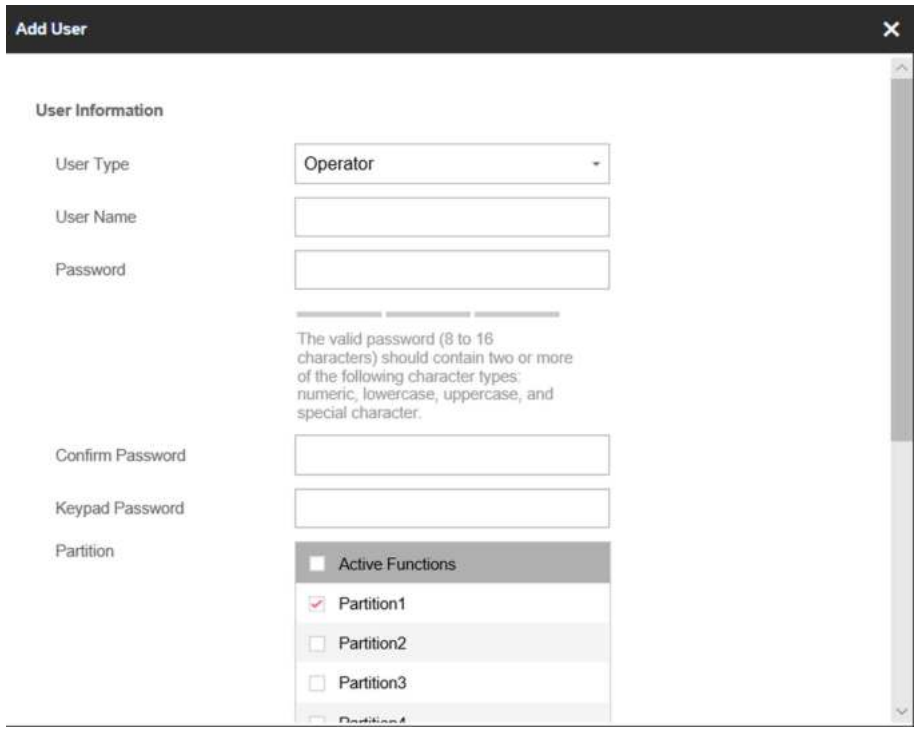


Figure 4-27 Add User Page

5. Set the keypad password (numeric, 8~16 characters).

Note

The keypad password +1 or -1 is the duress code. Use the duress code can operate the keyboard to arm and disarm normally and upload a duress alarm. For example, if the keypad password is 123456, the duress code is 123455 or 123457

6. Check partitions
7. Check the check boxes to set the user permission.

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

Note

The admin, the installer and the manufacture cannot be deleted.

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.

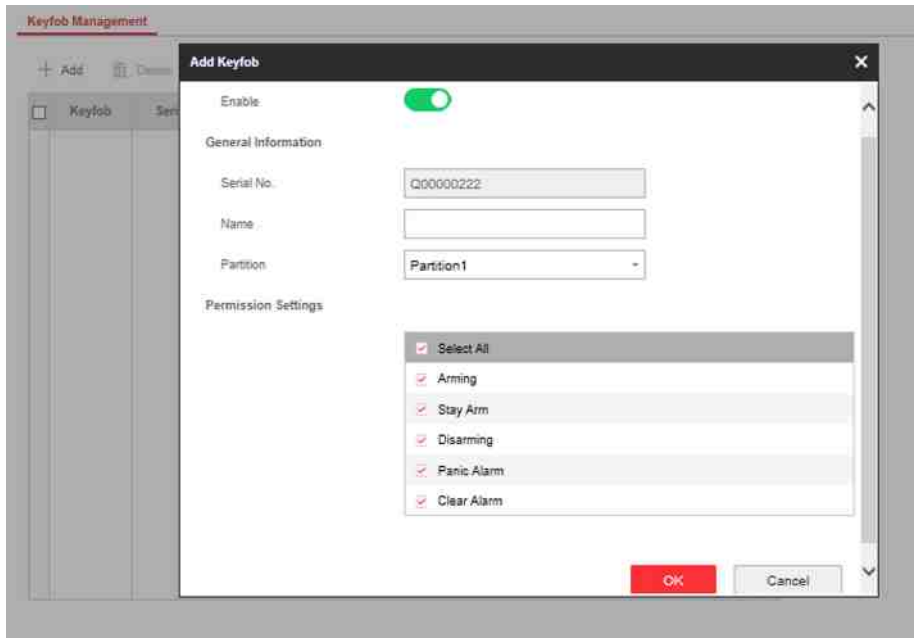


Figure 4-28 Keyfob Management

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 Card

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

Steps

1. Click **User Management → Card** to enter the management page.
2. Click **Add** and place a card on the card area of the control panel.

3. Customize a name for the card in the pop-up window.
4. Select the card type and card linked partition.
5. Select the permission for the card.

Note

You should allocate at least a permission for the card.

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

Note

The card supports at least 20-thousand serial numbers.

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

4.3.6 Maintenance

Test

The security control panel supports walk test function.

Steps

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

Note

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

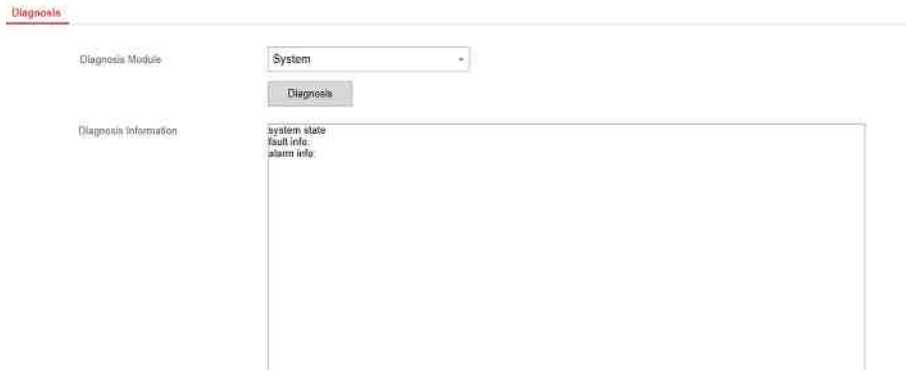
2. Check the **Test** check box to start walk test.
3. Click **Save** to complete the settings.
4. Trigger the detector in each zone.
5. Check the test result.

Diagnosis

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

Steps

1. Enter **Maintenance → Diagnosis** .



2. Select system, alarm, wireless device, Wi-Fi, cloud platform, cellular data network, network camera and alarm receiving center as the diagnosis module. Or you can select**Custom**, and enter the custom command (1~64) characters.
3. Click **Diagnosis** to start the operation.
4. View the diagnosis result in the information box.

Export File

You can export debugging file to the PC.

Steps

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

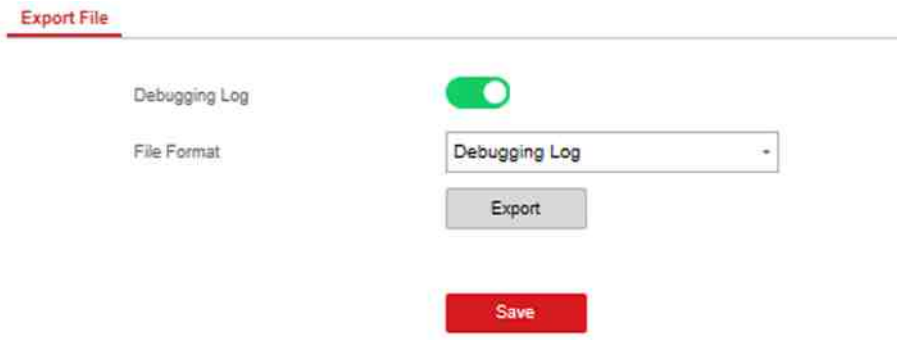


Figure 4-29 Export File Page

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